PROCEEDINGS OF

ITSN-2017

International Conference on

INFORMATION TECHNOLOGIES, SYSTEMS AND NETWORKS 2017

Chisinau, Republic of Moldova
17 – 18 October 2017

Veaceslav Perju,
Editor

PROCEEDINGS

ITSN

CZU 004.056(082)
I 52

ISBN 978-9975-45-069-0

The papers presented in this book were part of the workshop cited on the cover and title pages. They reflect the authors' opinions and are published herein as submitted. The editor and publisher are not responsible for the validity of the information or any outcomes results from reliance thereon.

Please use the following format to cite material from this book:

Author (Family Name, Initial of Given Name) "Title of Paper". In: Proceedings of ITSN-2017 International Conference on Information Technologies, Systems and Networks 2017, Chisinau, Republic of Moldova 17 – 18 Oct. 2017. Edited by Veacheslav Perju – Chisinau: ULIM, 2017, Page Numbers.

Deacrierea CIP a Camerei Nationale a Cartii

"Information Technologies, Systems And Networks 2017", intern.conf. (2017; Chisinau). International Conference on Information Technologies Systems and Networks 2017, 17-18 Oct. 2017 / ed. Veacheslav Perju – Ch.: ULIM, 2017. – ISBN 978-9975-45-069-0
Vol. 1. – 2017. – **356p**. – Bibliogr. la sfarsitul art. - ISBN 978-9975-45-070-6: 100ex.

Published by
ULIM – Free International University of Moldova
52, Vlaicu Pircalab Str., Chisinau, MD2012, Republic of Moldova
Tel: (37322)205920; http://www.ulim.md

ISBN 978-9975-45-069-0

PROCEEDINGS OF

ITSN-2017

International Conference on

INFORMATION TECHNOLOGIES, SYSTEMS AND NETWORKS 2017

Chisinau, Republic of Moldova
17 – 18 October 2017

Veaceslav Perju,
Editor

PROCEEDINGS
ITSN

CONTENTS

PREFACE

During 17-18 October 2017 in Chisinau, Republic of Moldova, took place the International Conference "Information Technologies, System and Networks" (ITSN-2017) at which were discussed 67 reports from state, academic, scientific and private institutions from Republic of Moldova, Russian Federation, Romania, Pakistan, Belgium, Ukraine, United Kingdom, USA, Israel and Bulgaria.

In this book there are presented the selected papers from the Conference. In the chapter "Information Technologies" there were presented the questions regarding quality of the software products and their successfulness; computer applications oriented to families of problems; non-linear concave transportation problems solving and implementation using wolfram language; modern networks technologies for providing access to e-infrastructure services; information technologies in managerial data analyzing, processing and synthesizing; information systems organizational forms and units functioning evolution; general aspects of the state tax critical information infrastructure management; security risk detection algorithms in artificial immune systems and the principles of the consciousness society creation based on natural and artificial intelligence.

In the chapter "IT in Distance Learning Education" there were described the principles of the advanced distributed learning in military specialists training; efficient methodologies in games creating for e-learning education; the importance of the massive open online courses as key to success in distance learning education; the design thinking as an innovative approach in training the future leaders of the digital world; a remote laboratory for servomotor studying and the bases of the quality assurance in on-line education.

In the chapter "Information and Cyber Security" there were examined the general aspects of the information technical protection; the problem of the boundaries determining in the information space; the modern security issues in software-defined networking; a "new harvard" architecture as computers with virus immunity; the principles of the network attacks detection based on cluster analysis; the ideas regarding the web users' activities tracking based on the beacons implementation; the document object model cross site scripting vulnerability testing; the principles of using the multidimensional matrices in cryptography and prospects of the cyber security development in digital economy.

In the chapter "Security and Defense" there were presented the general aspects of the information war preventing and combating; a modern view on access to shared services through federated identity provider; the results of the uncertainty analysis of attacker - defender interactions in networks based on game gspn with intuitionistic fuzzy parameters; the problems in circular economy and the principles of the estimating of the shadow economics scale in information technologies.

In the chapter "Signal and Image Processing in Security and Defense" there were examined a directory service for city video surveillance systems; the principles of high speed targets recognition systems design based on optimal combination of the optical and electronic processors; the bases of the image quality improvement based on the prediction theory and the theory and results regarding a comparative study of types, tools and techniques in solar irradiance forecasting.

Presented materials can be of interest for scientists and engineers engaged in information technologies, information and cyber security, security and defense, for students of the license, master and PhD levels of the specialties Information Security, Information Technologies, Computer Science, Applied Informatics, and for postdoctoral researchers.

Veaceslav Perju, DSC, Academician I.I.A.
Conference Chairman and Editor

CONFERENCE DATA

Conference Chairman: Perju Veaceslav, DSC, Academician I.I.A.

Conference Organizer: Free International University of Moldova

Conference Co-Organizers: Academy of Sciences of Moldova; Military Academy of Armed Forces "Alexandru cel Bun", Republic of Moldova

Conference Partners: Fiscservinform SE; Ministry of Education, Culture and Science**;** Ministry of Economy and Infrastructure; Sputnik Moldova – International Information Agency

Conference was Organized in Cooperation with: Academy of Economic Studies of Moldova; Cisco Academy, European Association for Security; Information Society Development Institute; Institute of Electronic Engineering and Nanotechnologies; Institute of Juridical and Political Research; Moscow Aviation Institute (Russian Federation); RENAM Association NGO; Society for Photo-optical Instrumentation Engineering SPIE-Moldova; Technical University of Moldova; University of Sussex (United Kingdom) and **with support of:** Information and Documentation Centre of NATO in Moldova; Iucosoft Ltd; Russian Center of Science and Culture in Republic of Moldova

Organizing Committee

Bogatencov Petru - RENAM Association, NGO
Coceban Vitalie - Fiscservinform SE
Cojocaru Igor - Information Society Development Institute, Academy of Sciences of Moldova
Coropceanu Iurie - Iucosoft Ltd
Donos Alexandru - Decart Ltd
Dubcovetschi Iurie - Free International University of Moldova
Paladi Florentin - State University of Moldova
Perju Veacheslav V. - Sputnik Moldova – International Information Agency
Sandu Sanda - Information and Documentation Centre on NATO in Moldova
Sidorenco Anatolie – Institute of Electronic Engineering and Nanotechnologies, ASM
Șarov Igor - Ministry of Education, Culture and Science, Republic of Moldova
Sofronescu Igor - Military Academy of Armed Forces "Alexandru cel Bun", Republic of Moldova
Tarlev Vitalie - Ministry of Economy and Infrastructure, Republic of Moldova
Todos Petru - Technical University of Moldova
Ursu Eugeniu - E – Government Centre, Republic of Moldova

Program Committee

Bouma Henri - Organization for Applied Scientific Research, Netherlands
Brekhov Oleg - Moscow Aviation Institute, Russian Federation
Butuc Marin - Military Academy of Armed Forces "Alexandru cel Bun", Republic of Moldova
Capatina Gheorghe - State University of Moldova
Cusnir Valeriu - Institute of Juridical and Political Research, ASM
Daradkeh Yousef - Prince Sattam bin Abdulaziz University, Jordan
Gaindric Constantin - Institute of Mathematics and Computer Science, ASM
Gutuleac Emil - Technical University of Moldova
Korzeniowski Leszek Fryderyk - European Association for Security
Maj Miroslaw - Cyber Security Foundation of Poland
Mishkoy Gheorghe - Free International University of Moldova
Ohrimenco Serghei - Academy of Economic Studies of Moldova
Rusnac Andrei – Information security expert, Republic of Moldova
Rusu Andrei - Information Society Development Institute, ASM
Secrieru Nicolae - Technical University of Moldova
Young Rupert - University of Sussex, United Kingdom

Technical Support Committee

Mititelu Vitalii, Aghesin Petru, Caldare Aurel, Bogdanov Vladislav, Timotin Stefan, Catana Alexandru - Free International University of Moldova

1. INFORMATION TECHNOLOGIES

Quality of the Software Products and their Successfulness

[1]Gillani Maryam, [1]Abbas Muhammad, [1]Rehman Saad, [1]A Khan Muazzam, [2]Ata Ullah

[1] National University of Sciences & Technology (NUST), Islamabad, Pakistan.
E-mails: maryam.gillani15@ce.ceme.edu.pk, m.abbas@ceme.nust.edu.pk,
saadrehman@ceme.nust.edu.pk, muazzam@ce.ceme.edu.pk

[2] National University of Modern Languages (NUML), Islamabad, Pakistan.
E-mail: aullah@numl.edu.pk

ABSTRACT

Quality of the software products are critically challenged in past few years due to not having properly designed and evaluated quality standards. Project failures are tremendously targeted on the basis of standards and processes adopted by Quality engineering and developmental teams. The parameters that must be held accountable to have proper check and balance on demonstration of quality is analyzed through various product management techniques i.e. correctness of processing activities, efficient required outputs, timeliness, and user friendliness. Software product management requires consistency in every factor that is making significant contribution towards brand success. Set of 1500 males were asked questions to have user based interactive responses for software product management. Results has shown that if a question is showing 100% result in favor of given option, it does not indicate that users actually wanted to opt that particular option. It merely indicates that it was the only possible solution left for the users to choose. Secondly, it also indicates that users are having their own experiences on the basis of which they are mentioning and choosing one particular option. A software product launch decision cannot actually take out on the criteria of majority voting.

Keywords: software, quality, product, project, management, user, decision, interactive, response

1. INTRODUCTION

Software Quality Assurance (SQA) is the key measure to test the intended functionalities, design and analysis to make software product successful. Software products are client centered entity that targets users' adaptability of liking and disliking. To cater needs of millions of users and to develop single software product that is adaptable enough to be liked by most of the users is itself a tedious task to accomplish for companies. Before a desired software product is launched, companies' opts different scenarios and different methods to analyze the need of market [1]. The desired feature of the software product is not to design something that is amazingly unique in comparison with all other related market software products, but primary concern is to launch a software product that wins most of the user attraction. Competitors of the software product determines and targets effective strategies that can gain more user output. Although, software product is also something to pay attention, but there might be a case when software product is of high features with high built in quality, but user output is not enough to praise it. This will not be declared as product side failure, but can be declared as software product management issue. When a quality rich and bug free software products failed in market, it gives many lessons to the company who launches it. For sure, the expenditure that comes on manufacturing the software product ends in smoke and expected revenue generation collapse as well. Quality Rich Software products can be described as the products that are flexible and extensible. Flexible in terms of ability to add and remove any feature and extensibility in terms of adding desired feature in a system without creating any hazard or damage. Secondly, how change is catered by a software product is significant in quality rich products [2]. Thirdly, maintainability and scalability is also considered in quality rich software products.

Success of the software products cannot be marked as making and launching product that retains high quality features with zero tolerance for imperfections in terms of bugs and failures. Success of software product is to take over market in terms of catching high number of users that will give enough of the admiration to the software product under usage [3]. Making software product quality admirable is much more critical factor to gain for product than just merely launch a software product that raises slogan of having “high quality” software product and does not attract users. Market trends are not supposed to be changed automatically, rather it is something to drive by effective software product management strategies. For example, ten years from now white and golden colors were considered as feminine and something that should be adopted by females to carry only. No one hardly noticed even a single man carrying white and golden colors. While noticing present conditions, men are adapted and very much likely to have these two colors in their daily routine software related products. This change is not occurred with the passage of time, but this kind of change is added in users’ behavior by realizing them i.e. they must try these colors too. Obviously, to change this feminine perspective, effective software product management worked to gain masculine attention of buyers to buy the software products accordingly.

We have identified the issue that *Can a company declares itself most successful company who launches quality rich products, but their products neither ranked among highest selling products nor they competed other market competitors?* Obviously, NO. A good quality software product followed by excellent software product management in terms of making it successful enough to cater major amount of users is the real success of products that is unfortunately least bothered. Company determines the level of quality being praised on the basis of user attention they gain to celebrate their quality rich software products [4]. This paper presents a brief insight of how software product management and project management are interlinked in software product success evaluation. Further, it discusses how high quality software products cannot be declared as successful products and successful software products cannot be marked as quality rich products through adapting methodology of questionnaires and then results are evaluated through graphs evaluation.

Rest of the Paper is organized as follows; section 2 explores the literature Review by including related schemes, section 3 discusses about the methodology and modeling, section 4 is Data Collection and section 5, is data evaluation and analysis. In the last, section 6 concludes the paper.

2. LITERATURE REVIEW

There are various quality assessments factors that can be declared as checklist to check quality of software products. Mainly, correctness of processing activities, efficient required outputs, timeliness, and user friendliness, impressive yet understandable graphical user interface and many more are the main focused points to access quality. Software products quality varies with types of products. Obviously, when it comes to cell phones, users opts for easy and understandable user interface with uninterrupted services. When it comes to Mp3 and sound players, users likes to have high quality sound and fast response time. We can say that quality of all software products cannot be declared in a single or specific definition. Quality factors varies with product to product and it also varies with brands. Every company determines its own quality factors as per criteria of software product under consideration [5]. The main point is not about how quality should be accessed of any software product, but the point is, how effectively a software product's quality can be used to gather maximum number of clients for product usage and to declare it as "quality successfully accomplished". Software product management major phases are illustrated in figure 1.

We cannot raise a "quality achieved" slogan by just only launching software product as per user expectation. Reason behind this lies in the fact that *do your software product is really successful if you are not able to even generate desired revenue out of it?* The answer of this question is NO. Quality factors plays its effective role until product development only [6]. Once the product is developed, what next? Obviously, quality together with successful gathering of high amount of users of that software product determines whether the product has attained what it was supposed to or not. Back in 1983, every leading company was in race of producing best cell phone with effective and admirable features to be declared as pioneer in terms of taking revolutionized step. Many software products were launched and gone without catering any user response. It was not software product's quality failure, but a software product management failure who failed in the critical time to make their software product successful. After so many product launches of mobile phones, Nokia launched its very new mobile hand set named as Nokia 3310. Nokia 3310 was sold up to 126 million users and was declared as most selling mobile phone of decade. Nokia focused on product management that ended up in 126 million sales of the same model in least amount of time. It was not merely a product quality, but a product management who defined the success associated with the product [7].

Customers are not attracted through quality of the software products, but with the quality of effective software product management. In comparison with Nokia 3310, there were numerous software products with WAP, GPS and Intel processors built in functions that were many steps ahead. Same is the case with Nokia 1100 that was sold to over 200 million users that marks it as great step ahead towards being successful. Nokia 3310 came first among all the defined product management strategies. Now, question arises *how software product management and software product related strategies are defined and made?* Answer to this question is by accessing what users want? The desires and wishes of users are gathered by various means and by various methodologies that ends up in accomplishing user desires.

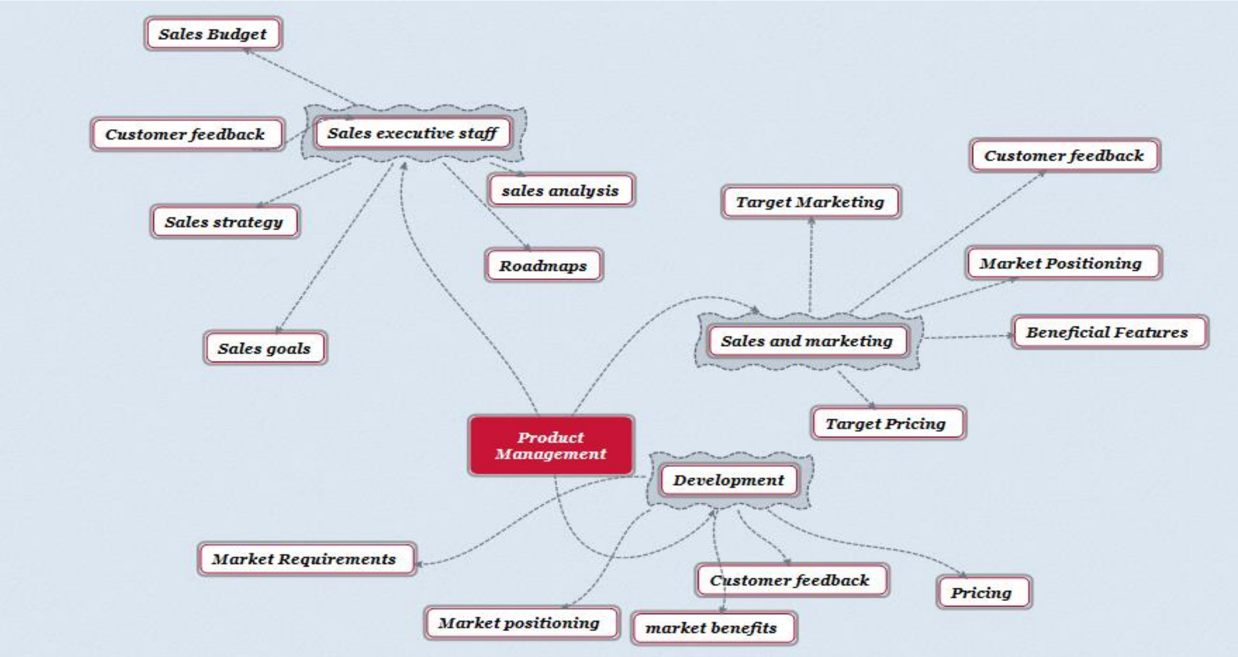


Figure 1. Software product Management Major Phases

One of the mostly adopted method is by designing questionnaires and to get them filled from particular set of customers to have statistical way of analyzing what is the need of market and how software product should be design [8]. Questionnaires are considered as most admiring and healthier way of achieving about what should be done next. Questions to be raised regarding software product management is:

Is it possible that all the failed software products were low in quality? Secondly, all the successful software products were excellent in quality? Both cases are not acceptable. Single Software quality factor can only seek customers if following cases are held true:

- If software product launching brand has already developed suitable name in market that users have started believing it blindly [9].
- Particular user is subjected to have all time good reaction with software product and it's now impossible for him/her to switch [10].
- Brand is pioneer in launching a certain software product and no one else owns the same launched technology in market [10].

"Only quality cannot drive software product success", this can be explained through the biggest example of Nokia Corporation. In details, Nokia started its journey back in 1865 to incorporate its roots in various platforms to have stable client gathering objectives. Nokia stabilized its roots on more than 120 countries with more than 50,000 employees. In 1990, Nokia hit the telecommunication industry with strongest features and technology that was most appreciated [11]. In April 2014, Microsoft finalized the deal and acquire Nokia by paying company's price [12]. What happened to this long succeeded journey? Nokia despite being popular as quality maintainers lost their battle in retaining the clients for the cell phones due to various conflicts. They lunched quality software product, but its other competitors might focused on Software product management as well. This is the biggest lost Nokia encountered and its CEO said that: "we didn't do anything wrong, but somehow, we lost" [13].

Moreover, successful software products are paramount for the success and survival of the firms [14]. Software product failure indicates various theoretical, practical and user based concerns for launching company. Software product management defines goals for effective strategy based on software products [15]. Customer service quality ranks are higher than software product quality. Customer can only be gathered through high quality of the software product, but to retain position in market, software product management plays its important part. Quality rich Product development and consumer attention seeking are two interlinked process. Although, users are cater through quality demonstration of the software products. Moreover, they will remain associated with every launch of specific software product on the basis of their one time software quality rich product experience. Effective Software product management is additional adds on feature for software quality display of the software products [16]. *It is matter of choice to show software quality side to users on the basis of software quality factors, else company can earn brand name, but soon will collapse for not showing its caliber in software product management.* Launching quality software product that catches no user attention will not even accomplish quality goals.

3. METHODOLOGY AND MODELING

A company that launches a questionnaires and gets the filled answers from customers to make critical decision about what to do next is not worth launching a quality directed software product. Implementing user based answers of the questionnaires directly on next software product designing will neither bring quality to the software product nor will give effective market place. To deduce effective decisions from the results of filled questionnaires, a company cannot follow directly what users have said to do. This is sole responsibility of questionnaires conducting body to *omit "what is desired" rather than following "what is expressed".* There is huge difference between desires shown by the users and things that will be like by users. There might be a case that when users will declare in questionnaires that they don't need a specific product in huge ratio, but after seeing actual software product they might show extreme interest. It does not indicate that company should not even think of launching software product that is declared as "no need" product by the market users.

It should be accessed that if huge percentage of users are not in favor of getting the specific idea than maybe they need a "change". For example, if the questionnaires were spread before 15 years to ask from all male users that whether they will buy white and golden color mobiles instead of black and grey? The answer of this question definitely could emerged as NO. Because, 15 year back from this time, white and golden colors was something restricted to feminisms. And why men should go for something adopted by females? The answer is very obvious that illustrates a company not to launch white and golden in huge quantity, because it is something not feasible and revenue making to launch a software product not suitable to all genders. While on the other hand, females were pretty much fine holding black and grey colored mobiles. From the majority percentage of men declaring themselves as not feasible holding white and black mobiles does not indicates to a company not to launch a white and golden mobiles. But, it indicates that men needs change. Many mobile companies stepped forward to launch white colored mobiles and since then majority of the males are opting to get white colored mobiles instead of black and grey. And it's been a decade, white mobiles are on top in terms of catching most of the customers' attention.

Questionnaires results are not supposed to be followed as it is or as declared by the users in results. It is not healthy strategy to deduce result like 90 percent users declared a specific option, so we (company) will follow the 90 percent option. Analysis of result deduced from questionnaires is something to be done quantitatively i.e. on the basis of success measuring criteria and chances of getting failures out of it. To prove this, we have taken data from 1500 males by asking them to fill questionnaires about software products. On this data, we analyzed *when there is right time to turn right.*

Critical point here is, we cannot use and utilize questionnaire based methodology to actually show how questionnaires results cannot be drive the way they seems to be effective. But, user perspective questionnaires are developed to actually locate that how their brand in known for them with various critical factors. *If a question is showing 100% result in favor of given option, it does not indicate that users actually wanted to opt that particular option. It merely indicates that it was the only possible solution left for the users to choose.* Secondly, it also indicates that users are having their own experience on the basis of which they are mentioning and choosing one particular option. *A software product launch decision cannot actually taken out on the criteria of majority voting.* What if majority defines the values that are not suitable for the company asking to give them favor of filling questionnaires? How to drive market on the basis of questionnaires results can be evaluated on the basis of software product and project management.

Project Management vs. Software product Management in context of SQA

Software product and project management not only varies within their domains, but they also works differently. Project management stands for managerial activities with defined inputs, outputs and end date. While on the other hand, Software product management is about providence of specific product to the unspecified amount and criteria of users. As per figure 1, Software product management revolves around three major areas of software product dealings i.e. Sales and marketing, sales and executive staff and development that are interrelated functional. Software product management, when it comes to brands related to mobile phone industry encounters other brand competitors at its peaks in relevance with other gadgets and technology products. Project management revolves around “domains within domains” structure [17]. For example, market segmentation comes under software product management which is further classified under sales executive staff and further in sales budget. But, point to be considered here is every development domain is supposed to be dealt separately even if it comes under multiple domains.

Project management merely strands for project making activities and these activities does not include any “after-project” dealings. We can say that project management is related to initial and final level of software product development. Whereas, software product management is operational after delivery of products and majorly during development of the project as well [18]. This is because of the reason that market trends i.e. new technological revolution, new features are to be monitored under software product management that must be cover during development of software product. Software product management remains operational during project management as well. Project Management areas includes initiation, planning, executing, monitoring and controlling and closing. These processes are independently functional during project management [19]. Although, software product management features are totally missing in the current process description, but most of the time software product management features are controlled by the clients who have ordered the certain product. Below mentioned Figure 2 illustrates complete view how software product and project management activities intermingle together.

Software product management and project management can share their core activities. It is not compulsory to differentiate every step of software product and project management. All the overlapping software product management activities are depicted in comparison with project management. In this scenario, every software product management's activity is sharing its interlinked activities with project management. The point to be considered here is although these activities are functional with both domains, but sharing same managerial area will ultimately collapse functioning of both areas.

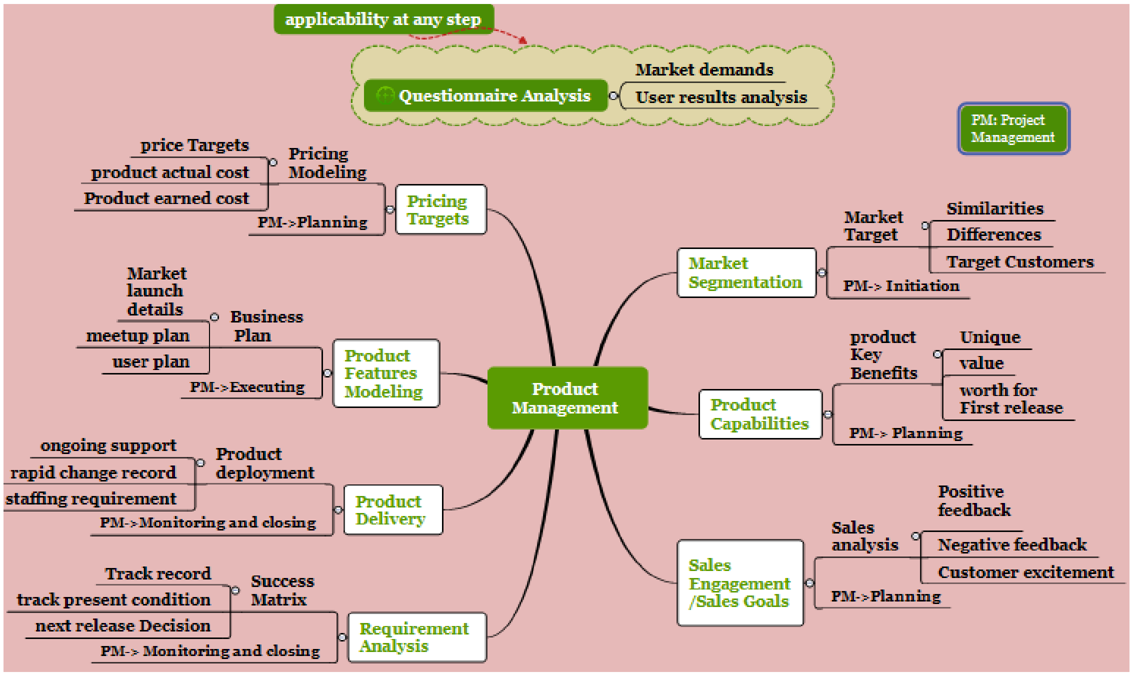


Figure 2. Software product Management activity overlapping with Project Management

4. DATA COLLECTION

Using questionnaires for data collection as methodology, Set of 1500 males were asked few questions to have user based interactive response for software product management. These questions were asked from the set of 1500 males from different fields like students, business people, educationalist, office workers. Questionnaires developing criteria is followed by below mentioned Table I.

These two questions were asked to 1500 males to have real interpretation that how software product management decision on the basis of questionnaires can be taken.

Question 1: Considering yourself 20 years before this era, and golden color as pure feminist color to adopt: Would you like to buy golden color mobile as male member of the society even if its operating system is latest one along with attractive applications? Possible choices: Yes or No?

Table 1. Questionnaires Criteria

Criteria	Questionnaires assessment questions
Brand promotional criteria	Whether customers are properly aware of brand promotions or not.
Brand know, how	Do people know about company software products, sales, technology and pricing details? Are they interested to find these things? Are they familiar with company intentions?
Marketing criteria	How company's marketing criteria is making increment sales, users and market rating. Is it effective or need change?
User interaction	How company software products are making interaction with users? Users are familiar with it or not? Users are interested in it or not?
New software product information	Users are given with sufficient knowledge about software product or not? Users are interested in getting new software product information or not? How software product information is delivered? What factors were considered for it?

Question 2: Considering yourself as male member of 2017, IF your favorite mobile brand offers Pink color mobile exclusively designed for Males along with attractive applications of Males. Would you like to buy it for now? Possible choices: Yes or No or I will decide after seeing software product.

With respect to question 1, 1458 out of 1500 answered NO. This is huge response in favor of not having golden mobile. The scenario was quite easy to adopt by any mobile phone brand. Considering this number against golden color usage, no mobile company will opt to launch golden color mobile. But, this is the right time to turn wrong. Users are always not impressive enough to decide what they really want. One thing to be considered here is "imagination" is something that must be done by the software product management. Users cannot imagine what actually product will look like and how they will be responding to the particular product once they said in questionnaire that they would not like to opt that. The sole responsibility of product management is to locate driving forces of users like including attractive applications before project management can actually starts performing their work. These results are not denying that customers says in majority that they might not like certain option that it should not be accepted, but these results are indicating that:

- ✓ Listen to the crowd actual wants rather than expressed needs [20].
- ✓ Being a part of software product management, dig out the wishes lies in users expressions.
- ✓ Project management hears few minds and make implementation possible for specific amount of clients as per their needs. But, software product management is supposed to target millions of minds with millions of adaptability and rejection factors. To conquer majority of the mind, software product management core responsibility is to evaluate questionnaires responses rather than just taking out the even and odd.
- ✓ Although 1458 males said that they will not accept golden color, but as per current trend, majority of the males are having golden mobiles. Is it due to the acceptance of attractive applications or the change of mood and psyche of Males? Quality of software applications was the attracting factor or not?

Another set of 1500 males (completely different from above) were asked in 2017:

Question 3: What mobile color would you like to have? Do you consider the attractively of applications Golden, White or Black?

With respect to the above mentioned question, 1225 males opted for golden mobile, 200 for white and 75 for black. There were 1000 also opted for attractive applications for audio, video, games and socializing. These questions are meant to prove that "companies who conducts questionnaires based evaluations should not merely depend upon the actual results that comes out as per users responses". Further, same group of 1458 males who opted for the option that they might not go for golden color mobile if they were 20 years back were asked about other mobile feminine colors.

Question 4: Would you like to opt other mobile colors (including feminine colors) for your mobile phones in upcoming years? Do you consider the availability of software products at play stores?

- If I Can opt Golden color than I Can opt other colors as well
- No, I will not take other colors: will keep on using Golden Color

Among 1458, 778 selected that they will not opt other colors, which is huge percentage that is not ready to select other colors including feministic colors. Moreover, 1200 also opted for availability of the attractive software products on play stores. It can be observed that Android phones were purchased in huge numbers as compared to Nokia Lumia that still ensured the high quality of operating system functionalities but lack in attractive applications at play store. Same is the case for iPhone stores and its sales for metallic colors.

Generically, this result deduced that a company should not opt for other colors mobile production. But, following previous history this is not the case. What If no company launched golden colored mobile, because huge percentage said that they will not opt for it. Same is the case with this questionnaire analysis. *Who knows, Silver will be new hit for mobile phone industry.* Companies should also consider the additional software quality needs to achieve overall success of product.

5. RESULTS AND ANALYSIS

On the basis of proposed questions and their answers percentages, software product management strategies can be interpreted by the following analysis points.

Consistency is required in every factor that is making significant contribution towards brand success. As per table 2, not even a single brand strategy is consistent. For example, effective marketing strategy was adopted in 2010 and 2012, but it was then faded away afterwards. If a company took initiative for brand strategy then things should not be stopped rather they must be used in modified and amended way as per needs of recent and upcoming years. Adaptability is being a part of market where brands are known for the latest technology innovations and newer introductory innovative ideas, adaptability is considered to provide users more or less same stuff. In this way, smooth traffic of users will remain associated to the brand. Users are not effective deliverer of what they want in future. Equipped with power of analyzing the demand of market is not something that can be acquired through users directly from filled questionnaires. A brand is responsible for making effective delivery of what we call as effective and quality based software product management [21]. The primary point to target here is users can only answer what is being asked from them. Secondly, you cannot access someone's mind on the basis of company's pre-settled evaluation criteria. But, to dig out main psyche of majority of users on the basis of their filled responses is something that holds in company's software product management hands. The point of difference arises when things are interpreted different rather than following same and common paths of quality product management [22].

Behavioral *modifications influencing quality*

A quality of company is primarily depicted by the behavior with users [23]. A company cannot impose its quality criteria merely by showing quality sign boards and through commercializing software products. Consistent behavior is the most crucial factor that is one step ahead in effective realizing to the customers that they are opting right software product [24].

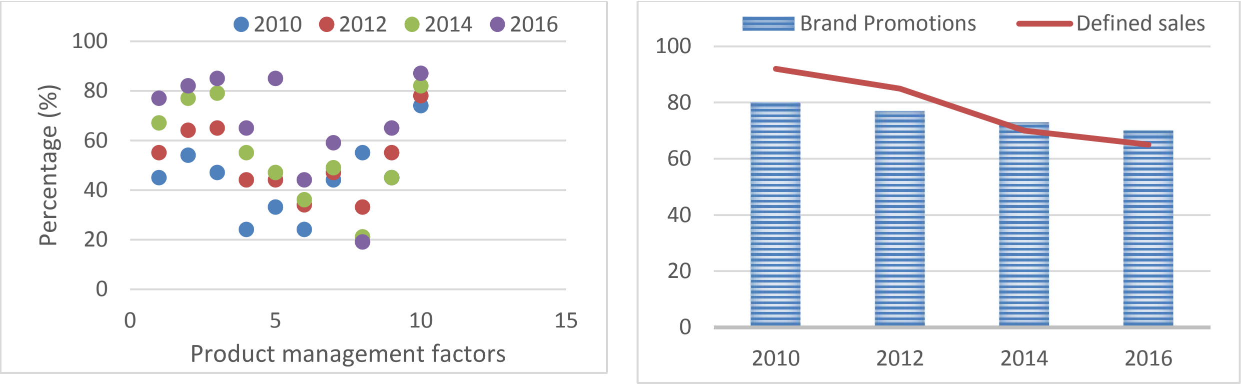


Figure 3. (a) Seven years of Inconsistencies in Software product Management Strategy (b) Instability of Software Product Management Strategy Factors

Behavioral modifications are quality and market driven. Initially market defines what modifications should be adopted and then company is subjected to decide what will go in favor and what will oppose company ratings with respect to quality [25]. Considering software product management strategy and sales, following are the figures of consideration that are taken into account to explain how various Software product management multiple factors are linked together and influence each other as well. Figure 3(a) depicts how quality software product management can be visualized from user's perspective. There are 11 quality software product management strategy factors that are narrating positions of 7 years (2010 to 2017). The overall graph is showing decreasing points year by year i.e. inconsistent. In figure 3(b), 2010 is indicating better software product strategy plan in comparisons with upcoming years. A significant decline is observed with short period of 7 years within extreme peak points of 96% up till 1%. Few percentage changes are something that can be easily bearable and company can cop up that intelligently. Point to ponder here is, a difference of 95% is not only difficult to attain, but it is also indicating software product management collapse of performance. Among all 11 factors, huge variance can be observed. The most critical factor is, not even a single factor of quality software product management is stable enough to show margin of few points. For example, if brand promotion is 100 in 2012 than it is declining with the rate of 88% and coming up to 65% within 3 years of difference.

In figure 4, two critical factors are taken. First one is brand promotions that is primarily considered in the time span of 7 years and the other is defined sales that is not targeted, but achieved through brand promotions. These two variables illustrate decline in company's software product management strategy. Defined sales is a category that not only helps in generating revenue, but it also makes clear evaluations of how company is proceeding ahead. Brand promotion department is actually a monitoring department that monitors whether all the associated users are informed enough? Or do company requires alternative criteria for information transfer. Secondly, is right information is given at right time? Or company is late in letting users know that they need to pay attention on something that might be useful for them. Thirdly, how brand promotions are effecting sales. If current brand promotion plan in neither increasing nor decreasing sales that means change is needed. Because, it is not effecting market and user either way.

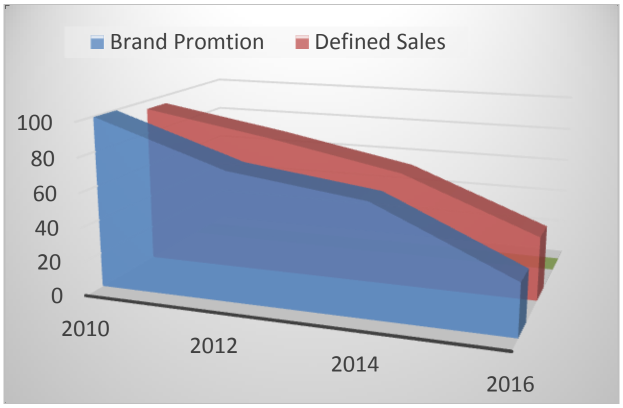


Figure 4. Decrease in Brand promotion and Defined Sales

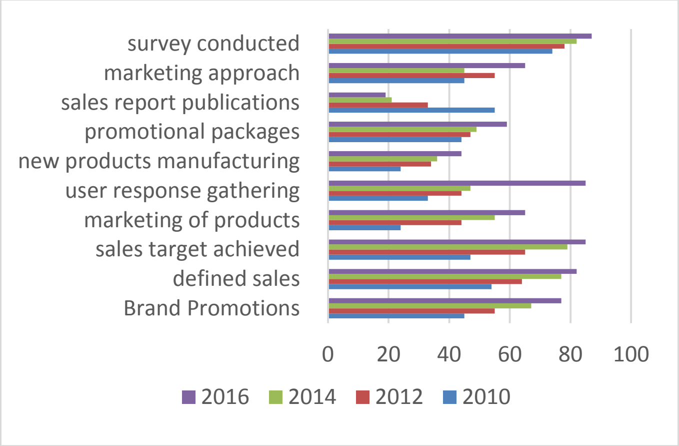


Figure 5. Yearly Software Product Management strategy Factors Ratio of inconsistencies

In Figure 5, percentages are defined with respect to single year performance. The intra year performance evaluation indicates that the factors are not even stable and consistent within one year as well. The performance is declining within span of 7 years, but factors are diverting from stable condition within the time span on 12 months. For example, observe new software product manufacturing factor that is itself showing peak in start of year than slope in the middle and then again peak in the last of the year. Three phases of transitions distracts user traffic, but also raises question mark on brand quality management.

6. CONCLUSION

Single software product that is adaptable enough to be liked by most of the users is itself a tedious task to accomplish for companies. Competitors of the software product determines and targets effective strategies that can gain more user output with effective software product management. Success of the software product cannot be marked as making and launching product that retains high quality features with zero tolerance for imperfections in terms of bugs and failures. Company determines the level of quality being praised on the basis of user attention they gain to celebrate their quality rich software products.

