II МІЖНАРОДНА НАУКОВО-ПРАКТИЧНА КОНФЕРЕНЦІЯ

# *"ІНФОРМАЦІЙНА БЕЗПЕКА ТА КОМП'ЮТЕРНІ ТЕХНОЛОГІЇ"*

*INFOSEC & COMPTECH*

**м. Кропивницький, 20-22 квітня 2017 року**


## ЗБІРНИК ТЕЗ ДОПОВІДЕЙ

ЦЕНТРАЛЬНОУКРАЇНСЬКИЙ НАЦІОНАЛЬНИЙ
ТЕХНІЧНИЙ УНІВЕРСИТЕТ

МЕХАНІКО-ТЕХНОЛОГІЧНИЙ ФАКУЛЬТЕТ

КАФЕДРА ПРОГРАМУВАННЯ ТА ЗАХИСТУ ІНФОРМАЦІЇ

ЗБІРНИК ТЕЗ ДОПОВІДЕЙ

ІІ МІЖНАРОДНОЇ НАУКОВО-ПРАКТИЧНОЇ КОНФЕРЕНЦІЇ

# *"ІНФОРМАЦІЙНА БЕЗПЕКА ТА КОМП'ЮТЕРНІ ТЕХНОЛОГІЇ"*

*INFOSEC & COMPTECH*

20-22 квітня 2017 року

м. Кропивницький

УДК 004

Інформаційна безпека та комп'ютерні технології: Збірник тез доповідей ІІ Міжнародної науково-практичної конференції, 20-22 квітня 2017 року, м. Кропивницький: ЦНТУ, 2017. – 211 с.

Збірник містить тези доповідей за матеріалами ІІ Міжнародної науково-практичної конференції "Інформаційна безпека та комп'ютерні технології", що відбулась 20-22 квітня 2017 року на базі кафедри програмування та захисту інформації Центральноукраїнського національного технічного університету.

## *ОРГАНІЗАЦІЙНИЙ КОМІТЕТ КОНФЕРЕНЦІЇ*

***Голова*** – **Левченко О.М.**, д.е.н., професор, проректор з наукової роботи Центральноукраїнського національного технічного університету.

***Заступники голови:***
**Смірнов О.А.**, д.т.н. професор, завідувач кафедри програмування та захисту інформації Центральноукраїнського національного технічного університету;
**Мелешко Є.В.**, к.т.н., доцент, доцент кафедри програмування та захисту інформації Центральноукраїнського національного технічного університету;
**Якименко М.С.**, к.ф.-м.н., доцент, доцент кафедри програмування та захисту інформації Центральноукраїнського національного технічного університету.

***Відповідальні секретарі:***
**Конопліцька-Слободенюк О.К.**, викладач кафедри програмування та захисту інформації Центральноукраїнського національного технічного університету;
**Константинова Л.В.**, викладач кафедри програмування та захисту інформації Центральноукраїнського національного технічного університету.

***Члени оргкомітету:***
Карпінський М.П., д.т.н., професор (м. Бельсько-Бяла, Польща).
Сєйлова Н.А., к.т.н. (м. Алмати, Казахстан).
Корченко О.Г., д.т.н., професор (НАУ, м. Київ).
Бурячок В.Л., д.т.н., с.н.с. (ДУТ, м. Київ).
Лахно В.А., д.т.н., доцент (ЄУ, м. Київ).
Кузнецов О.О., д.т.н., професор (ХНУ, м. Харків).
Семенов С.Г., д.т.н., професор (НТУ "ХПІ", м. Харків).

***Адреса редакційної колегії:***
25030, м. Кропивницький, пр. Університетський, 8,
Центральноукраїнський національний технічний університет,
тел.: (0522)390-449.

*Відповідальна за випуск:* Мелешко Є.В.

# ЗМІСТ

*Секція 1.*
***Інформаційна безпека держави, суспільства та особистості***

UDC 004.056

## Multidisciplinary problems of big data in information security

Aliguliyev R.M.[1], doctor of science,
Imamverdiyev Y.N.[2], PhD in tech. sciences,
Hajirahimova M. Sh.[3], PhD in tech. sciences
[1,.2,.3]*Institute of Information Technology of ANAS, Baku, Azerbaijan*

Recently, big data is becoming a strategic resource in many fields, and researchers draw attention to its new security challenges along with its benefits. Problems of big data and information security could be considered from two aspects: application of big data analytics to information security and information security of big data [1]. The main information security research areas are the followings: detection of cyber-attacks including DDoS attacks; detection of botnets; detection of malware; web security; management of information security risks; evaluation of information security; management of information security incidents. The paper aims to analyze multidisciplinary problems of big data in above-mentioned research fields.

**Security challenges of big data.** Access to big data while transferring in networks makes threats real such as capturing, changing, falsification of information by hackers. Also threats to the national security requires reduction of vulnerabilities and providing effective cybercrime fight by new advanced tools. For solving these problems interdisciplinary research approach is required, including fields such as mathematics, computer science, information security, cryptography, law and so on. In order to clearly understand the security of big data, the Cloud Security Alliance, a working group which studies big data security issues, suggests ten problems on the four various directions: infrastructure security, data privacy, data management, and reactive security. Compared with traditional information security problems (confidentiality, integrity and availability of information) security problems of big data are explained by the following features: big data usage increases privacy leakage; big data becomes a carrier of Advanced Persistent Threats (APTs), which are sophisticated, longterm, multiphase attacks targeting a particular organization.

Big Data lets us expand the data sources we use for processing, but it's hard to be certain that each data source meets the trustworthiness that our analysis algorithms require to produce accurate results. Therefore, we need to reconsider the authenticity and integrity of data used in our tools.

Access control is very important in dealing with big data. Due to the high number of users and dynamic change of authority in big data enviroments, implementing role based access control s is inefficient. More valid control mechanisms should be adopted for the ssecurity of data [2].

Big data introduces new ethical and legal challenges related to security and

privacy. As Data Mining technology evolves and becomes widely used, acquisition of more in-depth knowledge from big data poses a threat to the protection of extremely sensitive personal data [3]. We need to develop high speed encryption methods and multi-level security models for big data.

**Big data analytics challenges in security.** Data analysis technologies emerged from the intersection of sciences (computer sciences, statistics and mathematics). Several approaches like database management, data mining, text mining, web mining, NLP, knowledge management, machine learning and etc. are used for finding regularities in data and knowledge discovery. For improving the quality of data and results of data analysis data must undergo through pre-processing stage. Since data is generally collected from variety of sources, there are usually contradictions, incompleteness, and "noise" in data. Therefore, big data collection, cleaning, dimensionality reduction, transformation, and integration is very important pre-processing methods.

Big data analytics allows detection of abnormal behavior in the network in early stage, and preventing security incidents in time. Big data analytics differs from traditional threat detection systems, it predicts security incidents such as APT attacks, and enhances situational awareness, allows early detection of threats and risky behaviors, automated response to incidents, and better investigation of them; restore from incidents in a short time and with minimal costs. Considering high possibility of new security incidents may occur, we can detect unknown security incidents by big data analytics [4].

**Conclusion**

In recent years, in data-centric world, big-data processing and analytics have become an important tool for information security. Big Data problems in the field of information security are: privacy protection, Big data analytics for information security; high-speed cryptography; Big data collections for tests/scientific research; visualization for information security; fostering hacker-minded Data Scientists.

This work was supported by the Science Development Foundation under the President of the Republic of Azerbaijan – **Grant № EIF-KETPL-2-2015-1(25)-56/05/1**

**References**

1. Aliguliyev R.M., Hajirahimova M.Sh. "Big data" phenomenon: Challenges and Opportunities // Information Technology Problems, 2014, No 1, pp. 3-16.
2. Tene O., Polonetsky J. Big Data for all: Privacy and user control in the age of analytics // Northwestern Journal of Technology and Intellectual Property, 2013, vol.11, no.5, pp.239–273
3. Buczak A.L., Guven E. A survey of Data Mining and Machine Learning methods for cyber security intrusion detection //IEEE Communications Surveys & Tutorials, 2016, vol. 18, no. 2, pp.1153-1176
4. Wang J., Rossell D., etal. Network anomaly detection: A survey and comparative analysis of stochastic and deterministic Methods. https://arxiv.org/pdf/1309.4844.pdf

UDC 004.056

**Consensus ranking method of information security threats of a nation state**

Imamverdiyev Y.N., PhD in tech. sciences
*Institute of Information Technology of ANAS, Baku, Azerbaijan*

Threats to information security of nation states are directed against the national interests in the information sphere. According to experts, there was a significant expansion of the list of information security threats to nation states [1]. If a decade ago, threats were mainly economic in nature, now cyber threats to political, social, and military spheres are emerging. For an effective response against these threats, under limited resources, allocated for the cyber-defence, ranking of these threats is required. Despite the theoretical and practical significance of the issue, literature review shows that, a common approach to ranking of information security threats of nation states has not yet developed. Only few papers mainly consider the mentioned issue for organizations. The paper aims to develop an approach to ranking of information security threats tonation states.

**Threat modeling** includes the following iterative steps (from a hypothetical attacker's point of view) – potential threat identification, threat assessment, and threat prioritization (ranking). Threat modeling provides defenders with information to decide on the most relevant threats and implement response measures to reduce potential impacts from these threats. Numerous IT threat modeling methodologies are available (for example, STRIDE methodology of Microsoft) [2]. Threats are identified by using core components of a threat: threat actors, attack types, and known vulnerabilities. Threat actors may include criminals, hacktivists, recreational hackers, etc. Attack types may include distributed denial-of-service (DDoS), cyber espionage, etc. Attacks are carried out through vulnerabilities, which may be unpatched software, high-profile employee, etc.

Threat ranking rating is evaluated by combination of threat likelihood and threat impact. Threat likelihood is determined basing on capability and intent of threat actors. And threat impact is measured through effects of attacks on an organization's operations and strategic interests.

**Ranking of a nation state information security threats** can be viewed at the operational, tactical and strategic levels, in the short- and long-term perspective. As example of operational threat ranking, Multi-State Information Sharing and Analysis Center (MS-ISAC) determines Cyber Threat level, which shows the current level of malicious cyber activity and the potential damage [3]. This study considers strategic threats; they may cause incidents on national scale.

**Statement of the research problem.** Suppose that list of security threats are compiled (based on official documents, scientific researches and mass

media publications). Suppose there are $n$ experts, each of which produces a ranking for the threats containing in the threats list. Experts give greater ratings to those threats which are more likely to occur and which would have greater impact. Assessment of threats could be carried out on a 6-point scale: 0 – No threat; 1 – Low; 2 – Moderate; 3 – Average; 4 – Significant; 5 – High.

The proposed methodology is based on the concept of minimizing the distance (disagreement) between individual rankings.

**Optimization-based weighted consensus ranking.** In general, the formulation can be described as follows.

Let $r_{ij}$ be the rank of the $i^{\text{th}}$ expert on the $j^{\text{th}}$ threat ($i$ =1, …, $n$ and $j$ =1, …, $m$). If $c^j$ is the weighted consensus rank for the $j^{\text{th}}$ threat and a vector of weights $w = (w_1, \ldots, w_n)$ assigned to the corresponding experts, then weighted consensus ranking can be represented by the following optimization problem:

$$\arg\min_{w,r} (1-\lambda)\sum_{i=1}^{n} w_i \left\| r_i - c \right\|^2 + \lambda \left\| w \right\|^2,$$

$$s.t. \quad \sum_{i=1}^{n} w_i = 1;\ w_i \geq 0 \quad \forall i.$$

where $0 \leq \lambda \leq 1$ is the regularization parameter which specifies the tradeoff between the minimization of the weighted distance and the smoothness of weights. For simplicity, we use Euclidean distance. This is a quadratic function optimization problem with linear constraints, and can be computed quickly [4].

**Conclusion.** Ranking of threats is a very important process for information security. It allows to determine priorities of appropriate measures within the allocated budget. In the proposed model threats are ranked based on impact on the national interests and likelihood of threats, where these parameters are determined from the expert assessment.

**References**

1. Jang-Jaccard J., Nepal S. A survey of emerging threats in cybersecurity // Journal of Computer and System Sciences, 2014, vol. 80, no. 5, pp. 973-993.

2. Swiderski S., Snyder W. Threat Modeling, Microsoft Press, July 2004.

3. Multi-State Information Sharing & Analysis Center (MSISAC). http://msisac.cisecurity.org/alert-level/

4. Wang D., Li T. Weighted consensus multi-document summarization // Information Processing and Management, 2012, vol. 48, pp. 513–523.

UDC 32.019.5:351.86

## Methodical approach to detecting signs of information-psychological influence in the mass media

Mikhieiev Y., commander research laboratory, Ph.D
*Zhytomyr Military Institute named S.P. Korolev, Zhytomyr*

One of the tasks that arises during the confrontation to the Russian Federation's hybrid aggression is the task of creating a system of prevention and protection against external informational threats. Such system should foresee the emergence of negative information-psychological influence, to determine its degree of threat, to neutralize it and to provide suggestions for further development of the situation to appropriate bodies of military administration.

During the analysis of messages received by the means of monitoring from the system, task of evaluating of their content arises concerning the presence of destructive information-psychological impact in given messages. This fact can identified only by list of certain characteristics that should become a mean for disclosing special information operations' purposes (actions, activities) of an enemy, characteristics of objects, through which the influence is made and manipulation techniques. Ensuring of implementation of given task is possible by taking into account characteristics of information-psychological impact in the messages.

In several cases characteristics of information-psychological impact may be detected by analyzing the theme of message. However, it is not always disclose the whole essence of message content, and especially its influential component. So for detecting the characteristics of special information operation (actions, activities) based on the results of messages classification it is expedient to take into account the peculiarities of conducting the information operation at each stage. The content of the main stages of special information operation is considered in the report, namely: planning phase, phase of information drive development, phase of studying the characteristics of the target audience, the stage of exit from information operation.

Methodical approach to detection of information-psychological influence in the system of prevention and protection from external informational threats has been grounded.

For this purpose the analysis of methods for practical determination of the information messages impact on subliminal social groups and individuals is conducted:

phonetic analysis based on the formation of semantic differential applied to speech sounds;

linguistic analysis of positive and negative effects of certain words on the meaningful value of text completely;

color-sound analysis;

neurolinguistic programming to determine the load on the main sensory channels of human perception.

The implementation of the process of detection and analysis of corresponding phonetic meanings of words with using semantic differential allows to conduct the analysis of texts for determining their direction (presence of suggestive aspects), which foresees the using the dynamic semantic archive.

An essential stage in the analysis of content for presence of hidden information-psychological influence is also analysis of information about the source (author) of message. If the message has the character of news, usually the source (author), which formed information about the event is indicated. Thus, a rating and relevance of the source (author) by certain characteristics are formed.

The characteristic of the fact that the message contains information-psychological influence is the absence of primary source. These sources generally have a high rating among users viewing and reflect the current state of the situation that is happening.

For fast availability the message should be in a content category that is defined by specialization of edition, headings and according to the lexical requests.

It is important to determine the geographic orientation of the message, which can be identified by certain characteristics (marked geographical objects, map of the town, address). Main criteria used in determining the significance of the information message are grounded:

the importance of a specific message: the time of creation; credibility of the source; corresponding the theme plot with specialization information agency;

dynamics of the plot: integrity of the stream of messages; the period of time for which the message is in top news.

The significance of the information source is determined by the following factors:

number of citations of the sources by other news media;

speed determines how quickly publication responds to an event.

It is necessary to consider the fact that at the stage of message placement groups of similar documents (duplicates) are defined. Then from each group one message (master message) is left that can be given on the pages of the message and as the result of the search. Master message is determined by the time of its publication on the site by the results of comparative analysis of texts, by hyperlinks on the source. Duplicates are usually not displayed and are not involved in the search.

Today, there are software tools for searching the duplicate news messages. It uses algorithms that analyze relationships of message with headings and part of the text.

The result of research is formed activities, during which it is necessary to reveal the characteristics of conducting of special information operation.

Thus, suggested methodological approach allows to identify list of certain features that should become a mean for discoursing purposes of special information operations (actions, activities) of an enemy, characteristics of objects, through which the impact and methods of manipulation are made.

УДК 37.01:014.544:378 (045)

# Интеграция системы контроля доступа с единой информационной системой вуза на примере ФГБОУ ВО «Московский государственный университет пищевых производств»

Аитов В.Г., аспирант, начальник управления информационных технологий; Чекин И.И., аспирант, начальник отдела развития информационных технологий
*ФГБОУ ВО «Московский государственный университет пищевых производств», г. Москва.*

В настоящее время на рынке представлено большое количество систем контроля и управления доступа (СКУД), которых объединяет, в той или иной степени, закрытость ядра системы и отсутствие возможности полноценной интеграции в режиме реального времени с другими автоматизированными системами. В качестве примера такой интеграции можно привести необходимость принятия решения о допуске (или отказе в допуске) со стороны СКУД на основании информации, которая физически хранится в другой системе, например, базе данных отдела кадров, или базе данных ERP-системы.

Пользователю комплексной автоматизированной системы, состоящей из отдельных подсистем, может быть предоставлен визуальный интерфейс, в котором отображается информация, предварительно полученная из разных информационных систем, более того, иногда эта информация дополнительно обрабатывается на серверах бизнес-логики до передачи пользователю.

Исходя из вышесказанного, можно сформулировать миссию и главную цель создания и внедрения системы СКУД в единое информационное пространство образовательной организации: обеспечение безопасности сотрудников и обучающихся организации, с возможностью принятия решения о допуске в здания и помещения непосредственно сотрудниками кадровых служб. Структурно-логическая схема СКУД, реализующая такую интеграцию, представлена на рисунке 1.

Внедрение СКУД "МГУПП" происходило поэтапно с предварительной оценкой затрат и будущих перспектив. В результате внедрения СКУД были получены данные, подтверждающие экономическую и технологическую эффективность данной системы. Так, например, стоимость закупки системы "под ключ" для 1 точки входа из трех турникетов, составляет около 280 000 рублей, без учета установки оборудования. Принимая во внимание, что в текущей конфигурации СКУД МГУПП имеется 13 точек входа, а именно двадцать два турникета и два шлагбаума, то закупка готовой системы, без учета установки, обошлась бы более, чем в два миллиона рублей. При этом готовое

решение СКУД представляет из себя автономную, закрытую информационную систему, что противоречит главной цели внедрения - обеспечение создания единого информационного пространства и реализация концепции ERP на уровне организации.

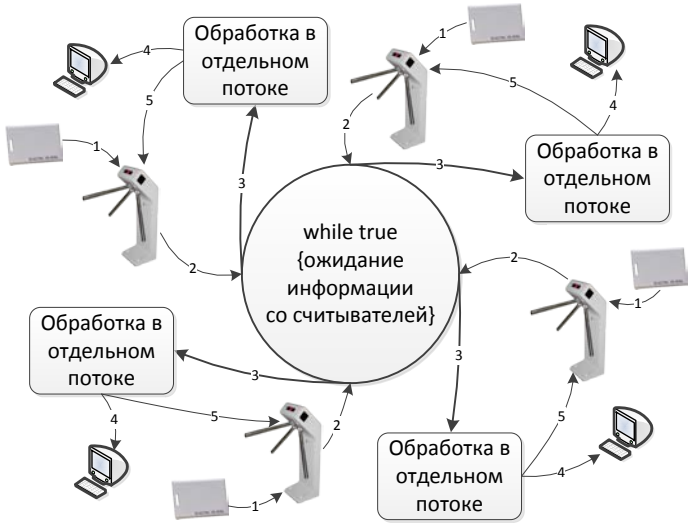



Рисунок 1. Структурно-логическая схема СКУД

При разработке СКУД МГУПП необходимо было учесть и возможность масштабирования системы путем расширения программно-аппаратной части. Немаловажен также такой показатель, как время отклика системы - большинство готовых решений не имеют выделенного сервера базы данных, а записывают данные в память микро-ЭВМ, что затрудняет чтение данных, так как формат записи в каждом случае уникален и не имеет сформированного API. Как следствие данные приходят на сервер с задержкой. В случае СКУД МГУПП данные поступают напрямую на репликационный сервер БД ERP системы, а затем, с интервалом менее секунды, попадают на основной сервер организации. Данный подход гарантирует задержки в пределах погрешности, актуальность данных и возможность как вертикального, так и горизонтального масштабирования.

УДК 81’23

**Інформаційна війна на сайтах новин: меми та медіавіруси**

Акімова Н.В., канд. філол. наук,
*Кіровоградський інститут державного та муніципального управління Класичного приватного університету, м. Кропивницький*

Останнім часом багато говорять про інформаційну війну в Україні, чи існує вона по-справжньому або це міф, мета якого збентежити суспільство? Якщо вона є, то які її реальні масштаби? Чому ефективні її методи? Які її засоби? Коротко визначити ці запитання спробуємо в цій доповіді.

Інформаційна війна, за визначенням самої популярної сьогодні енциклопедії, - це процес протиборства людських спільнот, спрямований на досягнення політичних, економічних, військових чи інших цілей стратегічного рівня, шляхом впливу на цивільне населення, влади та (або) збройні сили протилежної сторони, за допомогою поширення спеціально відібраної і підготовленої інформації, інформаційних матеріалів, і, протидії таким діям на власну бік [2]. Ефективними знаряддями такої війни є меми та медіа віруси. Мем – це складна одиниця культурного наслідування, на зразок гену, з владою змінювати спосіб мислення[3, с.485]. Меми в інтернеті є своєрідними замінами мовленнєвих штампів, прецедентними текстами, що позначають певний спосіб структурування мовної свідомості та стиль мовленнєвої поведінки. Медіавірус – це інформаційний вірус, який відшукує слабкі місця у свідомості реципієнта, прогалини у знаннях, псевдознання та вставляє туди власний код у формі мемів, що дозволяє маніпулювати картиною світу особистості [1, с.176]

Більшість українських наукових гуманітарних досліджень з теми маніпулювання свідомістю спираються на російські теоретичні джерела, одним з основних серед яких є фундаментальна праця С.Г.Кара-Мурзи [4]. Вчені часто також звертаються до американських розробок, в яких вперше і виникло дане поняття.

Згідно С.Г.Кара-Мурзі основним каналом інформаційної війни є засоби масової інформації. Головним серед ЗМІ сьогодні став інтернет. Він постійно під рукою завдяки гаджетам, wi-fi, мобільним операторам. На повідомлення в Мережі постійно посилаються телебачення і радіо. В цілому, інтернет став основним джерелом інформації для сучасної людини. Серед інтернет-ресурсів найбільш відвідувані сайти погоди, новин і пошукові системи. Хочеться вірити, що метеосайти з метою інформаційного тиску поки не використовують, принаймні нам не зустрічалося досліджень, які доводять протилежне. Маніпуляції свідомістю за допомогою пошукових систем пов'язані переважно, як відзначають фахівці, з механізмом контекстної реклами. А найбільш

спеціалізованим каналом інформаційної війни є, мабуть, сайти новин, на аналізі контенту яких слід зупинитися докладніше.

Говорячи про інформаційну війну частіше мають на увазі приклади маніпулювання політичною свідомістю та громадянською позицією. Прикладом таких провокацій в укрнеті може бути анонс з новинного сайту: «НБУ покарає шалапутів, через які впала гривня» [5]. У мовній свідомості українців лексема «шалапут» не має сталих асоціацій, вона є недостатньою девіантною мовленнєвою одиницею, це ускладнює рецепцію зазначеного анонсу. Цим текстом продуцент переключає увагу читачів з більш важливого факту інфляції валюти на менш значимий – покарання винних. Апелюючи до емоційної сфери читача (через використання розмовних слів та помилок, які відволікатимуть увагу) копірайтер вміло переносить акценти з подальших складних дій щодо гальмування інфляції до простого зрозумілого покарання шалапутів. За інвективом з розмитим значенням приховано імена тих, хто допустив помилки. Так підкріплюється медіавірус дієвості влади.

Цікавим прийомом маніпулювання на новинних сайтах є вживання форми множини щодо власних імен, зокрема такий приклад: «Муму и Януковичи» [7]. Поєднання двох прецедентних імен без коментарів в анонсі змушує читача відшукувати імпліцитний зміст. Відповідно можливі різні тактики інтерпретації на основі встановлення асоціативного зв'язку між «Муму» та «Януковичем» у процесі порівняння (наприклад, обидва мали проблеми у спілкуванні) чи аналогії (невтішний фінал для обох) тощо. Безліч асоціацій (надлишкова девіантність), спровокованих вживанням прізвища колишнього президента в оригінальному поєднанні, певно мають закріпити його негативні риси у суспільній свідомості, підкріпивши поширений мем. Використання для еталону персонажу з твору російського класика акцентує натяк, що повідомлення стосується росіян. Насправді у новині за таким гіперпосиланням розповідається, що в одній з донецьких шкіл створять музей відомих випускників, серед яких найбільш знані сини Януковича, також серед скарбу цієї школи є раритетне видання «Муму» 1930 року.

Авторитет українського політика можна корегувати подібним текстом: «Тимошенко з-за грат висунула Януковичу чотири вимоги» [6].

Часто засобом маніпулювання виступають мовні помилки, як у наступному прикладі: «У Порошенка назвали можливого прем'єра» [7]. На етапі інтерпретації відчутна неузгодженість текстових домінант цього анонсу. Вираз «у Порошенка» погано поєднується з наступним текстом. Для його узгодження потрібно уточнення, де саме «у Порошенка» (в гостях, в апараті тощо). Для заповнення цієї лакуни активізується механізм аперцепції (що позначиться активністю нижньої тімяної ділянки лівої півкулі та скроневих ділянок обох півкуль), від обраного варіанта залежить визнання ступеня офіційності новини та успішність емоційної ідентифікації. Використання предикату «назвали» у безособовій формі

покликане нібито приховати джерело інформації, між тим певні відомості про нього подані вже на початку тексту (до того ж у досить дивній формі), співставленні факти провокують когнітивний дисонанс, який змушує замислитися, що цим мав на увазі мовець. На відміну від більшості девіантних текстів Мережі, що стимулюють некретичне засвоєння контенту, аналізований анонс навпаки активізує критичність. На нашу думку, продуцент навмисно створює дисонанс, щоб акцентувати та змусити аналізувати наступний текст щодо «можливого прем'єра», але ж діючого ще ніхто не усував. Повідомлення формує несвідомі симпатії до Яценюка, який став об'єктом змови, та антипатії до Порошенка, якого представлено її зачинчиком. І на незадоволення президентом автор розраховує більше, саме тому лише його прізвище названо експліцитно. Умовна анонімність джерела інформації створює атмосферу розкритої таємниці, у яку посвятили широкий загал, чим сприяє підвищенню довіри до інформації (нам довірили державну таємницю). До того ж новина підтримує поширений мем про слабкість політичних позицій Яценюка, кінець його прем'єрства

Отже, на українських сайтах новин нерідко присутні маніпулятивні тексти, що є потенційною загрозою інформаційній безпеці України. Такі тексти можна відфільтрувати автоматизовано, розробивши спеціальне комп'ютерне забезпечення, в основу якого пропонуємо покласти теорію девіантних мовленнєвих одиниць. Робота у цьому напрямку є подальшою перспективою даного дослідження.

**Список літератури**

1. Акульшин О.В. Медіавірус як лінгвально-техногенний маніпулятивний дискурс // Інтернет-комунікація в діяльності інститутів сектору безпеки: теоретико-прикладний аспект : монографія / О. В. Акульшин. – К., Луганськ : Янтар, 2013. – С.152-199.

2. Википедия — свободная энциклопедия. [Электронный ресурс]. – Режим доступа: https://ru.wikipedia.org

3. Докинз Р. Расширенный фенотип: длинная рука гена / Ричард Докинз; пер. с англ. А.Гопко. – М.: АСТ: CORPUS, 2011. – 512 с.

4. Кара-Мурза С. Г. Манипуляция сознанием / С. Г. Кара-Мурза. – К. : Орияны, 2000. – 448 с.

5. Новини України від LB.ua: оперативна аналітика української політики, економіки, новини культури та спорту [Електронний ресурс] – Режим доступу : http://ukr.lb.ua/

6. Новини УНІАН. Останні новини України та світу [Електронний ресурс] – Режим доступу : http://www.unian.ua/

7. Останні новини України та світу. Корреспондент.net - свіжі новини дня [Електронний ресурс] – Режим доступу : http://korrespondent.net/

УДК 004.056.53

## Дослідження сучасного стану кіберзагроз

Безверха К.С., аспірант
Науковий керівник – Кінзерявий В.М., к.т.н., доцент
*Національний авіаційний університет, м. Київ*

У зв'язку зі стрімким збільшенням цифрової обробки даних, рівень ризику кіберзагроз зростає з кожним роком все більше і більше. І сьогодні перед керівниками організацій та представниками органів державної влади одним з найважливіших завдань є розуміння критичності ризиків стану кібербезпеки та належне управління ними. До недавнього часу лише великі компанії, органи національної безпеки забезпечували в себе інформаційну безпеку, що відповідала належному захисту. Сьогодні ж організації практично всіх сфер діяльності змушені оперативно реагувати на кіберзагрози і належним чином протидіяти кібератакам. Організації впроваджують інноваційні технології, як наприклад, хмарні рішення для забезпечення безпеки, аналізу великих даних, а також новітні системи аутентифікації і т.п. За даними які опубліковані у звіті з інформаційної безпеки за 2017 рів від компанії Cisco, приблизно в кожному четвертому випадку організація, піддалася атаці, втрачає бізнес- можливості. Четверо з десяти опитаних повідомляло, що подібні втрати мали велике значення. Кожна п'ята організація втратила замовників внаслідок кібератак [1]. За даними компанії Trend Micro Incorporated, які опубліковані у річному звіті з кібербезпеки за 2016 рік, фінансові втрати компаній від атак програмами-вимагачами по всьому світу склали 140 тис. доларів [2]. Україну епідемія кіберзлочинності також не оминула, лише за минулий рік було здійснено 247 кібератаки на системи органів державної влад [3]. Як показують наведені дані, рівень кіберзагроз зростає з кожним роком все більше. І хоча технології не стоять на місці і рівень захисту підвищується, зловмисники також прогресують та створюють нові, потужніші види кібератак. Тому дослідження актуальних кіберзагроз та можливі методи їх протидії є **актуальним** завданням, що дозволить організаціям оцінити існуючі заходи захисту від кібератак та при необхідності внести корективи для її покращення.

В роботі проведено аналіз поширеніших кібератак, а також кібератак, які лише набирають обертів та будуть прогресувати в просторі кіберзахисту найближчим часом.

DDos атаки залишаються одним з найпоширеніших методів здійснення кібератак. На сьогодні відомі такі DDos атаки як DDos атаки з використанням ботнетів, DDos атаки з використанням SSL з'єднаня, які стали активно поширюватись в другій половині 2016 року та за даними Kaspersky DDoS Protection, в поточному році кількість таких кібератак

зростатиме, адже системи захисту не на 100% вирішують проблеми захисту від розподілених атак [4].

Атаки з використання тактики множинних невеликих атак – зловмисники використовують таку тактику для того, щоб «вимотати» персонал служб IT-безпеки, а також щоб змусити компанію-жертву тримати у включеному стані засоби придушення атаки, які іноді можуть призводити до деградації послуг, які надаються компанією.

Атаки мережевого рівня – особливість цієї атаки полягає в використанні невеликих мережевих пакетів, що дозволяє зловмисникам добитися високої швидкості пересилання пакетів, а також високої пропускної здатності.

Атака SWEET32 - атака на шифри 3DES і Blowfish. З її допомогою можна отримати cookie, використовуються для аутентифікації з зашифрованого 3DES HTTPS-трафіку, а також відновлювати імена користувачів і паролі з зашифрованого за допомогою Blowfish трафіку, що передається через VPN [5].

За даними дослідження Cisco, шахрайство в Facebook займає 3-є місцк в рейтингу веб-атак, включаючи сфальсифіковані пропозиції, опитування і медіаконтент. Високі позиції Facebook-шахрайства в річному і піврічному рейтингах найбільш поширених видів шкідливого ПО свідчать про найважливішу роль соціального інжинірингу в реалізації значної частки кібератак [1].

**Висновки.** Проаналізовано кібератаки, які на сьогоднішній день являються найпоширенішими серед кіберзлочинців та показано проблему, яка існує в кіберпросторі, а саме кібератаки, яким піддавались та піддаються організації по всьому світу. Приведені дані дозволять скоординувати діяльність направлену на захисту інформації у потрібний вектор для своєчасного виявлення атаки та можливості її відбиття.

**Список літератури**

1. Cisco. Річний звіт з інформаційної безпеки, 2017. [Електронний ресурс]. – Режим доступу: http://www.cisco.com/c/dam/m/digital/elq-cmcglobal/witb/1301152/ReportUKR.pdf

2. Звіт з інформаційної безпеки за 2016 рік компанії TrendMicro.

3. Служба безпеки України [Електронний ресурс]. – Режим доступу: https://ssu.gov.ua/ua/news/1/category/2/view/2474#sthash.4E1VYLlG.dN4fEVOL.dpbs

4. Електронний ресурс: https://securelist.ru/analysis/malware-quarterly/29506/kaspersky-ddos-intelligence-report-for-q3-2016/

5. Sweet32: Birthday attacks on 64-bit block ciphers in TLS and open VPN [Електронний ресурс]. – Режим доступу: https://sweet32.info/

УДК 57.001

## Особливості розробки інформаційної системи ідентифікації особи за відбитками пальців

Бєсєдіна С.В., канд. техн. наук, доцент,
Литвин Ю.В., магістрант 1-го року навчання
*Черкаський національний університет імені Богдана Хмельницького, м. Черкаси*

Сьогодні, людство оперує численною кількістю інформації, велика частина якої підлягає тому чи іншому рівню конфіденційності із наданням доступу до неї лише певній людині чи групі людей. Тому інформаційна безпека є одним із основних критеріїв, за яким повинні обиратися такі системи. Захист із використанням біометричних систем аутентифікації, які використовують знання морфометрії, мають ряд незаперечних переваг: простота використання, зручність, надійність, мінімальна кількість затраченого часу та людських зусиль. Дослідження показали, що найбільш використовуваним з усіх біометричних методів для ідентифікації особистості (геометрія кисті руки, райдужна оболонка ока, сітківка ока, голосова ідентифікація, геометрія обличчя і т. ін.) є використання відбитка пальця, оскільки ймовірність помилки при ідентифікації користувача набагато менша у порівнянні з іншими біометричними методами та сам пристрій потребує небагато місця [1, 2].

Отже, постає задача експериментального дослідження результатів роботи існуючих методів аналізу відбитків пальців, для застосування на складних для аналізу ділянках шкіри пальця, а також реалізації шифрувального алгоритму, який надасть безпечне зберігання даних проаналізованих зображень.

Метою роботи є розробка захищеної системи ідентифікації особи за біометричними показниками, на основі досліджених методів дактилоскопії, що базуються на порівнянні мінуцій (точок обривання ліній та їх розгалуження) двох зображень відбитків.

Поставлене завдання вирішується застосуванням існуючих методів співставлення відбитків та розробки нового алгоритму, що дозволить розширити можливості існуючих. Шифрування зображення візерунку пальця та його даних реалізовуватиметься на базі криптографічного методу симетрії. Папілярні візерунки людини не співпадають із структурою відбитку будь-якої іншої людини, тому визначальними параметрами, для проведення аналізу малюнку, є співставлення кінців, ширини петель, розгалужень, їх положень в координатній площині та інших особливостей. Аналіз відбитку пальця може бути проведений з використанням різних класів алгоритмів, зокрема за оцінкою розташування мінуцій.

В основу методу покладено п’ять основних кроків обробки зображення відбитку [2]:

1. Фільтрація зображення, тобто виділення зон для аналізування.
2. Бінаризація, тобто окреслення однорідних областей.
3. «Потоншення» ліній для більш чіткого виявлення положення мінуцій.
4. Виділення особливих точок, тобто пошук обривання та розгалуження ліній.
5. Порівняння двох масивів точок, тобто співставлення значень із наявними у базі даних.

Блок-схема роботи алгоритму розпізнавання відбитку пальця розроблюваної системи подана на рисунку 1.

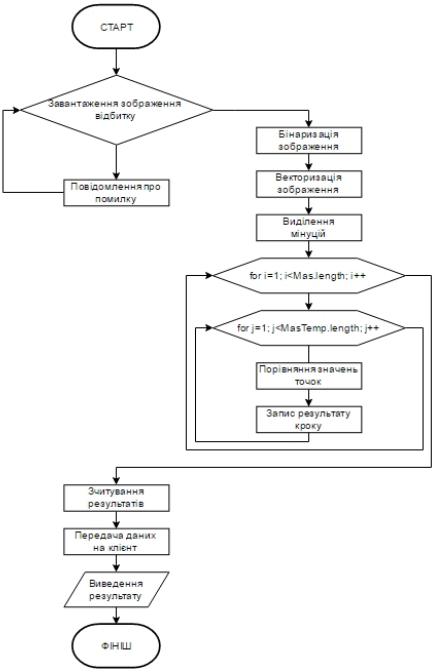



*Рисунок 1 – Блок-схема алгоритму дій процесу аналізу зображення відбитку*

Отже, актуальність розвитку біометричних технологій ідентифікації особи обумовлена збільшенням кількості об’єктів і потоків інформації, які необхідно захищати від несанкціонованого доступу. Точність аналізу відбитків пальців залежить від багатьох параметрів, її рівень коригує якість свого призначення. Метод ідентифікації особи за відбитками пальців є найбільш поширеним і в залежності від технології і способу розпізнавання має невеликий рівень помилок. Використання цього методу спрощує процедуру аутентифікації особи та піднімає надійність системи в цілому.

**Список літератури**

1. Задорожный Виталий Идентификация по отпечаткам пальцев. Часть 2 , 2004. [Електронний ресурс]. – Режим доступу: http://www.bre.ru/security/21052.html.

2. Фам Зуй Тхай Некоторые вопросы применения методов сравнения отпечатков пальцев для биометрических систем идентификации личности / Зуй Тхай Фам // Международный научно-исследовательский журнал, №7 (38). Часть 1. – 2015. – С.127-130 [Електронний ресурс]. – Режим доступу: http://research-journal.org/technical/nekotorye-voprosy-primeneniya-metodov-sravneniya-otpechatkov-palcev-dlya-biometricheskix-sistem-identifikacii-lichnosti.

УДК 004.056

# Методика кількісної оцінки ефективності стратегії інформаційної безпеки

Василевич Л.Ф., канд. техн. наук, доцент
*Київський університет імені Бориса Грінченка, м. Київ*

**Постановка задачі.** В сучасних умовах важливість розробки та реалізації ефективної стратегій інформаційної безпеки в силу її унікальності є актуальною проблемою. Неправильно вибрана стратегія або неефективна реалізація правильної стратегії не дають шансів на успіх забезпечення інформаційної безпеки. Прийняття рішень з вибору стратегії ґрунтується на таких основних універсальних принципах прийняття рішень: принципу цілі, принципу множини альтернатив, принципу оптимальності, принципу єдиноначальності та розділення повноважень і відповідальності, принципу вимірювання, принципу усвідомленої необхідності в прийнятті ризику, принципу керованості ризику, принципу забезпеченості ресурсами, принципу обліку часу, принципів синергетики та системності.

Проблема кількісної оцінки ефективності реалізації стратегії, аспекти якої розглядуються, пов'язана з тим, що, по-перше, саме це поняття показника ефективності реалізації стратегії не має визначеної кількісної характеристики. По-друге, ця задача є багатокритеріальною. Крім того, оцінки по-різним критеріям неможливо отримати чіткими [1].

**Основні результати.** При виборі стратегії потрібно застосовувати аксіоми, які зв'язують основні категорії інформаційної безпеки: інформацію, вартість, час та ризик.

**Аксіома 1** (взаємозв'язок між часом та вартістю). Чим на більший час розраховується функціонування системи інформаційній безпеки, тим більше її вартість.

**Аксіома 2** (взаємозв'язок між вартістю та ризиком). Чим менша вартість системи інформаційної безпеки, тим с більшим ризиком вона пов'язана.

**Аксіома 3** (взаємозв'язок між часом та ризиком). Більш тривалому функціонуванню системи інформаційної безпеки відповідає більш високий ризик.

**Аксіома 4.** Взаємозв'язок між ризиком ($R$), вартістю ($C$), часом ($T$) та інформацією ($I$), яка застосовується, визначається наступною якісною формулою:

$$R=T-I-C.$$

Ця формула охоплює всі аксіоми та деякі принципи вибору стратегії інформаційної безпеки. Із цього співвідношення визначимо центральний

принцип, який має бути принципом оптимальності: при виборі стратегії інформаційної безпеки вибирається та, яка при заданій вартості і заданому часу функціонування забезпечує мінімум ризику за наявності відповідної інформації. Інформація є основною, ключовою категорією інформаційної безпеки, а її взаємозв'язок з іншими категоріями визначає необхідність системного та синергетичного підходів при вибору та реалізації стратегії інформаційної безпеки [3].

При розробці методики кількісної оцінки ефективності реалізації стратегії потрібно розуміти різницю між «простотою» та «спрощенням». Альберт Ейнштейн іронічно висловив, що: «все слід спрощувати до тих пір, поки це можливо, але не більш того». Цей принцип, який називають «Лезо Ейнштейна», доповняє принцип «Бритви Оккама»: «пояснення будь якого явища тим ближче до істинного, чим на меншій кількості гіпотез воно основане і чим більш широке коло явищ основується на цих гіпотезах». «Бритва Оккама» та «Лезо Эйнштейна» відповідають і методиці Ньютона: «поясняти якомога більшу кількість фактів якомога меншою кількістю вихідних положень», тому застосовуються при виборі часткових показників ефективності стратегії інформаційної безпеки.

Узагальнений показник ефективності реалізації стратегії $У$, є деякою функцією часткових показників: $У = Ψ (X, Z, W, V,...)$. Визначити цей функціональний зв'язок навряд чи можливо. Єдине, що можне зробити – це визначити характер зміни узагальненого показника у залежності від зміни часткових показників $X, Z, W, V,....$ Тому для знаходження оцінки узагальненого показника $У$ пропонується застосовувати лінгвістичні змінні [1,3]. Термами лінгвістичної змінної «Ефективність реалізації стратегії» можуть бути наступні: $E_1$ – реалізація стратегії не ефективна; $E_2$ – низька ефективність реалізації стратегії; $E_3$ – середня ефективність реалізації стратегії; $E_4$ – добра ефективність реалізації стратегії; $E_5$ – висока ефективність реалізації стратегії.

Головне поняття теорії нечітких множин – функція належності, яка характеризує суб'єктивну достовірність того, що значення $x$ приналежить відповідному терму.

При виборі часткових показників пропонується також керуватися законам Парето та застосовувати систему збалансованих показників [4]. Збалансована система показників інформаційної безпеки має чотири складові: технічну; розвідувальне - аналітичну; управління та кадрову, кожна з яких визначається своїми частковими показниками. Крім того, деякі часткові показники повинні бути упереджуючі.

Недоліком збалансованої системи показників [4] є те, що в неї відсутня методика отримання кількісного узагальненого показника ефективності реалізації стратегії. В даній роботі при знаходженні кількісної оцінки ефективності реалізації стратегії використовується не просто адитивний узагальнений показник, а здійснюється згортання значень функцій приналежності до тих або інших термів лінгвістичних змінних, що

забезпечує коректність нечіткої моделі, яка застосовується.

При оцінці ефективності реалізації стратегії враховується різна важливість часткових показників. Для цього можна використовувати методи: Фішберна, Уея, Сааті та інші [5].

Привабливість застосування лінгвістичних змінних в задачі, яка розглядується, обумовлена її близькістю до природних мов [1]. Це спрощує процес створення як бази знань, так і доповідь про результати кількісної оцінки ефективності реалізації стратегії інформаційної безпеки особи, яка приймає та затверджує відповідні рішення. Так як в період військових дій потрібно частіше проводити моніторинг реалізації стратегії інформаційної безпеки, а при необхідності, проводити її коректування, то відповідна кількісна оцінка ефективності реалізації стратегії повинна бути простою і зрозумілою для осіб, які приймають відповідні рішення. Це також є перевагою методики, яка пропонується.

Методика на основі лінгвістичних змінних враховує невизначеність без використання ймовірнісних розподілів оцінок часткових показників, що особливо підходить для випадків, коли відповідні процеси не є стохастичними, або коли їхні імовірнісні оцінки не можуть бути отримані через не репрезентативність або неоднорідність відповідних вибірок. Крім того, стохастична невизначеність має справу з невизначеністю в майбутньому, а нечітка невизначеність, яку описує теорія нечітких множин, – з невизначеністю, що не залежить від часу її розгляду.

**Висновки.** Запропоновано застосування методики кількісної оцінки ефективності реалізації стратегії інформаційній безпеки на основі лінгвістичних змінних; розроблено алгоритм оцінки ефективності реалізації стратегії; при виборі часткових показників оцінки ефективності реалізації стратегії інформаційної безпеки запропоновано застосування методології системи збалансованих показників з урахуванням різної важливості часткових показників.

**Список літератури**

1. Нечеткие множества в моделях управления и искусственного интеллекта, Под ред. Б.А. Поспелова. – М.: Наука, 1986. – 326 с.

2. Василевич Л,Ф. Радиоэлектронное подавление: Учеб. Пособие. – Киев: КВВАИУ, 1989.- 178 с.

3. Василевич Л,Ф., Маловик К.Н., Смирнов С.Б. Количественные методы принятия решений в условиях риска: Учеб. Пособие. – Севастополь: СНУЯЭиП, 2007. -232 с.

4. Каплан Роберт С., Нортон Дейвид П. Организация,ориентированная на стратегию. Пер. с англ. – М.: ЗАО «Олимп – Бизнес», 2004.-416 с.

5. Василевич Л.Ф., Клятченко Я.М., Михайлюк А.Ю., Михайлюк О.С., Огнівчук Л.М., Тарасенко В.П. Порівняльний аналіз методів визначення коефіцієнтів пріоритетності часткових показників проектів ІІАС// Науковий вісник Чернівецького університету: Збірник наук. праць. – Чернівці: ЧНУ, 2011.

УДК 343.346.8

# Дослідження проблематики системи захисту кіберпростору України

Войтович В.С., курсант,
Гриник Р.О., викладач
*Львівський державний університет безпеки життєдіяльності, м. Львів*

В умовах сьогодення розвиток інформаційно-комунікаційних технологій супроводжується розробленням та появою нових способів кібератак, злочинів у мережі Інтернет, порушення роботи державних та приватних установ. Тому кібербезпека стає на ланку міжнародної політики. Але попри всі сподівання в Україні присутня єдина спроба врегулювання кібербезпеки, що набрала чинності з 1 липня 2006 року, це «Конвенція про кіберзлочинність».

Система кіберпростору України повинна щонайперше забезпечити певний взаємозв'язок державних органів, військових підрозділів, правоохоронних органів, навчальних та наукових установ, органів місцевого самоврядування, а також організацій і установ, що займаються у сфері з використанням електронних комунікацій, захисту інформації, з питань кібербезпеки.

Фундаментом системи повинні бути: Міністерство оборони України, Державна служба спеціального зв'язку та захисту інформації України, Служба безпеки України, Національна поліція України, Національний банк України, розвідувальні органи, на які мають бути поручені в установленому порядку певні завдання. Щодо Ради національної безпеки і оборони України згідно з Конституцією України та у канонізованому законом порядку має проводити координацію та контроль діяльності суб'єктів сектору безпеки і оборони, які забезпечують безпеку кіберпростору України.

Відповідно до законодавства дані структури повинні виконувати ряд вимог:

- формування, а також реалізація політики нашої держави стосовно захисту у кіберпросторі державних інформаційних ресурсів і таємної інформації, вимога відповідно захисту якої легалізована законом, кіберзахисту критичної інформаційної інфраструктури та державний контроль;
- проведення заходів для підготовки країни щодо воєнної агресії у кіберпросторі;
- налагодження військових взаємозв'язків з НАТО, які передусім тісно пов'язані з безпекою кіберпростору;

- попередження, виявлення злочинів насупроти безпеки миру і людства, що вчиненні у кіберпросторі та наступним кроком є розкриття та припинення їх;
- втілення координаційно-технічних заходів із блокування, розкриття й реагування на кібератаки і усунення їх наслідків, сповіщення про кіберзагрози та певні методи захисту від них;
- здійснення розвідувальної роботи для запобігання загрозам національній безпеці України у кіберпросторі, інших обставин, що перш за все торкається сфери кібербезпеки.

Для прикладу в Україні з 1 липня 2015 року у Державній службі спеціального зв'язку та захисту інформації України розпочав роботу Державний центр кіберзахисту та протидії кіберзагрозам. Одним із завдань Державного центру кіберзахисту є забезпечення функціонування команди реагування на комп'ютерні надзвичайні події України CERT-UA, крім того, контроль стану захищеності державних інформаційних ресурсів в інформаційних системах органів державної влади. А також ДЦКЗ повинне забезпечувати функціонування, безпеку та розвиток Національної системи конфіденційного зв'язку, функціонування та розвитку системи антивірусного захисту інформації для органів державної влади, забезпечення функціонування та модернізації Системи захищеного доступу до мережі Інтернет органів державної влади України та Захищеного вузлу Інтернет-доступу Держспецзв'язку.

Для відповідного функціонування системи кібепростору, потрібно залучати всі ограни, що безпосередньо пов'язані із кібербезпекою України. Вирішувати питання щодо запобігання та видалення наслідків кібератак, злочинні втручання в інформаційні системи, а також міжнародної координації по захисту кіберпростору. Держава повинна сприяти приєднанню наукових та навчальних установ, організацій, громадських об'єднань для впровадження певних заходів для усунення кіберзагроз та кібератак у теперішньому часі.

**Література**

1. Grediaga A. Application of neural networks in network control and information security / A. Grediaga, F. Ibarra, F. García [et al.] // LNCS. – 2006. – Vol. 3973. – P. 208- 213. 6. I
2. FERGUSON, Niels; SCHNEIER, Bruce. A cryptographic evaluation of IPsec. Counterpane Internet Security, Inc, 2000, 3031: 14.
3. Military and Security Deployments Involving the People's Republic of China //http://www.defense.gov/pubs/pdfs/2010_CMPR_Final.pdf
4. Закон України "Про захист інформації в інформаційно-телекомунікаційних системах" №2594-IV від 31.05.2006.

УДК 32.019.5

**Інформаційні війни на сучасному етапі людства**

Герасименко Л.В., начальник циклової комісії
з природничо-наукових дисциплін відділення підготовки
Військового коледжу сержантського складу,
Івоса В.В., викладач циклової комісії
з природничо-наукових дисциплін відділення підготовки
Військового коледжу сержантського складу
*Національна академія сухопутних військ імені гетьмана Петра Сагайдачного, м. Львів*

Протистояння в інформаційному просторі ведеться як у воєнний, так і в мирний час з метою відстоювання національних інтересів держав, впливу на політичні та економічні зони, території сировини й ринки збуту.

Воно постійно ведеться не тільки між державами, але й всередині кожної з них, в першу чергу, за владу і політичний вплив, за можливість маніпулювати настроями і поведінкою суспільства. Контролюючи зміст потоків інформації, керуючи її поданням масі людей, можна впливати на суспільні процеси загалом.

Інформаційна війна має на меті вплив на свідомість людини і проводиться, з одного боку з метою послаблення моральних сил противника, а з іншого – посилення своїх власних.

На відміну від реального збройного конфлікту, який направлений на фізичне знищення сил та засобів противника, інформаційна війна спрямовує свою дію на свідомість таким чином, щоб керувати суб'єктами та заставити їх діяти проти своїх власних інтересів.

Інформаційна війна, як і всі інші протистояння, має свої види, форми, цілі та методи, які збільшуючи свої масштаби постійно удосконалюються.

На сучасному етапі інформаційна війна – це не лише один з видів забезпечення операцій збройних сил, але й боротьба, можливості якої переходять далеко за ці межі.

Характерною ознакою сучасних інформаційних війн є швидкий розвиток інформаційних технологій, їх застосування як у повсякденному житті людей, організацій, так і в державі в цілому. В силу того, що інформаційні системи різних держав інтегруються до єдиного інформаційного простору, де проходить збір, накопичення, зберігання, обробка та обмін інформацією між суб'єктами (державами), масштаби ведення інформаційної боротьби постійно збільшуються та вдосконалюються.

Останнім часом загальноприйнятим для інформаційних війн стає те, що вони, незалежно від масштабу, місця чи мети проведення – мають

культурну та історичну основи і спрямовані на примусове "наповнення" вже сформованої психологічної ментальності людини.

Ціллю впливу виступає свідомість людини, метою – прагнення заволодіння нею для подальшого проведення необхідних маніпуляцій. Основним завданням є не фізичне знищення, а встановлення контролю над джерелами та потоками інформації з метою управління не лише окремими людьми, а й цілими народами. Інформаційна війна може вестись в будь-якій точці інформаційного простору, а особливо там, де є слабкі місця. По суті інформаційна війна – це боротьба існуючих інтелектуальних ресурсів противників. При цьому інформація, що подається, перекручується, ліквідуються небажані факти, спотворюється ті, яких неможливо позбутись. Ці дії міняють статус інформації, одночасно змінюючи відношення до її змісту та оцінку. Інформаційна боротьба може включати в себе різні маніпуляції не лише з інформацією, а й проведення аналогічних дій з людьми. По суті ця боротьба перетворює людей на предмети, а суб'єктів – на об'єкти.

Сучасні інформаційні війни широко застосовуються у воєнних, політичних та економічних протиріччях. В середині суспільства інформаційна війна може проводились керівництвом держави з метою утримання правлячого положення, тим самим підтримуючи збереження влади. Вміле застосування інформаційних технологій дає можливість проводити операції, які при цьому будуть висвітлені у дзеркальному відображенні. Розуміючи зосередження сил, аналізуючи інтереси людей та стан реальної обстановки можна впливати на свідомість суб'єктів всебічно.

Через спотворення дійсної інформації щодо економічних показників, політичної ситуації, іміджу, традиційних основ устрою, соціальних гарантій, загальних настроїв, системи задоволення релігійних потреб, що в тій чи іншій мірі впливає на свідомість суб'єкта, отримуємо результат – змінюється суспільний настрій, почуття, ламається система поглядів та переконань, з'являється незадоволення та (або) зневіра.

В доповіді зазначено, що на сучасному етапі інформаційна війна складає основу для реальної війни, передуючи їй чи протікаючи паралельно, а найчастіше – визначає її успіх.

Отже, для того, щоб психологічно роззброїти народ потрібно лише позбавити його основ, що закладені в культурі, ідеях та нормах. За допомогою спеціально орієнтованої інформації ці культурні витоки та ідеали розмиваються. Інформаційна війна не призводить до великих руйнувань та кровопролить, проте її руйнівна сила може зрівнятися з наслідками великомасштабних збройних конфліктів.

УДК 004.056.53

# Выбор программно-аппаратных средств для доступа к данным по биометрическим параметрам

Гивойно А.А., аспирант,
Прузан А.Н., аспирант,
Яковлев А.В., магистрант
Научный руководитель – Сечко Г.В., к.т.н., доцент
*Белорусский государственный университет информатики и радиоэлектроники, г. Минск*

**Постановка задачи**. В настоящее время данные различного назначения хранятся как в традиционных базах данных (в виде отдельных файлов [1] или архивов [2]), так и в облачных хранилищах [3]. Защита данных проводится в основном с помощью разрешения на доступ к ним, в том числе и по биометрическим параметрам. Общепринято считать, что разрешение доступа к данным по биометрическим параметрам может осуществляться на основе распознавания а) отпечатков пальцев; б) радужной оболочки глаза (РОГ); в) лица; г) геометрии руки; д) голоса; е) сетчатки глаза; ж) ряда дополнительных биометрических параметров (по ДНК, по термограммам, по запаху тела и т. д.) [4]. Из-за множества вариантов средств доступа перед собственником данных возникает задача их выбора.

**Предлагаемый вариант решения задачи**. 1.Определить несколько вариантов предпочтительных средств доступа (авторизационных систем, АС). 2. Выбрать набор технико-экономических показателей сравниваемых друг с другом АС. 3. Каждый выбранный показатель представить в виде балльной шкалы (чем предпочтительнее АС, тем выше балл), например, для показателя «цена АС»: 25 000 $ –7 баллов, 26 000 $ – 5 баллов, 27 000 $ – 3 балла. 4. Выбрать весовые коэффициенты каждого показателя так, чтобы сумма их равнялась единице. 5. Рассчитать критерий выбора АС как скалярное произведение вектора выбранных показателей и вектора весовых коэффициентов (чем предпочтительнее АС, тем выше критерий).

**Пример решения задачи**. Пусть необходимо выбрать АС, распознающую пользователя по РОГ, для защиты данных о прерывании беременности в роддоме. 1. Варианты предпочтительных АС – средство NPack [1–2] и программно-аппаратный комплекс (ПАК), описанный в [5]. 2. Выбранные технико-экономические показатели АС – её цена (без стоимости сканера, показатель 1), общая стоимость данных для пациентов (ущерб от разглашения, показатель 2), суммарная вероятность ошибок идентификации (вероятность пропуска «чужого» плюс вероятность ложного отказа в доступе, показатель 3). 3. Оценка показателей в баллах

(для ПАК информация только для примера, так как в [5] эти сведения отсутствуют и уточнить их у разработчика не удалось): ПАК – показатель 1 = 7 баллов, показатель 2 = 7 баллов, показатель 3 = 4 балла, средство NPack – показатель 1 = 5 баллов, показатель 2 = 7 баллов, показатель 3 = 6 баллов. 4. Весовые коэффициенты: для показателя 1 равен 0,250; для показателя 2 равен 0,400; для показателя 3 равен 0,350. 5. Критерий выбора авторизационной системы: для ПАК –

0,250•7 + 0,400•7 +0,350•4 = 5,95 (баллов);

для средства NPack –

0,250•5 + 0,400•7 + 0,350•6 = 6,15 (баллов).

Из сравнения рассчитанных критериев выбора АС ясно, что покупатель АС должен выбрать средство NPack. Ещё раз отмечаем, что приведенные в примере сведения о показателях 1 и 3 в [5] отсутствуют и уточнить их у разработчика не удалось, поэтому вышеприведенный пример иллюстрирует только пригодность предлагаемой методологии.

**ВЫВОД**: приведенный пример выбора программно-аппаратных средств для доступа к медицинским данным по РОГ показывает простоту предлагаемого способа выбора и его применимость в инженерной практике для проведения экспресс оценки критерия выбора АС.

**Список литературы**

1. Гивойно А.А., Ростовцев В.Н. Защита медицинских данных пациентов // Доклады БГУИР. – 2016. – № 7 (101). – С. 79–83.

2. Гивойно А.А. и др. Безопасное архивирование данных с помощью биометрических технологий // Веснік сувязі. – 2013. – № 6 (122). – С. 25–28.

3. Прузан А. Н., Николаенко В. Л., Сечко Г. В. Мониторинг инцидентов информационной безопасности в облачных вычислениях на малом предприятии // Доклады БГУИР. – 2015 – № 7 (93). – С. 126-128..

4. Прудник А.М., Власова Г.А., Рощупкин Я.В. Биометрические методы защиты информации: учебно-методическое пособие для специальности 1-98 01 02 «Защита информации в телекоммуникациях». – Минск: БГУИР, 2014. – 150 с.

5. Программно-аппаратный комплекс для идентификации личности по радужной оболочке глаза // Каталог завершённых разработок НАН Беларуси. – Минск: Беларуская навука, 2016. – 376 с.– С. 13–14.

УДК 004.056

## Протидія комп'ютерним атакам з переповненням буферу

Горелов О.Ю., студент 3 курсу
Науковий керівник – Кобзєв І.В., к.т.н., доцент
*Харківський національний університет радіоелектроніки, м. Харків*

Вразливості переповнення буфера є одним з можливих джерел небезпеки для інформаційних систем. У значній мірі вони використовують особливості деяких мов програмування. Наприклад, мова С припускає, що цілісність даних забезпечує сам програміст. Це дозволяє прискорити роботу програм, ефективно контролювати їх роботу та спростити мову. Але це може призвести до появи програм, схильних до переповнення буфера.

Для виявлення та запобігання переповнення буфера існують різні методи. Найнадійнішим способом є використання автоматичного захисту на рівні мови. Цей вид захисту, тим не менш, не може бути застосована до старого коду. Мова С не забезпечує вбудованих засобів захисту проти доступу або перезапису будь-якої частині пам'яті, хоча багато інших мови забезпечують перевірку під час виконання, а в деяких випадках і під час компіляції, та генерують попередження або виняток.

Захист виконання даних полягає у тому, що виконання інструкцій з сегменту даних заборонено на апаратному рівні чи рівні операційної системи. Хоча зловмисник зможе виконати переповнення буфера, але не зможе передати керування на інструкції коду та виконати його, тому що програму буде аварійно завершено. Деякі процесори підтримують спеціальну функцію під назвою NX («No Execute») або XD («Execute disabled») [1].

Інший засіб боротьби - ASLR (Address space layout randomization ) – технологія при використанні якої випадковим чином змінюється розташування в адресному просторі процесу важливих структур, наприклад бібліотек, купи і стека. Технологія ASLR дозволяє значно ускладнити успішну експлуатацію декількох типів уразливостей [2].

Переповнення буфера працює через зміну вказівників (в тому числі збережених). Було запропоновано розширення до компіляторів, та бібліотеки, які змінюють вказівники (наприклад, за допомогою функції XOR) таким чином, щоб їх важко було вгадати зловмисникові.

Ефективним методом боротьби є також використання «слів-канарок» («canary words»). Спосіб полягає в записі деякого спеціального значення в комірку пам'яті, наступну за буфером, який може бути модифікований під час роботи функції. Перед поверненням з функції, система здійснює перевірку цілісності цього значення. Порушення цілісності слова-канарки

просигналізує, що коректну адресу повернення з функції (або інші дані, наступні за буфером) було змінено [3].

За допомогою систем виявлення вторгнення (СВВ) також можна виявити і запобігти спробам віддаленого використання переповнення буфера. Через те, що в більшості випадків дані, призначені для переповнення буфера містять довгі масиви інструкцій No Operation (NOP або NOOP), СВВ просто блокує всі вхідні пакети, що містять велику кількість послідовних NOP-ів.

Запобігання виконання даних – це спосіб захисту від переповнення буфера, який передбачає заборону виконання коду в стеку або купі. Зловмисник може використовувати переповнення буфера для вставки довільного коду в пам'ять програми, але при використанні цього захисту це призведе до генерації винятку.

Окремі процесори підтримують обробку спеціального біту, який називається NX («No eXecute») або XD («eXecute Disabled»), що може бути використане для позначення сторінок даних у пам'яті тільки для читання та запису, але не для виконання. Деякі операційні системи Unix (наприклад, OpenBSD, OS X) випускаються із цим захистом. Сучасні версії Microsoft Windows також підтримують «запобігання виконання даних», (Data Execution Prevention).

Підводячи підсумки можна зробити висновок про те, що не існує єдиного методу, який повністю вирішує проблему переповнювання буфера. Існуючі сьогодні методи мають недоліки, а про захищеність системи можна говорити тільки при їх грамотному поєднанні. Повністю розв'язати проблему переповнювань можна двома шляхами: створити метод, який не залежить від розробників ПЗ або використовувати мови програмування, що не мають прямого доступу до пам'яті.

**Список літератури**

1. Execute Disable Bit [Електронний ресурс] – Режим доступу до ресурсу: http://biosgid.ru/parametry-bios-setup/zagruzka-i-bezopasnost/execute-disable-bit-no-execute-memory-protect.html.

2. ASLR [Електронний ресурс] // Материал из Википедии — свободной энциклопедии – Режим доступу до ресурсу: https://ru.wikipedia.org/wiki/ASLR

3. Коваленко Д. Защитись и замети! [Електронний ресурс] / Дмитрий Коваленко // Спецвыпуск Xakep, номер #045, стр. 045-068-3 – Режим доступу до ресурсу: http://xakep-archive.ru/spec/045/068/3.htm.

4. Сєвєрінов О. В. Аналіз сучасних систем виявлення вторгнень / О. В. Сєвєрінов, А. Г. Хрєнов. // Системи обробки інформації. – 2013. – №6. – С. 122–124.

УДК 681.3.001.63

## Дослідження стійкості криптосистеми Меркле-Хеллмана до атак побудованих на генетичному алгоритмі

Гриник Р.О., викладач
*Львівський державний університет безпеки життєдіяльності, м. Львів*

При сьогоднішніх надшвидких темпах розвитку кіберпростору, все більшого значення набувають проблеми захисту даних з допомогою використання криптографічних систем, а також дослідження цих систем на вразливість до розкриття за допомогою різноманітних алгоритмів. В даній роботі досліджувалась вразливість ранцевої криптосистеми Меркле-Хеллмана, яка є однією з перших асиметричних систем шифрування. Для розкриття системи використовувались два алгоритми: алгоритм повного перебору та модифікація генетичного алгоритму.

На сьогодні генетичні алгоритми використовують при криптоаналізі потокових шифрів, генерації ключів асиметричних алгоритмів шифрування, здійсненні криптоаналізу симетричних та асиметричних шифрів [2]. Основним завданням при застосуванні генетичного алгоритму є необхідність побудови цільової функції таким чином, щоб з наближенням знайденого рішення до реального, значення фітнес-функції прямувало до 0 [1].

Для вирішення поставленої задачі була побудована наступна фітнес-функція:

$$f(x) = \left| C - \sum_{i=1}^{n} x_i k_i \right|,$$

де вектор $k = \{k_1, k_2, ..., k_n\}$ являється відкритим ключем для шифру, $C$ - сама криптограма, $x = \{x_1, x_2, ..., x_n\}$ поточне рішення задачі. Якщо результат обчислення цільової функції буде рівним нулю – це означає що вектор $x = \{x_1, x_2, ..., x_n\}$ є ідентичним до вектора який був зашифрований з допомогою ключа $k = \{k_1, k_2, ..., k_n\}$ з чого випливає, що шифр розкритий. Загалом структура алгоритму для крипто аналізу має наступний вигляд:

1. Створення початкової популяції.
2. Обчислення значення фітнес-функції кожної особини популяції, якщо існує особина з пристосованістю нуль, то перейти до пункту 7.
3. Схрещення.
4. Мутація.

5. Формування нової популяції.
6. Обчислення значення фітнес-функції кожної особини новоутвореної популяції, якщо значення фітнес функції жодної особини не дорівнює нулю, перейти до пункту 3.
7. Завершити виконання програми.

Експериментальні обчислення з використання спеціально розробленого програмного забезпечення показали, що розкриття криптосистеми Меркле-Хеллмана за допомогою генетичного алгоритму є можливим і зазвичай займає менше часу, ніж розкриття повним перебором всіх можливих рішень. При проведенні експерименту використовувались два методи відбору хромосом батьків: селекція та метод рулетки. Схрещення відбувалось за допомогою двох точкового кросинговеру, а для формування нової популяції використовувався елітарний відбір. Для того, щоб розв'язок задачі не зводився до локального мінімуму, використовувалась мутація, коефіцієнт якої корегувався відповідно до довжини ключа та розміру популяції.

**Список літератури**

1. Гриник, Р.,О., Застосування генетичного алгоритму для криптоаналізу ранцевої криптосистеми Меркле-Хелмана / Р.О. Гриник, О.І.Полотай // Вісник ЛДУ БЖД : зб. наук. праць. – Львів : Вид-во ЛДУ БЖД. – 2016. – № 14. – С. 77-83.

2. Гриник Р.О., Застосування генетичного алгоритму для вирішення задач крипто аналізу. / Гриник Р.О. // Інформаційно-комунікаційні технології в сучасній освіті: досвід, проблеми, перспективи : IV Міжнар. наук.-практ. конф., 21-22 жовт. 2015 р. : зб. наук. пр. – Ч. 1. – Львів, Вид-во ЛДУ БЖД, 2015. – С. 168-170

3. Елисеев Г. О. Применение биоинспирированных методов оптимизации для реализации криптоанализа классических и блочных криптосистем / Елисеев Г. О., Чернышев Ю. О. // Весник Пермского университета – 2010.

УДК 519.688

# Програмно-апаратна реалізація генератора підключів для системи шифрування відеоінформації на основі клітинних автоматів

Демаш А.А., здобувач
Науковий керівник – Білан С.М., к.т.н., доцент
*Державний науково-дослідний інститут*
*спеціального зв'язку та захисту інформації України, м. Київ*

На даний час, для захисту візуальної інформації застосовуються ряд способів, [1-7], які вимагають удосконалення з точки зору представлення зображення і формування ключової послідовності, адаптованої до його розмірності.

У доповіді описаний метод шифрування відеоданих на основі клітинних автоматів (КА) [8], який дозволяє підвищити надійність захисту відеоінформації, збільшити довжину ключа шифрування, підвищити швидкодію засекречування зображення та спростити підготовку початкових установок блоку формування ключової гами. Описана програмно-апаратна реалізація генератора підключів на основі ПЛІС для системи шифрування та дешифрування відеоінформації.

**Суть зазначеного методу полягає в тому**, що зображення у графічному форматі типу BMP з носія інформації проектують на матричний оптико-електронний дискретний пристрій, здійснюють його сканування по заданому закону та зчитують двійковий код, який кодує колір та яскравість кожної клітини. Отримана послідовність біт представляє з себе послідовне об'єднання кодів кожного дискретного елемента вхідного дискретного пристрою. Кодування зображення також може бути виконано шляхом подання його у вигляді імпульсної послідовності, як описано в роботах [9, 10]. Кожну отриману послідовність імпульсів можливо перетворити у бітову послідовність. Згідно запропонованого алгоритму за допомогою підключів здійснюють потокове шифрування та розшифрування бітової послідовності, що описує зображення.

Для генерації підключів використовують спеціально розроблену структуру, яка реалізована на двох КА. Основний КА здійснює передачу сигналу збудження від клітини до клітини і відноситься до класів асинхронних КА. Додатковий КА здійснює зміну станів усіх власних клітин згідно заданої функції та вибраної околиці. Додатковий клітинний автомат є синхронним. Обидва КА здійснюють ефективне формування псевдовипадкової бітової послідовності та формують ключову гамму для перемішування усіх біт бітової послідовності, що описує вхідне зображення. Гама залежить від початкової карти станів КА та початкових налаштувань траєкторії руху сигналу збудження. Моделі генераторів

псевдовипадкових бітових послідовностей, які реалізовані на синхронних та асинхронних КА, описані у роботі [11].

Для реалізації генератора підключів для системи шифрування відеоінформації на основі КА була обрана мікросхема FPGA Cyclone II (EP2C35F672C6) корпорації Altera з високими показниками по швидкодії (70 Мбіт/с), що дозволяє зашифровувати відеоінформацію в реальному часі в процесі передачі її по каналах зв'язку.

**Література**

1. Патент України на корисну модель № 99465, Бюл. № 11 від 10.06.2015 р.

2. И.Л. Ерош, А.М. Сергеев, Г.П. Филатов. О защите цифровых изображений при передаче по каналам связи. Информационные управляющие системы, N5/2007.

3. А.В. Яковенко, В.В. Ларин, Р.В. Тарнополов. Подходы для защиты видеоинформации на основе устранения избыточности в инфокоммуникациях.// Сучасна спеціальна техніка. - №2(37),- 2014, - С.82-89.

4. Мироновский Л. А., Слаев В. А. Стрип-метод преобразования изображений и сигналов: Монография / СПб.: Политехника, СПб., 2006. 163.

5. L. Tang. Methods for encrypting and decrypting MPEG video data efficiently/ In Proceedings of the ACM Multimedia, Boston, USA, 1996. − P. 219 – 229.

6. H. Cheng and X. Li. On the Application of image Decomposition to Image Compression and Encryption. In P. Horster, editor, Communications and Multimedia Security II, IFIP TC6/TC11 Second Joint Working Conference on Communications and Multimedia Security, Essen, Germany, 1996. − P. 116 – 127.

7. T. Kunkelmann and U. Horn. Partial Video Encryption based on Scalable Coding in International Workshop on Systems, Signals and Image Processing, Zagreb, Croatia, 1998 − P. 215 – 218.

8. Патент України на корисну модель № 112182 від 12.12.2016.

9. Belan S., Belan N.. 2013. Temporal-Impulse Description of Complex Image Based on Cellular Automata. LNCS.- Vol. 7979.- Springer-Verlag Berlin Heidelberg: 291-295.

10. Belan S., Belan N.. 2012. Use of Cellular Automata to Create an Artificial System of Image Classification and Recognition. Springer-Verlag Berlin Heidelberg, ACRI2012, LNCS 7495: 483-493.

11. Bilan, S., Bilan, M., Motornyuk, R., Bilan, A., Bilan, S. (2016). Research and Analysis of the Pseudorandom Number Generators Implemented on Cellular Automata, WSEAS TRANSACTIONS on SYSTEMS, Volume 15, 275 - 281.

УДК 004.056.57

# Порівняльний аналіз негативних наслідків кібератак на критичну інформаційну інфраструктуру різних держав

Дрейс Ю.О., к.т.н., доцент
*Національний авіаційний університет, м. Київ*

Згідно чинного законодавства [1] ***критичною інформаційною інфраструктурою держави*** (далі – КІІД) є включені до переліку інформаційно-телекомунікаційні системи (ІТС) об'єктів критичної інфраструктури, що захищаються власниками (розпорядниками) таких систем від кібератак у першу чергу (пріоритетно) відповідно до законодавства у сфері захисту інформації та кібербезпеки. Тому в основу визначення об'єктів критичної інфраструктури та порядку формування переліку їх ІТС для першочергового захисту від кібератак й покладено саме принцип «негативний наслідок – критична інфраструктура». Отже, питання визначення негативних наслідків, величини та ступеня їх тяжкості, до яких може призвести кібератака на ІТС об'єкта критичної інфраструктури держави та\або КІІД є актуальним.

Також визначене і узагальнене поняття ***КІІД*** як [2]: сукупність ІТС держави та приватного сектору, що забезпечують функціонування та безпеку стратегічних інститутів держави і безпеку громадян.

На основі проведеного аналізу експертних думок та відповідних нормативно-правових документів [1-10] побудовано порівняльну таблицю можливих наслідків кібератак на КІІД у різних державах.

Таблиця 1 – Можливі наслідки кібератак на КІІД у різних державах

| Держава | Негативні наслідки кібератак на КІІД |
|---|---|
| Україна | ***Порядок формування переліку ІТС об'єктів критичної інфраструктури держави*** [1] |
| | *Негативними наслідками є:*<br>- виникнення надзвичайної ситуації техногенного характеру та/або негативний вплив на стан екологічної безпеки держави (регіону) (Н.1);<br>- негативний вплив на стан енергетичної безпеки держави (регіону) (Н.2);<br>- негативний вплив на стан економічної безпеки держави (Н.3);<br>- негативний вплив на стан обороноздатності, забезпечення національної безпеки та правопорядку у державі (Н.4);<br>- негативний вплив на систему управління державою (Н.5);<br>- негативний вплив на суспільно-політичну ситуацію в державі (Н.6);<br>- негативний вплив на імідж держави (Н.7);<br>- порушення сталого функціонування фінансової системи держави (Н.8);<br>- порушення сталого функціонування транспортної інфраструктури держави (регіону) (Н.9);<br>- порушення сталого функціонування інформаційної та/або телекомунікаційної інфраструктури держави (регіону), в тому числі її взаємодії з відповідними інфраструктурами інших держав (Н.10). |
| Російська Федерація | ***Методика віднесення об'єктів державної та недержавної власності до критично важливих об'єктів для національної безпеки Російської*** |

| | |
|---|---|
| | ***Федерації*** [3] |
| | *Значимість об'єкта для економіки держави:*<br>- вартість річного випуску товарної продукції, млн. руб. (П.1);<br>- загальна чисельність виробничого персоналу, тис. осіб (П.2);<br>- балансова вартість основних виробничих фондів, млн. руб. (П.3);<br>- складова основної продукції об'єкта в продукції того ж виду, що випускається в державі % (П.4).<br>*Нанесення шкоди престижу держави:*<br>- порушення керованості держави або регіону (П.5);<br>- нанесення шкоди авторитету держави, у тому числі на міжнародній арені (П.6);<br>- розкриття державних секретів, конфіденційної науково-технічної та комерційної інформації (П.7);<br>- порушення боєготовності та боєздатності Збройних Сил (П.8);<br>- порушення стабільності фінансової і банківської систем (П.9).<br>*Можливі загрози населенню і територіям:*<br>- широкомасштабне знищення національних ресурсів (природних, сільськогосподарських, продовольчих, виробничих, інформаційних) (П.10);<br>- територія зараження (забруднення) у разі аварії на об'єкті (П11);<br>- чисельність населення, яке може постраждати у разі надзвичайної ситуації на об'єкті (П.12);<br>- порушення систем забезпечення життєдіяльності міст та населених пунктів (П.13);<br>- масові порушення правопорядку (П.14);<br>- зупинка безперервних виробництв (П.15);<br>- аварії та катастрофи регіонального масштабу (П.16). |
| Австралія | ***Стратегічним планом Австрійської програми захисту життєво важливої інфраструктури*** [4] |
| | - кількість залучених громадян (здоров'я та соціальні наслідки);<br>- економічний ефект;<br>- вплив на навколишнє середовище;<br>- психологічний ефект;<br>- політичні наслідки;<br>- масштабність за територією;<br>- тривалість;<br>- відсутність варіантів заміщення;<br>- взаємозалежність секторів критичної інфраструктури (наслідком руйнації одного є руйнація інших). |
| Іспанія | ***Законом Королівства Іспанія про встановлення заходів щодо захисту критичної інфраструктури*** [5] |
| | - кількість залучених громадян (загиблі, поранені з тяжкими травмами та іншими серйозними наслідками для здоров'я);<br>- економічний ефект (екон. втрати та погіршення якості продукції та послуг);<br>- вплив на навколишнє середовище;<br>- політичні наслідки (довіра до органів державного управління) та соціальні наслідки (фізичні страждання, порушення повсякденного життя). |
| Швеція | ***Планом дій по захисту життєво важливих суспільних функцій та критичної інфраструктури Королівства Швеція*** [6] |
| | - кількість залучених громадян (біля 30 осіб загиблі або отримали поранення з тяжкими травмами);<br>- настання економічного ефекту або впливу на навколишнє середовище (прямі затрати складають майже 10 млн. євро);<br>- політичні наслідки або соціальний вплив (були вбиті громадяни, неможливість вплинути на інцидент, знизилась довіра до органів державного управління, розпочалось громадянське безладдя, пряма загроза для органів |

| | |
|---|---|
| | державної влади). |
| Нідерланди | ***Директива міністерства безпеки та юстиції Нідерландів щодо підвищення стійкості*** [7] |
| | *Категорія А – порушення інфраструктури будуть мати такі наслідки:*<br>- фінансові втрати держави більше 50 млрд. євро або падіння доходів в реальному виразі близько 5 %;<br>- загинуть, отримають каліцтва або хронічні захворювання більше 10 тис. осіб;<br>- більше 1 млн. осіб стануть на межу виживання або отримають серйозні моральні травми;<br>- щонайменше два інших сектори критичної інфраструктури почнуть руйнуватись.<br>*Категорія В – порушення інфраструктури будуть мати такі наслідки:*<br>- фінансові втрати держави більше 5 млрд. євро або падіння доходів в реальному виразі близько 1 %;<br>- загинуть, отримають каліцтва або хронічні захворювання більше 1тис. осіб;<br>- більше 100 тис.осіб стануть на межу виживання або отримають серйозні моральні травми. |
| Словенія | ***Концепція критичної інфраструктури у Словацькій Республіці, її захисту та оборони*** [8] |
| | *Основні критерії для визначення критичності інфраструктури є порушення системи, що призведе:*<br>- до загибелі більш ніж 50 осіб;<br>- до впливу на здоров'я наслідком якого стане госпіталізація більш ніж 100 осіб терміном на тиждень;<br>- до ускладнення здійснення внутрішньої безпеки держави;<br>- втрат більш ніж 10 млн. євро на день;<br>- неможливості постачання питної води або їжі протягом тижня для 100 тис. осіб;<br>- неможливості постачання електроенергії протягом 3 діб або природного газу протягом тижня для населення більш ніж 100 тис. осіб;<br>- неможливості постачання нафтопродуктів протягом тижня для населення більш ніж 100 тис. осіб;<br>- зараження поверхні більш ніж 100 га;<br>- втрати систем зв'язку протягом доби, що може спричинити збої в підтримці роботи інших критичних систем. |
| Ізраїль | ***Експертне джерело*** [8] |
| | - звичайна (типова) надзвичайна ситуація, коли в разі виникнення якоїсь надзвичайної ситуації страждають в першу чергу географічно близькі об'єкти (малоймовірна для кібератаки);<br>- багаторівневі каскадні збої та надзвичайні ситуації (руйнування системи управління в одній інфраструктурі (наприклад, водовідвідної інфраструктурі) призводить до збою у вторинній інфраструктурі (наприклад, в транспорті), а потім і в третинної (наприклад, ланцюжки поставок продуктів харчування та інших товарів) і т.д., навіть якщо прямий вплив на зазначені інфраструктури і не відбувся (найімовірніший наслідок для успішної кібератаки);<br>- наростаючі (збільшують) відмови (порушення роботи однієї інфраструктура (наприклад, мережі зв'язок) завдає шкоди здатності по відновленню і ліквідація наслідків інших аварій на інших інфраструктурах (відмова ліній зв'язку в ході усунення інший аварії, наприклад, на водоканал). |
| ЄС | ***Директива Європейської Комісії*** [9] |
| | *Масштаб* (географічне охоплення території, для якої втрата елементу критичної інфраструктури завдає значної шкоди) - міжнародний, національний, регіональний або територіальний;<br>*Важкість можливих наслідків за такими показниками:*<br>- вплив на населення (число постраждалих, загиблих, осіб, які отримали значні |

| | |
|---|---|
| | травми, а також чисельність евакуйованого населення);<br>- економічна шкода (вплив на ВВП, розмір екон. втрат, як прямих, так і непрямих);<br>- екологічна шкода (вплив на населення та навколишнє природне середовище);<br>- взаємозв'язок з іншими елементами критичної інфраструктури;<br>- політичний ефект (втрата впевненості в дієздатності влади);<br>- тривалість впливу (як саме і коли проявлятимуться наслідки, пов'язані зі втратою чи відмовою об'єктів критичної інфраструктури). |

Проведено аналіз та часткову уніфікацію можливих негативних наслідків кібератак на КІІД для формування єдиного класифікатора можливих наслідків з метою його подальшого використання при оцінюванні шкоди національній безпеці для визначення ІТС об'єктів критичної інфраструктури держави для першочергового захисту.

**Список літератури**

1. Про затвердження Порядку формування переліку інформаційно-телекомунікаційних систем об'єктів критичної інфраструктури держави / КМУ; Постанова, Порядок від 23.08.2016 № 563 // [Електронний ресурс]. – Режим доступу: http://zakon3.rada.gov.ua/laws/show/563-2016-%D0%BF.

2. Проект Закону «Про внесення змін до деяких законів України щодо забезпечення кібернетичної безпеки України». [Електронний ресурс]. – Режим доступу: http://search.ligazakon.ua/l_doc2.nsf/link1/JF8L100A.html.

3. Методика віднесення об'єктів державної та недержавної власності до критично важливих об'єктів для національної безпеки Російської Федерації : № 2-4-87-23-14. - Офіц.вид. – М. :МНС Росії, від 17.10.2012 р., 29 с. - (Нормативний документ МНС Росії).

4. Masterplan Österreichisches Programm zum Schutz Kritischer Infrastruktur (APCIP - Austrian Program for Critical Infrastructure Protection). [Електронний ресурс]. – Режим доступу: http://www.kiras.at/fileadmin/ dateien/allgemein/MRV APCIP Beilage Masterplan FINAL.pdf.

5. Ley 8/2011, de 28 de abril, por la que se establecen medidas para la protección de las infraestructuras críticas : офіц. текст : Boletín oficial del estado. Núm. 102. Viernes 29 de abril de 2011. Sec. I. Pág. 43370. 192

6. Action Plan for the Protection of Vital Societal Functions & Critical Infrastructure / Swedish Civil Contingencies Agency (MSB). Risk & Vulnerability Reduction Department. Natural Hazards & Critical Infrastructure Section. English Translation: James Butler – MSB. Order No: MSB695 - July 2014. – p. 13.

7. Ministerie van Veiligheid en Justitie. Directie Weerbaarheidsverhoging. 12 mei 2015. [Електронний ресурс]. – Режим доступу: https://www.nctv.nl/ binaries/voortgangsbrief-nationale-veiligheid-12-mei-2015_tcm31-32518.pdf.

8. Гриняев С. О взгляде на проблему безопасности критической инфраструктуры в государстве Израиль / Центр стратегических оценок и прогнозов [Електронний ресурс]. – Режим доступу: http://www.csef.ru/

9. On the identification and designation of European critical infrastructures and the assessment of the need to improve their protection : Council Directive 2008/114/ ЕС. [Електронний ресурс]. – Режим доступу: http://eur-lex.europa.eu

10. Дрейс Ю.О. Аналіз негативних наслідків кібератак на інформаційні ресурси об'єктів критичної інфраструктури держави / Ю.О. Дрейс, Мовчан М.С. // «Актуальні питання забезпечення кібербезпеки та захисту інформації»: тези доповідей учасників ІІІ Міжнародної наук.-практ. конференція (Закарпатська обл., Межигірський р-н, с. Верхнє Студене). – К: Вид-во Європейський університет, 2017. – (212 с.) – С.71-74.

УДК 004.056

**Модель інформаційного впливу**

Дудатьєв А.В., к.т.н., доцент,
Дудатьєва В.М., асистент,
Літушко О.А., студентка
*Вінницький національний технічний університет, м. Вінниця*

Національна безпека України у великій мірі залежить від стану комплексної інформаційної безпеки держави**.** У Доктрині інформаційної безпеки України зазначено, що одним з національних інтересів України в інформаційній сфері є захищеність від руйнівних інформаційно-психологічних впливів.

Проведення спеціальних інформаційно-психологічних операцій (ІПО) можуть викликати різні зміни в соціотехнічній системі (СТС), пов'язані зі зміною структури системи чи зміні зв'язків між елементами системи. Ці зміни можуть викликати перехід системи із початкового або стійкого стану в інший нестійкий стан. З урахуванням того, що СТС є багаторівневою системою, то і ризики деструктивного інформаційного впливу, в залежності від рівня впливу, можуть бути принципово різними. Результатом такого впливу можуть бути "потрібні" дії для супротивника, що можуть привести до нестійкого стану всієї системи. В першу чергу це актуально для систем управління так званих критичних систем, зокрема енергетичних систем, транспортних систем, військових систем тощо. Спеціальні інформаційні операції є механізмом проведення інформаційної війни, головною метою якої є перепрограмування свідомості людини. Саме тому розробка моделі розповсюдження інформаційних впливів у соціальній частині СТС є актуальною задачею.

**Основна частина.** Інформаційний вплив може бути реалізований з використанням двох каналів впливу: зовнішнього і внутрішнього. Зовнішній канал представляє всі потенційні канали або джерела впливу, які можна представити у вигляді такої множини:

$$Kan = \{Zmid, Tv, Int, Rm, Rk, Sp, Sz, Ld\}, \quad (1)$$

де: *Zmid* – друковані ЗМІ, *Tv* – телебачення, *Int* – мережа Internet, *Rm* – засоби радіомовлення, *Rk* – різноманітні реклами, *Sp* – канали, які реалізуються спеціальними засобами, *Sz* – канали впливу, які реалізуються проведенням масових заходів, які можуть бути представлені акціями масового протесту або підтримки, різноманітними фестивалями, зустрічами з впливовими людьми та відомими діячами, *Ld* – канал інформаційного впливу, який реалізується людиною, що знаходиться за межами соціуму, на який спрямований деструктивний вплив і яка стає джерелом розповсюдження спеціально підготовленої інформації.

Внутрішній канал розповсюдження реалізується через міжособистісне спілкування елементів соціуму. Тут також можуть бути випадкові люди, які

отримують зовні спеціально підготовлену інформацію і передають її іншим елементам соціуму, часто у спотвореному вигляді. За таким сценарієм процес розповсюдження інформації стає практично некерованим, а елемент соціуму стає каналом інформаційного впливу. У другому випадку внутрішнім каналом розповсюдження може бути спеціально підготовлена людина, яка розповсюджує спеціальну інформацію і цілеспрямовано займається пропагандою, агітацією тощо.

Запропонована модель розповсюдження інформаційного впливу, яка описує динаміку кількісних змін у соціумі, яку моделюють S-образною кривою, що характеризує так звані моделі "дифузії інновацій" [1]. Враховуючи показники зростання кількості змін у соціумі відповідно до S-образної кривої використаний експоненціальний закон розподілу умовних переходів елементів соціуму з початкового стану в інший. Доцільність експоненціального закону обґрунтовується також тим, що цей розподіл не враховує попередню історію розвитку системи, але враховує так звані "скриті дефекти" системи, які можна інтерпретувати як наявність завербованих елементів соціуму або наявність підготовлених внутрішніх каналів впливу.

Представлена модель враховує ймовірну кількість осіб, яка може підпасти під ефективно проведений інформаційний вплив [2], час до перших змін у соціумі, а також загальний час проведення спеціальної інформаційної операції.

**Висновки.** Світовий досвід показує, що проведення спеціальних інформаційних операцій є ефективною технологією проведення інформаційних війн. Запропонована модель інформаційного впливу базується на результатах аналізу мети його реалізації, можливих каналах розповсюдження інформації, базових ознаках об'єктів інформаційного впливу, аналізу можливостей соціуму щодо сприйняття деструктивного впливу тощо. Запропоновані моделі пропонується використовувати при побудові системи комплексного інформаційного захисту у відповідності до ISO/IEC 27001:2013.

**Список літератури**

1. Губанов Д.А., Новиков Д.А., Чхартишвили А.Г.Социальные сети: моделт информационного влияния, управления и противоборства /Д.А. Губанов, Д.А. Новиков, А.Г. Чхартишвили – М.: Физматлит, 2010. – 225 с.

2. Дудатьев А.В., Лужецкий В.А., Коротаев Д.О. Метод оценки информационной устойчивости социотехнических систем в условиях информационной войны / А.В. Дудатьєв, В.А Лужецкий, Д.А. Коротаев // Восточно-Европейский журнал передовых технологий. – 2016. – № 1. – С.4-11.

УДК 004.056:004.77

## Метод організації захищеного бездротового каналу з інтегрованим стегоконтейнером для моніторингової мережі відеокамер

Журавська І.М., к.т.н., доцент
*Чорноморський національний університет ім. Петра Могили, м. Миколаїв*

Для виконання завдань відеоаналізу просторово-розподілених об’єктів сучасним рішенням є створення гетерогенних (кабельних та бездротових, побудованих за різними технологіями) мереж відеокамер. Характерною проблемою є низька захищеність каналів зв'язку саме у мережах відеоспостереження. Використання стеганографічного підходу для вирішення передачі інформації з обмеженим доступом (ІзОД) є визнаним та дуже швидко поширюваним підходом. Але необхідно обирати між надійністю, швидкістю та енергоємністю передачі даних у системах з обмеженими обчислювальними потужностями. Такими є безпілотні літальних апаратів (БПЛА), де встановлені обговорювані відеокамери. Питанням захисту каналів передачі ІзОД у мобільних моніторингових мережах приділено недостатньо уваги.

Запропоновано метод організації безпечного каналу передачі даних в моніторинговій мережі відеокамер з використанням інтеграції стегоконтейнерів у вільні біти RGB-характеристик пікселів відеокадрів на основі алгоритму створення випадкової послідовності.

**Структура стегоконтейнеру при передачі даних.** Зазвичай в обчислювальних системах RGB-простір надають у вигляді кубу, кожна з координат якого представляють одним байтом. Разом вони займають 24 біта [1]. Але, для економії бітрейту, зазвичай у відеокамерах БПЛА використовують щонайбільше 16-бітний колір (з діапазоном відтінків 0–65535). Таким чином, в структурі RGB-значень пікселя 8 останніх (молодших) бітів можна «забрати» для утворення стегоконтейнера. Зміна зазначених бітів призводить до зміни числа лише на $3{,}04 \cdot 10^{-5}$ відсотка. Така дуже мала величина не порушує цілісність даних.

**Організація захищеного каналу за допомогою стегоконтейнерів.** Враховуючи вищезазначене, запропоновано метод, який дозволяє організувати захищений канал збору даних від віддалених відеокамер з використання стегоконтейнеру створення випадкової послідовності.

Для прихованої передачі GPS-координат об’єктів моніторингу такі координати можуть бути записані в 4 дійсних числа, кожне з яких має розмір 32 біти. Разом це становить $4 \cdot 32 = 128$ бітів даних.

Але на розкриття стегоконтейнеру такого розміру, побудованого за класичним алгоритмом, достатньо біля півгодини [2].

Тому доцільно посилити алгоритм стеганографії додатковими кроками впровадженням випадкової послідовності. В такому випадку алгоритм

набуває наступного вигляду:

1. Отримати GPS-координати об'єктів на кадрах відеопотоку, які не будуть стискатись [3].

2. Представити ці координати у вигляді послідовності бітів за допомогою функції, яка інтерпретує числа як послідовність бітів.

3. Представити молодші 8 бітів кожного числа даних про RGB-значення пікселя у вигляді послідовності бітів.

*Крок 3а. Обрати ключ (seed), за яким будується випадкова послідовність.*

*Крок 3б. Створити (seq) послідовність від 1 до n.*

4. Отримати *i*-й біт GPS-координат об'єктів.

5. Записати цей біт у *i*-й біт даних про RGB-значення пікселя.

6. Якщо є наступний біт, перейти до 2-го пункту; інакше завершити формування пакету даних.

7. За допомогою обраного протоколу переслати повідомлення іншому агенту Ad Hoc мережі (безпосередньо або через трансферний вузол).

8. На приймачі дані розкриваються за такою ж послідовністю чисел.

У такому разі, при розмірі даних 128 бітів, по формулі перестановок при спробі стегоаналізу знадобиться перебрати 128! варіантів.

**Висновки.** Запропонований метод організації захищеного бездротового каналу з інтегрованим стегоконтейнером для моніторингових мереж відеокамер. Впровадження розробленого алгоритму створення випадкової послідовності у стеганографічні перетворення потребує виконати більше ніж $3{,}856 \cdot 10^{215}$ перестановок для розкриття ІзОД у разі перехвату та стегоаналізу даних. Такий рівень криптостійкості є достатнім для забезпечення захисту інформації протягом часу її актуальності.

**Список літератури**

1. Singh K.U. Video steganography: text hiding in video by LSB substitution // International Journal of Engineering Research and Applications. – 2014. – Vol. 4, № 5(1). – P. 105–108.

2. Sloan T., Hernandez-Castro J. Forensic analysis of video steganography tools // PeerJ Computer Science. – 2015, May 27. – № 1:e7. – P. 1–16. doi: 10.7717/peerj-cs.7.

3. Burlachenko I., Zhuravska I., Musiyenko M. Method for video cameras' active coordination in optical navigation based on multi-agent approach // Eastern-European Journal of Enterprise Technologies. – 2017. – Vol. 1, № 9(85). – P. 17–25.

УДК 004.9

# Применение биометрических технологий в системах контроля доступа

Иашвили Г.Н., докторант,
*Грузинский Технический Университет, г. Тбилиси, Грузия*

Развитие информационных технологий предоставило широкие возможности использования биометрических методов и средств для повышения безопасности и удобства различных систем, требующих подтверждения личности пользователя. Сегодня биометрические технологии применяются в самых разных сферах – от организации доступа к рабочим местам до идентификации личности при осуществлении платежных операций.

В отличии от традиционных систем контроля доступа (СКД), работающих с различными электронными картами, в биометрических СКД идентификаторами являются палец, лицо, рука, сетчатка глаза и другие показатели личности.

Биометрические СКД позволяют решать следующие вопросы:

– предотвратить проникновение злоумышленников на охраняемые территории и в помещения за счет подделки, кражи документов, карт, ключей, паролей;

– обеспечить допуск к ответственным объектам только сертифицированных специалистов;

– исключить неудобства связанные с утерей, порчей ключей, жетонов, карт, паролей;

– организовать учет доступа лиц в помещения и на территории.

Предлагается построение системы биометрического контроля доступа на базе нескольких биометрических показателей личности человека. Например, это может быть одновременное применение трех показателей: отпечаток пальцев, геометрия лица и радужная оболочка глаза.

Применение трех биометрических характеристики личности с одной стороны значительно улучшит качество идентификации. Но с другой стороны при этом также значительно ухудшается эргономические показатели системы, т.к. идентификация личности одновременно по трем показателям не очень комфортна.

Разработаны схемы СКД с двумя и тремя биометрическими показателями, которые гарантируют, что право на доступ, нахождения и передвижения в помещениях (на территории объекта) получит личность с конкретными биометрическими показателями.

УДК 004.9

# Идентификация личности избирателя для повышения безопасности системы голосования

Имнаишвили Л.Ш., д.т.н.,
Иашвили Г.Н., докторант,
Бединеишвили М.М., д.т.н.
*Грузинский Технический Университет, г. Тбилиси, Грузия*

Современные информационные технологии дают возможность использовать биометрические методы и технологии для повышения эффективности и, что самое главное, безопасности различных систем, требующих подтверждения личности пользователя. Биометрические технологии применяются в самых разных сферах – от организации доступа к рабочим местам до идентификации личности при осуществлении платежных операций. Особенно актуально внедрение этих новейших средств защиты при ведении электронного бизнеса, осуществлении банковской деятельности. С уверенностью можно говорить о том, что скоро без биометрических технологий не можно будет решать проблемы идентификации личности во многих сферах.

В последние годы в избирательных процессах стали применять биометрические технологии, т.к. они наиболее успешно решают главную проблему выборов – гарантированную идентификацию избирателей.

Исследования последних лет подтверждают, что биометрические методы и технологии почти полностью исключают при проведении выборов не только нарушения, но и ошибки и преднамеренные фальсификации. США, Канада, Бразилия, Индия, многие страны Европы и некоторые другие страны имеют определенный опыт автоматизации и электронизации процессов выборов. В этом направлении продвинулись и некоторые постсоветские государства. Определенные эксперименты проводятся в Беларуси, Казахстане и России. На практике было установлено, что только применение биометрических методов, технологий и технических средств дает возможность исключить фальсификации не только при подготовке списков избирателей, но и непосредственно в самом процессе голосования.

Для биометрической идентификации можно применять различные характеристики и черты человека, которые подразделяются на статические, связанные с его физическими характеристиками, например, отпечатком пальца или формой уха, и динамические (или поведенческие), связанные с особенностями выполнения человеком каких-либо действий, например, походка.

На сегодняшний день из биометрических признаков идентификации наиболее разработано распознавание отпечатков пальцев (дактилоскопия). Основным преимуществом данного метода является высокая достоверность. Еще раз следует подчеркнуть, что наиболее развитыми на данный момент технологиями являются распознавание по отпечатку пальца, радужной оболочке глаза и изображению лица. Причем дактилоскопическая идентификация по применимости и доступности с финансовой точки зрения превосходит все другие технологии в несколько раз.

Выбор типа биометрической характеристики человека во многом определяет структуру избирательной системы и поэтому при выборе биометрических показателей необходимо учитывать следующие основные требования к биометрическим показателям: высокая надежность, устойчивость к фальсификациям, стабильность по времени, приемлемость, эргономичность и ряд других.

В Грузинском Техническом Университете в течении нескольких лет ведутся научно-исследовательские работы по применению биометрических технологий в избирательных процессах. Получены и практические результаты. Более шести лет находится в эксплуатации система биометрической регистрации педагогов на всех факультетах университета.

Предложена новая структура избирательной системы с использованием не одного, а одновременно трех биометрических характеристик избирателя. Применение трех биометрических характеристик значительно улучит качество идентификации избирателя. Однако при этом значительно ухудшаются эргономические показатели системы, т.к. идентификация избирателя одновременно по трем показателям не очень комфортна. Для решения данного вопроса предлагается следующий подход: в процессе составления списка избирателей каждый избиратель проходит исходную биометрическую регистрацию по трем показателям. При этом оценивается уровень качества всех трех показателей каждого конкретного избирателя, и устанавливаются соответствующие коэффициенты. Это дает возможность идентифицировать пришедшего на участок избирателя по тому показателю, у которого лучший показатель качества, т.е. у которого коэффициент больше.

В случае положительного ответа избиратель считается регистрированным. В случае отрицательного ответа избиратель проходит идентификацию по другому, показателю (у которого уровень качества следующий).

УДК 004.056.5

## Захист персональних даних в Інтернет

Коваль В.О. студент 2 курсу,
Константинова Л.В., викладач
*Центральноукраїнський національний технічний університет, м.Кропивницький*

Сучасні суспільні відносини вимагають не тільки вільного руху персональних даних, а й забезпечення їх надійного захисту. Прогрес у галузі інформаційних технологій, активність у створенні баз персональних даних створили загрози захисту приватного життя фізичних осіб, інших основних прав і свобод людини. Тому питання захисту персональних даних в Інтернет на сьогодні є актуальними і вимагають уваги.

В Законі персональні дані визначаються як: «відомості чи сукупність відомостей про фізичну особу, яка ідентифікована або може бути конкретно ідентифікована» [1].

У повсякденному житті люди залишають після себе цифрову інформацію про те: кому дзвонять, куди ходять, якій їжі віддають перевагу, що і де купують, де живуть і інші відомості про особисте життя. Інформація про суб'єкта збирається постійно, як тільки він звертається до лікувального закладу, оплачує комунальні послуги, укладає договір на послуги зв'язку і т. п. За цими даними можна дізнатися більше, ніж власне люди хотіли б про себе розповісти. Цифрові технології дозволяють досліджувати мільярди індивідуальних взаємодій, в ході яких люди обмінюються ідеями, грошима, товарами і чутками.

Доволі поширеним явищем є випадки незаконного збору та поширення персональних даних в системі органів внутрішніх справ та правоохоронних органів загалом, наприклад, незаконна дактилоскопія осіб. Порушенням є також поширення медичної інформації, збір банківськими установами надлишкової інформації тощо [1].

Згідно зі статистичними даними, більше 80% компаній несуть фінансові збитки через порушення цілісності та конфіденційності даних, що використовуються [2].

Дослідження ВГО «Українська асоціація захисту персональних даних» виявили вкрай низький рівень відкритості та прозорості обробки персональних даних в Інтернет [3]. Водночас, дослідження компанії GfK Ukraine показують, що українці в 85% випадків ознайомлюються з політикою приватності Інтернет-ресурсу, який вони відвідують. Понад 30% користувачів знають про існування Cookies та досить добре обізнані щодо механізму їх роботи. Понад 54% учасників дослідження підтвердили, що не мають достатньо знань для того, щоб управляти ними.

22% опитаних відповіли, що уважно прочитали інформацію щодо захисту персональних даних на сайті GfK Ukraine.

Користувачі мережі повинні постійно дотримуватися правил, щоб убезпечити свої персональні дані [2]:

1. Стежити за тим, яка інформація пересилається в повідомленні і кому.

2. Завжди уважно вивчати угоди про обробку персональних даних на сайтах, якими користуються.

3. Не довіряти важливу інформацію сайтам, які не містять угоди про обробку персональних даних.

3. Не прив'язувати банківську карту до платіжної системи сайту при користуванні послугами електронної комерції.

4. Звертатися до відповідних контролюючих органів при виявленні порушень законодавства в сфері захисту персональних даних.

Забезпечення безпеки персональних даних є одною з важливих проблем. Питання взаємодії з Європолом і Євроюстом можливі тільки за наявності належної системи захисту персональних даних [4].

Технологічний прогрес створює все ширше коло потреб та можливостей для збору та обробки персональних даних, а власне персональні дані знаходять все ширше використання в найрізноманітніших сферах. Нові технології, з одного боку, істотно спростили збір, обробку, зберігання, передачу даних, а з іншого – створили очевидні загрози їх незаконного обороту, що призводить до порушень прав особистості. У зв'язку з цим, розвиток системи захисту персональних даних є одним із найбільш актуальних завдань, які стоять перед українським суспільством на сучасному етапі.

**Список літератури**

1. Бем М. В., Городиський І. М., Саттон Г., Родіоненко О. М. Захист персональних даних: Правове регулювання та практичні аспекти: науково-практичний посібник. – К.: К.І.С., 2015. – 220 с.

2. Германова В.А. Атабекян А.С. Проблемы защиты персональных данных в сети интернет// Символ науки №12-3. -2016 [Електронний ресурс]. - Режим доступу: http://cyberleninka.ru/article/n/problemy-zaschity-personalnyh-dannyh-v-seti-internet

3. Козак В. Захист персональних даних та правила приватності при дослідженнях в Інтернет [Електронний ресурс]. - Режим доступу: http://uam.in.ua/upload/medialibrary/de7/de7199d7eeaf41d8582cbff76d2f4368.pdf

4. Маркіян Бем Незаконне поширення персональних даних громадян в інтернеті – одне з головних порушень прав людини в частині захисту персональних даних [Електронний ресурс]. – Режим доступу: http://www.ombudsman.gov.ua/ua/all-news/pr/28415-fp-sekretariat-upovnovazhenogo-razom-iz-gromadskistyu-obyednuyut-zusillya/

УДК 004.056

## Дослідження методів протидії тероризму у соціальних мережах

Константинова Л.В., викладач
*Центральноукраїнський національний технічний університет, м. Кропивницький*

Соціальні мережі сьогодні є приводом для обговорення і негативних явищ, таких як тероризм. Члени екстремістських рухів і терористичних груп завдяки новим засобам і способам комунікації, спрощення доступу до інформаційних ресурсів отримали можливість поширювати свою ідеологію, переконання в соцмережах, де чисельність аудиторії може досягати мільйонів. Тероризм, як явище глобального характеру, вважають ключовою проблемою сучасної безпеки [1]. Тому дослідження аспектів застосування інформаційної складової в тероризмі та питання про роль соціальних мереж, як інформаційної зброї у поширенні тероризму є актуальними та потребують уваги.

Під виглядом «обміну думками» в соцмережах в терористичних цілях застосування інформації включає пропаганду тероризму, вербовочну діяльність, збільшення кількості «співчуваючих» та навчання охочих [2].

У мережі функціонує велика кількість новинних агентств і сайтів безпосередньо не афілійованих з терористичними організаціями, але які поділяють їх ідеологію і надають терористам підтримку в різних формах. Багато сайтів спеціально постійно змінюють свої адреси, а в структури терористичних об'єднань все частіше входять хакери.

З огляду на те, що в соціальних мережах часто вказується особиста інформація, можливо цілеспрямоване поширення матеріалів, реклама спільнот, наприклад, для певної вікової групи користувачів для здійснення максимального впливу на них [3].

Протидія тероризму у соціальних мережах полягає у таких основних методах:

1. Постійний моніторинг соціальних мереж та виявлення терористичного контенту [4].
2. Блокування злочинної інформації [5].
3. Контрпропаганда. Аргументована критика тих чи інших положень, пряме викриття протиставленням істини екстремістським інсинуаціям [6].

Контрпропаганда повинна ґрунтуватись на наступних методологічних принципах [6]:

- наступальності – застосування таких методів і засобів, які розкривають реакційність, антигуманність, аморальність як ідеологічних установок, так і практичних кроків екстремістських лідерів;

- попередження – формування у громадян з дитинства установки на віротерпимість, повагу прав і свобод особистості, неприйняття ідеології тероризму; шанобливе ставлення до традиційних релігій;

- оперативності – здійснення поряд з постійним інформуванням населення позачергових заходів, викликаних різкими змінами обстановки.

Необхідно за допомогою фахівців теологів, соціологів, істориків та інших створювати агітаційно-пропагандистський продукт протидії ідеології екстремізму і тероризму і розміщувати цей продукт в соцмережах, популяризувати його за допомогою активних і популярних блогерів.

Для ефективної боротьби з пропагандою тероризму в соціальних мережах необхідна наявність дієвого механізму щодо здійснення безперервного моніторингу і контент-аналізу та оперативного блокування шкідливого контенту і вживання заходів у рамках законодавства щодо осіб, які розповсюджують цей контент.

**Список літератури**

1. Андреев М.В. Международный терроризм и международная безопасность нового качества // Закон и право. № 8. -М. :ЮНИТИ-ДАНА, 2008. -120 с.

2. Кубякин Е.О. Тенденции развития молодежного екстремизма в условиях прогресса информационно компьютерных технологий // Вестник МГИМО университета. №3(30). -2013 [Электронный ресурс]. – Режим доступа: http://cyberleninka.ru/article/n/tendentsii-razvitiya-molodezhnogo-ekstremizma-v-usloviyah-progressa-informatsionno-kompyuternyh-tehnologiy

3. Гладышев-Лядов В. Социальные сети как инстумент для пропаганды экстремизма // Обзор.НЦПТИ №2. -2013 [Электронный ресурс]. – Режим доступа: http://cyberleninka.ru/article/n/sotsialnye-seti-kak-instrument-dlya-propagandy-ekstremizma

4. Троегубов Ю. Н. Проблемы противодействия экстремизму в сети Интернет // Гуманитарный вектор.Серия: История, политология №3(39). -2014 [Электронный ресурс]. – Режим доступа: http://cyberleninka.ru/article/n/problemy-protivodeystviya-ekstremizmu-v-seti-internet

5. Канунникова Н. Г. Юридическая наука и правоохранительная практика // №3(29). -2014 [Электронный ресурс]. – Режим доступа: http://cyberleninka.ru/article/n/zarubezhnyy-opyt-protivodeystviya-mezhdunarodnomu-ekstremizmu-i-terrorizmu

6. Александров А.Г. Распространение молодежного экстремизма в глобальной сети интернет // Вестник Краснодарского университета МВД России №1(23). -2014 [Электронный ресурс]. – Режим доступа: http://cyberleninka.ru/article/n/rasprostranenie-molodezhnogo-ekstremizma-v-globalnoy-seti-internet

УДК 004.77:004.056

**Технічні засоби батьківського контролю онлайн-поведінки дітей**

Кухарська Н.П., к.ф.-м.н., доцент
*Львівський державний університет безпеки життєдіяльності, м. Львів*

Мережа Інтернет, разом з її ризиками і загрозами [1-2], стала невід'ємною частиною життя сучасних дітей. Новими стандартами початкової школи передбачено, що кожна дитина повинна мати доступ до комп'ютера, мережі Інтернет, а також набувати відповідного рівня медіаграмотності з метою протистояння інформаційній агресії.

Яке ставлення батьків до того, що їх діти є повноцінними громадянами цифрового світу і активно беруть участь у його розбудові?

Думка батьків доволі суперечлива. З одного боку, вони бачать переваги у використанні дітьми мережі Інтернет, які полягають, перш за все, у можливості дистанційно користуватися електронними освітніми ресурсами, швидко отримувати потрібну інформацію, у різноманітності її вибору. Батьки розглядають Інтернет як своєрідне джерело неформальної освіти та провідний чинник соціалізації дітей, що забезпечує їх комунікацію в онлайні. Разом з тим, мережа Інтернет має і негативний бік. На думку батьків, вона "затягує" дітей у свої тенета, відволікає їх від навчання, перенасичена неправдивою і психологічно шкідливою інформацією, перешкоджає живому спілкуванню дітей.

Європейські дослідники на основі результатів, отриманих у рамках проекту EU Kids Online II [3], виокремлюють п'ять можливих типів медіації батьків у процесі використання дітьми Інтернету.

- Активна медіація при використанні Інтернету – батьки присутні під час користування дитиною мережею Інтернет і допомагають їй.
- Активна медіація безпеки дитини в Інтернеті – батьки спілкуються з дитиною щодо безпечної поведінки в Інтернеті, дають поради.
- Обмежуюча медіація – батьки встановлюють правила і обмеження користування Інтернетом.
- Моніторинг – постійна перевірка батьками сайтів, котрі відвідує дитина, її контактів, повідомлень, профілів.
- Технічні обмеження передбачають використання батьками спеціальних програм, котрі дають змогу блокувати і фільтрувати сайти; відстежувати які саме сайти відвідує дитина; обмежувати доступ до мережі по днях та годинах; визначити типи файлів, доступні і заборонені для скачування; контролювати і обмежувати листування з конкретними користувачами в соціальних мережах, а також пересилання персональної інформації через Інтернет-пейджери, тощо.

Батьки українських дітей надають перевагу обмежуючій медіації. Вони

воліють діяти по-старому: заохочувати дітей, карати їх, встановлювати правила і проводити виховну роботу з ними. На жаль, багато батьків не знають про програмні засоби захисту дітей від Інтернет-загроз, про переваги їх використання, а деякі просто недооцінюють онлайн-ризики. Батьківський контроль за допомогою програмного забезпечення – нова можливість, яка наразі не знайшла належного зацікавлення у тих, кому вона адресована. Причин декілька: у першу чергу, як було зауважено вище, це незнання ризиків мережі Інтернет, надмірна зайнятість сучасних батьків, низький рівень їх комп'ютерної грамотності, чим можна пояснити зволікання, інертність у вирішенні питань інформаційної безпеки дітей.

Для більшої переконливості того, що технічними засобами батьківського контролю не слід нехтувати, а варто активно використовувати їх, наведемо результати тестування незалежного інформаційно-аналітичного центру Anti-Malware, який перевіряв ефективність фільтрування небажаних для дітей Інтернет-сайтів чотирнадцятьма популярними програмами. Найкращим виявився KinderGate Parental Control. Він заблокував 99 % небажаних для дітей сайтів, продемонструвавши при цьому 0,3 % помилкових спрацювань. Зовсім трохи відстав від лідера Kaspersky Internet Security, що заблокував понад 98 % небажаних сайтів. Його рівень помилкових спрацювань не перевищив 1 % [4].

**Висновки.** Батькам не слід кидати дітей в їх онлайновій діяльності напризволяще. Необхідно приділяти максимально серйозну увагу підвищенню рівня обізнаності дітей щодо загроз мережі Інтернет, сприяти формуванню їх медіаграмотності, а також на повну силу використовувати можливості, які пропонують технічні засоби батьківського контролю, з метою захисту дітей від медіаконтенту, що може зашкодити їх здоров'ю та розвитку.

**Список літератури**

1. Задорожна Х. О. Аналіз загроз інформаційній безпеці дітей в мережі Інтернет // Задорожна Х. О., Кухарська Н. П. / Інформаційна безпека та комп'ютерні технології : Міжнар. наук.-практ. конф., 24-25 березня 2016 р., м. Кіровоград, Україна : зб. тез доповідей. – Кіровоград, Вид-во КНТУ, 2016. – С. 38-39.

2. Кухарська Н. Цифрове дитинство: соціалізація і безпека / Кухарська Н., Задорожна Х. // Інформаційна безпека в сучасному суспільстві : ІІ Міжн. наук.-практ. конф. 24-25 листопада 2016 р., м. Львів, Україна : матер. конф. – Львів, Вид-во ЛДУ БЖД, 2016. – С. 55-57.

3. Russian Kids Online. Key findings of the EU Kids Online II survey in Russia // Galina Soldatova, Elena Rasskazova, Ekaterina Zotova, Maria Lebesheva, Marina Geer and Polina Roggendorf. – M : Foundation For Internet Development, 2013. – 235 p.

4. Тест родительских контролей (декабрь 2014) [Электронный ресурс]. – Режим доступа : https://www.anti-malware.ru/parental_control_test_2014

УДК 621.396.253

## Дослідження механізмів формування псевдовипадкових чисел

Лисенко І.А., асистент
*Центральноукраїнський національний технічний університет, м. Кропивницький*

Життєвий цикл системи захисту інформації складається з декількох етапів, найважливішими з яких є визначення послуг безпеки і вибір механізмів безпеки.

Визначено п'ять загальноприйнятих послуг безпеки: автентифікація, управління доступом, конфіденційність даних, цілісність даних, неможливість відмови (причетність).

Приведені послуги безпеки забезпечуються за допомогою механізмів безпеки, які складаються з таких основних елементів, як: механізми шифрування, механізми цифрового підпису, механізми керування доступом, механізми цілісності даних, механізми автентифікації.

Механізми шифрування припускають використання криптографічних перетворень даних. Значну частину серед них займає розробка перспективних методів і алгоритмів формування псевдовипадкових чисел.