Correctness of processing activities, efficient required outputs, timeliness, and user friendliness, impressive yet understandable graphical user interface and many more are the main focused points to access quality. Customers can never be gained through quality of the software products, but with the quality of effective software product management is must focus factor to target. Implementing user based answers of the questionnaires directly on next software product designing will neither bring quality to the product nor will give effective market place. Initially market defines what modifications should be adopted and then company is subjected to decide what will go in favor and what will oppose company ratings with respect to quality. The point is not to increase assets of company, but to increase sales with respect to development houses.

All of the leading companies targets brand strategy in terms of defining goals related to sales. When the sale limit is reached, goal is considered to be achieved. Above all, software product management is area of keen user interaction. There is huge difference between desires shown by users and things that will be like by users. There might be a case that when user will declare in questionnaires that they don’t need a specific software product in huge ratio. It does not indicate that company should not even think of launching software product that is declared as “no need” product by the market users. It should be accessed that if huge ratio of users are not in favor of getting the specific idea than they might need a “change”. A software product launch decision cannot actually taken out on the criteria of majority voting.

REFERENCES

1. Ming H., June V., Liming L. and Muhammad Ali B. "Software Quality and Agile Methods," in *28th Annual International Computer Software and Applications Conference (COMPSAC’04), IEEE* , 2004.
2. Parvez Mahmood K., Sufyan B. M.M. "Measuring Cost of Quality (CoQ) on SDLC Projects is Indispensible for Effective Software Quality Assurance," *International Journal of Soft Computing and Software Engineering* , vol. 2, No. 9, pp. 1-15, 2012.
3. Ko R. K., Lee S.S and Lee Eng W. "Business process management (BPM) standards: a survey," *Business Process Management, Emerald*, vol. 15, No. 5, pp. 744-791, 2009.
4. Meng X. "The effect of relationship management on project performance in construction," *International Journal of Project Management, ELSEVIER,* Vol. 30, No. 2, pp. 188–198, February 2012 .
5. Martinsuo M. "Project portfolio management in practice and in context," *International Journal of Project Management, ELSEVIER,* Vol. 31, No. 6, pp. 794–803, August 2013.
6. Junaid R., Muhammad Wasif N. "How to Improve a Software Quality Assurance In

Software Development- A Survey," *International Journal of Computer Science and Information Security (IJCSIS)* , vol. 14, No. 8, pp. 1-10, 2016.

7. Eric T., Patrick W. "The management of project management: A conceptual framework for project governance," *International Journal of Project Management, ELSEVIER,* Vol. 32, No. 8, pp. 1382–1394, November 2014.
8. Ming-Chang L. "Software Quality Factors and Software Quality Metrics to Enhance Software Quality Assurance," *British Journal of Applied Science & Technology,* vol. 4, No. 21, pp. 1-27, 2014.
9. Arto T., Marzieh S., Janne H. and Harri H., "Product portfolio management – Targets and key performance indicators for product portfolio renewal over life cycle," *International Journal of Production Economics, ELSEVIER,* Vols. 170, PART B, pp. 468-477, 2015.
10. Asghar A.J., Mohammad Ali H.G., Seyed Abbas M., Khaled N. and Seyed Mohammad Sadeq K. "The Study of effects of customer service quality and product quality customer satisfaction," *International Journal of Humanities and Social Science,* vol. 1, No. 7, pp. 1-8, 2011.
11. Stolle and Sarah, "The History of the Nokia Company," University of Tampere (Department of History), Germany, 2006.
12. Bouwman H. "How Nokia failed to nail the Smartphone market," in *25th European Regional Conference of the International Telecommunications Society (ITS),* Brussels, Belgium, 2014.
13. Jawabra Z., "Nokia CEO ended his speech saying this “we didn’t do anything wrong, but somehow, we lost”.," SIGHT Official , April 2014. [Online]. Available: http://sightofficial.blogspot.com/2016/02/nokia-ceo-ended-his-speech-saying-this.html. [Accessed 07 May 2016].
14. Aron C., Nima H. and Liem V., "Achieving new product success via the synchronization of exploration and exploitation across multiple levels and functional areas," *Industrial Marketing Management, ELSEVIER,* pp. 1-11, 2014.
15. Kevin V., W. Inge W. and Sjaak B. "Improving software product management: a knowledge management approach," *Int. Journal of Business Information Systems,* vol. 12, No. 1, pp. 1-20, 2013.
16. Juliane T., Alexander K., "An empirical investigation on how portfolio risk management influences project portfolio success," *International Journal of Project Management, ELSEVIER,* Vol. 31, No. 6, pp. 817–829, August 2013.
17. Emad S., "Practical Software Quality Prediction," in *IEEE International Conference on Software Maintenance and Evolution*, 2014.
18. Frederik A., Fedi El A., Michael K. and Axel H. "A process framework for theoretically grounded prescriptive research in the project management field," *International Journal of Project Management, ELSEVIER, The International Network for Business and Management Journals (INBAM) 2012,* Vol. 31, No. 1, pp. 43–56, January 2013.
19. Kelly R.C., Ashly H P., "National culture differences in project management: Comparing British and Arab project managers' perceptions of different planning areas," *International Journal of Project Management, ELSEVIER,* Vol. 31, No. 2, pp. 212–227, February 2013.
20. Per S., Peter A. "Rethinking project management: A structured literature review with a critical look at the brave new world," *International Journal of Project Management,*

ELSEVIER, Vol. 33, No. 2, pp. 278–290, February 2015.

21. Bresnena M. "Institutional development, divergence and change in the discipline of project management," *International Journal of Project Management, ELSEVIER*, Vol. 34, No. 2, pp. 328–338, February 2016.
22. Tyrone S P., Shankar S., Siegfried G. and Stewart R C. "Governing projects under complexity: theory and practice in project management," *International Journal of Project Management, ELSEVIER*, Vol. 32, No. 8, pp. 1285–1290, November 2014.
23. Demeulemeester E.K., Flex Serv M.A. "Project management and scheduling," *Flexible Services and Manufacturing Journal, Springer,* Vol. 25, No. 1, pp. 1–5, June 2013.
24. Juliane T., Barbara Natalie U., Alexander K. and Hans Georg G. "Formalization of project portfolio management: The moderating role of project portfolio complexity," *International Journal of Project Management, ELSEVIER, Special Issue on Project Portfolio Management,* Vol. 30, No. 5, pp. 596–607, July 2012.
25. Hornstein H.A. "The integration of project management and organizational change management is now a necessity," *International Journal of Project Management, ELSEVIER,* Vol. 33, No. 2, pp. 291–298, February 2015.
26. O. H. C. Data, "Official Sales data Record (2016)," Haier Manufacturing Unit, Pakistan, North, West and Centarl Region of Haier , 2001-2016.

Software Applications Oriented to Families of Problems

Capatana Gheorghe

State University of Moldova
60, Al. Mateevici str., Chisinau, MD-2009, Republic of Moldova,
Tel: 37367969956, e-mail: gh_capatana@yahoo.com

ABSTRACT

The most used paradigm for the development of software products is the imperative paradigm. In this paper the concepts of *family of problems*, *elaboration of software applications oriented to families of problems,* and some results of use of this methodology are exposed. Elaboration of software applications oriented to families of problems has been experienced by the author and some of his colleagues.

Keywords: problem, classification, elaboration, software, application, oriented, family

1. INTRODUCTION

It is known the fact that at the basis of those four generations of computers developed and implemented until now in the various areas of human activity there are the concepts of „*Turing Machine*” and „ *Imperative programming languages*”. *Information systems* (IS), used in various problem domains, are developed using predominantly the imperative paradigm.

The imperative paradigm has known several forms: unstructured programming, modular programming, functional programming, structured programming, object oriented programming (OOP) et al.

The use of imperative paradigm in the development of the information systems means, that at the request of the beneficiary to solve *n* problems in IS, the developer should elaborate *n* software systems. This state is similar to the situation when to listen a thousand of songs the user needs a thousand of music boxes.

Enterprises are evolving systems that activate in evolving environments. Each time one makes a change in enterprise environment, a change of its structure, eventually, it is necessary to adapt or renovate enterprise’s IS for the reason that it reflects the actions that are already in conflict with the real enterprise conditions. These changes require resources, sometimes considerable: human resources; time and financial resources. In addition, each disturbance of software may affect the reliability of the latter.

2. ACTIVITY DOMAINS

Human activity can be classified by domains of activity. Basic entities of the activity domains are the concepts of "*system*" and "*problem*".

*A **system** represents an ensemble of elements in a structural relationship of interdependency and reciprocal interaction, forming an organized whole* (adapted from the [1]). Each system operates in a certain application domain.

***Application domain** (abbreviated AD) is the AD = (O, R, P), where:*

(a) O - the set of objects AD;

(b) R - the set of relationships between these objects;

(c) P - the set of the processes of transformation of the objects from the O set.

The humans solve various problems in their activities. In the Explicative Dictionary of Romanian Language [2], *the problem* is defined as "a matter in which it is requested on the basis of hypotheses using the calculations or reasoning, to determine certain data, called the solution to the problem". Each problem may have a solution, many solutions, an infinite number or no solution.

The big companies, even using the imperative programming, exceed the limitations of this programming. For example, businesses do not develop an *custom operating system* for each user. The companies develop a *generic operating system*, which then generates a lot of specific, personalized operating systems for each computer on the basis of the parameter values which characterizes the computer. There is a similar situation in the case of programming tools, program packages, etc.

The life cycle of these software products consists of three main stages, carried out by three actors:

(a) the company specialized in the field of software development elaborates *software tools* or *generic parameterized software*;

(b) the developer elaborates *applicative software* with the software builds at step (a);

(c) the developer deploys and maintains software produced at the step (b) and the end-user operates with this software.

Note that in the case of software tools produced by the big companies, each developer elaborates programs which solve some elementary problems. The ability of the software product, which incorporates these modules, to be implemented on a set of computers, for a set of users or companies, represents a synergic property, obtained as a result of the effort of a number, often considerable number, of developers which program using imperative paradigm. In such cases, we notice, that large companies specialized in software development, elaborate the software oriented on families of problems, families of users or families of enterprises, etc.

3. METHODOLOGY

In order to standardize the architecture, technology of design, the operating conditions, to improve productivity, to reduce the costs of the elaboration etc., the software can be developed on computer oriented on *families of problems*.

We will consider *the family of problems* (FP) a set of problems, which may be realized with *a single software*, with *a unique technology of data processing, modes of the information processing* and *unique conditions of the hardware and software exploitation*.

To expound the methodology of the software development oriented to FP we will use *the generic model of the problem* proposed by S. Osuga [3]:

$$\boldsymbol{\mathit{\Pi}\ (Essence, Environment, BC) = true}. \ (2)$$

S. Osuga highlights the four classes of problems facing the society, depending on what is unknown in the model of problem:

1) *the essence* (***Essence***);
2) *the conditions of the external environment of the essence* (***Environment***);
3) *the characteristics of the behavior of the essence in accordance with the conditions the external environment* (***BC***);
4) *the relationship* (***Π***) between the first three components of the problem.

The first class – *the problems of analysis* - are the problems of determination of *the characteristics of the behavior* of the existing *essence* under the known *external environment conditions*:

$$\boldsymbol{\mathit{\Pi}\ (\mathit{Essence}, \mathit{Environment}, \overset{?}{\mathit{BC}}) = \mathit{true}.}$$

The second class - the *problems of the assessment of the external environment conditions* - contains the problems of determination of the external environment conditions, where essence would demonstrate *the behavior characteristics* required by the user:

$$\boldsymbol{\mathit{\Pi}\ (\mathit{Essence}, \overset{?}{\mathit{Environment}}, \mathit{BC}) = \mathit{true}.}$$

The third class, called *the problems of synthesis*, includes the problems of elaboration of *an essence*, which under *the certain external environment conditions*, would demonstrate *the behavior characteristics* desired by the final user:

$$\boldsymbol{\mathit{\Pi}\ (\overset{?}{\mathit{Essence}}, \mathit{Environment}, \mathit{BC}) = \mathit{true}.}$$

The fourth class, called the *class of relationship problems*, includes the problems of determination of *the relationship* between *the essence*, *the external environment conditions* and *the behavior characteristics of the essence* – all known:

$$\overset{?}{\boldsymbol{\Pi}}\ (\boldsymbol{Essence}, \boldsymbol{Environment}, \boldsymbol{BC}) = \boldsymbol{true}.$$

The problems in the first two classes can be resolved by applying the programming oriented to families of problems, by developing:

1) the language of the family of problems, specified by the beneficiary;
2) problems solver, who realizes the language elaborated on step 1);
3) the knowledge base with generic and specific models of the family of problems;
4) the intelligent user interface;
5) the database;
6) the auxiliary modules.

The language of the family of problems represents a structured subset of the natural language, which includes professional terms, used by the end user. It is clear, that the set of the terms is not significant.

The end user interface provides the dialog between the end user and system.

The problems solver represents an inference engine, which takes the knowledge from the knowledge base in order to build the procedure for deduction of the solution of the formulated problem.

The knowledge base keeps the specialized knowledge in the field of competence of the intelligent system.

The database is an auxiliary storage, where data, related to the problem to be solved, intermediate and final results are kept.

Problems of the third class may be solved by:

(a) developing a *generic software*;
(b) developing a specific software, using *the specific values of parameters* and *the generic model* (*the composer*).

The composer and generic software can be produced with the assistance of a *decision support system* (DSS). The problems of the fourth class (the relationship problems) could be solved by applying the artificial neuronal networks, data mining, big data, etc.

The classification of the problems is shown in Table 1.

4. RESULTS AND CONCLUSIONS

The effectiveness of solving problems on the computers depends primarily on the information technology used. In this paper, programming *oriented to families of problems* (OFP) has in view the paradigm, which allows to develop the applications, oriented to families of problems. These intelligent software products are capable to be adapted, implemented, and maintained by the end user, without any assistance of the developer.

POFP has been included in the curriculum of the State University of Moldova. The methodology of software development OFP has been applied during the elaboration of several PhD theses (Eleonora Seiciuc [4], Maria Beldiga [5], Victor Ciobu [6]; PhD students: Victor Seiciuc, Mariana Butnaru, Alexandru Popov, Elena Socolov, Gheorghe Carmocanu), master theses (Victoria Cravcenco, Mircea Munteanu, Valentin Nastasi), license theses (Alexandr Organ) et al.

Table 1. The classification of the universal set of problems

The class	The external environment	The essence	The behavior characteristics (BC)	The relationship (Π)
1	?	known	known	known
2	known	**?**	known	known
3	known	known	**?**	known
4	known	known	known	**?**
5	**?**	**?**	known	known
6	**?**	known	**?**	known
7	**?**	known	known	**?**
8	known	**?**	**?**	known
9	known	?	known	?
10	known	known	?	?
11	?	?	?	known
12	?	?	known	?
13	?	known	?	?
14	known	?	?	?
15	?	?	?	?

The problems of the classes 5-15 can be solved with the assistance of the intelligent DSS.

The OFP has been used in research projects at the USM and ASM for the development of the intelligent software. The first implementation of the OFP dates back to 1973 [7]. The described methodology has been included in the work plan of the Inter-Governmental Commission of the Socialist States for Computing (1983-1991). Software has been developed personally and in cooperation, for: the Government of the Republic of Moldova, Chisinau City Hall, Ministries (Light Industry, Food Industry, Health, Education), the Academy of Sciences, the National Council for Accreditation and Attestation, enterprises from the Republic of Moldova and the Russian Federation.

POFP may be realized in any instrumental language that allows the symbolic processing. The new methodology demonstrates the following advantages:

1) can be applied by a single IT specialist to develop the applications for the family of problems specified by the beneficiary.
2) Software OFP is an intelligent applicative software oriented to the family of problems specified by the beneficiary, and, at the same time, an intelligent software tool, which allows the beneficiary to operate, maintain and develop/extend software without the assistance of the developer.
3) Each OFP software is an expert system for the realized family of problems.

4) Each expert system realizes a formal system, which describes the specified family of problems. In this context the expert system may be considered a suitable system for the automatic theorem demonstration from AD.
5) The methodology of developing software OFP shows a high level of standardization, productivity and reliability.

ACKNOWLEDGMENTS

The presentation of this article is possible due to the institutional project "Development of the intelligent information systems oriented towards families of decision problems with application in education and research", 15.817.02.38A.

REFERENCES

1. Аверкин А. Н., Гаазе-Рапопорт М. Г., Поспелов Д. А. Толковый словарь по искусственному интеллекту. – М.: Радио и связь, 1992. – 256 с.,

2. http://www.gumer.info/bibliotek_Buks/Science/dict/index.php.

3. Dicționarul explicativ al limbii române, https://dexonline.ro/definitie/problema.

4. Осуга С. Обработка знаний. – М: Мир, 1989. - 185 с.

5. Seiciuc E. Rezolvarea aproximativă a ecuaţiilor integrale cu instrumentar software inteligent. Teza de doctor în ştiinţe fizico-matematice. - Chişinău, 2008. – 191 p., http://www.cnaa.acad.md/thesis/11667/

6. Beldiga M. Suport inteligent de e-learning orientat pe familii de probleme decizionale. Teza de doctor în informatică. – Chişinău, 2014. – 152 p.

7. Ciobu V. Modelarea adaptiv-parametrică a unor sisteme fizice complexe. Teza de doctor în științe fizice. – Chișinău, 2016. – 172 p., http://www.cnaa.acad.md/thesis/50909/

8. Капацына Г.Г. Генерирование программ свода документов. В кн.: Состояние и перспективы развития АСУ в легкой промышленности МССР. - Кишинев, 1973, с. 60-61.

Non-Linear Concave Transportation Problems Solving and Implementation Using Wolfram Language

Pașa Tatiana, Ungureanu Valeriu

State University of Moldova
60, A. Mateevici str. Chisinau, Republic of Moldova
E-mails: pasa.tatiana@yahoo.com, v.ungureanu@usm.md

ABSTRACT

In this paper, we analyze some theoretical aspects related to the structure of the non-linear transport problem and some proprieties of the related networks. We propose an approach to improve the method and algorithm proposed in [2]. We present the implementation of the improved method in the Wolfram Language and analyze the obtained results from solving several problems of different dimensions and complexities.

Keywords: nonlinear, programming, concave, transportation, network, optimal, solution, modeling

1. INTRODUCTION

The application of mathematics in economics presumes the application of mathematical methods as an instrument that supports a qualitative study and analysis of quantitative aspects of economic activities. For the article's purposes, the mathematical modeling of economical phenomena is used, which is the basis for obtaining optimal global solutions. Abstraction and generalization of studied earlier problems are provided to include in the same model different economic situations and phenomena.

It is a very good motivation to study the non-linear programming problems as descriptions of economic problems that are often based on nonlinear hypotheses. There are usually reductions to freight rates for big quantities of goods, therefore the cost of an additional unit of product transporting will tend to decrease. Therefore, the cost of transporting a quantity of the product can be described as a non-linear function. The transport problem with non-linear cost functions in respect to the flow on the arcs of the network is a widespread problem in the planning of product shipments and the location of the production sites [4], which is also standard problem in the design of communication networks [7] such as the electricity, gas and water networks. Beside the fact that the functions that describe the transport costs are concave, there can also be restriction on the amount of flow that can be transported from one point to another, so we can have restrictions of the type “no less than” or “no more than”. A transport network is given by a series of points and links between these points, but, as it often happens, we do not always have a direct link between two points, which means that we need to cross some intermediary points to reach the destination.

The transport has a very important role in the socio-economic development of a country because it facilitates the transportation of passengers and goods to the point of destination. The transportation efficiency or cost can be described by a concave nonlinear function, i.e. the cost will depend nonlinearly on the number of passengers or on the weight of the cargo being transported.

2. PROBLEM FORMULATION

Let us consider the transportation network [4, 5] described by the graph $G = (V, E)$, $|V| = n$, $|E| = m$. A real bounded function of production and consumption $q = V \to R$ is defined on the finite set of its vertices V. Concave cost functions $\varphi_e(x_e)$ which depend on arcs flow are defined for each arc. We need to determine such a flow x^* that minimizes a nonlinear objective function

$$F(x) = \sum_{e \in E} \varphi_e(x_e)$$

It is required to solve the nonlinear optimization problem:

$$F\left(x^*\right) = \min_{x \in X} F(x)$$

where X is a set of admissible flows on G described by the following system

$$\sum_{e \in E^+(v)} x(e) - \sum_{e \in E^-(v)} x(e) = q(v) \qquad (*)$$

with both non-negativity constraints and constraints on the transportation capacities of arcs $l(e) \leq x(e) \leq u(e)$, for all $e \in E$.

When we have a standard network, the quantity $p(v_0)$ of commodity available for the source v_0 coincides with the required demand $p(v_t)$ of destination v_t in commodity units and function of production and consumption is defines as it follows:

$$q(v) = \begin{cases} -p(v) & v = v_0 \\ 0, & V/\{v_0, v_t\} \\ p(v), & v = v_t \end{cases}$$

When we have a network with one source and several destinations, the quantity $p(v_0)$ of commodity available for the source v_0 coincides with the required demand $\sum_{v \in V_t} p(v)$ for the destinations V_t in commodity units and the function of production and consumption is defined as it follows:

$$q(v) = \begin{cases} \text{-}\sum\limits_{v\in V_t} p(v), & v = v_0 \\ 0, & V/V_t\backslash\{v_0\} \\ p(v), & v \in V_t \end{cases}$$

When we have a network with several sources and destinations, the quantity $\sum_{v\in V_0} p(v)$ of commodity available for the sources V_0 coincides with the required demand $\sum_{v\in V_t} p(v)$ for the destinations V_t in commodity units and the function of production and consumption is defined as it follows:

$$q(v) = \begin{cases} \text{-}\sum\limits_{v\in V_t} p(v), & v \in V_0 \\ 0, & V/(V_0 \cup V_t) \\ \sum\limits_{v\in V_0} p(v), & v \in V_t \end{cases}$$

3. PRELIMINARIES

Definition: A transportation network [10] is an oriented graph $G = (V, E)$, without loops, which satisfies the following properties:

1. There is a vertex (source) $v_0 \in V$ which has only outgoing edges;
2. There is a vertex (destination, sink) $v_t \in V$ which has only incoming edges;
3. For each arc it is associated a value $c(e)$, for any $e \in E$, named capacity of the arc.
   We can set for each edge a value that describes the maximal size or quantity of the goods which may be transported, distances between nodes, the time to cover the distance or the price to transport the cargo.

Definition: A flow in a network is a function $f: E \to \mathbb{R}$ which satisfies the following properties:

1. Capacity constraint: For all $e \in E$ the condition $f(e) \leq c(e)$ is satisfied;
2. Skew symmetry: For all $(v_1, v_2) \in V$ the condition $f(v_1, v_2) = \text{-}f(v_2, v_1)$ is satisfied;
3. Flow conservation: $\sum_{x\in E^+(v)} x(e) \text{-} \sum_{x\in E^-(v)} x(e) = 0$, where $E^+(t)$ is the set of edges that enter $t \in V$ and $E^-(s)$ - that exit $s \in V$.
   Capacity constraints limit the quantity that can be transported along an arc. Skew symmetry assumes that for each node the quantity of product entering the node equals the quantity that exits it, i.e. their modulus are equal. Flow conservation implies that the whole quantity of product that exits from the source reaches the destination and it is also impossible to have a surplus in the quantity when reaching the destination.
   Vectors $x = (x(e_1), x(e_2), \dots, x(e_m))$ that satisfy the condition (*), as it is known [4], in the m-dimensional space for a convex polyhedral set $X(G, q)$. We will assume that the network G admits flow, so $X(G, q) \neq \emptyset$.

Let x be a flow in G, then the subgraph formed by the arcs $e \in E$ for which $x(e) > 0$ will be denoted by
$G_x = (V_x, E_x)$. Below we highlight some proprieties [6] that describe the formulated problem.

Lemma 1: The set $X(G, q) \subseteq \mathbb{R}^m$ is bounded if and only if G doesn't contain chains.

Lemma 2: If $x^/ = (x^/(e_1), x^/(e_2), \dots, x^/(e_m))$ is an extreme point of the polyhedral convex set $X(G, q) \subseteq \mathbb{R}^m$, then the graph $G_{x^/} = (V_{x^/}, E_{x^/})$ doesn't contain cycles.

Theorem 1: If G doesn't contain cycles, then for the concave functions φ_e for any $e \in E$, there exists a flow x^* in the optimal flows of the transportation network problem such that G_{x^*} doesn't contain cycles.

Proof: Because G doesn't contain cycles according to lemma 1 the set $X(G, q)$ is bounded. Then the studied problem is a problem of minimizing of the concave functional (*) on the bounded convex polyhedral set $X(G, q)$. As it is known [9] the minimum value is reached at one of the extreme points $x^* = (x^*(e_1), x^*(e_2), \dots, x^*(e_m))$ where the graph G_{x^*} doesn't contain cycles according to lemma 2.

Theorem 2: The transportation network problem with concave function of cost φ_e for any $e \in E$ is NP-complete.

In conclusion, we can say that the transportation network problem with concave cost functions can be solved using finite algorithms that study all non-cyclic subgraphs to which a flow is associated and the size of the function is calculated.

In [3], the algorithm for solving the transportation network problem is described for the case when the flow on the network is bounded by an upper and lower value and the cost functions, $\varphi_e(x_e)$ for all $e \in E$, are piecewise concave functions because all concave functions can be approximated with some error to a series of linear functions.. Based on the several tests performed on networks of different sizes, it was concluded that the algorithm doesn't always give the optimum solution. This is due to the fact that the obtained optimum solution depends on the initial solution of the system (*), with which the algorithm begins and which can be obtained differently depending on the method used to solve the system, that will depend on the size and complexity.

By solving the system, we will obtain a general solution in which n base variables are expressed linearly in the other m-n secondary variables. A particular solution will be obtained by assigning zero values to all secondary variables and then calculating the basic variables. Since we can form groups of n base variables of the system, it is known that the number of groups is finite and equal to C_m^n. By modifying in turn each of the C_m^n groups of basic variables, we can obtain all the basic solutions. If all the components of a solution are nonnegative, we can call such a solution admissible. The set of admissible solutions form a polyhedral set of admissible solutions. Between the vertices of the polyhedron of admissible solutions and the basic solutions of the system there is a bijective correspondence, that's why the number of vertices of the polyhedral of admissible solutions coincides with the number of admissible base solutions of the system.

Theorem 3: The set of admissible solutions of a system of equations represents a convex polyhedral set.

Theorem 4: There is a bijective correspondence between the admissible basic solutions of a system of linear equations and the vertices of a polyhedral set of admissible solutions of this system. Each vertex of the polyhedral set is a basic solution.

Based on the above results, the algorithm that solves the transportation network problem with concave cost functions should be modified to start from m admissible solutions and the best to be chosen among the obtained optimum solutions. In this case we will surely get the best optimum solution, regardless of the structure complexity or the size of the graph that describes the transportation network or the concave cost functions.

Another aspect of the problem formulated above is the notion of an optimum solution for nonlinear problems with concave cost functions that has to be minimized in the constraints that have to be satisfied by such solution.

Definition: A function f is concave on an interval, if for all x and y from the interval and all $\alpha \in [0,1]$ the following is true: $f\big((1-\alpha)x + \alpha y\big) \geq (1-\alpha)f(x) + \alpha f(y)$.

In this paper, concave functions are non-decreasing piecewise functions, defined on the interval $[\mathbf{0}, +\infty]$. They describe the cost of shipping the product along an arc.

Definition: For a real function $f: D \in \mathbb{R}^m \longrightarrow \mathbb{R}$ with m real variables, a point $y = (y_1, y_2, \dots, y_m) \in D \subset \mathbb{R}$ is called a local minimum of the function if there exists a neighbourhood V of the point y such that $f(x_1, x_2, .., x_m) \geq f(y_1, y_2, .., y_m)$, for all $(x_1, x_2, .., x_m) \in V \cap D$.

Definition: Let $f: D \in \mathbb{R}^m \longrightarrow \mathbb{R}$ be a real function with m real variables. A point $y = (y_1, y_2, \dots, y_m) \in D \subset \mathbb{R}$ is called global minimum of the function if $f(x_1, x_2, .., x_m) \geq f(y_1, y_2, .., y_m)$ holds for all $(x_1, x_2, .., x_m) \in D$.

As it is known, for a problem of non-linear programming often an optimum solution is obtained as a result of determining a series of solutions and the user is the one that puts restrictions when to stop this series and to consider an approximate optimal solution as the final. Usually this decision is made depending on the available time, computer hardware or the complexity of computations.

Another aspect of the non-linear optimization problem is that it can have many local minimums which is a barrier in the successful solving of the problem, because most often the algorithms give a local minimum that is not necessarily closed enough to the global minimum. A similar situation was also observed in solving the problem formulated above using the algorithm proposed in [1] and improved as described in [2]. In this paper, we aim to increase the possibility of obtaining the global optimal solution.

4. DESCRIPTION AND IMPLEMENTATION OF THE ALGORITHM IN THE WOLFRAM LANGUAGE

Based on the above, we can improve the algorithm by repeating the steps to determine the optimal solution for a few initial solutions and then to select the best one, which will be the optimal solution. We will also examine the possibility of the minimum attaining for several initial/starting points.

4.1 Description of the algorithm

I. Initialization of the data

Step 1.

Construct a table containing k admissible solutions of the system

$$\begin{cases} \sum\limits_{e\in E^{+}(v)} x(e) - \sum\limits_{e\in E^{-}(v)} x(e) = q(v), & for\ all\ v\in V \\ x(e) \geq 0 & for\ all\ v\in V \end{cases}$$

which will be the initial solutions for obtaining the table of optimal solutions.

II. For every element of the table we obtain an optimal solution:

Step 2.

Determine the value of the function in the point:

$$F(x^0) = \sum_{e\in E} \varphi_e(x^0(e))$$

and compute the value of the coefficients:

$$C_e = \begin{cases} \dfrac{\varphi_e\left(x^0(e)\right)}{x^0(e)}, & x^0(e) > 0 \\ F_e^{'}(0), & x^0(e) = 0 \end{cases}$$

for every $e \in E$.

Step 3.

Solve the linear transport problem:

$$min \to z(x) = \sum_{e\in E} C_e x(e)$$

$$\begin{cases} \sum_{e\in E^+(v)} x(e) - \sum_{e\in E^-(v)} x(e) = q(v), & for\ all\ v \in V \\ x(e) \geq 0 & for\ all\ v \in V \end{cases}$$

and obtain the optimum solution $x^1 = \left(x^1(e_1), x^1(e_2), \ldots, x^1(e_m)\right)$.

Step 4.

Compare the values $z(x^1)$ and $F(x^0)$. If $z(x^1) < F(x^0)$ or $z(x^1) = F(x^0)$ and $x^1 \neq x^0$ substitute x^0 with x^1 and go to *Step 2*. If $z(x^1) > F(x^0)$ or $z(x^1) = F(x^0)$ and $x^1 = x^0$ then the optimal solution of the non-linear transport problem is considered the value $x^* = x^0$, the value $F(x^0)$ and $x^* = x^0$ that correspond to it is preserved; go to the next initial solution.

III. Obtain the optimum solution of the problem

Step 5.

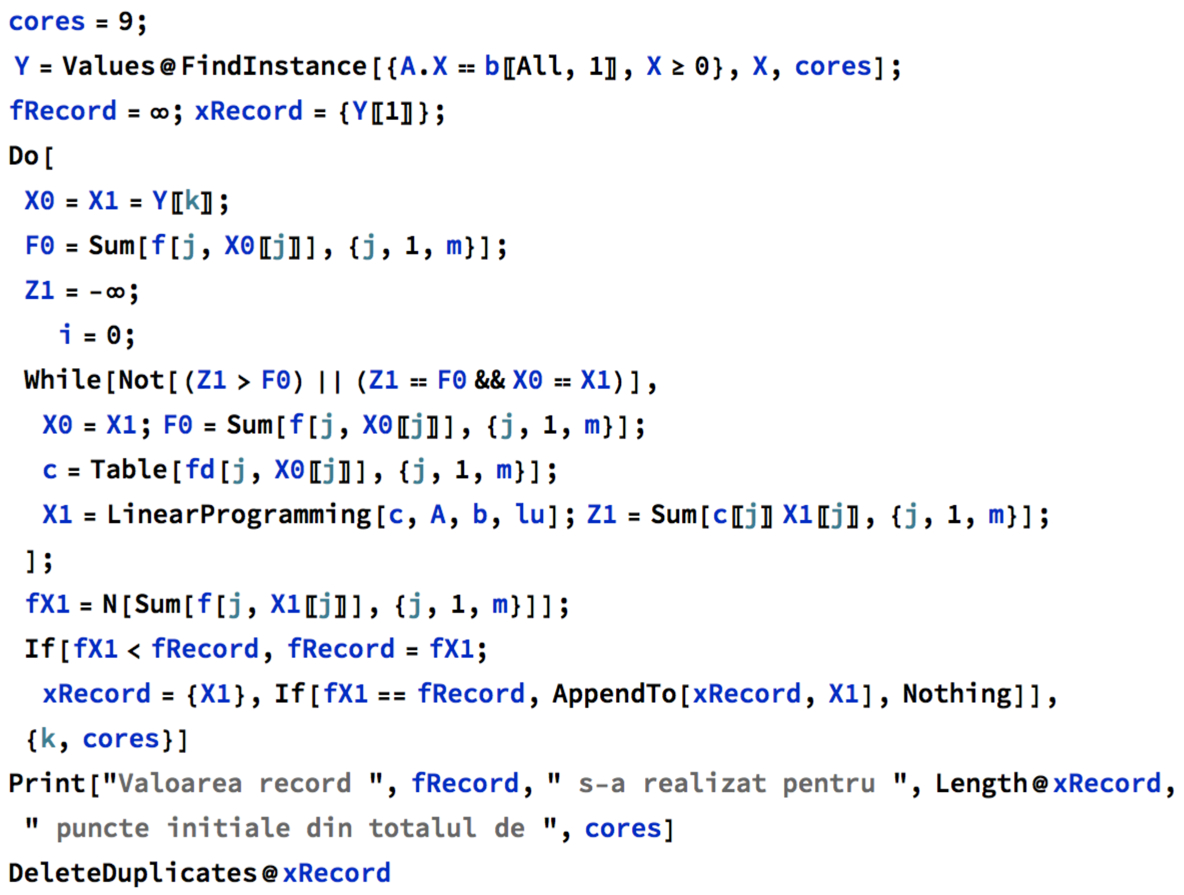
Compare the objective function's values obtained for different initial points and determine the minimal value; save it as the optimal solution and eliminate duplicates. **STOP**..

4.2 Implementation of the algorithm using the Wolfram language

Wolfram Language [11] makes it easy to implement the algorithm.. The code is compact, easy-to-read, it is easy to define new variables and functions.

To obtain an initial solution with which the program will start according to the algorithm, we use the *FindInstace[]* standard function which solves the system of equations. It provides the non-negative solutions and as a result we obtain one of the set of possible solutions on the basis of which a linear function is obtained. *LinearPrograming[]* is a standard function that solves the problem of linear programming. *AppendTo[]* is a standard function which allows adding a new element to the list. *DeleteDuplicates[]* is a standard function that allows to remove duplicates from a list. *Length[]* is a standard function that returns the length of a list, which is the total number of elements it contains.

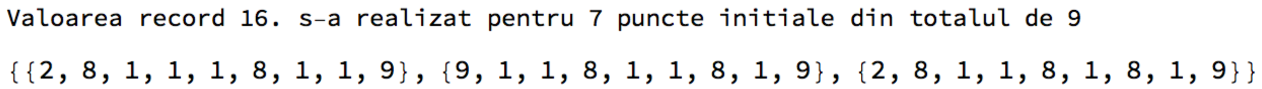
In Figure. 1, the code of the above algorithm is presented.



```
cores = 9;
 Y = Values@FindInstance[{A.X == b⟦All, 1⟧, X ≥ 0}, X, cores];
fRecord = ∞; xRecord = {Y⟦1⟧};
Do[
 X0 = X1 = Y⟦k⟧;
 F0 = Sum[f[j, X0⟦j⟧], {j, 1, m}];
 Z1 = -∞;
   i = 0;
 While[Not[(Z1 > F0) || (Z1 == F0 && X0 == X1)],
  X0 = X1; F0 = Sum[f[j, X0⟦j⟧], {j, 1, m}];
  c = Table[fd[j, X0⟦j⟧], {j, 1, m}];
  X1 = LinearProgramming[c, A, b, lu]; Z1 = Sum[c⟦j⟧ X1⟦j⟧, {j, 1, m}];
 ];
 fX1 = N[Sum[f[j, X1⟦j⟧], {j, 1, m}]];
 If[fX1 < fRecord, fRecord = fX1;
  xRecord = {X1}, If[fX1 == fRecord, AppendTo[xRecord, X1], Nothing]],
 {k, cores}]
Print["Valoarea record ", fRecord, " s-a realizat pentru ", Length@xRecord,
 " puncte initiale din totalul de ", cores]
DeleteDuplicates@xRecord
```

Figure 1. Implementation of the algorithm using the Wolfram language.

An example of the result of the program execution for particular data is presented in Figure 2.



```
Valoarea record 16. s-a realizat pentru 7 puncte initiale din totalul de 9
{{2, 8, 1, 1, 1, 8, 1, 1, 9}, {9, 1, 1, 8, 1, 1, 8, 1, 9}, {2, 8, 1, 1, 8, 1, 8, 1, 9}}
```

Figure 2. The result of the execution of the Wolfram language code

As we can see from the result given by the program, we can have the case when the minimal value of the function is reached in several points.

Function *Minimize[]* is used to obtain the exact global solution of the optimization problem that uses linear programming methods, the Lagrange multiplier method, integer programming and other analytical methods, which involve obtaining precise numeric or symbolic solutions.

Function *NMinimize []* is used to obtain a global numeric solution by applying: linear programming methods, Nelder-Mead method, random search, i.e. numerical methods, which implies obtaining a result from a series of approximations. We can use the attribute *Method* to select the method, e.g. *DifferentialEvolution*, *RandomSeach*, *SimulatedAnnealing*, *NelderMead*, by which the function *NMinimize* will use to solve the problem.

The obtained results using the described algorithm were compared with the results obtained from using standard functions.

4.3 Algorithm tests

All considered problems were solved by generating 100 initial solutions and the optimal solution was selected from the values obtained based on these initial solutions. A comparison between the obtained solutions and the execution time of the algorithm in each case was made.

Nr. of arcs (*m*)	For *m* initial solutions		For100 initial solutions		*Minimize*
	Execution Time	Nr. of optimal solutions	Execution Time	Nr. of optimal solutions	Execution Time
6	0.0781	1	0.6718	1	0.1280
7	0.9375	3	0.8282	3	0.2332
8	0.2187	1	1.9055	1	0.5189
9	0.4531	1	3.7220	1	1.1229
10	1.1562	2	9.9054	2	2,7257
11	1.9375	2	15.1700	2	17.0920
12	4.4531	4	4.4531	4	32.3139
13	10.0625	2	68.0372	2	72.2206
14	16.4063	4	99.1259	4	68.9724
15	40.6250	2	236.5117	2	81.7750
16	56.1250	2	313.3157	6	345.6110
17	140.9530	2	727.777	2	308.3290
18	333.2340	2	1599.7834	2	1827.4400

5. CONCLUSION

From the analysis of the results of the algorithm testing based on a series of problems of different dimensions, we can formulate the following conclusions:

1. The algorithm gives solutions as good as *Minimize[]* and better than *NMinimize[]*, as it gives an optimum solution only in 25% of cases;
2. The execution time increases with the number of initial solutions from which the algorithm starts, but also with the increase of the graph that describes the network;

3. The algorithm offers more solutions for obtained optimum, which in real life gives the possibility to choose the correct strategy in decision making;
4. To manage the execution time of the algorithm, we must carefully choose the number of initial solutions to be built. From the observed from the tests, the number of initial solutions must be at least equal to m, i.e. the number of variables the solution vector has. This will surely give a better final solution than using only one initial solution;
5. In most cases the number of initial solution doesn't increase even if the number of initial solutions with which the algorithm operates is increased.

REFERENCES

1. Pasha T., Lozovanu D. An algorithm for solving the transport problem on network with concave cost functions on flow of edges. Computer Science Journal of Moldova, vol. 10, no 3, Kishinev (2002), pp. 341-347.
2. Pașa T., Ungureanu V. Solving the transportation problem with piecewise-linear concave cost function on edge flows, A 20-a Conferință a SPSR, AFA "Henri Coandă", Departamentul de Științe Fundamentale și Management, Brașov, România, 28-29 aprilie 2017, Editura ASF, p.37
3. Pașa T., Ungureanu V.. Wolfram Mathematica as an enviroment for solving concave network transportation problems.. Proceeding CMSM4, The Fourth Conference of Mathematical Society of the Republic of Moldova dedicated to the centenary of Vladimir Andrunachevici (1917 - 1997), 28 iunie – 2 iulie 2017, Institute of Mathematics and Computer Science, Academy of Scieces of Moldova, Chișinău (2017), p. 429 – 432.
4. Гольштейн Е. Г., Юдин Д. Б. Задачи линейного программирования транспортного типа. М:. Наука, 1969.
5. Ермольев Ю. М., Мельник И. И. Экстремальные задачи на графах. Киев: Наукова думка, 1968.
6. Лозовану Д. Д. Экстремально-комбинаторные задачи и алгоритмы их решения. Кишинев, "Штиинца", 1991.
7. Трубин В. А. Свойства и методы решения задач оптимального синтеза. Киев изд. Общества "Знание", 1982.
8. Форд Л, Фалкерсон Д. Потоки в сетях. М: Мир, 1976.
9. Ху Т.. Целочисленное программирование и потоки в сетях. М:. Мир, 1974.
10. Trandafir R. Modele și algoritmi de optimizare, AGIR, București, 2004.
11. Wolfram S. An elementary introduction to the Wolfram Language. Friesens, Manitoba, Canada, 1-st edition, 2016.

Modern Networks Technologies for Providing Access to E-Infrastructure Services

Bogatencov Petru, Secrieru Grigore, Orbu Maxim Maxim

RENAM Association
Stefan cel Mare Bd., 168, Chisinau, MD-2004, Republic of Moldova
Phone: 373 22 739827; E-mail: bogatencov@renam.md

ABSTRACT

Considering approaches for development of regional and national optical networking infrastructure for providing access to services and technologies for the research and educational communities offered by Pan-European and regional e-Infrastructures. Development of regional connectivity and transferring of the national research and educational optical network in Moldova to use new technologies supported by European Eastern Partnership Programme. Over the several past years demands of research and education institutions for access to high-speed networking infrastructures, to large-scale computing and other e-Infrastructures' services are rapidly increasing. Modern e-Infrastructures integrating various ICT based resources, services and considered as a key enabler for scientific and social development. In the paper describing realization of solutions that are necessary for integrating various national e-Infrastructures and providing convenient, high speed and reliable access to various services that are deploying in Europe to support research and educational activities. Argued importance of National Research and Educational networks (NREN) as a key instruments for access to e-Infrastructures' resources and one of the most important supporters of e-Infrastructure development.

Keywords: optical, networking, infrastructure, regional, connectivity, modern, services

1. INTRODUCTION

The term e-Infrastructure refers to a combination and interworking of digitally-based technologies, resources, communications, and organizational structures needed to support modern, international leading collaborative research. Such infrastructures are oriented to support a distributed medium based on high-bandwidth networks, distributed computing Grid, scientific Cloud resources, HPC and respective data repositories [1]. E-infrastructures for providing modern services for research and education are actively developing in Europe and across the world. This process is important for support research and educational communities in European Eastern Partnership (EaP) countries, including for Moldova [2]. Initially different components and resources of e-Infrastructures were developing independently in every country or even by only one institution that need to use specific IT services. At this initial period, actions in this area were rather spontaneous (or even more like chaotic) because were dependent on abilities and interests of separate research teams, institutions or projects. These e-Infrastructure resources were created and used for support specific needs of research teams that owned the created infrastructures. Usually the resources were dedicated to solve only one narrow scientific problem with limited abilities to be re-used and to serve wider communities.

Since the beginning of 2000's in Europe started developing several well-structured programmes of creation of Pan-European e-Infrastructures that had the aim to increase their effectiveness by implementation of universal resources and services for common use by many institutions and researchers across the Europe [3]. As an examples of these successfully operating Pan-European universal e-Infrastructures we can mention:

- GEANT - high-bandwidth European networking backbone for Research and Education;
- EGI - distributed Grid and scientific Cloud resources;
- EUDAT - integrated data services and resources to support various research activities;
- OpenAIR – scientific data collection and open access data repositories;
- PRACE (Partnership for Advanced Computing in Europe) – European HPC initiative;
- Several ESFRI projects (ELIXIR (LS), CLARIN, DARIAH (CH), EMFL (European Magnetic Field Laboratory), BBMRI (BioMolecular Research Infrastructure), etc.) that are developing European level research infrastructures for providing specific services for many interested institutions.

There are other similar examples of created recently e-Infrastructures of common use in Europe and in other countries outside Europe that are dedicated to support specific research or to serve specific research communities like High Energy Physics, Life Science, Climatology, Genome research, etc.

2. REGIONAL INITIATIVES OF e-INTRASTRUCTURES DEVELOPMENT

Some of EaP countries, including Moldova started developing components of own e-Infrastructures and participate in European initiatives of Pan-European e-Infrastructures development, providing computing and storage resources to these infrastructures for common use in the mid of 2000'. The first initiatives in this area based on a serious of EU funded regional projects that included development of regional scientific computing infrastructures with the aim to integrate their resources and services in the existing at this time Pan-European computing infrastructures like Grid and distributed multiprocessors clusters [4].

In 2009 most of EaP countries became involved in projects of common Pan-European networking infrastructure development known as GEANT and received status of members of GEANT project consortium [5].

In 2006-2012 European Commission launched several feasibility study initiatives in EaP region that had the aim to harmonize development of Research and Educational resources and services in EaP countries with European strategy and e-Infrastructure realization approaches [6]:

- POS - "Porta Optica Study" project (2006-2007) that had the main goal stimulation and consolidation of initiatives to ensure the successful, dark-fiber based research network deployment in the Eastern Europe.
- Black sea Initiative - building a proper regional research and education network among South Caucasus and connecting it to GÉANT;
- SEENGINE - feasible study of research e-Infrastructures development in the Eastern Europe countries and coordination of the activities between national and pan-European e-Infrastructure initiatives;
- EAPConnect Concept Note - the aim to investigate possible solutions for integrating EaP region to GÉANT and support of potential project elaboration focused on regional research and education network creation.

To study possible solutions and promote implementation of regional connectivity, participation of EaP countries in creation of regional e-Infrastructures and related services for local research and educational communities in 2012 with support of European Commission (EC) was elaborated important document – EaPConnect Concept Note. The document contained specification of priority e-Infrastructure resources and services recommended for deployment in the region and requirements for elaboration of detail regional project focused on creation of regional networking infrastructure, extending connectivity to GEANT and development of e-Infrastructure services in the participating EaP countries.

To support creation and development of e-Infrastructures' resources, uniting and making widely accessible the existing in EaP countries e-Infrastructures on the base of the elaborated Concept Note the NRENs of EaP countries and experts from GEANT Consortium prepared and submitted to EC a project proposal named "EAPConnect" that was approved in 2015.

The main aims of the EaPConnect project are:

1. To establish and operate a high capacity regional network serving the needs of the user communities of the beneficiary countries;
2. To promote the use of the network for collaborative research and education programmes;
3. To build capacity and capabilities to maximise the benefit of research and education networking in the region;
4. To promote the project to stakeholders and prepare a sustainability plan for the programme beyond EaPConnect.

The project work programme envisaging the following principal directions of activities:

- Project Management and Reporting;
- Network Design, Network Connectivity and necessary Equipment for Network Infrastructure Implementation Procurement;
- Network Operations;
- Selection, Supporting and Promoting Applications and Services;
- Human Capacity Building and Knowledge Transfer;
- Sustainability Study and Actions Plan.

One of the most important output of EaPConnect project expected for realization is development of regional connections in EaP region and improvement of connectivity of all EaP countries to GEANT. General scheme of the creating regional network is presented in the Figure 1.

The elaborated scheme has clear advantages:

- Fulfils the connectivity and capacity requirements of all EaP NRENs;
- Provides a large capacity increase to South Caucasus countries;
- Provides backup connection to NRENs;
- Traffic between NRENs in Armenia, Azerbaijan, Belarus, Georgia, Moldova and Ukraine goes directly via Cross Border Fiber (CBF) connections over the dedicated network.

As a long term vision that would ensure best collaboration with EaP countries, in the E@P.connect Concept Note is proposed to establish two optical backbones:

- North to South backbone - possibly from Baltic States through Poland, Belarus, Ukraine, Moldova, Romania and further to Sofia and Athens;
- Black Sea ring – connect from Romania through Moldova, Ukraine, South Caucasus to Turkey and further to Sofia and Athens.

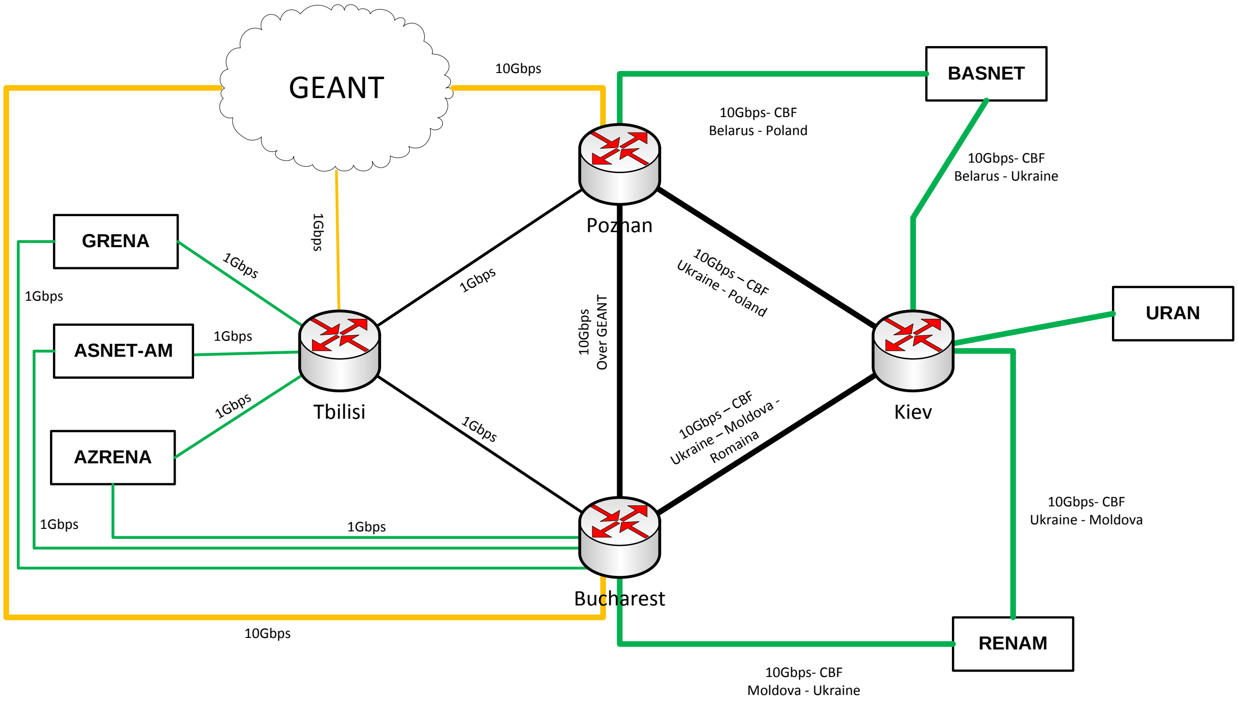


Figure 1. Regional network architecture for EaP countries

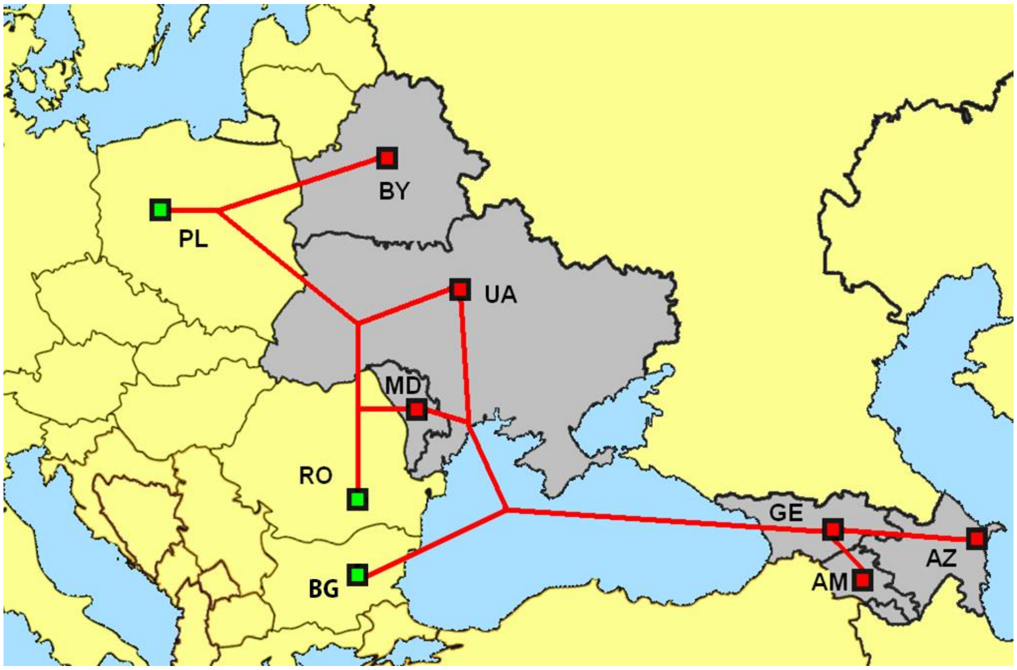


Figure 2. Geographical scheme of optical connections for EaP countries

As the kernel of the North to South optical arcs in the project considering creation in the western part of EaP region several CBF connections between EaP NRENs and optical links to neighbourhood NRENs from Central Europe that already effectively integrated to GEANT optical backbone (see Figure 2).

For Moldova the elaborated and proposed for realization topology is important from the point of view that new CBF connections plan for realization directed towards Romania and Ukraine. Preferable optical routes for regional network connections implementation for Moldova shown in Figure 3 [7].

3. RENAM COMMUNICATION INFRASTRUCTURE DEVELOPMENT

Research and Educational networks are key instruments for access to e-Infrastructures' resources and services. It is also one of the most important supporters of e-Infrastructure development. NREN infrastructure is significantly determines ability to deploy e-Infrastructure facilities and possibility to access to modern e-Infrastructure services [8].

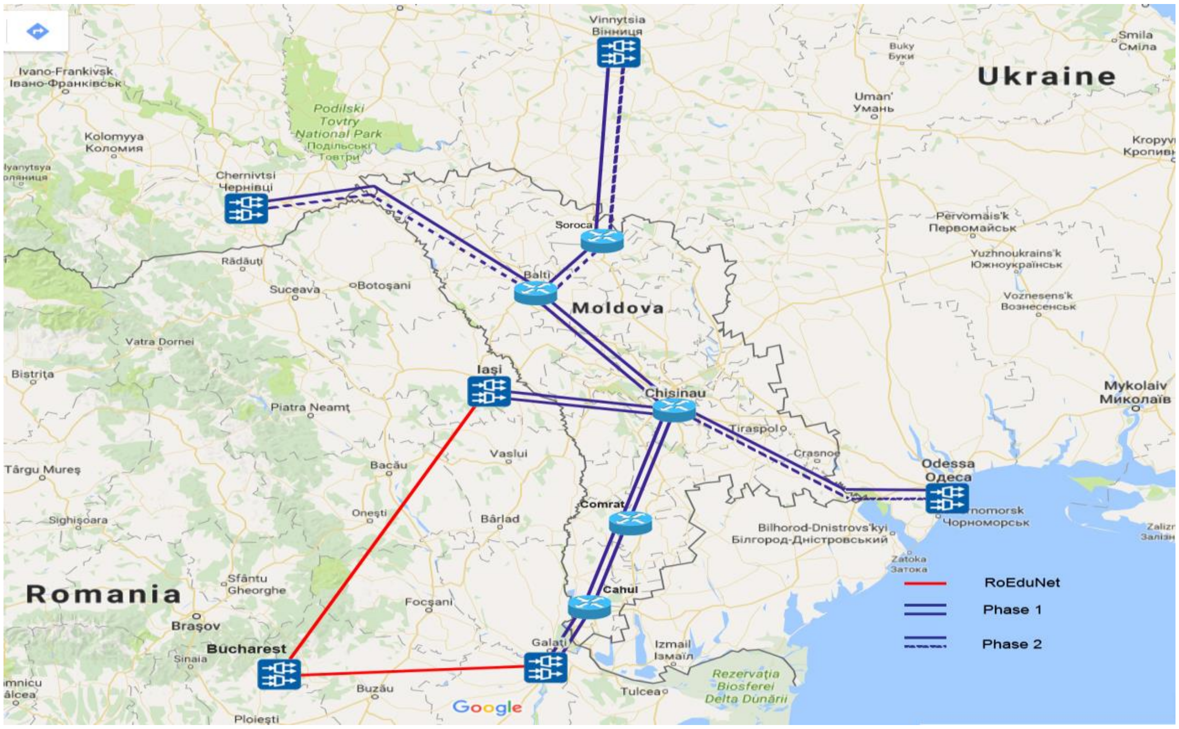


Figure 3. Regional UA-MD-RO CBF connections

RENAM internal network topology represents as a three-layer architecture [9]:

- The first level is local networks of universities' campuses, research organizations and institutions.
- The second level is the optical network for connection access nodes (points of presents, with current bandwidth 1Gbps and more) that linking local networks of research institutes and universities to RENAM network backbone.

- The third level comprises the central communication node that provides external access to the GEANT and global Internet via the main external fibre optics channel Chisinau - Iasi.

As a preferable solution for RENAM we considering further development of dark fiber based optical network that have a wide variety of network design approaches and technological choices. Such approach ensuring the fixed cost of the use of the infrastructure and at the same time provide scalability of the network grows up to Tbps capacity.

The mentioned above regional initiatives are oriented on developing of external connectivity for RENAM network. The development of external connections have to be complemented by realization of increased capacity of the national backbone to avoid creation of bottlenecks in the internal networking infrastructure.

The current infrastructure of RENAM network consists of the national wide data transmission backbone, optical backbone in Chisinau and optical channels for connection to GÉANT and global Internet. This reflects the real structure of the national research and higher education institutions location; they mainly concentrated in the capital of the country. At present existing covering of RENAM network extends to the south of Moldova (Cahul State University, State University of Taraclia) and north (University of Balti).

To eliminate the expecting misbalance in RENAM network infrastructure in 2014 started realization of new project of national networking backbone upgrading [10]. The aim of the proposed optical infrastructure modernization plan is significantly improving quality of access to the wide range of e-Infrastructure services and resources for various national users' communities. The proposed technical solution is focusing on transferring internal backbone to utilization of modern routing and switching equipment that will allow implementing new communication technologies and upgrade data transmission speed of the main internal connections to 10 Gbps.

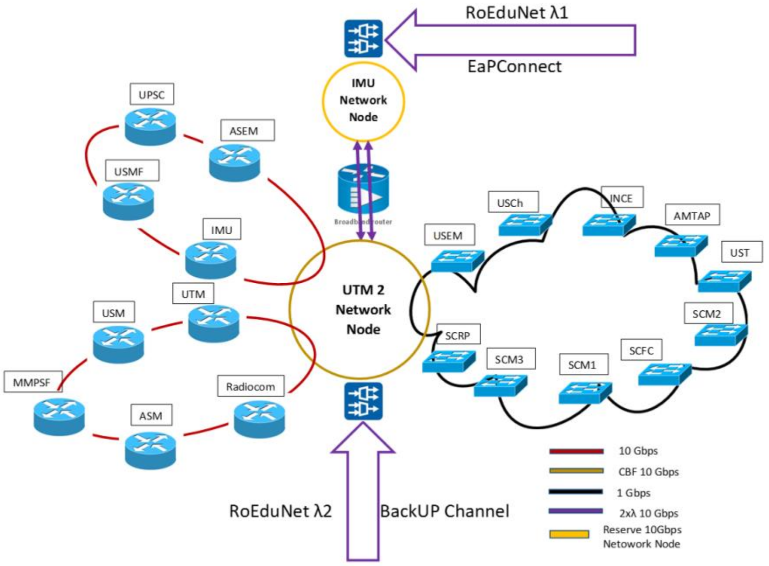


Figure 4. RENAM Network Internal Backbone Structure

The proposed and implementing now internal optical infrastructure of RENAM network represented in Figure 4 and can be considered as three optical rings interconnected in the Central communication node. RENAM Central node since 2002 is located in Chisinau in the block No 2 of the Technical University of Moldova. In this nod is also placed RENAM NOC (Network Operating Center). In the central node is operated Cisco Catalyst 6509 multi-level routing system that is ensuring external traffic distribution by using various transmission ports.

The elaborated programme of transition of RENAM infrastructure to 10Gbps transmission capacity presumes several stages of realization. New solutions of infrastructure upgrading include creation of two main reserved PoPs in Chisinau that needs to modify the existing logical structure of the network. In the existing central node (PoP1) located in the block No 2 of the Technical University of Moldova is expected to install new Juniper Core Router that will replace the existing equipment Cisco Catalyst 6509, which will be used as a basic router for the second communication node (PoP2) that is creating in the Institute of Emergency Medicine in Chisinau. PoPs in the main universities and in the Academy of Sciences will be equipped by modern Juniper and Corsa layer 3 switches and routers that support Open Flow protocols and can be virtualized to create configurable SDN networking segments.

4. REALIZATION OF THE UPDATED RENAM – ROEDUNET OPTICAL CONNECTIONS

The realization of new connections is envisaged for extending connectivity of RENAM Central communication node to GEANT PoP in Bucharest (Romania). In the elaborated technical project proposed implementation of two new CBF links as it shown in Figure 5 [11]. The final version of the solution for the optical circuits Bucharest - Chisinau realization based on use of Ciena DWDM optical equipment installed in Bucharest and Chisinau, intermediary Ciena 6500 shelfs in Iasi and Galati and implementation of joint RENAM – RoEduNet optical infrastructure management system. For ensuring the necessary level of internetwork connection resilience for creation of Chisinau - Bucharest CBF links proposed utilization of two different routes - via Galati and via Iasi.

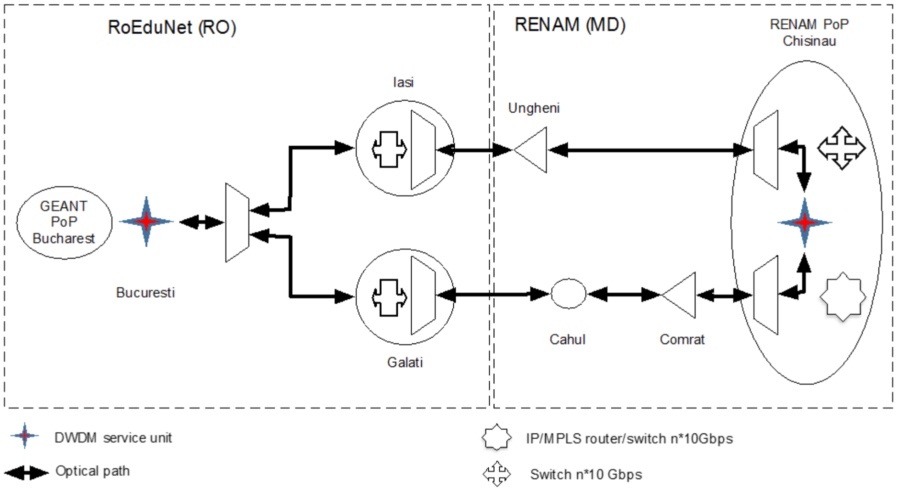


Figure 5. Logical structure of MD – RO connections implementation as a part of EaPConnect network.

The basic characteristics of the adopted technical solution are:

- Considering that the existing optical network does not have chromatic compensation - that is why selected 100Gbps cards that cope distances up to 600km;
- In Galati and Iasi is used branching optics;
- In Chisinau is using ROADM type fitting that allows access to the full spectrum; selected multiplexers supporting and offering 44 lambdas;
- Broadband cards carry 10 circuits of 10Gbps each multiplexed in 100Gbps optical channel.

In the Figure 5 are shown two parts of the joint optical infrastructure related to two participating networks – RENAM (Moldova) and RoEduNet (Romania). On the left represented RoEduNet optical infrastructure for CBF connections implementation. In the right part is shown technical solution that have to be implemented in RENAM network for the cross-border connections realization. There are two different paths from Bucharest to Chisinau for implementation of duplicated links for ensuring creation of reliable infrastructure.

The clarification of the left half of the presented in Figure 5 scheme: the cross indicates the muxponder that generates the coloured optical channels (lambdas); the trapeze indicate optical multiplexer and the rest of optical processing facilities (WSS, amplifier) in the site in Bucharest. The circles and the drawing details inside represent the optical branching processing items in Iasi and Galati where the lambdas from the optical link to Chisinau are entering in RoEduNet optical equipment.

The clarification of the right part of the drawing. In the upper path of the picture is shown the needed optical amplifier in Ungheni (represented as a triangle) because the distance from Iasi to Chisinau is too long and requiring the power loss to be compensated. For the path via Galati are needed two amplifiers (represented one as a circle and the other as a triangle) because of the long distance between Galati to Chisinau. The selected sites for optical amplification located in Cahul and Comrat. The both paths terminating in Chisinau after optical processing (amplification, WSS, demultiplexing) in the corresponding muxponder (depicted in the figure as cross).

The interconnection between RENAM Chisinau node and PoP GEANT in Bucharest will be done in two stages:

- Stage 1. Modernization of the existing Chisinau – Iasi connection – with upgraded optical equipment and extension to reach GEANT PoP in Bucharest;
- Stage 2. Implementation of the second cross-border connection to access GEANT PoP in Bucharest via Cahul and Galati RoEduNet node.

The realization of the first stage related to the path via RoEduNet Iasi node is planned to be completed in 2017.

5. CONCLUSION

During the last few years important development of e-Infrastructure in Moldova and other EaP countries has been made. Implementation of upgraded regional networking connections, improvement connectivity to GEANT Pan-European network are very essential for development of regional e-Infrastructures, for their effective integration with existing Pan-European e-Infrastructures and also for providing access to modern E-Infrastructure resources and services for national research and educational communities. Support from Governments and EC for the further development of e-Infrastructures in the region is important prerequisition for the integration of scientific potential of EaP countries in the European Research Area.

REFERENCES

1. Delivering the UK's e-Infrastructure for Research and Innovation, Report of the Department for Business Innovations and Skills, UK Research Councils, July, 2010.
2. Bogatencov P., Dombrougov M., Galagan V., Shkarupin V., Martynov E., Astsatryan A., Aliyev A., Kvatadze R., Tuzikov A., E-Infrastructures and E-Services in the Eastern Partnership Countries. "Networking in Education and Research", Proceedings of the 13th RoEduNet IEEE International Conference, Chisinau, Moldova, 11-12 September, 2014, pp. 25-30, ISSN-L 2068-1038.
3. Bogatencov P., Secrieru G. Regional E-Infrastructure and Services for Research and Education in EAP Countries. In: Eastern European Journal of Regional Studies, Vol. 3, issue 1, 2017, pp. 89-101. ISSN: 2537-6179
4. Bogatencov P., Sidorenco V., Mardare I., Andronic S., Altuhov A., Pocotilenco V., Bleih S., Savciuc I. Building of National Grid Infrastructure in Republic of Moldova. Proceedings of 6th RoEduNet International Conference. Craiova, Romania, 23-24 November, 2007. SITECH Craiova-Romania, 2007. ISBN 978-973-746-581-8. pp. 54-57.
5. Gigabit European Academic Network, http://www.geant.net/.
6. Andries A., Bogatencov P., Rusu O., Secrieru G. Regional Cross-Border Fiber Connections implementation in Eastern Europe. "Networking in Education and Research", Proceedings of the 11th RoEduNet IEEE International Conference, Sinaia, Romania, January 17-19, 2013, pp. 49-55. ISSN-L 2068-1038
7. Bogatencov P., Astsatryan H., Dombrougov M. et al. E-Infrastructures for Research and Education in Eastern Europe Partnership Countries. Computer Science and Information Technologies. Proceedings of the CSIT Conference, September 23-27, 2013, Erevan, Armenia, pp.231-235. ISBN 978-5-8080-0797-0.
8. Networks for Knowledge and Innovation. A strategic study of European research and education networking. SERENATE project summary report. TERENA, Amsterdam, 2003, 76 p., ISBN-90-77559-01-9.
9. Bogatencov P., Secrieru G., Iliuha N. Network Architecture for the Development of Scientific Computing Infrastructure in Moldova: Current state and prospects of the evolution. "Networking in Education and Research", Proceedings of the 12th RoEduNet IEEE International Conference, Constanta, Romania, 26-28 September, 2013, pp. 7-12. ISSN-L 2068-1038.
10. Bogatencov P., Secrieru G, Goncearuc A., Orbu M., Roșca P. New Technologies Implementation in RENAM National Backbone. 2015 Networking in Education and Research (NER'2015), Proceedings of the 14th RoEduNet International Conference, Craiova, Romania, 24-26 September, 2015, pp. 68-72. ISSN 978-1-4673-8179-6.
11. Bogatencov P., Secrieru G., Tighineanu I. E-Infrastructura RENAM - Platforma Interoperabilă de Colaborare, Resurse si Servicii Informaţionale in Cercetare si Educaţie. Revista de Ştiinţă, Inovare, Cultură si Artă "Ştiinţă si Inovare" (Akademos), Nr. 2 (45) 2017, Chisinau, ASM, 2017, pp. 19-26; ISSN 1857-0461.

Information Technologies in Managerial Data Analyzing, Processing and Synthesizing

Eni Natalia, Ciobu Victor, Paladi Florentin

Moldova State University, A. Mateevici Str. 60, Chisinau MD-2009
Tel.37379800700; e-mails: nataeni@gmail.com, vciobu@gmail.com, fpaladi@yahoo.com

ABSTRACT

It is presented the Information System developed to fulfill the rules of registration and roadworthiness tests for vehicles and trailers. The system is an adaptive one with distributed database. Oracle Database 11g Express Edition as distributed databases and Oracle Application Express were selected as development tools for the technical platform. The aim of the Information System is automating the process of annual technical testing of vehicles and it has been implemented at the national level.

Keywords: automatic, test, system, information, process, adaptive, database, distributed, data

1. INTRODUCTION

The main goal was to develop a national information system AutoTest (IS AutoTEST) for National Agency Transport Auto (ANTA), allowing experts to operate, maintain, adjust and develop at national level in accordance with the respective requirements legislation. The system has been implemented at 83 technical testing stations and ANTA [2].

The main objectives that led to creation of IS AutoTEST were to allow independent users to build, according to their professional interests, original versions of software called computer decision support systems (DSS) without the required assistance of IT specialists.

Management is defined as *"application of scientific method in analyzing and solving problems of managerial decision making"* and has following main characteristics [1]:

- systemic approach to decision-making situations;
- focus on adopting managerial decisions;
- decision-making on the basis of scientific methods;
- use of formal mathematical models;
- use knowledge and methods from various disciplines;
- use of ICT on a large scale.

As the IS AutoTEST platform, Oracle Database Express Edition 11g and Oracle Application Express were chosen as a development tool.

Application domains of IS AutoTEST are the support of the following processes:

a) registration;
b) technical testing;
c) on-demand search of motor vehicles and trailers, of car owners, in the field of evolutionary activity field;
d) generation of statistical reports for the governing bodies of the Republic of Moldova.

2. METHODOLOGY

2.1 Life Cycle - as a method of analyzing and designing computer data processing systems

Nowadays, elaboration of an IS of medium or large complexity can no longer be conceived without the use of analysis and design methods. *Methods of analysis and design* mean a lot of methods, techniques and recommendations used in the early stages of the life cycle of an IS, having as a final aim creation of an application model to be built.

The lifecycle of an IS represents all the steps that are taken in the development prose of the respective IS [3, p.16]. The most important stages are:

- ✓ *Collection of specifications (functional analysis)* - involves defining the problem; detailed specification of the functionality that must be supported by the application;
- ✓ *Analysis* - where the essential characteristics of all possible correct solutions are identified;
- ✓ *The design* – that adds to analyzed models new elements which define a particular solution based on certain optimizing criteria;
- ✓ *Implementation* - in which the realization of a particular solution of the executable project modeled in the design phase, takes place;
- ✓ *Testing* – where the result of implementation is verified and compared with model initially designed, and validates the fact that implementation meets the accuracy criteria identified in the analysis phase.

Each stage of the life cycle is characterized by specific activities and products resulting from the respective activities.

Adaptive methods are focused on rapid adaptation to changes. It is not exactly what will happen in the future. An adaptive team can report exactly what tasks will be performed next week and what is planned for the next month.

Predictive methods are focused on detailed planning activities over time. A predictive team can report exactly what is planned for the entire development process. The predictive team has difficulty changing the direction. The plan is optimized for the original destination and changing direction can require giving up current results and rescheduling activities. Only the changes considered important are taken into account.

The structure of the life cycle of adaptive applications is shown in Figure 1. From the figure it can be seen that the development of adaptive applications is as original life cycle, which combines the advantages of the life cycle of the *"cascade"* with type *"agile"*. Steps 1-7 correspond to the life cycle of *the cascade,* and 8-10 correspond to stages of the life cycle *"agile"*.

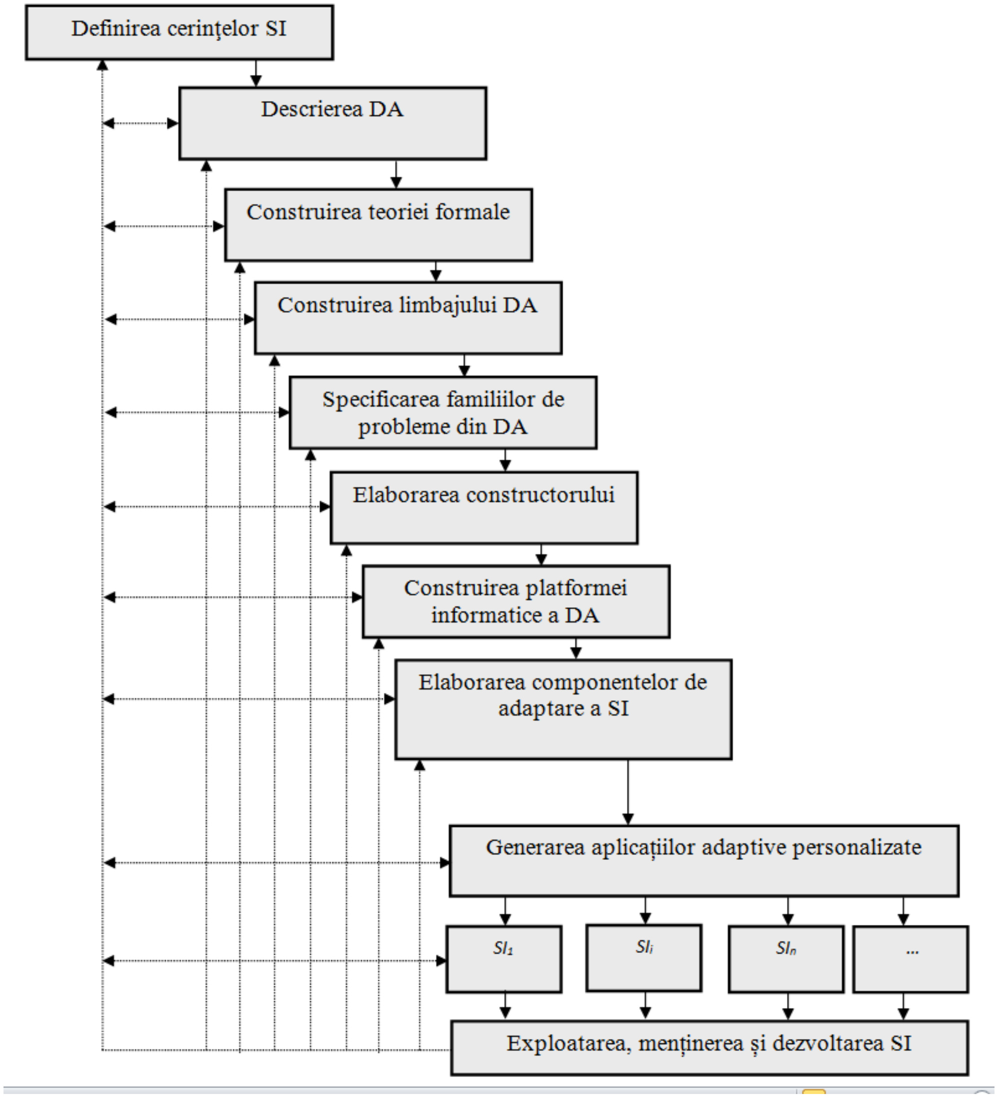

Definirea cerinţelor SI
Descrierea DA
Construirea teoriei formale
Construirea limbajului DA
Specificarea familiilor de probleme din DA
Elaborarea constructorului
Construirea platformei informatice a DA
Elaborarea componentelor de adaptare a SI
Generarea aplicaţiilor adaptive personalizate
SI_1
SI_i
SI_n
...
Exploatarea, menţinerea şi dezvoltarea SI

Fig. 1. Cycle of computer systems life.