До криптографічних методів формування псевдовипадкових чисел ставляться все більш високі вимоги як до швидкодії так і до стійкості. Особливе місце в області формування псевдовипадкових чисел займають методи, засновані на зведенні задачі криптоаналізу до розв'язання деякої добре відомої теоретико-числової задачі. Проте методи, засновані на доказово стійких перетвореннях володіють високими характеристиками статистичної безпеки, але є складними в реалізації і не формують псевдовипадкових послідовностей максимального періоду.

Таким чином існуючий математичний апарат, відомі методи та алгоритми формування псевдовипадкових чисел не дозволяють повною мірою забезпечити високі показники ефективності.

Для розв'язання цієї задачі необхідна розробка методів і алгоритмів формування псевдовипадкових чисел доказової стійкості, реалізація яких дозволить будувати генератори псевдовипадкових чисел з необхідними для практики властивостями.

Перспективним напрямком у цьому випадку є генератори псевдовипадкових чисел з використанням надлишкових кодів. Тоді завдання криптоаналізу зводиться до розв'язання задачі декодування випадкового коду, а відповідні методи формування псевдовипадкових чисел відносять до групи доказово стійких генераторів, які до того ж володіють високими показниками швидкодії як при програмній так і при апаратній реалізації.

УДК 003.26:004.056.55(043.2)

## Симетричний блоковий шифр LaKi

Лозінський І.Л., студент 5 курсу,
Степаненко І.В., студент 5 курсу
Науковий керівник – Кінзерявий В.М., к.т.н.
*Національний авіаційний університет, м. Київ*

З кожним днем інформатизація суспільства переходить все на вищий рівень. Більшість інформації зберігається в електронному вигляді. Персональні дані, листування, комерційні та державні таємниці, інша оцифрована цінна інформація, що не підлягає розголошенню – потребує надійного захисту. Для цього, зокрема, використовують криптографічні засоби, спрямовані на забезпечення конфіденційності інформації. Враховуючи стрімкий розвиток інформаційних технологій, такі засоби потребують постійного розвитку, тому виникає проблема розробки нових та вдосконалення вже існуючих криптографічних алгоритмів захисту даних.

Метою роботи є підвищення ефективності захисту даних за рахунок розробки нового блокового шифру LaKi.

Даний шифр побудований на основі симетричного блокового криптографічного алгоритму RC6, що має гнучку структуру. У якості параметрів алгоритм RC6 використовує розмір слова (субблока), кількість раундів та розмір секретного ключа. В конкурсі AES криптографічний алгоритм RC6 використовував наступні параметри: 32 біта – довжина субблока; 20 раундів шифрування; розмір секретного ключа 32 байта. Структура алгоритму RC6 передбачає застосування наступних операцій:

- часткове вхідне та вихідне відбілювання;
- операція побітового додавання за модулем 2;
- операція арифметичного додавання за модулем $2^{32}$;
- функція порозрядного циклічного зсуву;
- функція $f$, що виконує наступне квадратичне перетворення: $f(x) = x*(2x+1) \bmod 2^{32}$.

При розробці блокового шифру LaKi запропоновано змінити наступні параметри та операції у порівнянні із алгоритмом RC6:

- збільшити довжину субблока даних до 64 біт;
- зменшити кількість раундів шифрування до 16;
- збільшити довжину секретного ключа до 64 байт;
- удосконалити процедуру розширення раунових ключів;
- при шифруванні використовувати операції повного вхідного та вихідного відбілювання;
- використовувати операції арифметичного додавання за модулем $2^{64}$;

- повністю замінити використовувану при шифруванні функції $f$.

Запропонована функція $f$ обробляє 64-бітний вхідний субблок:

- субблок ділиться на 8 фрагментів по 8 біт кожен;
- над даними фрагментами виконується операція підстановки відповідно до визначених таблиць замін;
- результат замін множиться на фіксовану матрицю $M$.

Схема процедури шифрування блокового шифру LaKi зображена на рис. 1.

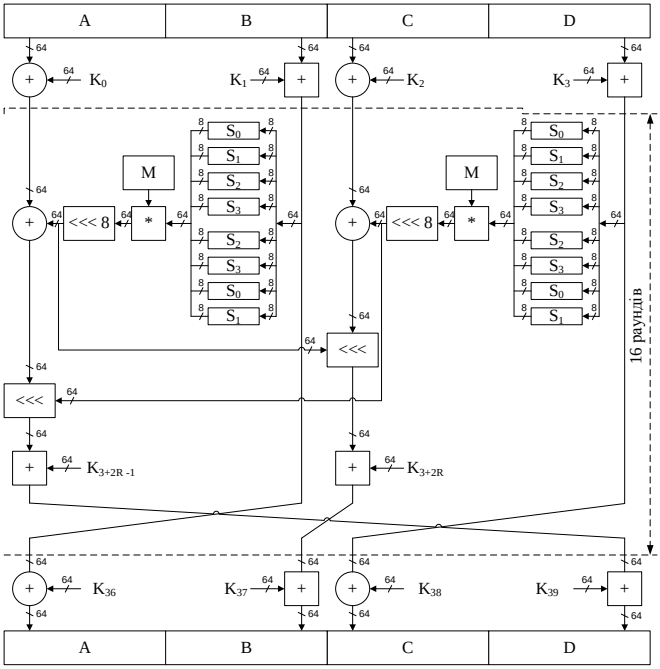



Рис. 1. Схема процедури шифрування блокового шифру LaKi

**Висновки.** Таким чином, запропоновано блоковий шифр LaKi, розроблений на основі криптографічного алгоритму RC6, може підвищити ефективність захисту даних, проте в майбутньому слід провести експериментальні та теоретичні дослідження для визначення його швидкісних характеристик, статистичних показників та стійкість проти відомих методів криптоаналізу.

**Список літератури**

1. Блоковий симетричний шифр «LaKi» / В.М. Кінзерявий, Р.О. Кулій, І.Л. Лозінський, І.В. Степаненко // Вісник Інженерної академії України. – 2016. – №2 – С. 76-80.

УДК 004.056.53

**Критерии обнаружения угроз безопасности по цели сетевого воздействия**

Мартовицкий В.А., аспирант
Научный руководитель – Рубан И.В., д.т.н., профессор
*Харьковский национальный университет радиоэлектроники, г. Харьков*

Сегодня обнаружение сетевых атак является одной из наиболее острых проблем сетевых технологий. Известен обширный перечень угроз информационной безопасности сетевых технологий, содержащий сотни позиций. Рассмотрение возможных угроз информационной безопасности проводится с целью определения полного набора требований к разрабатываемой системе обнаружения аномалий. Перечень угроз, оценки вероятностей их возникновения, а также модель нарушителя служат основой для анализа риска реализации угроз и формулирования требований к системе зашиты. Для выявления возможных угроз, целесообразно проведение анализа этих угроз на основе их воздействия. Каждый из критериев отражает одно из обобщенных требований к системе обнаружения аномалий. Угрозы, соответствующие каждому признаку классификации, позволяют детализировать требования отражаемые этим признаком.

Необходимость описания общих критериев угроз сетевой безопасности обусловлена тем, что хранимая и обрабатываемая информация в современных сетях подвержена воздействию чрезвычайно большого числа факторов. Эти критерии упростят интеллектуальную обработку больших объёмов данных для обнаружения аномальных состояний сети. В качестве критерия для классификации возьмём объекты сетевого воздействия атаки, то есть что именно выводится из строя.

Первый класс угроз — это нарушение функционирования сетевой инфраструктуры. Для реализации угрозы возможны следующие типы атак:

- Переполнение CAM-таблицы;
- VLAN Hopping;
- Атака на STP;
- MAC-снуфинг;
- Атака на DHCP.

Общим для всех типов атак направленных на нарушение функционирования сетевой инфраструктуры, является манипуляция с адресами и уникальными идентификаторами сетевых устройств.

Критерии обнаружения:

1. Список MAC-адресов внутри сети;
2. Количество фреймов с чужим MAC-адресом;

3. Количество широковещательных фреймов;
4. Частота поступления широковещательных фреймов пришедших на сетевое устройство.

Второй класс угроз, направленный на маршрутизаторы и их алгоритмы маршрутизации. Для данного класса угроз характерны следующие типы атак:

- Подмена маршрута RIP;
- Атака BGP Router Masquerading;
- Атаки на MD5 для BGP;
- «Слепые» DoS-атаки на BGP-маршрутизаторы.

Критериями обнаружения данных атак могут быть:

1. Тип и размер пакетов;
2. Пропажа пакетов (ошибки маршрутизации);
3. Уменьшение пропускной способности сети;
4. Количество повторной передачи пакетов;
5. Отсутствие маршрутов в сети.

Третий класс угроз, направленный на взаимодействие со стеком протоколов TCP/IP. Примерами данного класса угроз являются:

- Сканирование сети;
- Атака Teardrop;
- Атака на TCP;
- Атака на UDP.

Общими для данного класса угроз можно выделить следующие критерии:

1. Количество сегментов на определенный порт;
2. Размер сегментов;
3. Количество запросов на порт.

**Выводы**

Рост объёмов информации, проходящей по сети, и экономия на персонале требуют применения эффективных средств мониторинга сетевых ресурсов. Предложенные в работе критерии выявления сетевых угроз безопасности на основе их взаимодействия учитывают как специфику проведения, так и особенности проявления угроз.

Проанализированы возможности обнаружения угроз разными подсистемами и сформулированы критерии контролируемых параметров, позволяющие повысить вероятность обнаружения, в том числе, в условиях как пассивного так активного противодействия нарушителя средствам обнаружения. Сформулированные критерии можно использовать при структурном синтезе системы безопасности или разработке устройств обнаружения.

УДК 004.056.53

# Угрозы информационной безопасности проекта «Электронное правительство» в Республике Беларусь

Матвеев А.В., магистрант,
Савенко А.Г., магистрант
Научный руководитель – Николаенко В.Л., к.т.н., доцент
*Институт информационных технологий Белорусского государственного университета информатики и радиоэлектроники, г. Минск*

Электронное правительство представляет собой сложный комплекс аппаратно-программных средств и документов организационного обеспечения, позволяющих осуществлять взаимодействие между органами государственного и местного управления, а также самоуправления, гражданами и субъектами коммерческой деятельности [1]и предполагает три направления взаимодействия:

G2B/B2G (government to business, государство – бизнес/бизнес – государство),

G2G (government to government, государство – государство),

G2C/C2G (government to citizens, государство – граждане/граждане – государство).

В Беларуси работы по проекту «Электронное правительство» ведутся в соответствии с Национальной стратегией устойчивого социально-экономического развития Республики Беларусь на период до 2030 года [2].В докладе анализируются угрозы информационной безопасности для публичных точек доступа к интернету (ПТДкИ) в местных органах власти (направление взаимодействия G2C/C2G) [3] и в системе электронного документооборота(СЭД) «SMBUSINESS», внедрение которой в Академии управления при Президенте Республики Беларусь позволило Академии управления снизить трудозатраты, получать деловую информацию в стандартизованном виде, ускорить процесс согласования и подписания документа(направление взаимодействия G2G).

**Основные угрозы информационной безопасности и способы их парирования в ПТДкИ.** К ним относятся, во-первых, стандартные угрозы для ЛВС точки, во вторых, проблемы с идентификацией и аутентификацией граждан, обращающихся к местным органам власти. Для парирования выделенных угроз в докладе предлагаются стандартные мероприятия –защита информации в сети и ЭЦП.

**Основные угрозы информационной безопасности и способы их парирования в СЭД.**К этому классу относятся, во-первых, стандартные угрозы для аппаратно-программной части СЭД (компьютеры и сервера локальной вычислительной сети и другого оборудования). На них и на методах их парирования останавливаться не будем – они общеизвестны.

Во-вторых, это проблемы с идентификацией и аутентификацией пользователей СЭД с помощью ЭЦП. Часть из них была решена созданием республиканского центра инфраструктуры открытых ключей [4] с использованием программно-технического комплекса «Штрих-код», Оставшаяся часть проблем, возникающих при использовании ЭЦП в СЭД, может быть решена с помощью правильно разработанной политики информационной безопасности СЭД, которая должна содержать следующие разделы: 1) ОПРЕДЕЛЕНИЕ ЦЕЛЕЙ ПОЛИТИКИ (обеспечение функционирования СЭД и изложение основных понятий в данной области, 2) ФУНКЦИИ ЭЦП (авторизация, защита интересов получателя документа – приемника, защита интересов подписывающего лица – передатчика).

**Выводы.** Показана проблема в области информационной безопасности, которая возникает при разработке проекта «Электронное правительство» в Республике Беларусь. Кратко проанализированы основные угрозы информационной безопасности и мероприятия по их парированию.

**Список литературы**

1. Вечер, Л. С. Государственная служба: Курс лекций. – Минск: Академия управления при Президенте Республики Беларусь, 2005. – 233 с.

2. Национальная стратегия устойчивого социально-экономического развития Республики Беларусь на период до 2030 года (одобрена Президиумом Совета Министров Республики Беларусь 10 февраля 2015 г.) // Экономический бюллетень научно-исследовательского экономического института Министерства экономики Республики Беларусь. – 2015. – № 4 (214). – С. 2–99.

3. Дедюля, П. А., Гончар, С. Е. Угрозы информационной безопасности для публичных точек доступа к интернету в местных органах власти // Современные средства связи: материалы XX Междунар. науч.-техн. конф., 14–15 окт. 2015 года, Минск, Респ. Беларусь / редкол.: А. О. Зеневич [и др.]. – Минск: УО ВГКС, 2015. – 326 с. – С. 176–177.

4. Абламейко, С. В. и др. Обеспечение информационной безопасности в системе предоставления государственных информационных услуг // Тезисы докл. 5-й белорусско-российской НТК «Технические средства защиты информации», Нарочь, 28 мая–1 июня 2007 года). – Минск: БГУИР, 2007. – С. 7.

УДК 004.056.53

**Защита персональных данных в компьютере врача**

Матрунчик Д.А., магистрант,
Научный руководитель – Шпак И.И., к.т.н., доцент
*Белорусский государственный университет информатики и радиоэлектроники, г. Минск*

Под АРМом врача будем понимать аппаратно-программный комплекс (компьютер), который врач использует для автоматизации отдельных (обычно рутинных) операций своей работы, а также для хранения различной информации, в том числе и информации о пациентах.

Одной из важнейших задач по обеспечению информационной безопасности в АРМе врача является защита персональных данных пациентов. Под персональными данными при этом в России (в Беларуси такого закона нет) согласно Федеральному закону [1] понимается любая информация, относящаяся к определенному или определяемому на основании такой информации физическому лицу (субъекту персональных данных). К персональным данным по этому закону относятся фамилия, имя, отчество субъекта, его пол, год, месяц, дата и место его рождения, адрес, семейное, социальное, имущественное положение и т.д.

Имея доступ к персональным данным пациентов, злоумышленник может проводить их несанкционированное использование в различных целях: начиная от рассылки спама и телефонного маркетинга, заканчивая несанкционированным дебетованием средств с пластиковых карточек и различных форм мошенничества. Возникновение проблемы с персональными данными объясняется простотой и быстротой сбора и использования их в компьютерных сетях, а также стремящимися к нулю издержками на ее хранение и обработку. Кроме того, во многих случаях (например, сделки в интернет-магазинах) цифровая информация о человеке заменяет саму его личность и физическое присутствие.

При этом согласно белорусскому Закону о регистре населения к основным персональным данным относятся [2]:

а) идентификационный номер;

б) фамилия, собственное имя, отчество;

в) пол;

г) число, месяц, год рождения;

д) место рождения;

е) цифровой фотопортрет;

ж) данные о гражданстве (подданстве);

з) данные о регистрации по месту жительства и (или) месту пребывания;

и) данные о смерти или объявлении физического лица умершим,

признании безвестно отсутствующим, недееспособным, ограниченно дееспособным.

Из вышеперечисленных данных к данным, хранящимся в АРМе врача, относится информация по пп. «б», «в», «г» и «д». Кроме того, дополнительными персональными данными пациента являются данные о месте его работы и группе его крови. Естественно, что персональными данными пациента, хранящимся в АРМе врача, являются все сведения о его здоровье и историях болезней.

Говоря о мерах по защите персональных данных в медицинском учреждении не стоит забывать, что эти данные хранятся не только в электронном виде в АРМе врача, но, по состоянию на сегодня, и в бумажном виде – в регистратуре медицинского учреждения. И если зафиксировать факт несанкционированного доступа к данным или попытки такого доступа в АРМе врача технически несложно, то зафиксировать аналогичный факт в регистратуре медицинского учреждения практически невозможно. Более того, учитывая факт низкой зарплаты медрегистраторов (примерно 100 долларов или чуть выше), вероятность утечки персональных данных из регистратуры медицинского учреждения очень велика. В настоящее время в белорусских медицинских учреждениях предусмотрены только меры административной ответственности виновных в утечке (если виновные будут найдены). На наш взгляд, этого недостаточно.

**Вывод**: принятие любых мер по обеспечению информационной безопасности в АРМе врача бесполезно при отсутствии таких мер в регистратуре медицинского учреждения. А чтобы осуществить такие меры, целесообразно полностью автоматизировать регистратуру, разместив данные с её бумажных носителей в электронной базе данных медицинского учреждения. Это планируется Минзлравом РБ, но в связи с большими затратами на автоматизацию, когда будет, неизвестно. А пока персональные данные в АРМ врача дублируются в регистратуре и не защищены.

**Список литературы**

1. Федеральный закон Российской Федерации «О персональных данных» от 27.07.2006 N 152-ФЗ.

2. Закон Республики Беларусь «О регистре населения» от 21 июля 2008 г. № 418-З.

УДК 004.421

**Анализ характеристик вариантов сжатия знаково-цифровых представлений многоразрядных чисел**

Мельникова О.А., к.т.н., доцент кафедры БИТ,
Масленникова А.О., студентка 4 курса,
*Харьковский национальный университет радиоэлектроники, г. Харьков*

На сегодняшний день эллиптические кривые широко применяются в несимметричных криптосистемах.

Основная операция для эллиптических кривых — поиск кратных точек, то есть умножение точки кривой на скаляр на основе сложения и удвоения точки. Скалярное умножение применяется для генерации отрытого ключа при выполнении электронных цифровых подписей на основе криптопреобразования в группе точек эллиптических кривых. При этом важным критерием является сложность данной операции, что обуславливает актуальность поиска способов повышения ее эффективности. Одним из подходов, позволяющих уменьшить вычислительную сложность, является применение «нестандартных» (отличных от традиционной двоичной системы) форм представления целых чисел. Это имеет смысл в случаях многократного использования одного ключа (например, при проверке соответствия пары открытого и секретного ключа цифровой подписи). Еще один пример — многократное использование пары целых чисел ($r$, $s$), являющейся ЭЦП, для проверки сертификатов ключей. В тоже время, когда ЭЦП ($r$, $s$) формируется для однократной проверки сообщения (например, квитанции), знаково-цифровые представления задействовать не стоит, так как их формирование требует дополнительных вычислительных ресурсов.

Одним из примеров знаково-бинарных представлений является несмежная форма (NAF). NAF — это знаково-бинарное представление, обладающее свойством несмежности ($k_i \cdot k_{i+1} = 0$ для $\forall\ i \in \{0,\ldots,t\text{-}1\}$). Это означает, что такое представление всегда содержит нулевой бит после ненулевой цифры, поэтому можно уменьшить длину NAF. Суть сжатия состоит в том, чтобы записать представление без учета 0, идущих после ненулевых цифр, но учитывать их при использовании скаляра, например, во время выполнения скалярного умножения. Это позволит уменьшить объем памяти, необходимой для хранения представления. Назовем такое представление сжатым (compressed) NAF или C(NAF).

Таблица 1 – Описание сжимающего отображения NAF

| Bin | 0 | 01 | 11 |
|---|---|---|---|
| NAF | 0 | 01 | 0-1 |
| C(NAF) | 0 | 1 | -1 |

Приведем оценки пространственной сложности вариантов представлений:

$$\begin{aligned} &Len(k) = t(бит);\\ &Len(NAF(k)) \le t+1(цифр);\\ &Len(C(NAF(k))) \le t/3+1(цифр). \end{aligned} \quad (1)$$

где $t$ — количество бит исходного числа $k$.

Разряд C(NAF) может храниться не только в виде «цифр» (в байте или даже int), но и в более компактном виде двухбитовых комбинаций. Например, 1 будет хранится в виде 2-х бит 01, а -1 →11.

Оконный (window) wNAF целочисленного $k$ — это выражение вида:

$$k = \sum_{i=0}^{t-1} 2^i \cdot k_i\ , \quad (2)$$

где коэффициенты $k_i \in S \cup \{0\}$, $S = \{\pm 1, \ldots, \pm 2^{w-1}\}$ — множество нечетных чисел. При этом не более чем один из любых $w$ последовательных коэффициентов отличен от нуля.

Так как wNAF содержит $w$-1 нулевых бит после каждой значащей цифры, можно задействовать сжатие аналогичное C(NAF), осуществляя запись без учета $w$-1 нулей, следующих за каждой значащей цифрой. Обозначим такое представление как C(wNAF).

Таблица 2 – Описание сжимающего отображения wNAF

| Bin | 0 | 001 | … | $2^{w-1}-1$ | $2^{w-1}+1$ | … | $2^{w}-1$ |
|---|---|---|---|---|---|---|---|
| wNAF | 0 | $\underbrace{0\ldots0}_{w-1}1$ | | $\underbrace{0\ldots0}_{w-1}(2^{w-1}-1)$ | $\underbrace{0\ldots0}_{w-1}(-(2^{w-1}-1))$ | | $\underbrace{0\ldots0}_{w-1}-1$ |
| C(wNAF) | 0 | 1 | | $2^{w-1}-1$ | $-(2^{w-1}-1)$ | | $-1$ |

Для наглядности приведем пример для частного случая $w$= 3.

Таблица 3 – Пример сжимающего отображения wNAF для $w$=3

| Bin | 0 | 001 | 011 | 101 | 111 |
|---|---|---|---|---|---|
| wNAF | 0 | 001 | 003 | 00-3 | 00-1 |
| C(wNAF) | 0 | 1 | 3 | -3 | -1 |

Приведем оценки пространственной сложности:

$$\begin{aligned} &Len(k) = t(бит);\\ &Len(wNAF(k)) \le t+1(цифр);\\ &Len(C(wNAF(k))) \le (t/(w+1))+1(цифр). \end{aligned} \quad (3)$$

Таким образом, сжатие несмежных представлений наиболее эффективно при больших значениях $w$.

**Выводы.** В случаях многократного повторного использования ключа $k$ или ЭЦП ($r$, $s$) могут использоваться знаково-цифровые представления для сокращения времени вычислений. При этом, с целью уменьшения объема памяти для хранения представлений $k$ или ($r$, $s$), используется сжатие, а его эффективность зависит от параметра несмежности $w$.

УДК 004.056

# Анализ требований NIST к несимметричным криптопримитивам, подаваемым на конкурс Post-Quantum Crypto Project

Мельникова О.А., к.т.н., доцент кафедры БИТ,
Джурик О.В., студент 4 курса
*Харьковский национальный университет радиоэлектроники, г. Харьков*

В последние годы проводятся интенсивные исследования по разработке квантовых компьютеров, использующих квантово-механические явления для решения математических задач, трудноразрешимых для обычных компьютеров. Сроки создания крупномасштабного квантового компьютера, способного за приемлемое время осуществлять криптоанализ современных стандартизированных криптосистем, на данный момент неясны. По существующим оценкам, процесс создания достаточно мощных квантовых компьютеров может занять около двадцати лет, после чего под угрозой окажется безопасность многих широко используемых в настоящее время криптографических алгоритмов.

В связи с этим 15 декабря 2016 года NIST объявил конкурс с целью отбора ”постквантовых” алгоритмов для замены существующих стандартов в области несимметричной криптографии. Регистрация алгоритмов-кандидатов запланирована до 30 ноября 2017 года. Но процесс оценивания ”постквантовых” криптосистем, по предположениям NIST, окажется значительно сложнее и длительнее, чем оценка кандидатов SHA-3 и AES в предыдущих криптографических конкурсах. Продолжительность данного этапа прогнозируется, предварительно, от 3 до 5 лет. И одной из причин столь длительного оценивания является неопределенность перспектив и скорости наращивания мощности квантовых компьютеров. Криптосистемы, прошедшие отборочный этап, станут претендентами на последующую стандартизацию с целью замены действующих стандартов несимметричной криптографии, включая схемы ЭЦП (электронной цифровой подписи) стандарта FIPS 186-4, а также схемы установки ключей из специальных публикациях NIST SP 800-56 A и B. Таким образом, данный конкурс NIST призван отобрать возможные варианты замены существующих алгоритмов / стандартов ЭЦП, схем шифрования и протоколов обмена ключами.

Появление мощных квантовых компьютеров поставит под угрозу стойкость многих несимметричных криптосистем, включая RSA, DSA и криптосистемы на эллиптических кривых, которые в настоящее время широко используются для обеспечения конфиденциальности и аутентичности. Поэтому NIST не принимает к рассмотрению в данном конкурсе гибридные схемы, включающие шифрование или ЭЦП,

основанные на проблемах факторизации или дискретного логарифма.

В настоящее время "постквантовыми" вариантами считают криптосистемы на основе решеток, линейных кодов, мультивариативные криптосистемы, ЭЦП на основе хеш-функций, а также возможно появление принципиально новых разработок математического аппарата.

Первым из требований [1] к криптопримитивам-конкурсантам является открытая публикация всех деталей алгоритмов для интенсивного публичного обсуждения специалистами. Последующие требования детализируются отдельно для каждого типа криптопримитивов (ЭЦП, шифрования, протоколов обмена ключами). Для примера приведем основные требования безопасности, предъявляемые к схемам ЭЦП на данном конкурсе NIST. Описание ЭЦП должно содержать алгоритмы генерации открытых и личных конфиденциальных ключей, а также формирования и проверки подписи. Схемы ЭЦП должны поддерживать обработку сообщений длиной до $2^{63}$ бит.

Для последующей стандартизации планируется выбрать одну или нескольких схем ЭЦП, экзистенциально неподдельных по отношению к атаке адаптивно подобранных сообщений. При оценке безопасности рекомендуется предварительно предполагать, что атакующий имеет доступ к подписям не более $2^{64}$ выбранных сообщений. Однако, потенциально могут рассматриваться и атаки с большим количеством сообщений. Дополнительным требованием является экономичность обеспечения перспективной безопасности, с целью противостояния неизбежному последующему увеличению возможностей квантовых компьютеров. Следующее дополнительное требование – устойчивость к атакам со сторонних каналов при минимальных затратах и вычислительной сложности базовых операций. Третье дополнительное требование – устойчивость к мультиключевым атакам. А также, необходима устойчивость реализаций к сбоям, но данное требование сложно формализуемо в общем виде и предполагает уточнения для каждого рассматриваемого варианта криптографической схемы.

**Выводы.** Исходя из вышеописанного, Украина также поставлена перед фактом необходимости смены принятых ею стандартов несимметричной криптографии (как отечественных разработок, подобных ДСТУ 4145-2002, так и гармонизированных вариантов ряда международных стандартов).

**Список литературы**

1. Proposed Submission Requirements and Evaluation Criteria for the Post-Quantum Cryptography Standardization Process: [Электронный ресурс] / The National Institute of Standards and Technology. — Режим доступа: http://csrc.nist.gov/groups/ST/post-quantum-crypto/documents/call-for-proposals-final-dec-2016.pdf — Загл. с экрана.

УДК 621.391

# Дослідження процесу спільного явного резервування при маршрутизації багатоадресних потоків в телекомунікаційній мережі

Мерсні А., аспірант,
Науковий керівник – Поштаренко В.М., к.т.н., доцент
*Національний технічний університет «ХПІ», м. Харків*

Протоколи маршрутизації та резервування ресурсів є основними засобами забезпечення наскрізної якості обслуговування в сучасних телекомунікаційних мережах [1]. При цьому важливою вимогою до таких протоколів є використання адекватних математичних моделей та методів, здатних забезпечити оптимізацію збалансованого використання доступного мережного ресурсу – канального, буферного та обчислювального [2, 3]. У зв'язку з цим запропоновано та досліджено математичну модель узгодженого вирішення завдань щодо спільного явного резервування та багатоадресної маршрутизації, яка орієнтована на оптимізацію процесу збалансованого використання канального ресурсу телекомунікаційної мережі. Представлена модель є подальшим розвитком рішень, запропонованих в роботах [4-6].

Пропонована математична модель представлена лінійними виразами, які адекватно описують такі умови:

- збереження потоку;
- забезпечення зв'язності багатоадресних маршрутів;
- відсутність контурів в маршрутах, які розраховуються;
- запобігання перевантаженню каналів зв'язку, що адаптовані під реалізацію спільного явного резервування пропускної здатності;
- балансування використання мережного ресурсу.

В рамках запропонованої моделі задача спільного явного резервування при маршрутизації багатоадресних потоків в телекомунікаційній мережі сформульована в оптимізаційній формі. Вона відноситься до класу задач змішаного цілочисельного лінійного програмування та розв'язувалася за допомогою пакету Optimization Toolbox середовища MATLAB.

За допомогою запропонованої моделі проведено дослідження процесів спільного явного резервування при реалізації багатоадресної маршрутизації для різних мережних архітектур, які відрізнялись наступними вихідними даними:

по-перше, розмірами мережі, тобто кількістю маршрутизаторів та каналів зв'язку;

по-друге, числом потоків та груп резервування;

по-третє, типом використовуваного критерію оптимальності.

Крім того, досліджувались випадки погодженого та розподіленого розв'язання задач щодо резервування ресурсу та багатоадресної

маршрутизації. Результати дослідження, які отримані для різних вихідних даних, порівнювались за показником ефективності, що характеризував рівень використаного канального ресурсу (пропускної здатності каналів зв'язку). В цілому дослідження показало, що використання моделі дозволило оптимізувати процес спільного явного резервування при маршрутизації багатоадресних потоків в телекомунікаційній мережі, знизити рівень використання канального ресурсу в середньому від 15% до 25% та орієнтувати на забезпечення більш високих значень основних показників якості обслуговування у порівнянні з рішеннями, що отримані в ході розподіленого розв'язання поставлених задач. Особливо зростав виграш при збільшенні розмірів мережі, кількості потоків та груп спільного явного резервування.

**Список літератури**

1. Вегешна Ш. Качество обслуживания в сетях IP: пер. с англ. / Ш. Вегешна. – М.: Изд. дом «Вильямс», 2003. – 368 с.

2. Kompella K. Signalling Unnumbered Links in Resource ReSerVation Protocol - Traffic Engineering (RSVP-TE) / K. Kompella, Y. Rekhter. RFC 3477, January 2003. – 9 p.

3. Kompella K., Rekhter Y., Kullberg A. Signalling Unnumbered Links in CR-LDP (ConstraintRouting Label Distribution Protocol) / K. Kompella, Y. Rekhter, A. Kullberg, RFC 3480, February 2003. – 8 p.

4. Lemeshko A. Mathematical Model and Method of Routing with Resources Reservation in IP/IntServ Network / A. Lemeshko, A.M. Hailan, O.Yevsyeyeva // Modern Problems of Radio Engineering, Telecommunications and Computer Science. Proceedings of the international Conference TCSET'2012. – Lviv-Slavske, Ukraine, February 21-24, 2012: Publishing House of Lviv Polytechnic, 2012. – P. 325-326.

5. Лемешко А.В. Модель и метод иерархической маршрутизации на основе резервирования ресурсов в сети IP/IntSev / А.В. Лемешко, А.М. Хайлан, М.В. Семеняка // Радиотехника: Всеукр. межвед. науч.-техн. сб. 2010. – Вып. 163. – С. 79-84.

6. Мерсни А. Исследование потоковой модели балансировки нагрузки в телекоммуникационной сети с неоднородной архитектурой [Електронний ресурс] / А. Мерсни // Проблеми телекомунікацій. – 2016. – № 2 (19). – С. 59 - 80. – Режим доступу до журн.: http://pt.journal.kh.ua/ 2016/2/1/162_mersni_routing.pdf .

УДК004.031.4

## Технологические вызовы информационной безопасности электронного государства

Мехтиев Ш.А., зав. отделом
*Институт Информационных Технологий НАНА, г. Баку, Азербайджан*

Обеспечение информационной безопасности требует комплексного подхода с учетом юридических, организационных и технологических аспектов.

Среда информационной безопасности динамически развивается, появляются новые атакующие технологии и соответственно совершенствуются ответные меры.

Целями данной работы являются анализ вызовов информационной безопасности э-государства и пути их решения. Можно выделить следующие компоненты национальных интересов в сфере информации:

- обеспечение информационной свободы граждан;
- охрана и развитие национальных и моральных принципов и традиций, культурного и научного потенциалов;
- защита персонального, группового и коллективного разумов от злонамеренного влияния;
- обеспечение безопасности электронных услуг (э-правительство, э-здравоохранение, э-бизнес, э-финансы, э-банкинг, э-выборы и др.);
- защита конфиденциальности персональных данных;
- информационная поддержка государственной политики;
- конфиденциальность, полнота и достоверность информационных ресурсов;
- обеспечение безопасности телекоммуникационных и других критичных инфраструктур;
- обеспечение конкурентоспособного производства в области информационных технологий.

Информационная безопасность э-государства требует информационно-технических (например, кибервойны) и информационно-психологических (информационные войны) подходов. Чтобы соответствовать этим критериям, идеальным является достижение технологической независимости в указанных ниже областях:

- аппаратная платформа (процессоры, запоминающие устройства, сетевое оборудование, GPS), особенно военного и промышленного назначения;
- программная платформа (операционные системы, офисные программы, браузеры, антивирусные программы);

- мобильная платформа (оборудование, операционные системы, прикладные программы);
- независимая интернет-инфраструктура;
- информационная инфраструктура (поисковые системы, традиционные и электронные СМИ, социальные медиа, on-line информационные службы);
- контент-ресурсы и аналитика;
- безопасный интернет для детей;
- системы управления информационным влиянием (мониторинг и анализ социальных медиа и трафика, фильтрация трафика, человеческие и технические ресурсы для распространения информации);
- мониторинговая система для контроля информационного пространства (мониторинг и выявление атак, их предотвращение, блокирование и превентивное контрнаступление).

Однако и для развитых стран проблематично комплексное решение этих задач. Например, в 2005 году начались исследования в области аппаратных троянов, когда Министерство обороны США выразило обеспокоенность в связи с использованием импортированных микросхем зарубежного производства. По оценкам многих ученых, проектированием и производством чипов занимаются сотни разбросанных по миру предприятий и существует вероятность отсутствия контроля в некоторых звеньях технологической цепи. Аппаратные трояны могут быть внедрены как на этапах проектирования, так и на этапах производства, упаковки и реализации, когда готовые чипы могут быть подвержены модификации с помощью сфокусированного пучка ионов для нарушения некоторых логических связей между элементами.

Для развивающихся стран стратегия может заключаться в адекватной оценке составляющих рисков и объединения усилий стран союзников.

В первую очередь необходимо обеспечить устойчивость и безопасность национального сегмента Интернета, оперативно пресекать попытки дестабилизации его работы. С этой целью для защиты суверенитета страны на основе проведения межотраслевых, межучережденческих учений в данной области составляется план действий. Также соответственно усиливаются меры по защите коммуникационных сетей, государственных и частных информационных ресурсов от кибератак. Защита граждан от ожидаемых рисков в on-line среде также является функцией э-государства.

Здесь целесообразно учитывать и использовать практики передовых ведущих стран. Другое направление работ – развитие собственных технологий, техники и информационных продуктов. В то же время необходимо стимулировать их применение в госструктурах и частных предприятиях.

УДК 004.738.5:004.056.5(045)

## Методи маніпуляцій суспільною думкою у соціальних інтернет-сервісах

Молодецька-Гринчук К.В., к.т.н., доцент
*Житомирський національний агроекологічний університет, м. Житомир*

В сучасних умовах соціальні інтернет-сервіси (СІС) є найбільш популярним інструментом соціальних комунікації їх користувачів – акторів. Проте, позитивні комунікаційні характеристики СІС перетворили віртуальні спільноти на ефективний засіб проведення інформаційних операцій проти особистості, суспільства держави. Під час взаємодії акторів у СІС виникає низка психологічних явищ [1-2], використання яких зловмисниками для проведення інформаційних операцій створює передумови для маніпулювання суспільною думкою, впливу на свободу вибору акторів, емоційний і психічний стан, дискредитацію існуючої системи управління в державі тощо. Це призвело до появи протиріччя між новими загрозами інформаційній безпеці держави у СІС та існуючими науковими методами автоматизованого їх виявлення. Тому аналіз маніпулятивних технологій, які застосовуються для впливу на акторів є актуальним завданням на шляху забезпечення інформаційної безпеки держави. Серед найбільш дієвих технологій, які використовуються у віртуальних спільнотах СІС під час проведення інформаційних операцій, узагальнивши, виділимо наступні [1-3].

*«Спіраль мовчання»* – це модель комунікації, запропонована Е. Ноель-Нойманн, яка показала свою ефективність в СІС і описує особливості процесів висловлювання та поширення громадської думки. Суть моделі полягає в приховуванні акторами своєї громадянської позиції, якщо вона не співпадає з точкою зору більшості.

*Стадний інстинкт* акторів СІС пов'язаний з колективною поведінкою особистості й полягає в тому, що більша увага приділяється публікаціям контенту або віртуальним спільнотам з великою кількістю коментарів, «лайків», репостів, учасників тощо. Такими діями досягається соціалізація заданого контенту чи віртуальної спільноти, створюється ілюзія активного обговорення, їх значущості і критичності для учасників віртуальної спільноти.

*Лідери думок* в СІС представляють собою акторів або віртуальні спільноти акторів, які обізнані в деякій галузі. Вони публікують контент з власною оцінкою, поясненнями і аргументацією подій, а менш активні актори сприймають його як пояснення явищ й фактів. Лідери думок в СІС опосередковано впливають на сприйняття фактів більшістю учасників віртуальних спільнот.

*Посилання на анонімний авторитет* зводиться до згадування в якості

джерела контенту авторитетних осіб, наприклад, політиків, науковців, духовенства тощо. З метою збільшення переконливості контенту наводяться оцінки експертів, свідчення учасників подій, документи.

*Емоційний резонанс* в СІС використовується для створення у акторів віртуальних спільнот заданого емоційного стану і одночасної передачі контенту. Такий підхід забезпечує сприйняття контенту на рівні емоцій і вимкнення механізмів логіки і критичного мислення.

*Відволікання уваги* акторів спрямоване на їх перефокусування від першочергового контенту до другорядного, який поданий як сенсація. Таким чином створюється інформаційний шум в СІС, який приховує важливі події.

*Міфи* або *фейки* – це прийом поширення в СІС контенту, який містить викривлені, спотворені, вигадані факти про дійсність. Метою даної технології маніпуляції є забезпечення сприйняття акторами контенту як правди без критичного осмислення і перевірки фактів.

*Нейролінгвістичне програмування* застосовується у СІС для управління свідомістю акторів з використанням спеціальних лінгвістичних конструкцій контенту, образів, зображень, відео тощо.

Результати аналізу академічної літератури [1-3] показали, що узагальнюючи частинні ознаки маніпулятивного впливу на акторів СІС для їх виявлення доцільно виділити наступні: сумнівність викладених фактів; емоційне забарвлення контенту; тональність, сенсаційність, прихований (імпліцитний) зміст.

**Висновок.** Результати аналізу сучасних методів маніпуляції суспільною думкою у СІС і узагальнення їх ознак було покладено в основу методики виявлення інформаційних операцій. Формалізація ознак маніпуляцій дозволила створити науковий базис для подальшого підвищення ефективності функціонування системи забезпечення інформаційної безпеки держави у СІС.

**Список літератури**

1. Поліщук Ю. Я. Масмедіа як канал маніпулятивного впливу на суспільство / Ю. Я. Поліщук, С. О. Гнатюк, Н. А. Сєйлова // Інформаційна безпека. – 2015. – Т. 21, Ч. 3. – С. 301–308.

2. Сугестивні технології маніпулятивного впливу : навч. посіб. / [В. М. Петрик, М. М. Присяжнюк, Л. Ф. Компанцева та ін.] ; за заг. ред. Є. Д. Скулиша. – [2-ге вид.] – К. : ЗАТ "ВІПОЛ", 2011. – 248 с.

3. Грищук Р. В. Основи кібернетичної безпеки : моногр. / Р. В. Грищук, Ю. Г. Даник ; під заг. ред. проф. Ю. Г. Даника. – Житомир : ЖНАЕУ, 2016. – 636 с.

УДК 004.056.53

**Опыт защиты банкоматов в Минском «Белгазпромбанке»**

Никифоров В.В., магистрант
Научный руководитель – Шпак И.И., к.т.н., доцент
*Белорусский государственный университет информатики и радиоэлектроники, г. Минск*

В современном обществе устройства по обслуживанию пластиковых карт (банкоматы) пользуются всё более возрастающей популярностью. Банковские счета открываются повсеместно. Для надёжного хранения и удобства управления своими деньгами люди пользуются банковскими картами. Согласно оценкам компании Retail Banking Research Ltd, в мире установлено свыше 1,2 млн. банкоматов. Банкомат становится объектом криминальных действий мошенников.

**Наиболее распространенными типами атак являются:**1) заедание карточки (Cardjamming, в период заедания злоумышленник считывает с карточки персональные данные владельца); 2) подкачка карточки (Cardswapping); 3) компромат по PIN-коду (Compromise of PINnumber); 4) вандализм; 5) диверсии [1].

Производители банкоматов, пытаются делать все возможное для того, чтобы вся конфиденциальная информация была в сохранности. К конфиденциальным данным относиться:

• номер держателя карты,
• пин-код
• CVV-код, используется для проверки подлинности карты.

Банки-владельцы банкоматов стараются оградить клиентуру от различных видов мошенничества. Полностью избежать таких ситуаций, к сожалению, невозможно, потому как злоумышленники так же изобретают различные приспособления, устройства, находят иные способы реализации их планов.

За многолетнюю практику в банке «Белгазпромбанк» было зафиксировано множество попыток хищения конфиденциальной информации применительно к банкоматам. Основные методы хищения носили технологический характер. Для защиты банкоматов была установлена сигнализация, предотвращающая несанкционированное вскрытие сейфа и отсека с оборудованием. На банкоматы были установлены антискиминговые накладки (на считыватель карт) и усилено видеонаблюдение, затрудняющие установку оборудования злоумышленника.

Однако основные мероприятия коснулись системы обнаружения вторжений. Для этого было решено ввести ряд технических доработок. Так как многие АТМ находятся удаленно от основного сервера банка, то

отследить вторжение на сетевом уровне достаточно тяжело. Поэтому были внедрены дополнительные аппаратные и программные средства защиты.

Основным аппаратным средством, внедрённым в «Белгазпромбанке», стали маршрутизатор (router) с интегрированными сервисами Cisco 881V-K9 (интерфейс WAN – Fast Ethernet 10/100 Мбит / с, сетевой интерфейс – управляемый коммутатор с 4 портами 10/100 Мбит / с, [3]) и маршрутизатор (router) с интегрированными сервисами для небольших офисов CISCO 871-K9 (интерфейс WAN и сетевой интерфейс – те же, что и для Cisco 881V-K9, [4]). Эти два устройства были выбраны именно потому, что в них используются любые виды алгоритмов шифрования, без конкретизации их стойкости. Именно поэтому в выбранных устройствах Cisco в наименовании модели присутствует окончание K9.

Программным средством для поддержки VPN в выбранных аппаратных продуктах Cisco стал набор протоколов IPSec. IPSec обеспечивает следующие возможности VPN в сетях Cisco:

• Конфиденциальность данных. Отправитель данных IPSec имеет возможность шифровать пакеты перед тем, как передавать их по сети.

• Целостность данных. Получатель данных IPSec имеет возможность аутентифицировать сообщающиеся с ним стороны (устройства или программное обеспечение, в которых начинаются и заканчиваются туннели IPSec) и пакеты IPSec, посылаемые этими сторонами, чтобы быть уверенным в том, что данные не были изменены в пути.

• Аутентификация источника данных. Получатель данных IPSec имеет возможность аутентифицировать источник получаемых пакетов IPSec. Этот сервис зависит от сервиса целостности данных.

• Защита от воспроизведения. Получатель данных IPSec может обнаруживать и отвергать воспроизведённые пакеты, не допуская их фальсификации и проведения атак внедрения посредника [2].

**ВЫВОД**: Принятый комплекс мер защиты конфиденциальной информации клиента не дал стопроцентной гарантии информационной безопасности. Число хищений информации сократилось, но злоумышленникам все же иногда удается завладеть данными карты клиента.

**Список литературы**

1. Алексей В. Мошенничество в платежной сфере / В. Алексей – Москва: издательская группа «Альпина Паблишер», 2016

2. Соммервил И. Инженерия программного обеспечения. 6-е изд./ И. Сомервиль – Санкт-Петербург, Киев: Издательский дом «Вильямс», 2002

3. Cisco 880 Series Integrated Services Routers Data Sheet – Cisco [Электронный ресурс]. – Режим доступа: www.cisco.com › ... › Data Sheets.

4. Cisco 870 Series Integrated Services Routers for Small Offices – Cisco [Электронный ресурс]. – Режим доступа: www.cisco.com › ... › Data Sheets.

УДК004:001.895

**Аналіз основних аспектів безпеки інформаційних ресурсів національної інноваційної системи**

Омельяненко В.А., к.е.н., асистент
*Сумський державний університет, м. Суми*

Конкурентоспроможність як фактор національної безпеки базується на інноваційній системі. З моменту набуття незалежності в Україні відбувається формування інституційного середовища інноваційної діяльності, що має бути адекватним глобальним викликам та забезпечувати зростання національної конкурентоздатності. Однак міжнародні рейтинги та вітчизняна статистика інновацій переконливо свідчать, що тенденції технологічного відставання економіки та ряд інших деструктивних процесів (відтік інноваційних інвестицій, інноваційний розрив між регіонами, відтік кадрів) продовжують поглиблюватися, створюючи серйозні загрози національній безпеці.

В попередніх дослідженнях ми показали, що однією з основних проблем розвитку інноваційної діяльності є відсутність необхідної інформаційної взаємодії між учасниками інноваційних процесів [1]. Зазначений висновок та значення інформаційної складової інноваційного розвитку підтверджується положеннями міжнародного стандарту зі статистичного дослідження інноваційної діяльності [2], в якому до пріоритетних напрямків розвитку інноваційної діяльності включені інформаційний обмін (розвиток інформаційних мереж тощо), джерела інформації для інновацій та виявлення бар'єрів інноваційного процесу.

Науково-інформаційне забезпечення інноваційної діяльності можна розглянути як цілеспрямоване надання багатоаспектної та максимально повної інформації споживачам, що здійснюють пошук нових ідей, концепцій і методів, в тому числі з різних напрямків розвитку різних підприємств і виробництв, регіонів та країни в цілому, а також вивчення вітчизняного та зарубіжного досвіду в області розробки і застосування нової техніки і високоефективних технологій [3]. На основі аналізу світового досвіду та можливостей сучасних програмних комплексів вважаємо за доцільне розглядати інформаційно-аналітичне забезпечення як цілеспрямовану діяльність зі збору, обробки та аналізу інформації про інноваційні аспекти функціонування складних (що самоорганізуються і саморозвиваються) економічних систем.

Інформаційно-аналітичне забезпечення ми пропонуємо розглядати в рамках ресурсного забезпечення, що є сукупністю внутрішніх та зовнішніх ресурсів, необхідних для стійкого функціонування інноваційної системи та її підсистем. Інформаційно-аналітичне забезпечення визначає раціональне використання всього комплексу національних ресурсів, що є фактором визначення місця країни в світовому економічному обороті.

На основі моделі Innovation Helixes інформаційний фактор важливий для формування інноваційних структур (кластерів, мереж тощо), а також для інтеграції в глобальні ланцюжки доданої вартості (global value chains) через моніторинг ступеня сприйнятливості та зацікавленості закордонних ринків у розробках та маркетингові дослідження світових ринків високих технологій. При цьому інформаційно-аналітичне забезпечення є важливим на всіх стадіях інноваційного циклу від появи ідеї про інновації стадії до прийняття рішення про їх впровадження.

На макрорівні для прийняття рішень щодо вибору національних інноваційних пріоритетів необхідним є аналіз конкурентів (інших країн), для чого важливим використання розробленої на основі єдиних міжнародних стандартів Статистики науки та інновацій, що була заснована в 1989 р. за ініціативою OECD.

Таким чином, інформаційна інфраструктура інноваційних процесів переходить на якісно новий рівень, а саме створюється інтегрована інформаційна система про науково-технологічний потенціал. Відтак бази даних вітчизняних інформаційних систем мають бути гармонізовані за форматами інформації та формам доступу із аналогічними світовими інформаційними мережами, що дозволить приймати ефективні рішення, швидко знаходити потрібну інформацію та партнерів.

В результаті інформаційного розриву поглибленню дисбалансу міжнародного ринку технологій сприяє наявність конкурентних переваг у країн, що мають у своєму розпорядженні значні вільні ресурси для підтримки процесів інформатизації та розвитку інформаційно-комунікаційної інфраструктури. Таким чином, запобігання небезпек і загроз національній безпеці неможливо без певних інформаційно-керуючих впливів. До основних аспектів забезпечення безпеки інформаційних ресурсів інноваційного розвитку можемо віднести:

1) формування, обробка та передача інформації про стан інноваційних процесів та національної безпеки;

2) забезпечення технологічної незалежності в найважливіших областях інформатизації, телекомунікації і зв'язку, що визначають її безпеку, в т.ч. при інноваційному забезпеченні оборонного комплексу.

**Список літератури**

1. Omelyanenko V. A. Innovation priorities optimization in the context of national technological security ensuring // Marketing and Management of Innovations. – 2016. – №4. – pp. 226–234.

2. Методическое руководство по статистическому исследованию инновационной деятельности // ОЭСЭР, Евростат, 2005.

3. Боровик М.А., Шемберко Л.В. Научно-информационное обеспечение инновационного развития России на основе комплексного использования электронных ресурсов по социальным и гуманитарным наукам: задачи, состояние и перспективы [Электронный ресурс]// Информационно-аналитический портал Клуба субъектов инновационного и технологического развития, 2012. – Режим доступа:innclub.info/wp-content/uploads/2012/05/Боровик _Шемберко.rtf

УДК 004.056.5

## Спосіб визначення характерних ознак потенційно небезпечних кібератак

Охрімчук В.В., старший науковий співробітник
*Житомирський військовий інститут імені С. П. Корольова, Житомир*

Стрімкий розвиток інформаційних технологій та впровадження їх у всі сфери людської діяльності призводить до збільшення кількості та технологічної складності кібератак. На сьогоднішній день одним з найбільш пріоритетних напрямків наукових досліджень у галузі забезпечення інформаційної та кібернетичної безпеки є створення нових та дієвих методів, засобів виявлення кібератак (КбА) для захисту комп'ютерних систем та мереж (КСМ) державного та приватного секторів національної економіки. Але нажаль постійне вдосконалення або модернізація діючих систем забезпечення інформаційної та кібернетичної безпеки не може сьогодні гарантувати повноцінного захисту КСМ від невідомих кібератак. Здебільшого це пов'язано з існуванням основного недоліку технологічних процедур зі створення сигнатур шаблонів КбА, так званого "ефекту запізнення". Таким чином, знаходження нових шляхів підвищення рівня захищеності КСМ залишається актуальною як науковою, так і практичною проблемою.

Одним із перспективних шляхів вирішення цієї проблеми вважається розроблення шаблонів потенційно небезпечних КбА. Процедура розроблення таких шаблонів достатньо складна. Потреба забезпечення високої достовірності обумовлює необхідність урахування багатьох інформативних характеристик, які зможуть описати шаблон потенційно небезпечної КбА.

На даний час існує велика кількість баз даних про відомі кіберзагрози. Всі вони містять в собі відомості про вразливості програмного забезпечення, шаблони мережевого трафіку, шаблони нормальної поведінки, сигнатури відомих КбА, шаблони дій зловмисника при проведенні КбА тощо. Нині як бази даних шаблонів КбА досить широко застосовуються бази KDD-99 та CAPEC. Але інформації з цих баз недостатньо для визначення характерних ознак потенційно небезпечних КбА тобто тих, які найімовірніше загрожуватимуть безпеці. Визначити ці характерні ознаки допоможе глибоке дослідження стандартного функціонального профілю захищеності (СФПЗ) конкретної КСМ. Знання СФПЗ КСМ дозволяє виявити її найменш та найбільш захищені компоненти.

Відповідно до нормативного документу системи технічного захисту інформації НД ТЗІ 2.5–005–99 СФПЗ – це перелік мінімально необхідних рівнів послуг, які повинен реалізовувати комплекс засобів захисту інформації КСМ, щоб відповідати визначеним вимогам щодо захищеності інформації, яка обробляється в даній КСМ.

Відомо, що СФПЗ розробляються для КСМ на підставі відповідності встановленим вимогам із захисту інформації від загроз та відомих на сьогодні функціональних послуг, що дозволяють протистояти даним загрозам і забезпечують виконання поставлених вимог.

Функціональні послуги в НД ТЗІ 2.5–005–99 розбиті на чотири групи: конфіденційності, доступності, цілісності та спостережності. Кожна з груп критеріїв включає в себе послуги, що направлені на забезпечення кіберзахисту від відповідних загроз. Всього визначено 22 послуги. Схему критеріїв, назву та зміст послуг наведено в [3]. Кожна послуга являє собою набір функцій, метою яких є протистояння визначеній множині загроз. Як відомо, послуга може включати декілька рівнів. Чим вищий рівень послуги, тим більш повно вона забезпечує захист від певного виду загроз. Послуги різних видів та рівнів, що об'єднані між собою, формують СФПЗ КСМ. Профіль – це мінімально необхідний перелік послуг, який може забезпечити СЗІ, щоб відповідати певним вимогам щодо рівня захищеності від КбА в КСМ. Всього на сьогодні визначено 90 СФПЗ.

Таким чином, можна стверджувати, що дослідження СФПЗ забезпечить можливість визначення характерних ознак потенційно небезпечних КбА. Так, для прикладу, якщо СФПЗ направлений на забезпечення доступності інформації в КСМ, то з високою ймовірністю можна стверджувати, що потенційно небезпечна КбА буде характеризуватися ознаками притаманними для такого типу КбА як DoS.

Для більш повного опису ознак, які характеризують потенційно небезпечну КбА слід скористатися класифікатором КбА. Вважається, що найбільш повною та систематизованою класифікацією КбА, що використовується на практиці для вирішення ряду прикладних завдань, є узагальнена класифікація КбА, розроблена професором Корченко О. Г. Перевагою обраного підходу до узагальненої класифікації КбА є застосування ознакового принципу для опису різних класів КбА. На відміну від відомих підходів до побудови класифікацій, ознаковий принцип забезпечує опис не тільки відомих на сьогодні класів КбА, а й дозволяє розширювати ознаковий простір для опису нових невідомих, і, відповідно, потенційно небезпечних класів.

Таким чином, комплексування можливостей ознакової класифікації КбА професора Корченко О. Г. та СФПЗ надасть змогу визначити множину найбільш характерних ознак потенційно небезпечних КбА.

**Список літератури**

1. Грищук Р. В., Даник Ю. Г. Основи кібернетичної безпеки. Монографія/ Р. В. Грищук, Ю. Г. Даник; за заг. ред. Проф. Ю. Г. Даника. – Житомир: ЖНАЕУ, 2016. – 636 с.

2. Грищук Р. В. Джерела первинних даних для розроблення шаблонів потенційно небезпечних кібератак/ Р. В. Грищук, В. В. Охрімчук, // Захист інформації – К.: 2016. Том 18. - №1 С. 21 – 29

3. НД ТЗІ 2.5-005-99 " Критерії оцінки захищеності інформації в комп'ютерних системах від несанкціонованого доступу".

УДК 004.056.55

**Безопасность информации в облачных хранилищах**

Пешков О.О. студент 1 курса
Научный руководитель – Мелешко Е.В, к.т.н, доцент
*Центральноукраинский национальный технический университет, г. Кропивницкий*

**Облачное хранилище (ОХ)** - онлайн-хранилище, в котором данные хранятся на большом количестве распределённых по всему миру сетевых серверах, предоставляемых провайдером для нужд своих пользователей. Будь-то обычный пользователь, фирма или банковская компания.

Данные обрабатываются и хранятся в так называемом «облаке», которое является одним большим виртуальным сервером. С помощью ОХ пользователь сможет получить доступ к персональным данным с любого устройства, имеющего выход в сеть Интернет.

Популярные облачные сервисы для хранения данных - Microsoft OneDrive, Google Drive и Apple iCloud.

**Удобство использования облачного хранилища.** Со стремительным развитием технологий будет стремительно увеличиваться потребность в хранении большого количества информации, поскольку это оптимальное решение потребностей в хранении данных не только для обычных пользователей, но и для разного рода бизнес предприятий, для которых использование облачного хранилища является хорошим вместилищем данных без затрат денежных ресурсов на покупку дорогого оборудования и выделения для него территории.

Корпоративные предприниматели все же могут строить частные «облака», размещая серверное оборудование на собственной территории. Такой тип сервисов пользуется особым спросом, где заказчики предпочитают лучше сохранять «полный» контроль над своими данными. Данный метод действительно является хорошим способ защитить свои данные от нежелательной утечки. И, тем не менее, такой способ хранения не защитит данные на 100%, ведь всегда присутствует человеческий фактор. В большинстве стран, если поступит официальный запрос, компетентные органы имеют право получить доступ к любым хранилищам данных.

**Защита информации в облачном хранилище.** Действенного решения в 100% случаях, очевидно, нет, но можно смело утверждать, что основой для любой архитектуры в информационной безопасности служит криптография. Повсеместно криптография используется для защиты интернет-коммерции и глобальных платежных сервисах, провайдеры облачных хранилищ могут довериться ей как лучшему способу гарантировать защиту, которая предотвратит потерю данных и сохранит

целостность и доступность для своих потребителей.

Относительно, криптографии и других способов защиты информации в облачном хранилище, такие решения существуют, но они есть только для того, чтобы усложнить проникновение тому, кто хочет получить ваши данные. Решений, позволяющих гарантировать 100% защиту информации, нет, так что, если в облаках будут храниться действительно важные данные, вероятность потери конфиденциальности этих данных резко возрастает.