3. DESCRIPTION OF IS AUTOTEST

3.1 Functional description of IS AutoTEST

Testing of transport units and trailers shall be carried out during the calendar year. For public passenger transport units and transport units of dangerous goods, mandatory technical testing is carried out every six months. For other types of transport units, mandatory technical testing shall be carried out once every 12 months.

The applicant (the individual accompanying the transport unit (TU)) addresses any technical testing station in order to perform the technical test of TU.

The following actors participate in the technical test (see Table 1):

Table 1. The actors of the technical testing process of TU

Nr. d/o	Actor's name	Description

1	Applicant	Initiates TU testing;
		Accompanies TU;
		Holds the entry documents.

2	Registrar	Records the applicant's request;
		Identifies TU and TU owner;
		Ensures data entry.

3	Tester	Accompanies the TU at the test station; Provides the collection of technical test parameters.
4	Expert	Takes the decision on the technical state of the TU; Releases the technical verification report of TU and the technical verification hologram.
5	Statistician	Generates current, analytical and statistical reports.

When addressing, *the applicant* shall submit testing station set of documents:

$$D_{Inpu} = \{D_{input}\,1,_{inpu}D2,_{input}D\,3D_{inpu}\,4,_{secto}D\,5D_{input}\,6\} \qquad (1)$$

where

- $D_{input\ 1}$ - identity card (for individuals);
- $D_{input\ 2}$ - copy of registration certificate of the company (for legal entities);
- $D_{input\ 3}$ - registration document transport unit;
- $D_{input\ 4}$ - delegation or other document certifying the rights conferred on the transport unit;
- $D_{input\ 5}$ - certificate on compulsory insurance of civil liability;
- $D_{input,\ 6}$ - a receipt confirming payment of the amount of testing and road tax.

IS assists the *registrar* to enter personal data about the owner of TU, data of the TU responsible person and information about TU. The introduction of these data can be both manual and automated by online extraction of data from State Registers. The Registrar of the State Register of Population (RSP), the State Register of Law Units (SRLU) and the State Transport Register (STR) is the state enterprise

"State Information Resources Center" REGISTRU"". At the automatic extraction, *the registrar* compares the data extracted with one from presented documents.

The procedure of extracting data from the State Registers must comply with the Personal Data Protection Legislation.

Tester places TU on the test platform and initiates the procedure of testing the technical condition of TU. At the same time, it ensures the automatic input of the data obtained from the platform in the information system. If the test platform is unable to transmit data automatically, *testator* manually enters this data in IS. During TU's positioning on the test platform, the automatically processed picture of TU is taken.

Expert analyzes the documents D_{input} and data about testing the technical and decides whether the TU can be safely operated on the public roads. This decision is introduced in IS Astfel, that is de facto a decision support system (DSS). Based on positive decision, the *Report of technical verification* with a *badge hologram* is issued for *the applicant* under the strict registration.

However, the printed number of the report is introduces into the system and is associated with all the documents of $D_{input.}$ The technical report after the stamp is applied is given to the *applicant* and *the* hologram badge shall be sticked in right bottom corner of the inside of the TU windshield from the inside part or for new registration plates – at the established place on the panel. In case of identifying technical defects *expert* cancels previous decisions on the UT and prohibits its operation thereof or indicates a period of 30 days to liquidate defects.

The functional model of the actor IS "AutoTEST" is shown graphically in Figure 2.

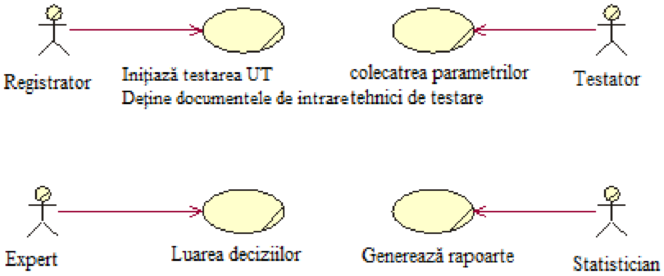


Fig. 2. The functional IS "AutoTEST"

3.2 Functional diagrams IS "AutoTEST"

IS "AutoTEST" has been designed according to the combined methodology of lifecycle methods of *"Cascade"* and *"agile" types* and technical regulation "Lifecycle processes of software" [4] taking into account the information flow analysis.

IS is characterized by the ability to compensate structural changes of the driven object. This is due to designed on-line management strategy that is based on a mathematical model or the most complete information about the process [5].

Strictly important is not to introduce into the system structure limitations that will not allow for an on-line change of leadership strategy. IS integrates a family of processes organized on hierarchical levels that actualizes on a computer the whole range of documents related to these processes (see Table 2).

Table 2. The functional and adaptation levels of IS AutoTEST

	Documents	**Processes**
Central level, *conducted by ANTA*	- classifiers - authorizations (stations, experts) - document types - normative parameters - etc.	- the accumulation of data from the entire adaptive information system; - interconnection with other institutions; - adding and removing nodes; - initiating the deployment of new modules; - generating different statistical reports
Local aggregate level, *carried out by the aggregate test station*	Documents Processed / issued by All Subordinate Stations: - technical status report; - certificates (CEMT, INTERBUS, ADR, CEMT); - technical parameters of vehicle; - picture	- data accumulation from subordinate stations; - interaction with subordinate stations; - initiating the right timing of the synchronization act; - deploying new versions
Local level, *carried out by the Ordinary Testing Station*	Processed/Issued Documents Only by Current Ordinary Station: -the technical verification report; - certificates (CEMT, INTERBUS, ADR, CEMT); - technical parameters of vehicle; - picture	- obtaining technical test and vehicle photo data; - input and accumulation of data from current ordinary stations; - interaction with other institutions on the territory of the station (commercial banks and insurers); - initiating the right timing of the synchronization act; - deploying new versions

At the central level, data exchange with external institutions is achieved through *technology web-service*, the protocol SOAP (see Figure 3).

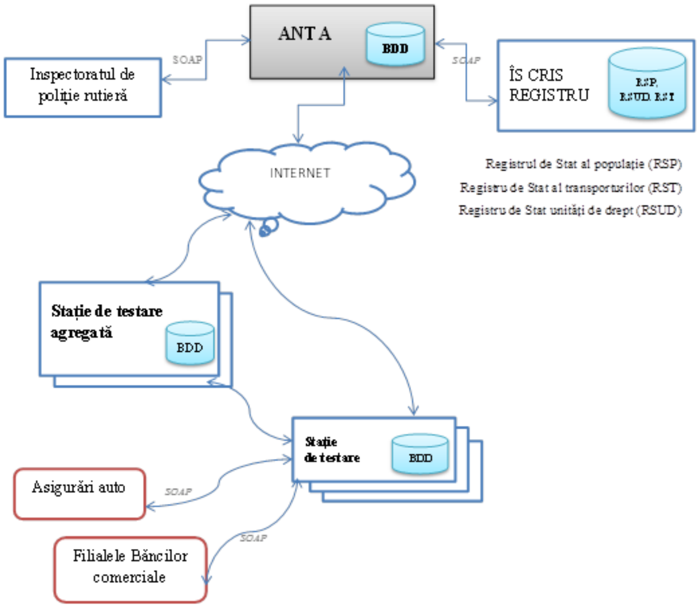

ANTA
BDD
SOAP
Inspectoratul de poliție rutieră
SOAP
ÎS CRIS REGISTRU
RSP, RSUD, RST
INTERNET
Registrul de Stat al populației (RSP)
Registru de Stat al transporturilor (RST)
Registru de Stat unități de drept (RSUD)
Stație de testare agregată
BDD
Stație de testare
BDD
Asigurări auto
SOAP
SOAP
Filialele Băncilor comerciale

Fig. 3 Fig. 3. Diagram of information flows IS AutoTEST.

For the local level of IS AutoTEST, the flow of information is shown on the figure below.

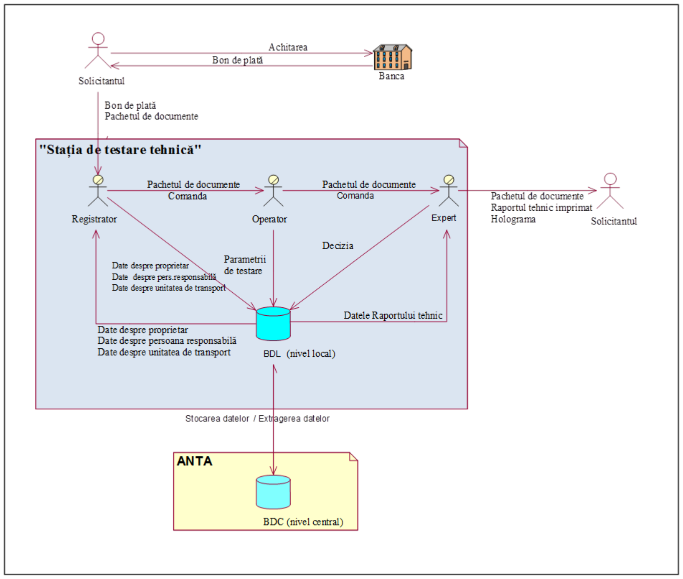


Fig. 4. Chart information flows at the local level (at the test station).

Viewed from the perspective of mathematical logic DA "AutoTEST" represents a formal (axiomatic) theory in the sense of Mendelson. The finite alphabet of DA's formal theory "AutoTEST" represents the basic concepts of this field.

Recall that a formal theory (axiomatized) of an activity is defined by the following components: *alphabet finite set of expressions* - the set of words finished over this alphabet, *the set of formulas* - a subset of the set phrases and *set of axioms* - a subset of the set of formulas, *set of inference rules.*

<formal (axiomated) theory of DA "AutoTEST"> :: = (1)
< DA alphabet "AutoTest">
<the set of finite words over the DA alphabet "AutoTEST"> |
<set of DA formulas "AutoTEST"> |
<set of axioms YES "AutoTEST">
<set of inference rules YES "Autotest">

1) *<alphabet DA "AutoTEST">*
::= (2)
{<ST>
<ANTA>
<ST associations>
<input frames>,
<technical test reports>,
<statistical reports>}

2) Many words finished over alphabet specified in (2) represents universal sets of RS, frame inputs of technical and statistical reports. These sets can represent, for example, adaptations of IS (Generic) Auto Testing in different countries.

3) *<the set of formulas over the DA alphabet "AutoTEST"> :: =* (3)
<universal RS set>
<universal set of input frames of AutoTEST>,
<universal set of AutoTEST output documents>
IS "AutoTEST" is adapted to the conditions of the Republic of Moldova.

4) The set of axioms:
RS "AutoTEST" is a dynamic object, the structure of which evolves over time.
So,

$$RS=\{ RS^{(1),} RS^{(2),} ...,R^{(k),} ...\} \quad (4)$$

where

$$RS^{(i)} = RS (t) \text{ and } t^{(i)} \leq t \leq t_{inc}{}^{(i)}{}_{fine}$$

In the set of axioms, the set of valid registered documents is also included.

5) The set of inference rules is performed on the computer by the IS AutoTEST modules.

6) In the context of the formal theory described in the test reports and statistical reports obtained using inference rules, they can be seen as theorems of the formal theory of DA "AutoTEST".

Based on the formal theory described, IS AutoTEST was developed.

The IS AutoTEST database

Referring to the adaptive IS database it is a strictly necessary condition to maintain as much flexibility as possible of the chosen architecture. When the organization is geographically dispersed, there are two options of database selection: *one centralized database* or *a distributed database.*

A *centralized database (CDB)* is a collection of data on a single node of a computer network. A *distributed database (BDD)* is a distributed shared database that is physically distanced on the nodes of a computer network.

Generally, it is possible to develop an adaptive information system with both a centralized database and a distributed database. But, if the deployment objects are geographically dispersed, an adaptive IS with the BDD is more appropriate due to the fact that information objects are provided, even in the case of computer network interruptions. A distributed database management is performed by a *management system of a distributed database* (DBMS), which is able to operate the database with a DBMS centralized similar to [6].

BDD are divided into two classes: *BDD homogeneous,* in which all nodes have a soft, a structure of the interface and of an identical database; *BDD heterogeneous,* which can have different DBMS models and database structures, interfaces and different software.

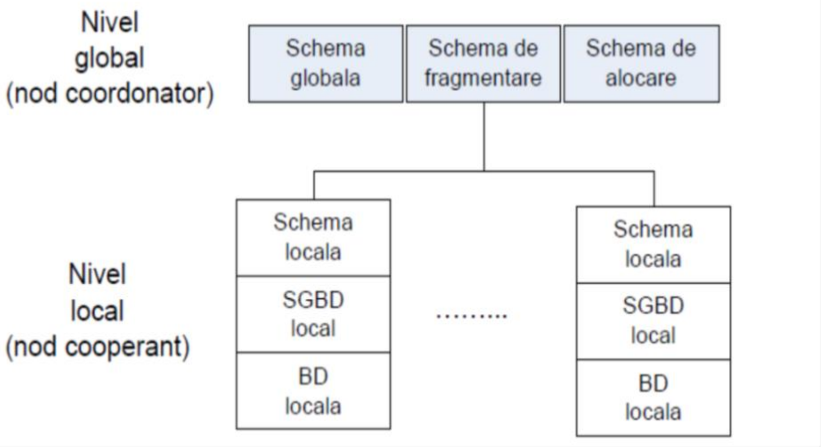


Fig. 5. Architecture reference for homogeneously distributed DBMS.

As a BDD the BBD homogeneous was selected (see Figure 5). The reason is that the developed information system must be robust to possible problems with the network, effort and, finally, the cost of development and implementation must be optimal. We note that each implementation object is a separate private institution with its own computer technology and with a degree of decisional autonomy.

In homogeneous BDD *data dictionary* and *objects structure* are identical for all nodes and data are fragmented by the adaptive copy. This adaptive process of copying data is called *actualization (copying in one direction)* or *synchronization (copying in both directions)* of the data.

Information flows within the information system are carried out by the mechanisms developed to synchronize the BDD.

The IS AutoTEST database, ANTA level, consists of 57 tables and 9 representations. Local database consists of 47 tables and a representation.

According to the functions fulfilled, the tables can be divided into three families:

- Factual tables;
- Classifiers;
- Service tables.

BDL has relational architecture and was designed in the third normal form.

Oracle database contains a procedural language that allows modern and execution algorithms needed within the database as *procedures, functions, packages* and *triggers.*

Below we explain the most relevant modules of IS AutoTEST.

4. RESULTS

4.1 Web applications of IS AutoTEST

Web application is a collection of Web pages in a single security designed to solve a problem.

It would be natural for each employee to have a single web application to perform the job duties.

To find out which Web applications we need, we build the process-to-table table (after the organization's generic structure) with the framework processes of the information system (see Table 1). *The applicant* is not an actor of the information system, because he is a recipient of the service test. For other information systems, especially for on-line services, the beneficiary may be a system actor.

The organizational structure of both large stations and small stations was studied at the design stage. Some stations observed a merging of functions of the *Registrar* and *Tester* players in a certain role actor. Therefore, it was decided to create actors *Registrar* and *Tester* one Web application that finally was called by beneficiary *"AutoTest"* with internal ID 162.

Expert's web application actor system due to the management functionality and decision making at the local level was named *"Administrator"* with internal ID 164.

Web application for actor *Statistician due to its* functionalities to generate statistical and analytical reports on a local level, was named *"Reports"* with internal ID 163.

This application is also used for the central ANTA level with internal ID 100. The difference is the data source, centrally operated with data from all stations.

The algorithm validation is a logical expression linked to a web page that is checked after filling the fields on the page by the final user. This algorithm is associated with a final-user error message that is displayed on the Web page.

Next, the main adaptive decision elements on the web interface of each of these three applications will be displayed.

Table 3. Relationship between IS "AutoTEST" actors

Actors Processes	Registrar	Tester	Expert	Statistician
P_1 - registration of the test order	✓			
P_2 - testing technical condition of UT		✓		
P_3 - extraction data from State Registers	✓			
P_4 – TU photographing		✓		
P_5 - verification and validation of data			✓	
P_6 - print the Report of technical verification of the TU			✓	
P_7 - saving data in BDL			✓	
P_8 - cancellation, doubling of Report of technical verification of TU			✓	
P_9 - managing final users (see (3.2))			✓	
P_{10} - System configuration			✓	
P_{11} - manually synchronization of BD			✓	
P_{12} – installation of new versions			✓	
P_{13} – generation of reports				✓

5. CONCLUSION

IS AutoTEST was designed and conducted to ensure the principle of *data mining as the* examined information must be *complete*, *current* and *accurate*.

Complete and current qualities of information are accomplished through online communication and pooling of data from the central node of ANTA. Transactional *consistency* mechanism is performed on each document, provided by Oracle DBMS.

Veracity of information is ensured by the multiple conditions of validating forms of information entry with the extensive use of classifiers.

It is required in the perspective of implementing predictive forms with cognitive validation methods.

REFERENCES

1. Filip F. Decision Support Systems. Ed. II, rev. Bucharest: Technical Publishing House. 2007.

2. Ciobu V. Develop national information system adaptive process automation technical testing of vehicles, the scientific journal of the State University of Moldova "Studia Universitatis Moldaviae" (series information). 2 (82) 2015, pp. 3-9., pp. 3-4.

3. Langer A. Guide to Software Development: Designing and Managing the Life Cycle, Springer-Verlag London Limited, 2012, 350 p.

4. Order No.78 of 01.06.2006 on approval of the technical regulation "processes lifecycle software" RT 38370656-002: 2006 "" Official Gazette published. 95-97., Particularities of Implementing IT Projects in Tax Administration https://servicii.fisc.md/Press_Releases_List.aspx?id=

5. Dumitrache I., Peter E., C. Wicks Automatic volume II, Romanian Academy Publishing House, Bucharest. 2013. pp.390-391.

6. Cârştoiu D. distributed database systems. Conspress Publishing House, Bucharest, 2013.

Analysis of the Economic Information Systems' Organizational Forms and Units Functioning Evolution

Leahu Tudor, Perju Veaceslav

Free International University of Moldova
Vlaicu Pircalab Str., 52, Chişinău, Republic of Moldova
leahu.ts@mail.ru, vlperju@yahoo.com

ABSTRACT

The essence and content of some fundamental terms of the general and applied informatics, the latest regarding to the economic informational activities, are cleared up. It confirmed the correctness of the application of these terms, their scientific and practical importance in development (advancing) of the investigations and efficiently daily working of economic informatics systems (E.Ic.S.). All these it refers mostly to the organizational stage of the unitary informational process of the economic management system. In this regard are highlighted and analyzed the evolution, notions, premises and trends of development of the organizational forms and units what ensuring the daily functioning of the E.Ic.S.

As one the most progressive at one and in immediate prospect is formulated a variant of the notion of the data bank (D.Bn.) - internal informatics organizational form, the factors, what are contributed to it constitution and working. Are distinguished the trend of final evolution of this bank.

Keywords: analysis, informatics, evolution, organizational, form, unit, functioning, economic, system, data, bank

1. INTRODUCTION

At present is characteristic the massive infiltration of the specialists of miscellaneous news professions in informatics sector. Such phenomenon contributing, on the one hand, to the pronounced dynamics of the technical – scientific progress in any sphere of human activity (material, spiritual, informational), but on the other hand, creating the complex problems of genuine communication between various categories of designers and users of the informatics resources.

At once and in forthcoming future it's ruling the fact that the projection, putting in functioning and ensuring of the efficient daily working of any informatics system on the scientific basis can't be effectuated without specialists as the diverse personnel of the informatics technical service, programmers, technologists, mathematicians, office workers of administration of economic unit, economists, lawyers, etc. Each of these users possessing the varied basic studies, qualification level and professional language. The many objective (insufficient informatics studies, ignoring of the role of scientific knowledge, etc.) and subjective factors (capacity of feature, low interest given the new more efficient and productive means and methods, etc.) are caused to the formation of one informatics amalgam language. As a consequently, at present increasingly more it observing the shallow attitude to the formerly exactly formulated terms, addressing to the others news, invents denominations through loan from the vocabulary of basic non-informatics studies of specialty. Moreover, some “authors” of this approach considering and doing exceedingly the advertise of so – called “modern terminology”, being appreciated right innovative and of the superior performance.

The formed juncture has become acute perceptible once with direct physical access of any user to informatics technique, especially at the electronic personal computers (E.P.C.). To the creation of such of state are contributed the solution of constitution and functioning of the local and global computers networks.

Their two basic, but and the subjective, factors in the making decisive during the evolution of computing technique, have produced the erroneous impression not only end users (functional employers), but and investigators and designers of the economic informatics domain, to the effect that all informational activities or most of them are entirely automated, and in some cases – fully automatic, which are far truth. That is why in last decades increasingly evidently are observed the neglecting, forgetting, substituting, mangling of the essence of content of one part of the fundamental informatics notions.

Regretfully, such attitude has become traditional and practice encouraged at the majority of professional creators of economic informatics systems (E.Ic.S.) and their end users (functional workers). The single justification advanced of they consist in that to the effect that the respectively term is rare or no longer apply in the daily professional language. Moreover, often one and the same content is expressed by different terms, so tuning is considered as advancement.

The created situation was formed in the first place as a result of that fact from the outset some terms have been formulated not so clear, precisely and entirely of the investigators and practitioners of computerization domain. About this, the discordant development of the resources of automatized (automatic) achievement of functioning of the domain has led to the advancement of the terminology of some at them, at others – it stagnating.

Conventionally, these two conditions can being considered rightly objective, but subjective factor also is at the decisive role. Because of rapidly progress of informatics components, especially, of the hardware and software, the human society was taken by surprise regarding the training of the different categories specialists, the last (diversity) is caused by sinergical and varied character of composition of the resources of elucidated sphere. As a result, was place the massive infiltration in the examined domain of many practitioners and researchers, uninitiated neither in informatics, neither in area of the application. Regrettable is and getting of the high scientific degrees of the such ”specialists”,

Subsequently they are permitted, through dictate and not through rightfulness, the introducing at the terms, what is referring more at the realm of available basic higher education. Through this it and explained the vast spreading of dilettantism in the practice and theory of the general and, mainly, of the applied informatics.

The enumerated circumstances and other events, at what it reached and possibly one wait coming, has created a state of the total chaos, mainly, in the economic informatics, it being conducted by the scientists of mathematical, technical, physical and another not informatics or economic studies. At the same time, it is well known that the possession and operation with a perfectly, profoundly, rational established vocabulary, is impossible at obtained a lot of knowledge and durable practical skills in certain activities. With this occasion, it requiring the education, establishment and maintenance of a professional culture thanks of handling with a adequate terminology of constituents of the aria of concrete preoccupations. Therefore, any success can be achieved primarily through a firm mastering a authentic vocabulary.

The correct and full approach of the essence and comprehension of terminology allowing not only to penetrate in the meaning of the concept, but also to accumulate the crowd knowledge about origin, existence and evolution, to predict the trend of the events of the domain of objects.

All those analyzed so far has required the formulation a unitary vision concerning at the fundamental informatics terms, the evolution and trend of the organizational forms and units of functioning of the economic informatics systems (E.Ic.S.), which as well as many others, affiliated of the informatics area, not was spared of different unseasonable interpretations.

At the same raisons it available of decency to meditate not only concerning correctness of the substance, sense and completeness of content of economic data banks, of going to reach them, but and their final perspective. In the milieu of the considerable volumes and compound composition of information and works exerted concerning them, it requiring the necessity to create the certain organizational premises with a view to facilitate the calculation and uncalculating transformation (processing) of initial data values.

The increasing of the promptness of processing, of the quality of obtained in they result informational products at the technical means, effective methods and procedures, but and the most rational forms of data organizing and organizational units, which ensuring daily working of the E.Ic.S. The firsts is considered internal, the seconds – external.

The forms of data organizing are considered right internal, because they are not achieved on the milieu of supports. Their functioning to depend on the category of latter, the physical (chemical, biological, etc.) features and possibilities methods data organizing on their space. At the same time, the organizational units are deemed as external, since they themselves to referring to the daily organizing, in interconnection and interaction, of all resources (human, technical, technological, etc.) in the shape of the unitary ensemble, what manufacturing the informational products.

2.EXISTING SITUATION CONCERNING SOME FUNDAMENTAL NOTIONS OF GENERAL AND APPLIED INFORMATICS

After how was said, now for examined domain is unjustified the replacement of each individual with a single general term. Thus, by the terms “informatics”, it substituting any term of the constituents – “program”, “technique”, “technology”, “information”, etc. Through this is misled not only the end users, but the designers and producers.

In our opinion, for to avoid this state of things, it calls the determination of the distinction between the notion of the “informatics” and them constituent resources, the lasts being named with them concrete denominations.

Identically don’t it do the distinction between the terms of the ”general informatics” and “applied informatics”, often mistakenly replacing one on another. The correctness of their application demanding first of all, as it can possible, to establish them authentic and full content. Starting of this finding, would be, as in the first place it be determined the content of the universal term, at the philosophical order of informatics, then – of a terms “general informatics” and “applied informatics”.

So, in universal aspect the informatics it presented in the shape of the branch of human knowledge and skills, their administering contributing to the obtaining in the automatized (automatic) way in the first stage – only informational, and the final stage –of material, spiritual products.

However, the notion of the “general informatics” is of the compositional order, including in self any means and methods, suitable for the one certain physical milieu. That is why, it, as a rule, it enumerated the informatics technique, organizing, structuring and physical processing of information as data, as well as the programming. Therefore all the resources and processing are attached to the physical (biological, chemical, etc.) environment of their working. In this interpretation, the universal informatics derived from the human capacities, while the general – from technical “possibilities”.

As concerns “applied informatics”, it refers to the involving of the resources of the general informatics in the sphere on the human specific branch preoccupations (economics, technique, medicine, law and so an). In such manner, in the given plan, can be distinguished the enough varied of informatics – economic, technical, medical, legal, so on as many subject preoccupations.

Certainly, and in applied informatics all is adapted to the technical physical entourage, but permanently taking into account of the strictly respecting and keeping of logical meaning of the processed informational units. For this reason, if in general informatics it operating expressly with physical notions, then in the applied – by combining the physical with the functional (of concrete, real), considered as virtual (imaginary, analogical of those physical) notion. By such circumstances and it explaining the formation, existence and manipulation with the terms of the unitary denomination, but the two contents - physical and logical. The first of the later usually is operated by the builders and technical exploiters, by the logical content have – do prevalent the technologists, programmers and end users.

Referring the clear distinction between the various informatics professions languages, and necessity in daily organic pressing collaboration among them representatives, with a view of maintaining in state of the performance of this collaboration, in every time it fitting and specified: what kind of data file, collection, base, etc. it's in examination – physical or logical? This indication is important for any user, because it concrete describing the specifically variety of data structural unit – constructive or functional.

At the point of view of the origin and evolution in [4,159-160] is specified that the term "informatics" is a French neologism, introduced in 1962 by Philippe Dreyfus and formed by combining of the words "information" and "automatique". Also, here the informatics is considered as ensemble of organizational, technical and socio- economic knowledge of the scientifically order, destined for automated (automatic) processing of the information.

In 1967 the French Academy has defined the "informatics" as being the science of rational processing of the information, especially using the automated equipment. However, in English, the examined term disposing of such synonymous as "computer science", "data processing", "information technology".

In our opinion, the French definitions more authentic comparative with his English synonymous, because it including and symbolizing the principal two components (information and automation), without the others (computer, processing, technology) and would lose it's sense and therefore are them derivatives. Then, such term will be advisable for any informatics professional terminology of anybody professional language. More so that, in English it's present the term "informatics"[4, 162].

In the same source, at the most generalizing level, it distinguishing the five areas of informatics: theoretical, physical, technical, methodological and applied. Still are distinguished and described of board, departmental, distributive, graphic, images, industrial, mobile (nomadic), strategic and scientific informatics, itself who names are situating in the domain of application. However, the majority of them are referring to the material processes and only those scientific, banking, stock exchange and juridical – to the informational.

Regretfully, not – has founded its place the term of the economic informatics, which being out it considered right domain, very much as it including (covering) any material or informational human activities,. It's of the most largest social character, regarding to the every of production, distribution (commercialization) and consumption of material and spiritual goods, at any management level – from the each individual until human society.

That is why we think that the economic informatics is present wherever and whenever, permanently feeling the need in it. This and justifying the highlighting in her framework the two sub-domains: economic material informatics (production, trade, consumption) and economic informational informatics (standardization, regulation, forecasting, accounting, analysis, formulation and taking the decisions).

Another informatics term of general order is the “informatization” (computerization), under he it understanding “the process of automation of various parts and charge of the enterprise ”[4, 162]. Such interpretation is not too successful, because as such the informatization had, has and will place not directly through automation, but and manual. Anything else that at once because of objective well known reasons even more insistently one requiring it application.

In this regard it would be more adequate “informatics achievement”, which would reflecting the fact that the informational and material processes are fulfilled in informatics mode, not without fail automatically and entirely, but by different informatics means and technological methods of this category.

The last period it characterized and by massive application of the term “informational technologies”, which also requiring the certain concretizations, since everywhere it understanding them achievement by technical means, what not always it’s correctly. In this connection we mentioning that the informational technologies can be realized entirely manual, partly automatic, partly manual, while the informatics – totally automatically. The lasts are considered internal, being realized in the physical environment of the technical means.

A separate clarifying requiring and the notion of involved technique in any informational act, in the practice and theory massive nominated the “computing technique”. This notion is of long – expected to be analogized with the unitary informational process, which consists of three stages: initially (primary), processing (informational, structural, of calculus) and of use. Each of that stages including lots of operations and procedures, what need to be accomplished by technical means.

For the mentioned reason, it’s would be more authentic the term “informatics technique” that would including such of it categories, as the primary data (of extraction, recording, multiplication, transmission), processing and of utilization (values analysis) of informational units.

Incidentally, it comes out that starting from the existent level of classical and technical sciences, the integral informatics achievement in fullness of the unitary informational process can be achieved on the next two basic directions:
1) by creating and implementing the technical means for each operation of the unitary informational process;
2) by equipping a one technical mean with all necessary devices for to fulfill in interconnection all the processing operations of any issue information..

Until with more successful it’s noted a some progress out the second direction. Thus, E.P.C., as a part of the structural and calculus processing, more fulfilling and the procedures of data storage, transmission, at distance data exchange, data analysis, etc. In this context would be welcome and the substituting of the term “computer network” with the “informatics network”, the first being just of technical contain, while the second it’s of the procedural nature and, therefore, more near and analogous of named informational process.

In majority, any economic activity, being material of informational, it’s achieved by many performers, through involving in interconnection and interaction of different resources. That is why iy soliciting them systemically approach, both organizational, and procedural point of view. In this case, any massive and compositional varied information are required to be organized in the shape of system.

In the area of the economic informational processes it distinguished three basic notions: “system of information”, “informational system” and “informatics system”. The first including express the according the certain criteria systemically organized informational entities, the second – not only these entities, but and the technical and manual means and technological methods of them processing, while the informatics system foreseeing the entirely automatically achievement of the informational compartment of the unitary management process. Because insufficient informatics achievement of the data initial and utilization stages, in the economics all these systems are informational.

3. THE EVOLUTION AND PROSPECT OF THE ECONOMIC INFORMATION SYSTEMS ORGANIZATIONAL FORMS DEVELOPMENT

On the route of its evolution, the forms of organizing of the named information were in predicted perspective will be constituted in base of the two categories of supports – manual and technical. In case of the manual, when all procedures and operations are performed by the subject, the information is organized in different ways, the latter being conditioned to them functional categories and predestination. So some of the information is organized as a card index (card index of the primary evidence), another part – in the ensembles of the folders (dossiers), ring – books stored in the shelves, in planks, etc., as well as and in shape of various lists with reference data, prices, rats, etc.

The daily organizing of the information fixed on the manual supports to taking place individually, at each job and depends of the composition and specific features of solved problems, in what this information is involved, of the possibilities of placing of the supports in relation to them place of processing. The long keeping of information on the manual supports requiring the preliminary elaboration and organization to the one well – built and reasonably made scheme, what mast itself being concretely known and on this basis – involved in various purposes for respectively users.

At mentioned red – handed that the organizing of the information in the manual version, after all, it reducing of the organizing of the supports, on that itself containing. In this connection itself imposing the recording of multiple times at the same data values in the sets of the documents, as in basis of these values occurring the recognition (identification) of the ownership of the informational entities and them structural and informational processing.

Also, and the values of the attributes physical are separated each from other, but the original order of them placement on the support, usually, not always it's concordant with all necessary variants for them processing. For example, of such ways of organizing of information can serve the forms of the account memorial – order and log – order, the linear foreseeing, etc.

In event of applying the informatics technical means, the fund of the information of leaded object can be organized in the shape of card index, bobbin (reel) index, diskette index, hard disk index, etc. As and for the manual supports, the card index, organized in base of the perforated cards and bands, respectively of the cardboard and of the paper, the logical organization totally depends of physical specific features of these media. Regarding the supports with magnetic properties, this thesis is fair only for the bobbin index.

The data logical organization on the packs of the hard magnetic disks and C.D. packages, as well as on magnetic cylinders (drums) and cards to a certain extent is become independent of the physical properties of these media, which allowed to be elaborated and to bring into operation such new organizational modality, managed in programmatically mode, in the form of database. The last essentially it distinguished on the manual organizational forms and on the others informatics forms at this type through fact that the location and processing (transformation) of values of the informational units it occur in automatically mode on account of the elaboration and functioning of them management system under form of the programs complex. Simultaneously, such system does not exclude, but presupposing the application of the magnetic bands, on which can be located all the information with the variable values.

Off the positions of the programming management, the forms of the organization of information created in base of the documents, perforated cards and bands, presupposing the compulsory involve at the subject and therefore for their milieu aren't features the manual manipulation data.

The application of the organized on the basis of the technical supports data processing systems has created the conditions for achieving of such new forms of the organization of the administration of economic informational activities, as the organizational forms of card – tabular the book - keeping automated tabular, automatic (electronics), as well as the forms of the forecasting, analysis, etc.

The previously elucidated technical forms of data organizing has evolved in the following stages of logical data organization: data elements (elementary, primary units) → separately data files ensembles of the data files → data collections → database of managed → object.

After how were, at the initial stages underlined above the composition and the volume of the information, as well as and the supports, and the base of them were organized, not allowed (sometimes this neither not require) them organizing on the supports in shape of the informational entities of great volumes. Latter on such necessity it becomes more acute. Once with this has been established the conditions in order such necessity must be satisfied by means of the informatics supports.

The creating of databases and them application in practice of economic informational activities confirms the fact that in perspective most effective will be those forms of data organization, the logic of them elaboration and functioning don't will depends of physical specific of the support.

The elucidated so far confirms the fact of the trend of performance evolution of economic informational systems through gradual transition from centralized to the distributed informatics systems. That transition is composed not only by the necessity of achievement of the informational connections between objects of diverse hierarchical levels, as well as and of the constitution a unitary informational base for the national economy, but and the development of the advanced technique.

The created situation it contributed to the idea of passing from separately databases to the distributed databases system. The final goal of those distributed consists in achievement of database it producing concordant a data model of certain category (hierarchical, reticular, and relational). In most cases, as a rule, it resort only one type of model, particularly if it is a superior generalized level and through its agency can be achieved other models.

For example, in the current economic informatics activities mainly it operating with relational databases, which, in our opinion, is not justified, as it requires the news interfaces and complicating the process of the problems solving. At given raison most effective would be the use of the reticular model for the achievement of the connections between data flow belonged different management levels – the hierarchical models, etc.

Therefore, the unitary database of entirely managed object must be constructed according to various types of data models, very important remaining achievement of the interconnections between various data models of each compartment of database.

4.TREND OF THE ECONOMIC INFORMATION SYSTEMS ORGANIZATIONAL FORMS EVOLUTION AND DEVELOPMENT

The efficiency of the financial administration of economic material resources directly depending on the quality of informational resources. This fact becoming evident in current conditions of market economy entourage, which is characterized by the decisive role of information and complexity of it composition. Such circumstances, as well as the evolution of the informatics technique has contributed to the necessity of functioning of the information resources on the system basis not only in the management economic system, but and in informatics system (on physical interior).

Along its development, the economic informational resources has traversed the followings two stages (forms) of organization in informatics milieu:
1) at the first stage the informational resources were organized in the shape of the separate (autonomous, local) data files for each particularly application, without taking in consideration the information links between the solved problems;
2) at the second stage these resources has organized starting from of the existent and possible information interconnections of all issues, in them solving are involved one and the same data. Such integrated way of informatics data organization was achieved in the shape of the database (D.Bs.).

For the first stage, except the separate data organization else was characteristic that each programmer fully answer not only at the elaboration of applicative programs of data processing, but of the correctness of data organizing on informatics memory space. Out of this given raison, each applicative program and particularly the same process of the solving each issue were effective.

However, because the economic problems are characterized by lots of information relations, it requiring the necessity to take into account the efficiency of the overall informational system, which is more essential and more voluminous than the sum of the efficiency of the solving of each separately issue.

The relevant form of organization of elucidated resources led to considerable duplication of recording of one and the same data on computer memory. In such situation it requiring the often repetition (doubling) of the data introduction, the latter usually being effected in manual mode. Such modality of data organization was characteristic for the 1 and 2 generations of the electronic computer machines (E.C.M.).