**Защита данных со стороны пользователя**

1) Самый простой в использовании способ защиты это - RAR-архив, в котором есть пароль. Файлы, входящие в архив, будут иметь зашифрованные имена, которые будут понятны только владельцу. Это наиболее приемлемый способ, большое количество пользователей пользуются архивами по всему миру, это мешает выделить информацию конкретного пользователя среди большого количества всей остальной информации, вдобавок архив еще будет иметь пароль.

2) TrueCrypt – это open-source криптографическое программное обеспечение, которое создает на жестком диске криптографический контейнер, в который можно поместить файлы, или папки с файлами.

3) Использование облачных сервисов, в которых процесс шифрования автоматизирован. Это в частности, SpiderOak и Wuala. Принцип их работы следующий, перед передачей информации на сервер она шифруется пользователем локально, в результате – что хранится на серверах не знают даже сами владельцы сервера, так как ключ находиться в пользовательском ПО. Процесс установки и настройки клиента SpiderOak слегка сложнее, чем Dropbox, зато присутствуют уникальные возможности, например, защита паролем файлов с открытым доступом некоторому кругу лиц и т.д.

4) Шифрование файлов по отдельности – при небольшом количестве файлов, есть смысл просто запаковать нужные файлы в зашифрованный архив. Для этих целей отлично подходит популярный архиватор 7zip.

5) Простая осторожность – следует уделить большое внимание настройкам безопасности пользовательского аккаунта в облачных хранилищах и всех остальных сервисах: использовать безопасное https-соединение, придумывать сложные пароли и игнорировать не запрошенные сообщения от неизвестных личностей – ссылки в таких сообщениях могут вести на вредоносное программы или фишинговые сайты.

УДК 004.056

**Аналіз сучасних методів біометричної ідентифікації особистості**

Пономар М.С., студент 4 курсу
Науковий керівник – Бабенко В.Г., к.т.н., доцент
*Черкаський державний технологічний університет, Черкаси*

В загальному випадку, ідентифікація особистості – це процес встановлення особи користувача системи за певними ознаками. В залежності від особливостей системи та досліджуваного об'єкта використовують різноманітні методи дослідження, серед яких не останнє місце посідають біометричні методи ідентифікації, тобто методи, які основані на вимірюванні фізіологічних властивостей, або особливостях поведінки.

За останні п'ять років інтерес до біометричних технологій значно зріс. Зараз для фізичного і логічного доступу наряду з картами все частіше застосовується біометрична ідентифікація. Якщо ще десять років тому використання біометрії здавалося нездійсненним завданням, то сьогодні подібні рішення активно впроваджуються, замінюючи пластикові карти.

Для аналізу методів біометричної ідентифікації особистості розглянемо найбільш розповсюджені технології розпізнавання за статичними характеристиками: за відбитками пальців, радужною оболонкою ока та рисунку вен на руках.

**Ідентифікація за відбитками пальців** – метод, заснований на розпізнаванні образа, коли папілярні візерунки пальців порівнюються з зареєстрованими даними. Процес ідентифікації виконується в три етапи.

1. Формується зображення відбитка пальця. Захоплення зображення може проводитися за допомогою вбудованої камери зчитувача або за допомогою реєстрації різниці потенціалів електричного поля між горбками і западинами папілярного візерунка. В результаті виходить цифровий чорно-білий знімок візерунків відбитка пальця.

2. Зображення відбитка пальця перетворюється в математичну модель, в якій унікальні ознаки, такі як дуги, завитки, петлі і відстані між ними, зберігаються у вигляді цифрового коду.

3. Проводиться порівняння ідентифікованої цифрової моделі з шаблонами в базі даних і виконується пошук відповідників.

Біометрія за відбитками пальців має ряд переваг: перевірка відбитка пальця набагато зручніше для користувача, ніж сканування форми кисті руки; технологія перевірки відбитка пальця проста в порівнянні з технологією сканування форми особи; перевірка відбитка пальця надійніше деяких інших технологій, наприклад, сканування малюнка вен на руках; технологія перевірки відбитка пальця доступна в порівнянні з новими складними системами, такими як перевірка ДНК користувача.

**Ідентифікація за райдужною оболонкою ока** – один з найточніших методів біометричної ідентифікації. Система ідентифікації особи за райдужною оболонкою логічно ділиться на дві частини: пристрій захоплення зображення, його первинної обробки і передачі обчислювачеві та обчислювач, що виконує порівняння зображення із зображеннями, які зберігаються у базі даних, і передає команду про допуск виконавчому пристрою. Час первинної обробки зображення в сучасних системах приблизно 300-500мс, швидкість порівняння отриманого зображення з базою має рівень 50000-150000 порівнянь в секунду на звичайному ПК. Така швидкість порівняння не накладає обмежень на застосування методу в великих організаціях при використанні в системах доступу. При використанні ж спеціалізованих обчислювачів і алгоритмів оптимізації пошуку стає навіть можливим ідентифікувати людину серед жителів цілої країни.

**Ідентифікація за рисунком вен на руках.** Метод сканування підшкірних вен долоні заснований на зчитуванні відбитого від людської долоні випромінювання в інфрачервоній області спектра з довжиною хвилі 760 нм. Оскільки відновлений гемоглобін крові поглинає інфрачервоне випромінювання, то від венозних судин долоні відбивається випромінювання меншої інтенсивності, ніж від решти її поверхні. Так формується унікальний малюнок венозних судин, і вени стають видимими при скануванні в ІК-променях.

Метод біометричної ідентифікації за допомогою сканування малюнка вен полягає в зчитуванні розташування підшкірних вен на долоні за допомогою інфрачервоного сканера. Потім малюнок порівнюється зі збереженим в базі даних.

Метод доповнює собою наявний ряд технологій біометричної ідентифікації, таких як сканування відбитків пальців, райдужної оболонки ока або лиця. Він має ряд переваг: малюнки вен унікальні навіть у повністю ідентичних близнюків, не змінюються в залежності від віку, а також гарантовано захищені від підробок, так як невидимі неозброєним оком.

Відмінні особливості та переваги: застосування безконтактного методу ідентифікації; зручність використання; висока надійність (ідентифікація не залежить від вологості та забрудненості долонь); неможливість фальсифікації (малюнок вен долоні видно тільки в ІК-діапазоні); зручність використання.

**Висновок.** Технологія аутентифікації із застосуванням біометричних методів має достатньо суттєві переваги. Оскільки кожен із методів має як свої переваги, так і недоліки, то при монопольному використанні існуючих методів доцільно співставляти їх переваги і недоліки з особливостями та вимогами цільової області їх застосування. В перспективі, доцільно комбінувати різноманітні методи ідентифікації особистості для отримання якнайкращих результатів.

УДК 004.056.55

## Методи захисту персональних даних громадян

Придибайло Ю.О., студентка 2 курсу
Науковий керівник – Мелешко Є.В., к.т.н, доцент
*Центральноукраїнський національний технічний університет, м. Кропивницький*

Сьогодні життєдіяльність людини є неможливою без надання інформації про себе іншим членам суспільства, державним органам, громадським організаціям. Відповідно до Закону України "Про захист персональних даних" персональні дані (ПД) – відомості чи сукупність відомостей про фізичну особу, яка ідентифікована або може бути конкретно ідентифікована. Законом також регулюються відносини, пов'язані із захистом персональних даних під час їх обробки. Стаття 2 Закону України "Про захист персональних даних" вводить наступні поняття:

– суб'єкт персональних даних – це фізична особа, стосовно якої відповідно до закону здійснюється обробка її персональних даних;

– база персональних даних – це іменована сукупність упорядкованих персональних даних, яка існує в електронній формі та/або у формі картотеки;

– володілець бази персональних даних – це фізична або юридична особа, якій законом або за згодою суб'єкта персональних даних надано право на обробку цих даних та яка затверджує мету обробки персональних даних у цій базі даних,

**Класифікація персональних даних** [1]

**Перша група** ПД створюється та збирається органами державної влади і місцевого самоврядування відповідно до вимог закону.

**Друга група** ПД створюється та збирається суб'єктами права власності і господарювання відповідно до вимог закону.

**Третя група** ПД самостійно надається фізичними особами органам державної влади і місцевого самоврядування та суб'єктам права власності і господарювання у визначені законом терміни та ситуації.

**Четверта група** персональних даних створюється суб'єктами права власності і господарювання згідно з угодами між ними та фізичними особами, що описуються цими даними.

Розглянемо юридичні та криптографічні (можуть бути реалізовані програмно та апаратно) методи захисту персональної інформації.

**Закони, які регулюють захист персональних даних** [2, 3]

Вперше тема захисту особи прозвучала в Загальній декларації прав людини, прийнятій на третій сесії Генеральної Асамблеї ООН і підписаній 10 грудня 1948 року. Потім у Конвенції про захист прав людини і

основоположних свобод, підписаній 4 листопада 1950 року. Норми про захист прав людини містяться у статті 32 Конституції України. Також є такі закони як: Закон України "Про інформацію" стаття 23, Постанова КМ України "Про затвердження Порядку ведення особових справ державних службовців в органах виконавчої влади" від 25 травня 1998 р. № 731, Постанова ВР України "Про затвердження положення про паспорт громадянина України" від 26 червня 1992 р. № 2503- XII, Закон України "Про захист персональних даних" від 1 червня 2010 року № 2297-VI.

**Основні методи криптографічного захисту персональних даних**

Криптографія – наука про математичні методи забезпечення конфіденційності (неможливості прочитання інформації сторонніми) і автентичності (цілісності і справжності автора) інформації [4]. Основні методи криптографічного захисту інформації можуть бути класифіковані різним чином, але найчастіше їх розподіляють в залежності від способу використання та за типом ключа [4-6]:

– системи без ключа – не використовуються ключі (хеш-функції, генерація псевдовипадкових чисел, односторонні перестановки);

– системи з таємним ключем – використовується один секретний ключ – (симетричне шифрування, ідентифікація);

– системи з відкритим ключем – використовуються два ключі – відкритий/публічний та закритий/приватний (асиметричне шифрування, цифровий підпис, автентифікація).

**Список літератури**

1. Обуховська Т. Класифікація персональних даних та режиму доступу до них / Т. Обуховська // Вісник Національної академії державного управління при Президентові України. - 2013. - № 1. - С. 97-104

2. Оніщенко О.В. Захист персональних даних / О. В. Оніщенко // Юридичний вісник. Повітряне і космічне право. - 2012. - № 1. - С. 60-64

3. Козак В. Захист персональних даних та правила приватності при дослідженнях в Інтернет / В. Козак // Маркетинг в Україні. - 2013. - № 3. - С. 49-70

4. Мінгальова, Ю.І. Новітні криптографічні методи захисту інформації // "Науково-дослідна робота молодих учених: стан, проблеми, перспективи". ІІ Всеукраїнська науково-практична Інтернет-конференція, присвячена 95-річчю Херсонського державного університету, 12-16 листопада 2012 р., Херсон - С. 373-378

5. Водолазський В. Комерційні системи шифрування: основні алгоритми та їх реалізація. / / Монітор. - 1992. - N 6-7. - С. 14 - 19.

6. Бабак В.П. Теоретичні основи захисту інформації / В. П. Бабак: Підручник. – Книжкове видавництво НАУ, 2008. – 752 с.

УДК004.93.11

**Анализ алгоритмов идентификации по отпечаткам пальцев с помощью вейвлет-преобразования**

Присяжная О.А., студентка 4-го курса
*Харьковский национальный университет радиоэлектроники, г. Харьков*

Одним из основных элементов обеспечения информационной безопасности является идентификация человека. Достоинства биометрических идентификаторов на основе уникальных физиологических особенностей человека, однозначно удостоверяющих личность, привели к интенсивному развитию средств биометрической идентификации.

Сфера исследований идентификации по отпечаткам пальцев весьма разнообразна и получила освещение в ряде научных направлений:

– Тест безопасности на обнаружение «живучести». В качестве ключевого параметра выступает вопрос о подлинности, является ли источник входного сигнала живой палец.

– Использование признаков, вычисленных из поддиапазонов вейвлет-трансформированных изображений и статистических функций для увеличения шансов успешной идентификации.

– Идентификация по отпечаткам пальцев, которая состоит из трех этапов: предварительной обработки изображения отпечатка пальца, выделения особых точек отпечатка и совпадения характеристик.

В основе всех рассмотренных алгоритмов лежит дискретное вейвлет-преобразование (ДВП) исходного изображения. В докладе были рассмотрены следующие преимущества и недостатки исследуемых алгоритмов:

1) Алгоритм основан на обнаружении картины потовыделения из двух последовательных отпечатков пальцев, захваченных на нулевой секунде и через пять секунд. Обнаружение "живучести" в дактилоскопических устройствах обеспечивает возможное решение для атак подмены.

Потение может быть использовано в качестве меры обнаружения "живучести" в случае соответствия отпечатков пальцев системе. В отличие от неживых или подмененных пальцев, живые пальцы демонстрируют характерный влажный шаблон, в случае физического контакта с захваченной поверхностью сканера отпечатков пальцев. Эта модель развивается во времени из-за физиологического явления потовыделения, и, следовательно, ее можно назвать «шаблоном потовыделения».

Основные недостатки метода заключаются в том, что захваченные изображения могут быть:

– нечистыми из-за пыли на пальцах рук;

– различного среднего контраста, из-за неравномерного давления в момент захвата;

– слишком слабыми или слишком темными в зависимости от того слишком сухие или слишком влажные пальцы.

2) Идентификация по отпечаткам пальцев с использованием вейвлет-преобразования и статистических функций.

В данном методе ДВП применяется на множестве изображений отпечатков пальцев. Статистические характеристики, такие как среднее и стандартное отклонение извлекаются из аппроксимации и детализации областей ДВП разложенного изображения, в разных масштабах.

Различные комбинации статистических функций высокого порядка применяют для проверки отпечатков пальцев и выбора набора лучших векторов. Для того, чтобы повысить вероятность успеха проверки, матрица смежности рассчитывает для исходного изображения, аппроксимацию и детализацию поддиапазонов 1-уровня ДВП разложенного изображения и извлекает дополнительные функции. Эти дополнительные функции в сочетании с вышеназванными выбранными лучшими наборами вейвлет статистических функций показывают, что вероятность успеха значительно повышается путем объединения вышеупомянутых функций.

3) Алгоритм идентификации по отпечаткам пальцев, основанный на характеристике коэффициентов ДВП.

В этом методе приводится алгоритм идентификации отпечатков пальцев по обобщенным вероятностям гауссовского распределения коэффициентов ДВП.

Этот алгоритм имеет два шага для извлечения признаков изображения отпечатка пальца и функции совпадения. Первым шагом является совпадение особой точки отпечатка пальца и калибровки изображения отпечатка пальца. На втором шаге, вейвлет-коэффициенты используются для второго совпадения. Алгоритм имеет простой процесс предварительной обработки, он практически не изменил исходное изображение при извлечении функции распознавания отпечатков пальцев, поэтому скорость идентификации была улучшена. Алгоритм требует только хранение пары коэффициентов ДВП, что значительно уменьшило емкость хранения характеристики отпечатка пальца.

Проведенный анализ показал, что в настоящее время биометрическая аутентификация не только является неотъемлемой процедурой для получения допуска к объектам повышенной секретности, но и входит в нашу повседневную жизнь.

Таким образом, наиболее эффективным алгоритмом является идентификация по отпечаткам пальцев, который основан на использовании коэффициентов ДВП, так как он не требует больших объемов памяти и может преодолеть негативные последствия от вращения изображения и его сдвига, обеспечивая высокую надежность.

УДК 004.056.55

# Способи побудови хеш-функцій для забезпечення цілісності електронних документів

Розломій І.О., аспірант
Науковий керівник – Косенюк Г.В., к.т.н., доцент
*Черкаський національний університет ім. Б.Хмельницького, м. Черкаси*

Основним способом забезпечення цілісності електронного документу (ЕД) є електронний цифровий підпис (ЕЦП). ЕЦП представляє собою контрольну суму бітів, отриману в результаті аналізу ЕД, яка потім додається або логічно об'єднується з документом. В найпростішому випадку ЕЦП – це результат обчислення хеш-функції. Хеш-функцію можна використовувати для перетворення довільного вхідного тексту у відповідний формат. Процес обчислення хеш-функції називають хешуванням, а результат виконання – хешем ЕД.

До цього часу відомо багато способів отримання хеш-функції, досліджено принципи їх побудови, але більшість з них не здатні в повній мірі забезпечити надійний захист ЕД. Звідси, очевидною є необхідність розробки алгоритмів обчислення хеш-функції ЕД. Вченими розроблено багато схем отримання хеш-функції, проте, дотепер не використовувалося матричне криптографічне перетворення для побудови алгоритмів обчислення хеш-функції ЕД.

До обчислення хеш-функції ЕД існує багато підходів, на основі яких можна будувати алгоритми хешування з різною складністю виконання, структурою та результатом. На рис. 1 показані способи обчислення хеш-функції ЕД, в результаті обчислення яких за першим способом отримуємо байт інформації, за другим – матрицю, за третім способом – результат перетворення паролю, доданого до матриці.

Згідно першого способу отримання хеш-функції можна побудувати алгоритми, які базуються на послідовному чи паралельному додаванні за модулем двох байтів інформації. Такі алгоритми можна ускладнити шляхом використання матричного криптографічного перетворення.

В результаті обчислень за алгоритмами побудованими за другим способом отримуємо матрицю фіксованого розміру, яка змінена на основі аналізу інформації. Рядки вихідної матриці додаються за модулем два за визначеним алгоритмом. Інформація виступає в ролі псевдовипадкової послідовності, задаючи правила керування матрицею. В деяких випадках зберігати матрицю, як результат хешування не зручно. Тому, до матриці можна додати пароль і зберігати результат його перетворення.

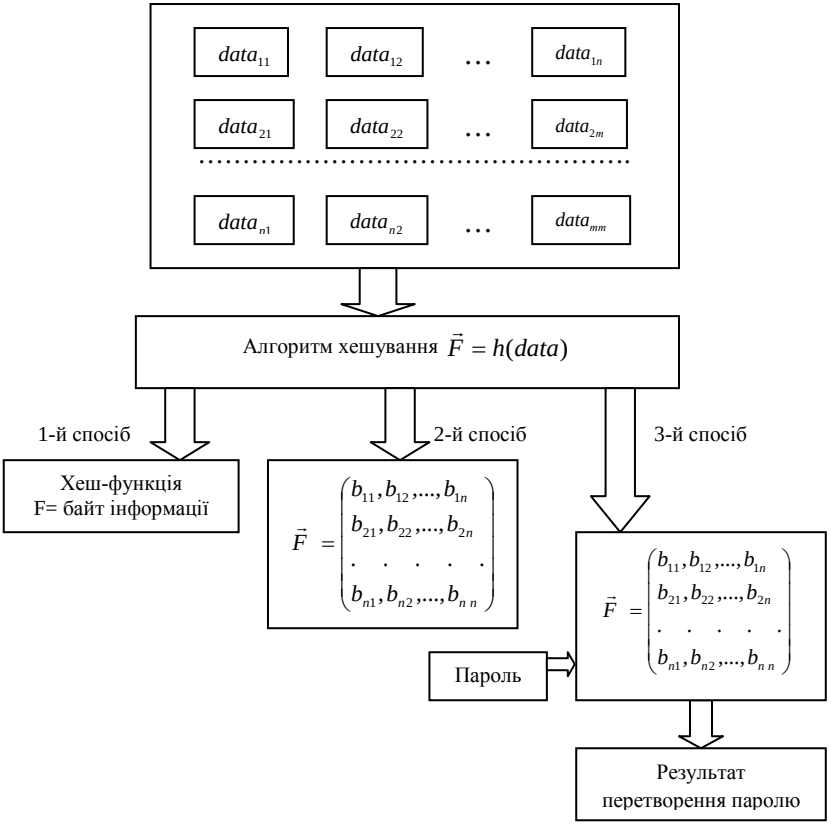



Рисунок 1 – Способи обчислення хеш-функції ЕД

**Висновки.** Таким чином, в статті розкрито проблему розробки алгоритмів обчислення хеш-функції ЕД, як основного засобу забезпечення цілісності інформації. На основі запропонованих способів, можна побудувати безліч алгоритмів хешування різної структури та складності. Алгоритми можна модифікувати шляхом використання матричного криптографічного перетворення, додаванням паролю, зміною послідовності виконання операцій. Перспективи даного дослідження полягають у розробці методів виявлення фальсифікацій в ЕД, на основі алгоритмів обчислення хеш-функцій.

УДК 004.41:004.056

**Метод управления рисками разработки программного обеспечения на основе алгоритмов анализа уязвимостей**

Смирнов А.А., д.т.н., професор; Коваленко А.В., к.т.н., доцент;
Коваленко А.С., к.т.н.
*Центральноукраинский национальный технический университет, м. Кропивницький*

В настоящее время в большинстве организаций и предприятий различных форм собственности все больше внимания уделяется вопросам анализа и оценки рисков. Но, несмотря на это проблемы и вопросы, относящиеся к общей теории и методологии анализа, оценки и управления рисками требуют адаптации к подходам и положениям современного менеджмента, учета новых факторов становления и развития технологий, объединения известных «устоявшихся» положений теории рисков с новыми, прогрессирующими подходами анализа и синтеза. Всеобщие процессы глобализации экономических, финансовых, социальных и информационных отношений способствовали развитию направления риск-менеджмента. Однако общемировые финансовые кризисы показали недостаточно внимательное отношение к управлению рисками со стороны большинства представителей руководства организаций, в том числе и в Украине. Несмотря на достаточно глубокую историю развития понятия «риск» и попытки ряда известных авторов сконцентрировать свои разработки в область управления рисками отдельных отраслей и направлений деятельности, разработка новых, перспективных научных положений в этой области все же несколько «заужена» финансовой деятельностью. В то же время широкое использование в нашей работе информационных технологий требует повышенного внимания к этому направлению, и соответственно, более глубокого освещения вопросов риск-менеджмента IT-индустрии. Для управления рисками разработки программного обеспечения, в частности предлагается использовать следующие методы.

**Алгоритм анализа DOM XSS уязвимости**. Уязвимость DOM XSS представляет собой подвид XSS, в случае которой результат атаки находится не в ответе сервера и, соответственно, не в HTML коде, а в DOM структуре HTML страницы. Результаты атак посредством таких уязвимостей можно обнаружить только в процессе выполнения или анализе DOM структуры. Сам механизм атаки, а именно инъекция Javascript кода в уязвимый сегмент, остается неизменным.

**Алгоритм анализа уязвимости к атакам SQL Injection.** SQL инъекция возможна, если входные данные используются в запросах к БД без предварительной валидации. В данной реализации выполняется анализ параметров GET запроса на предмет наличия уязвимости.

УДК 004.056.5

**Застосування принципу математичного більярду Сіная для передачі шифрованної інформації**

Собінов О.Г., викладач,
*Центральноукраїнський національний технічний університет, м. Кропивницький*

Сьогодні немає потреби говорити про важливість захисту інформації в комп'ютерних системах (КС). Як державні, військові та комерційні КС, так і приватні потребують захисту інформації. В наш час існує велика кількість засобів та методів криптографічного захисту.

В даній роботі, нас будуть цікавити не стільки класичні КС, скільки системи побудовані на ARM мікроконтролерах (ARM МК). Так, наприклад, для підвищення захищеності своїх додатків компанія STMicroelectronics випустила програмний пакет X-CUBE-CRYPTOLIB. В цьому пакеті реалізовані найбільш популярні алгоритми захисту даних для всієї родини ARMMK, навіть для тих, які не мають у своєму складі апаратної підтримки криптографії [1].

Крім того STMicroelectronics випустив ARMMK - STM32F405 і STM32F407 та STM32F415 і STM32F417, в які вбудовано crypto/hash-процесор. Цей процесор забезпечує апаратне прискорення AES 128, 192, 256, Triple DES, HASH (MD5, SHA-1). Пропускна здатність шифрування по AES-256 досягає 149,33 Мбайт/с. Як бачимо, зростання потужності (швидкодії МК), та збільшення їх використання в IT надає нові можливості, які пов'язані з забезпеченням захисту даних [2].

В [3] запропоновано простий метод шифрування, що побудовано на теорії математичного більярду (МБ). Цей метод відрізняється простотою реалізації і може слугувати прототипом створення окремої незалежної системи індивідуального криптозахисту POINT-TO-POINT.

В даному випадку на засадах МК створюються два програмно залежних прилади. В кожному з них реалізується алгоритм математичного більярду Сіная [4] (рис. 1).

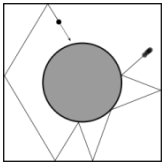


Рисунок 1 – Математичний більярд Сіная

Особливостями запропонованого алгоритму є:

- в системі МБ використовується три об'єкти – дві кульки малого

радіусу ***r*** і "шайба" радіусу ***R<L*** (довжина сторони більярда);

- для кожної пари пристроїв встановлюються індивідуальні початкові координати об'єктів ***x,y*** та швидкості (***dx, dy***);

- відкритий ключ генерується RTC і є унікальним при кожному сеансі передачі як в одну так і іншу сторону;

- відкритий ключ передає інформацію про зміщення встановлених даних на деякі малі дискретні дані.

Якщо в якості ключа використовувати значення поточної дати та часу передачі і у цьому ключі передавати послідовно значення, то:

- $dx_1$, $dx_2$,$dx_p$, $dy_1$, $dy_2$,$dy_p$ – зміщення координат кульок та шайби на більярдному столі від встановлених у програмній парі МК;
- $V_{1x}$, $V_{2x}$, $V_{1y}$, $V_{2y}$ – швидкості (напрямок руху кульок);
- $dR_{xy}$– інертність шайби;
- $r_1$, $r_2$, $R_p$– радіуси кульок та шайби.

Як бачимо, відкритий ключ складається з 14*N, де N – розрядність МК. Для 16 розрядного МК ключ буде мати довжину 14*16=224 біти, для 32 розрядного МК відповідно 14*32=448. Для збільшення ефективності секретності для кожної пари POINT-TO-POINTМК початкові значення, що передаються з відкритим ключем, можна встановити окрему послідовність вхідних параметрів, що складе 14!=871782911200 комбінацій. Таким чином можна забезпечити ще один секретний ключ, який притаманний тільки відповідній парі МК.

Технічно шифрування/дешифрування на принципі МБ Сіная може полягати в простому виконанні операції XOR між сигналом та ключем.

Враховуючи вищесказане і те, що кожний згенерований псевдовипадковий ряд (ключ шифрування) в системі більярда Сіная є ергодичним [5], можна вважати, що хаотичність створена системою не дозволяє відкрити переданий шифр будь-якої довжини за прийнятний час.

**Список літератури**

1. Новости электроники №10 (156), 2016 г. Информационно технический журнал. Учредитель – ООО «КОМПЭЛ».

2. Новости электроники №6 (44), 2012 г. Информационно технический журнал. Учредитель – ООО «КОМПЭЛ».

3. Собінов О. Г. Простий генератор псевдовипадкової послідовності / О. Г. Собінов // Інформаційні технології та комп'ютерна інженерія : зб. тез доп. наук.-практ. конф., м. Кіровоград, 4 груд. 2014 р. – Кіровоград: КНТУ, 2014. – С. 184.

4. Гальперин Г.А., Земляков А.Н. Математические бильярды. Бильярдные задачи и смежные вопросыматематики и механики – М.: Наука, 1990. – 288 с.

5. Ганапольский Е.М. О природе квантового хаоса в рассеивающей бильярдной К-системе / Е. М. Ганапольский // Доповіді Національної академії наук України. - 2012. - № 3. - С. 85-91.

УДК 004.056.53 (083.73)

**Удосконалений метод захисту програмного коду**

Степаненко І.В., студент 5 курсу,
Лозінський І.Л., студент 5 курсу,
Науковий керівник – Кінзерявий В.М., к.т.н., доцент кафедри БІТ
*Національний авіаційний університет, м. Київ*

Однією з першочергових цілей для побудови демократичної високорозвиненої країни у сфері інформаційних технологій є забезпечення дотримання норм авторського права та інтелектуальної власності. З огляду на те, що в Україні не достатньо повно прописана процедура відшкодувань і стягнень за порушення даних норм, як це зроблено в США де за неправомірне використання інтелектуальної власності без дозволу власника можлива кримінальна відповідальність. Таким чином постає питання про розробку надійного механізму захисту програмного забезпечення.

Метою даної роботи є розробка надійного механізму захисту програмного забезпечення за рахунок вдосконалення обфускаційного методу захисту вихідного коду програми.

Для виконання поставленої мети були проаналізовані сучасні літературні джерела, в яких представлені обфускаційні алгоритми захисту та проведений аналіз раніше розробленого методу захисту програмного коду «StiK». Провівши аналіз існуючих джерел були встановлені основні критерії обфускаційних перетворень, визначений механізми забезпечення захисту.

У результаті проведення експериментальних досліджень обфускаційного методу «StiK», було встановлено, що середня швидкість процесу обфускації становить 140.6 КБ/с; середній відсоток відмінностей трансформованого коду від початкового становить 36.21%. У цілому даний метод має позитивні показники при проведені експерименту, проте існують певні недоліки, що потребують подальшого опрацювання: 1) недостатня кількість реалізованих перетворень обфускаційного захисту, призводить до легкого розуміння процесу роботи програмного коду; 2) відсутній аналіз показників розміру виконавчих файлів до та після проведення процесу обфускації; 3) відсутній порівняльний аналіз ефективності даного методу з відомими методами.

Для подальшого вдосконалення методу «StiK» пропонується впровадити обфускаційне перетворення з більшим використанням міток goto. Використання великої кількості операторів goto при програмуванні на мовах високого рівня призводить до порушення логіки роботи програми та створення нечитабельного заплутаного коду. Після кожного етапу трансформації коду методу «StiK» необхідно виконувати дане перетворення, що дозводить підвищити ефективність захисту коду програм.

Розроблено псевдокод даного методу захисту програмного коду.

Input: *NameFile* − ім'я файлу із початковим кодом, перетворення $S$, $P$, $V$.
Output: *NameFileNew* − ім'я файлу із трансформованим кодом.

1. $A = OpenFile(NameFile)$;
2. $\{A_x\} = DivFunction(A)$, $A = (A_1, ..., A_n)$, $A_x$ – логічна частина $A$, $n \in N$, $x = \overline{1,n}$;
3. $for(x = 1; x \le n; x++)$
   - 3.1. $\{A_x\} = FunGoTo(\{A_x\})$;
   - 3.2. $for(x_1 = 1; x_1 \le 3; x_1++)$
     - 3.2.1. $\{i\} = FunRand(S)$;
     - 3.2.2. $A_x = CodeStructure(A_x, S, i)$, $i \in \overline{1,6}$;
   - 3.3. $\{A_x\} = FunGoTo(\{A_x\})$;
   - 3.4. $B = AssociationF(\{A_x\})$;
4. $\{B_y\} = DivFunction(B)$, $B = (B_1, ..., B_m)$, $B_y$ – логічна частина $B$, $m \in N$, $y = \overline{1,m}$;
5. $for(y = 1; y \le m; y++)$
   - 5.1. $\{B_y\} = FunGoTo(\{B_y\})$;
   - 5.2. $for(y_1 = 1; y_1 \le 2; y_1++)$
     - 5.2.1. $\{j\} = FunRand(V)$;
     - 5.2.2. $B_y = VariableFun(B_y, V, j)$, $j \in \overline{1,4}$;
   - 5.3. $\{B_y\} = FunGoTo(\{B_y\})$;
   - 5.4. $C = AssociationF(\{B_y\})$;
6. $\{C_z\} = DivFunction(C)$, $C = (C_1, ..., C_g)$, $C_g$ – логічна частина $C$, $g \in N$, $y = \overline{1,g}$;
7. $for(z = 1; z \le g; z++)$
   - 7.1. $\{C_g\} = FunGoTo(\{C_g\})$;
   - 7.2. $for(z_1 = 1; z_1 \le 1; z_1++)$
     - 7.2.1. $C_z = PunctionFun(C_z, P, z)$;
   - 7.3. $\{C_g\} = FunGoTo(\{C_g\})$;
   - 7.4. $D = AssociationF(\{C_z\})$;
8. $Cheking(D)$;
9. $WriteFile(D, NameFileNew)$

**Висновки.** У даній роботі вдосконалено метод обфускаційного захисту програмного коду «StiK» на основі впровадженням більшої кількості перетворень структури коду – міток goto, це дозволить збільшити показник показник середньої відмінності трансформованого коду до початкового та показник розміру виконавчого файлу.

УДК 004.056.5

# Сценарій атаки засліплення на механізм досягнення консенсусу криптовалюти Bitcoin

Стеценко П.І., аспірант кафедри БІТ,
Науковий керівник – Халімов Г.З., д.т.н., професор
*Харківський національний університет радіоелектроніки, м. Харків*

Останнім часом криптовалюти роблять все більший вплив на електронну комерцію, витісняючи звичайні електронні перекази. Криптовалюта Bitcoin є найпопулярнішою з них. Дана робота присвячена формалізації сценарію атаки засліплення, спрямованої на механізм досягнення консенсусу Bitcoin.

**Визначення 1.** Криптовалюта – це форма цифрової валюти, заснована на математиці і в якій технології шифрування застосовуються для регулювання генерації грошових одиниць валюти та для перевірки фінансових транзакцій. Криптовалюти функціонують незалежно від центрального банку.

**Визначення 2.** Механізм досягнення консенсусу – процес, здійснюваний групою однорангових вузлів, щодо забезпечення використання розподіленого регістра Blockchain для досягнення консенсусу.

**Визначення 3.** Консенсус – угода, яка означає, що транзакція на регістрі Blockchain підтверджена мережею. Після підтвердження транзакція не може бути відкликана або двічі використана, і чим більше угод має транзакція, тим складніше щодо неї реалізувати атаку подвійної витрати.

**Визначення 4.** Атака засліплення – атака, що відноситься до класу атак на таблиці маршрутизації і спрямована на вузол однорангової пірингової мережі з зовнішньою IP-адресою. Включає в себе наступні етапи проведення:

1) заповнення таблиці перевірених адрес адресами вузлів зловмисника;

2) перезапис адрес в таблиці нових адрес IP-адресами, які не є частиною мережі Bitcoin;

3) вибір нових вихідних підключень з таблиць перевірених і нових адрес в постійному сховищі та продовження атаки до перезапуску вузла, що атакується;

4) отримання контролю над рештою 117 вхідними підключеннями вузла, що атакується.

Сценарій атаки розглядається з наступними спрощеннями середовища та можливостями зловмисника:

- обчислювальна потужність майнінгу зловмисника становить частку $0 < q < 0,5$ від загальної обчислювальної потужності майнінгу. При

$q > 0,5$ зловмисник утримує більшу частину обчислювальної потужності майнінгу, в цьому випадку Bitcoin не може забезпечити безпеку будь-якої транзакції;

- однорангова мережа криптовалюти коректно відкалібрована таким чином, що кожен блок виробляється приблизно один раз кожні 10 хвилин з урахуванням поточної обчислювальної потужності майнінгу;

- атака засліплення є успішною незалежно від обставин. Атака засліплення ймовірно може спричинити за собою деякі витрати, але вони не враховуються через складність їх оцінки. Наприклад, у найзагальнішому випадку, може знадобитися ботнет. З іншого боку, якщо торговець фізично доступний і має тільки один, незахищений бездротовий канал з Інтернетом, атаки засліплення стають набагато простішими і дешевшими. Також передбачається, що зловмисник не запускає DoS атаку щодо чесних майнерів.

**Сценарій атаки засліплення.** Зловмисник запускає атаку засліплення щодо одного або декількох торговців. Він відводить свою обчислювальну потужність майнінгу *q* від основної гілки ланцюжка блоків Blockchain для майнінгу альтернативної гілки. Така гілка містить в самому ранньому блоці транзакцію, яка переводить монети торговцю; потім блоки направляються торговцю в тому вигляді, у якому вони отримані в результаті майнінгу. Після того, як зловмисник досягає *z* блоків на своїй гілці, торговець відпускає товар зловмисникові. Далі зловмисник припиняє процес майнінгу на своїй гілці та чекає, поки основна гілка не обжене його власну. Потім він перестає засліплювати торговця, дозволяючи йому зрозуміти, що фактична найдовша гілка не містить транзакції, що передає йому монету.

В принципі, зловмисник має необмежену кількість часу, щоб зробити *z* блоків для розблокування товарів. Він обмежений тільки кількістю часу, протягом якого він здатний засліплювати торговця, і часом, протягом якого він буде відводити свою обчислювальну потужність майнінгу від основної гілки Blockchain. Проте, торговець, ймовірно, буде здогадуватися, що він засліплений, якщо фактичний час, який потрібен для нього, щоб отримати *z* блоків, буде значно відрізнятися від очікуваного часу (приблизно 10 хвилин на блок). Таким чином, вважається, що торговець відмовляється передати товар, якщо *z* блоків не було отримано в крайній термін *d*. З огляду на цю зміну в політиці, зловмисник буде природно регулювати припинення майнінгу на власній гілці, коли або вже отримано *z* блоків, або крайній термін *d* закінчився.

Таким чином, нагороди за генерацію нових блоків, отриманих на гілці зловмисника, є марними.

УДК 004.056.5

# Порівняльний аналіз доказу виконаної роботи та візантійської відмовостійкості

Стеценко П.І., аспірант кафедри БІТ,
Перекопський О.О., аспірант кафедри БІТ,
*Харківський національний університет радіоелектроніки, м. Харків*

У теперішній час впроваджується широке коло децентралізованих систем на основі концепції криптовалюти Bitcoin у різні сфери економіки та бізнесу. Однак низька продуктивність регістрів Blockchain на основі доказу виконаної роботи, що використовується у Bitcoin, стає неактуальною. Зокрема, ряд сучасних платформ криптовалют, призначених для довільних розподілених додатків на технології Blockchain, потребують набагато більш високої продуктивності. Такий підхід змушує платформи криптовалюти відійти від своєї первісної мети і ввести домен протоколів реплікації баз даних і їх варіанти, що володіють Візантійською відмовостійкістю.

У роботі представлений порівняльний аналіз механізмів досягнення консенсусу на основі доказу виконаної роботи та Візантійської відмовостійкості, щодо такої важливої властивості регістру Blockchain, як управління ідентифікаторами вузлів.

**Порівняльний аналіз.** Порівняльний аналіз механізму досягнення консенсусу на основі доказу виконаної роботи і Візантійської відмовостійкості в контексті такої важливої властивості як управління ідентифікаторами вузла регістру Blockchain представлений в табл. 1.

Таблиця 1.

Порівняльний аналіз доказу виконаної роботи і Візантійської відмовостійкості

| Критерій | Доказ виконаної роботи | Візантійська відмовостійкість |
|---|---|---|
| Управління ідентифікаторами вузла | **відкрите, повністю децентралізоване** | дозволені вузли повинні знати ідентифікатори всіх інших вузлів |

Запис, виділений жирним шрифтом, означає перевагу механізму досягнення консенсусу.

**Управління ідентифікаторами вузлів.** Найбільш принципова відмінність доказу виконаної роботи від Візантійської відмовостійкості полягає в управлінні ідентифікаторами вузла. Особливістю доказу виконаної роботи є децентралізоване управління ідентифікаторами. Наприклад, будь-який бажаючий може скачати код для майнера Bitcoin, і

почати брати участь в протоколі, знаючи, в основному тільки один спеціальний робочий вузол.

Це дуже потужна особливість доказу виконаної роботи і головна причина, чому вони є так званим сімейством «відкритих» регістрів Blockchain, в яких може брати участь будь-який користувач. Доказ виконаної роботи пов'язано з атакою Сібіли в анонімних мережах [1]. Зокрема, в регістрах Blockchain, заснованих на доказі виконаної роботи, здатність вузла вплинути на результат досягнення консенсусу залежить від обчислювальної потужності вузла.

На противагу цьому, Візантійська відмовостійкість, як правило, вимагає, щоб кожен вузол знав весь набір своїх тимчасових вузлів, що беруть участь в консенсусі. Це, в свою чергу, вимагає (логічного) централізованого управління ідентифікаторами вузлів, в якому довірена сторона видає ідентифікатори і криптографічні сертифікати вузлів.

Важливо відзначити, що після початкового завантаження регістру Blockchain на основі Візантійської відмовостійкості, вузли, які вже приєдналися до Blockchain, можуть самі діяти разом як розподілена довірена сторона і можуть реконфігурувати систему [2, 3]. Цей аспект Візантійської відмовостійкості ставить її в невигідне становище по відношенню до доказу виконаної роботи. Проте, в ряді нових додатків на базі технології Blockchain (наприклад, регістри банкінгу, фінансів, земельної власності і нерухомості) вимоги до відомих ідентифікаторів вузлів в будь-якому випадку може бути накладено на систему з юридичних причин. Це пояснює, чому механізм досягнення консенсусу на основі Візантійської відмовостійкості є технологією, яку вибирають для так званих "дозволених" регістрів Blockchain, що вимагають, щоб ідентифікатори учасників були відомі.

Таким чином, для децентралізованих платформ, які не вимагають суворої ідентифікації учасників, необхідно застосовувати механізм досягнення консенсусу на основі доказу виконаної роботи. У системах, що виключають анонімність користувачів, навпаки, необхідно використовувати Візантійську відмовостійкість.

**Список використаних джерел:**

1. John R. Douceur. The sybil attack. In Peer-to-Peer Systems, First International Workshop, IPTPS. – 2002. – pp. 251-260.
2. Rodrigues R., Liskov B., Chen K. Automatic reconfiguration for large-scale reliable storage systems. IEEE Trans. Dependable Sec. Comput. – Vol. 9(2). – 2012. – pp. 145-158.
3. Bessani A., Sousa J., AlchieriE. State machine replication for the masses with BFT-SMART. In 44th Annual IEEE/IFIP International Conference on Dependable Systems and Networks, DSN. – 2014. – pp. 355-362.

УДК 004.056:004.7

**Обзор угроз для мобильных устройств и методов защиты от них**

Татарова К.В., студентка 3 курса,
Научный руководитель – Охрименко С.А., д.э.н., профессор,
*Молдавская Экономическая Академия, г. Кишинев, Республика Молдова*

За последнее десятилетие современные технологии сильно изменили жизнь общества. Беспроводные технологии развивались так быстро, что человек не заметил, как сильно стал от них зависим. Таким образом, сегодня, невозможно представить жизнь без мобильного устройства и связи. Теперь мобильное устройство – это миниатюрный компьютер. В его памяти хранятся контакты людей, PIN- коды банковских карточек, идентификационные данные. С помощью современных коммуникаторов управляются банковские счета, производится вход в Интернет, охраняются дома и машины. Поэтому очень важно, чтобы устройства, которым люди стали доверять, не стали причиной разного рода неприятностей. Мобильные устройства становятся все меньше, и все больше проникают во все сферы деятельности каждого человека. В связи с этим есть необходимость в определении терминов:

Мобильные устройства – ряд устройств, который объединяет в себя смартфоны, планшеты, электронные книги, телефоны, КПК, главной особенностью которых является размер, способность к транспортированию, а также количество выполняемых ими функций.

Угроза – это потенциально возможное событие, действие, процесс или явление, которое может привести к понятию ущерба чьим-либо интересам.

В зависимости от характеристик мобильных устройств, им присущи свои специфические угрозы, а также меры и средства безопасности. В докладе подробно рассматривается состав и структура угроз для мобильных устройств. К таковым относятся: Естественные (природные, технические); Искусственные (преднамеренные, непреднамеренные); Внутренние; Внешние; Активные; Пассивные; Программные (вредоносное ПО; угрозы, исходящие от локального нарушителя; угрозы, исходящие от удаленного нарушителя); Физические (утеря устройства, ущерб от физического доступа, специфические функции устройства); Сетевые (съем голоса/данных по сети, съем голоса/данных "по воздуху", GPS/ Геолокация, затопление (Flooding), затор (Jamming), раскрытие данных за счет побочных электромагнитных излучений и наводок); WEB-угрозы (использование уязвимого браузера, загрузка "на лету"); Использование уязвимых мобильных ОС и приложений.

Проведя анализ угроз, есть необходимость рассмотреть методы защиты мобильных устройств. В их число входит: шифрование данных на

устройстве, сильный пароль, сильная аутентификация, защита от вредоносного ПО (вирусов, шпионских атак), фишинга, спама и регулярное сканирование на наличие вирусов, защита от взлома устройства, специальная политика безопасности для смартфонов/ планшетов, контроль утечки данных, межсетевой экран, управление обновлениями ПО, соблюдение осторожности при установке всевозможных приложений на смартфон, контроль использования внешних устройств, создание резервных копий файлов, использование защищенного соединения с сетью Wi-Fi и т.д. Наиболее распространенной мерой обеспечения мобильной безопасности является использование антивирусной защиты. К ней относятся: Dr.Web Mobile Security, Kaspersky Mobile Security, AVG Mobilation Anti-Virus Pro и др. Большинство мобильных антивирусов включает в себя фиксированный набор компонентов безопасности: антивирусное ядро (сканер и монитор), антивор, фильтрацию звонков и SMS, родительский контроль (веб-фильтрация, контроль запуска приложений), защиту личных данных (блокировка приложений паролем, удаленное сокрытие личных данных).

Следует отметить, что за «мобилизацией» кроются различные риски и угрозы, которые необходимо соотносить с перспективами и выгодами. Развитие средств и методов обеспечения безопасности в области информационных технологий всегда отстает от развития самих ИТ. Однако для мобильных технологий этот разрыв существенно шире, чем для стандартных ИТ: постоянно выпускаются новые мобильные приложения, модели мобильных платформ и операционных систем с новейшими функциями. Между тем, средства и методы обеспечения безопасности мобильных технологий уже частично сформированы и продолжают развиваться как самостоятельное направление информационной безопасности. Вместе с тем самые совершенные разработки в сфере безопасности будут неэффективны без базовых знаний и дисциплины пользователя. Поэтому основная причина опасности «мобилизации» кроется в самом пользователе, в его недостаточных знаниях и опыте в вопросах личной безопасности.

В заключении, рассматриваемые классификации являются незаконченными, ввиду роста мобильных устройств и соответственно их угроз. Требуются исследования и дополнительный класс угроз по отношению к мобильным устройствам, разработка методики оценки потенциального ущерба от дискредитации мобильного устройства в условиях цифровой экономики.

УДК 004.415.53

# Генерування моделі соціальної мережі для дослідження впливу її структури на розповсюдження інформаційних впливів

Улічев О.С., аспірант
Науковий керівник – Мелешко Є.В., канд. техн. наук, доцент
*Центральноукраїнський національний технічний університет, м. Кропивницький*

Сьогодні соціальні мережі (СМ) наскрізь пронизують життя сучасної людини. З огляду на це, СМ активно використовуються для соціальних досліджень, маркетингових і рекламних компаній, політичної боротьби.

Мета дослідження полягає у виявленні впливу структури СМ і місця розташування у ній джерела інформаційного впливу (ідеї) на швидкість і динаміку розповсюдження ідеї. Для проведення дослідження розробляється програмна модель, в основі якої генерується структура СМ.

Звичайно, модель будь-якого реального процесу або явища спрощує його в порівнянні з об'єктивно існуючим (процесом, явищем). У той же час, вдало створена модель може бути ціннішою для дослідження, ніж сам процес або явище. Оскільки в складних системах осягнути всю сукупність зв'язків і складність структури важко, як наслідок – складно виявити закономірності. Модель же дозволяє параметризувати процес: включати або відключати ті чи інші зв'язки, змінювати їх для того, щоб зрозуміти їх важливість для поведінки системи в цілому, визначити закономірності в поведінці моделі, виявити стійкі характеристики і показники.

В ході генерації безпосередньо моделі мережі виникає питання підходу до цього процесу.

Більшість класифікацій СМ проводяться за типами послуг, що надаються (особисте спілкування, ділове спілкування, геолокації, блогінг і т.д.), по доступності (відкриті, закриті, змішані), по регіону (світ, країна, організація). Даний підхід до класифікації констатує поточний стан, дозволяє згрупувати СМ тільки за певними зовнішніми ознаками, але не враховує впливу структури на процеси, що відбуваються в СМ.

Пропонується розглядати СМ як набір певних підмножин, кластерів і розглядати СМ с точки зору мережевого підходу [1, 2, 4] з урахуванням певних обмежень. Пропонується генерувати мережу на основі комбінацій трьох типів підмножин:

Група (Г) – граф з таким набором зв'язків, що дозволяє встановити зв'язок між будь-якими двома вузлами графу напряму або використовуючи проміжні вузли. В літературі таку підмножину часто називають – «цілісна мережа» [5].

Кліка (К) – граф, в якому кожен вузол зв'язаний з кожним.

Лідерська група (ЛГ) – підвид групи з одним або кількома вираженими

вузлами, що мають зв'язки з усіма іншими вузлами групи.

Варіативність генерування структури СМ можна досягати за рахунок домішування (або у випадку «К» – вилучення) певної міри випадкових зв'язків. «Пом'якшений» варіант кліки називають К-плекс (поняття введено в [3]) – в такій підмножині не всі, але переважна більшість вузлів зв'язані між собою. Такий варіант є ближчим до реальності.

Підмножина типу «Г» в реальності, зазвичай, має певну кількість надлишкових зв'язків відносно означення.

«ЛГ» – фактично є підвидом «Г» з точки зору теорії графів, але суттєво відрізняється з точки зору структури побудови комунікацій і розвитку. Такі підгрупи утворюються за умови наявності в кластері явного лідера. В класифікаціях можна зустріти тип «его-мережа», підмережа з яскраво вираженим домінуючим лідером, що тяжіє до закритості (мінімум зв'язків з вузлами поза межами даної групи). Варто розглядати також багатополюсні «ЛГ» – коли в групі не один, а декілька вузлів – лідерів. Але з урахуванням того, що метою дослідження на основі даної моделі є динаміка розповсюдження інформаційного впливу, немає сенсу розглядати «ЛГ» з більш як двома полюсами (ідея – контрідея, антагоніст – протагоніст). Навіть при наявності більшої кількості центрів в розрізі конкретного інформаційного впливу вони поділяться на: прихильників, противників та нейтрально налаштованих відносно певної ідеї, і комплексно їх можна об'єднати в два полюси впливу.

Основним обмеженням є прийняття того факту, що соціальні мережі в Інтернеті реалізують, насамперед, міжособистісну комунікацію суб'єктів на основі наявної структури. Тому первинним чинником, що має безпосередній вплив, є структура мережі і її особливості, а поведінка суб'єкта має розглядатися як похідна цієї структури.

**Список літератури**

1. Сазанов В.М. Социальные сети как новая общественная сфера. – М.: Лаборатория СВМ, 2010. – 180 с.

2. Хоган Б. Анализ социальных сетей в интернете [Электронный ресурс] / Б. Хоган // ПостНаука. – 2013. – Режим доступа: http://postnauka.ru/longreads/20259

3. Seidman, S. B., & Foster, B. L. (1978). A graph-theoretic generalization of the clique concept. Journal of Mathematical Sociology, 6, 139–154.

4. Moody, J., & White, D. R. (2003). Structural cohesion and embeddedness. American Sociological Review, 68(1), 103–128.

5. Wellman, B., Hogan, B., Berg, K et al. (2006). Connected lives: The project. In P. Purcell (Ed.), The networked neighborhood (pp. 161–216).

УДК004.031.4

**Обеспечение безопасности электронной науки**

Фаталиев Т.Х., зав. отделом
*Институт Информационных Технологий НАНА, г. Баку, Азербайджан*

Целями э-науки, интенсивно развивающегося сегмента государственной программы «Э-Азербайджан», являются перестройка деятельности научных организаций республики с применением современных ИКТ, формирование единой национальной научной онлайновой инфраструктуры и информационного пространства.

Решение поставленных целей вывело на первый план формирование сетевой и вычислительной инфраструктуры э-науки. Как результат проведенных работ в этом направлении были созданы сетевая платформа э-науки AzScienceNet и Центр Обработки Данных, имеющий значительные вычислительные и запоминающие ресурсы. Действующая сеть и вычислительная э-инфраструктура создают скоростную связь между научными организациями, предоставляют многочисленные услуги (хостинг, AzCloud, AzStorage, eduroam, э-почта, дистанционное образование и т.д.) и создают возможности интеграции с международными сетями.

Здесь среди приоритетов выделяется задача обеспечения безопасности э-науки, как важной части в системе национальной безопасности.

Охрана э-науки, как единой сложной системы, очень важна с точки зрения безопасности и является как технологической, так и социальной проблемой.

Рассмотрим основные направления организации и осуществления эффективной охраны э-науки.

***Вопросы безопасности проектирования э-науки:***

• Проектирование сетевой и вычислительной инфраструктуры в соответствии с требованиями безопасности;

• Выбор безопасных конфигураций для оборудования и программных средств мобильных устройств, компьютеров, рабочих станций и серверов;

• Выбор безопасных конфигураций для сетевых устройств (межсетевые экраны, маршрутизаторы, коммутаторыи т.д.);

• Применение программных продуктов безопасности;

• Инвентаризация разрешенных и несанкционированных устройств и программных средств;

• Организация ограничения и контроля сетевых портов, протоколов и служб;

• Выбор границы защиты.

***Вопросы контроля безопасности и защиты э-науки:***

• Контроль входа в соответствии с полномочиями;

• Контроль беспроводного входа;

• Контроль использования административных привилегий;

• Защита от вредных программ;
• Защита данных;
• Учет возможностей восстановления данных.

***Вопросы управления безопасности э-науки:***

• Организация технического обслуживания, мониторинга, аудита и анализ соответствующих им журналов;
• Подготовка отчетов мониторинга и контроля;
• Ответ на инциденты и управление инцидентами;
• Непрерывная оценка угроз и их устранение;
• Применение тестов и горячих обучающих команд;
• Проведение учений по выявлению недостатков и оценке информационной безопасности.

Для минимизации возможных угрози совершенствования управления сетевыми и информационными ресурсами Национальной Академии Наук Азербайджана были разработаны единая политика формирования принципов и соответствующие организационно-методические базы системы информационной безопасности.

Создана система реестров пользовательских компьютеров с целью эффективного использования возможностей AzScienceNet. Сведения о сети AzScienceNet и о подключенных к ней компьютерах накапливаются в единой базе данных реестра. Эта система оказывает помощь решению следующих задач:

• Предотвращение несанкционированного доступа пользователей к сети;
• Более точное проведение анализа результатов системы мониторинга;
• Ведение борьбы против угроз;
• Минимизация вреда внутренними сетевыми угрозами;
• Предотвращение обращений пользователей к запрещенным сайтам и веб-ресурсам, не соответствующим профилю сети;
• Предотвращение нагрузки ненужной информацией сетевого трафика.

Создана и работает система мониторинга сетевой безопасности (МСБ) с целью эффективного управления и обеспечения безопасности AzScienceNet. Основные задачи МСБ можно объяснить так:

• Наблюдение и регистрация Internet-трафика;
• Контроль безопасности систем в режиме реального времени;
• Безопасность, конфиденциальность и охрана пользователей Internet;
• Обнаружение уязвимостей в системах;
• Непрерывность деятельности; и оценка рисков.

Создана служба AzScienceCERT (CERT – Computer Emergency Response/Readiness Team) с целью управления рисками информационной безопасности.

Данная работа выполнена при финансовой поддержке Фонда Развития Науки при Президенте Азербайджанской Республики – **Грант № EİF-2014-9(24) - KETPL-14/02/1**

УДК 004.056.55

# Дослідження вразливості переповнення буфера у комп'ютерних системах

Хох В.Д., аспірант,
Мелешко Є.В., к.т.н., доцент
*Центральноукраїнський національний технічний університет, м. Кропивницький*

Розповсюдження інформаційних технологій у сучасному світі значно збільшує об'єм чутливої інформації, що зберігається або циркулює мережами. Разом із зростанням об'ємів чутливої інформації постійно зростають і вимоги до систем захисту цієї інформації. Великі успіхи у галузі інформаційної безпеки зроблені зі сторони криптографічних засобів. Зараз приблизно 11% українського трафіку захищено за допомогою SSL [1], і це число зростає. Але попри все, деякі вразливості залишаються незмінними, однією з таких є переповнення буфера.

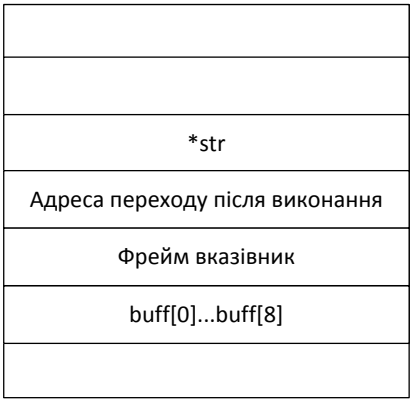
Переповнення буфера стеку є дуже примітивною проблемою, тим не менш вона є однією з найбільш поширених і найчастіше використовуваних. Варто зауважити, що ця проблема характерна для коду програми, який безпосередньо виконується на процесорі комп'ютера.

Розглянемо приклад вразливої програми та її стеку (рис. 1):

```
void overflowedfunc(char *str)
{
      char buff[9];
      strcpy(buff, str);
}

Int main(int argc, char **argv)
{
      char bbuff[10];
      overflowedfunc(bbuff);
      return 1;
}
```

Вразлива програма




Стек виклику overflowedfunc

Рис. 1 – Приклад вразливої програми та стеку виклику вразливої функції

В даному прикладі функція overflowedfunc є вразливою. Проблема полягає у використанні функції strcpy, яка не перевіряє розмір буфера і копіює його безпосередньо. Таким чином, в даній програмі після виклику

функції overflowedfunc буде перезаписана пам’ять, яка знаходиться зверху від блока з buff. Блок з адресою переходу містить адресу пам’яті, на яку буде виконано перехід, і з якої буде продовжено виконання інструкцій.

Використання вразливості переповнення буфера полягає у спробі переписати адресу переходу таким чином, щоб вона вказувала на той набір інструкцій, який цікавить спеціаліста. Для використання цієї вразливості, окрім відомостей про вразливі механізми програми, необхідно розмістити безпосередньо набір інструкцій у пам’яті комп’ютера-жертви. Наприклад, якщо вразлива функція виконує обробку певних даних з файлу – тоді ці інструкції має сенс розмістити у самому файлі, що виконає переповнення. Ще однією з проблем, з якою стикнеться спеціаліст – це визначення адреси, з якої починається його набір інструкцій, на практиці це вирішується за допомогою побудови так званих NOP sled [2] – це щось на зразок посадкової смуги для вказівника переходу. Ідея полягає у записі іноді тисяч або сотень інструкцій NOP (no-op) перед набором інструкцій, які необхідно виконати. NOP`и вказують процесору нічого не робити (no operation – англ. немає інструкції). Використовуючи такий прийом, спеціалісту необхідно знати лише приблизне місце розташування свого набору інструкцій.