At the same time, on the positions of maximum utilization of the physical capacities of the technique means, for the second stage, which soliciting the data organization in interconnection, it certifying the followings negative moments:
1) the efficiency of each applicative program, from the view point of the speed (promptness), the solving of each issue in the milieu of automated data bank (A.D.Bn.) may be more reduced then in conditions of the separate data files:
2) it soliciting the considerable expenses for elaboration of the economic informatics system, based on the database management system (D.Bs.M.S.) and for the creation of the D.Bs.;
3) the utilization of the conception of D.Bs. requiring the additional space of memory and moreover of the working time of the processor, because the latter is involved in the fulfilling of any type of procedures or operations.

In connection with this appearing the dilemma of to determine what is more valuable – the efficiency of each applicative program or the flexibility of the D.Bs.? Initially, A.D.Bn.are effected only informational procedures, coherently of data registration and reading from various at memory types. Subsequently, they also are fulfilled and the diverse procedures of data structural processing (searching, sorting, correction, etc.). Such banks are considered open, because them database management systems are included in composition of the algorithmic input (of basis) language in the shape of the independent compartment.

At present A.D.Bn. effecting not only the structural and of calculation processing, but and the majority informational procedures, that is, practice all the data integral transformative process. That is why them (A.D.Bn.) not resorting to the services of other programming languages and out this raison they are considered right closed.

Essential for the study and analysis of D. Bn. are the organizational (compositional) and functional aspects. That is why it notion must established (formulated) on the two positions – after content and structurally (compositionally). On the first at them, this notion comprising the component parts, which directly are involved in curs of the physical solution of issue. In such case, right A.D.Bn. it considering the informatics complex, which consisting at two basic compartments – D.Bs. and D.Bs.M.S. Simultaneously, A.D.Bn. to can to existing and working and without other component parts. From on organizational positions, it may being interpreted as to the system, which consists at the D.Bs., programming, linguistic, technical and methodical – organizational resources, fated for to ensure the collective data processing and utilization.

Except the need of achieving systemic approach of the economic informational processes, to the massive constitution and implementation of A.D.Bn. are contributed and other premises, through which of basic are the followings :
1) as all the economic material objects and activities are find in the constantly interconnections and interactions, it is necessary as well as the information, which them describe (reflected), to being organized and recorded (stored) in the same way. At these requirements and meet the concept of A.D.Bn., but D.Bs.is not anything else than a informational model of material reality;
2) the informational needs of the end users (functional workers) also themselves intersecting and, therefore, not only the description of the economic material reality, but and informational requirements of the end users imposing the data organization and transforming in integrated way, starting from their involvement links;
3) in the process of the solution of various economic informational problems in the milieu of the A.D.Bn. it creating the real possibilities at to constitute and put in functioning a unitary informational fund for entirely managed object and all it ownerships structural component parts and processes. Then, meta – information (service information, information for description the information, information about the information) can be separated at the functional (of content) information;
4) the modern performance level at the technical and programmed resources, as well as the disposing of certain experience in the domain.

Although, the A.D.Bn. presenting the most adequate form of internal informatics organization of the economic information, them have both the priorities and not free and of drawbaks. So, comparatively to other forms of data organization, processing and utilization, the basic priorities of the A.D.Bn.it reducing to the followings:
1) the reducing until minimum a data redundancy and ensuring at the achievement of any new issues (applications), thanks to having in consideration of the all possible informational links between them;
2) increasing of the flexibility and handling of the informatics system (Ic.S.) in base of hunting out and working of all feasible informational interconnections;
3) facility of verification of integrity and incoherency of data values;
4) a signification reduction of the expenses coherently not only at creation, but and the processing data;
5) the applicative programmers are free of organization data values on the memory;
6) it achieving the independence of the applicative programs of them processing data;
7) the access to the data is far greater thoroughly.

The essential drawbacks of the A.D.Bn. consists in followings:
1) the upward complexity of informatics systems (Ic.S.);

2) the utilization of integrated D.Bs. can being to led at the diminution of the efficiency of solution a each issue;
3) the independence of the functional data from the applicative programs, which them utilizing, is ensured through supplementary works of their structuration. That is why coming out the necessity of elaboration and application of the new information of service (meta- information). Therefore, the named independence solicited moreover the new works of data structuring and supplementary volume of the memory;
4) increasing the requirements given of the technique and programmed resources;
5) a part at the resources of the technique means are used directly for the needs of D.Bs.M.S.;
6) in case of data deterioration, this can being led even to the Ic.S.

In milieu of the E.Ic.S. given of the A.D.Bn. it increasing the followings exigencies:
1) the adequate description of the economic material reality;
2) the possibility of communication with diverse users ;
3) ensuring of data confidentiality and integrity, them protection;
4) ensuring of the independence of application programs of them data;
5) ensuring the bests conditions of functioning of the A.D.Bn.

5.THE EVOLUTION AND TREND OF THE ECONOMIC INFORMATION SYSTEMS UNITS FUNCTIONING

The fabrication of any product or achievement of certain destination requiring the determination of the composition, succession and modality of effecting of the certain works.

The maintaining, compliance and ensuring of the achievement of these three key factors becoming possible in the case of the elaboration, organizing and functioning of the certain technology, what, in his turn, relies on the some resources (human, financial, material) distributed and used concordant of the necessities of them framework of unitary process oriented to obtaining a common result.

Every day making of any technology requiring the constitution, putting in action and ensuring of the daily effective functioning of certain organizational unit. In the domain informational economic activities such unit initially is considered right the “computing installation”, but in present – right the ”industry of manufacturing of the information”. But, at the beginning and in present under this notion it understood not something else than the organizational unit of exploitation of the informatics technique.

The variety of these forms and the succession of them functioning were conditioned first of all of the class of technical means, on them basis they were organized. In its evolution such units are'nt organized as computing office, station, center, automated system for the data collection, transmission and processing, the informatics post of the activity of specialist and network of their.
For the present and foreseeable prospect the most performance organizational unit of functioning of economic informatics systems (E.Ic.S.) are considered the network of the posts of the activity of

specialists (N.Ic.P.A.S.), because it literally are become a technical infrastructure of informational processes.

Therefore, so far the information “clothing” of the technical coat, or, more precisely, being said, the technique “dictate” the modality of organizing and processing of information, afterwards in the present we are the witnesses of the begin of the “clothing of the informational coat” of the technical means, or, better said, the information influencing the composition and structuring the technique, which confirms the superior level of development of the latter. On the route of its evolution such “enterprises of information manufacturing” have covered miscellaneous news rays of the economic informative domain, with extended varied composition of the achieved works. About this confessing the data are presenting in the Table 1.

The conventionally of the “enterprise of informational manufacturing” it´s motivated by the fact that in physical aspect really so “enterprise” not working separately of the economic unit – producer of material goods, constantly being in them composition. This again once abundantly confirms the correctness that affirmation that, not being the mater, the information is indivisibly connected (is not merged) of it, even and in cases, when it is obtained not manually, but automatically, with applying miscellaneous news informatics technical means.

Table 1. The evolution of covering of the economic informational activities by the organizational units, what ensuring the functioning of the economic informatics systems (EIS)

N/o	The organizational informatics units of functioning of EIS	The ray of covering of the informational activities by the organizational units of functioning of EIS							
1.	Computing office	A.O.							
2.	Computing station	A.O.	S.P.						
3.	Computing center	A.O.	S.P.	I.P.	S.D.	P.D.	U.I.		
4.	Automatized system for the data collection, transmission and processing	A.O.	S.P..	I.P.	S.D.	P.D.	U.I.	M.F.	
5.	Informatics post of the activity of specialist	A.O.	S.P.	I.P.	S.D.	P.D.	U.I.	M.F.	
6.	Network of the informatics posts of the activity of specialists	A.O.	.S.P.	I.P.	S.D.	P.D.	U.I.	M.F.	M.S.

In the Table 1 are allowed the followings significations: A.O. – arithmetical operations, S.P. – structural procedures, I.P. – informational procedures, S.D. – standardized decisions, P.D. – procedures of obtaining of the values of the primary informational units, M.F. – management functions, M.S. – management system.

At the presented analysis is clearly the trend of the specialization of informational activities in dependence of them functional content, according of growth of the volume and them complication. If initially a specialist achieving entirely the informational system (I_l.S.), afterwards – some group of the specialists (G.S.), each achieving a few one complex of informational issues (C.I_l.I.), what subsequently where organized in certain subdivisions (SD) (such as book – keeping, planning department, department of standardization, etc.) that achieving each a few one informational function ($I_{l.}$F.). In it interior the specialists can be organized after complexes of informational function (for example, the book – keepers on the evidence of material values, the book – keepers on the evidence of work and it payment, etc.).

To the last stage and prevalent so far the organizational form of achievement of the informational activities is presented by certain system (orderly conglomerate) of the subdivisions, each of they, fully or partially achieving of informational function, in interior of which the specialists in groups or individually, also, are organized on the complex or on the each informational issue.

Analytical the chain of the evolution and of perspective of informatics organizational forms, with indicating of the technical base and the level of extending of the ray of informatics achievement of economic informational activities is presented in the following mode:

C.O.(C.M.K.;A.O.) → C.S.(C.P.M.;O.A.,S.P.) → C.C.(E.C.M.,T.P.D.,T.D.T.;A.O.,S.P.,P.D.,U.I.,M.F.) →
Ic.P.A.S.(E.P.C.,D.T.T.;A.O.,S.P.,I.P.,S.D.,P.D.,U.I.,M.F.) → Ic.C.S. (T.D.T.,T.P.D,E.C.M.,E.P.C.;

A.O.,S.P..P.O.I.P.U.I.,S.(T.).D.) → C.N., .Ic.P.A.S.,Ic.N.(T.D.T.,T.P.D.,E.P.C.;A.O.,S.P.,P.O.I.,P.U.I.,S.(T.) →
D.,C.D.,M.F.). → At.(Az.) M.S.(T.D.T.,T.P.D.,E.P.C.T.U.I.;A.O.,S.P.,P.O.I.,P.U.I.,S.(T)..D.,C.D.,M.F,M.S.) →
→ A. U. M_l. - I_l N.(I_l.F.M.;M.S.);

where:

a) the informatics organizational units: C.O. – computing office; C.S. – computing station, C.C. – computing center, Ic.P.A,S. – informatics post of the activity of specialist, Ic,C. S. – informatics computing system, C.N. – computer network, Ic.N. – informatics network, N.Ic.P.A.S. – network of the informatics posts of the activity of the specialists, A.(Az.).M.S. – automatic(automated) management system A.U.$M_{l.}$- $I_{l.}$N. – automatic unitary material – informational nucleus;

b) technical base of the organizational units: C.M.K. – computing machines with keyboard, C.P.M.- computing perforation machines, E.C.M. – electronic computing machines, E.P.C. – electronic personal computers, T.P.D. – technique of primary data, T.D.T.- technique of data transmission, T.U.I. – technique of utilization of the information, I_l.F.M. – informational physical models;

c) area of informatics achievement: A.O. –arithmetical operations, S.P. – structural procedures, P.O.I. – procedures for obtaining the initial information, P.U.I. – procedures of utilization the information, S.(T.)D. – standardized (typified) decisions, C.D. – complex of decisions, M.F. – management functions, M.S. – management system.

6. CONCLUSION

1. In prospect these most efficient will be those forms of data organizing, the building and functioning not will depending of the physical specific of the support;

2. Such material and spiritual processes, which evolving in integrate way, it requiring as and economic information, which them reflecting and influenced, can being approached and processed in synergic mode;

3. The pressing necessity in the strictly respecting of this concept and in it automatic achieving, as well as the higher performance level of the informatics technique, step by step have led to the formation of the idea of D.Bn;

4. The principle of data banks to become impending once with obtaining the social character of human material and spiritual activities. But the notion, as such, was formulated and used together by the massive invention and implementation of informatics technical means with the unconceivable capacities of storage of data volumes and speeds of processing;

5. Depending of the class of informatics technique and data supports utilized by them, D.Bn. have covered the followings three stages:

a) D.Bn. achieved thanks to the location and handling of the paper and cardboard supports;

b) D.Bn. based on the content and processing interconnections of the informational entities, according to that it elaborating and working the unitary scheme of organizing to all units of system of information;

c) D.Bn., which working grace the physical features of supports.

In accordance with this classification, conventionally, can being affirming what exists the D.Bn., which working manual, mechanized, automated and automatic. At once, in the economic material and informational environment all D.Bn. based on the electronic personal computers (E. P. C.) are considered atomated, but the automatic presenting a difficult determinable prospect. The first can being identified through Az.E.D.Bn. (automated economic data bank), and the second – through At.E.D.Bn.(automatic economic data bank);

6. After content and predestination of the obtained informational products can being distinguished the automated economic informative data bank (Az.E.Iv.D.Bn.) and automated economic intelligent data bank (Az.E.Ig.D.Bn.). The informative producing such informational products, which only reflecting the situation of the object at a given moment or in certain bound, while those intelligent producing diverse decisions, which altering them evolution;

7. If initially the Az.E.D.Bn. fulfilled only informational procedures (registering, reading, searching), subsequently – and structural procedures (sorting, concatenation, correction, a.s.o.) and the operations of the calculus;

8. The Az.E.D.Bn will fulfill in common informational processes with the material, permanently interacting and influencing some on others in both directions. In such conditions the economic material unit it turns into automated (automatic) unitary informational – material nucleus (Az.(At.) $U.I_l.M_l.N.$);

9. Concomitantly with the increasing of the complexity of organizational form it producing the ramification (specialization) even more detailed profoundly of effected informational activities in them framework;

10. The specialization of informational technologies will be place on the basis of the functional content of examined activity, without the concretization until to the level of procedures and operations;

11. For the economic material milieu entirely will be producing the automatic achievement of informational (informative, decisional) sub-compartments in case of constitution and functioning of automatic (or automated) management system (At.(Az).Mg.S.);

12.Az.M.S. will evolving în At.M.S.;

13. The last, through constitution and putting in function of miscellaneous news physics (chemical, biological, etc.) models, the automatic connection will achieving entirely both the informational and material compartment of the unitary economic management process;

14. In such situation any managed object will turn into interconnected and interacted material – informational (informative and decisional) single nucleus, which and constituting the ideal of any management system of material activities;

15. The organizational informatics forms and units have evolved and will evolving from the computing office until the automatic unitary material – informational nucleus, the technical base – from the computing machines with keyboard until the informational physical models, but the area of covering of informational activities on the informatics means and methods – from the arithmetical operations until management system.

The thoroughly and entirely knowledge of the informational and informatics terminology, as well as the role, place of the informatics organizational forms and units, trend at them evolution will contributing to the constitution and functioning of a unitary system of automatic fabrication at the material, informative and decisional products with ideal performance.

REFERENCES

1. Leahu T. Organizarea, structurarea şi transformarea informaţiilor sistemului managerial economic. Chişinău, C.E.P.U.S.M., 2009, pp.7-14, 97 – 128.

2. Leahu T. One vision regarding to the evolution,notion, premises and trend of thehe development of automated economic data bankks (A.E,D.Bn.), pp.320 – 325.Conference Proceedings. The 12th International Conference on Informatics in Economy 2013, Bucharest, 684 p.

3. Leahu T. Trend of the evolutionn, ,prospect and concordance of the organizational forms and units of functioning of the economicic informatics systems (E.Ic.S.). Proceedings of thee 37th ARA Congress, p.511 – 515, Central Publishing House, Chişinău, 2013, 680 p.

4. Leahu T. The evolution, specific and problems of constitution and functioning of automatized banks of intelligent economic datata (A.Bn.Ig.E.D.).The proceedings of the seventh international conference on informatics in economy, Bucharest, may 2005. INFOREC Printing House, pp.845-851

5. Leahu T. The functional – conceptual aspect of the composition,structure and working relations of the automated banks of intelligent economic data (A.Bn.Ig.E.D.). The 2nd supplement of the review "Informatica economică". 2006,Volume II, pp.89 – 96.

6.Larousse. Dicţionar de informatică.Coordonare:PierreMorvan. Bucureşti, EdituraNiculescu SRL, 2003, pp.41, 43 – 44,1992, pp.71, 97, 117, 146, 163, 207, 233.

7. Mardare I., Perju V. Restoration of the images by neural networks and associative memory. In Information Technologies-2004. A.Andries, V.Perju, Editors. Proc. SPIE 5822 (2005), USA. P.35-45.

General Aspects of the State Tax Critical Information Infrastructure Management

[1]Coceban Vitalie, [2]Rusnac Andrei

[1]"Fiscservinform" State Enterprise
6, Constantin Tanase Str., Chisinau, MD-2005, Republic of Moldova
Tel: 37322822000, e-mail: fiscservinform@fsi.fisc.md

[2] Information security expert, Republic of Moldova
E-mail: rusnacandrei79@gmail.com

ABSTRACT

The article describes the general aspects of organizing and managing the functionality of the critical information infrastructure within the information system of the State Tax Service.

Keywords: critical, information, infrastructure, security, tax system, state, tax, service.

1. INTRODUCTION

The basic mission of State Enterprise "Fiscservinform" is the efficiency of the fiscal administration through the continuous development and maintenance of the fiscal information system able to offer modern electronic services to the taxpayers in their interaction with the State Tax Service and its integration into the e-Government infrastructure in the Republic of Moldova, as well as training all the related taxpayers to use fiscal electronic services that will increase transparency and good governance.

In order to accomplish the assigned mission, the Enterprise sets out the following strategic objectives:

1) Improving the use of the information technology infrastructure of the State Tax Service;
2) Building the Integrated Information System of the State Tax Service;
3) Ensure the security of the State Tax Service's Information System, personal data and business processes within the Enterprise;
4) Development of services, systems and products in accordance with customer requirements.

In the process of meeting the mentioned objectives, the Company assumes a large part of the responsibilities related to providing of all the services without intermission to the taxpayers as well as to the STS (State Tax Service).

The STS (State Tax Service) Information System consists of a large number of info-communicative components, some heterogeneous and partially independent, others integrated with each other through interoperable services created and developed in a modular manner according to the platforms used at the time of development. The colossal volume of information accumulated, the changes in the fiscal policy of the Republic of Moldova, the institutional reform highlight the necessity of the continuous development of the functional components. The complexity of system solutions and components requires engineering of the Fiscal Management Information System (FMIS)platform based on the modern principles of information systems development, ensuring the unification and centralization of infrastructure components, process applications, data structures and risk analysis tools. Major attention is drawn to the information security infrastructure that includes all the Fiscal Management Information System (FMIS) components.

Today the system develops on the basis of the following requirements:

1) developing a safe and secure collaboration environment that provides collaborative tools to all STS employees, regardless of their physical location, as well as the means to ensure the integration of FIS (Fiscal Information System) with external systems;

2) ensuring access to the information subsystems specific to the activity of authorized users (STS collaborators, public authorities, taxpayers) through an integrated mechanism: the FIS (Fiscal Information System) web portal, depending on the roles and rights of the users;

3) providing a universal, reliable and efficient document circulation platform, applicable to the modeling and computerization of all STS workflows that are provided with efficient means of processing, monitoring, disseminating and tracing processes;

4) consolidation and management of a data warehouse related to the STS activity and interaction with external information resources for generating reports and analyzes, aimed at assisting the decision-making process at STS level, the Ministry of Finance or other state institutions;

5) ensuring the authenticity, protection and integrity of data in the process of collection, storage, processing and use in the SIS IT subsystems;

6) the automation of the public data dissemination processes or the authorized delivery of specific processed data intended for the activity of other public authorities of the Republic of Moldova or the taxpayers;

7) computerization of primary data collection or dissemination processes through automated interaction processes with information systems of public authorities in the Republic of Moldova.

As the indispensable component of the state economic sector, as well as in the context of the inclusion / assurance of the state fiscal statistics, the electronic information and communication systems of the national automated fiscal environment, for the collecting, processing and transmission of tax information, the managed information system by State Enterprise "Fiscservinform" is an object of national economic importance, which is part of the informational critical infrastructure of the Republic of Moldova.

In the context of the above, „Fiscservinform” has obligations to ensure the security of the critical infrastructure managed by implementing measures for the stable, secure and continuous operation of the managed object. This process includes in itself a several of legal, organizational and technical measures for the creation and exploitation of security information systems and modules for the object of critical information infrastructure.

2. THE FISCAL INFORMATION SYSTEM - CRITICAL INFRASTRUCTURE

Critical Information Infrastructure is a totality of automated Critical Infrastructure Management Systems that are essential for maintaining the vital functions of the state and disturbance or destruction of which will have a significant impact at national level due to the inability to maintain the given functions. State Enterprise „Fiscservinform", being the technological administrator of the Fiscal Management Information System (FMIS), pays maximum attention to the critical infrastructure security by approving and gradually implementing the information security policy approved in 2011.

The Fiscal Management Information System (FMIS) architecture model is developed to incorporate the information security features within the organization, the information-communication infrastructure, IT systems, and the technological computing and storage architectures. This approach helps to increase the prominence of these issues and leads us to gain a deeper understanding of the security aspects of architectures.

Information security is included in the meta-model of architecture to ensure the integration of information into business processes.

This approach for each area of information security covers the following:

1) data availability;
2) data integrity;
3) confidentiality of data;
4) responsibility;
5) non-repudiation.

The security architecture is shown in figure no. 1 which covers both the regulatory framework and the technological framework.

3. PROTECTION OF THE FISCAL INFORMATION SYSTEM

The mentioned system being an object of the critical information infrastructure is subject to increased danger and its impairment or stopping will lead to loss of management of the part of the national economy (fiscal field), as well as to a significant reduction of the protection of the vital functions of the taxpayers.

In the given context, „Fiscservinform" undertakes measures aimed at ensuring the functioning, continuity and integrity of the critical information infrastructure in order to neutralize the identified threats and risks. The nominated assurance involves in itself a series of legal, organizational and technical measures for the creation and operation of the security systems of the Fiscal Information System, in particular:

1) Correctly assessing the level of risk of the infrastructure and identifying the measures necessary for the prevented intervention and diminishing them;

2) Establishing the main directions of activity and ensuring the normative regulation of the actions related to the security of the object proper;

3) Development and implementation of security programs / plans;

4) Establishing mandatory requirements for the modules and subsystems that make part of the Fiscal Information System;

5) Organizing and performing of the security audit of the critical information infrastructure object in management;

6) Identifying risks and threats to object security, as well as detect, prevent, and minimize damage from security incidents.

The security system implemented within the Enterprise ensures:

1) Preventing unauthorized access, wholly or partially infringing information as well as committing other illegal actions as regards the mechanisms that control and monitor the technological processes of the critical information infrastructure object;

2) Prevention of the impact on the technical means of information processing, which could disrupt or block the functioning of the Fiscal Information System;

3) Responsibility for information security incidents;

4) Immediate restoration of the integrity and operation of the critical infrastructure object;

5) Storage of information of major importance for ensuring the management of technological processes, such as storage of technological processes of object management.

State Enterprise "Fiscservinform" managed to create a technological and operational platform for the management and security of the object of the critical information infrastructure in the management. For the management and documentation of information security activities, the process of implementing the Information Security Management System (ISMS) in the context of the overall activities and risks to which the tax authority is exposed was launched in 2011.

Information Security Management System (ISMS) is designed to ensure adequate and proportionate selection of security measures that protect information resources and ensure the confidence of the parties involved.

The STS defines the scope of application of Information Security Management System (ISMS) in order to determine which information is to be protected and in what way. Such information is protected, whether stored, processed or transferred inside or outside the scope of Information Security Management System (ISMS).

The scope of the Information Security Management System (ISMS)I covers the processes and services within the STS, the structural subdivisions and functional units, the locations and the technological and network infrastructure, other elements applicable in the context of ensuring the security of those data.

Information Security Management System (ISMS) is part of the entire management system that has at its center a risk approach that is used to establish, implement, operate, monitor, review, maintain and improve information security.

Adopting and maintaining an Information Security Management System (ISMS) gives to administration of STS the opportunity to make informed choices about how to control risks by planning, implementing, and monitoring measures taken to reduce / transfer risks and to be able to manage potential incidents.

Information Security Management System (ISMS) offers a set of benefits for STS, including:

1) the credibility, trust and security of taxpayers;

2) savings of funds in process of removing information security breaches;

3) developing of a security culture appropriate to the proper functioning of STS;

4) continuous improvement through the continuous development, monitoring and improvement of both SMSI and tax administration processes.

In terms of the modern trends of Information Security Management System (ISMS) implementation in both commercial companies and state entities as well as taking into account the specific activity of the latter, there is a need for the elaboration and approval of a national framework for implementation and certification of SMS by public authorities and institutions ability.

4. OBJECTIVES IN THE FIELD OF INFORMATION SECURITY INSURANCE

According to the STS Development Plan for 2011-2018 (p.4.3.4) - "Ensuring information security implies ensuring the confidentiality of information, by preventing access to information by persons without appropriate rights and powers, ensuring the logical integrity of information, by preventing the unauthorized introduction, updating and destruction of information, ensuring the physical integrity of information, ensuring the protection of the information infrastructure against deterioration and attempts to modify the operation.

To achieve this overall goal, STS proposes the following specific objectives:

1) implementing appropriate measures to ensure data protection (security, integrity, definition and documentation of feedback) and their review on a regular basis;

2) maintaining the security of information systems in order to ensure the confidentiality of information on taxpayers, the protection of personal data."

5. MEASURES TO ENSURE INFORMATION SECURITY

All STS information security measures are applied in accordance with applicable laws and regulations as well as standards, guides and codes of practice in the field.

Legal and organizational measures aimed at preventing the disclosure, modification and unauthorized destruction of confidential information:

1) Establishment of the Interdepartmental Commission for Information Security, by the Order of the no.1634 of 06.09.2013;

2) The implementation of the Initial Action Plan on Information Security Assurance within the STS, approved by the Order no. 2079 of 23.10.2013;

3) Regularly conducting internal and external audits of information security;

4) Implementation of the requirements for personal data security, in accordance with the Order no.63 of 13.02.2012;

5) Implementation of information security management system, according to ISO27001 standard;

6) Elaboration and implementation of internal documents regulating the security of data and fiscal administration processes;

7) Analysis of information security risks involving the elaboration and implementation of the risk management plan;

8) Training of employees in the field of information security and signing of confidentiality clauses with them;

9) Collaboration with law enforcement and other state institutions.

The technical-applicative measures, based on information protection are:

1) Redesigning and switching from "FoxPro" system to modern database systems;
2) Centralization and unification of Active Directory for all STS institutions, with configuration of security (group) policies, rights delimitation etc;
3) Developing web applications that enable users to authenticate and identify and log their actions (electronic services);
4) Implementation of applicative solutions, which ensure the monitoring and control of the circulation of information, portable media, etc;
5) Maintain and equip the Data Center with the most advanced security systems in line with international standards;
6) Document management in electronic format;
7) Classify, manage and record information that is classified as confidential (fiscal secret, personal data) in both electronic and paper formats;
8) Strict control of physical access and video surveillance of people in restricted areas.

6. THE HUMAN FACTOR - A PRIMARY ASPECT

One of the most vulnerable links of the information security system is the human factor. Thus, an important element of information security is the knowledge and the respect by the users of the methods and procedures for prevention and counteraction of the informational security hazards.

Security of information and technology is a shared responsibility of all STS staff.

Permanent training of STS employees on the functionality and rules of operation (administration) of information system components, technical and program resources, as well as in the field of informational security is continuously ongoing.

The general rights and obligations for fiscal officers are stipulated in the STS Information Security Policy, approved by the Order no.778 of 18.06.2013:

"2.2.5. The Service (State Tax Service) reserves the right to monitor the use of information resources in the performance of user functional obligations. "

"4.5.1. The user is in the right:

a) to gain access to the information resources and databases necessary for the performance of the functional obligations or the obligations stipulated in the contract or agreement signed with the Service (State Tax Service);

b) to benefit from equipment and program access to information resources and databases;

c) if necessary, address the system administrator for methodological assistance;

d) to receive training and qualification in the field of his activity. "

4.5.2 The user is obliged:

a) to know and to observe the provisions of normative acts in the field of information security;

b) maintain the confidentiality of the processed data;

c) not to allow unsolicited copying and distribution of the information received;

d) to take appropriate technical and organizational measures for the protection of confidential data;

e) to immediately inform immediately the chief or, as the case may be, the management about a situation in which the data were accessed / processed in violation of the legal norms

f) execute the "clean screen" policy (disconnecting or blocking the workstation).

4.5.3 The computer user is responsible for the information stored on his / her computer, for the proper technical condition of the computer and the equipment entrusted to it.

4.5.4 The User is not allowed to add, modify, or remove equipment to / from the corporate network of the Inspectorate without the consent of the System Administrator.

4.5.5 The user is solely responsible for the entire information exchange that takes place between his computer and other computers in the local or non-domestic network.

4.5.6 For violation of the above mentioned obligations, the user is liable in accordance with civil, contravention or criminal law."

If Fiscal officials disclose confidential information and their actions / inactions meet the constituent elements of the offense prescribed by law or may be classified as disciplinary offense, the STS informs law enforcement and / or disciplinary sanctions in the way set by the legislation.

Concerning the human factor, we add that, with only a functional platform at the level of decision-makers of the top level, it is possible to ensure the planned implementation of the measures in the field of information security, as well as to ensure the control of the execution of the information security requirements on both horizontal and vertical.

This within the STS is ensured by the initiatives of the STS Chief to promote and raise awareness of compliance with the information security requirements by the tax officers.

7. CONCLUSION

Finally, we can mention that the implementation of measures to reduce information security risks to an acceptable level is a continuous process and is carried out taking into account the identified risks, the requirements and constraints of the regulations in force and the technical and financial possibilities of the STS.

At the same time, new methods of further strengthening of information security activities are identified, aiming to increase the users' trust in the developed solutions for the provision of electronic services, to strengthen the placement of STS in the service of taxpayers and, more generally speaking, to capitalize on the potential of e-commerce in the best possible safety way.

In particular, it is to be summed up that currently the notion of "critical information infrastructure" is not provided for in the legislative framework in force and that the area is not regulated. This situation needs to be examined by the relevant institutions for the swift approval of the appropriate legislative framework necessary for identifying, designating and evaluating the level of protection of critical information infrastructure (vital / state) infrastructure to ensure stability, security and the security of national economic systems.

REFERENCES

1. Tax code of the Republic of Moldova of 04.24.1997, No. 1163-XIII;

2. Law on Electronic Communications of 15.11.2007, No. 241-XVI;

3. Law on Informatization and State Information Resources of 11.21.2003, No. 467-XV;

4. Law on Commercial Secrets of 07.06.1994, No. 171-XIII;

5. Government Decision on the establishment of the State Enterprise "Fiscservinform" of 09.19.2008, No 065;

6. Government Decision on Piloting the Information and Document Management System of 04.15.2013, No. 262;

7. Government Decision "On the approval of the Action Plan for 2012 for the implementation of the Strategic Technology Modernization of Government (e-Transformation)" Program of 01.26.2012, No. 44;

8. Government Decision on the National Strategy for Information Society Development “Digital Moldova 2020” of 10.31.2013, No. 857;

9. Government Decision "On the Creation of the State Automated Information Systems and Resources" of 05.22.2006, No. 562.

Security Risk Detection Algorithms in Artificial Immune Systems

Sheikh Kanza, Rehman Saad, Khan Khattak Muazzam A., Riaz Farhan

National University of Sciences and Technology, Islamabad, Pakistan
Rawalpindi-46000, Tel:+923218527037,+923348198705
E-mails: kanza.sheikh15@ce.ceme.edu.pk, saadrehman@ceme.nust.edu.pk,
muazzamak@ce.ceme.edu.pk

ABSTRACT

Artificial Immune Systems (AIS) are algorithms with the origin from principles and functioning of the innate immune system. These algorithms exploit the characteristics of biological immune systems like learning and memory as a way to formulate problem. To prevent and minimize the security risks, there is severe need to integrate the Artificially Immune Systems for the security of networks. In the recent years various AIS algorithms with fabulous functionality have been proposed. In order to give the comprehensive review of all the AIS algorithms meant for risk detection and give direction for further research, a review of the AIS algorithms is discussed in depth in this paper. Qualitatively, based on primary algorithms, we show that all these algorithms once done with classification for the first time do not check its validity of being correctly classified. So we found that deterministic DCA is best among all the existing techniques of AIS based risk detection and proposed Enhanced Dendric Cell Algorithm (EDCA) to make it more efficient.

Keywords: artificial, immune, system, automated, response, risk, detection, security, algorithm

1. INTRODUCTION

AIS provide Network perfect algorithm range for network risk detection. Be that as it may, there is a critical restriction with recent AIS in that the safe motivated algorithms [1]. In request to secure the networks, it is basic that the created "responsive" AIS can react notwithstanding performing recognition.

This issue gives a chance to promote AIS on two fronts, in giving a perfect situation to testing this present reality utilization of invulnerable motivated algorithms and the capability to create new responsive AIS. This is basic for the assurance of the networks as the central idea is to make self-administrated system without human intervention. Adjustments are made in to the deterministic DCA to improve the features of responsive AIS systems for risk detection.

This incorporates how models of differing qualities in T-cell responses can be consolidated into safe enlivened risk detection frameworks to make future AIS for this reason. The fundamental commitment of this research is to give review on security which is a reasonable issue to be explained by AIS.

A survey of the utilization of AIS in risk detection where we look at how current invulnerable motivated calculations could be utilized as a part of request to give security for the networks, and show how current AIS should be altered with a specific end goal to wind up distinctly skillful for this purpose [2,3]. The security of the networks could be a conceivably intriguing and valuable use of a resistant enlivened observing framework. In any case, this would need to reconsider of how we infer, develop and apply AIS. AIS have so far concentrated simply on little models of particular elements of particular cell sorts, for instance in the risk flag handling components of the DCA, single instruments are preoccupied to tackle single issues. Resistant system approaches [4] profit by the circulated also, versatile properties and are maybe the most reasonable sort of AIS to be connected

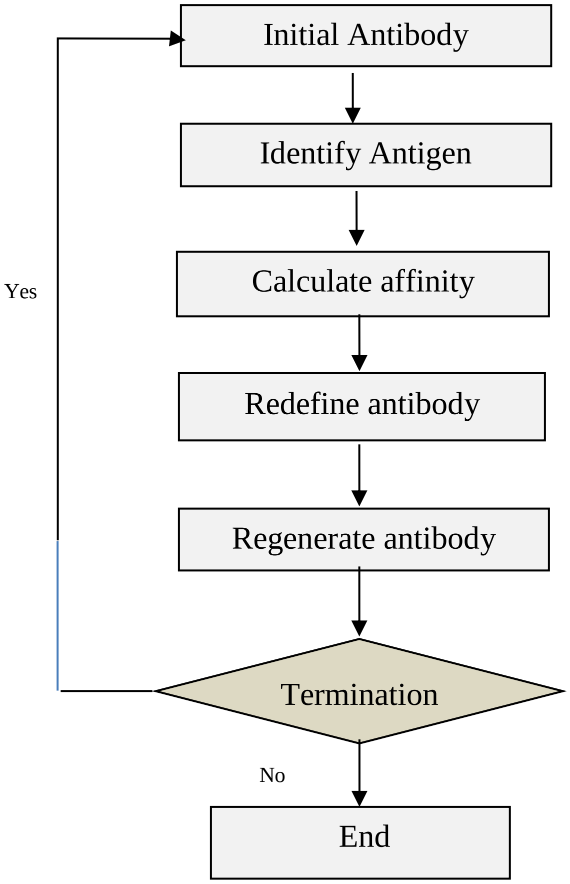


Fig. 1. General Strategy of AIS Algorithms (Adapted from [28])

specifically to this issue, as they by and large depend on creating powerful and versatile practices [5]. Once more, they have high computational cost. At last, the DCA [6] has been appeared to be lightweight in wording of computational unpredictability, has been connected beforehand to inserted gadgets.

It is vigorous and mistake tolerant, however it is not versatile. Once the information sources have been sorted for the flag handling segment, they don’t adjust and as a result false negative arrangements can arise [7].This varies from the human invulnerable framework where the "immunological neural connection" exists between the versatile and innate invulnerable frameworks, with the particular capacity of controlling and creating suitable effecter responses.

This paper tries to gaps the existing algorithms and proposed small changes in the DCA is effective for risk detection purposes. Fig1 is the general strategy followed by AIS algorithms.

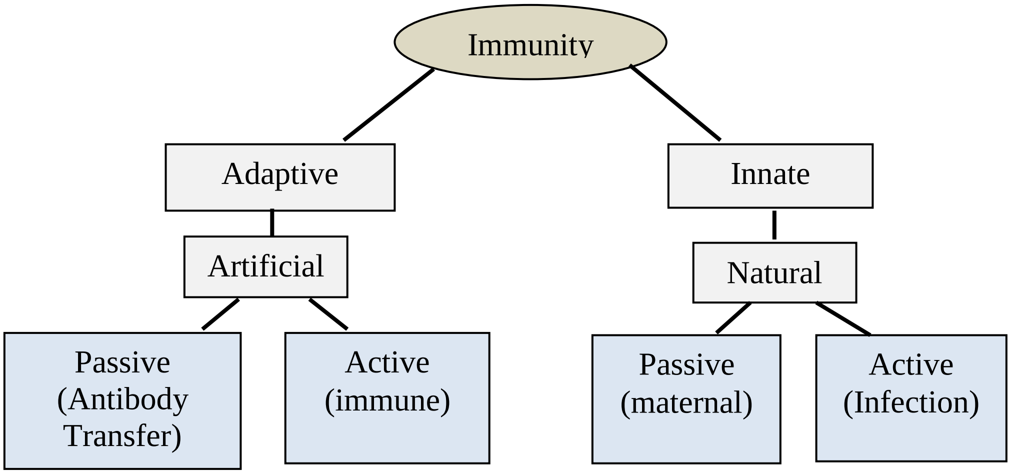


Fig. 2. Classification of Immunity based System (Adapted from [29])

2. LITERATURE REVIEW

The Human Immune System is self-organized, distributed and lightweight nature has multi-layered protection architecture, including physical and physiological limitations [8]. A method AIS is inspired from some parts of this architecture. AIS methods can be categorized into two main classes. As seen in the Fig 2.