Вразливість досить примітивна, і це робить її досить поширеною, оскільки перевірка розмірів буферів часто буває проігнорованою у зв’язку з уявленням про те, що розроблювана програма буде працювати у штатному режимі і функції, що використовують/викликають вразливі функції просто не можуть передати данні більших розмірів. Іноді програмісти вказують просто великий розмір буферу з розрахунку на те, що нікому в голову не прийде спробувати передати їх програмі більшу кількість даних, або, наприклад, обмежують розміри полів вводу. Також варто зауважити, що концепція віртуальної пам’яті, що поширена в сучасних операційних системах, дозволяє проводити аналіз програмного забезпечення на наявність такого роду вразливостей у досить детермінованому просторі, що робить можливим цей процес частково автоматизувати. До того ж, концепція віртуальної пам’яті дозволяє використовувати вразливість на різних машинах для однакових вразливих програм.

**Список літератури**

1. Статистика українського інтернету [Електронний ресурс] // ukralio. – 2017. – Режим доступу до ресурсу: https://www.ukralio.com/statistika-ukrainskogo-internetu

2. How security flaws work: The buffer overflow [Електронний ресурс] // arstechnica. – 2015. – Режим доступу до ресурсу: https://arstechnica.com/security/2015/08/how-security-flaws-work-the-buffer-overflow/

УДК 004.056

# Розробка системи підтримки рішень з управління кіберзахистом об'єкту інформатизації

Чернишов В.О., аспірант
Науковий керівник – Лахно В.А., д.т.н., доцент
*ПВНЗ «Європейський університет», м. Київ*

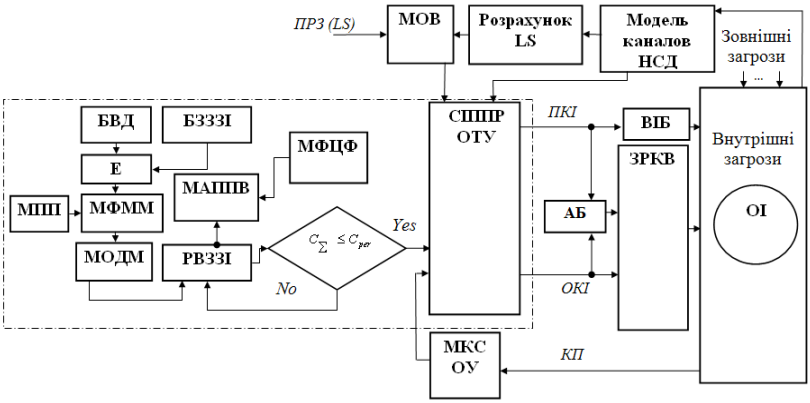
Сучасний рівень та перспективи подальшого розвитку інформаційно-комунікаційних систем (ІКС) в різних сферах людської діяльності неможливо уявити без підвищеної уваги до питань інформаційної (ІБ) та кібербезпеки (КБ), зокрема через зростаючу кількість кіберзагроз та деструктивних впливів на об'єкти інформатизації (ОІ). Стрімке зростання кількості інцидентів у сфері ІБ показало, що існуючи системи захисту інформації (СЗІ), побудовані на основі виявлення відомих загроз та атак, не завжди ефективні при появі нових класів кібернападів спрямованих, зокрема, проти широко поширених корпоративних інформаційних систем (КІС), автоматизованих систем управління (АСУ, або SCADA) в енергетиці, промисловості, транспорті, банківській та ін. сферах.

Тому для успішного використання сучасних ІКС необхідно не тільки результативно управляти їхніми функціональними ресурсами, а й створювати ефективні системи управління захистом інформації (СУЗІ). Оскільки об'єкти управління – СУЗІ є досить складними організаційно-технічними структурами (ОТС), що функціонують в умовах невизначеності, ефективне управління подібними системами повинно базуватися на інноваційних інформаційних технологіях підтримки прийняття рішень в питаннях ІБ та КБ [1–3].

Одним з варіантів вирішення даної проблеми є застосування систем підтримки рішень (СПР) з управління КБ на основі інтелектуальних ІТ (ІІТ). Це, в свою чергу, робить актуальними дослідження з вдосконалення існуючих та розробки нових методів, моделей, алгоритмів та програмного забезпечення (ПЗ) для оперативного управління захистом інформації (ЗІ) в ОІ, зокрема, в умовах невизначеності, суперечливості та неповноти знань про стан ІКС. Даному напряму досліджень були присвячені роботи [3–7].

На основі аналізу принципів управління в умовах невизначеності, запропонована узагальнена архітектура СУЗІ та КБ, рис. 1.

У якості керованої змінної використовується показник – рівень захищеності (*LS*) [1, 4, 6]. Значення *LS* залежить від максимального рівня критичності інформації, яка опрацьовується у даний час у ІКС.




Прийняті скорочення: АБ – адміністратор ІБ; БВД – блок вводу даних; БЗЗЗІ – база знань засобів захисту інформації; ВІБ – відділ інформаційної безпеки; Е – експерти; ЗРКВ – засоби реалізації керуючих впливів на вбудовані в ЗЗІ керуючі модулі; КП – контрольовані параметри (удосконалено алгоритм розбиття простору ознак аномалій та кібератак на кластери в ході реалізації процедури розпізнавання деструктивних впливів на ОІ); МАППВ – модуль реалізації алгоритму повного перебору варіантів поєднуваних програмно-апаратних засобів; МКС ОУ – модуль контролю стану об'єкта управління; МОВ – модуль оцінки відхилення КП та оцінювання аномалій у ОІ; МОДМ – модуль опрацювання додаткових матриць; МПП – матриці попарних порівнянь; МФММ – модуль формування морфологічних матриць; МФЦФ – модуль формування цільової функції; ОКІ – оперативна командна інформація; ПРЗ – початковий рівень захищеності;
ПКІ – планова командна інформація; РВЗЗІ – раціональні варіанти засобів захисту інформації; СІППР – система інтелектуальної підтримки прийняття рішень з управління захистом ОІ.

Рисунок 1. Структура СІППР з організаційно-технічного управління ЗІ

Контур організаційно-технічного управління (ОТУ) [6, 7] захистом інформації у ОІ удосконалено за рахунок імплементації блока, який дозволяє контролювати задані параметри ІБ та КБ. У блоці КП (контрольованих параметрів) реалізовано алгоритм розбиття простору ознак аномалій та кібератак на кластери в ході реалізації процедури розпізнавання деструктивних впливів на ОІ. Відповідно, удосконалено алгоритм роботи модуля оцінки відхилення КП та оцінювання аномалій у ОІ за рахунок оптимізації перевірочних допустимих відхилень на кожен клас аномалій або кібератак.

Розроблена в ході досліджень модель та відповідний алгоритм, відрізняється від існуючих рішень, можливістю одночасної оптимізації при обчислення контрольних допусків аномалій та кібератак в ході аналізу рівня захищеності ОІ у режимі реального часу.

Також, в ході досліджень запропоновано метод виявлення атак на ОІ на основі трактування СІППР важко пояснюваних ознак та побудови прогнозної моделі дій різних керуючих впливів у СУІБ. При цьому подальші дослідження направлені на розробку алгоритму навчання СІППР у складі систем КБ ОІ. Метод являє собою ітераційну процедуру та дозволяє на кожному кроці навчання СІППР змінювати перевірочні допустимі відхилення для всіх ознак параметрів, які підлягають контролю СУІБ, одночасно.

На основі запропонованої структури СІППР для оцінки ризику порушення ІБ, розроблені програмні комплекси для автоматизованої системи інтелектуальної підтримки організаційно – технічного і оперативного управління ЗІ ОІ.

**Список літератури**

1. Zhang, Y. Distributed Intrusion Detection System in a Multi-Layer Network Architecture of Smart Grids / Y. Zhang, L. Wang, W. Sun, R.C. Green, M. Alam // IEEE Transactions on Smart Grid. – 2011. – Vol. 2, No. 4. – p. 796–808.

2. Al-Jarrah, O. Network Intrusion Detection System using attack behavior classification / O. Al-Jarrah, A. Arafat // Information and Communication Systems (ICICS), 2014 5th International Conference, p. 1–6.

3. Louvieris, P. Effects-based feature identification for network intrusion detection / P. Louvieris, N. Clewley, X. Liu // Neurocomputing. – 2013. – Vol. 121, Iss. 9. – p. 265–273.

4. Lakhno, V. Creation of the adaptive cyber threat detection system on the basis of fuzzy feature clustering / V. Lakhno // Eastern–European Journal of Enterprise Technologies. – 2016. – Vol. 2, No 9(80). – p. 18–25.

5. Atymtayeva, L. Building a Knowledge Base for Expert System in Information Security / L. Atymtayeva, K. Kozhakhmet, G. Bortsova // Chapter Soft Computing in Artificial Intelligence of the series Advances in Intelligent Systems and Computing. – 2014. – Vol. 270. – p. 57–76.

6. Машкина И.В. Разработка метода и функциональной модели численной оценки риска нарушения информационной безопасности и уровня защищенности информации на основе вероятностно-статического подхода / И.В. Машкина, С.Н. Алекса // Известия Южного федерального университета. Технические науки. – 2008. – № 8. – С. 47 – 54.

7. Машкина И.В. Методика построения модели комплексной оценки угроз информации, циркулирующей на объекте информатизации / И.В. Машкина, В.И. Васильев, Е.А. Рахимов // Информационная безопасность: Известия ТРТУ. – 2006. –№7(62). – С. 70 – 76.

УДК 007

**Соціальні медіа як джерело загроз інформаційній безпеці**

Шульга В.І., доцент кафедри економіки підприємства,
канд. екон. наук, доцент
*Східноєвропейський університет економіки і менеджменту, м. Черкаси*

Відповідно до законодавства України поняття «інформаційна безпека» має таке визначення:«стан захищеності життєвоважливих інтересів людини, суспільства і держави, при якому запобігається нанесення шкоди через: неповноту, невчасність та невірогідність інформації, що використовується; негативний інформаційний вплив; негативні наслідки застосування інформаційних технологій; несанкціоноване поширення, використання, порушення цілісності, конфіденційності та доступності інформації».

Очевидним є, що соціальні медіа є найціннішим джерелом інформації для будь-якого кібер-шпигуна та кібер-злочинця, надаючи абсолютно на легальних умовах різнобічну інформацію про людей, події, установи, продукти та інше, а відтак і потенційною загрозою інформаційній безпеці як окремому індивідууму так і будь-якому підприємству та країні в цілому. Останнім часом широке поширення отримали такі явища, як інформаційні операції, активна інформаційна протидія в рамках інформаційної боротьби, які в багатьох випадках базуються на маніпулюванні даними саме в соціальних медіа.

Соціальні медіа являють собою сукупність онлайн-сервісів та інтернет-додатків, які дозволяють користувачам спілкуватися один з одним, у тому числі і в режимі реального часу. Соціальні медіа базуються на ідеологічній і технологічній базі Веб 2.0, що дозволяє створення та обмін контентом, створеним самими користувачами (User-GeneratedContent), на відміну від попередньої концепції веба, яка передбачає, як і у випадку традиційних засобів масової інформації, централізоване створення контенту, що поставляється користувачам-читачам.

Виділяють *сім різновидів соціальних медіа*: це соціальні мережі, блоги, форуми, сайти відгуків, сервери фото- і відеохостингу, віртуальні служби знайомств і геосоціальні мережі. Слід зазначити, що чіткі межі між цими різновидами розмиті.

Все прогресивне людство, а віднедавна і Україна, вступили в епоху, коли обсяг і різноманітність інформації в мережі дозволяють будь-якій

людині видобувати справжню картину подій і взаємозв'язків (повну базу даних), що раніше було доступно лише спецслужбам з їх агентурною мережею і засобами перехоплення і прослуховування.

До списку найбільш «цікавих» для різного роду кібер-злочинців, можна сміливо включити: «ВКонтакте», «МойКруг», Twitter, Facebook, Google+, LinkedIn, Badoo, LaveJournal. Саме через їх популярність, кількості зареєстрованих користувачів, об'єм щоденної інформації, перераховані соціальні медіа несуть в собі загрозу Вашій інформаційній безпеці.

Інформація перетворилася зараз на глобальний ресурс, використання якого дає змогу значно збільшити ефективність керування усіма життєвими сферами.

Нещодавно Facebook поновив налаштування конфіденційності. Кожен відвідувач відтепер автоматично вважається таким, що прийняв нові умови. Основні зміни в новій політиці полягають в тому, що Facebook має право збирати персональні дані користувача від будь-якого переглянутого ним «партнерського сайту» та в самій мережі. Це може бути будь-який сайт, що використовує рекламну платформу Atlas.

При цьому Facebook не дозволяє відмовитись від свого збору даних.

Соціальні мережі зловмисники використовують не лише з метою заволодіти відповідною конфіденційною інформацією, а й для поширення дезінформації з метою впливу на свідомість користувачів. Враховуючи велику кількість інструментальних засобів пошуку, аналізу та збору інформації в соціальних мережах, а також те, що значна їх кількість є у вільному доступі, можна з впевненістю стверджувати, що жодна окрема особа чи підприємство (фірма) не можуть гарантувати собі 100%-ї інформаційної безпеки.

За деякими оцінками, у мережі зараз зберігається понад 1200 екзабайт інформації, і 90% цієї кількості було створено за останні 2-3 роки.

Факти здійснення інформаційного впливу на широку аудиторію можна виявити протягом усієї історії суспільства. Бажаємо ми того чи ні, відвідуючи соціальні медіа ми піддаємося інформаційному впливу. Тобто, організованому цілеспрямованому застосуванню спеціальних інформаційних засобів і технологій для внесення деструктивних змін у нашу свідомість.

Інформаційний вплив варто поділяти на інформаційно-технічний та інформаційно-психологічний.

*Інформаційно-технічний вплив* – це вплив на інформаційно-технічну інфраструктуру об'єкта з метою забезпечення реалізації необхідних змін у їїфункціонуванні (зупинка роботи, несанкціонований доступ до

інформації та її перекручення (спотворення), програмування на певні помилки, зниження швидкості оброблення інформації тощо), а також вплив на фізичний стан людини.

*Інформаційно-психологічний вплив* – це вплив на свідомість та підсвідомість особистості й населення з метою внесення змін у їхню поведінку ісвітогляд.

**Література:**

1. Додонов А.Г. Конкурентнаяразведка в компьютерныхсетях / А.Г. Додонов, Д.В. Ландэ, В.В. Прищепа, В.Г. Путятин. – К.: ИПРИ НАН Украины, 2013. – 250 с.

2. Могильний С.Б. Методи та інструменти ділової розвідки в Internet. – К.: 2010. – 264 с.

3. Бутузов В.М. Протидія комп'ютерній злочинності в Україні (системно-структурний аналіз): монографія / В.М. Бутузов. – К.: КИТ, 2010. 407 с.

4. Інформаційна безпека [Електронний ресурс].
Режим доступу :ukr.vipreshebnik.ru/entsiklopedia/55-i/1943-informatsija-bezpeka.html.

5. Проект "Доктрини інформаційної безпеки України". На виконання абзацу 4 пункту 5 рішення РНБОУкраїни від 21 березня 2008 року "Про невідкладні заходи щодо забезпечення інформаційної безпеки України", введеного в дію Указом Президента України № 377 від 23 квітня 2008 року. [Електронний ресурс]. Режим доступу : http://www.rnbo.gov.ua/news/930.html.

UDC 004.75

**Promotion of Internet resources and environment link**

Basyuk T.M., Ph.D., Associate professor
*National University "Lviv Polytechnic", Lviv*

**Introduction.** Developers of search engines strive to ensure that the user of the system receives links to his/her requests to the most suitable online resources that contain exactly the information he/she is looking for. Thus, the degree of semantic content compliance of this resource to corresponding search request is called relevance and the process of order appointment to resource in which they will be located in the search results for a particular request is called the site ranking [1, 2]. Algorithms of sites ranking have changed during evolution as a global network and search engines. In particular, at the phase of development for webmasters it was enough to specify in the meta tags the following: themes, description and keywords to be referred to relevant topics and to be rank highly by the keywords by search engines. Over time, there are more and more online resources and first optimizers with the purpose of attracting more visitors to the resource began to prescribe in meta tags popular keywords that actually did not correspond to the site topic, which served as the impetus for significant improvement of algorithms ranking by taking into account: content of online resource, its trust rank and reference environment.

**Overview of literature.** The analysis of publications [3] shows that there is a set of researches related to the influence of content quality and trust rank of the resource in its ranking. However, there are almost no authoritative studies relating to reference environment impact analysis, and existing attempts [1] lie in tries of some researchers and seo optimizers to fill this niche. Given that the important task of the research is: to determine the impact on the environment reference on resource ranking in the search engine and formation of the methodological basis for the implementation of recommendation systems of popularization of Internet resources.

**Major research results.** The conducted analysis of the popularization features of internet sources shows that two types of links are used in practice: internal and external. The use of internal links can equally distribute the weight between the pages of Internet resources. Thus, they can implement a reference as at the beginning of the current page (anchor) and another page of parent resource. This not only facilitates to transfer of pages weight and accordingly to promotion under a particular topic, but also affects the usability of internet resource. It creates a kind of links with the use of attribute *name* (*bookmark name*) tag *A* (*creating bookmarks page1*):

*<a name="page1">Page 1</a>*

Then the name of the bookmark is needed to be specified for the jump in *a*

tag (or so-called internal address of the jump):

*<a href="#page1">Link to page 1</a>*

Address begins with # sign, followed by the bookmark name – *page1*. Similarly links to bookmark to another resource document are implemented (*document name # bookmark name*):

*<a href="author.html#page1"> Links on the page 1 of another document </a>*

External links to other resources are also created by using the tag attribute <*A*> - *href*, which is used as the meaning of URL-address:

*< a href="URL-address "> link text (anchor)< /a>*

This type of links is assessed by using the technology TrustRank, which is a filter of search engine. The task of TrustRank is a division of "useful" resources from the "extra" ones, created exclusively for the promotion of Internet resources. In particular, if there are a lot of links from the resource and they lead to websites with low attendance and trust rank, TrustRank introduces algorithm of resource weight reduction in the search results.

The conducted study showed that the most important criteria to be considered in creating a reference environment are the following: the number of links (the optimum number of outgoing links depends on the topic of Internet resources, with not more than five on one page); topicality (online resource from the pages of which there are links to resources of various topics, can be perceived by search engine as advertising space specializing in links sale leading to the downgrade); trust rate (outgoing links to resources with high ratings are positively assessed by search engine, particularly if their trust rate is higher than the resource that is moving).

**Conclusion.** The article shows the influence of the reference environment on a ranking of the resource in the search engine and highlights the main criteria to be considered in the promotion process. The proposed approach creates the methodological basis for further implementation of recommendation systems of Internet resources popularization in a global network.

**References**

1. **J. Jantsch and P. Singleton. 2016.** SEO for Growth: The Ultimate Guide for Marketers, Web Designers & Entrepreneurs. Wiley, 238p

2. **T. Basyuk. 2016.** Popularization of website and without anchor promotion. Proceedings of the XI International Scientific and Technical Conference «Computer science and information technologies CSIT-2016», 193-195, IEEE (DOI:10.1109/STC-CSIT.2016.7589904).

3. **Alpar, M. Koczy, M. Metzen, 2015.** SEO – Strategie, Taktik und Technik. Springer Gabler, 538 (in German).

UDC 004.62

## Developing applications for MongoDB using Java

Parfonov Y.E., Ph.D., Senior researcher
*Simon Kuznets Khahkiv National University of Economics,Kharkiv*
Kavun S.V., Prof., Dr.Sc., Ph.D., Head of IT Department
*Kharkiv Educational and Scientific Institute of the University of Banking (KhESI UB), Kharkiv*

Currently, a lot of database applications have to process large amounts of rapidly changing, semi-structured or unstructured data. This has led to the emergence of new approaches to data storage and processing, one of which is NoSQL.

Nowadays, there are many types of NoSQL solutions. The main of them are [1, 2]:

Key-value stores;

Wide column stores;

Document databases;

Graph databases.

Due to their flexibility, productivity and ease of use, document databases are the most popular. According to the DB-Engines Ranking [3], the first place among NoSQL solutions and the fifth among all known DBMS take MongoDB, an open source document DBMS developed by MongoDB Inc. The current version of MongoDB is 3.4

For NoSQL solutions in general and MongoDB, in particular, there is no standard query language like SQL. Instead, each vendor provides some specialized API for their products, allowing them to perform data operations.

Access to MongoDB from Java application is done using the corresponding driver. The driver libraries can be added to the project in one of two ways. The first method is to download from the MongoDB website and directly import the mongodb-driver-3.4.2.jar file. In this case, you will also have to add its dependencies bson-3.4.2.jar and mongodb-driver-core-3.4.2.jar likewise. The recommended way to add the driver library to the project is to use some framework to automate the assembly of projects, such as Apache Maven.

Direct use of the Java driver has both advantages and disadvantages. On the one hand, ithas a rather low-level API, which provides wide opportunities to develop software systems working with data. On the other hand, the applications using Java driver will inevitably contain a large amount of code not directly related to their business logic. This likely results in increasing spending to develop such systems.

One of the ways to improve the effectiveness of application development for MongoDB is using one of the frameworks for object-document mapping. The frameworks provide transparent data mapping from the object model of the

programming language to the DBMS document model and backward.

To interact with MongoDB from the Java application, there are about twenty such frameworks. One of the most popular is open source software Morphia [4]. The current version of the framework is 1.3.2.Morphia is the software shell for the Java driver discussed above. This framework provides high-level abstractions for converting domain objects to MongoDB documents, while at the same time enabling the use of low-level capabilities of the base driver, if necessary.To map domain objects on the corresponding MongoDB documents, you need to describe one or more entity classes. These are ordinary POJO classes with annotations for the classes themselves and their elements.

Let's consider the basic annotations:

@Entity - specifies the name of the MongoDB document collection. Applies to the entity class whose objects will be stored in the document collection. The annotation is optional, if it does not exist, the collection name will be the same as the class name.

@Id - an annotation for the field of the entity class, which will correspond to the field _id of the database document. Required for class fields whose objects are mapped to MongoDB documents, except for those embedded in other documents.

@Reference is an annotation indicating that this field of an entity class will match a reference to a document in a different collection.

@Embedded - can be applied to an entity class or its field. For a class, this annotation determines that its objects will be mapped on a document embedded in another document. For the class field - that it will match the reference to the embedded document.

So, although the Java driver allows you to develop applications for MongoDB, its direct use has a number of drawbacks. To improve the efficiency of the development process, it is recommended to use an object-document mapping framework, good choice of which is Morphia.

**References**

1. Types of NoSQL Database Management Systems. [Electronic resource]. – Access mode: https://www.mongodb.com/scale/types-of-nosql-database-management-systems.
2. List of NoSQL Databases. [Electronic resource]. – Access mode:http://nosql-database.org.
3. DB-Engines Ranking. [Electronic resource]. – Access mode:http://db-engines.com/en/ranking.
4. The Java Object Document Mapper for MongoDB. [Electronic resource]. – Access mode: https://mongodb.github.io/morphia/.

УДК 004.6:004.42

## Особливості розробки інформаційно-довідкової системи ветеринарної клініки

Бабенко В.Г., к.т.н., доцент; Купецький В.П., студент 4 курсу
*Черкаський державний технологічний університет, м. Черкаси*

Розробка інформаційно-довідкової системи (ІДС) ветеринарної клініки потребує, в першу чергу, застосування умінь і навичок проектування бази даних, призначеної для функціонування автоматизованої інформаційної системи, що полягає у здійсненні розробки реляційної бази даних та інтерфейсу роботи з нею. ІДС призначена для збору, зберігання, пошуку, обробки та видачі необхідної інформації про цю предметну область. Для реалізації поставленого завдання потрібно спочатку спроектувати базу даних призначену для інформаційного забезпечення автоматизації процесів, і яка міститиме необхідну інформацію про лікарів, пацієнтів, їх власників та процедури. Схема взаємозв'язків процесів та інформаційних потоків, що підлягають автоматизації, зображено на рис. 1.

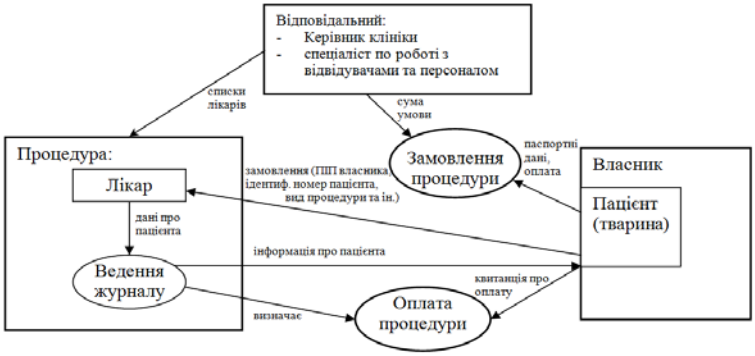



Рисунок 1 – Схема взаємозв'язку процесів та інформаційних потоків

Основні вимоги до функціональних характеристик програмного забезпечення ІДС ветеринарної клініки: дані, що вносяться користувачем повинні автоматично заноситися в базу даних; необхідний контроль правильності внесених даних, у разі помилки, дані не повинні заноситися в базу даних; можливість додавати в базу даних нові записи, видаляти застарілі або непотрібні записи, редагувати існуючі; виконувати необхідні запити на отримання потрібних даних; зручний і досить простий інтерфейс, який буде зрозумілий і некваліфікованому користувачеві; отримання переліку та загальної кількості пацієнтів, що відвідали клініку, за весь період або за деякий період; отримання переліку і загальної кількості власників тварин, які замовляли послуги за певний період; отримання відомостей про конкретного пацієнта та його власника, про

конкретного лікаря ветеринарної медицини та про кількість процедур, проведених ним, про пацієнтів конкретного лікаря ветеринарної медицини та суму оплати наданих ним послуг; отримання списку пацієнтів, які повинні відвідати клініку за певний період згідно запланованого графіку процедур; отримання даних про загальні суми сплат за процедури; отримання кількості вільних або зайнятих лікарів на даний момент згідно графіку процедур; отримання відомостей про конкретну процедуру. Вхідною інформацією є дані про лікарів, пацієнтів та їх власників, а також процедур та послуг, що надаються клінікою. Вихідні дані організовуються у вигляді відповіді на запит, який виводиться на головне вікно або звіту. Після перегляду результату є можливість виконати наступний запит або роздрукувати звіт.

Розробка бази даних здійснена за допомогою СУБД Microsoft Access 2013, вибір якої базувався на результатах аналізу наявного, доступного та фінансово виправданого програмного забезпечення для клініки даного рівня прибутковості. Крім того однією з основних переваг даної СУБД є те, що БД зберігається як локальний файл, який зручно транспортувати. Дана СУБД надає можливість створювати внутрішні форми для роботи з БД, що значно полегшує роботу програмісту та кінцевому користувачу, підтримує виконання запитів за допомогою підтримки мови SQL. У Access повною мірою реалізовано управління реляційними базами даних. Система підтримує первинні та зовнішні ключі і забезпечує цілісність даних на рівні ядра, що запобігає несумісним операціям оновлення або видалення даних. Крім того, таблиці в Access забезпечені засобами перевірки допустимості даних, що запобігають некоректному введенні даних. Середовище системи Access підтримує обробку транзакцій з гарантією їхньої цілісності. Крім того, передбачений захист на рівні користувача, що дозволяє контролювати доступ до даних окремих користувачів і груп користувачів. Для зручності роботи з БД розроблений графічний інтерфейс користувача мовою Visual Basic for Applications. В якості головного меню створена головна кнопкова форма з метою навігації по БД. Елементами головної кнопкової форми є об'єкти форм і звітів. Запити та таблиці не є елементами головної кнопкової форми, тому для створення кнопок «Запити» або «Таблиці» на кнопковій формі можна використовувати макроси.

**Висновок.** Розробка ІДС ветеринарної клініки та її впровадження в дію призначена підвищити рівень ефективності діяльності організації за рахунок автоматизації основних процесів ведення обліку та звітності, підвищити якість управління та планування процесами на основі розширення можливості контролю та звітності кількісних та якісних показників діяльності, зекономити час та зменшити трудомісткість робіт, що раніше виконувались вручну на паперових носіях, наприклад, ведення журналів обліку відвідування та переліку процедур, які надані та плануються згідно з дотриманням термінів, пацієнтам даної клініки.

УДК 517.518.2

## Развитие информационного обеспечения процесса автоматического управления в переменных базовых режимах

Бурлака А.А., студент 5 курса, Швачка А.И., к.т.н., доцент
*ГВУЗ "Украинский государственный химико-технологический университет", г. Днепр*

Современные тенденции развития науки и техники характеризуются разработкой, внедрением и широким использованием компьютерных систем поддержки принятия решений, в основу которых положены методы математического моделирования. В тоже время развитие предприятий металлургического комплекса, решение проблем энергосбережения, повышение качества и конкурентоспособности продукции на мировом рынке требует усовершенствования систем использования информации для управления отдельными технологическими процессами и производства в целом [1]. Необходимы надежные методы переработки информации для анализа и прогноза, для принятия решений и контроля за их исполнением.

Одним из важнейших условий создания эффективных систем управления таких объектов является совершенствование математических моделей, которые позволяют получить информацию о процессах в промышленных агрегатах, осуществлять оптимизацию их режимных параметров, разрабатывать и совершенствовать алгоритмы управления технологическими и техническими системами.

В качестве объекта исследования принят тепловой режим доменной плавки с точки зрения управления «снизу», т.е. изменением характеристик дутья. Нестабильность энергетической базы металлургического предприятия определило целесообразность перехода к задаче множественного выбора [2] и определения критерия управления в виде:

$$(K,(-P)) \rightarrow min,$$

где Р - производительность печи, *т чуг/ час*; К- удельный расход кокса, *кг/т чуг*.

В рассматриваемой задаче снижение энергопотребления объекта управления должно сопровождаться повышением производительности. В основе решения задачи принцип бинарного отношения предпочтения Парето [3]. Перебор и анализ точек конкурирующих решений выполнен с использованием понятия «конуса» на плоскости искомых величин.

На рис. 1 представлены результаты вычислительного эксперимента. Адекватность модели оценена путем сопоставления решения задачи с производственными данными по объекту исследования. Отличительной особенностью является множество точек решения конкурирующих в том

или ином отношении по энергопотреблению. Построена линия, определяющая тенденцию изменения точек решения (—) для выполнения анализа.

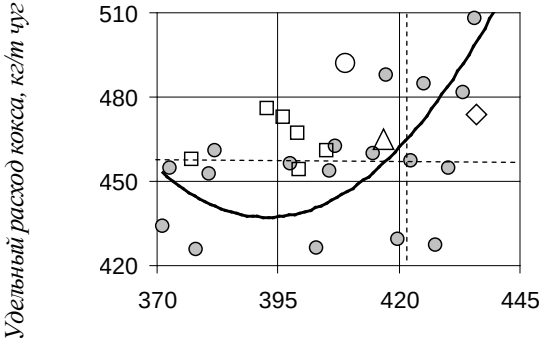



Рис. 1. Компромиссные решение задачи векторной оптимизации в области «удельный расход кокса - производительность» на ДП №9 ПАО «АрселорМиттал Кривой Рог» (АМКР):

o - результаты вычислительного эксперимента; (—)- тоже, тенденция изменения; (---)- то же, экстремальная тенденция; производственные данные ДП№9 ПАО «АМКР»: ◊- 1977 г., Δ- 1981 г., □- (1985-1990)гг., ○- 2007 г.

Для выбора реализуемого технологического режима, среди полученных точек, необходимо формирование глобального максимума с учетом наличия и объемов энергетической базы предприятия, технической возможности оборудования и практической целесообразности. Вариант реализации, представленный на рис. 1 (---), определяет тенденцию наращивания производства при стабилизации энергопотребления.

Использование алгоритма решения задачи векторной оптимизации в составе системы управления доменной печью позволяет дополнить информационно-управляющую систему производственного процесса формализованными методами поддержки выбора управляющих решений.

**Литература**

1. Спирин, Н. А. Компьютерные методы моделирования доменного процесса [Текст] / Н. А. Спирин ; под ред. Н. А. Спирина - Екатеринбург: УГТУ - УПИ, 2005. 301с.

2. Бородулин, А. В. Домна в энергетическом измерении [Текст]/ А. В. Бородулин / А. Д. Горбунов, В. И. Романенко, С. П. Сущев - Днепродзержинск, 2006. - 450 с.

3. Цымбал, В. П. Математическое моделирование сложных систем в металлургии [Текст] / В.П. Цымбал - М.: Издательское объединение «Российские университеты»; Кузбасвузиздат - АСТШ, 2006.- 431 с.

УДК 004.056.5

# Програмна реалізація визначення функціонального профілю захищеності інформаційно-телекомунікаційної системи від несанкціонованого доступу

Бучик С.С., д.т.н, доцент,
Нетребко Р.В., викладач
*Житомирський військовий інститут імені С.П. Корольова, м. Житомир*

Сучасні методи обробки, передачі й накопичення інформації сприяли появі загроз, що забезпечують можливість втрати, перекручування та розкриття даних. Тому побудова надійного захисту автоматизованої системи залишається актуальною, звідки виникає необхідне завдання високоякісного забезпечення безпеки інформаційно-телекомунікаційних систем (ІТС), яке неможливо виконати без попереднього аналізу можливих загроз безпеки системи [2, с. 50].

Не прийняття мір та заходів щодо захисту державних інформаційних ресурсів, які мають відповідне матеріальне вираження і вимагають захисту від різноманітних за своєю сутністю загроз, може призвести до зниження цінності даних ресурсів.

Проаналізувавши нормативно-правову базу (НПБ), а саме НД ТЗІ 2.5-004-99 та НД ТЗІ 2.5-005-99 авторами було проведено моделювання процесів визначення функціональних профілів захищеності (ФПЗ) за допомогою діаграм та алгоритмів. На рис. 1 наведено декомпозовану діаграму процесу визначення ФПЗ.

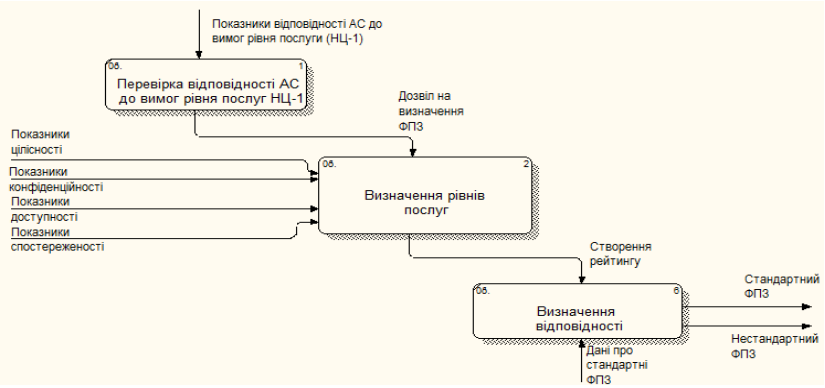



Рисунок 1 – Декомпозована діаграма процесу визначення ФПЗ

Діаграма включає наступні блоки: блок перевірки відповідності АС до вимог рівня послуги комплексу засобів захисту НЦ-1, блок отримання

ФПЗ АС від несанкціонованого доступу (НСД), блок перевірки відповідності визначеного профілю захищеності до стандартного ФПЗ.

На основі розроблених діаграм, алгоритмів та проведених авторами досліджень в роботі [1], було розроблено програмне забезпечення для автоматизованого визначення ФПЗ. Програмне забезпечення "ОФПАС 1.0" призначене для оцінювання функціонального профілю АС та створення ФПЗ оброблюваної інформації від НСД відповідно до нормативних документів України в галузі інформаційної безпеки. Результат роботи програми по визначенню стандартного ФПЗ показано на рис. 2.

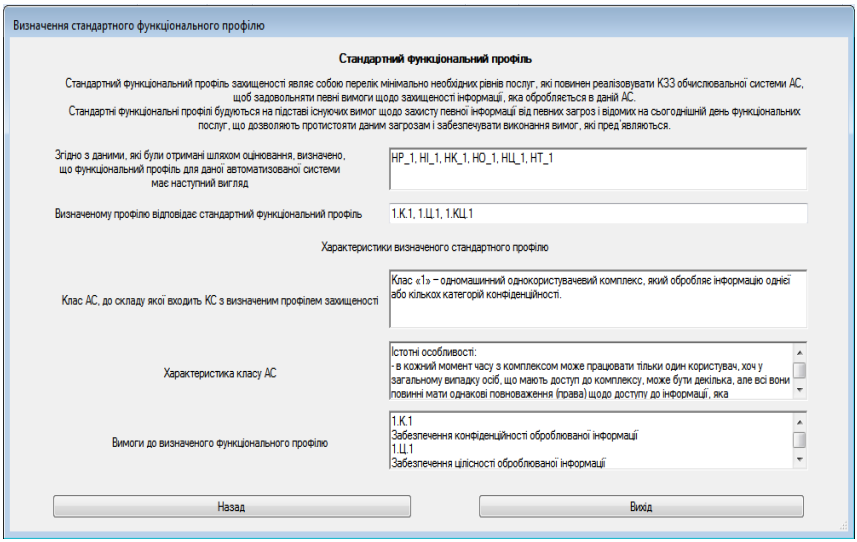



Рисунок 2 – Визначення ФПЗ

**Висновки.** Промодельована основа визначення ФПЗ, визначено основні блоки, які потрібно розробити в програмному забезпечені та реалізовано програмне забезпечення.

**Список літератури**

1. Юдін О. К. Теоретичні основи визначення стандартних функціональних профілів захищеності автоматизованої системи від несанкціонованого доступу / О. К. Юдін, С. С. Бучик, С. В. Мельник // Наукоємні технології. – 2016. – № 2 (30). – С.195 – 205, doi.org/10.18372/2310-5461.30.10564

2. Юдін О. К. Державні інформаційні ресурси. Методологія побудови класифікатора загроз : монографія / О. К. Юдін, С. С. Бучик – К.: НАУ, 2015. – 214 с.

УДК 621.396.946.2

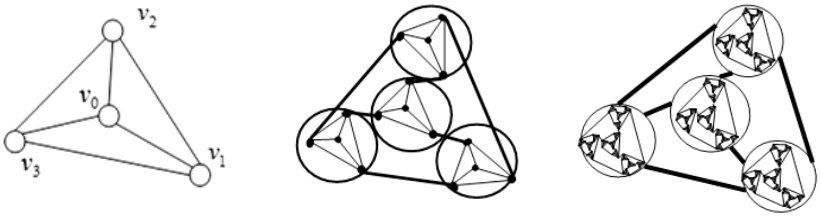
# Синтез складних ієрархічних структур с використанням спектральної теорії графів

Воротніков В.В., к. т. н., доцент,
Бойченко О.С., науковий співробітник,
Гуменюк І. В., ад'юнкт,
*Житомирський військовий інститут імені С. П. Корольова,*
*м. Житомир*

При дослідженні мережевих систем, необхідно вирішувати не тільки задачу розпізнавання архітектури вже існуючої мережі, а й самого процесу розвитку структури мережевої системи. В теорії графів широко розвинуті спеціальні методи для вирішення різних завдань, але ще мало загальних методів, що дозволяють одноманітно вирішувати цілі класи задач. В якості джерел створення таких досить загальних методів найчастіше виступають інші, раніше сформовані, області математики. Прикладом може служити лінійна алгебра, в результаті застосування якої в теорії графів виник новий напрям – спектральна теорія графів, заснована на алгебраїчних інваріантах графа (його спектрах) і знайшла широке застосування при вирішенні конкретних прикладних задач, які виникають в теорії інформаційних, комунікаційних і транспортних мереж.

В роботі запропоновано метод побудови складних ієрархічних мережевих систем з використанням передфрактальних графів і рекурсивного методу розрахунку спектра графів (елементи головної матриці інцидентності структури прирівнюються значенням спектра графа, отриманого на попередньому рівні побудови).

**Побудова передфрактального графа мережі.** В графі $G = (V, E)$, що описує топологію деякої мережі, кожну вершину з'єднуємо ребром з однією з вершин первинного графа $H = (W, Q)$ (рис. 1а).




а) б) в)

Рисунок 1 - Процес побудови передфрактального графа
а) первинний граф; б) I ітерація; в) II ітерація

Передфрактальний граф позначимо через $G_L = (V_L, E_L)$, де $V_L$ – множина вершин графа, а $E_L$ – множина його ребер. Визначимо його рекурентно, замінюючи в побудованому на попередньому етапі графі $G_l = (V_l, E_l)$ кожну його вершину первинним графом $H = (W, Q)$.

Процес побудови передфрактального графа $G_L$ є процесом побудови послідовності передфрактальних графів $G_1, G_2, ..., G_l, ..., G_L$, що називається траєкторією [1].

**Розрахунок спектра графа мережі.** Під спектром графа розуміють множину, що складається з власних значень матриці суміжності. Власні значення матриці $A$ (нулі багаточлена $|\lambda I - A|$) і спектр матриці $A$ (складається з власних значень) називаються власними значеннями і спектром графа. Відомо, що ізоморфні мультиграфи (мультиорграфи) мають однаковий спектр [2].

Для розрахунку спектра первинного графа використаємо формулу характеристичного багаточлена, прирівнявши його значення до нуля. Відповідно, маючи матрицю суміжності отримаємо вигляд характеристичного полінома $\lambda^3 - 3\lambda - 2 = 0$ з відповідними власними значеннями $\lambda_1 = 2$, $\lambda_2 = -1$, $\lambda_3 = -1$. Використовуючи поняття блочної матриці для передфрактального графа, проведемо заміну значень головної діагоналі матриці суміжності отриманим характеристичним поліномом. Таким чином первинний граф представимо у вигляді елемента передфрактального графа на першому етапі побудови (рис. 1б), для якого розрахуємо спектр $-\lambda^9 + 12\lambda^7 + 6\lambda^6 - 48\lambda^5 - 48\lambda^4 + 55\lambda^3 + 96\lambda^2 + 36\lambda$ з власними значеннями: $\lambda^*_1 = \lambda^3 - 3\lambda$, $\lambda^*_2 = \lambda^3 - 3\lambda - 3$, $\lambda^*_3 = \lambda^3 - 3\lambda - 3$.

**Висновки.** Процес розвитку мережевих структур відповідає певним правилам побудови передфрактальних графів, що в свою чергу дозволить синтезувати більш складні ієрархічні мережеві структури з використанням простих математичних операцій. Для формування ієрархічних мережевих структур вищого рівня необхідно оцінювати спектр структури на ранг нижче, нехтуючи всіма іншими.

**Список літератури**

1. Synthesis of complex networks regular fractals / Danik Yu., Kulakov Yu., Vorotnikov V., Gumenyuk I. // The advanced science journal, 2014. – Vol. 1, Issue 10. – P. 72-78.

2. Лебідь В.О., Нижник Л.П. Спектральний аналіз зіркового графа з одним нескінченним променем //Наук. зап. НаУКМА. – 2013. С. 18–22.

УДК 004.056.53

## Огляд програмних засобів аналізу соціальних мереж

Гермак В.С., викладач,
Науковий керівник – Мелешко Є.В., к.т.н., доцент
*Центральноукраїнський національний технічний університет, м. Кропивницький*

Виходячи з реалій сьогодення фактично не можна назвати жодної грані людської діяльності, до якої б не дотягнулась павутинка мережі Інтернет. Зокрема, мало хто з нас може сказати що не знайомий з таким поняттям як он-лайнові соціальні мережі. Для сучасної людини, темп життя якої майже не залишає часу на живе спілкування, соціальні мережі мають дуже велике значення. А те, що цікавить особистість, цікавить і суспільство в цілому. Тому наразі дуже актуальним постає питання моніторингу та аналізу соціальних мереж. Попит, як відомо, породжує пропозицію, тому зараз існує безліч систем та програм, які дозволяють аналізувати соціальні мережі.

Щоб якось зорієнтуватись в цьому розмаїтті, слід розуміти, які цілі буде ставити перед собою користувач та в чому полягає суть моніторингу та аналізу соціальних мереж. Моніторинг включає отримання та структуризацію первинних даних. Збираються тексти повідомлень, зв'язки між користувачами, посилання на зовнішні ресурси. Системи, що підтримують моніторинг в режимі реального часу, складніші в реалізації, але є кращими з точки зору користувача за рахунок актуальності отримуваних даних, ніж ті, які використовують ретроспективний збір даних. Аналіз включає в себе кілька етапів обробки даних. Початковим етапом є обчислення базових кількісних показників, далі виявляються статистичні та структурні закономірності в даних, що дає розуміння природи досліджуваної мережі. На основі результатів аналізу поточного стану мережі можна виконати прогноз поведінки мережі з часом. Прогноз можливий після ідентифікації математичної моделі інформаційного процесу. Одним з найскладніших в реалізації є управління соціальною мережею, яке полягає в здійсненні цілеспрямованих впливів на соціальну мережу для переведення інформаційних процесів в бажаний стан. Завдання аналізу, прогнозування та управління можуть бути різними, в першу чергу, в залежності від того, хто є кінцевим користувачем системи.

Можна виділити наступні типи кінцевих користувачів, зацікавлених в аналізі, прогнозуванні та управлінні соціальними мережами: органи державної влади та місцевого самоврядування; підприємства державного та приватного сектору економіки (комерційні організації особливо «брендові», дослідницькі організації, засоби масової інформації, силові структури); суспільство (політичні партії, окремі фізичні особи). На даний

час найбільш розвинутими є системи аналізу соціальних мереж для комерційних організацій.

Також системи аналізу соціальних мереж можна класифікувати за такими ознаками:

- рівень аналізу соціальних мереж (моніторинг, аналіз, прогнозування, керування);
- моделі соціальних мереж, реалізовані в системі (структурні моделі, моделі розповсюдження інформації та ін.);
- методи аналізу даних, що реалізовані в системі (статистичні, методи аналізу графів, семантичні та ін.);
- об'єкти аналізу (мережі в цілому, співтовариства, окремі користувачі);
- режими аналізу даних (лише моніторинг, ретроспективний аналіз, аналіз в реальному часі);
- режими збору даних (збір даних відсутній, ретроспективний, в реальному часі, дані в цілому або за вказаною тематикою);
- джерела оброблюваної інформації (класичні он-лайнові соціальні мережі, блоги, мікроблоги, сервіси для обміну мультимедіа, форуми та ін.);
- обсяги даних що можуть оброблятись;
- можливості візуалізації проаналізованої мережі.

Зважаючи на все вищевказане можна виділити декілька груп систем аналізу соціальних мереж. Перша група це системи призначені в основному для моніторингу даних, вони мають невисокі можливості для аналізу, але їх використання не вимагає від користувача якоїсь особливої підготовки. Це різні пошукові системи (наприклад search.twitter.com, blogsearch.google.com та ін.), системи моніторингу GoogleAlerts, Twilert, GoogleTrends, GoogleReader, Yahoo! Pipes, Komfo, Edgerankchecker, Wildfire Social Media Monitor, SocialSeek та ін. Друга група це системи моніторингу і аналізу соціальних мереж для комерційних організацій. Сюди можна віднести такі системи як IQbuzz, Babkee, Wobot, Brandwatch, BuzzLook, YouScan, HootSuite та ін. Окремо слід виділити програмні засоби, які дають можливість аналізу соціальних мереж та їх візуалізації. Найпопулярнішими з них є наступні: Gephi, NetLogo, Igraph, Pajek, UCINet, NodeXL, NetDraw, NetViz, Inflow, Touch Graph, R, NetworkX, SoNIA.

Наприкінці слід зауважити, що більшість програмних засобів для аналізу соціальних мереж є зарубіжними, що свідчить про те, що на сучасному етапі даному питанню в нашій державі приділяється недостатньо уваги.

УДК 004.056.55

# Дослідження методу "Кидання променів" у комп'ютерній графіці

Грищенко О.В., магістрант,
Науковий керівник – Резніченко В.А., викладач
*Центральноукраїнський національний технічний університет, м. Кропивницький*

**Метод "Кидання променів"** – це алгоритм комп'ютерної графіки на основі "кидання" променя немов би "з очей" глядача, крізь кожен піксел екрана, і знаходження найближчого об'єкта, що блокує хід такого променя. Використавши властивості матеріалу і освітлення сцени, можна отримати шуканий колір пікселя. Терміни "кидання променів" і "трасування променів" часто плутають. Однак термін "метод кидання променів" (у відношенні до рендерингу) фактично означає спрощений, нерекурсивний варіант трасування променів, бо у ньому не відбувається подальша обробка відбитих чи заломлених променів, а враховується лише перша поверхня-перешкода на шляху променів. Цей метод застосовується у відеоіграх із 80-х років. Він досить неточний, тож для збільшення реалістичності зображення розробникам доводиться послуговуватися стандартними для сучасних ігор прийомами затінення (текстурні мапи тіней та ін.). Однак цей метод дозволяє добре обробляти конічні чи сферичні поверхні, які важко реалістично імітувати, скажімо, полігонами.

Термін "кидання променів" був вперше використаний у комп'ютерній графіці в 1982 році в роботі Скотта Рота, який застосував його для опису методу рендерингу CSG-моделей.

**Принцип роботи методу "Кидання променя"**

Око/камера (eye) та екран (screen) встановлюються в 3D-просторі

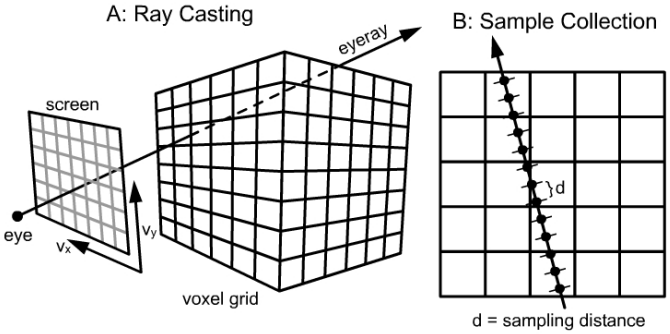



Рисунок 1 – Метод "Кидання променя"

поряд з об'ємною сіткою (voxel grid) (рис. 1 А).

Для збору значень функції "Кидання променю", промінь випускається з ока через кожен піксель трьохвимірного зображення. Значення функції збирають вздовж руху променя всередині воксельної сітки (рис 1 В). Відстань між вибірками задається користувачем; більша відстань призводить до більш чіткої та добре апроксимованої поверхні об'єктів на екрані. Для прийнятної якості зображення, відстань між вибірками повинна бути меншою, ніж розмір вокселя.

**Застосування методу "Кидання променя"**

Популярні ігрові двигуни, такі як Unity3D, CryEngine, UnrealEngine включають в себе реалізацію методу "Кидання променів".

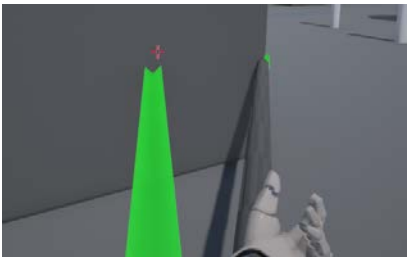


Рисунок 2 – Використання методу "Кидання променя"

Метод "Кидання променів" може застосовуватися для вирішення різних проблем, таких як:

- Загальна проблема визначення першого об'єкта, перетнутого променем.
- Видалення невидимих поверхонь на основі знаходження першого перетину променя, що "кинутий" з "ока" через кожен піксель зображення.
- Реалізація нерекурсивного алгоритму "трасування променів", який відкидає первинні промені.
- Реалізація прямого методу "об'ємної візуалізації", відомого також як "об'ємне кидання променя", в якому промінь "пробиває" об'єкт і залишає відбиток всередині скалярнго 3D-поля.

**Список літератури**

1. Scientific Visualization: Volume Surface Rendering. [Електронний ресурс] – Режим доступу http://johnrichie.com/V2/richie/isosurface/volume.html – Останній доступ: 2017.

2. Ray casting. [Електронний ресурс] – Режим доступу https://en.wikipedia.org/wiki/Ray_casting – Останній доступ: 2017.

УДК 004.92

**Автоматизація вилучення рухомих об'єктів з серії фотографічних зображень отриманих незафіксованою камерою**

Дрєєв О.М., к.т.н.,
Дрєєва Г.М., асистент,
*Центральноукраїнський національний технічний університет,*
*м. Кропивницький*

В процесі отримання художніх або архітектурних фотознімків, при наявності рухомих об'єктів, використовувалися довгі витримки з темними світлофільтрами. В результаті рухомі об'єкти, автомобілі або люди, залишали змазані треки, але за ними досить чітко виступали деталі будівель або пейзажів. Така технологія вимагала жорсткої фіксації камери.

Сучасні цифрові фотографічні засоби дозволяють використовувати більш складні та якісні засоби виділення нерухомої частини зображення з відсутністю шляхів руху сторонніх об'єктів. Авторами вдосконалено алгоритм медіанного відбору пікселів з серії кадрів, де залишаються пікселі цифрового фото, які частіше зустрічаються на окремих кадрах, та відрізняється від відомих методів наявністю маскування нерухомих зон та використанням фотокадрів з незафіксованої камери (фото з руки).

Рішення про пріоритет обробки фотографічного зображення перед відеорядом прийнято з причини значно вищої якості одиночних фотографій на переважній більшості пристроїв, які призначено для отримання цифрового зображення. Тому, при отриманні серії знімків з інтервалом 0,1-1,5 секунди, спостерігається значне зміщення поля зору камери за рахунок тремтіння рук користувача. Дослідження показало, що використання алгоритмів пошуку потоків руху для зведення полів кадрів є недоцільним з точки зору продуктивності системи так і її точності, бо між кадрами присутня суттєва зміна. Тому тут дає кращі результати вирівнювання кадрів за допомогою алгоритму градієнтного спуску, коли за скалярне поле приймається функція суми квадратичного відхилення:

$$\Delta = \sum_{i,j} \left( A_{i,j} - B_{x(i,j),y(i,j)} \right)^2,$$

де A, B – відповідні інтенсивності пікселів на зображеннях; відповідність координат задається шуканим перетворенням:

$$\begin{cases} x = di + i\cos(\alpha) - j\sin(\alpha) \\ y = dj + i\sin(\alpha) + j\cos(\alpha) \end{cases}.$$

Тут шукані параметри *di, dj* – зміщення координат та $\alpha$ – кут повороту зображення. Попереднє розмиття зображення дозволяє зробити процес більш стійким. Практика показала, що процес каскадного пошуку перетворення починаючи зі зменшених копій, дозволяє пришвидшити процес до 10 раз у випадках значних зсувів камери при отриманні зображень.

З метою покращення якості отриманого результату, перед обробкою проводиться порівняння різкості фотографічних зображень. В якості ключового кадру береться кадр з максимальною якістю, кадри з недостатньою якістю відбраковуються. Суміщення кадрів відбувається по ключовому кадру.

Після суміщення фонів будується усереднена мапа міжкадрових змін. Це дало змогу виявити зони, де не спостерігалося рухомих об'єктів і ці зони переносяться до результату без змін з ключового кадру. Інші пікселі проходять міжкадрову медіанну фільтрацію. Нехай маємо кадри $B_{k,i,j}$, де $k$ – номер кадру а $i, j$ – координати пікселю, $n$ – кількість кадрів в обробці. Тоді результатом буде:

$$R_{i,j} = \underset{k=1..n}{sort}(B_{k,i,j})_{[n/2]}.$$

Тобто, кожен піксель є середнім елементом відсортованих за яскравістю відповідних пікселів з усіх кадрів. В результаті, вихідне зображення матиме набір пікселів, які більш часто зустрічаються на серії фотографічних зображень. Однак, у випадках високої інтенсивності руху, часто відбувається подія, коли фон більш часто закритий одним з рухомих об'єктів. В такому випадку запропонований метод обробки зображення є незастосовним.

В результаті роботи побудоване програмне забезпечення автоматизації отримання з групи фотографічних зображень, зображення з відсутніми рухомими об'єктами. Система дозволяє отримувати відмінні результати й при зніманні з рук без фіксування камери.

**Список літератури**

1. Гурський Ю. Комп'ютерна графіка. Трюки і Ефекти, – СПб.: Питер, 2005.

2. Заставна Л.А. Комп'ютерна графіка: Практикум. – М.: ЛБЗ, 2005.

3. Інженерна та комп'ютерна графіка. – М.: Вища школа, 2004.

4. Калиткин Н.Н. Численные методы. – М.: «Наука», 1978.

УДК 004.928

**Автоматизована система «Trener»**

Дубонос А.С., студент 4 курсу
Науковий керівник – Корнієнко С.К., к.т.н., доцент
*Запорізький національний технічний університет, м. Запоріжжя*

Розроблена система спрощує роботу тренера щодо побудови тактичної моделі гри команди, допомагає вести облік складу команди, розкладу матчів і тренувань.

Додаток розроблений на мові програмування C# з використанням технології WPF.

Головною функцією додатку є побудова анімованих схем переміщень гравців. Дана функція реалізована за допомогою вбудованих функцій анімацій у програмному фреймворку.

Кожен елемент на схемі має власний шлях переміщення, який складається з контрольних точок на часовій смузі. Кожна контрольна точка це позиція об'єкту на схемі у певний період часу.


Рисунок 1 – Вікно для створення схеми переміщень гравців

Алгоритм роботи побудови анімації переміщень гравців.

1. Отримаємо список усіх об’єктів анімації з їхніми контрольними точками. Відмальовуємо усі об’єкти на Canvas.

2. Перебираємо кожну секунду відтворення, якщо якийсь об’єкт має на даній секунді контрольну точку, то створюється анімація для усіх об’єктів до їх позицій. Якщо у об’єкту у даний момент часу немає контрольної точки, то проводиться апроксимація його позиції між двома сусідніми контрольними точками.

3. Після створення анімації переміщення усіх об’єктів, для кожного переміщення створюється анімація відображення стрілок.