Characteristics of AIS Algorithms

AIS methods originate from the adaptive immune system and develop into methodologies like Negative selection [9], Chaotic Immune Clonal Selection Algorithm [10] and immune network [11] are meant for cooperate to separate self from non-self antigens is first generation AIS depending on adaptive immune systems only. Second generation AIS Method inspired from adaptive and innate immune systems towards this methodology of Danger Theory arises. Based on danger signal different immune responses are chosen. This feature attracts us to choose danger theory based approach to propose application. In this method Dendritic Cells (DC) [12] Structural toll-like receptors (STLR) [13], acts as an identifier of danger signal. Proposed application, choose DC methodology due its well suited future. Dendritic Cell (DC) is the first defense line for HIS that will reach the place where antigens are first intruded and then swallowed the latter to the pieces. These pieces will be then associated with APCs and forwarded to the T-cells [14].

DC has 3 states: Mature, Semi-mature and Immature [15]. DCs are inspected at cellular level, which comprises of the different states, interaction with antigen and signals [16].Signals, DC states and antigen representations form the core of this abstraction. The below mentioned properties of DC [17], is inherited as follows since same methodology is adopted to the proposal. For enhancing resiliency, an autonomic architecture in cyber physical system with self management properties is proposed [18].A Bayesian network method for learning the informal relations among physical and cyber variables, unlabeled data and computations to manage the heterogeneous properties of the physical and cyber data, so to use integrated dataset for learning the parameters and structure of Bayesian network. Various techniques on immune system basis were presented in recent years including integrating the DCA and Dempster Belief theory in fuzzy logic techniques, Rule-based Detections, state transition approaches, Pattern Structure. But false alarm rate was elevated. The problem of correlation and will solve issue of not known and vastly evolving harmful attacks [19]. Anomaly detection has main feature to discover the attack types not seen before, making it suitable as a second line of defense. It utilizes machine learning and data mining algorithms, to detect anomalies at runtime when deviations from the normality model. Supervisory Control and Data Acquisition (SCADA) system for real-time analysis and detection of contaminants from data given by water quality sensors [20].

A more integrated technique is to integrate different immune mechanisms may be needed for producing a complete application that capitalize the problem solving mechanisms based on human immune system. This could conceivably prompt to the advancement of considerably more intense AIS. Different cell sorts are utilized to coordinate particular reactions to particular dangers in the human insusceptible framework. Subsequently, AIS which consolidate various systems will require to be created to accomplish these limitations. Multiple AIS could be consolidated utilizing thoughts from gathering techniques, bootstrapping distinctive current AIS together, as proposed by Chen et al.

Immune network approaches capitalize on the adaptive and distributed properties and are though the most appropriate type of AIS to be directly applied to resolve this problem because they have adaptive and robust nature. But they are costly in terms of computation. Finally, the DCA has been seen to be frivolous with respect to computational complexity, has been implemented earlier for embedded devices. It is considered as error tolerant and robust, but lack adaptive nature. The inputs do not adapt after classification and resulting in false negative classifications [21]. The lines between interruption recognition and in-susceptibility have for quite some time been the wellspring of motivation for AIS scientists, however customary PC systems don't nearly look like the dynamic, dispersed and liquid nature of living beings and their resistant frameworks well. There is, be that as it may, a sort of system that shares a significant number of these highlights: sensor systems. In the accompanying areas, we present this sort of system what's more, diagram one famous steering convention, known as Directed Diffusion [22].

Comparison table of the current progress in the AIS algorithms and methods are given in the Table 1 where focus on risk detection is medium and support for large scalability is no because considers target only selected domain data but capability of multi domain but inefficient in case of large dataset. Focus on security is high(H) and support for large scalability is L(low) because considers multiple domain data andinefficient in case of abnormal data.

Focus on security is low and support for large scalability is no because considers only selected domain data and inefficient in case of abnormal data. Computational cost is high. As far as the computational cost is concerned it is high, medium and low on the basis of more than 3, 3 and two steps of classifying the threat respectively. Efficiency is decided on the basis of low computational cost and high focus on security as well as scalability supported.

3. SURVEY OF TYPICAL AIS ALGORITHM

Many algorithms have been presented till now for the risk detection of AIS based system most of them are the enhancements or the modifications of previous algorithms. It is not possible to give the detail of every algorithm till now. So here are few base algorithms that are described in the following sub section. Only those algorithms are discussed in detail that are popular and reflect the state-of-the-art of research work on AIS based risk detection, those which present new ideas, trends and are currently in practice, are not complex and adequately introduce the basic concepts and background of AIS system or those which are published in top international conferences or journals.

3.1 The Dendritic Cell Algorithm

The DCA is motivated by elements of the Dendric cells (DCs) of the inborn safe framework, which shapes part of the body’s first line of resistance against intruders. DCs show the capacity to consolidate a large number of sub-atomic data and to translate this data for the T-cells of the versatile resistant framework. This could prompt to the acceptance of different safe reactions against seen pathogenic dangers. In this way, DCs are regularly observed as indicators in charge of policing diverse tissues [23] and in addition inductive go between an assortment of resistant reactions. All in all, two sorts of atomic data are handled by DCs, in particular “flag” and “antigen”.

Signs are gathered by DCs from their neighborhood surroundings and comprise of pointers of the wellbeing status Fig. 3. A state-graph depicting the three conditions of an individual DC. of the observed tissue. All through its life expectancy, an individual DC will exist in one of three states, to be specific “juvenile”, “semi-develop” furthermore, completely “develop”, as appeared in Fig. 3. In the underlying juvenile state, DCs are presented to a blend of signs. In view of the centralization of introduced signs, DCs separate into either a “completely develop” frame to actuate the versatile safe framework, or a “semi-develop” shape to stifle it. In the event that a DC is presented to a mix of signs produced from a solid or relentless state tissue environment, for example, no event of tissue harm, it more probable turns into a semi-develop DC.

On the other hand, if a DC is given a blend of signs produced from a harmed tissue environment, for example, the nearness of unregulated cell demise, it more likely separates into a completely develop DC. Normal DCs tie to furthermore, handle numerous cytokine signals. In a dynamic model of DC conduct created by Greensmith (2007), the accompanying classes are characterized. PAMPs (Pathogenetic Associated Molecular Patterns) are atomic marks of pathogens which are perceived by Toll-Like Receptors (TLRs) on the surface of DCs. Amid the juvenile state, DCs additionally gather flotsam and jetsam in the tissues which are in this manner consolidated with the natural signs. A portion of the "suspicious" flotsam and jetsam gathered are called antigens, and they are proteins starting from potential attacking substances. DCs join the "suspect" antigens with confirmation as signs to accurately teach the versatile safe framework to react, or turned out to be tolerant to the exhibited antigens.

For more nitty-gritty data concerning fundamental natural components, please allude to Greensmith (2007) and Lutz and Schuler (2002). It is supposed that two data streams are strongly bonded. Antigens are un-mitigated qualities that can be different conditions of an issue area or the substances of intrigue connected with an observed system. Signals are actually real-valued vectors and meant for monitored systems measure status within specific time intervals whereas antigens deal with classification problem domain. IDs in computer security issues [24] ,positions and orientations of robots on small scale, the sensor proximity of online robotic systems (Mokhtar et al., 2009), or the data in terms of time stamps gathered in biometric data (Gu et al., 2009) are the examples of signals. Categories of signals include PAMP, Danger or Safe. Following is the brief description of these signals: PAMP: detect the anomalous behavior and confidence indicator of the events that can definitely cause harm to the system. Danger: detect possible anomalies, as the values in-creases. Safe: enhances conjunction value with detected normal behavior and safe signal suppress the PAMP result and Danger signals in algorithm, as seen in the normal framework.

The property (immunological)explained above is fused inside the DCA as predefined weights for every flag class, for the change from information signs to yield signals, which are “CSM” and “K” signals. The CSM flag mirrors the measure of data a DC has prepared, i.e. at the point when to decide, while the K flag is a measure showing the polarization towards peculiarity or ordinariness, i.e. step by step instructions to decide.

The yield signs are utilized to assess the status of the framework observed by the investigation part of the calculation. Such a flag change process is shown in Fig.3. Keeping in mind the end goal to accomplish its discovery capacity, the DCA initializes a populace of manufactured DCs working in parallel as locators. Each DC is given a particular breaking point of its life expectancy, which makes an element time window impact in the populace (Oates et al., 2008). This leads to similar information streams of flag and antigen being handled by each DC, amid various eras over the dissected time arrangement. When the DC”s life expectancy achieves zero, it quits signal processing change and worldly connection. Once a developed DC has introduced the prepared data, it is reset to its default frame. Here, the populace size is by and large kept steady, yet can be client indicated.

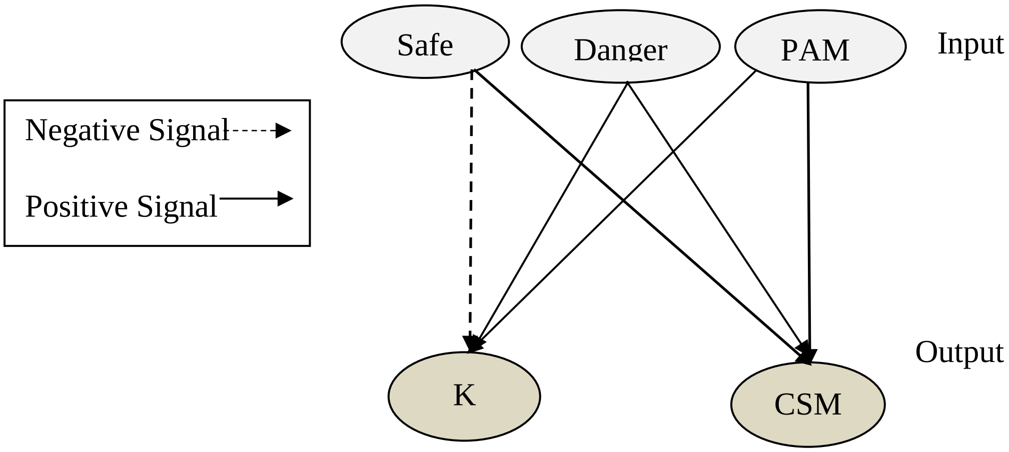


Fig. 3. Signal Transformation Process of the DCA (Adapted from [30])

3.2 Saaty Selection

Thomas Saaty created Analytical Hierarchy Process (AHP) [27] at the Wharton School of Business in the 1970s for asset, resource designation and for weapons tradeoffs. There he was stood up to with the issue of overseeing high costs and an expansive gathering of considerations with numerous components that conflicted with each other or were not adequately decided. AHP uses the judgments of boss to shape a deterioration of issues into levels of leadership. Issue versatile quality is addressed by the amount of levels in the hierarchy of leadership which join with the central's model of SESUG 2012.

The issue to be lit up. The levels of leadership is used to decide extent scaled measures for decision choices and the relative regard that alternatives have against progressive destinations (shopper devotion, thing/advantage, budgetary, human resource, and definitive ampleness) and wander risks. AHP uses lattice variable based math to manage components to meet up at a numerically perfect course of action. AHP is a period attempted method that has been used as a piece of multi-billion dollar decisions. AHP gets extent scales from coordinated connections of components and choice options. Normal applications where AHP has been used are in:

Sorting out components and necessities that impact programming change and productivity, Choosing among a couple of strategies for improving danger location highlights in motor vehicles, Estimating cost and booking choices for material requirements masterminding (MRP), Selecting needed programming portions from a couple programming dealers, Evaluating the way of research or wander recommendation. AHP moreover uses genuine measures like esteem, counts, or subjective evaluations as commitments to a numerical system. The yields join extent scales and consistency records surmised by figuring Eigen values and eigenvectors [25]. Saaty allowed a couple measures of anomaly (standard with subjective human judgment) when associated with the method of reasoning of slants. Abnormalities develop when taking a gander at three things, A, B, and C.

3.3 Sheep Flock

Sheep flock heredity model algorithm (SFHMA) is one of Evolutionary algorithms and are in fixed in accordance with optimum schedule. The Manufacturing cost minimization is to discover a timetable that fulfills the association's standards, machine allotment and Customers necessities. The Machine work designation plan is worried with doling out machine stack in light of necessities, allotting number of workers into a given arrangement of movements over a settled timeframe and week assignment. The various leveled approach, which was initially proposed by Brandimarte was actualized for definition of target capacity and tackling the planning issues with goal of minimizing assembling cost [27]. With a specific end goal to diminish the unpredictability, this strategy considering relegating machine assignment as sub issue and sequencing the request as another sub issue independently.

3.4 Negative Selection

Selection is an effective constrain in development, and it works from various perspectives. At last, notwithstanding, choice always deals with the variety that is created by transformations to choose the fit and expel the unfit, while disregarding unbiased changes. A couple of unmistakable sorts of determination in Fig. 3. Settling determination keeps the populace at one stable ideal esteem.

Directional determination changes the estimation of a characteristic by expanding the recurrence of people more like a removed ideal. Problematic choice builds the recurrence of vast and little estimations of a characteristic to the detriment of moderate qualities. Adjusting determination chooses the trade off among a few imperatives. On the off chance that negative choice is excessively powerless, making it impossible to expel unsafe changes, then injurious transformation aggregation will happen.

This can prompt to annihilation for a few animal types on the off chance that it proceeds sufficiently long; in any case, the subsequent far reaching presence of harmful transformations in such a genome will in the end addition-ally prompt to the event of back mutations, which (among numerous different variables) can essentially contribute toward support of a sensible level of respectability in the genome of different species in the long haul.

3.5 The Tolk-like Receptor Algorithm

The Tolk-like Receptor algorithm (TLR) combination of dendritic cells (DCs) and T-cells. The DCs has a function in TLR to gather antigen from an antigen store, and process signals. Other immunological approach for Intrusion Detection 225 ARIMA categories of input signals are not worked, with focusing on the nature of the relations between DCs and T-cells. In TLR, DCs are generated as immature detectors which signs and antigens for a limited indicated timeframe. On the off chance that the DC gets a flag amid antigen gathering, it is named develop, and on the other hand, DCs which did not recognize the nearness of a flag are named semi-mature.

Following is the list of acronyms used for AIS methods.

• DT	Danger Theory
• CAIS	Cooperative AIS
• SOM	Self Organizing Map
• IIS	Innate Immune System
• PAR	Principle Of Antigen antibody Reactions
• NS	Negative Selection
• ANN	Artificial Neural Network
• CS	Clonal Selection
• IIDA	Immune Intrusion Detection Algorithm
• DCA	Dendritic Cell Algorithm
• SFA	Sheep Flock Algorithms
• KM	K-Means
• DGA	Detector Generating Algorithm
• CA	Clever Algorithms
• SS	Saaty Selection
• AR	Algorithm Of Realization
• AD	Anomaly Detection
• MD	Malware Detection
• MCD	Malicious Code Detection
• ID	Intrusion Detection
• HIF	Harmful Information Filtering
• WSN	Wireless Sensor Networks
• TSFC	Two-Stage Fixed-Charge
• CC	Customer Clustering
• SIR	Symbol Images Recognition

4. SOLUTION TO THE RESEARCH CHALLENGES

Detailed DCA description was presented in previous section and a flowchart of the Enhanced DCA (EDCA) is shown in fig 4. EDCA is a variation of DCA that is designed to detect risk. EDCA has almost similar properties as described in the previous section but with the difference of recursive classification nature . EDCA collects signals from multiple data sources.Fig.4 shows that a DC processing a new output continuously with new signals and antigens are gathered at every DC maturing cycle. This allows a DC to gather signals representing a almost same context status despite being created asynchronously.

Information flow between signals and antigens is in a temporal style: antigens (interests) are collected when signals are created. Depending on signal type, pairing between signal and antigens is possible. For example a given antigen can be monitored by multiple signals in a contradictory manner "semi-mature" and "mature".

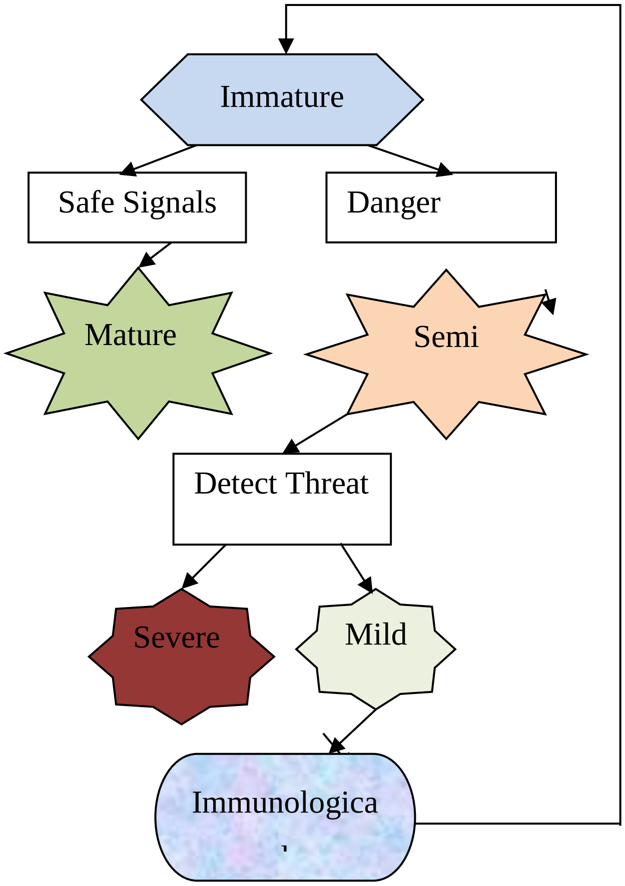


Figure 4. Flow of Enhanced Dentric Cell Algorithm

A final step by assigning a threat level. It is meant for detecting an on-going attack. EDCA detects an attack by monitoring a disobeying rate of given node via generated signals. After that the data (=antigens) for the next AIS algorithm pattern matching detection is gathered, which is necessary to generate responses. In replying, an AIS desires to react to a harmful antigen before it destroys the observed system and causes false signal generations. Artificial Immune Responder necessarily need pattern matching based detection. Therefore, EDCA also comprises of innate immune system that provides the context information with antigens matching to the adaptive immune system.

5. CONCLUSION AND FUTURE WORK

5.1 Conclusion

To sum up AIS algorithms are best for security purposes in terms of risk detection. The steps involved in the algorithm are based on few strong assumptions about the targeted domain. This paper presents the comprehensive survey of AIS algorithms for detection.

The purpose of this paper is to survey the AIS algorithms for risk detection and study their detection and classification and selection principles. We discuss in detail about few algorithms that support latest trends in research as well as keeping the base identity of AIS systems.

Then we propose that Dendric cell algorithm is best among all and enhanced Dendric cell algorithm was presented to fill the gaps in the very basic Dendric cell algorithm.

Table 2 Comparison of existing AIS Algorithms

Year	Ref.	AIS Methods	Approach	FS	SS	Eff	CC
2007	[2]	TLR	AD	M	N	L	M
	[18]	CAIS	MD	H	N	L	M
2008	[14]	DCA,SOM	MD	H	N	H	L
	[19]	IIS	M CD	M	Y	M	H
2009	[30]	POA	ID	L	N	L	H
	[8]	NS	ID	L	Y	L	H
2010	[9]	ANN	MD,IDS	M	Y	M	H
	[24]	CS	MD processes	H	Y	M	H
2011	[26]	IID	ID	L	Y	L	M
	[27]	AI	HIF	M	Y	M	M
2012	[20]	EN S	ID	M	Y	H	M
	[7]	DCA	MD	H	Y	H	L
2013	[22]	DCA	ID for WSN	H	Y	H	L
	[17]	HND	ID	M	Y	L	M
2014	[23]	SFA	TSFC	M	N	M	H

	[24]	KM	CC	L	N	H	M
2015	[20]	DGA	ID	L	N	M	L
	[7]	CA	CC	H	Y	M	H
2016	[20]	SS	1D local search	H	N	L	L
	[7]	AR	SIR	L	N	H	H

Fs-Focus on Security SS-Scalability Supported Eff-Efficiency CC-Computational Cost

5.2 Future Work

Following are the main issues need to be consider in future.

1) Scalability; this issue is not only related to AIS algorithms but also with other risk detection algorithms. There is a need to design an algorithm that is scalable with respect to number of inputs signal taken.
2) Security; further research is needed to investigate how to stop an intrusion so that clear and trust worthy classification is done by algorithms.
3) Heterogeneity; most of the algorithm even the Dendric cell lack versatility they deal with similar type of input signals. This issue need to be resolved in future.

REFERENCES

1. Greensmith. “Securing the Internet of Things with Responsive Artificial Immune Systems”, Proceedings of the 2015 on Genetic and Evolutionary Computation Conference - GECCO “15, 2015.
2. Chen, Liu C. and Xiao L. “A Security Situation Sense Model Based on Artificial Immune System in the Internet of Things”, AMR, vol. 403-408, pp. 2457-2460, 2011.
3. Ding, Jin Y., Ren L. and Hao K. “An Intelligent Self-Organization Scheme for the Internet of Things”, IEEE Computational Intelligence Magazine, vol. 8, no. 3, pp. 41-53, 2013.
4. Ning and Liu H. “Cyber-physical-social-thinking space based science and technology framework for the Internet of Things”, Science China Information Sciences, vol. 58, no. 3, pp. 1-19, 2015.
5. Sutavani, Bradley R., Ramage J., Jackson A., Durrant L. and Spendlove I. “CD55 Costimulation Induces Differentiation of a Discrete T Regulatory Type 1 Cell Population with a Stable Phenotype”, The Journal of Immunology, vol. 191, no. 12, pp. 5895-5903, 2013.
6. Gu, Greensmith J. and Aickelin U. “Theoretical formulation and analysis of the deterministic dendritic cell algorithm”, Biosystems, vol. 111, no. 2, pp. 127-135, 2013.
7. Greensmith, “Securing the Internet of Things with Responsive Artificial Immune Systems”, 2015.
8. Wu and Banzhaf W. “The use of computational intelligence in intrusion detection systems: A review”, Applied Soft Computing, vol. 10, no. 1, pp. 1-35, 2010.
9. Haktanirlar Ulutas and Kulturel-Konak S. “A review of clonal selection algorithm and its applications”, Artificial Intelligence Review, vol. 36, no. 2, pp. 117-138, 2011.
10. Zainal and Jali M. “A Perception Model of Spam Risk Assessment Inspired by Danger Theory of Artificial Immune Systems”, Procedia Computer Science, vol. 59, pp. 152-161, 2015.
11. Macpherson, Geuking M. and McCoy K. “Homeland Security: IgA immunity at the frontiers of the body”, Trends in Immunology, vol. 33, no. 4, pp. 160-167, 2012.

12. Greensmith. Dendritic Cell Algorithm, Ph.D. Thesis, The University of Nottingham, (2007).
13. Boshra Pishgoo ”STLR: A Novel Danger Theory Based Structural TLR Algorithm The ISC International Journal of Information Security” ,Volume 5, Number 2 (pp. 209225) July (2013)
14. Sun. ”Artificial Immune Danger Theory Based Model for Network Security Evaluation Journal Of Networks”, Vol. 6, No. 2, February 2011
15. Christian Lundquist Automotive. ” Sensor Fusion for Situation Awareness Linkping University”, SE-581 83 Linkping Sweden PhD thesis 2014
16. Li, Toulgoat M., Zhou Y. and Lamont L. “Logical Link Control and Channel Scheduling for Multichannel Underwater Sensor Networks”, ICST Transactions on Mobile Communications and Applications, vol. 12, no. 2, p. e2, 2012.
17. Kumaraswamy Y.S. ” Autonomic Self Healing Archi-tecture for Resiliency in Cyber Physical System International Journal of Multimedia and Ubiquitous Engineering”, Vol. 9, No. 11 (2014), pp. 75-84
18. Krishnamurthy. “Scalable Anomaly Detection And Isolation In Cyber- Physical Systems Using Bayesian Networks”, in Proceedings of DSCC 2014 ASME 2014 Dynamic Systems and Control Conference, 2014.
19. Kumaraswamy Y. “On Autonomic Self Healing Architec-ture for Resiliency in Cyber Physical System”, International Journal of Multimedia and Ubiquitous Engineering, vol. 9, no. 11, pp. 75-84, 2014.
20. Raciti. ” Anomaly Detection and its Adaptation: Studies on Cyber- Physical Systems”, PhD thesis 2013.
21. Sun. “Artificial Immune Danger Theory Based Model for Network Security Evaluation Journal Of Networks”, Vol. 6, No. 2, February 2011.
22. Chen, Liu C. and Xiao L. “A Security Situation Sense Model Based on Artificial Immune System in the Internet of Things”, AMR, vol. 403-408, pp. 2457-2460, 2011.
23. Weber. ”Internet of Things New security and privacy challenges”, Computer Law Security Review, vol. 26, no. 1, pp. 23-30, 2010.
24. Kannan, Govindan K. and Soleimani H. “Artificial immune system and sheep flock algorithms for two-stage fixed-charge transportation problem”, Optimization, vol. 63, no. 10, pp. 1465-1479, 2014.
25. Chiang, Chen N.J. ”Integration of artificial immune system and k-means algorithm for customer clustering. Applied Artificial Intelligence”, 28(6), 577-596, 2014.
26. Cheng and Kozikowski A. “We Need 2C but Not 2B: Developing Serotonin 2C (5-HT 2C) Receptor Agonists for the Treatment of CNS Disorders”, ChemMedChem, vol. 10, no. 12, pp. 1963-1967, 2015
27. Slesarev V. “The Algorithm of Artificial Immune System Simulation With Saaty Selection Operator And One-Dimensional Local Search.”, Scientific Bulletin of National Mining University, 2016.
28. Application of artificial immune systems combines collaborative filtering in movie recommendation system. In Computer Supported Cooperative Work in Design (CSCWD), Proceedings of the 2014 IEEE 18th International Conference. 2014, May 21. P. 279.
29. Artificial Immunity. Boundless, 2017. [Online]. Available: https://www.boundless.com/microbiology/textbooks/boundless-microbiology-textbook/immunology-11/classifying-immunities-146/artificial-immunity-735-5007/. [Accessed: 17- Jan- 2017].
30. Hypothetical definition and examination of the deterministic dendritic cell calculation. Bio-systems. 2013 Feb 28;111(2):127-35.

Consciousness Society Creation based on Natural and Artificial Intelligence

[1]Todoroi Dumitru, [2]Mihalcea Radu, [3]Todoroi Nicoleta, [3]Belinski Dumitru,
[4]Nechita Elena, [5]Belinski Tinca, [6]Vidu Ruxanda, [7]Micuşa Dumitru

[1]Academy of Economic Studies of Moldova
61, Mitropolit Gavriil Bănulescu-Bodoni Str., Chișinău, MD-2005, Republic of Moldova
E-mail: todoroi@ase.md

[2]Illinois University, Chicago, USA
1200 W Harrison St, Chicago, IL 60607, USA

[3]Academy of Muzics "Gh.Dima", Cluj-Napoca
Str. Ion I.C.Brătianu, nr. 25, 400079, Cluj-Napoca, Romania

[4]"V. Alecsandri" University at Bacău, Romania
157, Calea Mărăşeşti Str., Bacău, 600115, Romania

[5]LYNN University, Florida, USA
3601 N Military Trl, Boca Raton, FL 33431, USA

[6]University College Davis, California, USA
1 Shields Ave, Davis, CA 95616, USA

[7] Free International University of Moldova
52, Vlaicu Pircalab Str., Chisinau, MD-2012, Republic of Moldova

ABSTRACT

Consciousness Society is characterized by equality of structured Natural Intelligence (NIstructured) and Artificial (AI) ROBO-Intelligence. The purpose of research constitute adaptable algorithmic process of robotic implementation of Artificial, Robotic Intelligences (AI) elements; there are used Adaptable Tools as Technological information methodology basis. There are analyzed creative, emotional, temperamental, and sensual sets of **items** which are to be implemented in ROBO-intelligences**.** They represent one **axe** of robotic tables constituting first level of ROBO-intelligences elements. Another dimension of these tables represents items' evolution functions. Functions are located on other **axe** of robotic matrices. This second axe represents intellectual, emotional, sensual, and spiritual evolution **steps.** Using adaptable tools of algorithmic definitions of robotic elements are defined superior, next level elements of ROBO - intelligences. Presented adaptable information technology for ROBO-intelligence’s creation process is used in the institutional project "Creating Consciousness Society" that is developed in the period 2008 - 2018 by the team of AESM and supporters.

Keywords: consciousness, natural, artificial, intelligence, robot, creativity, adaptability, society

1. INTRODUCTION

Taking "A machine can act intelligently" as a working hypothesis, many researchers have attempted to build such a machine. **The purpose of the research** is to find out the common moral principles for Artificial and Natural Intelligence that would serve a basis for successful interacting of robots with humans in future Consciousness Society.

Creative ROBO-intelligences will possess features which characterize highly creative people (natural intelligence). Character’s creativity and emotion intelligences which are to be implemented in Character ROBO-intelligences and Emotional ROBO-intelligences are analysed and developed.

(1) **The last time in European Community.** Publications [1-3] confirm the **European Community** international interest [4] for AESM research results in the Branch of Conscience Society Creation process and in its engine for the process of creation ROBO-intelligences, represented by the Adaptable Tools.

(2) **Robots in Homo - Robotic Conscience Society. C**ommittee on the problems of the European Parliament endorsed the draft recommendations, as well as the administrative regulations on the civil-engineering production of robots. For that document voted PRO: 17 deputies, Against: 2 deputies, and Obtained: 2 deputies.

(3) **Robot’s Econometrics.** According to data of the European Parliament, in the period 2010-2014 the average sales of robots was 17% annual and in 2015 has risen to 29 percent. Growth of robots developed the volume of patents in relation to robots - in the last 10 years the volume has doubled. Artificial intelligence will determine economic efficiency in such spheres as manufacturing, commerce, transport, medical service, education, case-law and agriculture.

(4) Robot - legal status. It is not yet determined the **legal status of robots,** which soon will overwhelm us. Scientists are, as some carriers of artificial intelligence, provided with self-education capacity, separately, will need to be identified as "**electronic faces**" with corresponding Passport.

The document will contain the framework conditions for producers and users of robots, formulated since the great writer Isaac Azimov: 3 principles - the basic conditions in humans. collaboration with robots.

(5) Isaac Azimov: 3 principles. Asimov's Three Laws of Robotics, as they are called, have survived to the present:

1. Robots must never harm human beings or, through inaction, allow a human being to come to harm.
2.Robots must follow instructions from humans without violating rule 1.
3.Robots must protect themselves without violating the other rules.

2. CREATIVE APPROACHES FOR EQUALITY

Creative ROBO-intelligences (Creative IQ) will possess features which characterize highly creative people, Natural Intelligence (NIstructured).

Currently popular creative approaches include
- Statistical methods,
- Computational intelligence and
- Adaptable symbolic IQ.

There are an enormous number of tools used in AI, including versions of:
- search and
- mathematical optimization,
- adaptable systems,
- logic,
- methods based on probability,
- economics,
- and many others.

3. PROBLEM'S SOLUTION STEPS

It is known: To solve the problem, computer specialist classically must:
1) formulates the problem,
2) formalizes the problem,
3) creates the algorithm of its solution,
4) codes the algorithm with the help of one of the programming languages,
5) debugs the program,
6) gathers documentation and
7) uses and maintain the obtained program - product

2.1. Our goal is to use Adaptable Tools [5,11] to develop first 3 steps of the ROBO-intelligences creation.

2.2. **Intelligence evolution**: Piirto's 7i features which characterize highly creative people in ascending adaptable process of Piirto's Six Steps to the Creativity top develops next (2nd) level of IQ elements.

2.**3. Creative ROBO-intelligences [6]**

Creative ROBO-intelligences in Conscience Society (Creative IQ) will possess the first level intelligent features (Piirto's 7i):
1. inspiration,
2. imagery (imaginerie),
3. imagination,
4. intuition,
5. insights (înseninare, озарение),

6. improvisation, and
7. incubation
which characterize highly creative people

Creative IQ will be touched by the hierarchical process of (1st level) 6 steps to the Creativity top:
1. acquiring knowledge,
2. developing curiosity,
3. becoming interested,
4. passion,
5. dedication, and
6. professionalism

4. ROBO-INTELLIGENCES SOLUTION USING ADAPTABLE TOOLS

Adaptabily Tools [5] represent our solution for Robotic problem. The adapter, as a meta-system tool, supports adaptable software and hardware flexibility: extension and reduction of ROBO-intelligences possibilities.

By the help of adapter it can be presented **pragmatics, syntax, semantics, environment,** and **examples** of new or modified **(next, 2nd, level)** elements of ROBO-intelligences.

4.1. The 2nd Level IQ's elements: Adapter's general scheme:
_BL_ < Pragmatics of ROBO-intelligence element >
_SY_ < Syntax of ROBO-intelligence element>
(1)_SE _ < Semantics of ROBO-intelligence element>
_CO_ < Context of ROBO-intelligence element>
_EX_ < Examples of ROBO-intelligence element >
_EL_
and example (2) of it's implementation

4.2. The 2nd Level IQ's elements: Example: Using adapter it is defined one of the new (2nd level) ROBO's element "Inspired passion":
_BL_ < Inspired passion's pragmatics>
_SY_ < Inspired passion's syntax>
_SE _ < Inspired passion's semantics>
_CO_ < Inspired passion's usage context>
_EX_ < Inspired passion's examples call>
_EL

4.3. The 2nd Level IQ's elements: Commentaries:
(1) Pragmatics: name "Inspired passion";
(2) Syntax: "Inspiration in passion";

(3) Semantics: Correlation of functionalities of the 1st level of IQ elements: “Inspiration” and “Passion”;

(4) Usage context: Evaluation from “Inspired passion” situation “Inspiratio become interested” to the next (top) situation “Inspired professionalism”;

(5) Examples of “Inspired passion” (See: Next Table): “ROBO-intelligence became passionate by it business, it begin think to social profit.”

Table 1. The 2nd Level IQ’s elements

Creativity top versus Creative feature	**Acquire Knowledge**	**Develop Curiosity**	**Become Interested**	**Passion**	**Dedication**	**Professionalism**
Inspiration	**Inspiration in acquiring Knowledge**			**Inspired passion**		
Imagery		**Imagery developing Curiosity**				
Imagination			**Imagination becoming interested**			
Intuition				**Intuition’s passion**		
Insights					**Insights dedication**	
Improvisation						**Improvisation in professionalism**
Incubation		**Incubation developing Curiosity**				

4.4. The 2nd Level IQ's elements (*Table 1*): Theorem "Creative ROBO-intelligence"

If there are done:

- the 1st level of Creative ROBO-intelligence's Piirto's 7i features which characterize highly creative people,
- the 1st level of Creative ROBO-intelligence's Piirto's six steps of the creativity top, and
- Adaptable tools

it is possible to create all 2nd level elements of Creative ROBO-intelligence based on these IQ's 1st level elements.

Table 2. Adaptable evaluation steps

Evolution of Emotions	Self-awareness	Managing emotions	Motivation	Empathy	Handling relationships
Happiness	Happiness self-awareness				
Fear					Fear handling relationships
Surprise		Surprise managing			
Disgust			Disgust motivation		
Sadness					
Anger				Anger empathy	

5. EMOTIONAL INTELLIGENCE

Emotional ROBO-intelligence (EQ) refers to artificial (robotic) intelligence's ability to monitor their own and other intelligence's emotional states and to use this information to act wisely in relationships.

5.1. The 1st level of EQ elements: basic emotions.

Many psychologists believe that there are six main types of emotions, also called basic emotions. They are: 1.Happiness, 2. Sadness, 3. Fear, 4. Anger, 5. Disgust and 6. Surprise.

5.2.Adaptable evaluation steps (*Table 2*): the 2nd level EQ elements

Emotional intelligence's adaptable evaluation steps are represented by:
1) Self-awareness: recognizing internal feelings;
2) Managing emotions: finding ways to handle emotions that are appropriate to the situation;
3) Motivation: using self-control to channel emotions toward a goal;
4) Empathy: understanding the emotional perspective of other people;
5) Handling relationships: using personal information and information about others to handle social relationships and to develop interpersonal skills

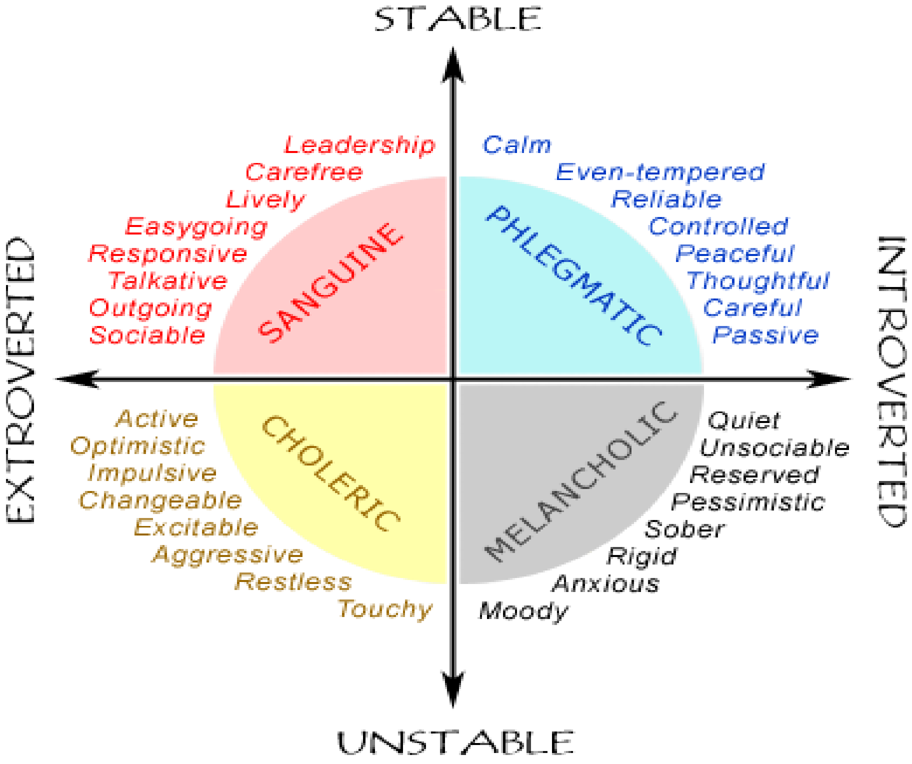


Figure 1. Temperaments

6. ROBO-TEMPERAMENTS

6.1. ROBO-Temperaments 1st level EQ elements

There exist four temperaments that a relatively simple but powerful way of classifying personalities: Melancholic, Phlegmatic, Choleric, and Sanguine

6.2. Theorem “Sanguine ROBO-intelligence”

If there are done:

- the main features, characteristics, and functions of Sanguine type of temperaments (*Figure 1*),
- the Piirto’s 7i features which characterize highly creative people, and
- Adaptable Tools

it is possible to create Sanguine ROBO-intelligence with such features of creative artificial intelligence.

6.3. The 2nd level of Character ROBO-intelligences with seven features which characterize highly creative intelligence.

In the *Table 3* there are present some 2nd level elements o IQ which are presented by adaptable algorithms created on the base of temperament characteristics in composition with the seven features which characterize highly creative intelligence.

6.4. The 2nd level of Character ROBO-intelligences evolution with Piirto’s Six Steps to the Creativity top

In the *Table 4* there are present some 2nd level elements o IQ which are presented by adaptable algorithms created on the base of temperament characteristics in composition with the Six Steps to the Creativity top.

6.5. Theorem “Choleric ROBO-intelligence”

If there are done

(1) the main features, characteristics, and functions of Choleric type of temperaments; (2) the first level Six Steps to the Creativity top elements of Character ROBO-intelligence (*Table 4*), and

(3) Adaptable Tools

it is possible to create Choleric ROBO-intelligence.

6.6. Theorem “Emotional Phlegmatic ROBO-intelligence”

If there are done:

(1) the main features, characteristics, and functions of Phlegmatic type of temperaments,

(2) the first level Six Types of emotions elements of Character ROBO-intelligence, and

(3) Adaptable Tools

it is possible to create Emotional Phlegmatic ROBO-intelligence.

6.7. Hierarchy of theorems

Demonstration of Theorem “Choleric ROBO-intelligence” is based on such Lemmas as “Choleric acquires Knowledge”, “Choleric develop Curiosity ” and so on, which demonstrate the process of adaptable creation of 2nd level elements of Character ROBO-intelligences.

Table 3. Temperament & Creativity

Creative feature versus Personality	**Inspiration**	**Imagery**	**Imagination**	**Intuition**	**Insights**	**Improvisation**	**Incubation**
Choleric	Choleric's Inspiration	Choleric's Imagery			Choleric's Insight		
Sanguine				Sanguine's Intuition		Sanguine's Inprovisation	
Phlegmatic	Phlegmatic's Inspiration						**Phlegmatic's Iprovisation**
Melancholic	**Melancho-lic's Inspiration**		**Melancholic's Imagination**				

Human Aura in very important part is created by the energies eliminated by the creative, emotion, temperament, sensual human elements. Such energies have to constitute the basis for creating of

ROBO-intelligences Aura.

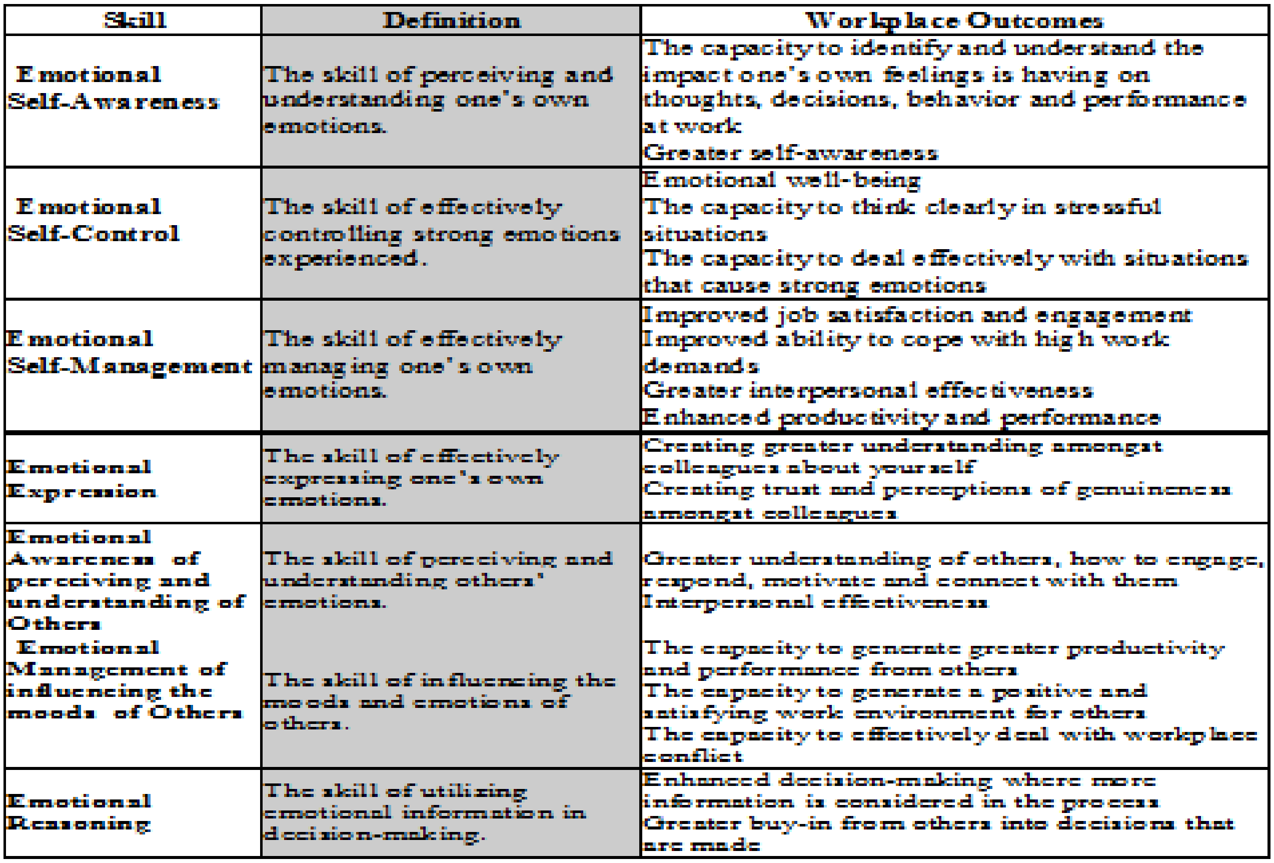
Table 4. Temperament & Creativity evolution

Creativity top versus Peronalities	**Acquire Knowledge**	**Develop Curiosity**	**Become Interested**	**Passion**	**Dedication**	**Professionalism**
Choleric		Choleric develop Curiosity				
Sanguine	Sanguine acquires Knowledge				Sanguine's dedication	
Phlegmatic			Phlegmatic become Interested			
Melancholic				**Melancholic passion**		**Melancholic professionalism**

7. ENERGETIC MEASURES

Genos Emotional Intelligence Inventory (**Genos EI:** ***Table 5***) is a **360-degree measure** of energies of emotionally intelligent workplaces and behaviour. It represents first step of measure of human body energies to be implemented in creation the robotic Aura.

Table 5. Genos EI



Skill	Definition	Workplace Outcomes
Emotional Self-Awareness	The skill of perceiving and understanding one's own emotions.	The capacity to identify and understand the impact one's own feelings is having on thoughts, decisions, behavior and performance at work Greater self-awareness
Emotional Self-Control	The skill of effectively controlling strong emotions experienced.	Emotional well-being The capacity to think clearly in stressful situations The capacity to deal effectively with situations that cause strong emotions
Emotional Self-Management	The skill of effectively managing one's own emotions.	Improved job satisfaction and engagement Improved ability to cope with high work demands Greater interpersonal effectiveness Enhanced productivity and performance
Emotional Expression	The skill of effectively expressing one's own emotions.	Creating greater understanding amongst colleagues about yourself Creating trust and perceptions of genuineness amongst colleagues
Emotional Awareness of perceiving and understanding of Others	The skill of perceiving and understanding others' emotions.	Greater understanding of others, how to engage, respond, motivate and connect with them Interpersonal effectiveness
Emotional Management of influencing the moods of Others	The skill of influencing the moods and emotions of others.	The capacity to generate greater productivity and performance from others The capacity to generate a positive and satisfying work environment for others The capacity to effectively deal with workplace conflict
Emotional Reasoning	The skill of utilizing emotional information in decision-making.	Enhanced decision-making where more information is considered in the process Greater buy-in from others into decisions that are made

8. CONCLUSION

The 1st step. To create ROBO-intelligences which possess 1st level elements – intelligences, emotions and temperaments – it is necessary first of all to introduce them in robotic heart and robotic head.

This consists in creation corresponding Computer Based Information Systems for each of: Intelligences (7i), Tops (6s), Emotions (6), Temperaments (4), and Sentiments (positive & negative)

The 2nd step. Next step in creation process of ROBO-intelligences consists in elaboration of their 2nd level elements based on its 1st level elements using Adaptable Tools for its definitions.

The 3rd step. Each definition of ROBO-intelligences 2nd level elements is composed from definition of such it's characteristics as: pragmatics, syntax, semantics, environment, and examples. These definitions represent the Adaptable Algorithmic Knowledge Robotic Base which help to create real ROBO-intelligence using Adaptable Tools for its development, verification, and experimentation.

The **4th step. Measure** of ROBO-intelligence energies for each creativities, emotions, temperaments, sentiments.

These measures represent the Energetic Knowledge Robotic Base which help to create real ROBO-intelligence using Adaptable Tools for its development, verification, and experimentation.

Consciousness Society Creation Theorem: Having the Enegetic Knowledge ROBO-intelligence Warehouse it is possible algorithmically to implement in ROBO-intelligences the creative, emotion, temperament and sensual human characteristics!

REFERENCES

1. Todoroi D. Conscience Society Creation, 6th Edition, ARA Publisher, University of California Davis, USA, 2017, 236 pages, ISBN: 978-1-935924-21-0, (Proc. Of the 6th international TELECONFERENCE of young researchers "Conscience Society Creation", April 21-22, 2017, Bacău-Bucureşti-Boston-Chicago-Chişinău-Cluj Napoca-Florida-Iaşi-Los Angeles), http://www.AmericanRomanianAcademy.org.

2. Todoroi D. Creative Robotic Intelligences, Editions Universitaires Europeennes, Saarbrucken, New York, 2017, 123 pages, ISBN: 978-3-639-65426-4.

3. Todoroi D. Creativity in Conscience Society, LAMBERT Academic Publishing, Saarbrucken, Germany, 2012, 120 pages. ISBN: 978-3-8484-2335-4

4. Moldova Suverana, 25.01.2017, Nr. 8(2095), utro.ru

5. Todoroi D., Micuşa.D. Sisteme adaptabile, Editura Alma Mater, Bacău, România, 2014, 148 pagini. ISBN 978-606-527-347-4.

6. Todoroi D. Crearea societăţii conştiinţei, Materialele primei Teleconferinţe Internaţionale a tinerilor cercetători "Crearea Societăţii Conştiinţei", 7-8 aprilie 2012, Chişinău, 169 pages / coord.: Dumitru Todoroi: ASEM, ARA, UAIC, ASE. ISBN 978-9975-75-611-2.

7. Society Consciousness Computers, Volume 1, 2014, Alma Mater Publishing House, Bacău, /Honorary Editor Dumitru Todoroi, Editor in Chief Elena Nechita/, 176 pages. ISSN 2359-7321, ISSN-L2359-7321.

8. Todoroi D. Crearea societăţii conştiinţei, MaterialeleTeleconferinţei Internaţionale a tinerilor cercetători "Crearea Societăţii Conştiinţei", Ed. a 3-a, 11-12 aprilie 2014, Chişinău, 129 pagini / coord.: Dumitru Todoroi: ASEM (Chisinau, Republic of Moldova), ARA (CalTech, Los Angeles, USA), UAIC (Iashi, România), ISU (Chicago, USA), UB (Bacău, România), UC (Cluj, România), ASE (Bucharest, România). ISBN 978-9975-75-612-6.

9. Society Consciousness Computers, Volume 2, Bacău-Bucureşti-Chicago-Chişinău-Cluj Napoca-Iaşi-Los Angeles, 2015, Alma Mater Publishing House, Bacău, 81 pages, ISSN 2359-7321, ISSN-L 2359-7321.

10. Society Consciousness Computers, Volume 3, Bacău-Bucureşti-Boston-Chicago-Chişinău-Cluj Napoca-Iaşi-Los Angeles, May 2016, Alma Mater Publishing House, Bacău, 183 pages, ISSN 2359-7321,ISSN-L2359-7321

11. Todoroi D. "Adaptable ROBO-intelligences". // Proc. of the 41th ARA Congress, Craiova, Romania, July 19-July 22, 2017, ARA Publisher, University of California Davis, USA, ISBN: 978-1-935924-21-0 (To be published), http://www.AmericanRomanianAcademy.org/

2. IT in DISTANCE LEARNING EDUCATION

Advanced Distributed Learning in Military Specialists Training

[1]Perju Veaceslav, [2]Bucliş Mihai , [3]Sofronescu Igor

[1]Institute of Advanced Information Technologies, FIUM
52, Vlaicu Pircalab Str., Chisinau, Republic of Moldova
Tel: (373)79431225, e-mail: vlperju@yahoo.com

[2]Republic of Moldova National Army General Stuff
84, Hincesti Str., Chisinau, Republic of Moldova
E-mail: mihail.buclis@army.md

[3]Armed Forces Military Academy ”Alexandru cel Bun”, Republic of Moldova
23, Haltei Str., Chisinau, Republic of Moldova
E-mail: igor.sofronescu@academy.army.md

ABSTRACT

In the article was described the system of military specialists training in different countries and institutions. There were presented the trends in military specialists training based on Information Technologies and Advanced Distributed Learning (ADL). There were determined ADL Capacity Building. It is described situation regarding ADL in military academies and civil universities. There were presented the educational architectures for preparing of the military specialists in civil universities. It was selected a set of the courses which can be successfully used for preparing of the military specialists in civil universities.

1. INTRODUCTION

The necessity to enhance the security on the regional and multinational levels, the processes of the international consolidation and globalization increase the requirements to the quality of the military specialists training in civil and military sectors of education.

Taking into account this fact, in the article was analyzed the systems of military specialists training in different countries and institutions (chapter 2).

It was described one of the trends in military specialists training based on Information Technologies and Advanced Distributed Learning (chapter 3). It was established that exists the ADL Capacity

Building which consists of legislative basis for distance learning education, the methodological basis of the this kind of education, interuniversity communication networks. It was analyzed the experience and successes of the Partnership for Peace Consortium of Defense Academies and Security Study Institutes (PfPC) in the elaboration and implementation of the learning management system ILIAS, different courses elaborated by the countries members of the PfPC. It is proposed to use the LMS ILIAS for preparing of the military specialists in civil universities.

It is described the situation regarding advanced distributed learning in military academies (chapter 4) and civil universities (chapter 5). There were described the educational architectures for preparing of the military specialists in civil universities using LMS ILIAS (chapter 5).

It was selected a set of the courses from PfPC server which can be successfully used for preparing of the military specialists in civil universities (chapter 6).

2. SYSTEMS OF MILITARY SPECIALISTS PREPARING

At present in NATO countries the military specialists are prepared in military academies. In many countries from former Soviet Union exists a distributed system of military specialists training. In accordance with this system, the military specialists there are prepared in the Military Academies (operating officers) and in the civil universities (officers of reserve). In second group of countries annually more than 90% of the graduates militaries are prepared in the civil universities [1].

The necessity to enhance the security on the regional and multinational levels, the processes of the international consolidation and globalization increase the requirements to the quality of the military specialists training in civil and military sectors.

3. TRENDS IN DISTANCE LEARNING EDUCATION

One of the modern and effective directions of high quality military specialists training is based on the Information Technologies (IT) and Distant Learning Education (DLE) or Advanced Distributed Learning (ADL).

There were formed the main directions of activities in DLE such as[2-4]:

1. Creation of the interuniversity communications network;
2. Elaboration of the methodological basis of the DLE;
3. Selection/elaboration of the LMS for DLE;
4. Creation of the DLE laboratories in the universities;
5. Elaboration of the educational plans;
6. Preparing of the teachers;
7. Creation of the electronic courses;
8. Creation of the digital libraries etc.

Due to set of the USA, European and NATO projects, in many EU countries and some countries from former Soviet Union (Republic of Moldova, Ukraine, Belarus, Georgia, Armenia, Azerbaijan) there were created the interuniversity research and education communication networks. At present, the majority of the universities are connected to Internet via this networks to the European network GEANT, which permit the access to different educational and scientific databases.

There have been performed a number of research activities and experimental tests regarding the integration of innovative methods and modern information technologies, including DLE, in education.

Some significant results of these activities represent the elaborated documents: Distance Learning Concept and Terminology. Initiation Guide; Development of the information resources for distance education; Computer assisted testing. Methodology; The study guide on the development of information resources for distance education; The Introduction to distance education; The Glossary of terms used in the distance education; The computer-aided testing methodology.

One of the key components in DLE represents Learning Management System (LMS). In different universities there were studied the research/testing/elaboration of the LMS for DLE, such as: AEL (Advanced E-Learning),   Moodle (Modular Object-Oriented Dynamic Learning Environment), ILIAS, Claorline, Dokheos etc.

The AEL (Advanced E-Learning) system developed by the company SIVECO and used in the schools and lyceums.
Another studied system was Moodle (Modular Object-Oriented Dynamic Learning Environment), which from the point of view of the performance is one of the most powerful and most commonly used open platforms for e-learning.

Of a great interest is the LMS ILIAS, elaborated by Partnership for Peace Consortium of Military Academies and Security Studies Institutes (PfPC). This LMS integrate the necessary functions and advantages of other LMS, and it is in the permanent development taking into account the requirements of the users. Another very important aspect represents the e-courses, created by PfPC countries members.

4. ADVANCED DISTRIBUTED LEARNING IN MILITARY ACADEMIES

Advanced Distributed Learning was implemented in the educational and training process in many Military Academies from NATO and partner countries[5].

For example, in Armed Forces Military Academy "Alexandru cel Bun" from Republic of Moldova was created Continuous Training Centre, Military Academy becomes a member of the ADL

Working Group within the Partnership for Peace Consortium, there were elaborated different on-line courses[1, 6].

The implementation of ADL in the Military Academy it was an important step in the military development in the National Army, contributing to the use of new knowledge through modern efficient learning allowing access without geographical borders. This form of learning has provided training military personnel from the army in accordance with the requirements and international quality standards.

5. PREPARING OF THE MILITARY SPECIALISTS IN THE CIVIL UNIVERSITIES

Military departments of the civil universities do not using ADL training technologies at present. Taking into account this fact and the good successes of the military academies and PfPC in direction of the elaboration and development of the Learning Management System, SCORM Editor, DB of the courses, we propose to introduce ADL technologies for military specialists training in civil universities.

The main directions of activities to realize this proposal are:

1. Establishment of a good cooperation between universities and institution of the central public administration in education - responsible for education process in the civil universities, and Ministry of Defense – responsible for education at the military departments in the civil universities;

2. Elaboration of the methodology of the military specialists preparing in the civil universities using LMS ILIAS;

3. Creation of the ADL laboratories in the universities;

4. Acknowledgment of the universities with the LMS, SCORM Editor, PfPC DB of the courses;

5. Development of the interuniversity communication networks;

6. Organization of the seminars, trainings, consulting; Implementation of the LMS in the civil universities;

7. Elaboration of the e-courses for military specialties.

There were proposed the possible educational architectures (EA) using LMS (Figures 1-3). The architecture EA1 is destined for the utilization of the LMS to access the PfPC courses(Figure 1). The architecture EA2 (Figure 2) supposes the utilization of the LMS for local DLE. The architecture EA3 (Figure 3) supposes the utilization of the LMS for PfPC and local DLE.

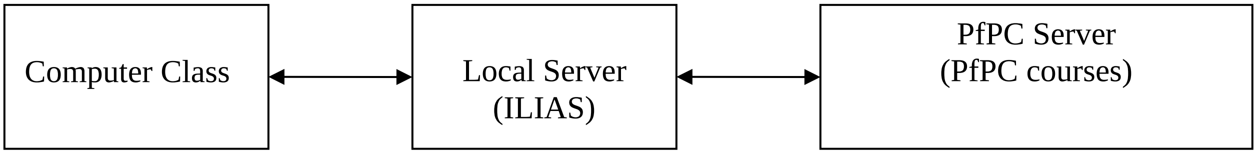


Figure 1. The educational architecture 1: the utilization of the ILIAS to access the PfPC courses (the standard PfPC educational architecture)

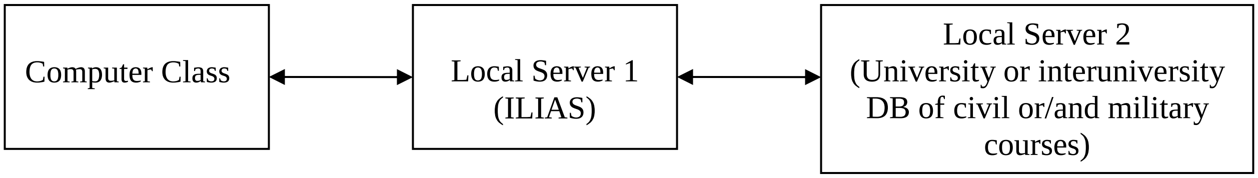


Figure 2. The educational architecture 2: the utilization of the LMS for the local DLE

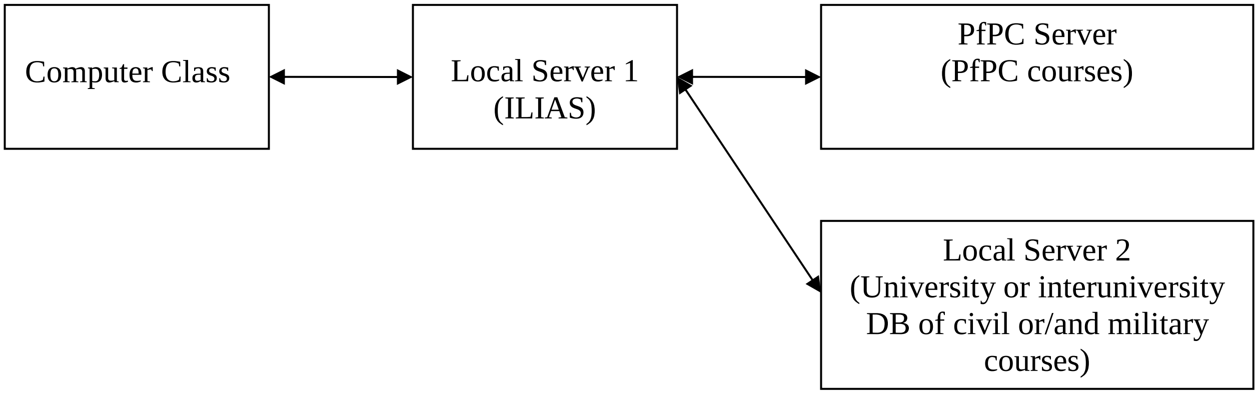


Figure 3. The educational architecture 3: the utilization of the LMS for the PfPC and local DLE

8. E-COURSES FOR MILITARY SPECIALISTS TRAINING

The results of the analysis of the electronic courses elaborated in the universities shows that in different universities the courses on the same subject are different due to different curricular. It is necessary to create an interuniversity education commission for elaboration of the unique curricular. The existing electronic courses have to be developed to be used by LMS.

We analyzed the courses from PfPC server and selected a part of them which can be successfully used for military and civil specialists preparing in the civil universities:

1. English Language Training Enhancement Course.
2. Developing Security Strategy: the U.S. Approach.
3. Building Defense Institutions
4. Chemical and Biological Weapons Non-Proliferation
5. CIMIC Overview for NATO SCHOOL
6. Combating Trafficking in Human Beings
7. Conducting a Computer Assisted Exercise
8. Conflict Management and Negotiation
9. Critical Infrastructure Awareness
10. Defense Against Suicide Bombing
11. English Skills for Staff Officers
12. Ethnic Conflict and Peace Operations: European Security and Defence Policy
13. Fundamentals of CBRN Defense
14. Human Trafficking: Causes, Consequences, Counter-strategies
15. Introduction to Human Rights: Introduction to Information Operations
16. Introduction to International Humanitarian Law
17. Introduction to NATO Introduction to Satellite Operations
18. International Security Risks (Drugs, Migration, Climate, Finance, Terrorism)
19. Information Security Fundamentals: Introduction to Medical Intelligence
20. Map Reading Multinational Crisis Management
21. National Security and Defense Strategy Estrategia de Seguridad y Defensa Nacional: NATO Partner Joint Medical Planners' Course
22. NATO Major Incident Medical Management
23. NATO/Partner Operational Staff Officer's Module: NATO Partner Senior Medical Staff Officers' Course Module
24. NATO's Space Support
25. NATO's Reserve Forces
26. NATO Modeling and Simulation (M&S) Orientation Course: Operations in the Information Age Peace Keeping Techniques Security in the Information Age: SPIRIT: Security Policy, International Relations, and Information Technology
27. Combating Terrorism and Illegal Trafficking Combined Joint Task Force Training Modules
28. Intro to Environmental Awareness: Law of Armed Conflict: NATO Peace Support Operations
29. European Politics, Security and Economy: Introduction to NATO Public
30. Information   Resource Management in NATO

9. CONCLUSION

1. There are described the systems of military specialists training in NATO countries and some countries from former Soviet Union. It is stipulated than in second group of countries annually more than 90% of the graduates militaries are prepared in the civil universities.

2. There were presented the trends and obtained results in distance learning education – formation of the main directions of activities; creation of the interuniversity research and education communication networks; experimental tests regarding the integration of innovative methods and modern information technologies in education; analysis of the different Learning Management Systems.

3. There are described the results of the advanced distributed learning implementation in the educational and training process in Military Academies from NATO and partner countries and at the military specialists preparing in the civil universities.

4. It is proposed to introduce ADL technologies for military specialists training in civil universities. There are formulated the main activities in this direction. There were proposed the possible educational architectures. There were analyzed the courses from PfPC server and selected a part of them which can be successfully used for military and civil specialists preparing in the civil universities.

REFERENCES

1. Perju V., Bucliş M., Sofronescu I., Orlov D. ADL Based Military Specialists Training in Republic of Moldova. Revista Militară, nr.2, 2016, p.143-150 (0,5 c.a.)
2. Perju V. Distance Learning Education in Republic of Moldova. Partnership for Peace Consortium of Defense Academies and Security Studies Institutes, Advanced Distributed Learning Working Group Conference, May 18-21, 2010, Chisinau, Republic of Moldova.
3. Perju V. Military /civil ADL Capacity Building in Moldova. The Partners View: Best Practices and Way Ahead. 13th Annual Conference of Partnership For Peace Consortium of Defense Academies and Security Studies Institutes. George C. Marshall Center, Garmisch-Partenkirchen, Germany, 21-24 June 2011.
4. Perju V. Military - civil ADL activities in the Republic of Moldova. Partnership for Peace Consortium of Defense Academies and Security Studies Institutes, Advanced Distributed Learning Working Group Conference, November 1-3, 2011, Tbilisi, Georgia.
5. Advanced Distributed Learning. https://pfp-consortium.org/index. php/activities/advanced-distributed-learning
6. Education on distance. http://www.academy.army.md/studii/invatamint-distribuit-la-distanta.

Efficient IT Methodologies in Games Creating for E-Learning Education

Seiciuc Victor

Moldava State University
60, Alexei Mateevici str., Chisinau, MD-2009, Republic of Moldova
Tel: 37369238003, e-mail: runsmaric@gmail.com

ABSTRACT

Development of some efficient IT methodology in creation of games for e-learning education on mobile devices and PC, are elaborated and described. There are described steps, elements and events that ensure elaboration of the games, using minimum time and IT resources. Elaborated are the artificial intelligence elements that allow the categorization of the proposed games as intelligent support systems.

Keywords: information, technologies, methodology, creation, games, e-learning, education, mobile, device, system

1. INTRODUCTION

Video Games and *distance eLearning* play an important role in the daily life of students. These two activities can be combined so that the educational effect becomes as effective as possible. *Video Games* - Business and highly profitable training. *Initial* - execution on PC or on console devices with TV connection. *Currently* - use of mobile devices equipped with modern Technology, created by giant companies Google, Apple, Amazon, Microsoft, Blackbery etc. *As a result* - demand for games in the informatics market has increased considerably; - modern *IT Methodologies* for creation game - making technologies are very appreciated.

Proposed *IT Methodologies* can create *Video Games* using minimum resources. These *Video Games* can be adapted and used as effective tools in training on Learning Management System (LMS) which is an essential tool for eLearning professionals. Fortunately, there are a variety of different Open Source LMSs that can offer you the dynamic and flexible eLearning platform you need.

Here are the top of Open Source LMS solutions you can to consider (see [1-2]): Moodle, ATutor, Eliademy, Forma LMS, Dokeos, ILIAS, Opigno, OLAT, AeL, etc.

2. THE BASIC GOALS OF THE IT METHODOLOGY AND STAGES OF GAME DEVELOPMENT

The proposed and developed *IT Methodology* represent a set of Programs and Computer Techniques organized in such a way, to allow creation on PC or on mobile device the desired Game, using minimum time and IT resources.

The basic *goals* of the proposed *IT Methodology* are to ensure (see [3]):

(1) The *simplicity* and *comfort* of the building process of needed applications in Games elaboration;

(2) Minimal *time* and *IT resources* in creation a certain type of Game requested by the customer.

The *stages* of Game development are:

(1) *Writing scripts*;
(2) *Integrating sound objects*;
(3) *Integrating graphic objects*;
(4) *Creating the actions and the functional elements for their management*;
(5) *Compiling and exporting to mobile platforms*;
(6) *Testing the application;*
(7) *Final on-line realization.*

Concurrently with Computer Techniques for create of Games, are exposed adjustment and delivery Tools of completed Games on widely known on-line Platforms (Figure 1).

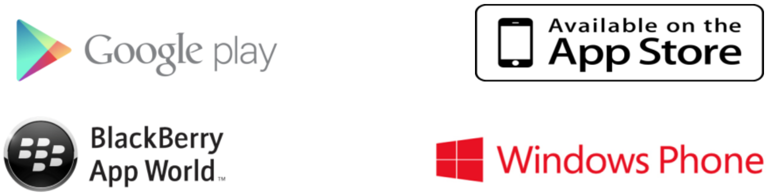


Figure 1. *On-line Platforms for created Games.*

3. IMPLEMENTATION OF IT METHODOLOGY IN GAMES DEVELOPMENT

This *IT Methodology* can be applied to the development different types of *Video Games*, for example: 1) *Arcade*; 2) *Simulators*; 3) *Action*; 4) *Platforms*; 5) *Speed*; 6) *Training*; 7) *eLearning*; 8) *Gambling*, etc.

The spectrum of use is greatly and depends of the imagination and the developer's purpose. Overall the *Video-Game* is organized on several *levels*. Each *level* contains its characteristic *elements (buttons)* that are responsible for the realization of certain concrete *events*, which lead step by step to the full development of the *Video-Game* in question.

Remark 1. The *result* of the *actions* made by activating the *Video-Game* buttons are still called *events*, and the respective *buttons* are called *functional elements* of this *Video-Game*.
Any *functional element* of the *Video-Game* disappears when it is activated and the resulting *events* occur. *Events* may be one or more.

Remark 2. We call the *purpose event*, the one who achieves the main result in the *Video-Game* level. Otherwise, the *event* is called an *attendant event*.

4. RESULTS: EXAMPLES OF VIDEO GAMES

Action Game - *Izolda Ninja Girl* (Figure 2 - Figure 7). It's a fun game, developed for mobile platform Google Play. The game contains three objects with ten levels of play in which the player passes various obstacles and faces different opponents.

Figure 2. *Game-Izolda Ninja Girl.*

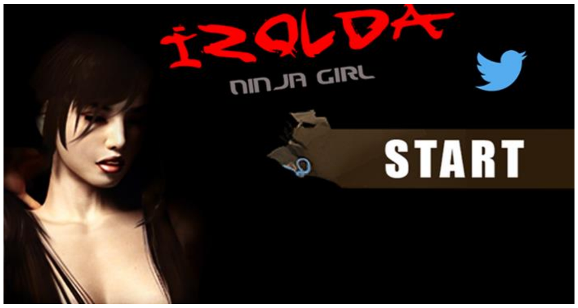


Figure. 3. *Izolda Ninja Girl - Main menu.*

Object no.1 is the *Main menu* (Figure 2 - Figure.3). The *Main menu* contains the Start menu *elements* and *events*. It contains the *functional elements: Start button* - for launching the first play level of the Game, *Twitter social button* - to share experiences; *Graphic elements* - Game name and Icon of main character. The *Purpose event* in the *Main menu* is to activate the first play level of the Game *Izolda Ninja Girl.* The *Attendant event* is communication on Twitter.

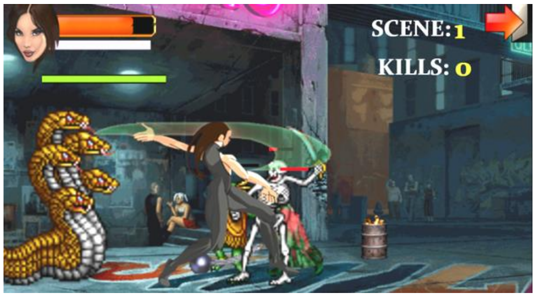


Figure 4. *Level 1. Game actions*

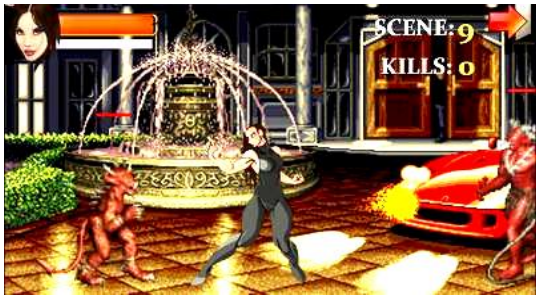


Figure 5. *Level 9.Game actions*

Object no.2 is the compartment in which the actions of the Game take place. Here the user identifies himself with the main character, who is to perform the tasks of the Game (Figure 4 - Figure.7). The compartment is made up of ten levels. They contain all the components of the Game: main and auxiliary characters, battle scenes, sounds, bonuses, current information panels, stop Game - continue Game - exit Game, etc.

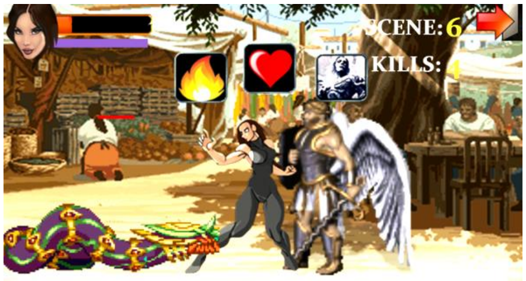


Figure 6. *Level 6. Game bonuses*

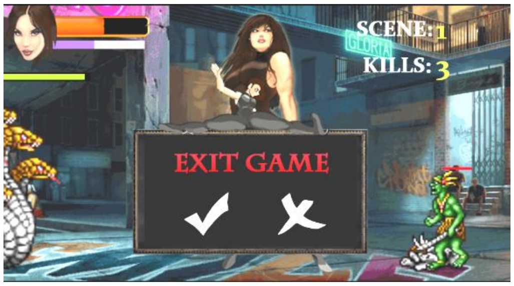


Figure. 7. *Level 1. Stop Game*

Here are the following *elements (buttons)* and *events*: *Touch screen button* - for launching the movement for main characters. If the characters are near, then the movement passes automatically into battle scenes; *stop Game button* - the top right arrow, fig. 4-6; *continue Game button* and *exit Game button*- see fig. 7; *bonuses buttons*, fig. 6: *fire* - to weaken the Monsters, *heart* - to regenerate the energy level of the main character, *invincible angel* which helps you fight for 30 seconds.

Current information panels show: energy level (the red line) and bonus staging level (blue line) of the main character; energy level of the auxiliary characters; the number of Monsters destroyed; the number of the scene. The *purpose event* in the play levels of the Game is to destroy the Monsters and to move to the next level. Everything else are *attendant events*.

Object no.3 is the compartment in which one of two options is made: 1) Displaying the information that the Game has been *successfully completed*. 2) unlimited *automatically restart* in the level where the main character was destroyed and the possibility to continue the Game.

Elements of *Artificial Intelligence*. The *main character* as well as auxiliaries (*Monsters*) possesses elements of *Artificial Intelligence*, allowing them to interact by themselves. It is composed of the following parameters: 1) moving and stopping the movement, 2) recognition to the target object and distance calculation to him, 3) change of animation and behavior, 4) combat mode, 5) regeneration.

Conclusion 1. The presence of *Artificial Intelligence* elements classifies the *characters* as some *Intelligent Support Systems* (see [4]), depending on the possibilities of making decisions by themselves.

Conclusion 2. Depending on the *purpose event*, the Action Game - *Izolda Ninja Girl* turns from a *System Support for Decisions* to *Intelligent Support System*.

Speed Game – *Space Runner* (Figure 8. - Figure. 11). It's a Game of speed and reaction, developed for mobile platform Google Play. The *Main menu* contains two variants of the Game: 1) *button Map 1*- obstacles to fall into the deep, 2) *button Map 2*- obstacles over which is jumping. In the *Start menu* we have the *button Tap* for Start the Game. *Touch screen button* - for jump over obstacles (Figure 10. - Figure. 11). The *purpose event* in the Game is to jump over obstacles and accumulate *maximum points.* The *attendant events* - communication on Twitter, etc.