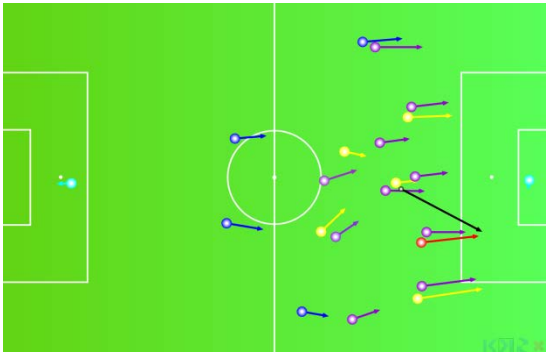


Рисунок 2 – Результат роботи алгоритму створення анімації

Іншою важливою функцією додатку є ведення розкладу матчів і тренувань. Для зручності роботи з даним типом даних були розроблені спеціальні елементи керування.

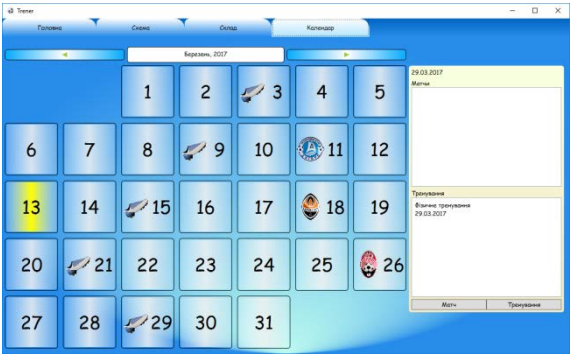



Рисунок 3 – Вікно для роботи з розкладом матчів і тренувань

УДК 621.391

**Реалізація захисту шлюзу «за замовчуванням» при підвищенні відмовостійкості в IP мережі**

Єременко О.С., докторант,
Тарікі Н., аспірант,
*Харківський національний університет радіоелектроніки, м. Харків*

Одним з ефективних засобів підвищення відмовостійкості телекомунікаційної мережі (ТКС) є маршрутизація. Саме в процесі маршрутизації потоків пакетів можуть бути визначені такі маршрути, при використанні яких можливо забезпечити необхідний рівень надійності їх доставки. Головним завданням при цьому є вибір шлюзу для передачі пакетів з мережі доступу (Access Network) в транспортну мережу (Transport Network). Наприклад, в разі організації транспортної мережі на основі IP/MPLS для підвищення відмовостійкості використовується технологія Fast ReRoute [1-3]. Тоді як для вирішення завдань захисту шлюзу існують спеціальні протоколи.

Найбільш популярні протоколи відмовостійкої маршрутизації в IP мережах (Fault-Tolerant IP Routing) для захисту шлюзів «за замовчуванням» включають в себе протокол гарячого резерву маршрутизатора (Hot Standby Router Protocol, HSRP), протокол резервування віртуального маршрутизатора (Virtual Router Redundancy Protocol, VRRP), протокол балансування навантаження на шлюз (Gateway Load Balancing Protocol, GLBP). Крім того, широко використовується протокол дуплікації загальної адреси (Common Address Redundancy Protocol, CARP) як альтернатива попереднім протокольним рішенням.

Необхідно відзначити суттєві недоліки в існуючих рішеннях відмовостійкої маршрутизації в IP мережах, а саме:

- не враховується потоковий характер мережного трафіку;
- відсутність узгодженого розв'язання пов'язаних задач вибору шлюзу та маршрутизації в транспортній мережі;
- обмежені можливості існуючих протоколів щодо балансування навантаження.

У зв'язку з цим пропонується схема захисту шлюзу в рамках відмовостійкої маршрутизації в IP мережі, яка заснована на вдосконаленні відповідної потокової математичної моделі [4, 5]. В рамках запропонованої моделі задача відмовостійкої маршрутизації була зведена до розв'язання оптимізаційної задачі нелінійного програмування, де частина керуючих змінних відповідає за вибір шлюзу в мережі доступу, а деякі – за вибір шляху/шляхів при маршрутизації в транспортній мережі.

Реалізація функцій відмовостійкості була забезпечена за рахунок введення додаткових маршрутних змінних, які відповідають за

визначення резервного шлюзу «за замовченням» і відповідного шляху (або множини шляхів в разі реалізації багатошляхової маршрутизації) в транспортній мережі. Ця схема була реалізована з метою захисту пропускної здатності для розрахованого шляху або множини шляхів. Тоді як реалізація цільової функції дозволила мінімізувати умовну вартість використання ресурсів мережі доступу та транспортної мережі при розв'язанні задачі відмовостійкої маршрутизації. Вибір маршрутних метрик виконувався таким чином, що вибір шлюзу «за замовчуванням» реалізовувався за критерієм максимальної доступності, а вибір маршруту в транспортній мережі – відповідно до критерію максимальної пропускної здатності (за аналогією з протоколом IGRP).

Розрахункові приклади продемонстрували особливості застосування запропонованої моделі при організації захисту шлюзу в ході відмовостійкої маршрутизації в IP мережі для випадку одношляхової та багатошляхової маршрутизації. Отримані результати підтвердили ефективність та адекватність запропонованої моделі.

**Список літератури**

1. Rak, J. Resilient Routing in Communication Networks (Computer Communications and Networks). 1st edition [Text] / J. Rak. – Springer, 2015. – 181 p.

2. Hariyawan, M.Y. Comparison Analysis of Recovery Mechanism at MPLS Network [Text] / M.Y. Hariyawan // International Journal of Electrical and Computer Engineering (IJECE). – 2011. Vol. 1, No. 2. – P. 151-160.

3. Papán, J. Analysis of existing IP Fast Reroute mechanisms [Text] / J. Papán, P. Segeč, P. Palúch // IEEE 2015 International Conference on Information and Digital Technologies (IDT), 2015. – P. 291-297. DOI: 10.1109/DT.2015.7222986.

4. Лемешко, А.В. Повышение масштабируемости и производительности решений по отказоустойчивой маршрутизации в телекоммуникационных сетях [Текст] / А.В. Лемешко, А.С. Еременко, Н. Тарики, К.М. Арус // Системи обробки інформації. – 2016. – № 1(138). – С. 152-156.

5. Lemeshko, O.V. Fault-Tolerance Improvement for Core and Edge of IP Network [Text] / O.V. Lemeshko, O.S. Yeremenko, N. Tariki, A.M. Hailan // IEEE 2016 XIth International Scientific and Technical Conference "Com-puter Sciences and Information Technologies" (CSIT), 2016. – P. 161-164. DOI: 10.1109/STC-CSIT.2016.7589895.

УДК 681.518

**Огляд інформаційно-програмного забезпечення для керування комплексом моделювання динамічної повітряної обстановки пілотованих та безпілотних літальних апаратів**

Єршов В.В., аспірант
Науковий керівник – Ізвалов О.В., к.т.н., доцент
*КЛА НАУ, м. Кропивницький*

Існуюча тенденція зростання інтенсивності повітряного руху (ПР) призводить до появи та розвитку програмного забезпечення, призначеного для моделювання динамічної повітряної обстановки. Важливо відмітити також поширення безпілотних літальних апаратів (БПЛА), зокрема, дронів, квадрокоптерів тощо. З огляду на вищенаведене, доцільним є дослідити існуючі програмні засоби моделювання динамічної повітряної обстановки.

*VATSIM Network* - загальнодоступна спеціалізована міжнародна комп'ютерна мережа, створена ентузіастами віртуальної авіації. Метою її є відтворення в мережі реальних процедур взаємодії екіпажів повітряних суден та диспетчерів служби управління повітряним рухом. VATSIM об'єднує людей в десятках країн. Набір технічних засобів дозволяє відтворити в комп'ютерній мережі взаємодію різних ланок цивільної авіації, відтворити роботу авіакомпаній, органів управління повітряним рухом, аеродромів усього світу. Як і в реальності, весь повітряний простір розділено на регіональні повітряні зони, відповідальність за які лежить на певних диспетчерських пунктах, підпорядкованих регіональним організаціям. Віртуальний повітряний простір симулюється декількома з'єднаними між собою серверами, до яких проводиться безпосереднє підключення учасників мережі (диспетчерів і пілотів).

*IVAO* (The International Virtual Aviation Organisation) - онлайн-сервіс, призначений для ентузіастів віртуальної авіації в усьому світі. Для роботи з мережею необхідна спеціальна програма-клієнт. Існують версії для Prepar3D і X-Plane. В якості основних інструментів використовуються Ivac (симулятор авіадиспетчера) і Ivap (симулятор радіо-панелі пілота). Віртуальна мережа поділена на дивізіони, відповідно до географічної приналежності до країни. Пілот керує літаком в авіасимуляторі, спостерігаючи навколо себе інші підключені до мережі повітряні судна. Всі вони, в свою чергу, з'являються у вигляді міток на екранах диспетчерських програм, де передбачені можливості подібні до можливостей реальних автоматизованих систем управління повітряним рухом. Пілот і диспетчер взаємодіють завдяки можливості складання і коригування плану польоту, за допомогою голосового та текстового спілкування. Завдяки використанню актуальної метерологічної інформації

(METAR) в мережі по можливості створюються реальні погодні умови в районі аеродромів та на ешелоні.

*Автоматизоване робоче місце диспетчера УПР «Оріон»* призначене для використання в якості засобу обробки і відображення інформації на робочих місцях (пультах) диспетчерів управління повітряним рухом в районах аеродромів, районах центрах, а також на вишках АКДП. Виріб може вбудовуватися в типові диспетчерські пульти, в тому числі пульти, що виготовляються АТ «Азимут».

Програмне забезпечення для управління черговістю *OSYRIS Queue Management* компанії Barco розроблене для забезпечення цілісності організації повітряного руху, посадки, зльоту і руху повітряного транспорту і відповідає специфічним потребам і вимогам постачальників послуг повітряної навігації і учасників повітряного руху в усьому світі.

Програмне забезпечення для управління прибуттям компанії Barco Arrival Manager дозволяє підвищити пропускну спроможність аеропортів і скоротити робоче навантаження на авіадиспетчерів, оптимізуючи транспортні потоки. Програма Arrival Manager дає можливість оптимально використовувати доступні ресурси, більш ефективно організовує роботу авіаліній, підвищує якість профілів польотів та скорочує число польотів у зоні очікування, знижуючи екологічне навантаження і рівень шуму. Програма Arrival Manager автоматично обчислює послідовність прильотів, ґрунтуючись на даних про бажані терміни прибуття літаків і обмеженнях, обумовлених оперативною обстановкою.

Враховуючи значну кількість програмних засобів моделювання повітряної обстановки, можна зробити висновки, що галузь автоматизації систем обслуговування повітряного руху є цікавою для подальших досліджень.

**Список літератури**

1. Revisiting the "swiss cheese" model of accidents – Бордо: Евроконтроль, 2005 – 35 с.

2. Schmidt D.K. A queuing analysis of air traffic controllers' workload / D.K. Schmidt // IEEE Transactionson Systems, Manand Cybernetics. SMCV – N8(6) – 1978 – Pp. 492-298.

3. Sperandio J.C. Variation of operator's strategies and regulating effects on workload / J.C. Sperandio // Ergonomics – N 14 – London: IEHF, 1971. – Pp 571.

3. SSADM Manual. Version 4. – Blackwell: National Computing Centre, 1990. - 1400 p.

УДК 621.372; 621.373

# Применение волоконно-оптических систем связи в системах технической диагностики энергетического оборудования

[1]Зайцев Е.А., с.н.с., к.т.н., с.н.с.,
[2]Сидорчук В.Е., доцент., к.т.н.,
[1]Архипова Л.В., ведущий инженер
*[1] Институт электродинамики НАН Украины, г.Киев*
*[2]Киевский национальный торгово-экономический университет, г. Киев*

Современные системы технической диагностики энергетического оборудования во время эксплуатации подвержены влиянию сильных электромагнитных полей. Повышение помехоустойчивости систем технической диагностики может быть достигнуто за счет применения в их структуре волоконно-оптических линий связи (ВОЛС) вместо громоздких коаксиальных линий.

Структурная схема системы технической диагностики с ВОЛС приведена на рис.1, где ПКССК – преобразователь код-свет и свет-код; ППОС – приемно-передающая оптическая система. Работа системы заключается в следующем: диагностическая информация с сенсоров поступает в модуль обмена данными, в котором преобразуется в последовательный код типа NRZ. Далее в ПКССК закодированная в электрическом сигнале информация преобразуется в модулированный оптический сигнал с помощью ППОС в случае передачи данных или, наоборот, в случае приема данных. Модулированный оптический сигнал передается далее по волоконно-оптическому кабелю. В месте приема (ППОП), в ПКССК с помощью фотоприемника оптический сигнал будет вновь преобразован в электрический и усилен до необходимого уровня логических сигналов. Далее информационные данные поступают в модуль сбора, обработки и анализа информационных данных системы технической диагностики, которая находится на безопасном расстоянии от объекта наблюдения.

*Применение ВОЛС в структуре систем технической диагностики позволяет достичь:*

1) высокой помехозащищенности от внешних электромагнитных воздействий и от межканальных наводок, что особенно важно при повышенной плотности электромагнитных помех;

2) минимизации габаритов и массы при отказе от тяжелых экранирующих оболочек в случае использования ВОЛС (по сравнению с линиями проводной связи выигрыш по этим показателям в 3-5 раз);

3)секретности передачи информации: излучение в окружающее пространство ВОЛС почти отсутствует, а изготовление отводов оптической энергии без разрушения кабеля невозможно;

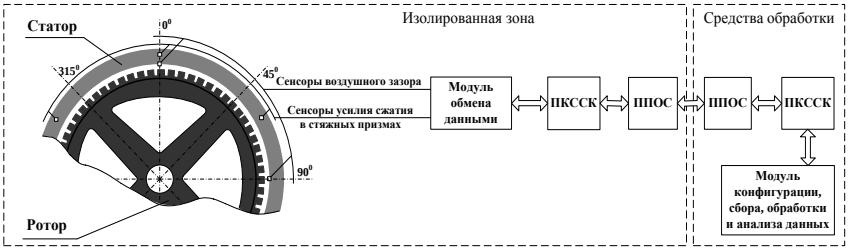



Рис.1 Структурная схема системы технической диагностики с ВОЛС

4) потенциально низкой стоимости (замена дорогостоящих цветных металлов (медь, свинец) на материалы с неограниченным сырьевым ресурсом (стекло, кварц, полимеры) для изготовления ВОЛС);

5) высокой взрывобезопасности волоконно-оптического тракта в среде с температурой самовоспламенения 450 – 600°С (смесь водорода, метана, пропана и подобных газов с воздухом), которая обеспечивается при уровне передаваемой оптической мощности, не превышающей 0,5d мВт, где d – диаметр световедущей жилы (мкм) оптического волокна.

*Преимуществами применения ВОЛС являются:*

1) почти идеальная электрическая изоляция элементов схем: в современной электронике основными элементами, обеспечивающими электрическую изоляцию блоков и узлов, являются трансформаторы и конденсаторы, недостатки которых достаточно известны: конструктивная и технологическая несовместимость с интегральными схемами, наличие обратных связей выхода с входом через паразитные реактивности, узкий частотный диапазон, большие масса и габариты, оптическая связь резко минимизирует эти недостатки и может обеспечивать передачу данных между участками схемы с электрическими потенциалами, отличающимися более чем 1000 В;

2) односторонняя передача сигнала от излучателя к фотоприемнику: практически отсутствует обратная паразитная связь, возникающая при передаче сигнала с выхода на вход (от фотоприемника к излучателю);

3) возможность получения информации о состоянии отдельных узлов в виде световых сигналов, что обеспечивает повышение достоверности контроля;

4) низкий уровень шумов вследствие разделения сигналов на два информационных канала – оптический и электрический.

**Вывод:** Использование волоконно-оптических линий связи **позволяет повысить достоверность технической диагностики энергетического оборудования за счет высокой степени помехозащищенности информационных волоконно-оптических линий связи.**

УДК 004.65

## Створення бази даних медичної установи

Карвацька А.Є., студент
Науковий керівник – Полотай О.І., к.т.н., доцент
*Львівський державний університет безпеки життєдіяльності, м. Львів*

Останнім часом, інформаційно-комунікаційні технології набувають стрімкого розвитку, відбувається стрімкий перехід від паперового до електронного документообігу. Але існують такі установи, які і до тепер користуються застарілими технологіями. Серед таких установ є установи, які не можуть відійти від радянських стереотипів і потребують примусової зміни способу існування та ведення своєї діяльності. До таких установ можна віднести державні установи, такі як громадські бібліотеки, поліклініки, сільські школи, лікарні, тощо.

З метою часткового вирішення цих проблем, було прийнято рішення створити базу даних (БД) пологового будинку, у якій зберігалася б інформація про стан породіль, перебіг їх вагітності, пологів та ін. Ці дані мають цінність і потребують структурованого та централізованого зберігання.

Алгоритм роботи запропонованої БД якої полягає у наступному. При натисненні на кнопку Старт розпочинається безпосереднє наповнення БД вище згаданими даними, а саме: анамнез матері; соматичні захворювання; інформація про перебіг вагітності; інформація про пологи; акушерський та лактаційний аналіз; інформація про новонародженого; дані параклітичних досліджень дитини; історія грудного вигодовування в пологовому будинку; катамнез; психомоторний розвиток; перенесені захворювання; грудне вигодовування на дільниці; зміна способу вигодовування; ставлення матері до грудного вигодовування; сімейний анамнез; харчування матері; планування сім'ї; з якого віку мати почала вводити додаткові продукти харчування при грудному вигодовуванні. Всі ці дані необхідно вводити в порядку відкриття відповідної форми. Дані, які вже введені в БД, у подальшому можуть бути редаговані чи доповненні. Функція безпосереднього введенння даних покладена на акушера-гінеколога.

Всього в БД налічується 21 таблиця: anamnez_materi, anketa, dodat1, dodatok2, doslidg_dutunu, grydne_vugod, grydne_vugod_dil1, grydne_vugod_dil2, grydne_vugod_dil3, katamnez, mother, novonarodgenuj, planyvannja_simji, pologu, psuxomotornuj, simejnuj_anamnez, stavlennja, vagitnist, xarchyvannja, zaxvor, zaxvoruvannja. та 22 форми з аналогічними назвами, враховуючи стартову сторінку.

На рис. 1 показано вигляд форми БД «Sstavlennja», яка є шістнадцятою по рахунку.


Рис. 1. Форма «Ставлення матері до грудного вигодовування»

Кожна з 21 форм має приблизно аналогічний вигляд і призначена для введення необхідної інформації. Після заповнення форми усією інформацією, потрібно натиснути кнопку «Вперед», щоб перейти до наступної форми. Введена інформація вводиться у відповідні таблиці БД та готова до використання.

Для відкриття БД, відповідальному працівнику, надається пароль для роботи з нею.

Основне призначення розробленої БД полягає у зберіганні зібраної у пацієнтів та працівників та медперсоналу для використання у майбутньому. Це можуть бути різноманітні запити, статистичне дослідження, побудова статистичних звітів, зберігання архівної інформації.

**Список літератури**

1. Послед Б.Г. Access 2003. БД / Б.Г. Послед. – К. : Изд-во "ДиаСофт", 2000. – 512 с.

2. Леонтьев В.Ю. Microsoft Office: Access 2003 / В.Ю. Леонтьєв. – К. : Вид-во Фенікс. 2008. – 455 с.

УДК 532.5

# Комп'ютерне моделювання ударної взаємодії рідини та тіла, що знаходиться на її вільній поверхні

Катан В.О., к. ф.-м. н., доцент,
Гоман О.Г., д. ф.-м.н., професор,
Клим В.Ю., к.т.н.
*Дніпровський національний університет імені Олеся Гончара, м. Дніпро*

**Складна система: ударна взаємодія рідини та твердого тіла**

Теоретичне та експериментальне дослідження задач гідродинаміки течій з вільними границями викликано широким колом застосовування в сучасному інжинірингу: занурення твердого тіла в рідину, ударна взаємодія рідини та твердих тіл, які плавають на її вільній поверхні, хвильові явища, підйом тіла з вільної поверхні рідини, кавітаційне обтікання тіл, рух і коливання резервуарів з рідиною та ряд інших явищ. Серед вказаних проблем ударна взаємодія тіл і рідини з вільною поверхнею займає особливе місце саме тому, що з одного боку, їй притаманні суттєві і характерні властивості явищ, які вивчаються, а з іншого боку – миттєвий характер протікання удару, що надає можливість зведення вказаної задачі до задач математичної фізики і теорії функцій із отриманням аналітичних розв'язків. Крім цього, ударна взаємодія є межовим випадком при розгляді нестаціонарних течій. Таким чином, очевидна актуальність комп'ютерного моделювання складної системи: ударної взаємодії тіл і рідини з вільною поверхнею.

**Загальні постановка та розв'язання задачі гідродинамічного удару для комп'ютерного моделювання**

Вказана задача за допомогою конформного відображення області гідродинамічної течії на верхню півплощину зводиться до класичної змішаної задачі Келдиша-Сєдова для характеристичної аналітичної функції течії [1–2].

Наведена загальна формула розв'язку задачі Келдиша-Сєдова в квадратурах. На основі варіаційного принципу Огазо запропоновано підхід визначення положення граничних точок зон відриву рідини від поверхні тіла [3–4].

На прикладі тестової задачі удару по горизонтальній пластинці з обертанням проведено детальний аналіз запропонованого авторами підходу щодо зведення задач удару до проблеми Келдиша-Сєдова та щодо використання нового способу визначення зони відриву за допомогою апарату сингулярних квадратур у сенсі скінченної частини за Адамаром.

Запропонований підхід застосовано до розв'язку задачі про удар похилої пластинки з обертанням. Отримано рівняння з інтегралами в сенсі Адамара, що визначає положення точки відриву. Обчислення інтегралів в

сенсі Адамара виконувалось за відомою процедурою Адамара-Манглера з додатковою її модифікацією: ці інтеграли, крім особливості типу Адамара на одному кінці інтегрування, на іншому кінці інтервалу інтегрування мають інтегровані за Ріманом особливості, які доводилось аналітично інтегрувати в малому околі цієї точки.

**Результати комп'ютерного моделювання**

Незважаючи на спрощення при постановці задач ударної взаємодії, характеристики течій – коефіцієнти приєднаних мас – добре співпадають зі значеннями, які отримані експериментально. Визначені розподіли імпульсивного тиску, нормальної та дотичної складової швидкості, а також, коефіцієнти приєднаних мас та моментів. Досліджено задачі про удар пластинки з обертанням, яка попередньо занурена у рідину у вертикальному або в горизонтальному положенні. Залежність параметра, що визначає положення зони відриву, та між деяким кінематичним параметром ретельно проаналізована, прорахована і проведено порівняння з відповідною залежністю, визначеною аналітичними розв'язками вказаних задач [5–6].

**Список літератури**

1. Седов Л.И. Плоские задачи гидродинамики и аэродинамики. – М.: Наука. – 1980. – 448 с.

2. Мусхелишвили Н. И. Некоторые основные задачи математической теории упругости.– М.: Наука. – 1966. –707с.

3. Общая теория аэродинамики больших скоростей под редакцией У.Р. Сирса – М.: Воениздат. – 1962. – 300 с.

4. Адамар Ж. Задача Коши для линейных уравнений с частными производными гиперболического типа. – М.: Наука. – 1978. – 352 с.

5. Гоман О.Г., Катан В.А. Математическое моделирование взаимодействия несжимаемой жидкости и вертикальной пластины, плавающей на ее поверхности при ударе с вращением в условиях отрыва // Вісник ДНУ. Серія: Механіка. – 2012. – № 5/ 20. – Вип. 16, Т.1. – С. 87 – 93.

6. Гоман О.Г., Катан В.А. Ударное взаимодействие несжимаемой жидкости и вертикальной пластины, плавающей на ее поверхности, в условиях образования одной зоны отрыва и наличии вращения / О.Г. Гоман, В.А. Катан // Вісник ДНУ. Серія:Механіка. – 2013. – № 5/21. – Вип. 17. Т.1. – С. 191 – 205..

УДК 004.415.2.043

# Використання патерну проектування SMVC для побудови сервісно-орієнтованої архітектури WEB-додатку

Кравченко О.К., студент,
Науковий керівник – Афанасьєва І.В., к.т.н., доцент
*Харківський національний університет радіоелектроніки, м. Харків*

**Service-Model-View-Controller** (SMVC, «Сервіс-Модель-Представлення-Контролер») – схема поділу сторонніх сервісів, даних, інтерфейсу та керуючої логіки, що складається з чотирьох окремих компонентів: сторонній сервіс, модель, представлення та контролер. Таким чином, компонент зв'язку зі сторонніми сервісами відділяється від логіки інших компонентів і виноситься окремо для власних модифікацій.

**Характеристика основних складових патерну**

1. Сервіс – представляє інтерфейс для роботи з зовнішніми сторонніми ресурсами, реагує на команди моделі та контролера, передає управління контролеру для зміни стану моделі.

2. Модель – це інтерфейс для роботи з даними додатка, що реагує на команди контролера, змінюючи свій стан, може передавати управління сервісу.

3. Представлення – це інтерфейс для користувача щодо роботи з самим додатком, реагує на зміни моделі й отримує початкову інформацію від контролера.

4. Контролер – це інтерфейс для обробки дій, посилає команди моделі, створює початкові дані для представлення та реагує на запити сервісу.

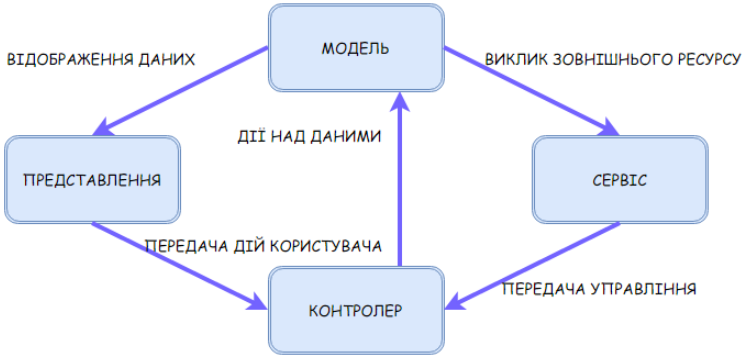



Рисунок 1 – Схема Service-Model-View-Controller патерну

Цей патерн проектування бере за основу Model-View-Controller (MVC, «Модель-Представлення-Контролер») з головною відмінністю у

відділенні зв'язку з зовнішніми сторонніми ресурсами (рис. 1) від компонентів: моделі та контролера. Основною метою SMVC є подальший розвиток та сучасна модифікація MVC (рис. 2) у житті об'єктно-орієнтованих програмних додатків.

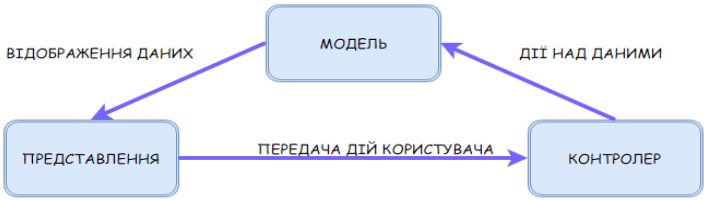



Рисунок 2 – Схема Model-View-Controller патерну

Відокремлення нового компоненту в представленому патерні (SMVC), структура та логіка якого були розбиті в моделі та контролері патерну MVC, обумовлено тим, що останнім часом бізнес-завдання додатків нарощуються та стають менш підтримуваними розробниками з огляду на порушення принципів єдиної відповідальності класів у проектуванні програми. Кожен сервіс створюється для виконання однієї бізнес-логіки, забезпечуючи поділ зв'язків між різними моделями.

При використанні SMVC передбачається, що конвенція про іменування контролерів і представлень не порушуватиме ідею архітектурного стилю в REST-підході. Таким чином, назвами контролерів слід обрати ресурси, а використані в них методи будуть брати свої назви статично для всього проекту в рамках CRUD-методів (Create-Read-Update-Delete): додавання, читання, оновлення та редагування на рівні одного та групи ресурсів.

Застосування патерну SMVC покращує розуміння коду, прискорює процес створення програми, збільшує гнучкість при роботі з Agile-методологіями та підвищує якість проектування для побудови сервісно-орієнтованого додатку.

**Список літератури**

1. Приемы объектно-ориентированного проектирования. Паттерны проектирования / . Гамма Э., Хелм Р., Джонсон Р., Влиссидес Дж. – СПб: Питер, 2001. – 368 с.

УДК 621.396.9

## Аналіз розвитку мобільного зв'язку

Куницька С.Ю., к.т.н., доцент
*Черкаський державний технологічний університет, м. Черкаси*

Мобільні технології зародились саме з ідей мобільного зв'язку, зі спроби однієї людини спілкуватись з іншою на великих відстанях. З їх допомогою можна купувати будь-які товари, проводити банківські транзакції і навіть працювати, не виходячи з дому. Роль мобільних пристроїв значно зросла, адже це новий етап в еволюції технологій взагалі.

**Розглянемо розвиток технології мобільного зв'язку.**

На даний момент можна виділити чотири основні етапи розвитку:

- 1G – це аналоговий зв'язок, що працює за стандартом NMT.
- 2G – покоління цифрового зв'язку з комутацією каналів, що працюють за стандартами GSM і CDMA,
- Третє покоління - 3G використовують стандарт UMTS, який передбачає разом з комутацією каналів і пакетну передачу даних. 3G - це набір засобів, що дозволяє використовувати як високошвидкісний мобільний Інтернет, так і технологію радіозв'язку, яка створює канал передачі даних. 3G мобільний зв'язок будується на основі пакетної передачі даних. Мережі третього покоління 3G працюють на частотах дециметрового діапазону, як правило в діапазоні близько 2 ГГц, передаючи дані зі швидкістю до 14 Мбіт/с. Вони дозволяють використовувати всі засоби передачі даних, що доступні навіть з персональних комп'ютерів.
- 4G – це новітнє покоління мобільного зв'язку майбутнього, що характеризується високою швидкістю передачі даних і підвищеною якістю голосового зв'язку. Сучасні мобільні засоби зв'язку підтримують цю нову технологію і в списку послуг операторів мобільного зв'язку доступ в Інтернет через 4G не рідкість. Системи зв'язку 4G засновані на пакетних протоколах передачі даних. Для пересилання даних використовується протокол IPv4, а також, в майбутньому планується підтримка IPv6. До четвертого покоління прийнято відносити перспективні технології, що дозволяють здійснювати передачу даних зі швидкістю, що перевищує 100 Мбіт/с.

Основна відмінність мереж четвертого покоління від третього, з точки зору способів і технологій передачі даних, полягає в тому, що технологія 4G повністю заснована на протоколах пакетної передачі даних, в той час як 3G поєднує в собі передачу голосового трафіку і «пакетів». Для передачі голосових даних в 4G передбачена технологія VoIP, що дозволяє здійснювати голосові дзвінки, застосовуючи швидку «пакетну»

передачу даних. Технологія 4G, зокрема, дозволяє абонентам дивитися багатоканальні телетрансляції високої чіткості та управляти домашньою побутовою технікою за допомогою мобільного пристрою, здійснювати дешеві міжміські телефонні дзвінки.

Такий інформаційний гігант як компанія Google є безперечно лідером у розвитку мобільних технологій взагалі. Почався розвиток нового проекту компанії – проекту під назвою «Fi». Суть даного проекту полягає в спрощенні користування мобільними пристроями в будь-якій точці планети. Принцип роботи полягає в оптимальному використанні мобільного трафіка для будь-яких цілей. Всі дзвінки, відправлення повідомлень, відвідування веб-сторінок – все проводиться через Інтернет-мережу. Якщо абонент знаходиться в тому районі, де покриття мобільного зв'язку доступне тільки від одного оператора, то передача даних проводиться традиційно – за допомогою принципів стільникового зв'язку. Але якщо в конкретній точці є дві доступних мережі стільникового зв'язку, то спеціальний алгоритм на основі даних смартфону та місцевості обирає самостійно найшвидшу мережу. Якщо в конкретній точці, де зараз знаходиться користувач доступна можливість підключення до мережі Інтернет через Wi-Fi доступ, то спеціальний алгоритм налаштовує передачу усіх даних саме через цю мережу. Також даний проект звільняє від асоціації мобільного зв'язку з мобільними телефонами. Користувач мережі Fi має змогу прийняти дзвінок чи повідомлення з будь-якого свого пристрою (смартфон, планшет, персональний комп'ютер чи розумний годинник).

**Висновки.** Розвиток мобільних технологій стрімко зростає. Завдяки таким інформаційним гігантам як Google, розвиток мобільних технологій здобув новий рівень. Відсоток використання мобільних пристроїв значно зріс у порівнянні з персональними комп'ютерами, а також взаємозв'язок мобільних пристроїв дозволяє стверджувати, що в майбутньому всі технології зможуть поєднуватись в одну мережу для найбільш зручного їх використання.

**Список літератури**

1. Коган М., Бурмистров А.В. Современные технологии мобильной связи, журнал «Успехи современного естествознания» №7, 2011.

2. Рябухина Ю. Project Fi – виртуальный мобильный оператор от Google, 2015.

3. Бабков В. Ю., Полынцев П. В., Устюжанин В. И. Качество услуг мобильной связи. Оценка, контроль и управление. М.: Горячая линия-Телеком, 2005. - 160 с.

УДК 004.912

# Обработка данных, полученных от стороннего API на примере сайта туристического агентства

Ляшенко Д.О., студент 4 курса,
Рызоль О.А., ассистент
*Днепровский национальный университет имени Олеся Гончара, г. Днепр*

При разработке web-приложения часто возникает необходимость в использовании API (от англ. A*pplication Programming Interface*). Делается это для того, чтобы воспользоваться функционалом стороннего приложения. Обычно такое взаимодействие происходит за счет передачи параметров через URL или как часть тела HTTP-запроса. Как правило, во множестве онлайн-ресурсов используется вход через социальные сети, это один из самых популярных примеров использования API, когда сайт, на котором хочет авторизоваться пользователь, запрашивает информацию о нем с другого сайта с помощью специально предоставленного для этого интерфейса. Другим популярным способом использования этой технологии является загрузка целых HTML-документов, содержащих данные и правила для их отображения. В некоторых случаях их формат не подходит по определенным причинам (неправильное отображение или несоответствие дизайну приложения). Именно с такой ситуацией обратился сайт туристического агентства, который использовал для поисковой выдачи API внешнего сайта, результаты которого абсолютно не вписывались в рамки современного дизайна.

Поэтому, для решения данной проблемы было предложено добавить промежуточную обработку данных, полученных от API, а именно – добавить механизм, который будет преобразовывать данные в DOM (от англ. *Document Object Model*) и изменять их в зависимости от наших потребностей.

В связи с тем, что проект был реализован на базе WP CMS, для осуществления такого парсинга использовался скриптовый язык PHP и технология AJAX, которая позволила сделать это динамически, не перезагружая страницу.

Структурой организации кода было выбрано ООП. Объектно-ориентированные программы просты для восприятия и мобильны, их просто модифицировать и поддерживать, в отличии от процедурного метода программирования, где при добавлении значительного количества функций код становится настолько сложным, что его сопровождение становится практически невозможным.

Логика реализованного функционала следующая:

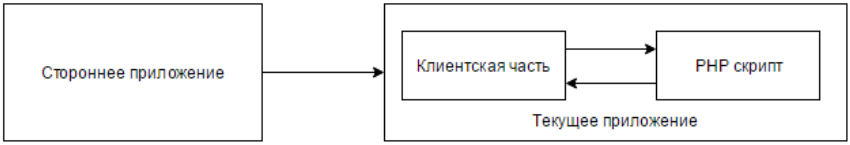



Рисунок 1 - Схема взаимодействия между приложениями

PHP скрипт (рис.1) выполняет:

1. Проверку являются ли полученные данные валидными.
2. Использует класс DOMDocument, который входит в стандартные возможности языка PHP, чтобы преобразовать данные с текстового представления в объектное.
3. Содержит два класса, первый из которых будет модифицировать DOM, а второй будет вызывать необходимые методы первого класса, передавая ему DOM-объект как параметр, в случае корректной отработки шагов 1-2.

Практическая ценность данного метода заключается в том, что довольно часто возникает потребность в динамическом изменении HTML-документов, а в результате работы такого алгоритма мы очистим структуру от ненужного текста и добавим свои стили, задающие вид, который нам необходим. К тому же выбранный подход позволяет легко модифицировать код для решения подобных задач в рамках других проектов.

**Литература**

1. API [Электронный ресурс] – Режим доступа к ресурсу: https://ru.wikipedia.org/wiki/API.
2. Mitchell L. J. PHP Web Services: APIs for the Modern Web / L. J. Mitchell - 2016
3. What is the Document Object Model? [Электронный ресурс] – Режим доступа к ресурсу: https://www.w3.org/TR/REC-DOM-Level-1/introduction.html
4. Professional WordPress: Design and Development/2nd Edition / B.Williams, D.Damstra, H.Stern - 2013
5. AJAX [Электронный ресурс] – Режим доступа к ресурсу: https://ru.wikipedia.org/wiki/AJAX
6. The DOMDocument class [Электронный ресурс] – Режим доступа к ресурсу: http://php.net/manual/en/class.domdocument.php

УДК 004.62

**Огляд систем веб-аналітики з відкритим програмним кодом**

Майоров Є.О., студент 3 курсу
Науковий керівник – Мелешко Є.В., к.т.н., доцент
*Центральноукраїнський національний технічний університет, м. Кропивницький*

Система веб-аналітики – система, яка збирає і аналізує діяльність користувачів веб-сайтів з подальшою інтерпретацією у вигляді звітів, таблиць, діаграм, і т.д.

Використання систем веб-аналітики з відкритим кодом має свої переваги:

- Можлива кастомізація системи під окремі випадки користування.
- Не використовуються програмні модулі третіх сторін або партнерів.

Прикладами таких систем є наступні: AWStats, Graylog, Open Web Analytics, Piwik.

**AWStats**

Була розроблена у 2003 році Laurent Destailleur. Особливостями AWStats є наступні:

- Написана на мові програмування Perl.
- Формує звіт про стан кластерів сервера для збалансованого співвідношення навантаження на сервер.
- Працює з командного рядка і з браузера, як CGI (з динамічними фільтрами для деяких діаграм).

**Graylog**

Була розроблена у 2006 року Graylog, Inc. Особливостями Graylog є наступні:

- Здатна оброблювати різні джерела інформації (сторінки сайтів, таблиці) для формування звітів в лог-файлах.
- Здатна взаємодіяти з різними сторонніми лог-збирачами (такими як fluentd або nxlog).
- Має власну систему повідомлень та тригерів для миттєвого реагування на різні події, такі як, наприклад, невдалі спроби входу в систему, зниження продуктивності сервера, його вимкнення.
- Має можливість розширити доступ для цілої команди адміністраторів до файлів конфігурації і логів без навантаження на сервери Graylog.
- Для спрощення управління правами доступу, має можливість групування користувачів для надання особливих функцій, наприклад, перегляду лог-файлів.

**Open Web Analytics**

Була розроблена у 2006 році Peter Adams. Особливостями Open Web Analytics **(**OWA**)** є наступні:

- Надає можливість запитувати і працювати з даними за допомогою Data Access REST API, ззовні OWA.
- Модульна архітектура OWA сприяє легкій розробці власних модулів.
- OWA має інтерфейс командного рядка (CLI), який дозволяє адміністраторам виконувати певні команди з оболонки сервера, а не через Інтернет.
- Має два види обробки подій – синхронний та асинхронний.

**Piwik**

Була розроблена у 2008 році Piwik Analytics. Особливостями Piwik є наступні:

- Розвинена інтеграція з великою кількістю програмних продуктів, від кроссплатформових клієнтних API для більшості платформ і SDK для фреймворків до систем управління контентом (Wordpress, Joomla, Drupal, ModX, Magento).
- Android SDK, IOS SDK.
- Оновлення бази даних в режимі реального часу.
- Розширена геолокація: місцезнаходження користувачів за IP-адресами відображаються на інтерактивній карті в режимі реального часу.
- Дозволяє з'єднати воєдино дані заданого користувача, зібрані з декількох пристроїв і декількох браузерів в єдиний ідентифікатор користувача.
- Підтримує роботу з серверами через проксі, з IPv6, з Intranet-системами.
- Має власні cookies (зазвичай, лише вони і використовуються) і підтримує cookies третіх сторін. Є можливість взагалі їх відключити.
- Є можливість анонімізувати IP-адреси користувачів.
- Є підтримка DoNotTrack за замовчуванням.

**Висновки**

Аналізуючи системи веб-аналітики з відкритим вихідним кодом можна їх розділити за сферами оптимального використання:

AWStats – для сайтів з невеликим набором функцій, які потребують базового аудиту діяльності користувачів.

Graylog – для сайтів з великою кількістю користувачів, але ще не потребують повноцінного аудиту.

Open Web Analytics – для сайтів з великим набором функцій, які вимагають розробки індивідуальних модулів аудиту.

Piwik – для сайтів з великим навантаженням і не менш великою кількістю користувачів.

УДК 004.056.53

# Алгоритми комп'ютерного аналізу текстів на природній мові

Мелешко Є.В., к.т.н., доцент
Науковий керівник – Смірнов О.А., д.т.н., професор
*Центральноукраїнський національний технічний університет, м. Кропивницький*

Комп'ютерний аналіз текстів використовується в багатьох інформаційних системах, наприклад, в пошукових роботах, пошуковій оптимізації, реферуванні текстів, системах питання-відповідь, машинному перекладі, представленні знань, експертних системах і т.д.

Типові задачі аналізу текстів: класифікація, кластеризація, автоматичне анотування, визначення ключових понять тощо.

Рівні подання лінгвістичної та екстралінгвістичної інформації [1]: 1) акустико-фонетичний рівень; 2) морфологічний рівень; 3) лексичний рівень; 4) синтаксичний рівень; 5) семантичний рівень. При обробці текстів зазвичай розглядаються 2-5 рівні обробки інформації.

**Алгоритми морфологічного аналізу** приводять кожне слово до нормальної форми та знаходять його морфологічні характеристики [2]. До них відносяться стемінг та лематизація [3]. Стемінг – ототожнення основи семантично схожих словоформ. Лематизація також здійснює ототожнення основ слів, але враховує при цьому частини мови, до яких відносяться словоформи, що підвищує точність ототожнення.

**Алгоритми лексичного аналізу** дозволяють розпізнавати лексичні одиниці тексту. Одним з фундаментальних алгоритмів лексичного аналізу є лексична декомпозиція, яка передбачає розбивку тексту на токени [3]. Токен – найчастіше слово, але може бути окремою морфемою або словосполученням. Для проведення стемінга слід спочатку розбити текст на токени; на основі списку токенів як правило виконується синтаксична декомпозиція.

**Алгоритми синтаксичного аналізу** здійснюють синтаксичну декомпозицію – розпізнавання речень на основі символів форматування тексту [3], та генерацію дерева синтаксичного виводу речень [2]. З цією метою використовуються парсери (синтаксичні аналізатори) – програми, що перетворюють вхідний текст в деревовидну структуру даних, яка відображає синтаксичну структуру вхідної послідовності.

**Алгоритми семантичного аналізу** виявляють взаємозв'язки між термінами в документах та взаємозв'язки між різними документами [2]. На рівні семантичного аналізу визначають ключові слова у тексті, зв'язки між ключовими словами, будують семантичні мережі та онтології [1, 2, 4].

Алгоритми семантичного аналізу розбирають синтаксичні дерева тексту за допомогою онтологічної бази знань та генерують семантичну

структуру речень [2]. Потім семантичні структури речень інтегруються в семантичний граф тексту.

На даному рівні вирішуються такі задачі як визначення тематики тексту, генерація реферату, смисловий переклад з однієї мови на іншу, підтримка діалогу з користувачем на природній мові тощо.

Однозначне визначення семантичної мережі на даний час відсутнє. В інженерії знань під нею мається на увазі граф, що відображає зміст цілісного образу. Вузли графа відповідають поняттям і об'єктам, а дуги – відносинам між об'єктами. Формально семантичну мережу можна задати в наступному вигляді:

$$H = <I, C, G>,$$

де I – множина понять; C – множина типів зв'язків між поняттями; G – відображення, що задає конкретні відносини з наявних типів C між елементами I.

Існує два типи семантичних мереж: однорідні мережі з асоціативними зв'язками та неоднорідні мережі, що містять зв'язки різних типів.

Об'єктами семантичної мережі можуть бути: сутності, властивості, дії, величини [4]. Можна виділити декілька часто використовуваних класів відносин в неоднорідних семантичних мережах: ієрархії, агрегації, функціональні, семіотичні, тотожності, кореляції [4].

Розробка алгоритмів комп'ютерного аналізу текстів передбачає співпрацю лінгвістів та програмістів. Перед комп'ютерною лінгвістикою стоять, перш за все, завдання лінгвістичного забезпечення процесів збору, накопичення, обробки та пошуку інформації. Центральними науковими проблемами комп'ютерної лінгвістики є проблема моделювання процесу розуміння змісту текстів і проблема генерації природної мови.

**Список літератури**

1. Харламов А. А. Когнитивный подход к смысловому анализу текстов // М.: Вестник МГЛУ. – 2013. – Вып. №13 (673). – С. 196-205

2. Марченко О.О. Алгоритми семантичного аналізу природномовних текстів : автореф. дис. на здобуття наук. ступеня канд. фіз.-мат. наук : спец. 01.05.01 "Теоретичні основи інформатики та кібернетики" / Марченко Олександр Олександрович. – Київ, 2005. – 13 с.

3. Яцко В. А. Алгоритмы и программы автоматической обработки текста // Иркутск: Вестник ИГЛУ. – 2012. – Вып. №1 (17). – С.150-160.

4. Найханова Л.В. Основные типы семантических отношений между терминами предметной области // Известия ВУЗов. Поволжский регион. Технические науки. 2008. №1. – С.62-71.

УДК 004.65

# Особливості обробки даних великих об'ємів (BigData) з використанням нереляційних баз даних

Охотний С.М., студент 3 курсу
Науковий керівник – Сидоренко В.В., старший викладач
*Центральноукраїнський національний технічний університет, м. Кропивницький*

З кожним роком кількість даних, що опрацьовуються комп'ютерами, постійно зростає. Для того, щоб справлятися зі зростаючими об'ємами інформації, були розроблені нові засоби її обробки, які узагальнюють терміном BigData.

*BigData* – набір методів та інструментів для опрацювання структурованих і неструктурованих даних величезних розмірів, що є ефективними в умовах безперервного приросту інформації та розподілення навантаження по багатьом вузлам обчислювальної мережі.

*Основні властивості BigData:*

–зберігання та обробка великої кількості даних;

–висока швидкість роботи;

–обробка даних різних форматів починаючи від структурованих даних, прийнятих у традиційних базах даних, до неструктурованих текстових документів, аудіо, відео, даних біржових зведень та фінансових операцій.

*Основні принципи BigData:*

1)горизонтальна розширюваність – при збільшенні об'єму даних збільшується кількість апаратних засобів обробки (в обчислювальну мережу можна легко додавати нові машини);

2)відмовостійкість – система продовжує працювати, якщо деякі машини обчислювальної мережі виходять з ладу;

3)локальність даних – обробка даних повинна виконуватись по можливості в тому ж місці, де вони зберігаються, щоб уникнути витрат часу для передачі даних з одного сервера на інший.

Найрозповсюдженішим засобом для роботи з BigData є Apache Hadoop. Hadoop є фреймворком для зберігання, обробки та аналізу даних у великих масштабах і має повністю відкритий вихідний код. Він може працювати на загальнодоступному апаратному забезпеченні, що робить його простим у використанні в існуючих датацентрах, або навіть для проведення аналізу в хмарі.

Для роботи з великими об'ємами даних в Hadoop застосовують нереляційні (NoSQL – not only SQL) бази даних (БД), які забезпечують інші механізми зберігання та видобування даних. Особливості NoSQL баз даних:

–не використовується SQL;

– неструктуровані;
– слабкі ACID;
– розподіл даних по вузлам;
– NoSQL бази даних в переважній більшості мають відкритий вихідний код.

Усі NoSQL БД розділяються в залежності від способу зберігання та обробки даних:
– сховища типу «ключ-значення»;
– розширювані розподілені сховища;
– графові бази даних;
– документно-орієнтовані сховища.

За замовчуванням в Hadoop використовується HBase – колонково-орієнтована, розширювана NoSQL база даних. Дані організовані в таблиці, проіндексовані первинним ключем, який в HBase має назву RowKey. Для кожного RowKey зберігається необмежений набір атрибутів (або колонок). Колонки організовані в групи колонок і мають назву ColumnFamily. Для кожного атрибуту може зберігатися декілька різних версій. Різні версії мають різний timestamp (часова мітка). Усі записи зберігаються у відсортованому по RowKey порядку.

Схожою на HBase є Apache Cassandra – колонково-орієнтована, розширювана розподілена система керування базами даних (РСКБД), розрахована на створення високомасштабованих і надійних сховищ величезних масивів даних, представлених у вигляді хеша. Вона може використовуватися як з Hadoop так і самостійно. Cassandra має свою мову структурованих запитів CQL, яка дещо нагадує SQL. Cassandra є доцільним вибором у наступних умовах:
– швидке зчитування і запис даних (нині Cassandra є найшвидшою РСКБД);
– додавання нових машин, якщо необхідно більше потужності;
– надійна реплікація даних між датацентрами.

*Реплікація* – одна з технік масштабування баз даних (як реляційних так і NoSQL), яка, за рахунок постійного копіювання даних, значно зменшує ймовірність втрати даних.

З Hadoop можна використовувати інші NoSQL бази даних. Для роботи з великими об'ємами даних можна використати й інші засоби. Вибір тої чи іншої технології залежить від результатів проведеного аналізу поставленої задачі.

**Список літератури**

1. Big Data от А до Я. Часть 1 [Електронний ресурс] – Режим доступу до ресурсу: https://habrahabr.ru/company/dca/blog/267361/.
2. NoSQL базы данных: понимаем суть [Електронний ресурс] – Режим доступу до ресурсу: https://habrahabr.ru/post/152477/.

УДК 004.6

# Збирання даних про користувачів віртуальної соціальної мережі за допомогою web-кроулера

Охотний С.М., студент 3 курсу,
Мелешко Є.В., канд. техн. наук, доцент
*Центральноукраїнський національний технічний університет, м. Кропивницький*

На сьогоднішній день соціальні мережі стали основою спілкування людей і відіграють ключову роль в інформаційній глобалізації суспільства. Соціальні мережі активно використовуються для розповсюдження реклами та маніпулювання свідомістю громадськості. Тому важливим питанням сучасності є захист людей від впливу негативної та шкідливої інформації, яка може нашкодити їхньому життю.

Соціальну мережу можна представити у вигляді графу, кожна вершина якого є її користувачем, а ребро – зв'язком між користувачами. Нині найбільшою соціальною мережею є Facebook, який має 1,7 млрд. користувачів, серед яких 5,4 млн. українців. Завантажити інформацію про користувачів соціальної мережі можна двома шляхами: використовуючи API, яке надається розробниками, або аналізуючи html-сторінки сайту мережі. За останній час багато соціальних мереж закрили можливість вільно збирати інформацію про користувачів (або ускладнили її), надаючи засоби в основному для розробки додатків. Крім того розробник стає залежним від змін в API соціальної мережі. При аналізі html-сторінок така залежність відпадає, але потрібно пам'ятати про розмітку сайтів, яка може змінюватися, а це у свою чергу вимагає постійної перевірки і внесення змін в розроблені для цього парсери html-сторінок. Слід зазначити, що можливість внесення змін розробниками сайту в html-розмітку можна попередньо закласти в архітектуру розроблюваного ПЗ, щоб зменшити та полегшити правки, які треба буде вносити у такому випадку. При аналізі html-сторінок не є практичним намагання отримати граф усієї соціальної мережі, адже для цього знадобиться завантажити близько 300 ТБ даних і обробити їх.

Для збору інформації з веб-сторінок використовують спеціалізоване ПЗ, яке можна узагальнити під термінами веб-кроулер, пошуковий робот або павук. Його застосовують для обходу сторінок Інтернету з метою збору необхідної інформації. Павуки є найважливішим елементом будь-якої пошукової Інтернет системи. Вони здійснюють загальний пошук інформації в Інтернеті, повідомляють про зміст знайденого документа, індексують його і добувають підсумкові дані. Вони також переглядають заголовки, деякі посилання і відправляють проіндексовану інформацію до бази даних пошукового механізму.

Найпростішим алгоритмом збирання даних з соціальної мережі є алгоритм Breadth-first-search (BFS), який відомий як пошук у ширину в графі. Алгоритм розпочинає роботу з стартової вершини, знаходить перших сусідів цієї вершини і поміщає їх у чергу з типом організації даних (First In, First Out) FIFO. Вершини черги відвідуються в порядку появи. BFS дає можливість обходити граф по рівням, а також можливість задати необхідну їх кількість, таким чином контролюючи глибину обходу.

Архітектура BFS-кроулера соціальної мережі базується на агенті, який завантажує дані про користувача з його веб-сторінки, та черги FIFO. Він розпочинає свою роботу з ідентифікатора стартового користувача, витягуючи необхідну інформацію про нього, і отримує список ідентифікаторів його друзів. Список ідентифікаторів поступово додається до черги FIFO. Після чого з неї вибирається наступний користувач і його друзі знову додаються в чергу. При використанні BFS-кроулера соціальної мережі важливим є рівень глибини обходу, оскільки черга заповнюється на порядок швидше, ніж вивільняється, а отже необхідні значні обсяги оперативної пам'яті (від 16 Гб). Беручи до уваги теорію «шести рукостискань» (яка говорить про те, що будь-які дві людини на Землі розділені між собою не більше ніж шістьма рівнями зв'язків) для обходу усіх користувачів соціальної мережі (за умови, якщо вони не входять до замкнутих кіл) вистачить п'яти або шести рівнів глибини обходу.

Завантажену веб-кроулером інформацію про користувачів та їх зв'язки необхідно зберігати в БД, для їх подальшого аналізу. Оскільки природною репрезентацією соціальної мережі є граф – доцільно використати графову систему керування базами даних (ГСКБД), яка має графову модель збереження та обробки даних. Такою є NoSQL (NotonlySQL) ГСКБД Neo4j. На даний момент це найпоширеніша ГСКБД з відкритим програмним кодом, реалізована на Java американською компанією Neo Technology (розробка ведеться з 2003 року). Neo4j не вимагає розміщення всіх даних в оперативній пам'яті, що дозволяє її використовувати для обробки значних за розміром графів. Крім того Neo4j у повній мірі підтримує ACID (Atomicity, Consistency, Isolation, Durability – властивості, що гарантують надійну роботу транзакцій бази даних – атомарність, узгодженість, ізольованість, довговічність). Neo4j має свою орієнтовану на роботу з графами декларативну мову запитів Cypher. Запити до БД також можна виконувати використовуючи JavaAPIабо мову Gremlin.

При інсталяції Neo4j вказується робоча директорія, в якій розміщуватимуться бази даних. Neo4j спроектована працювати лише з однією базою даних. Щоб переключитися на інший граф необхідно зупинити сервер Neo4j перемкнути БД і знову запустити його.

Для створення нового вузла необхідно виконати такий запит:

```
CREATE (root:Person {name:"Bob"})
RETURN root
```

Якщо потрібно створити нові вузли із зв'язками можна виконати наступний запит:

```
MATCH (root:Person {name:"Bob"})
FOREACH (name in ["Leonardo", "Raphael", "Michelangelo",
"Donatello","Splinter"] |
CREATE (root)-[:FRIEND]->(:Person {name:name}))
```

Додавання нових зв'язків між вже створеними вузлами (результат виконання запитів див. на рис. 1):

```
MATCH (sensei:Person {name:"Splinter"}),
(ninja:Person)
WHERE ninja.name in ["Leonardo", "Raphael",
"Michelangelo", "Donatello"]
MERGE (ninja)-[:FOLLOWER]->(sensei)
```

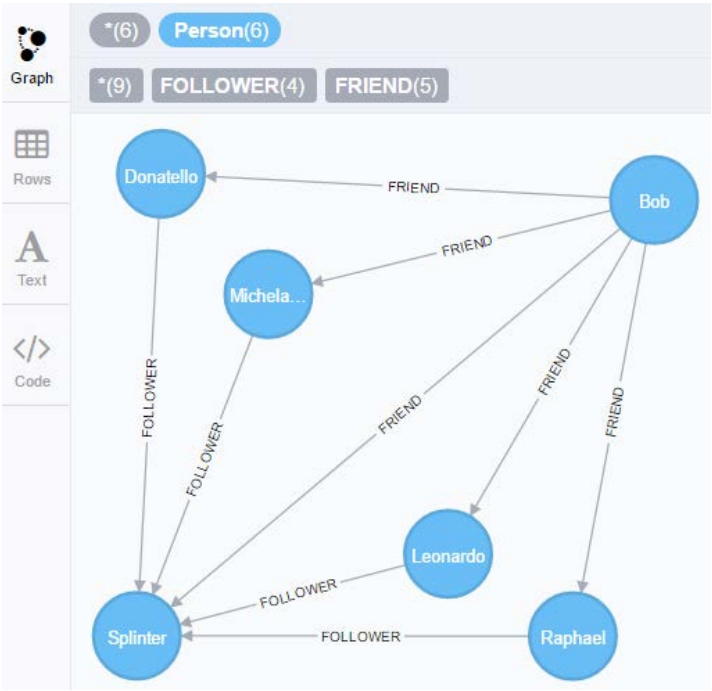



Рисунок 1 – Результати виконання запитів

Інтерфейс програмування додатків для Neo4j реалізовано для багатьох мов програмування, включаючи Java, .Net, Python, Clojure, Ruby, PHP. На великих об'ємах даних Neo4j працює набагато швидше, ніж реляційні БД і є зручною у використанні, тому вона ідеально підходить для побудови системи аналізу соціальних мереж.

УДК 519.83

**Дослідження методів розв'язання ігор-головоломок типу «Flip-Flop»**

Пархоменко Ю.М., к.т.н., доцент,
Бокій А.Р. студент 1 курса
*Центральноукраїнський національний технічний університет, м. Кропивницький*

Гра, як один з різновидів розумового людського спілкування, з'явилася ще у глибоку давнину, наприклад, шахи та шашки. Зі зростанням рівня освіти характер ігор ускладнюється, а коло їх любителів зростає. Поступово гра стає не лише елементом змагання, але і об'єктом наукового дослідження. На рубежі XIX і XX століть зародилася теорія ігор, яка безперервно розвивається і застосовується в економіці, соціології, біології, техніці, кібернетиці, військовій стратегії та інших галузях людської діяльності. Моделюються ігрові ситуації, аналізується поведінка гравців, розробляються математичні методи прийняття оптимальних рішень.

Нашу увагу привернула гра-головоломка «Flip-Flop», яка представлена в Інтернет-мережі в різних варіаціях дизайнерського та програмного виконання. Сутність гри полягає в наступному. На початку гри комірки матриці 4×4 заповнюються генератором випадкових чисел кодами «0» і «1». При активації довільної комірки матриці програма змінює вміст усього рядка та стовпчика, які знаходяться на перехресті активованої комірки, на протилежні коди, тобто «0» на «1» і навпаки. Задача гравця полягає в тому, щоб в результаті кінцевої послідовності кроків усі комірки матриці були заповнені «нулями» або «одиницями», в залежності від заданої мети.

Огляд існуючих методів дослідження: теорії ігор [1, 2]; дискретної математики [3]; штучного інтелекту [4]; комбінаторики [5] та подібних ігор-головоломок на сайті **Ігри розуму: braingames.ru** показав, що при визначенні алгоритмів виконання послідовності дій у грі «Flip-Flop», необхідно застосовувати методи моделювання ситуацій, логічного аналізу та комбінаторики.

Було виконано пошук оптимальних алгоритмів, які б базувалися на визначенні жорсткої послідовності дій. В результаті було досліджено алгоритми розв'язання гри головоломки «Flip-Flop» за виділеною ознакою, метод «струмка» та метод «змійка».

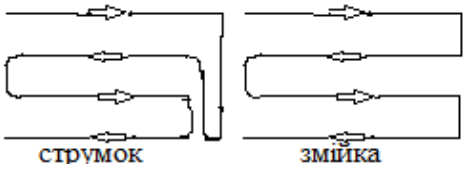



Рисунок 1 – Типи обходу комірок

В подальшому визначили декілька їх модифікацій та шляхи оптимізації.

**Висновки.** Результати дослідження показали, що застосування методу логічного аналізу кожної поточної комбінації в матрицях 4×4 і вище з метою прийняття оптимального рішення при визначенні наступного кроку є процесом складним і неефективним.

Для розв'язання подібних задач необхідно знаходити нестандартні рішення такі як, наприклад: метод виділення характерних ознак і розробки на цій основі алгоритму виконання послідовних дій; метод виділення комірок з кодом «1» або «0» з правилом їх нумерації на вхідній матриці і розробки на цій основі правил виконання послідовності дій (методи «струмка» та «змійки»). Для оптимізації кількості кроків, при застосуванні вказаних алгоритмів, необхідно аналізувати поточні комбінації і своєчасно вмішуватися в процес (при методі виділених ознак) або вміст вхідної матриці, з метою оптимізації кількості комірок з кодами «0» або «1» (при методі «змійки»).

**Список літератури**

1. Раскин М.А. Введение в теорию игр // Летняя школа «Современная математика». - Дубна, 2008.
2. Мазалов В.В. Математическая теория игр и приложения. — Санкт-Петербург - Москва - Краснодар: Лань, 2010. - 446 с.
3. Яблонский С.В. Введение в дискретную математику. – М.: Высш. шк., 2003. – 384 с.
4. Міщенко Н. Штучний інтелект-виклик часу //Науковий світ. - 2006. - № 10. - С. 12-13
5. Виленкин Н.Я. Популярная комбинаторика. - М.: Наука, 1975.

УДК 004.65

**Автоматизована інформаційна система обліку продажу товарів обчислювальної техніки**

Піхур Н.В., студент
Науковий керівник – Миронюк Т.В., старший викладач
*Черкаський Державний Технологічний Університет, м. Черкаси*

Автоматизовані інформаційні системи надають можливість оптимізувати і раціоналізувати функції управління. Автоматизація завжди допомагає досягти найбільшої керованості своєї фірми чи організації, відчувати зміни ринку і швидко на них реагувати. Застосування автоматизованих систем посилює функцію контролю правильності і доцільності записів, не підвищуючи трудомісткості ведення обліку.

Процес обліку є досить трудомістким і разом з тим небезпечним, тому що навіть одна помилка може стати причиною цілого ряду порушень, це відіб'ється на господарському процесі та інформації про фінансово-майновий стан підприємства. Тому питання спрощення та мінімізації ризику даного процесу є досить актуальним. Один з основних шляхів вирішення даної проблеми є автоматизація бухгалтерського обліку за допомогою сучасних інформаційних технологій.

Запропоновано інформаційну систему обліку продажу товарів обчислювальної техніки, яка спростить і покращить роботу підприємства, а також виконуватиме ряд функцій:

- облік витрат і розрахунок собівартості;
- облік обчислювальної техніки;
- управління складами підприємства;
- управління закупівлею та продажами обчислювальної техніки;
- формування товарних звітів про реалізацію обчислювальної техніки.

Інформаційна система обліку продажу обчислювальної техніки позбавить співробітників від рутинної повсякденної роботи по виписці прибуткових і видаткових накладних на підприємстві, забезпечить автоматизацію облікових операцій, дозволить значно скоротити час на створення інших первинних документів і вихідних звітностей. Результати виконання операцій реєструються у відповідних журналах. Автоматизація цих процесів дозволить зберігати інформацію в одній базі, а зручність введення інформації забезпечить зрозумілий інтерфейс.

Розроблювана інформаційна система реалізована на базі програмного продукту 1С версії 8.3. На рисунку 1 представлена структура системи обліку продажу обчислювальної техніки:

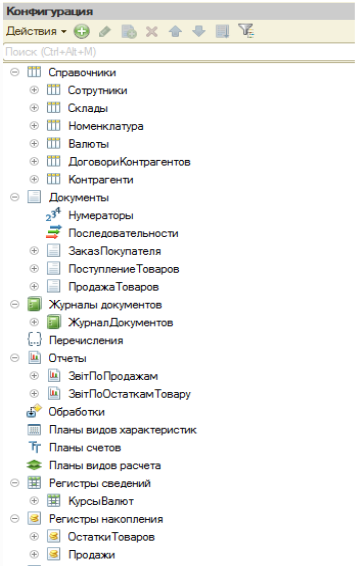



Рис. 1 – Структура автоматизованої інформаційної системи в режимі конфігуратор

Були розроблені наступні документи для ведення обліку закупки-продажу товарів, перелік яких приведено нижче:

- надходження товару. Цей документ надає можливість вносити інформацію про закупки та ввести облік по закупкам.
- замовлення покупців. Документ, що дозволяє вносити та переглядати інформацію про замовлення клієнта;
- продаж товарів. Документ, що використовується для ведення обліку продажу товарів.

Також в програмі розроблено наступного типу довідники: контрагенти, що містять інформацію про покупців та постачальників товару; номенклатура - для внесення і перегляду даних про товар, склади, договір контрагентів; працівники, що містить інформацію про працівників підприємства. Регістр відомостей (курси валют) створений для того, щоб користувачі мали змогу вносити та порівнювати курси валют. Для зручного перегляду інформації про операції на даному підприємстві в інформаційній системі використовуються регістри накопичення у вигляді звітів наступного типу:

- залишки товарів (для перегляду кількості товарів на складах);
- продажі (містить інформацію по операціях здійснених з товаром.)

Дана інформаційна система дозволить легко і ефективно контролювати а також удосконалювати діяльність підприємства.

УДК 004.92

# Влияние временных ограничений на процесс визуализации 3D-моделей

Пономаренко В.А. студент
*Национальный технический университет «Харьковский политехнический институт», г. Харьков*

Трехмерная графика – быстро развивающаяся область информационных технологий. С помощью 3D-графики создаются и обрабатываются графические изображения. Процесс получения трехмерного изображения на плоскости состоит из ряда определенных этапов. Одним из ключевых этапов генерации изображения является визуализация.

Визуализация – ресурсоемкий процесс, результат которого зависит от взаимодействия большого количества факторов. Основная сложность визуализации заключается в длительном времени рендеринга сцены и большом количестве разнообразных настроек. Главной задачей в процессе визуализации является оптимизация этих настроек и выбор соответствующего поставленным задачам алгоритма. Это позволит проводить большее количество времени в роботе над проектом, а не ожидать результат длительное время, которое по факту является простоем в работе.

Время визуализации, в первую очередь, зависит от производительности аппаратной части компьютера. Существуют специальные рендер-фермы, которые обладают огромным производительным потенциалом. Такие сервисы позволяют рендерить анимацию и тяжелые сцены в особо больших количествах, что является их главной задачей и несомненным плюсом.

Главным и существенным минусом этого подхода к визуализации является его стоимость, так как не каждый 3D-художник готов к таким финансовым затратам. Так же стоит отметить, что передача 3D-моделей третьим лицам влечет за собой определенные риски.

Вторым, но не менее важным фактором, является программная составляющая компьютера. Программная часть включает в себя колоссальное количество настроек, начиная от операционной системы и заканчивая настройками материалов и освещения в сцене. Несмотря на большое количество разных настроек визуализатора, ключевым параметром является выбор алгоритма для просчета глобального освещения, так как отскоки лучей света являются крайне ресурсоемкой частью визуализации. Также следует учесть, что глобальное освещение имеет два вида отскоков – первичные и вторичные (primary bounces,

secondary bounces), что, в свою очередь, влияет на результат и время просчета.

Для того чтобы сократить время рендеринга необходимо использовать конкретный алгоритм для решения соответствующих задач.

**Алгоритмы глобального освещения**

1. Brute force – базовый алгоритм, устанавливающий фиксированное количество вторичных лучей, отраженных от точки в сцене после попадания в нее первичного луча от источника света. Преимуществом данного алгоритма является сохранение мелких деталей, отсутствие дефекта мерцания в анимации. Недостатком является скорость просчета, так как отсутствует адаптивность.

2. Irradiance map – это адаптивный алгоритм просчета отскоков глобального освещения. Основная особенность его работы заключается в выявлении наиболее значимых детализированных зон визуализируемой сцены, вычислении в них глобального освещения и игнорировании менее важных зон, с последующим заполнением информации о глобальном освещении в них путем интерполяции информации из уже просчитанных важных зон. Это является достоинством, и одновременно недостатком алгоритма, так как могут быть проигнорированы важные мелкие детали.

3. Light cache – это алгоритм отображения глобального освещения в сцене. Light cache построен путем отслеживания многих лучей от камеры. Алгоритм не является адаптивным. Освещение вычисляется с фиксированным разрешением, которое определяется пользователем. Light cache имеет легкие и понятные настройки. Во многих случаях может быть использован для быстрого превью освещения в сцене.

**Выводы.** Из вышеперечисленного можно сделать вывод, что вариант с использованием рендер-ферм подходит для киноиндустрии, проектов с большим количеством визуализаций, а также для дедлайнов, где скорость визуализации имеет наибольший приоритет. В большинстве остальных ситуаций можно ограничиться возможностями личного компьютера.

Для оптимизации программной части необходимо уделить внимание алгоритмам глобального освещения. Лучшим вариантом для выбора primary bounces является алгоритм Irradiance map. Он адаптивен, что является главным плюсом и дает ускоренный результат. Если в сцене присутствует большое количество мелких деталей и артефакты, полученные при использовании Irradiance map, то следует воспользоваться алгоритмом Brute force. Он уберет погрешности, но время визуализации значительно увеличится.

Для secondary bounces лучше всего подходит алгоритм Light cache, так как Irradiance map, в силу специфики своего алгоритма, не может быть использован для вторичного отскока, а Brute force слишком ресурсоемок.

УДК 004.056.55

# Застосування експертних систем у сфері аудиту інформаційної безпеки

Попов І.С., магістрант
Науковий керівник – аспірант Хох В.Д.
*Центральноукраїнський національний технічний університет, м. Кропивницький*

В сучасному світі інформація набуває великого значення. Викрадення чи пошкодження інформації може призвести до серйозних наслідків (як мінімум до матеріальних втрат), тому актуальною є проблема її захисту. Використання експертних систем (ЕС) може значно спростити спеціалістам з захисту інформації їх завдання. Експертні системи широко застосовуються у багатьох галузях, в тому числі й інформаційній безпеці. Оскільки ЕС ефективніше працюють у більш вузьких напрямах, вони створюються для вирішення конкретних, спеціалізованих, задач.

Експертні системи забезпечують можливість проведення оцінки ефективності захисту інформації на передпроектній стадії створення систем захисту інформації шляхом проведення аудиту інформаційної безпеки для визначення відповідності інформаційних систем вимогам безпеки. Типове оцінювання ефективності захисту інформації включає: підготовку вхідних даних, проведення контролю реалізації вимог, розрахунок показників оцінки стану системи захисту інформації.

Системи, які включають функціонал для аналізу налаштувань фаєрвола, на додачу до своїх правил, повинні отримувати список доступу та опис топології мережі. Розпізнавання потоку дозволених даних є базовою проблемою в аналізі списку доступу. Тому для успішної роботи таким системам необхідно знати відповідь на наступні запитання:

- Які сервіси доступні на даному хості?
- Чи даний хост доступний з іншого джерела?
- Який вид трафіку дозволений?

На додачу, експертні системи можуть розпізнавати загальні проблеми конфігурації та помилки. Наприклад:

- Фаєрвол не блокує прямі передачі (пакети, призначені для іншої адреси з під'єднаної мережі).
- Недостатнє запобігання підміни адрес як для вхідних, так і вихідних пакетів.
- DNS-сервер досяжний лише через протокол UDP (зазвичай залишається непоміченим, оскільки працює в 99% випадків) [1].

Зазвичай, для експертних систем аудиту інформаційної безпеки вхідні дані фільтруються та перетворюються у зрозумілу для ЕС форму, а вже після цього система починає обробку даних. Прикладом обробки вихідних

даних може бути система AudES [2], в якій всі можливі порушення, які було виявлено, відображаються, зберігаються та очікують рішення аудитора. Разом з цими даними зберігається й уся необхідна інформація - команди, ресурси та, найголовніше, відповідні рекомендації рішень для аудитора, які він повинен прийняти відповідно до вказівок аудиту безпеки. Після завершення консультації, аудитор може отримати копію результатів. На додачу, кожна консультація записується в окремий файл, який пізніше може бути використаний для відтворення консультації чи перевірки минулих аудитів [3].

Застосування нечіткої логіки в таких ЕС дозволяє охарактеризувати нечітко визначені змінні, визначити зв`язок між змінними, що базуються на знаннях експертів та використовувати їх для обчислення результатів. Використання нечіткої логіки в ЕС достатнє для емуляції прийняття рішень експертом [4, 5].

Перевагами експертних систем є те, що рівень їх знань не знижується, може передаватись, відтворюватись та підвищуватись; зниження ймовірності виникнення людського фактору; вартість розробки компенсується низькою вартістю використання.

Недоліком експертних систем є те, що вони не надто добре пристосовані до навчання новим правилам і концепціям. Використання експертних систем у більшості випадків дозволяє відмовитись від висококваліфікованих експертів, але передбачає наявність спеціаліста більш низької кваліфікації.

Таким чином, експертні системи можна розглядати як інструмент для підвищення інтелектуальної потужності в даній предметній області.

**Список літератури**

1. Pasi E. An expert system for analyzing firewall rules / E. Pasi, Z. Jukka. // Helsinki University of Technology. – 2001. – №1. – С. 1–8.

2. Kanatov M. Expert systems for Information Security Management and Audit. Implementation phase issues / M. Kanatov, L. Lyazzat, B. Bagdat. // SCIS&ISIS. – 2014. – №14. – С. 896–900.

3. Tsudik G. AudES - an Expert System for Security Auditing / G. Tsudik, R. Summers. // IAAI Proceedings. – 1990. – №1. – С. 221–232.

4. Кущ С. Використання експертних та нечіткологічних систем для оцінки ризиків інформаційної безпеки інформаційно-телекомунікаційних систем / С. Кущ, В. Шутовський. // Вісник Національного технічного університету України. – 2012. – №50. – С. 114–120.

УДК 004.853

# Моделирование и управление траекториями обучения студентов в облачном сервисе

Прохоров А.В., к.т.н., доцент,
Шелехов С.М., магистрант
*Национальный аэрокосмический университет им. Н. Е. Жуковского «ХАИ»*

Концепция процессного управления Business Process Management (BPM) для вуза, приводит к рассмотрению бизнес-процессов его основных контуров, а именно, управления учебным процессом, научно-исследовательской деятельностью, финансовой и административно-хозяйственной деятельностью, как особых ресурсов, непрерывно адаптируемых к постоянным изменениям в соответствии с современными стандартами профессионального образования и требованиями рынка труда. На первый план выходят задачи моделирования бизнес-процессов с использованием формальных нотаций, использования программного обеспечения моделирования, симуляции, мониторинга и анализа бизнес-процессов. При этом сегодня акценты смещаются с обычного workflow в сторону эффективности бизнеса – прозрачности и измеряемости, а также с middleware-систем в сторону cloud-систем. Среди облачных сервисов, которые решают вопросы управления бизнес-процессами в организациях можно выделить IBM BlueWorks, ОС Corezoid и др.

В данной работе рассматриваются специфичные вопросы моделирования и автоматизации исполнения бизнес-процессов контура управления учебным процессом в вузе для мониторинга и контроля их исполнения всеми BPM-участниками – преподавателями, сотрудниками и студентами. Особая роль отводится формализации образовательных траекторий студентов в виде последовательности изучаемых дисциплин. Участники процесса смогут автоматически получать задачи в веб-интерфейсе системы, когда выполнение процесса будет доходить до соответствующего шага. В любой момент можно отследить, на какой стадии находится выполнение процесса, получать статусы задач в реальном времени, анализировать данные в процессе исполнения, автоматически формировать и просматривать сводные отчеты в любом разрезе, получать информацию об «узких местах» процесса для принятия мер. Действия, связанные с загрузкой или передачей информации выполняются при помощи API-запросов соответствующим информационным системам вуза.

Таким образом, вуз получает прозрачные бизнес-процессы и выделенные состояния, которые можно легко контролировать, анализировать и оптимизировать.

УДК 004.75

## Методи проектування гібридних систем доставки контенту

Сергєєв А.В., аспірант
Науковий керівник – Порєв Г.В., д.т.н., доцент
*Київський національний університет імені Тараса Шевченка, м. Київ*

Сучасні об'єми інформації, що циркулюють у комп'ютерних мережах призводять до навантаження з яким мережі з класичною, клієнт-серверною архітектурою, не завжди можуть впоратися. Основним чинником проблем у такому випадку є єдиний сервер, який є тонким місцем всієї мережі, так як у випадку його виходу з ладу, відмовляє вся система.

Вирішенням даних проблем може бути використання децентралізованих однорангових мереж (p2p) або систем доставки контенту (CDN – Content Delivery Network). Однорангові мережі працюють за принципом повної децентралізації, тобто кожен елемент мережі одночасно є як клієнтом, так і сервером. У той же час у основі систем доставки контенту лежить принцип віддзеркалення даних від основного до периферійних серверів, до яких і йдуть запити від кінцевих користувачів, при цьому запит до основного серверу йде тільки у тому випадку, якщо інформацію не було знайдено на локальних серверах. Найвідомішим представником систем доставки контенту можна вважати мережу Akamai [1]. Обидва підходи значно зменшують навантаження на сервери мережі, а отже підвищують надійність всієї системи.

Втім, кожна з цих мереж має і свої недоліки. У випадку значної географічної розосередженості між вузлами однорангової мережі, може з'явитися значна затримка у пошуку та доставці інформації. В той же час підтримка у актуальному стані серверів CDN потребує значних фінансових ресурсів, що можуть бути доступними не для всіх.

Можливим подоланням даних проблем є створення гібридної системи доставки контенту – мережі, що архітектурно поєднує CDN та p2p. На цей момент існує два методи побудови гібридних систем доставки контенту [2]:

1. Система, у якій основну роль відіграє саме класична CDN, при цьому ресурси однорангової мережі застосовуються тільки за необхідності.
2. Зворотній варіант, при якому основні ресурси надаються одноранговою мережею, а CDN-сервери виконують роль резерву.

Наразі існує лише декілька спроб реалізації гібридних систем доставки контенту, причому всі вони належать до другого типу. Єдиною ж спробою практичної реалізації системи на даний момент залишається CoralCDN [3],

яка успішно функціонувала у період 2004 - 2012 рр., але не змогла конкурувати з іншими типами мереж через деякі недоліки.

У основі CoralCDN лежить однорангова мережа побудована із застосуванням розподіленої хеш-таблиці (DHT – Distributed Hash Table)під назвою Kademlia [4].

Розподілені хеш-таблиці працюють за принципом асоціативного масиву, тобто інформація знаходиться за певним ключем, який у даному випадку, частіше за все, являє собою результат певної хеш-функції від назви шуканого файлу. Основними перевагами таких систем є масштабованість (тобто ефективність функціонування мережі не залежить від кількості елементів в ній) та відмовостійкість (мережа буде надійною у процесі динамічного вибування елементів та підключення нових). Найвідомішим представником реалізованих розподілених хеш-таблиць є BitTorrent.

Для кінцевого користувача робота з CoralCDN полягала у приєднанні до URLсайту суфікс nyud.net. Це означало, що даний сайт кешувався мережею і його контент починав розподілятися у її інфраструктурі.

Головним недоліком [5], через який мережа не витримала конкуренції з іншими архітектурними рішеннями є значна кількість втрачених мережевих пакетів у випадку різкого збільшення навантаження на мережу.

**Висновки.** Підсумовуючі слід зазначити, що не дивлячись на те, що розробка гібридної системи доставки контенту може вирішити великий спектр проблем, питання стосовно її реалізації залишається відкритим і потребує подальших наукових досліджень.

**Список літератури**

1. E. Nygren, R.K. Sitaraman, and J. Sun. The Akamai Network: A platform for high-performance Internet applications. ACM SIGOPS Operating Systems Review, 44(3):2–19, 2010.

2. Евсеева, О. Ю. Математическая модель управления ресурсами гибридной сети доставки контента с гарантированным качеством обслуживания / О. Ю. Евсеева, М. Б. Кадер // Радиотехника : Всеукр. межвед. науч.-техн. сб. – Харьков, 2013. – Вып. 175. – С. 170 – 177.

3. M. J. Freedman, E. Freudenthal, and D. Mazieres. Democratizing content ` publication with Coral. In NSDI, Mar. 2004.

4. Maymounkov P. Kademlia: A Peer-to-Peer Information System Based on the XOR Metric / Maymounkov P., Mazieres D. // IPTPS 2002, 7-8 March 2002 р.

5. P. Sun, M. Yu, M. J. Freedman, and J. Rexford. Identifying Performance Bottlenecks in CDNs through TCP-Level Monitoring. In SIGCOMM Workshop on Meas. Up the Stack, August 2011.

УДК 004.92

# Ігровий 2D фреймворк для Android: Canvas та Open GL ES

Старкіна О.Д., студентка 2 курсу
Науковий керівник – Мелешко Є.В., к.т.н., доцент
*Центральноукраїнський національний технічний університет, м. Кропивницький*

**Ігровий фреймворк –** основа для створення гри, містить у собі модулі графіки, звуку, користувацького вводу та ін. Містить один або декілька інтерфейсів, кожен з яких містить хоча б одну реалізацію.

**Canvas –** спеціальний клас для роботи з графікою, що дозволяє створювати анімацію та малювати складні зображення.

**Open GL ES (OpenGL** for **E**mbedded **S**ystems – OpenGL для вбудованих систем) **–** Open Graphics Library бібліотека з відкритим вихідним кодом для роботи з 2D та 3D графікою.

**Малювання графіки**

Canvas працює як спеціальний інтерфейс, що символізує поверхню, на якій можна малювати. За допомогою Canvas малювання відбувається на растровому зображенні (Bitmap), яке потім розміщується на екрані.

У ігрових програмах Canvas використовується разом з SurfaceView.

SurfaceView – спеціальний підклас View, який надає поверхню для малювання в ієрархії View. Ціль у тому, щоб надати цю поверхню іншому потокові та зменшити витрати часу на очікування готовності ієрархії View до малювання. Замість цього інший потік, який має посилання на SurfaceView, може малювати на своєму Canvas та у власному темпі.

Для роботи слід створити екземпляр класу SurfaceView та імплементувати SurfaceHolder. Callback, описати клас Thread, де буде відбуватися процес малювання.

При використанні Open GL ES слід розуміти як працювати з двома основними класами: GLSurfaceView та GLSurfaceView.Renderer.

GLSurfaceView – це View де можна малювати об'єкти та управляти ними, схожий на SurfaceView.

GLSurfaceView.Renderer – інтерфейс, що визначає методи для малювання у GLSurfaceView. Для роботи треба реалізувати даний інтерфейс та приєднати його до екземпляру GLSurfaceView, використовуючи GLSurfaceView.setRenderer().

**Застосування**

Canvas підходить для створення простих ігор, невибагливих до швидкості малювання графіки, Open GL ES чудово підходить для роботи із складною графікою, забезпечуючи оптимальну швидкість.

В рамках Global Game Jam 2017 автором була розроблена гра для пристроїв з ОС Android на базі рушія створеного власноруч.

Рушій складається з кількох модулів:

- Графічного.
- Звукового.
- Користувацького вводу (данні з датчиків пристрою).

Оскільки час на Global Game Jam обмежений та гра не потребувала великої кількості ресурсів, графічна частина рушія створена з використанням Canvas.

Графічний модуль складається з простої ієрархії моделей, що є представленнями об'єктів малювання та сцени (рис. 1), опису потоку малювання та View для відображення.

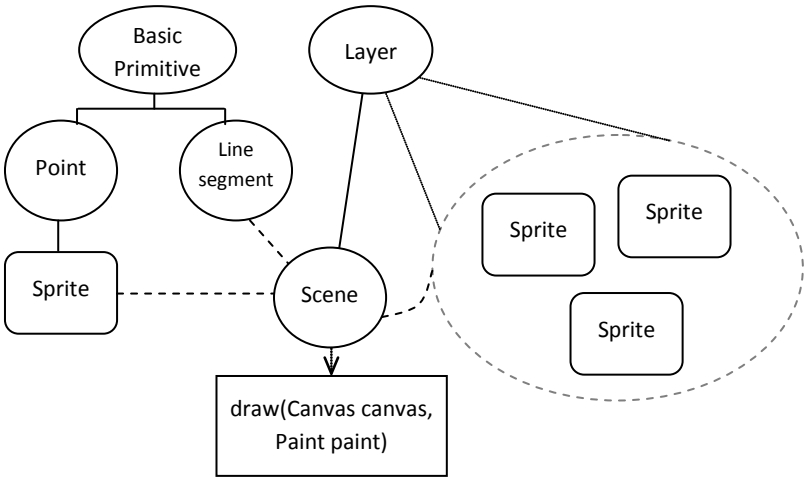



Рис. 1 – Ієрархія моделей та представлення ігрової сцени

Малювання ігрової сцени влаштоване наступним чином: сцена промальовується шар за шаром, об'єкт за об'єктом. Усі об'єкти наслідуються від базового примітиву і перевизначають його абстрактний метод onDraw, прототип якого передбачає малювання за допомогою Canvas.

Такий метод дуже простий, але наочний і якнайкраще підходить для вивчення та опанування програмування ігрового фреймворку для Android, але представлений рушій (його графічну частину) можна переписати за допомогою Open GL ES.

**Список літератури**

1. Ди Марцио Д. Разработка игр под Android. – СПб.: Питер, 2014. – 224 с.
2. Цехнер М. Программирование игрпод Android. – СПб: Питер, 2013. – 688 с.

УДК 621.391

**Анализ сценариев оркестровки сервисов в облачных технологиях**

Ткачева Е.Б., к.т.н., доцент
*Харьковский национальный университет радиоэлектроники, г. Харьков*
Мухи-Алдин Х.М., аспирант
*Одесский национальный политехнический университет, г. Одесса*

Переход к облачным технологиям хранения и обработки данных позволяет существенно упростить процессы предоставления и уменьшить стоимость сетевых сервисов [1, 2]. Однако стремительное увеличение объемов предоставляемых сервисов, их динамическая природа и гетерогенность ведут к необходимости постоянной модификации системы управления и мониторинга, в частности, оркестровки сервисов.

Согласно исследованию [3] определено 19 различных сценариев оркестровки сервисов, которые затрагивают все модели предоставления сервисов: программное обеспечение как сервис (SaaS), инфраструктура как сервис (IaaS), платформа как сервис (PaaS). В процессе оркестровки сервисов в облачной среде сталкивается с рядом трудностей. Возникающие проблемы в первую очередь связанны с разнородностью программного обеспечения и аппаратных ресурсов, сложностью их интеграции и взаимодействия.

Проблемы, возникающие в разных сервис-моделях, имеют существенные отличия. Анализ особенностей и проблем, возникающих в процессе предоставления сервисов в каждой из приведенных выше сервис моделей, позволил сформировать ряд рекомендаций к процессу оркестровки сервисов с целью повышения их эффективности.

IaaS подразумевает предоставление таких ресурсов и сервисов, как центры распределения, хранения и обработки данных, сеть и оборудование. Сервисы IaaS предоставляются посредством ряда технологий виртуализации оборудования Xen, Citrix, VMware и др. Основное внимание в процессе оркестровки сервисов IaaS уделяется CPU, объемам и типу выделяемой памяти.

Сценарий оркестровки IaaS включает следующие процессы:

- выбор оптимального типа ресурсов с учетом их местоположения (выбор, монтаж и запуск экземпляра сервиса);
- динамическое перераспределение ресурсов сети с учетом их стоимости и эффективности (мониторинг, обеспечение миграции и переконфигурации сетевых параметров);
- управление параллельными процессами и мониторинг возникновения «QoS перекрытия» ресурсов;
- обеспечение безопасности и конфиденциальности данных (поддержка процессов аутентификации и авторизации);

- хранение информации о сетевых ресурсах.

PaaS включает обширный набор программного обеспечения и приложений (веб-серверов, серверов базы данных, балансировка нагрузки, сервер авторизации и т.д.), отвечает за выбор типа виртуализации, языка и платформы для реализации сервиса (Java, .NET, PHP, Ruby и т.д.).

Сценарий оркестровки PaaS включает следующие процессы:

- выбор программного обеспечения и платформы предоставления сервисов;
- интеграция приложений и гармонизация их взаимодействия;
- комплексный мониторинг за состоянием приложений, включая проверку соответствия как программных, так и аппаратных ресурсов требованиям QoS (оценка масштабируемости, синхронизация и репликация данных);
- обеспечение безопасности приложений (шифрование/дешифрование данных, аутентификация и авторизация пользователей).

SaaS осуществляет бесшовную интеграцию и взаимодействие компонентов PaaS и IaaS с целью предоставления высококачественных услуг оконечным пользователям. Посредством SaaS обеспечивается предоставление таких услуг, как системы управления взаимодействия с клиентами, социальные сети и д.р.

Сценарий оркестровки SaaS включает следующие процессы:

- контроль и поддержка взаимодействия приложений;
- мониторинг и управление большими объемами данных;
- оптимизация сетевых ресурсов на уровне приложений с поддержкой гарантированного уровня QoS;
- обеспечение конфиденциальности и безопасности данных.

Ряд функций, принадлежащих разным сервис-моделям совпадает. QoS характеристики данных функций являются ключевыми в процессе оркестации.

**Список литературы**

1. Wang L. et al. Cloud Computing: Methodology, Systems, and Applications/ Wang L. – CRC Press, 2011. – 44 p.

2. Bauer E., Adams R. Reliability and availability of cloud computing / E. Bauer, R. Adams. – USA: Willey, 2012. – 345 p.

3. Open Data Center Alliance [Electronic resourse] – Available at: https://opendatacenteralliance.org/

УДК 004.942

# Ігровий рушій Unity як засіб демонстраційного моделювання динамічних фізичних явищ

Цвик С.О., студент 4 курсу,
Якименко М.С., к.ф.-м.н., доцент
*Центральноукраїнський національний технічний університет, м. Кропивницький*

Дослід – відтворення якого-небудь явища або спостереження за новим явищем у певних умовах з метою вивчення, дослідження. Демонстрація досліду – важлива частина навчання. Але є явища, які в силу своєї складності або відсутності необхідної матеріальної бази неможливо відтворити. В цьому випадку нам на виручку приходить комп'ютерне моделювання. Комп'ютерна модель розроблена на базі ігрового рушія може бути досить гнучкою, щоб можна було змінювати деякі вхідні дані, що робить її на порядок інтерактивнішою за будь-які відеоматеріали. Сучасні ігрові рушії, такі як Unity [1], забезпечують міжплатформенну підтримку, що дозволяє запустити розроблений додаток на широкому переліку пристроїв від звичайних ПК до телефонів під управлінням ОС Android.

На відміну від спеціалізованого програмного забезпечення для наукових досліджень ігрові рушії мають ряд переваг для демонстраційних та навчальних цілей, такі як краща інтерактивність, орієнтованість на візуальне представлення, вбудовані моделі багатьох процесів та явищ, можливість сумісної роботи над моделями та їх представленнями у візуальному середовищі декількома розробниками. Менша точність відтворення процесів реального світу в даному випадку не є суттєвим недоліком, більше того, це дозволяє пришвидшити обробку і забезпечити інтерактивну взаємодію.

Використання ігрових рушіїв із вбудованими моделями твердих тіл, гравітацією, системою зіткнень дозволяє спростити моделювання механічних систем твердих тіл, а також моделювання систем багатьох частинок в термодинаміці та статистичній фізиці. Такий підхід дозволяє полегшити засвоєння студентами окремих розділів, що традиційно є складними для вивчення. Так, використовуючи рушій TEALSim [2] у віртуальному середовищі проводиться, візуалізація та дослідження електричних та магнітних полів, закону електромагнітної індукції Фарадея.

У навчальному курсі [3] університету штату Огайо розглядається моделювання динаміки точок та твердих тіл, рух тіл Сонячної системи, динаміка деформівних тіл та гідродинаміка, а також питання обробки зіткнень із використання Unity. Як завершальний проект студентам

пропонується написання власних ігор із використанням законів фізики реального світу.

В даній роботі пропонується використання ігрового рушія Unity для демонстраційного моделювання процесів електропровідності напівпровідників та роботи напівпровідникових пристроїв. Для створення 3D-моделей об'єктів доцільно використовувати редактор Blender [4]. Спершу проводиться моделювання руху електронів провідності та дірок для чистого напівпровідника засобами ігрового рушія, використовуючи вбудовану модель зіткнень електронів, яку слід доповнити додатковими взаємодіями із атомами; при цьому ймовірність розриву ковалентних зв'язків слід описати окремим параметром, який має фізичний зміст внутрішньої енергії (термодинамічної температури). Окремо описуються граничні умови на межі напівпровідника.

Далі, вводячи в середовище атоми домішок із іншими умовами на можливу кількість електронів, отримуються напівпровідники p- та n-типів, поєднуючи які можна утворити моделі напівпровідникових діодів, біполярних та польових транзисторів.

Слід зауважити, що подібне моделювання має демонстраційний та якісний характер і не може використовуватися для будь-яких кількісних розрахунків, що випливає із грубого характеру моделі. Проте такі механістичні пояснення часто використовуються при наочних демонстраціях і можуть розглядатися як перший крок до більш строгого дослідження відповідних явищ засобами фізики твердого тіла із врахуванням хвильової природи мікрочастинок.

Крім демонстраційних застосувань використання Unity дозволяє модифікувати програму для створення віртуальних лабораторних робіт, інтерактивних довідників тощо.

**Список літератури**

1. Хокинг Дж. Unity в действии. Мультиплатформенная разработка на C# / Дж. Хокинг. СПб.: Питер, 2016. – 336 с.
2. Pirker J. Understanding Physical Concepts using an Immersive Virtual Learning Environment / J. Pirker, S. Berger, C. Gutl, J. Belcher, P.H. Bailey // Proceedings of the 2nd European Immersive Summit (Paris, 26-27 November 2012). – P. 183-191.
3. CSE 3541:Computer Game and Animation Techniques [Електронний ресурс]. – Режим доступу: http://web.cse.ohio-state.edu/~wang.3602/courses/cse3541-2015-spring/
4. Kent B.R. 3D Scientific Visualizationwith Blender / B.R. Kent. – San Rafael: Morgan&Claypool Publishers, 2015. – 91 p.

УДК 004.9

**Методи автоматичного аналізу настроїв в соціальних мережах**

Шингалов Д.В., аспірант; Тріщ О.В., аспірантка;
Минайленко Р.М., к.т.н., доцент
*Центральноукраїнський національний технічний університет, м. Кропивницький*

Аналіз настроїв користувачів віртуальних соціальних мереж, таких як Twitter або Facebook, відноситься до класу методів, заснованих на обчислювальній обробці, що використовується для ідентифікації, вилучення та характеристики суб'єктивної інформації, наприклад, думок, виражених в тій чи іншій частині тексту. Основна мета аналізу настроїв класифікувати ставлення автора до різних тем в позитивні, негативні або нейтральні категорії. Аналіз настроїв має безліч застосувань в різних галузях, включаючи бізнес-аналітику, політику, соціологію і т.д.

Основні два методи автоматичного аналізу настроїв – це метод на основі використання лексем (неконтрольований підхід) і метод, машинного навчання (контрольований підхід), які використовують спеціалізовані словники. При машинному навчанні застосовуються класифікатори на базі юніграмм або їх комбінацій (N-грам) в якості ознак. У лексемному методі основі лежать юніграмми, які знаходяться в словнику і мають відповідні бали поляності.

Перед застосуванням будь-якого з методів вилучення настрою, звичайною є практика попередньої обробки даних. Попередньо оброблені дані дозволяють забезпечити високу якість класифікації тексту і зменшити обчислювальну складність. Типова процедура попередньої обробки включає в себе наступні кроки:

- Розмітка за частинами мови. Цей процес дозволяє автоматично визначити кожне слово речення як частину мови.
- Зведення до кореня. Процедура відсікання суфіксів та закінчень від кореня. Розмірність слів зменшується, коли корінь схожих слів відображаються як одне слово.
- Видалення некорисних слів. Це слова, які несуть в собі сполучну функцію в реченнях, наприклад, прийменники, артиклі і т.д.
- Обробка заперечень. Заперечення відноситься до процесу перетворення настроїв тексту з позитивного на негативний або з негативного на позитивний, використовуючи спеціальні слова: "ні", "не" і т.д.
- Умовні оператори. Фрази на кшталт "але", "за винятком", "за винятком того, що", "за винятком для" взагалі можуть кардинально змінити полярність частини тексту, що іде слідом за ними.

- Токенізація в N-грами. Токенізація - це процес створення словнику зі слів тексту.

**Лексемно-орієнтований підхід** обчислює настрій заданого тексту в залежності від полярності слів або фрази в цьому тексті.

Методика розрахунку настрою [1] полягає у наступному: після попередньої обробки тексту, відбувається перевірка маркера кожного слова на його полярність в лексиконі. Якщо слово не знайдено у лексиконі, тоді його полярність вважається нульовою. Після призначення балів полярності W всім словам, що містяться у тексті, остаточна оцінка S настрою тексту розраховується діленням суми балів слів, які задають настрій тексту (крім нульових) на кількість m таких слів:

$$S = \frac{1}{m}\sum_{i=1}^{m} Wi$$

Усереднення балу дозволяє отримати значення балу настрою у діапазоні від -1 до 1, де 1 означає сильне позитивне почуття, -1 означає сильний негативний настрій і 0 означає, що текст є нейтральним. Якість класифікації багато в чому залежить від якості словника.

Словники можуть бути створені з використанням різних методів:

- Вручну побудовані словники [2] (простий, повільний метод);
- Словники з підготовлених даних.

**Метод машинного навчання для аналізу текстів** - це контрольований алгоритм, який аналізує дані, які раніше були помічені як позитивні, негативні або нейтральні.

У спрощеному вигляді, задача класифікації текстів може бути описана наступним чином – задано набір маркованих даних:

$$T_{data} = \{(t_1, L_1), \dots (T, n)\},$$

де кожен текст належить до набору даних T і мітка $L_i$ є попередньо встановленим класом всередині групи класів L, мета полягає в тому, щоб побудувати алгоритм навчання, який буде приймати в якості вхідних даних навчальний набір $T_{data}$ і створити модель, яка буде точно класифікувати немарковані тексти.

Найпопулярнішими алгоритмами навчання для класифікації текстів є метод опорних векторів [3], наївний класифікатор Бейєса [4], дерева прийняття рішень [5], метод максимальної ентропії.

Машинне навчання для класифікації текстів починається з аналізу навчальних даних за допомогою алгоритму класифікації. Тут атрибутом маркеру є клас настрою або класифікатор, представлений у вигляді правил класифікації. Тестові дані використовуються для оцінки точності правил класифікації. Якщо точність вважається прийнятною, то правила

можуть застосовуватися до класифікації нових кортежів даних. Точністю класифікатора для даного тестового набору є відсоток тестових наборів кортежів, які правильно класифіковані класифікатором, тому що клас – мітка кожного навчального кортежу забезпечує крок також відомий як «навчання з учителем». Настрій кожного слова з документа визначається за допомогою функції агрегації, загальний же настрій документа визначається різними алгоритмами.

Для цього найчастіше використовується наївний класифікатор Бейєса. Цей класифікатор передбачає, що вплив значення атрибута на даному класі не залежить від значень інших атрибутів. Це припущення називається класом умовної незалежності. Для підвищення якості класифікації застосовується метод максимальної ентропії. На відміну від наївного класифікатора Бейєса, він не припускає, що ознаки умовно незалежні одна від одної. Цей класифікатор засновано на принципі максимальної ентропії усіх моделей, які відповідають даним навчання.

Будь-який з методів автоматичної класифікації тексту не може дати беззаперечних результатів. Поліпшити результати автоматичного визначення тональності тексту можливо за допомогою використання декількох систем класифікації, застосуванням гібридних методів класифікації. Також важливу роль відіграє використання методів автоматичного виправлення орфографічних помилок, вдосконалення словників (для методів, заснованих на словниках) і навчальної вибірки (для методів машинного навчання).

**Список літератури**

1. Stone, P. J. and Hunt, E. B. (1963). A computer approach to content analysis: Studies using the general inquirer system. In Proceedings of the May 21-23, 1963, Spring Joint Computer Conference, AFIPS '63 (Spring), pages 241–256, New York, NY,USA. ACM.

2. Wiebe, J. (2000). Learning subjective adjectives from corpora. In Proceedings of the Seventeenth National Conference on Artificial Intelligence and Twelfth Conference on Innovative Applications of Artificial Intelligence, pages 735–740. AAAI Press.

3. Cortes, C. and Vapnik, V. (1995). Support-vector networks. In Machine Learning, volume 20, pages 273–297, Hingham, MA, USA. Kluwer Academic Publishers.

4. Narayanan, V., Arora, I., and Bhatia, A. (2013). Fast and accurate sentiment classification using an enhanced naive bayes model. In Yin, H., Tang, K., Gao, Y., Klawonn, F., Lee, M., Weise, T., Li, B., and Yao, X., editors, Intelligent Data Engineering and Automated Learning IDEAL 2013, volume 8206 of Lecture Notes in Computer Science, pages 194–201. Springer Berlin Heidelberg.

5. Mitchell, T. M. (1996). Machine Learning. McGrwa Hill, New York, New York, NY, USA.

УДК 004.043

# Автоматизація збору інформації для дослідження ключових слів з метою покращення роботи SEO-спеціаліста над ранжуванням сайту

Шуліка Я.П., студент
Науковий керівник – Константинова Л.В., викладач
*Центральноукраїнський національний технічний університет, м. Кропивницький*

Створення сайту це лише половина роботи в процесі успішного позиціонування компанії на просторах Інтернету. На будь-яку тематику в Інтернеті є сотні сайтів і для того, щоб користувач попав саме на сайт компанії, то цей сайт потрібно просувати – покращувати його рейтинг в пошукових системах, тобто покращувати ранжування. Просування сайту - комплекс заходів по забезпеченню сайту користувачами, які зацікавлені в придбанні товарів чи послуг, що є на сайті [1].

Основна задача покращення ранжування сайту – просунути сайт на першу сторінку пошукової видачі. Більшість людей задовольняється першою сторінкою пошукової видачі [2].

Ранжування відбувається за певними ключовими словами. Деякі ключові слова люди шукають частіше, ніж інші. Те наскільки часто люди шукають ключове слово називається частотністю. Якщо сайт ранжуватиметься за найчастотнішим ключовим словом, то він матиме більшу аудиторію [3].

Для цього спеціалісти з оптимізації у пошукових системах виконують такий тип робіт як дослідження ключових слів. Використовуючи різні сервіси, що збирають інформацію про те, які ключові запити і з якою частотністю шукають люди, спеціалісти отримують інформацію по ключовим словам, які відповідають темі сайту. Найбільше часу у цьому типі робіт витрачається на форматування та аналіз отриманої інформації. Отримавши велику кількість даних з різних сервісів у різних форматах потрібно скласти її єдиний файл для аналізу [4].

Аналіз доволі складний процес, що включає дуже велику кількість нюансів, яку навіть сучасний штучний інтелект не може враховувати, але зібрати всю інформацію в єдине місце набагато простіше.

При цьому є певні вимоги:

1) У зв’язку з тим що аналіз виконується у електронних таблицях, тому що вони надають найкраще представлення зібраних даних для аналізу, потрібно, щоб інформація легко експортувалася в електронні таблиці або була виконана в них.

2) Робота з програмою або таблицею повинна бути зручною для користувача та швидкою.

Для виконання цієї задачі була розроблена електронна таблиця, що

збирає дані з Інтернету та форматує їх для дослідження ключових слів. Після форматування дані готові до аналізу.

Тобто електронна таблиця, використовуючи стандартні формули має змогу:

1) Посилати url запити до Інтернету, та записувати вміст сторінки, тобто записувати html-код сторінок або працювати з прикладним програмним інтерфейсом веб-сервісів.

2) Обробляти великі об'єми інформації за допомогою формул з елементарною логікою.

Реалізація таких можливостей за допомогою програми коштувала б дорожче, тому що програмісту знадобилася б велика кількість часу, в той час як електронні таблиці можна використовувати набагато зручніше, ніж програму. Для доповнення програми знадобилося б втручання програміста, а доповнити таблицю зможе будь-який користувач.

Електронна таблиця, не використовуючи додаткового програмного коду, а використовуючи лише елементарні формули має можливість отримати інформацію з Інтернету у вигляді json-масиву, декодувати отримані масиви та, маючи велику кількість масивів у комірках, скласти їх у дуже зручну для аналізу форму. Тобто звичайна електронна таблиця може працювати навіть краще її програмного аналогу, обробляти API-запити та збирати велику кількість текстових даних.

За допомогою електронних таблиць можна легко оптимізувати виконання великої кількості складної роботи. А реалізація таблиць набагато вигідніша за реалізацію програм.

**Список літератури**

1. Бабаев А.Н., Раскрутка: секреты эффективного продвижения сайтов [текст] Бабаев А.Н., Евдокимов С.И., Штарев А.М. // Санкт-Петербург, 2013 г. – 347 с

2. CTR позиций в поисковой выдаче // Хабрахабр. 27/8/2007 [Електронний ресурс]. Режим доступу: https://habrahabr.ru/post/13551/

3. Ранжирование сайта. Внешние и внутренние факторы // PR.CY. 3/9/2016 [Електронний ресурс]. Режим доступу:http://pr-cy.ru/lib/seo/Ranzhirovanie-sayta-Vneshnie-i-vnutrennie-faktory

4. Подбор ключевых слов – руководство по SEO для начинающих // Блог ContentMonster. 6/2014 [Електронний ресурс]. Режим доступу: http://blog.contentmonster.ru/2014/06/seo-guide-5/

УДК 004.042

## Програми-імітатори для мультимедійних систем навчання

Якубенко Я.І., учень 10 класу НВО СЗНЗ «Гармонія»
Науковий керівник – Дрєєв О.М., к.т.н.
*Мала академія наук учнівської молоді, м. Кропивницький*

Сучасні технічні засоби навчання надають значні переваги щодо якості подання знань. Але в більшості випадків викладачі обмежуються статичними слайдами або звичним відео, що для засобів мультимедіа є неповноцінним і не унікальним використанням. В роботі пропонується використання програмного забезпечення для спрощеної імітації роботи цифрових систем, фізичних та інших явищ. Імітація дозволить в процесі викладання не лише спостерігати за роботою пристроїв, але й втручатися в їх роботу. Така демонстрація є дійсно інтерактивною, це значно підвищує якість подання інформації і оправдовує використання засобів мультимедіа, бо інтерактивну систему іншими засобами реалізувати значно важче.

В роботі запропоновано програмне забезпечення імітації роботи гіпотетичного процесору (див. рисунок 1).

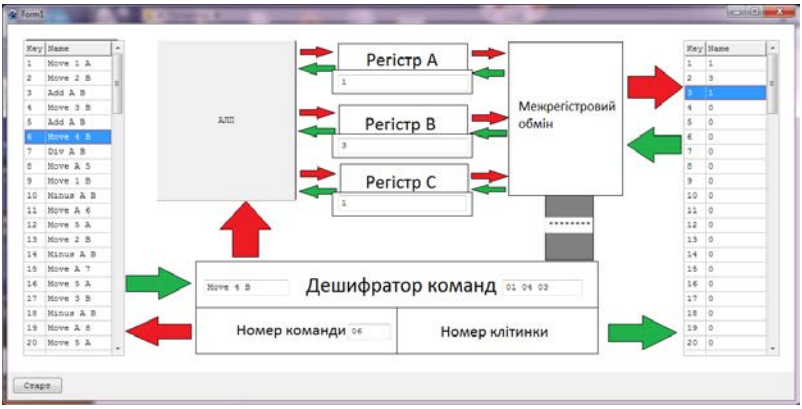



Рисунок 1 – Програма-імітатор роботи процесора

Програма містить таблиці послідовності команд та оперативної пам’яті даних, де є заготовлені користувачем початкові дані та програма для обробки цих даних. Також під час виконання програмного коду програма демонструє послідовність обробки кожної з команд та пересування даних.

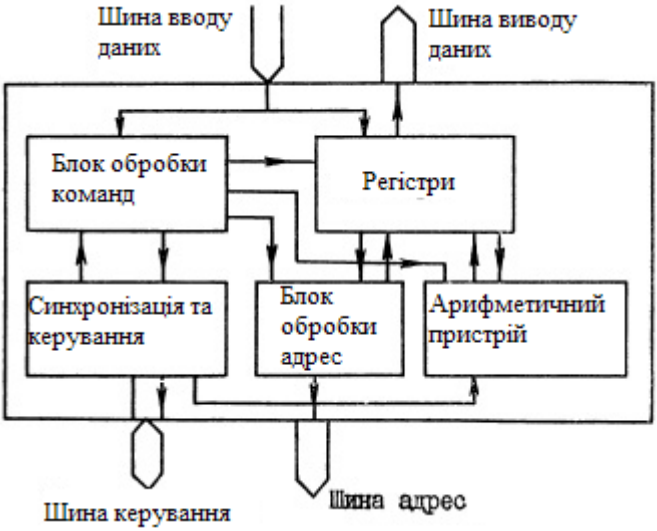



Рисунок 2 – Узагальнена структура процесора

Як видно з рис. 2, програма в своєму вигляді повторює узагальнену структуру центрального процесора. Цей факт дозволяє більш легко пов'язати дії програми та теоретичні відомості отримані на лекціях. Тому у програми передбачено можливість переробки для створення інтерпретатора власного набору команд. Така переробка, в якості індивідуального завдання, значно покращить розуміння процесів, які проходять при виконанні команд процесором.

**Список літератури**

1. Балашов Е. П., Григорьев В. Л., Петров Г. А. Микро- и миниЭВМ. Л.: Энергоатомиздат, 1984. 376 с.

2. Микропроцессоры: В 3-х кн. / Под ред. Преснухина. М.: Высшая шко-ла, 1986. Кн.1. 495 с. Кн. 2. 383 с. Кн. 3. 351 с.

3. Леонтьев В.П. Новейшая энциклопедия персонального компьютера 2005. – М.: ОЛМА-ПРЕСС Образование, 2005. - 800с.

UDC 004.056.55

## Application of machine learning methods for malware detection problems

Chumachenko K.I.[1], student,
Chumachenko D.I.[2], Teaching Assistant
[1]*Kharkiv National University of Radioelectronics, Kharkiv*
[2]*National Aerospace University "Kharkiv Aviation Intstitute", Kharkiv*

The obfuscation methods used in malicious software are developing rapidly and common detection methods are not able to detect polymorphic and zero-day malware anymore. Polymorphic malware is able to propagate while changing its attributes and therefore signatures, while for zero-day malware signatures are not created yet. This problem defines the need for new detection methods, that would be based on the actual behavior of the malware, e.g. machine learning based methods.

This study was aimed towards finding the most accurate machine learning method that would result in the best accuracy for both the binary classification problem, where classification is done into benign and malicious classes; and for the multiclass classification, where the goal is to find the appropriate malware family, to which the item belongs.

In this research, a total of 1150 malicious files were used. They were of families Dridex, Locky, TeslaCrypt, Vawtrak, Zeus, DarkComet, CyberGate, Xtreme, CTB-Locker. In addition to that, 980 benign files were collected. For the feature set, the successful and failed API calls were used, along with appropriate return codes. All samples were run in the secure virtual environment (sandbox), that produced the behavioral report after completion. These reports were subsequently parsed for API calls, which were written in the form of combined matrix. After feature selection, machine learning algorithms were applied. They included Decision Trees and Random Forest. These methods were selected as the most accurate ones, according to multiple previous works in the field.

The advantage of both of these methods is the good performance on noisy datasets and the removed need for feature selection – it should only be used when there is a need for dimensionality reduction, which is our case as well, since the initial feature set consisted of 70 000 features.

The results showed, that for the binary classification problems, the results were: Decision Tree – 94.6%, Random Forest – 96.8%. For multiclass classification, results were: Decision Tree – 93.3%, Random Forest – 95.69%.

As it can be seen, both methods resulted in fair accuracy. This accuracy was also higher than the one achieved when using the signature-based method.

УДК 519.237.8:519.254:004.9

**Нечітка кластеризація результатів міні-мульт тесту для визначення психологічних особливостей хворих**

Байбуз О.Г., зав. кафедри математичного забезпечення ЕОМ, д.т.н., професор; Сидорова М.Г., доцент, к.т.н.; Лапец О.В. аспірантка
*Дніпровський національний університет імені Олеся Гончара, м. Дніпро*

Застосування кластерного аналізу є корисним у різноманітних предметних галузях у тому числі і в медицині, і в психології, оскільки методи кластеризації дозволяють дослідити структуру даних у ознаковому просторі, виділити однорідні за певним формальним критерієм подібності групи (кластери), виявити аномалії, скоротити вихідну вибірку, сформулювати та перевірити гіпотези на основі виявленої схожості досліджуваних об'єктів. Методи нечіткої кластеризації дозволяють одному і тому ж об'єкту належати одночасно кільком (або навіть всім) кластерам, але з різним ступенем приналежності. Таким чином можна проаналізувати ступінь відокремленості кластерів один від одного та виявити їх перетини.

Метою цієї роботи було провести нечітку кластеризацію даних, які є результатом дослідження когнітивних функцій хворих на артеріальну гіпертензію II і III стадії (з давністю перенесеного інсульту не менш 6 місяців). Для визначення психологічних особливостей хворих було використано міні-мульт тест, який являє собою скорочений варіант MMPI тесту та має 11 шкал (з них 3 – оцінні: відвертості, вірогідності, корекції та 8 базисних: іпохондрії, депресії, істерії, психопатії, паранойяльності, психастенії, шизоїдності, гіпоманії), дійсні числа. Необхідно розробити математичне та програмне забезпечення, що дозволить зрозуміти, яка кластерна структура притаманна досліджуваним даним, проаналізувати отримані кластери, виявити схожість властивостей об'єктів аналізу, візуалізувати отримані результати для подальшої їх інтерпретації.

В результаті роботи розроблено програмний продукт кластерного аналізу даних, що реалізує алгоритми C-Means, Густафсона-Кесселя, Даве-Сена, Уіндхема, ансамблеві алгоритми на основі нечіткої агрегації. Програма дозволяє проводити оцінювання якості результатів на основі нечітких критеріїв Рубенса, Хіє-Бені та зовнішніх – Ренда, Жаккарда, Фолка-Меллоу; здійснювати налаштування параметрів (вибір метрики, кількості кластерів, коефіцієнту нечіткості, t-норми тощо) та візуалізацію результатів. Досліджено кластерну структуру даних, виявлено два кластери, проаналізовано нечіткість приналежності об'єктів кожній з груп, а також статистичні характеристики усіх ознак за кожним кластером.

УДК 004.896 + 004.932

# Дослідження методів передискретизації зображень на основі машинного навчання

Ізонін І.В., к.т.н., асистент
*Національний університет "Львівська політехніка", м. Львів*

Методи та засоби забезпечення якості цифрових зображень займають велику нішу в наукових дослідженнях і сьогодні. В останні роки в науковій літературі набувають значного розвитку методи забезпечення надвисокої роздільної здатності зображень (ЗНРЗЗ) на основі машинного навчання. Різноманітний інструментарій, який використовується в цих цілях, сприяє всебічному розвитку методів цього класу, проте вимагає їх дослідження, аналізу та порівняння.

У роботі порівнюються найбільш вживані на сьогодні методи ЗНРЗЗ з використанням машинного навчання. Методи *SRCNN* [1] та *NLS GTM* [2] використовують засоби обчислювального інтелекту для реалізації процедури навчання. *SRCNN* ґрунтується на використанні тришарової конволюційної нейронної мережі глибокого навчання і вимагає великих часових затрат для реалізації процедури навчання. Метод на основі нейроподібних структур моделі геометричних перетворень *NLS GTM* забезпечує швидке навчання, проте дозволяє здійснювати процес передискретизації лише із заданими в процесі навчання параметрами нейроподібної структури, які впливають на якість результуючих зображень. Метод ЗНРЗЗ *Yang et al* [3] на етапі навчання встановлює відповідності між парами зображень низької/високої роздільної здатності на основі просторового представлення зображення. Основним недоліком методу є великі обчислювальні ресурси, необхідні для його роботи. Метод *Zeyde et al.* [3] базується на тій же моделі, що й попередній – навчання і застосування. За рахунок використання методу аналізу головних компонент він зменшує ресурсовитрати в порівнянні з *Yang et al*, а також, дещо покращує результати передискретизації. Метод *Gradient Profile Prior (GP)* [3], розв'язує задачу ЗНРЗЗ шляхом використання градієнтних профілів. Їх застосування пояснюється високою стійкістю при масштабуванні зображень. Цей метод шукає відповідності між статистиками форми (в цьому випадку – градієнтні профілі різкості) пар навчальних зображень. Отримана інформація використовується для накладання обмежень на основі градієнта у процесі реконструкції. Основний недолік – висока обчислювальна складність його роботи.

Ефективність (згідно PSNR) описаних вище методів досліджувалася шляхом експериментального порівняння отриманих ними, збільшених утричі зображень. Результати моделювання для зображень, які подано на рис. 1, наведено на рис. 2 (на осі *y* подано номер зображення).

1 2 3 4

Рисунок 1 – Зображення ( 168×168 пікселів) тестової вибірки

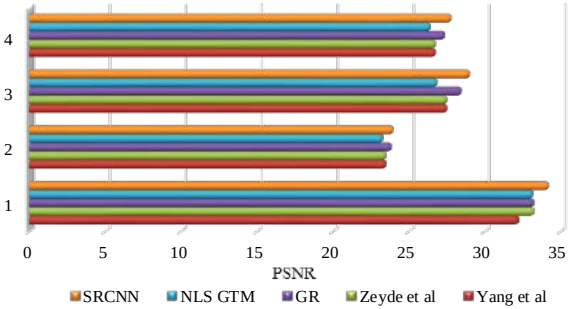



Рисунок 2 – Значення PSNR для зображень, отриманих різними методами ЗНРЗЗ на основі машинного навчання

**Висновки.** Проведено дослідження та аналіз методів забезпечення надвисокої роздільної здатності різних класів зображень на основі машинного навчання. Експериментальним шляхом встановлено, що серед усіх розглянутих методів найкращі результати, згідно PSNR демонструє метод на основі конволюційної нейронної мережі (SRCNN).

**Список літератури**

6. C. Dong, C. C. Loy, K. He X. Tang, Image Super-Resolution Using Deep Convolutional Networks, in *IEEE Transactions on Pattern Analysis and Machine Intelligence*, vol. 38, no. 2, Feb. 1 2016, pp. 295-307.

7. Ткаченко Р. О. Передискретизація зображень засобами машинного навчання / Р. О. Ткаченко, І. В. Ізонін, Д. А. Батюк, Р. В. Сидоренко, В. І. Прострельчук // Математичне та комп'ютерне моделювання. Сер.: Технічні науки. - 2016. - Вип.13. - С. 176-183.

8. Timofte R. Anchored Neighborhood Regression for Fast Example-Based Super-Resolution / Radu Timofte, Vincent De Smet, Luc Van Gool // International Conference on Computer Vision (ICCV 2013), 2013, pp. 1-15.

УДК 004.89

**Класифікація проявів колективного інтелекту у мережі Інтеренет**

Конопліцька-Слободенюк О.К., викладач, Мелешко Є.В., к.т.н., доцент
*Центральноукраїнський національний технічний університет, м. Кропивницький*

Колективний інтелект – здатність групи знаходити рішення певної задачі краще, ніж здатний будь-який з індивідуумів групи самостійно.

Термін колективний інтелект використовується уже декілька десятиліть, але став важливим і популярним з появою нових комунікаційних технологій, зокрема, технологій web 2.0 та соціальних мереж. Цей вираз може викликати асоціації з груповою свідомістю або надприродними явищами, та з практичної точки зору у інформаційних технологіях під ним часто розуміють одержання нових знань з об'єднання та аналізу інформації про вподобання (лайки, оцінки, рейтинги), поведінки (зафіксовані дії користувачів на веб-сайтах) та висловлювань (пости, коментарі) деякої групи людей у мережі Інтеренет [1].

Колективний інтелект може проявлятися у об’єднаних у групу вірусів, бактерій, тварин, людей, а також роботів зі штучним інтелектом (напр., багатоагентні системи, ройовий інтелект). Рівень інтелектуальності групи прямо залежить від кількості учасників у ній.

Автори пропонують класифікувати прояви колективного інтелекту у мережі Інтернет за суб’єктом його використання:

1) використовують члени групи;

2) використовують треті особи;

3) несвідомі спонтанні прояви.

*Прояви колективного інтелекту, свідомо ініційовані членами групи.* Коли збирається разом група однодумців для вирішення конкретних завдань, то в їх спільному "мозковому штурмі", спільній роботі чи спільних діях народжується щось нове. Цей принцип покладено у безліч сайтів, побудованих за принципом технології web 2.0. Прикладами можуть слугувати Вікіпедія та подібні їй сайти (вікі-проекти), краудсорсингові та краудфандингові сайти, системи запитань і відповідей, спеціалізовані соціальні мережі та групи у звичайних неспеціалізованих соціальних мережах тощо.

*Прояви колективного інтелекту, свідомо ініційовані третіми особами.* Використовується маркетологами, політтехнологами, соціологами тощо. Засновані на методах збору статистики з веб-сайтів та обробки отриманих даних. Інформацію про вподобання можна збирати по-різному. Іноді даними є куплені відвідувачами сайту товари, а думки про ці товари представляються у вигляді голосування. Згодом, ці статистичні дані обробляють і використовують для своїх інтересів,

наприклад, для розповсюдження рекламних оголошень, різних музичних чи відео вподобань з посиланням на конкретні сайти (фірми). Великі організації можуть заощадити мільйони доларів, застосувавши алгоритми колективного інтелекту для ефективної організації ланцюжків постачальників і точного прогнозу попиту на продукцію в різних областях. Для аналізу зібраних масивів даних часто застосовуються методи оптимізації та машинного навчання. Прикладами таких проявів колективного розуму можуть бути рекомендаційні мережі, таргетована реклама, обробка великих даних для вибору стратегії політичної кампанії або рекламної акції тощо.

*Несвідомі спонтанні прояви колективного інтелекту.* Прикладом можуть слугувати деякі біржові ігри, де учасники реагують продажем або навпаки покупкою акцій, дивлячись на тенденції, які задають оточуючі гравці. Також сюди належить вірусне поширення інформації та її вірусне редагування [2]. Вірусне поширення інформації означає проходження теми через безліч приватних фільтрів інтересу, що передбачає повтор значимого і опускання другорядного. Під час тисяч повторень здійснюються тисячі мікроредактур, в результаті кожен блогер вносить щось своє у поширювану інформацію.

Колективний інтелект представляє собою потужний інструмент для вирішення багатьох практичних задач. Але водночас він породжує значну низку проблем, пов'язаних з можливістю використання його для політичних маніпуляцій опортуністів та втратою конфіденційності особистих даних [3]. Тож, разом з розвитком методів використання колективного інтелекту, неминуче виникає необхідність вдосконалювати методи забезпечення інформаційної безпеки та шукати шляхи підтримки балансу між новими можливостями інформаційних технологій та безпекою окремої особистості.

**Список літератури**

1. Сегаран Т. Программируем коллективный разум. – Пер. с англ. – СПб: Символ-Плюс, 2013. – 368 с.

2. Дабежа В.В. Вирусная информация и вирусное редактирование в сети Интернет / В.В. Дабежа // Приднестровский государственный университет им. Т. Г. Шевченко. – 2016. – №2. – С. 93–96.

3. Коваленко А. Темная сторона больших данных: потеря конфиденциальности [Електронний ресурс] / А. Коваленко – 2014. – Режим доступу до ресурсу: http://datareview.info/article/temnaya-storona-bolshih-dannyih-poteryа-konfidentsialnosti/

УДК 519.237.8:519.254:004.9

## Кластерний аналіз текстових документів на основі гібридних алгоритмів

Коробіхіна І.С., студентка 5 курсу
Науковий керівник – Сидорова М. Г., канд. техн. наук, доцент
*Дніпровський національний університет імені Олеся Гончара, м. Дніпро*

Проблема кластерного аналізу текстів є досить актуальною в різних сферах науки та бізнесу. В останні роки об’єми оброблюваних даних істотно зростають, тому виникає задача підвищення точності і прискорення алгоритмів обробки інформації, у тому числі виділення однорідних груп об’єктів для подальшого аналізу кожної з них, а також кращого розуміння притаманної даним структури.

Результати кластеризації, отримані існуючими, орієнтованими на перевірку заздалегідь сформульованих гіпотез та на «грубий» аналіз методами, напряму залежать від форми початкового набору даних у ознаковому просторі. Оскільки така форма заздалегідь ніколи не відома, то вибір певного методу не завжди є вдалим, що ускладнює отримання досить точних результатів, зберігаючи високу швидкість роботи. Тому виникає необхідність використовувати деякий гібрид існуючих методів.

В останні роки стали інтенсивно розвиватися гібридні інтелектуальні системи. Вони дозволяють використовувати переваги звичайних засобів штучного інтелекту, а також мінімізують основні їхні недоліки. Гібридні системи створюються для вирішення задач, які важко або взагалі неможливо вирішити окремими методами.

Використання гібридних методів ґрунтується на тому, що тільки комбінація моделей досягає повного спектру обчислювальних можливостей. Досить очевидним є те, що гібридні методи є значно сильнішими, ніж сума різних концепцій окремо.

Гібридні підходи у кластерному аналізі – це своєрідне поєднання структурної та еволюційної методик розроблення методів. Вони є найбільш перспективними, оскільки дозволяють досягти тієї самої золотої середини, що в даному випадку є високою точністю та швидкістю кластеризації текстових документів.

В результаті цієї роботи розроблено обчислювальні схеми та нове оригінальне програмне забезпечення, яке кластеризує текстові документи на основі гібридного підходу, латентно-семантичного аналізу (ЛСА) та методу K-means з попередньою обробкою інформації у вигляді стеммінгу Портера та виключення стоп-слів, забезпечуючи виділення однорідних за змістом груп текстових документів на основі частотної матриці терми-на-документи.

Латентно-семантичний аналіз – це метод обробки текстів, написаних природною мовою, оснований на аналізі взаємозв'язків між текстовими документами та певними термінами, які в них зустрічаються. Особливістю методу є виявлення латентних (скритих) зв'язків між об'єктами. При цьому використовується статистична обробка текстів.

Одним із етапів ЛСА є сингулярне розкладання матриці (SVD - Singular Value Decomposition). Його особливість полягає у виділенні ключових складових матриці, що дозволяє ігнорувати шуми.

Для розробки програмного забезпечення було обрано мову програмування – Java, середовище розробки – IntellijIDEA 2016.3.5, засіб розробки інтерфейсу – JavaFX. JavaFX – бібліотека для розробки графічного інтерфейсу користувача. Використовує fxml файли – xml подібні документи, що містять розмітку форми. Це значно спрощує розробку графічного інтерфейсу і надає можливість використання css-стилів, що робить програму приємною на вигляд. Вибір засобу розробки зумовлено великими можливостям JavaFX та візуальним конструктором JavaFX Scene Builder. IntelliJ IDEA – комерційне інтегроване середовище розробки для Java від компанії JetBrains (для розробки використовувалася приватна ліцензія).

Розроблена програма має одну форму, яка є головною. На формі здійснюється перехід між двома вкладками (рис. 1):

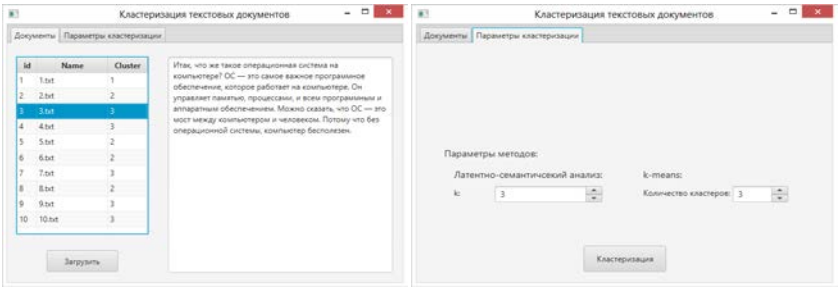



Рис. 1. Інтерфейс розробленого програмного забезпечення

Користувачеві необхідно завантажити текстові документи формату *.txt та встановити параметри кластеризації. Програмне забезпечення також дозволяє переглянути зміст кожного завантаженого файлу. Результатом є відображення номеру кластера напроти назви документу.

Програма зручна у використанні і детально протестована на різних наборах даних.

УДК 004.89: 004.912

# Модель визначення найбільш інформативних компонентів природно-мовного тексту з позиції автоматичної адресації цих повідомлень різним класам контрагентів

Кубявка М.Б., ад'юнкт,
Кубявка Л.Б., к.т.н.
*Військовий інститут Київського національного університету імені Тараса Шевченка, м. Київ*

Одним із різновидів інтелектуальних систем є рефлекторні інтелектуальні системи, які є не чим іншим, як програмними або технічними системи, що формують реакції на несилові впливи, в основі функціонування яких знаходиться рефлекторний алгоритм, який працює за принципом формування реакції-відповіді (рефлексу) на набір вхідних даних (зовнішній вплив). Але цей підхід поки що ніким не використовувався для визначення адресатів повідомлення. Тому для вирішення поставленої задачі запропоновано використати ймовірністно-рефлекторний підхід. В основі рефлексів полягає наступний тезис: якщо це вже було, і деяка реакція була позитивно підкріплена, то необхідно зробити теж саме.

Рефлекторний підхід забезпечує вибір найбільш імовірної реакції на безліч вхідних впливів, при відомих ймовірностях вибору реакції на кожний вхідний вплив, а також на деякі комбінації вхідних впливів.

Під реакцією будемо розуміти правильне визначення адресності інформації.

**Адреса інформації** - результат, який продукується інтелектуальним апаратом людини. Семантична складова інформації, яка є суттю і продуктом процесів несилової (інформаційної) взаємодії в інтелектуальному апараті людини, визначає її адресність.

**Визначення: Адресність повідомлення –** визначений клас контрагентів, на який найбільше впливає зміст повідомлення.

Адресність передбачає розуміння того, кому призначена це повідомлення.

За основу вирішення даної проблематики взято числову міру впливу на характеристики визначення адресності інформації. В основі розрахунку інформаційного впливу покладено правильно визначена адресність (цілеорієнтація) інформації. Для формалізації цього відслідкуємо різноманітні впливи на процес ідентифікації адресності інформації, що дозволить отримати залежність відхилення автоматично визначеної адресності інформації від адресності, визначеної експертом.

Для оцінки ймовірності правильно визначеного адресата інформації необхідно застосувати вже існуючу модель визначення найбільш інформативних компонентів природно-мовного тексту, де повідомлення розкладається на множину фрагментів:

$$I = \{ i_f \}, \; f = \overline{1, g},$$

де $I$ – Інформація (повідомлення);

$i_f$ – фрагмент, який часто повторюється; $g$ – кількість фрагментів.

та по оцінці сумісної умовної ймовірності правильно визначеної адресності інформації і по частковим умовним і безумовній ймовірностям із застосуванням методу оцінки сумісної умовної ймовірності по частковим вибирається та адресність, яка була б визначена і експертом:

$$p(\eta_{\text{Mo}}(A_g / I) \geq \eta_{\text{Mo}}(A_g / I) / \; p(A_g / I) \geq p(A_g / I)) \rightarrow \max,$$

Для вирішення поставленої задачі застосуємо математичну модель взаємозалежності впливів та поведінки контрагента взаємодії але вже не по відношенню до впливу на нього, а по відношенню до визначення адресата інформації.

Отримаємо формулу для оцінки величини впливу деякого фрагменту $i_f$ на адресність повідомлення $A_i$:

1. Якщо $k_i > b_i \wedge b_i > 0$: $w(A_i / i_f) = \dfrac{b_i \cdot (1 - p(A_i))}{(k_i - b_i) \cdot p(A_i)}$;

2. Якщо $k_i = b_i \vee b_i = 0$: $w(A_i / i_f) = \dfrac{(b_i + 1) \cdot (1 - p(A_i))}{(k_i - b_i + 1) \cdot p(A_i)}$,

де $w(A_i / i_f)$ – оцінка величини впливу фрагменту повідомлення $i_f$ на реакцію (вибір адресата) $A_i$;$b_i$ - кількість випробувань, коли було правильно визначено необхідну адресність інформації; $k_i$ - загальна кількість випробувань.

Нова ймовірності вибору адресата $A_i$:

$$p(A_i / I) = \frac{w(A_i / I) \cdot p(A_i)}{1 + p(A_i) \cdot (w(A_i / I) - 1)},$$

де $p(A_i / I)$ – оцінка ймовірності вибору адресата$A_i$.

Сутність новизни моделі полягає у використанні ймовірністно-рефлекторного підходу для визначення адресата повідомлень. Запропонована модель відрізняється від існуючої ідентифікацією різниці в умовних ймовірностях появи адресатів повідомлень як величини інформаційного впливу фрагментів природно-мовного тексту, що дозволило автоматично визначати найбільш імовірних адресатів цих повідомлень.

УДК 004.042:004.8

# Використання принципів генетичного алгоритму для навчання штучних нейронних мереж

Кущевський Д.Р., учень 11 класу обласного навчально-виховного комплексу (гімназія-школа-інтернат) «Пролісок»,
Науковий керівник – Дрєєв О.М., к.т.н.
*Мала академія наук учнівської молоді, м. Кропивницький*

В процесі створення автоматичних ігрових персонажів потрібно враховувати значну кількість можливих ситуацій, таких як зміни навколишніх умов, наявність перешкод та загроз, зміна мапи, дії інших персонажів та інше. Все це створює значну кількість комбінацій зовнішніх чинників і вимагає застосування штучного інтелекту персонажа на основі складних скінченних автоматів [1]. Також, задля спрощення програмування та використаної структури керування, може бути застосовано кілька автоматів з пріоритетами. Вказані технології дозволяють реалізовувати складну поведінку ігрових персонажів, але така поведінка є фіксованою і не змінюється з часом, що дозволяє гравцеві підібрати досить просту тактику поведінки і використовувати її до кінця гри. Тому створення системи, яка може виконувати задачі ігрового штучного інтелекту з можливістю змінювати власну тактику за діями гравця, є актуальною задачею.

Створення ШІ (штучного інтелекту) для ігрового персонажу з можливостями навчання вимагає використання гнучких систем, які мають засоби зміни власної структури та поведінки. Однією з таких систем є нейронна мережа, яка навчається. Існує декілька алгоритмів навчання нейронних мереж: навчання з вчителем, навчання без вчителя, навчання з підкріпленням [2]. У випадку ігрового процесу правильність відповіді нейронної мережі не можна визначити в переважній більшості, також в більшості випадків декілька відповідей можна вважати правильними, тому тут застосовні методи навчання з підкріпленням. В цій роботі запропоновано метод оптимізації коефіцієнтів нейронної мережі алгоритмом близьким до генетичного:

1) Формується множина з N однотипних мереж.

2) Для кожної з мереж моделюється ігрова ситуація з нарахуванням балів та штрафів.

3) За результатами моделювання обирається $n<N$ мереж з найкращими показниками, якщо до списку найкращих мереж претендує декілька з однаковими балами, обирається перша зі списку, або випадкова мережа.

4) Відбувається цикл комбінації мереж. Для випадкової пари мереж формується нова мережа шляхом випадкового вибору коефіцієнтів з першої чи другої вхідних мереж. Кількість мереж доповнюється до

кількості N.

5) Для отриманих мереж відбувається «мутація»: кожен коефіцієнт змінюється на випадкову величину.

6) Пункти 2-5 повторюються до отримання задовільного результату.

Передбачається, що в процесі гри, кожен ігровий персонаж керується своїм екземпляром нейронної мережі. Завдяки цьому процес відбору можна продовжувати. В результаті очікується така властивість ігрової програми, як пристосування до тактики гравця, що змусить його корегувати свої дії. Це зробить гру більш динамічною та цікавою.

В конкретній реалізації, автором було створено N=100 повнозв'язних між шарами мереж з 25 входами, 5 виходами (сигнали «вгору», «вниз», «вправо», «вліво», «стоп») та трьома шарами. Перші два шари містять нейрони по кількості входів, лише останній шар містить нейрони по кількості виходів. В якості вхідних сигналів обрано рівні «-0,5» – клітина поля з ворогом, «0» – непрохідна клітина, «0,5» – порожня клітина, «1,0» – мета пересування. Як показала практика, в значній мірі якість та швидкість навчання мережі залежить від позначення вхідних сигналів. Тому перші спроби навчання мереж були невдалими. Також є проблема невдалої початкової генерації N мереж. Це пояснює невдалі спроби навчання на початкових стадіях. Тому можна зазначити, щоб отримати початкові мережі з помітними відмінностями в поведінці, є необхідним значною мірою збільшувати їх кількість N. Достатню кількість автором було визначено експериментально.

Систему навчання та використання нейронної мережі реалізовано засобами мови програмування FreePascal. Початкове навчання мережі виконано в окремому програмному забезпеченні, що дозволило отримати адекватну поведінку ігрових персонажів на початку гри.

**Список літератури**

1. Программирование мобильных устройств на платформе .Net Compact Framework.: Пер. англ. – М.: Издательский дом «Вильямс», 2006. – 736 с.

2. Тимощук П. В. Штучні нейронні мережі Навчальний посібник. Львів: Видавництво Львівської політехніки, 2011. 444 с.

УДК 004.048

# Автоматизована система відбору спортсменів шляхом багатокритеріального вибору альтернатив методом згортання нечітких чисел

Морока Д.Ю. асистент,
Корнієнко С.К., доцент, к.т.н.
*Запорізький національний технічний університет, м. Запоріжжя*

Зараз всі ми можемо бачити наслідки злиття бізнесу та спорту. Будь-яка спортивна команда поряд з досягненням високих спортивних цілей прагне стрімко розвиватись і в фінансовому плані. Успіхи спортсменів і клубів залежать не тільки від кількості грошей, які в них вкладені, а й від самих спортсменів, від їх таланту, здібностей, нарешті, здатності самовіддачі.

Тож для цього дуже важливо якісно підібрати професійний персонал (гравців), оскільки в умовах сучасної ринкової економіки саме набраний персонал є ключем до успіху або провалу організації.

Розроблена автоматизована система відбору гравців до спортивних клубів базується на використанні методики багатокритеріального вибору альтернатив методом згортання нечітких чисел.

**Опис запропонованої методики**

Рішенням є множина нечітких трикутних чисел. Оцінка альтернатив відбувається на основі упорядкування точок перетину функцій приналежності отриманих трикутних чисел.

Припустимо, що маємо n альтернатив, які можуть оцінюватися за m критеріями, тоді у якості прикладу розглянемо задачу вибору гравців до команди з п'яти претендентів: $u_1$, $u_2$, $u_3$, $u_4$, $u_5$. Претенденти оцінюються за такими критеріями: $g_1$ - вік, $g_2$ – зріст, $g_3$ - позиція, $g_4$ – ігровий досвід, $g_5$ – кількість забитих голів в середньому за гру. Тоді:

$$\widetilde{g_i} = \sum_{j-1}^{n} \frac{\mu_{g_i}(u_j)}{u_j} (i = \overline{1,m})$$

Визначається лінгвістична змінна «оцінка» (альтернатив за критеріями) на наступних нечітких змінних «пог.», «зад.», «доб.», «відм.». Графічне позначення введених нечітких змінних у вигляді трикутних чисел показано на рисунку 1.

Визначаються назви відповідних нечітких змінних: «несуттєвий», «не дуже важливий», «доволі важливий», «важливий», «дуже важливий», «надзвичайно важливий» (НС, НДВ, ДоВ, В, ДВ, НВ) [1]. Сукупність оцінок представляється у вигляді матриці розміром $m \times n$ [2].

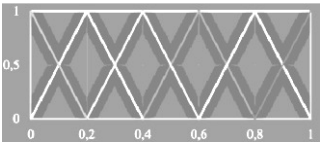



Рисунок 1 – Графічне представлення введених лінгвістичних змінних у вигляді трикутних чисел

Рівні значимості (ваги) критеріїв представлені у вигляді сукупності трикутних нечітких чисел:

$$\widetilde{W} = \sum_{i=1}^{m} \frac{\mu_{w_i}(g_i)}{g_i}$$

Будуємо матрицю $1 \times m$ оцінок важливості:

$$\widetilde{W} = \begin{pmatrix} \text{ДоВ} & \text{В} & \text{НДВ} & \text{ДВ} & \text{НВ} & \text{ДоВ} \\ g_1 & g_2 & g_3 & g_4 & g_5 & g_6 \end{pmatrix}$$

Тоді композиція $\widetilde{D} = \widetilde{W} \circ \widetilde{G}$ знайдеться так:

$$\widetilde{D} = \sum_{j=1}^{n} \frac{\mu_{\widetilde{D}_j}(u_j)}{u_j} = \begin{pmatrix} 3.0 & 4.3 & 3.7 & 3.2 & 3.9 \\ u1 & u2 & u3 & u4 & u5 \end{pmatrix}$$

Отримані n=5 нечітких трикутних чисел, які характеризують пріоритет вибору кожної з альтернатив, показано на рисунку 2.

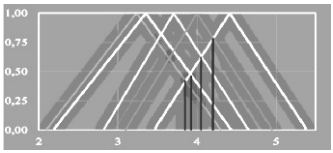



Рисунок 2 – Графічне представлення пріоритетів вибору альтернатив у вигляді трикутних чисел

Використання методики дозволяє визначити кандидатів на вільні у команді позиції, а також на основі матеріалів, розміщених у профайлі знайденого кандидата, прийняти рішення про прийняття до команди.

Дана методика може бути застосованою в різноманітних організаціях для відбору кваліфікованого персоналу.

**Список літератури**

1. Павлов, А. Н., Принятие решений в условиях нечеткой информации. / А.Н. Павлов, Б.В.Соколов, Санкт-Петербургский гос. университет аэрокосмического приборостроения. – СПб: ГУАП, 2006 – 72 с.

2. Алтунин, А.Е. Модели и алгоритмы принятия решений в нечетких условиях / А.Е. Алтунин, М.В. Семухин; Тюменский гос. университет. – Тюмень: ТГУ, 2000. – 352 с.

УДК 004.855

# Логічні закономірності в задачах класифікації даних у технологіях комп'ютерного зору

Охотний С.М., студент 3 курсу
Науковий керівник – Якименко Н.М., к.ф.-м.н., доцент
*Центральноукраїнський національний технічний університет, м. Кропивницький*

Область застосування комп'ютерного зору дуже широка: системи відеонагляду, системи взаємодії, системи доповненої реальності, системи обробки зображень в медицині та багато інших.

Комп'ютерний зір – це теорія та технологія створення машин, які можуть виявляти, відслідковувати і класифікувати об'єкти. Для реалізації систем комп'ютерного зору використовують технології машинного навчання. Машинне навчання – це широкий підрозділ штучного інтелекту, що вивчає методи побудови алгоритмів, які здатні навчатися.

Розрізняють два типи машинного навчання:

– прецедентне навчання (або індуктивне навчання) – засноване на виявленні загальних закономірностей в емпіричних даних, є основою машинного навчання;

– дедуктивне навчання – передбачає формалізацію знань експертів, які переносяться в комп'ютер у вигляді бази знань. Дедуктивне навчання прийнято відносити до області експертних систем.

Машинне навчання передбачає, що комп'ютеру подається навчальний набір даних (з позитивними і негативними прикладами), на основі якого він вчиться працювати з новими даними, які вже не входять до навчальної вибірки. Навчальний набір даних можна представити списком об'єктів. Кожен об'єкт можна описати за допомогою ознак та характеристик. Якщо проаналізувати декілька об'єктів одного класу – можна визначити їх спільні властивості і, при вивченні нового об'єкту, відштовхуватися від інформації про відомий клас, для того щоб зрозуміти чи відноситься новий об'єкт до нього. Наприклад, для того щоб була можливість розпізнавати на певній картинці людину, необхідний навчальний набір даних, який міститиме і не міститиме людей. Люди повинні бути різні – високі, низькі, худі, товсті, в різних позах та в різному одязі. Внаслідок обробки навчальної вибірки формується класифікатор, який містить опис властивостей людей. При його застосуванні до нового зображення, він виявлятиме людей з певним відсотком на основі ознак, які співпали.

Класифікація – це один із розділів машинного навчання, який вивчає побудову алгоритмів класифікації будь-яких об'єктів на основі навчального набору. Для її виконання необхідно знаходити логічні закономірності, на основі яких можна відшукувати спільні ознаки та характеристики між різними об'єктами, для того щоб віднести їх до певного класу.

Логічна закономірність в задачах класифікації – це просте правило, яке легко інтерпретується і виділяє з навчального набору достатньо багато об'єктів одного класу і практично не виділяє об'єкти інших класів.

Нехай $X$ – множина об'єктів, $Y$ – множина імен класів, $X^m = (x_i, y_i)_{i=1}^m$ – навчальна вибірка. $y \in Y$ – фіксований клас, будемо називати об'єкти цього класу позитивними, а всі інші – негативними. Предикат $\varphi: X \to \{0,1\}$ покриває об'єкт $x$, якщо φ(x) = 1.

Закономірністю називається предикат φ($x$), який задовільняє умовам інтерпретованості та інформативності. Додатково до логічних класифікаторів висувають вимогу взаємодоповнюваності:

– інтерпретованість – предикат φ($x$) можна назвати правилом тоді, коли він описаний простою формулою і є добре зрозумілим експертам даної прикладної області;

– інформативність – предикат є інформативним тоді, коли $p_y(\varphi) \to max$ та $n_y(\varphi) \to min$, де:

$P_y(\varphi) = \sum_{i=1}^m [y_i = y]$ – число позитивних об'єктів у вибірці $X^m$;

$N_y(\varphi) = \sum_{i=1}^m [y_i \neq y]$ – число негативних об'єктів у вибірці $X^m$;

$p_y(\varphi) = \sum_{i=1}^m [\varphi(x_i) = 1][y_i = y]$ – число позитивних об'єктів, що виділяються правилом$\varphi$;

$p_y(\varphi) = \sum_{i=1}^m [\varphi(x_i) = 1][y_i \neq y]$ – число негативних об'єктів, що виділяються правилом φ;

– взаємодоповнюваність – набір закономірностей повинен утворювати алгоритм класифікації $\alpha: X \to Y$. Найчастіше логічний класифікатор представляє собою зважену суму закономірностей:

$\alpha(x) = argmax_{y \in Y} \sum_{t=1}^{T_y} \alpha_{yt} \varphi_{yt}(x)$, де:

α($x$) – невід'ємні ваги. У даній формі можуть бути представлені також вирішальні списки та дерева. Вимога взаємодоповнюваності закономірностей означає, що для будь-якого об'єкта вибірки повинна знайтися закономірність $\varphi_{yt}$, яка виділяє даний об'єкт. В іншому випадку алгоритм α($x$) – не зможе класифікувати його.

Використовуючи логічні закономірності можна побудувати класифікатор зображень, який разом з алгоритмами аналізу зображень, дасть можливість розробити систему комп'ютерного зору, для використання в цільовій сфері діяльності.

**Список літератури**

1. Машинне навчання [Електронний ресурс] – Режим доступу до ресурсу: http://www.machinelearning.ru.

2. Машинное обучение – для компьютерного зрения [Електронний ресурс] – Режим доступу до ресурсу: http://my-it-notes.com/2013/05/05-machine-learning-image-classification.

УДК 004.8

# Особливості використання методів кластерного аналізу для вирішення задач конструкторсько-технологічної класифікації

Савеленко О.К., викладач
*Центральноукраїнський національний технічний університет, м. Кропивницький*

На сьогодення при проведенні конструкторсько-технологічної підготовки виробництва (КТПВ) особлива увага приділяється впровадженню та подальшому вдосконаленню концепції CALS, яка передбачає інформаційну підтримку виробу впродовж усього життєвого циклу в єдиному інтегрованому інформаційному просторі на основі використання автоматизованих систем: CAD, CAM, CAE, PDM (PLM).

Це пояснюється тим, що автоматизація КТПВ є однією із складних і слабоформалізуємих задач. Велика різноманітність конструктивних і технологічних ознак технічних об'єктів/виробів (ОВ), можливість використання різних методів КТПВ (в залежності від ступені автоматизації виробничих процесів) до них, призводить до виникнення багатоваріантності рішень. Вирішення цієї задачі можливе лише шляхом використання типових та уніфікованих технологічних процесів (УТП)] розробка яких базується на основі кодування і групування конструкторсько-технологічних ознак ОВ.

Проте питання автоматизації процесу класифікації ОВ за їх конструкторсько-технологічними ознаками (КТО) залишилось фактично на інтерактивному рівні, що призводить до появи небажаних факторів: збільшення термінів КТПВ, сприяє зниженню її якісних показників тощо. Тому робота, спрямована на автоматизацію процесу класифікації ОВ на основі використання методів кластерного аналізу, є на сьогодення актуальною та нагальною.

Алгоритми кластеризації розділяють сукупність даних на підмножини (кластери). Мета цих алгоритмів - створити кластери, однорідні усередині, але які чітко відрізняються один від одного. Дані або вектори характеристик, множини, що є елементами, всередині кластера мають бути максимально схожими один на одного, але в той же час максимально відрізнятися від елементів іншого кластера.

В якості математичної основи для вирішення поставленої задачі пропонуємо використати теорію кластерного аналізу. Це дозволить об'єднувати різні об'єкти в групи за допомогою обчислення значень функцій близькості і схожості (метрик).

Основна складність зображення ОВ в просторі X полягає в забезпеченні можливості порівняння параметрів класифікації. Істотно полегшує вирішення вказаної проблеми введення варіаційного ряду

градацій для кожного параметра. При цьому кожній градації ставиться у відповідність деяка числова характеристика залежно від розташування градацій у варіаційному ряду.

Нехай дана деяка множина ОВ. Вважатимемо, що кожен з параметрів ідентифікується деяким числом. Розглянемо деяку множину ρ параметрів, точки $x = \{x_1, x_2, \dots x_p\}$, де $x_p$ – р-й параметр ОВ, що лежить в просторі Евкліда $R_p$ розмірності Р**.** В цьому випадку природно назвати точку $x \in R_p$ зображенням ОВ. Таким чином, ОВ вважатимемо схожими тоді, коли їх відповідні параметри співпадатимуть.

В даному випадку завдання класифікації полягає в розбитті множини деталей $X = \{x_1, x_2, \dots x_i\}$ на групи, що попарно не перетинаються, число S яких є кінцевим. Очевидно, що максимальне число груп, на які можна розбити послідовність зображень $x_1, x_2, \dots x_i$ рівне загальному числу ОВ в даній множині, тобто кожна деталь утворює групу. Мінімальне ж число груп дорівнює одиниці, тобто усі деталі належать одній групі.

Вказане визначення схожості означає, що ідентичними будуть деталі із ознаками, які зібрані в компактні групи. Тобто, алгоритм, що реалізує рішення задачі, повинен виділяти в просторі X області з великою щільністю зображень з послідовності $x_1, x_2, \dots x_i$ і ігнорувати ті області, де ця щільність мала.

Параметри класифікації в різній мірі впливають на віднесення ОВ до тієї або іншої групи. Тому введемо коефіцієнт $W_i$, що характеризує значущість і-го параметра при класифікації.

Необхідно усунути ряд проблем, пов'язаних з пошуком базових груп (центрів групування(ЦГ)). ЦГ групуванням будемо вважати підмножини об'єктів, розташованих в областях багатовимірного простору ознак, з найбільш високою щільністю зображень ОВ. Після утворення базових груп класифікуються зображення ОВ, що залишилися поза базовими групами. Для визначення приналежності ОВ до однієї з базових груп визначається відстань від її зображення до ЦГ. ОВ належатиме до групи з мінімальною відстанню до ЦГ, а міра схожості – максимальна.

На підставі проведеного в даній роботі аналізу можна зробити наступні висновки: автоматизація процедури класифікації деталей у складі САПР є актуальною проблемою; ключовим моментом є вибір способу класифікації ОВ; одним з найбільш ефективних методів класифікації ОВ є використання методів кластерного аналізу на основі розроблених математичних моделей представлення ОВ.

**Список літератури**

1. Тимченко А.А. Основи САПР та системного проектування складних об'єктів. / За ред. В.І. Бикова – 2-ге вид.- К.: Либідь, 2003. – 272 с.

2. Каталог решений PDM/CAD/CAM/CAE фирмы АСКОН- КИЕВ в области автоматизации конструкторско-технологической подготовки производства и управления предприятием. К.: Аскон, 2004. -40с.

УДК 004.93

## Принцип масової розмірності для аналізу вибірок даних

Субботін С.О., д.т.н., професор
*Запорізький національний технічний університет, м. Запоріжжя*

У задачах скорочення розмірності даних актуальною проблемою є створення показників, що характеризують властивості вибірок. Метою даної роботи було створення методу визначення показників якості вибірок на основі масової розмірності [1].

Розглянемо розбиття простору ознак на компактні області – кластери однакового розміру і форми. Кожен кластер буде містити близько розташовані екземпляри, що мають подібні значення описових ознак. Очевидно, що варіюючи розмір кластера, ми одержимо різні рівні деталізації вибірки. Даний принцип відповідає принципу масової розмірності [1] та покладено в основу пропонованого методу оцінювання характеристик вибірок.

Етап ініціалізації. Задати нормовану вибірку $<x, y>$ – набір $S$ прецедентів про залежність $y(x)$, $x = \{x^s\}$, $y=\{y^s\}$, $s = 1, 2, ..., S$, що характеризуються набором $N$ вхідних ознак $\{x_j\}$, $j = 1, 2, ..., N$, де $j$ – номер ознаки, і вихідною ознакою $y$. Кожен $s$-й прецедент подамо як $<x^s, y^s>$, $x^s=\{x^s_j\}$, де $x^s_j$ – значення $j$-ї вхідної, а $y^s$ – значення вихідної ознаки для $s$-го прецедента (екземпляра) вибірки, $y^s \in \{1, 2, ..., K\}$, де $K$ – кількість класів, $K>1$. Задати одиничний радіус $r$: $0<r<1$.

Етап аналізу класів. Для кожного класу $k=1,2,...,K$: знайти центр мас $k$-го класу $C^k=\{C^k_j\}$ серед усіх наявних у вибірці екземплярів даного $k$-го класу: $C^k_j = S^{-k}\Sigma_{s=1}^{S}\left\{x^s_j \middle| y^s = k\right\}$, $j = 1,2,...,N$; установити номер поточного кластера $k$-го класу $q=1$; виконати етап аналізу $q$-го кластера.

Етап аналізу $q$-го кластера: якщо поточний кластер виявився порожнім (не містить екземплярів $k$-го класу), то прийняти як центр поточного кластера найбільш віддалений від поточного центра екземпляр того ж класу; у зоні, що відстоїть від центра $k$-го класу не більше ніж на $r$, знайти відстані між екземплярами відповідного класу:

$$R^{k,q}(s,p) = \sqrt{\sum_{j=1}^{N}\left(\left(x^s_j - x^p_j\right)^2 \middle| R(x^s, C^{k,q}) \le r, R(x^p, C^{k,q}) \le r, y^s = y^p = k\right)}, \quad R(x^s, C^{k,q}) = \sqrt{\sum_{j=1}^{N}\left(x^s_j - C^{k,q}_j\right)^2},$$

$s = 1, 2, ..., S$, $p = s+1, s+2, ..., S$; визначити середнє відстаней:

$$\overline{R} = \frac{1}{S(S-1)}\sum_{s=1}^{S}\left\{\sum_{p=s+1}^{S}\left\{R^{k,q}(s,p) \middle| R(x^p, C^{k,q}) \le r, y^p = k\right\} \middle| R(x^s, C^{k,q}) \le r, y^s = k\right\};$$

визначити:

– масу екземплярів кластера: $M^{k,q} = \sum_{s=1}^{S}\left(1 + R(x^s, C^{k,q})\right)^{-1}$,

– щільність екземплярів кластера: $\rho^{k,q} = M^{k,q} / S^{k,q}$,

– площу поверхні гіперсфери розмірності $N$ для $q$-го кластера $k$-го класу: $P_s^{k,q} = NC_N\left(\frac{1}{2}\max_{j=1,2,...,N}\{x_{j,\max}^{k,q} - x_{j,\min}^{k,q}\}\right)^{N-1}$, де $C_N = \pi^{\frac{N}{2}} / \Gamma(0{,}5N+1)$, $x_{j,\max}^{k,q}, x_{j,\min}^{k,q}$ – відповідно, максимальне і мінімальне значення $j$-ї ознаки для екземплярів, що належать до $q$-го кластера $k$-го класу,

– об'єм $N$-вимірної кулі, обмеженої гіперсферою розмірності $N$ для $q$-го кластера $k$-го класу: $V_s^{k,q} = C_N\left(\frac{1}{2}\max_{j=1,2,...,N}\{x_{j,\max}^{k,q} - x_{j,\min}^{k,q}\}\right)^N$,

– відношення обсягу до площі поверхні кластера: $\upsilon_s^{k,q} = V_s^{k,q} / P_s^{k,q}$;

видалити з розгляду екземпляри відповідного $q$-го кластера $k$-го класу. Якщо серед екземплярів, що залишилися, у вибірці усе ще маються екземпляри $k$-го класу, то покласти $q$=$q$+1, скорегувати значення $S^k$ і $C^k$, перейти до етапу аналізу $q$-го кластера; у протилежному випадку – повернути вихідне значення $S^k$ і перейти до етапу аналізу вибірки.

Етап аналізу вибірки. Для $k$=1, 2, ..., $K$ визначити:

– масу екземплярів класу відносно центрів мас його кластерів:

$$M^k = \sum_q \left\{ \frac{M^{k,q}}{1 + R(C^{k,q}, C^k)} \right\}, \quad R(C^{k,q}, C^k) = \sqrt{\sum_{j=1}^{N} \left(C_j^{k,q} - C_j^k\right)^2};$$

– щільність екземплярів класу: $\rho^k = M^k / S^k$.

Після чого визначити середньозважену рівномірність розташування екземплярів вибірки: $\xi = S^{-1}\sum_{k=1}^{K} M^k$ .

Запропонований метод дозволяє визначити комплекс показників, що характеризують властивості кластерів, класів і вибірки в цілому.

Для дослідження комплексу запропонованих показників вибірок і моделей вони були програмно реалізовані.

Розроблене програмне забезпечення використовувалося для проведення обчислювальних експериментів по дослідженню застосовності запропонованих показників на прикладі вирішення задач побудови діагностичних моделей. Проведені експерименти підтвердили працездатність запропонованих методів і програмних засобів, що їх реалізують.

**Список літератури**

1. Чумак О. В. Энтропии и фракталы в анализе данных / О. В. Чумак. – М.–Ижевск: НИЦ «Регулярная и хаотическая динамика», Институт компьютерных исследований, 2011. – 164 с.

УДК 621.311.22:658.012.001.24

# Предварительная обработка информации в экспертных системах при проведении экспериментальных медико-биологических исследований

Ухина А.В. [1)], аспирант,
Научный руководитель - Ситников В.С. [1)], д.т.н., професор;
- Ситникова В.А. [2)], д.мед.н., професор
[1)] Одесский национальный политехнический университет, г. Одесса, Украина
[2)] Одесский национальный медицинский университет, г. Одесса, Украина

Интенсивное развитие и применение экспертных систем при проведении научных исследований затронуло и медико-биологическую сферы деятельности исследователей. Современные медико-биологические исследования строятся на концепции доказательной медицины. В настоящее время технология рандомизированных контролируемых испытаний считается стандартом качества научных исследований эффективности лечения. Для этого экспертная система должна учитывать условия проведения эксперимента или исследования (клинические или лабораторные), снизить субъективный фактор исследователя и пациента, а также уменьшить систематическую ошибку, повысить объективность данных и т.п. Один из путей решения этой задачи фильтрация экспериментальных данных для устранения артефактов и шумов измерения. Однако применение стандартных и жестких алгоритмов фильтрации усложняет работу экспертной системы и приводит к многократной обработке исходных данных.

Неопределенность условий фильтрации в таких системах приводит к задаче адаптации или перестройке работы предварительной обработки экспериментальных данных на основе заданных критериев. При этом используемые адаптивные алгоритмы в основном акцентируют внимание на подавлении сигнала без перестройки частотного диапазона.

Построение таких трактов базируется на перестраиваемых алгоритмах второго порядка общего вида:

$$y[n] = a_0 \cdot x[n] + a_1 \cdot x[n-1] + a_2 \cdot x[n-2] - b_1 \cdot y[n-1] - b_2 \cdot x[n-2],$$

где $a_0$, $a_1$, $a_2$, $b_1$, $b_2$ – действительные коэффициенты, $x[n]$ и $y[n]$ – соответственно входной и выходной набор данных.

Например, с технической точки зрения для фильтрации экспериментальных данных в основном используются полосовые частотно-зависимые алгоритмы. Особенность такого алгоритма состоит в

необходимости перестройки его относительной центральной частоты фильтрации $\overline{w_0}$, а возможно и полосы пропускания $\Delta\overline{w}$, а не только коэффициента усиления.

Анализ полосовых алгоритмов такого обобщенного вида показал, что действительные коэффициенты при входных данных имеют следующие соотношения:

$$a_0 > 0, a_1 = 0, a_2 < 0, a_0 = -a_2.$$

Однако, частотные свойства алгоритмов зависят от коэффициентов $b_1$, $b_2$. Проведенные исследования указывают на наличии зависимости коэффициентов $b_1$, $b_2$ и $a_0$ от параметров фильтрации: относительной центральной частоты $\overline{w_0}$ и полосы пропускания $\Delta\overline{w}$.

Частотный анализ таких алгоритмов дает возможность получить соотношения, которые позволяют описать эти зависимости и выполнить управление свойствами алгоритма:

$$\begin{cases} b_2 = \dfrac{cos(\Delta\overline{w}) - sin(\Delta\overline{w})}{cos(\Delta\overline{w}) + sin(\Delta\overline{w})}; \\ b_1 = -2\dfrac{\cos(\overline{w}_0)}{cos(\Delta\overline{w}) - sin(\Delta\overline{w})}; \\ a_0 = \dfrac{sin(\Delta\overline{w})}{cos(\Delta\overline{w}) + sin(\Delta\overline{w})}. \end{cases}$$

Очень важным моментом при управлении свойствами алгоритма является вопрос обеспечения устойчивости алгоритма фильтрации. Устойчивость алгоритма второго порядка описывается треугольником устойчивости в координатах коэффициентов b1 и b2.

Следует отметить, что при уменьшении полосы пропускания Δ коэффициент b2 смещается в сторону увеличения до 1, а при увеличении полосы пропускания Δ коэффициент b2 стремится к 0. Поэтому при изменении полосы пропускания Δ возможен выход на границу устойчивости, что приводит к «разносу» выходных данных.

Таким образом, исследования управления свойствами частотно-зависимого алгоритма фильтрации второго порядка позволило получить простые соотношения, которые можно реализовать на микропроцессорном блоке предварительной обработки в составе экспертной системы, а анализ устойчивости выявить критические области управления и выхода за пределы устойчивости.

УДК 004.9: 614.8.01

**Застосування генетичних алгоритмів для професійного відбору для небезпечних виробництв**

Чемерис М.М., к.т.н., доцент
*Черкаський національний університет імені Богдана Хмельницького*

Основною метою сучасного професійного відбору є виявлення у обстежуваного претендента професійно важливих якостей, необхідних для успішного виконання посадових функціональних обов'язків. Головним в профвідборі є можливість до початку роботи отримати індивідуальну оцінку професійним якостями претендента, попереджаючи заздалегідь трагедії та аварійні ситуації.

Отримання даних про функціональний стан претендента, їх обробка та видача висновків про профпридатність стають досить трудомістким процесом. Сформована ситуація виникла через відсутність у фахівців зручного та ефективного діагностичного інструментарію, що дозволяє професійний відбір зробити високопродуктивним, зручним, якісним і з мінімальним показником суб'єктивізму.

Одним з методів досягнення бажаного результату являється побудова системи підтримки прийняття рішень відбору кадрів на основі генетичного алгоритму.

На вхід системи подаються вхідні дані двох типів: перелік працівників та їх оцінювання (психомоторні якості, просторово-часова екстраполяція, увага, орієнтація у просторі, зорова пам'ять, стійкість до впливу стресів тощо, оцінені за 100 бальною системою), а також опції роботи генетичних алгоритмів. Після знаходження кожним генетичним алгоритмом "найсильніших" команд, вони передаються на панель для очного порівняння та вибору найкращих (рис.1).

Користувач має можливість налаштування параметрів вибору команд (задати кількість осіб в одній групі, кількість потрібних груп, кількість критеріїв при відборі), налаштування генетичного алгоритму (задати мінімальне відхилення, кількість ітерацій, шанс мутації, шанс кросинговеру), обрати вид кросинговеру (одноточковий, двоточковий) та тип мутації (слабка, середня, сильна).

**Принцип роботи генетичних алгоритмів.** При роботі генетичного алгоритму №1 (рис. 1) формуються масиви хромосом (що являються групами працівників), потім вони сортуються за пристосованістю та перевіряється умова пристосованості. Якщо жодна з хромосом не задовольняє цій умові, то відбувається процес кросинговеру обраного користувачем виду та один із видів мутації. Пізніше обирається найкраща хромосома популяції і знову перевіряється на відповідність до умови

пристосованості. Процес відбувається до тих пір, доки не виконається умова і користувач отримає найкраще пристосовану хромосому.

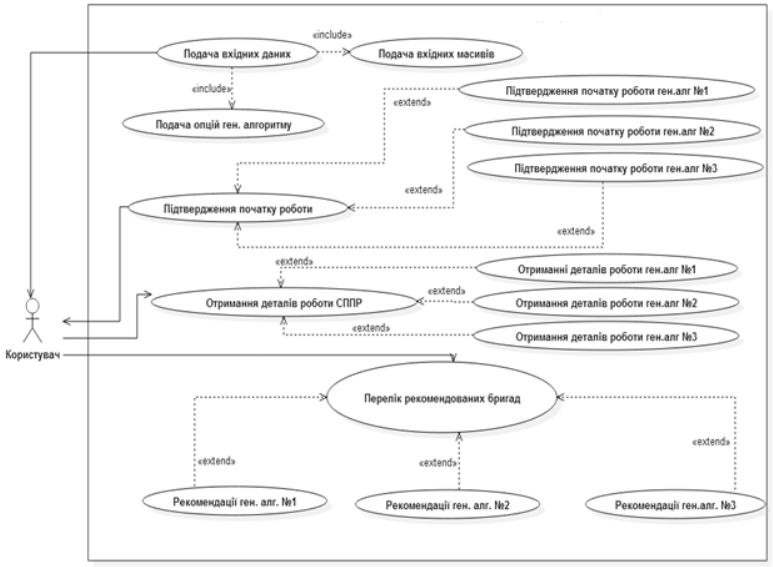



Рисунок 1 – Використання СППР на основі генетичних алгоритмів

Принцип роботи генетичних алгоритмів №2 і №3 аналогічний, різниця полягає в наявності функції очищення даних від повторів. Генетичний алгоритм №3 має інший, відмінний від попередніх, вид мутації та форму для покрокового виведення результатів. Результати роботи СППР зображено на рис. 2.


Рисунок 2 – Представлення модуля формування результатів

Розроблені алгоритми можуть бути застосовані у різних сферах діяльності, що знаходяться в зоні підвищеної небезпеки для людини.

УДК 004.822

**Використання штучних нейронних мереж для вирішення специфічних завдань митної служби**

Яковенко В.О., професор кафедри інформаційних систем та технологій, д.т.н, доцент; Ульяновська Ю.В., доцент кафедри інформаційних систем та технологій, к.т.н., доцент
*Університет митної справи та фінансів, м. Дніпро*

Різноманіття проблем, що виникають при забезпеченні життєдіяльності підприємства є предметом прогнозування, призводять до появи великої кількості різноманітних прогнозів, розроблюваних на основі певних методів прогнозування. Прогнозування обсягу митних зборів на наступні періоди є важливим чинником для планування економіки держави, оскільки саме митні платежі складають вагому частину надходжень до бюджету країни. Сучасна наука має велику кількість різноманітних методів прогнозування, кожен фахівець з планування повинен оволодіти навичками прикладного прогнозування і вміти зробити правильний вибір методу прогнозування.Одним з сучасних математичних методів, який може бути використаним для розв'язання поставленого завдання є штучні нейронні мережі.

Метою роботи є моделювання та автоматизація процесу отримання прогнозних значень показників діяльності структурного підрозділу митної служби з використанням штучних нейронних мереж.

Штучний (математичний) нейрон виконує перетворення вхідного вектора сигналів, наступним чином:

$$y = I(S); S = \sum_{i=1}^{n} w_i x_i \ ,$$

де $w_i$– ваговий вектор нейрона (ваги синаптичних зв'язків); $S$ – результат зваженого додавання; $I$– функція активації нейрона.

Математична постановка задачі: задано набір $\{y(t_1), y(t_2), \ldots, y(t_n)\}$ значень у, що представляють поведінку системи у моменти часу $t_1$, $t_2$, …, $t_n$. Необхідно за попередньою поведінкою системи передбачити її поведінку $y(t_{n+1})$ у момент часу $t_{n+1}$.

Основною задачею розробленого програмного продукту є реалізація функції прогнозування, виконаної на основі штучних нейронних мереж. Для успішного виконання поставленої цілі, отримання стабільності,

швидкодії, гнучкості в основі програми лежить використання бібліотеки мови Java – «Neuroph 2.3.1».

Прогнозування здійснюється на основі методу зворотного поширення помилки, що застосовується до персептрону з одним прихованим шаром, декількома нейронами на вхідному та прихованому шарі (в залежності від навчаючої вибірки) та одним вихідним нейроном.

Навчання нейронної мережі виконується методом зворотного поширення помилки, що застосовується до багатошарового персептрону з чотирма нейронами на вхідному шарі, дев'ятьма нейронами на прихованому шарі і одним вихідним нейроном. Для навчання та демонстрації роботи системи були використані статистичні дані сайту http://www.ukrstat.org/

При створені нової штучної нейронної мережі є можливість вказати кількість нейронів на кожному з шарів, максимальну похибку, швидкість навчання, кількість ітерацій, що необхідно виконати, коефіцієнти впливу на ваги тощо.

Проводячи багаторазові експерименти з даною вибіркою, була виявлена досить цікава та дивна залежність, яка не піддається поясненню статичними законами.

Отримані дані мали досить схожі результати прогнозування, та залежності. Так обов'язковим атрибутом всіх прогнозувань був спад економіки (криза) в 2014, 2015 роках. Таке поводження було тяжко пояснити, адже в навчаючій вибірці жодного разу економічний спад не тривав понад один рік. У той же час події в Україні починаючи з 2013 р. підтвердили розраховані показники.

УДК 519.816: 519.243

## Математичне та програмне забезпечення підтримки прийняття рішень на основі алгоритмів колективного вибору

Яковенко Д. Г., магістрантка
Науковий керівник – Сидорова М. Г., канд. техн. наук, доцент
*Дніпровський національний університет імені Олеся Гончара, м. Дніпро*

Задача прийняття рішень постійно виникає у професійній практиці та повсякденному житті людини. Під прийняттям рішень будемо розуміти особливий процес людської діяльності, спрямований на вибір найкращого варіанта дії.

Метою роботи було розробити математичне та програмне забезпечення, яке дозволяло б швидко та якісно сформувати рекомендації особі, що приймає рішення, на основі експертних оцінок та методів колективного вибору.

У різних сферах діяльності, як правило, існує декілька способів досягнення мети, тобто варіантів рішення, які в теорії підтримки прийняття рішень називаються альтернативами. Розроблена автором система розглядає задану множину альтернатив $A = \{A_i; i = \overline{1,N}\}$, що оцінюється *M* експертами за одним або *K* критеріями. Програма дозволяє:

–здійснювати вибір із заданої множини альтернатив найкращої, в тому числі і по відношенню до деякого якісного критерію $k \in \overline{1,K}$;

–ранжувати задану множину альтернатив (в тому числі по відношенню до деякого якісного критерію $k \in \overline{1,K}$) так, що альтернативі $A_p$ присвоюється ранг $r_p$, а альтернативі $A_h$ – ранг $r_h$, при цьому $r_p < r_h$, якщо альтернатива $A_p$ краща за альтернативу $A_h$.

Математичну основу цієї роботи склали обчислювальні схеми на основі методів Сааті, Борда, Коупленда, плюралітарного та множинного аналізу, а також забезпечення можливості оцінювання компетентності та узгодженості експертів, що є досить важливим у методах агрегування переваг.

Розроблено нове оригінальне програмне забезпечення у вигляді веб-додатку, яке дозволяє створювати та проводити експертизу щодо оцінювання альтернатив різними експертами та формування рекомендацій особі, що приймає рішення у будь-якій предметній галузі. Автор експертизи має можливість обирати експертний склад комісії, виставлені оцінки зберігаються у базі даних та використовуються як вхідні дані для колективних методів прийняття рішень. Програма забезпечує зручну процедуру проведення експертизи та детально протестована.

НАУКОВЕ ВИДАННЯ

ЗБІРНИК ТЕЗ ДОПОВІДЕЙ

II МІЖНАРОДНОЇ НАУКОВО-ПРАКТИЧНОЇ КОНФЕРЕНЦІЇ

“ІНФОРМАЦІЙНА БЕЗПЕКА ТА
КОМП’ЮТЕРНІ ТЕХНОЛОГІЇ”

*INFOSEC & COMPTECH*

20-22 квітня 2017 року

Тези доповідей надруковано в авторській редакції.
Відповідальність за зміст несуть автори.

Відповідальна за випуск: Мелешко Є.В.

---

©Кафедра програмування та захисту інформації ЦНТУ,
м.Кропивницький, пр.Університетський, 8.
Тел. (0522) 39-04-49

---

Формат 60х84 1/16. Ум. друк. арк 12,32. Облік. видав арк. 11,15. Тираж 60. Зам 253.

Підписано до друку 14.04.2017
Видавець і виготовлювач СПД ФО Лисенко В. Ф.
25028, м. Кропивницький, вул. Пацаєва, 14, корп. 1, кв. 101. Тел.: (0522) 322-326
Свідоцтво суб’єкта видавничої справи: серія ДК № 3904 від 22.10.2010