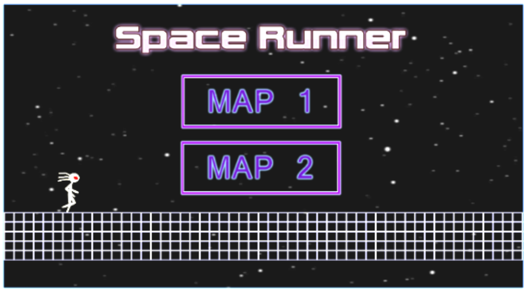


Figure 8. *Space Runner- Main menu*

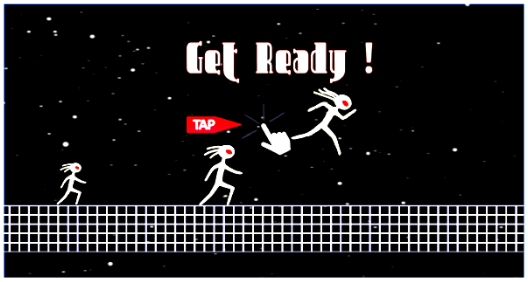


Figure. 9. *Space Runner- Start menu*

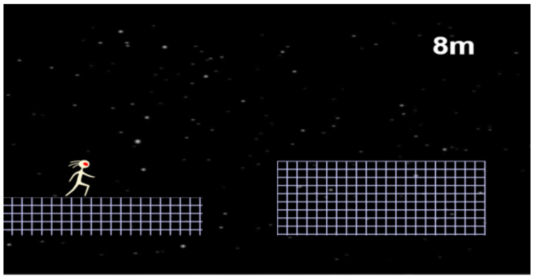


Figure 10.*Obstacles to fall into the deep*

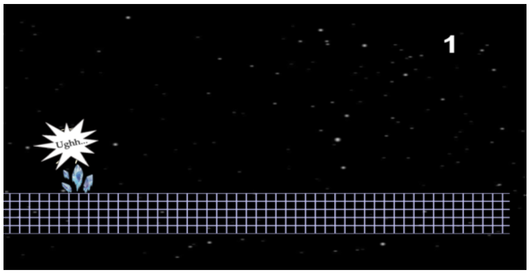


Figure 11. *Obstacles to jump*

The *main character* of speed Game possesses **elements of *Artificial Intelligence*** - the variation of the speed of movement according to the distance traveled.

Conclusion 3. Depending on the *purpose event*, the Speed Game – *Space Runner* turns also from a *System Support for Decisions* to *Intelligent Support System*.

E-learning Game - *Test-Game TP.T1*: The *Test-Game TP.T1* is developed for testing the knowledge for the distance learning (see [5]). The test contains a set of evaluation questions and variants of answers to the course Theory of Probability and Mathematical Statistics, placed on the Moodle platform at Trade Co-operative University of Moldova (TCUM), HYPERLINK „*http://www.uccm.md/*”. This *Test-Game TP.T1* was developed for mobile devices and PC and runs on Windows and / or Mac OS. The mobile version can be accessed on Google Play, PC version - accessed on the site TCUM.

For the Start menu we have (Figure 12):

(1) *Functional elements* - *Start button* and *Instruction button.* The *Start button* launches the *Test-Game TP.T1* and the *Instruction button* displays Testing Rules, submitted Figure13;
(2) *Graphic elements* – Game name *Evaluation Test!* and ornament;
(3) *Purpose event* - activation of first play level of *Test-Game TP.T1*;
(4) *Attendant event* is presentation of Testing Rules.

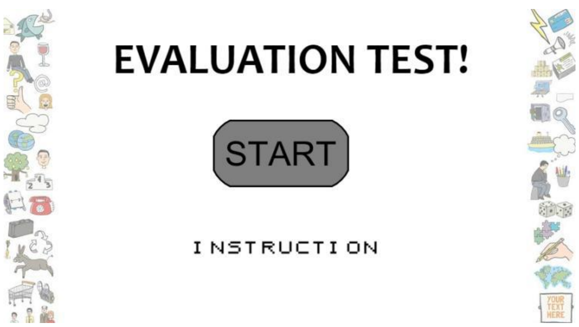

EVALUATION TEST!

Figure12. *Release Test–Game TP.T1*

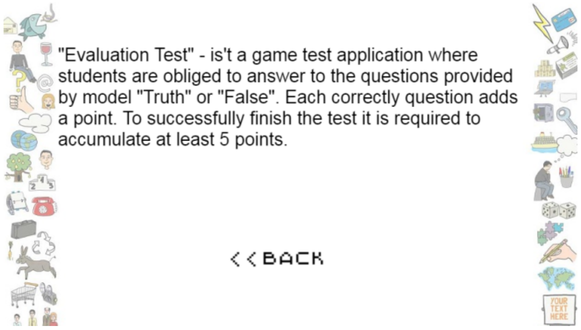
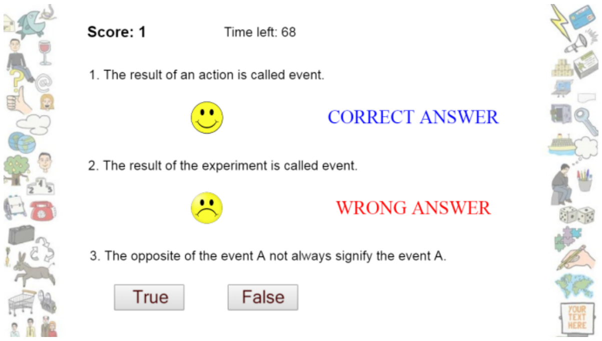

"Evaluation Test" - is't a game test application where students are obliged to answer to the questions provided by model "Truth" or "False". Each correctly question adds a point. To successfully finish the test it is required to accumulate at least 5 points.

Figure13.*Testing Rules*

Next, on every page of *Test-Game TP.T1* shows up three questions accompanied by the *buttons True*, *False* (Figure 14). By pressing one of *buttons* we give the answer, which may be *true* or *false*. After pressing the *button*, they both disappear and this excludes repeating the answer. The correct answer is accompanied by a *pleasant sound*, a *mascot who smiles* and announcement *Correct Answer*. The incorrect answer is accompanied by an *unpleasant sound*, a *sad mascot* and announcement *Wrong Answer* (Figure 14 - Figure 15).


Score: 1 Time left: 68

1. The result of an action is called event.

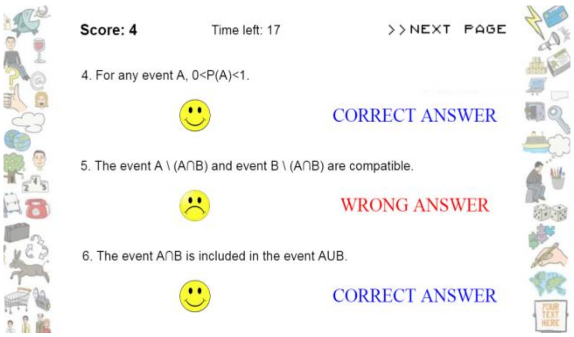
CORRECT ANSWER

2. The result of the experiment is called event.

WRONG ANSWER

3. The opposite of the event A not always signify the event A.

Figure 14. *Level in achievement*


Score: 4 Time left: 17

4. For any event A, 0<P(A)<1.

CORRECT ANSWER

5. The event A \ (A∩B) and event B \ (A∩B) are compatible.

WRONG ANSWER

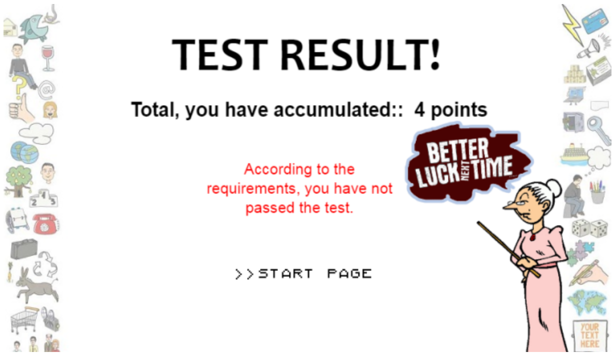
6. The event A∩B is included in the event AUB.

CORRECT ANSWER

Figure 15. *Level achieved*

The finish level contains the *elements* and *events* shown in Figure 16 and Figure 17. The *Start page button* (*functional element*) returns to the *Start menu* position. The *purpose event* in the finish level is the display of the final result *Test result!*, so the number of points accumulated in the field: *Total, you have accumulated* :: *4 points* - you have not passed the test (Figure16); *Total, you have accumulated:: 7 points* - you have passed the test (Figure17). In this example, the condition to pass the test is to accumulate a minimum 5 points of 9 possible. *Attendant events*: 1) if the test is not passed (Figure16), then we have announced messages *According to the requirements, you have not passed the test* and

Better luck next time (graphic element); 2) if the test is passed (Figure17), then it is announced message *As required, you passed the test, graphic element - firework* and pleasant *sound element.*



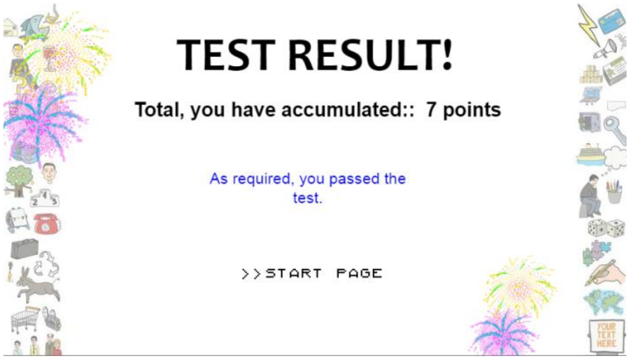
TEST RESULT!

Total, you have accumulated:: 4 points

According to the requirements, you have not passed the test.

BETTER LUCK NEXT TIME

>>START PAGE



TEST RESULT!

Total, you have accumulated:: 7 points

As required, you passed the test.

>>START PAGE

Figure16. *Display negative result*

Figure17. *Display positive result*

The *purpose event* in test levels is to get a *maximum of points* in the Score field, placed at the top left of the page. *Attendant event - measuring* of the *test time*, leads to the test results with one of two possibilities (Figure18):

(1) *Normal Random Event (NRE)* when the cut-off time was not consumed;

(2) *Forced Random Event (FRE)* when the cut-off time is consumed.

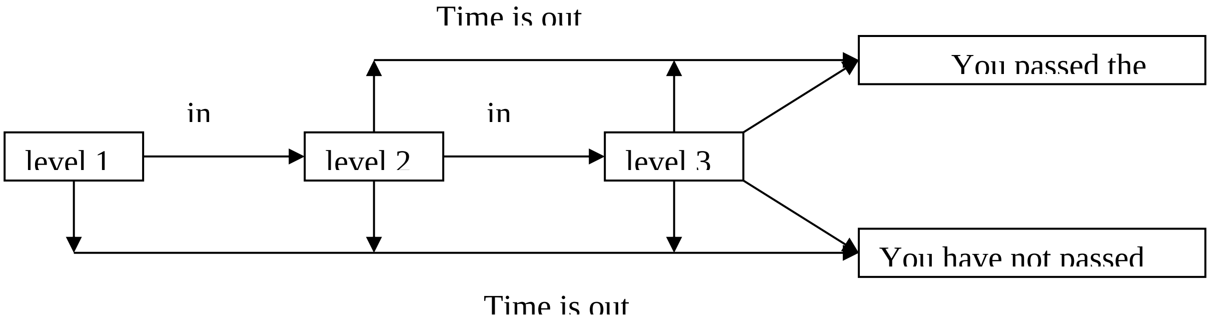


Figure 18. *Test-Game TP.T1 route according to test time consumed*

Conclusion 4. The time reserved for testing is *optimal* if the probabilities *P(NRE)* and *P(S)* are almost equal, where *P(S)* is the statistical probability of success.

Elements of *Artificial Intelligence* in *Test-Game TP.T1* are possibilities to finish the Game, depending of the *test time* on the test.

Conclusion 5. Depending on the *purpose event* and of the *test time*, the *Test-Game TP.T1* turns from a *System Support for Decisions* to *Intelligent Support System* (see [4]).

5. IT RESOURCES IN CREATING THE GAMES AND THE OPEN SOURCE LMS WHERE PROPOSED GAMES CAN BE USED

Proposed *IT Methodologies* can create Games using minimum resources.The presented Games were created using three tools: *Construct 2* **-** the game modeling platform at the Programming level and Visual Design level. *Photoshop* **-** tools for creating Graphics. *Audacity* **-** Tools for creating and editing Sounds. These Games can be adapted and used as effective tools in training on LMS which is an essential tool for eLearning professionals. Here are the top of Open Source LMS solutions you can to consider (see [1-2]): Moodle, ATutor, Eliademy, Forma LMS, Dokeos, ILIAS, Opigno, OLAT, AeL.

1. **MOODLE** (see [1]). Moodle is one of the most popular Open Source LMS options available today. It features dashboards, learner tracking, and multimedia support. This Open Source LMS also gives you the ability to create mobile-friendly online courses and integrate third party add-ons. One of the standouts of this tool is the user community. Unlike many other open source LMS solutions, you can get answers to pressing questions almost immediately by accessing the online support database, and download pre-made eLearning courses that can save you the time and trouble of creating them from scratch. It's worth mentioning that Moodle may be a bit more complicated for new users, but mastering the tool is well worth it if you want total design freedom.
2. **A Tutor** (see [1]). This Open Source LMS boasts a variety of useful features, ranging from email notifications to file storage. One of the notable highlights of ATutor is that it is user-friendly and easily accessible, which makes it an ideal match for those who may be new to the world of eLearning design and development. It also offers a wide selection of eLearning assessment tools, file backups, analytics, and poll integration.
3. **Eliademy** (see [1]). The Open Source LMS Eliamedy is completely free for eLearning facilitators, except for the Premium version for users. It features eLearning course catalogs, eLearning assessment tools, and even a mobile Android applications for educators who wish to develop mobile learning modules for their users.
4. **Forma LMS** (see [1]). This Open Source LMS is very good suited for corporate training programs and offers an active online community where you can find advice, tips to get the most out of the Open Source tool. Forma LMS is packed with variety of features. It also has certificates, competency management support, and a wide range of virtual classroom management tools, including calendars and event managers.
5. **Dokeos** (see [1]). The Dokeos features a variety of eLearning templates and eLearning course authoring tools that we can use to create rapid eLearning. It also features a wealth of useful information, including video tutorials that which will accompany you step by step. The interface is user-friendly and intuitive, which makes it a perfect match for newer eLearning professionals.
6. **ILIAS** (see [1]). This Open Source LMS holds the distinction of being the first open source LMS that is SCORM 1.2 and SCORM 2004 compliant. ILIAS is one of the few LMS tools that also doubles as a full-fledged collaborative eLearning platform, as you can communicate with your team and share documents all in one place. It's free of charge for all eLearning developers and organizations, as well as educational institutions, regardless of the number of users.
7. **Opigno** (see [1]). The Open Source Opigno encourages us when it comes to features. Certificates, class calendars, online forums, eLearning authoring tools, eLearning assessments, and video galleries

are just some of the highlights. This Open Source LMS is based on Drupal and you have the ability to manage your virtual training program, track learner skill development, and integrate e-commerce using just one tool. Opigno also offers online surveys, instant messaging, and chat, which makes it a great feedback and collaboration tool.

8. **OLAT** (see [1]). OLAT's advantages over many of the other Open Source LMS solutions are: eLearning Evaluation Tools, social learning integration, and learner start-ups. Here we have a class calendar, email notifications, eLearning course bookmarks, file storage and certificates. OLAT simplifies the addition of users and groups, as well as the development of catalogs in eLearning courses. Another advantage is the browser verification feature, which gives you the opportunity to test the eLearning course on a wide range of browsers to make sure it is compatible. Thus OLAT is ideal for multi-platform e-learning courses that need to run on a variety of different devices.

9. **AeL** (see [2]). AeL is a modern eLearning solution, offering facilities for management and presentation of various types of digital content such as educational interactive multimedia content, interactive guides, exercises, simulations and tests. AeL eLearning solution is based on international principles and standards that support modern education, being designed as complementary tool to classical teaching/learning methods. AeL offers support for all participants in the educational process (students, teachers, administrative personnel, parents, civil society). AeL can be used successfully in the teaching and learning process, testing and evaluation, educational content administration, monitoring the results of training and evaluation, education forecasting, trends and prognosis. Today, AeL eLearning solution is successfully deployed in over 15,000 schools from Europe, Middle East, Africa and CIS. The AeL eContent Library comprises 3,700 interactive lessons, covering over 20 subjects and includes over 16,000 reusable learning objects (RLOs). AeL is MathML, SVG and SCORM compatible, is perfectly adapted to the Romanian educational legislation, modularized, powerful and extremely flexible, thus can be customised and easily translated in any other language. AeL is optimized for: 1) *Synchronous learning* - the teacher controls the whole educational process, creating, adapting and monitoring the training; 2) *Asynchronous learning* – pupils study at their own pace, enables collaborative projects; 3) *Testing and evaluation* – meant to meet the needs of educational institutions and to measure the impact and effectiveness over the educational process. Over 7 million beneficiaries worldwide are currently using the successful AeL eLearning solution.

REFERENCES

1. Pappas Christoforos. *The Top 8 Open Source Learning Management Systems.* https:// elearningindustry.com/top-open-source-learning-management-systems

2. Neagu Andreea. *AeL Educational Presentation.* http://www.advancedelearning.com/index.php/articles/c311

3. Seichiuc V.V. "*Game Development Techniques for Mobile Devices",* in: Transactions of XVII International Symposium „Discrete singularities methods in mathematical physics" (DSMMPh-2015). Kharkov-Sumy, Ukraine, pp.227-231(2015).

4. Filip F.G. *Sisteme suport pentru decizii.* – Ed. a II–a, Bucureşti: Editura Tehnică, 2007. - 363 p.

5. Bragaru T., Căpăţână Gh., Pleşca N., Latul Gh., Cîrhana V., Efros I., Crăciun I., Baban T., Baron Gh. *Învăţământ la distanţă: concept şi terminologie.*Ghid de iniţiere. / Redactor ştiinţific: Căpăţână Gh. – Chişinău: CEP USM, 2008. - 101 p.

Massive Open Online Courses - the Key to Success in Distance Learning Education

Bragaru Tudor

State University of Moldova
60, A. Mateevici str., Chisinau, MD-2009, Republic of Moldova
Tel: (+373)79-291-997, e-mail: theosnume@gmail.com

ABSTRACT

Scientific and technical progress and rapid development and obsolescence of knowledge in the Global Information Society requires adequate methods of knowledge upgrade and transmission. e-Learning and open Distance Learning (ODL) based on digital, multimedia and interactive educational resources aim at addressing this problem. The purpose of this paper is to present author's own experience of developing an ODL system and review of the trend of Massive Open Online Courses (MOOCs), suitable for most of universities.

Keywords: open, distance, learning, educational, platform, massive, online, courses, digital, content.

1. INTRODUCTION

The development prospects for education technologies in the following 10 years will be pinpointed by ***change***. One of the most important changes in the area of tertiary degree education, which is evident today, is the development of open distance learning [10] in the form of massive open online courses (MOOCs) [1, 2] and the general move towards open, free access to education for everyone without any limitations.

In fact, the education system is on the verge of radical transformations, predetermined by the rapid development of the Internet, modern information and communication technologies (ICT) and data processing devices such as notebook, netbook, tablet, phablet, iphone, etc. and their integration into all educational processes. Thanks to these changes, it is now possible to organize ODL everywhere, often with video, interactive and game elements, and researchers and teachers can receive instant feedback from hundreds of thousands of students for further improving the efficiency of teaching and improving e-content. *This technology is effective, surprisingly cheap and global in its objectives, which allows ODL to expand and develop without limits.*

The significant progress ODL has made in the last ten years can greatly influence the results and quality of education and the development of society as a whole. Thanks to MOOCs, education in digital form is now practically *accessible globally*, *for anyone wishing to use it,* while allowing, at the same time, to personally choose one's own tailored training content. We are talking about giving the widest audience free access to the study of a wide range of academic courses of leading and prestigious universities around the world. MOOCs have become a worldwide trend in continuous higher education, but can also become such trend for the primary and secondary education, which is supported by the experience of the Khan-a Academy [3], even though it does not quite fit the definition of MOOCs.

ODL responds to enormous training needs, while providing greater quality, flexibility and efficiency than traditional forms while reducing overall costs. The use of ICT in all learning processes, especially for self-study, self-monitoring and self-assessment allows:

- To increase the volume of taken in meaningful data and knowledge (awareness);
- To reduce learning time due to better search ability and localization of necessary information;
- To improve memorizing through multimedia, gaming and interactive learning resources, etc.

According to Roediger, Larsen [5, 12] systematic (self) testing, which is only really possible with the use of ICT, is much more effective than with a single test at the end of the course Figure 1).

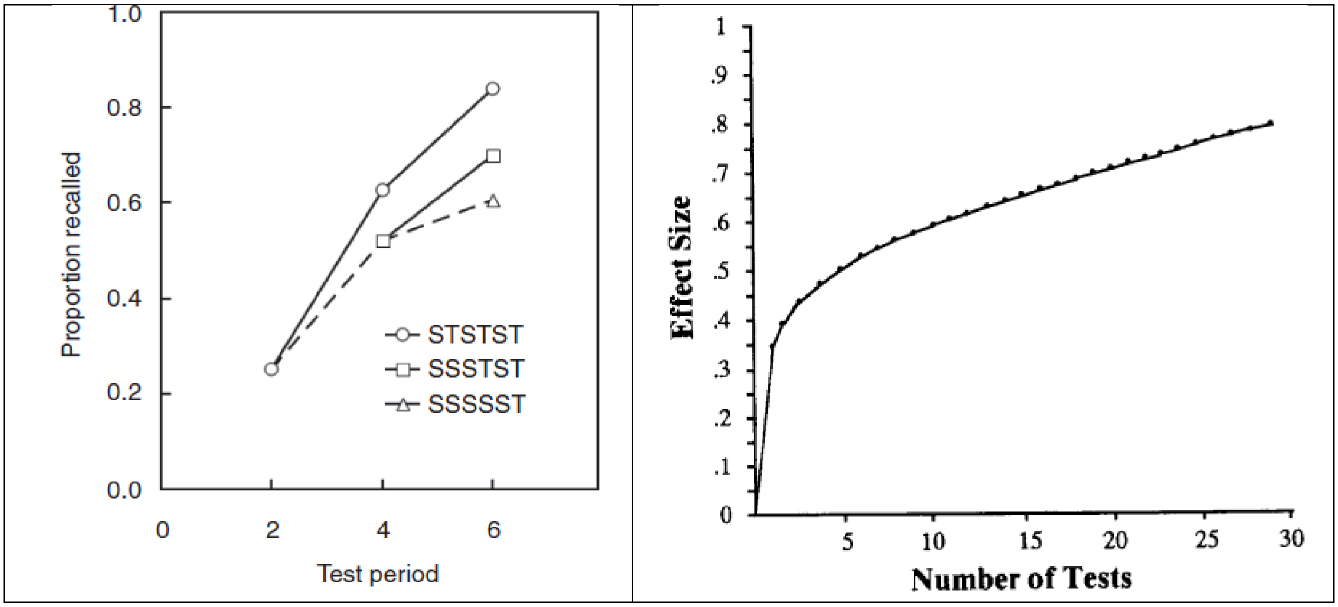


Figure.1. The effect of systematic testing [5, 12]

This paper outlines the author's experience over the past decade in the development and implementation of ODL, as well as MOOCs, as the most pronounced trend in education innovation over the past 100 years.

2. THE PHENOMENON OF MOOCs

2.1. Historical backdrop

In the opinion of its founders (Sebastian Thran, Andrew Ang and al) MOOCs are the greatest, most important change in education in the last century and a revolution since the appearance of lecture classes. MOOCs allow *to revolutionize learning for students, teaching for professors and tutors, managerial processes for education administrators,* including the sector of continuous corporate education in the domain of life-long learning [4].

But the very idea of distance learning is far from new. According to Forbes [6], distance learning began back in 1892, when the University of Chicago created the first distance learning program at the college level using mail for correspondence with students. Later distance learning expanded to live broadcasts on radio in 1921 and to television broadcasting in 1963. In 1969 the Open University was founded (in the UK), in 1970 - Coastline Community College became the first college without physical space, offering only television courses. The last time such revival in educational methods was observed in 1906 when it was hoped that new education methods can be supported by new developments in the postal communication system.

The first MOOCs were proposed in 2008, but the ultimate idea brake through in 2011, first in the US, and then in Europe. At the end of 2011, the free pilot MOOC course "Artificial Intelligence" attracted 160 thousand students from all over the world and 23 thousand of them successfully graduated. The course was offered by Sebastian Thran, Google's vice president and professor of computer science at Stanford University as well as by Peter Norvig. Six months later, two of the participants in this project retired from their jobs and organized the company Coursera. They were Andrew Ang, who masterminded the Coursera platform and Daphne Keller, together co-founding the company aiming *"to bring quality education to everyone who will not be able to study at Stanford."* [1]. Then Tran launched the Udacity project (establishing an on-line school), the success of which led to the emergence of many start-ups. Tran, being the head of the online school Udacity, believes that *"higher education is the fundamental right of any person, which should be affordable from a financial point of view." ."* [1].

Another and one of the best examples of radical innovations in education, is the Khan Academy (*https://ru.khanacademy.org/*), whose open and free lessons on the network have been reviewed by at least 270 million times. Salman Khan, the founder of the academy, with the aid of YouTubehas built a free virtual school in which anyone can learn anything. The academy is sponsored by some of the richest people in the world (Bill Gates, Carlos Slim) and hundreds of sponsors of a smaller scale, whereas Google finances translation of Khan's lectures into various languages. Khan aims to change, with the help of ICT and the concept of an "inverted school class", a school institution that has been established over the centuries *to give every child in the world the opportunity to study at the speed which it is convenient for them, rather than making the student dependet on the general way of instruction in clas*s [3].

The New York Times proclaimed 2012 the “Year of MOOCS” (http://www.onlineobuchenie.ru/online/«moocs»/). Indeed, the speed with which online courses develop is amazing. By March 2013, Coursera has accumulated over 2.5 million students, Udacity has almost half a million [7]. In 2016, the number of MOOCs increased to 6850, involving more than 700 universities and more than 68 million of students [7]. Three of the five largest MOOCs suppliers [7] are Coursera (http://www.coursera.org), edX (http://www.edx.org) and Udacity (http://www.udacity.org) - all based in the US and began to work in 2011-2012; XuetangX - opened in China in 2013, FutureLearn - launched in England in 2012.

Udacity is currently more focused on professional courses for professionals, in 2016 more than 4 million users were registered **Coursera**, the largest online provider of online courses from leading universities from around the world, focuses on providing education, complementary to "traditional", and offers courses by elite universities. As of February 2017, 24 million users, over 2000 courses and 160 specializations from 149 educational institutions were registered [7].

edX differs from other MOOC providers, such as Coursera and Udacity, in that it is a non-profit organization and operates on the free Open edX open source software platform. More than 70 schools, non-profit organizations and corporations offer or plan to offer courses on the edX website. As of December 29, 2016, edX had about 10 million students, more than 1270 courses. edX has expanded its MicroMasters certification for 14 different universities. [7, 9].

XuetangX now offers about 400 courses, including 133 owned; about 30 courses are licensed for edX; has more than 6 million registered students (https://www.class-central.com/report/xuetangx/).

FutureLearn as of January 2017 unites 109 British and international partners, 5.3 million (https://www.topuniversities.com/student-info/daily-news012/futurelearn-evolution-moocs/).

Very quickly, many European and American universities, feeling the threat of tough, boundless, global competition, began to promote their own MOOCs, which provide an opportunity to receive, amongst other things, quality "traditional" university education.

Based on the above, **a new approach to education will be able to significantly improve the quality of training and its effectiveness**, including for those students who, in the old ways, continue to receive knowledge in physical spaces of the educational institutions. Less than 10 years from their inception, MOOCs today mean an **unparalleled educational offer**, including the pedagogy of online learning, successful marketing and convincing evidence that MOOCs can reach a huge number of people around the world, forcing universities to revolutionize [4].

From its earliest days, the process of online learning of millions of students through the *MOOCs is constantly being studied, analyzed, evaluated and, as necessary, adjusted*. All the founders of MOOCs will say their main aim is not the growth of sales of training videos or e-content, *but the improvement of education system through scientifically based and effective use of data based on integrating ICT into* *all learning processes.* It is supposed to work towards a common goal to "reinvent" education on a global scale and make it accessible to everyone.

If MOOCs projects will continue to be successful, if they progress to implementing systems which are able to take into account the level of each given student's knowledge and offers a tailored study plan, *MOOCs will be regarded as the most important innovation in the field of education in the last 200 years*.

Rapid growth in the popularity MOOCs can be explained by the many advantages that they offer. But the main reason is probably *the effectiveness of methods used for developing, arranging and allowing utilization of digital learning content*, without any access restrictions, regardless of geographic location, age, training level and at any suitable / convenient time for the student.

Universal accessibility allows students, wherever they are, *to have access to virtually any type of educational content they want, at any time, when they want, on virtually any device they choose*.
All that is needed to participate in MOOCs it is access to the Internet whereas exams may be conducted either in authorized test centers around the world, or online with an aid of special programs that allow to confirm the identity of the user.

2.2. Opportunities provided by MOOCs

MOOCs create new opportunities for the democratization of education. All MOOCs training materials are available on the Internet. There is a choice of how to learn and share knowledge, synchronously or asynchronously in traditional, virtual or inverted classes. All course content is available through RSS feeds and students can use their usual devices (for example, desktop computer, netbook, notebook, IPhone, phablet etc.); choose communication tools (for example, blog posts, Second Life or synchronous online meetings), choose a course from the best universities in the world, such as MIT and Harvard - and all this often free of charge. Many of the courses are now available to the user when they want. And the rate of mastering the course is now also individual for each user. As a consequence of their own choice, students are trained with greater responsibility and pleasure.

Multimedia format of providing material, audio, video resources, online forums, webinars, interactive tasks, educational games, virtual laboratories, etc. make learning an exciting activity. Many believe that such "old" complex formats, manifested in e-learning, are renewed and more efficiently applied in MOOCs format, while successfully replacing textbooks perceived as boring and making learning more focused. An obvious example of this being the case is the success of Khan Academy.

Relevance, quality and novelty of the courses. The typical MOOC is strikingly different from the early distance learning courses. Each such course is the merging of video lectures, tests and study assignments, as well as a special forum where students communicate and ask questions, and teachers and other students respond to them. Due to the almost instantaneous feedback, course developers, administrators, tutors, designers and subject experts all have the ability to quickly respond and improve courses, create better training materials. MOOCs can also assist to alleviate the shortage of qualified teachers by providing the courses developed by a group of expert teachers on the subject.

Personalization and diversification. MOOCs do not look like "traditional" e-courses, targeted at specific specific groups of users. Its orientation toward thousands of students simultaneously requires automated generation, adaptation, personalization of content in accordance with individual needs and abilities, all the while offering the same content. Agency technologies will soon allow to "individualize" generating content for each particular student. On the other hand, variety of MOOCs platforms and providers offers different visions of the same content, which allow for different learning styles which prospective students can compare, evaluate and select the course that best fit their vision and style. Various MOOCs platforms experiment with various learning models and strategies. Which models are better and which providers will survive remains to be seen. The tough competition amongst MOOCs providers is un doubtfully invaluable for improving future realizations of the respective systems aims.

Studying of **new business models to support and monetize education**. As a rule, today's MOOCs do not come at a charge and don’t offer accreditation, however some versions of courses begin to offer accreditation and some solutions for monetization for providers are already available. For example, while MOOC provides a free course, additional support for the student, p2p coaching, exams and textbooks can have a small cost. When the course is designed for just 20-30 people the cost to offer it at say 20,000-30000 euros can be exorbitantly high for many Universities. However, if same course is able to cater for 1000 people and the content cost per participant is reduced to 25-50 euros it can translate into great return on investment. Practice shows that the number of participants for some courses exceeds tens of thousands, or the cost per participant is further reduced to just 3-5 euros! This is especially important for developing countries, the free access matters a great deal to them. Notwithstanding these noble goals, at times monetization aims can rate higher than mass character. Many certificates start being available at a cost. For most courses via Coursera one is charged even for assessment of assignments.

2.3. Challenges of MOOCs

In fairness, *MOOCs are currently in an embryonic state, with a lot of experiments and discussions around the merits and significance of MOOCs, their design, delivery methods, etc.* Some view MOOCs as a means of reducing the number of classes and instructors to achieve significant economies of scale and cost reduction. Others recognize the problems, try to study them, deciding how MOOCs can improve teaching and learning for the broad masses for symbolic payment. *Many critics point to a number of problems.* There are wide variations in relation to various providers’ teaching, some institutions simply offer online learning with access in the "open to all" style, while others really think about the importance of quality and what should happen in terms of logistics, support and pedagogical design, so that people are really taught what they are promised by the course and so that it is truly available for anyone

In addition, there are some misconceptions about the potential disappearance of printed publications at the MOOCs and ODL develop, about the fact that MOOCs can the just about anything, as well as some misconceptions about openness and costs. Naturally no content can be absolutely free, so mass courses face a range of issues relate to the development and translation of content, copyright, monetization, certification, etc.

Elite approach. Most of the known MOOCs platforms offer only courses of elite institutions, mostly members of the Association of American Universities or the "five" of the best universities of countries outside of North America. For example, Coursera [8] has agreements with 62 universities with which it cooperates. In EdX, only 12 universities are taught, including two of its founders (Massachusetts Institute of Technology and Harvard University). According to many, the elitist approach of these companies is viable only at the initial stage. This situation has already prompted most of the leading universities by the end of 2013 to offer their own MOOCs.

Large drop-out rates. Indeed, drop-out rates for MOOCs courses are currently quite high (for xMOOCs (technical disciplines) up to 85%, for cMOOCs (humanitarian disciplines) up to 40% [11] since courses are mostly independent, without any fees and obligations on the part of students. It is also true that early MOOCs had a monotonous approach. However, over time, designers, course writers and teachers experimented with various ways of interacting, discussing and connecting, including blogs, forums, online discussions and video conferences, achieving good learning outcomes.

Quality of content. The future success of MOOCs training depends not only on the strategy of openness *(4A – Anyone, Anywhere, Anytime, Anytime)*, but also in the quality of content. The substance of e-content should strictly correspond to what the student requires, no more no less, therefore the trend for content development should go towards adaptive teaching.

Several reflections on what a quality online learning means nowadays are briefly reminded in the article [13] and about transformation of online courses article [14]. The major advantages of creating a responsive e-learning course and how to create and distribute a responsive e-learning course and see [15].

2.4. Two main formats of MOOCs

The MOOCs experiment combines information and educational technologies for the education management system, including video, discussion forums, instant messaging to support cadets, etc., to reach more students around the world. There is a distinction between constructivist MOOCs (cMOOCs) focused on the creation and generation of humanitarian knowledge and xMOOCs with an emphasis on expanding knowledge in technical disciplines [11].

xMOOC is focused on the study of technical disciplines, where it is possible to automate the assessment of completed assignments, there are practically no observers in the course, teachers perform predominantly supervisory roles, courses are open to all.

cMOOC is designed to study humanitarian disciplines, usually attracts a huge number of participants in the course, teachers perform different roles, the course is characterized by openness of learning, dialogue, discussion and conversations, etc.

According to the level of offered services, we distinguish three types of MOOC, described below.
MOOC "content only" consist almost exclusively of educational content posted on the Internet for independent and informal education. Organizers do not make any efforts or attempts to participate in the training process of the client, assessment, assistance, certification, etc., which are the functions beyond the scope of providing content only material. The benefit of this type of courses on education is minimal. These are just collections of digital training materials available via the Internet, no better or no worse than other teaching aids. At the same time, the effect of using such MOOCs may drastically improve is content was offered through interactive modeling, teaching video games, adaptive learning, testing, videos of inspiring professors etc. For students with high self-motivation, such MOOCs would be very useful.

MOOC "content + technology" is an attempt to make it feel like a real school, providing certain aspects of the traditional school experience. For example, online consultations with teachers for all or some categories of students, professional tests, including certification, test reports, etc.
MOOC "regular online courses" are traditional distance learning courses that *are accredited, organized, provided, evaluated and certified in due course,* but simply use online channels to communicate with students. Such courses are rarely "mass" or "open" in the sense that the material is not provided free of charge to anyone who has access to the Internet. Most of these courses charge substantial fee for classes, and certification. It is necessary to pay to the conducting institution, administrators, teachers, mentors, including paying for using the platform, infrastructure, etc. The influence of this type of course is significant for the education system, as it strengthens the pedagogical aspirations and outreach potential of the institution. These are offered by prestigious schools and universities, and online courses are just one of their education tools.

3. CONCLUSION

Today, MOOCs represent the most important trend in open distance e-learning and become more and more popular. The success of the MOOCs platforms such as Coursera, edX, XuetangX, Khan Academy and many other commercial universities and non-profit organizations whose free online resources are available on the Internet, demonstrate the exceptional importance of online education in the form of MOOCs and the rapid rise of its providers.

While one can still deliberate about delivery methods, MOOCs' assessments effectiveness, courses quality, monetization methods, etc., no one can deny this educational phenomenon’ mass appeal due to its universal access availability at an extremely low price, as well as the radical changes that it brings about for the ways of delivering and administering online education and education at large. Analysts have called mass online courses the greatest revolution in education since the invention of the Gutenberg printing press [16].

Universal and unrestricted access to information through new communication technologies, providing interaction with students and instant feedback as well as development of digital content and tools for its improvement – all represent the critical success factors for the development of distance education in the near future. Present day fast paced and wide-spread technologies such as a smartphones or Ipads call for creating electronic training resources that will work effectively on all emerging devices, not just on desktop or tablet computers.

Many believe that if MOOCs continue to succeed and progress to solutions able to tailor course offerings to individual needs of numerous students it will be truly the most important innovation in the field of education over the past 200 years.

MOOCs characterized by flexible delivery, high-quality and copy-righted educational content has potential to go beyond higher and continuing education and eventually start impacting the primary and secondary education. But can individuals of the future be trusted to do it wisely when choosing their education platform in much the same way as they shop for a toothbrush in a supermarket or bread in a bakery? This is a challenging question that remains to be addressed. It may be sooner than we might think that individuals would be able to choose between a course offered by a certain local University versus similar courses offered by Harvard, Stanford or other local higher education institutions. Creators of MOOCs should see their aims in not solely increasing sales of training videos or e-content, but in the improvement of the education systems through scientifically based and effective use of information as well as in joining the efforts to "reinvent" education at large, making it accessible to anyone. This is a serious challenge for the traditional system of full-time classroom education which often comes at a substantial cost for whoever wants to engage in quality and prestigious education.

REFERENCES

(All online sources quoted were accessed on October 10, 2017)

1. MOOCs: вторая жизнь высшего образования. http://agora.len.su/ viewtopic.php?p=6871&sid= 21656ab74d24d714c81cc03c5409c2ed.

2. Development of distance learning: world trends, http://inyaz-school.ru/

3. Forbes: one man, one computer, millions of students: how Khan’s Academy is changing the education system, http://www.forbes.ru/tehno/ internet-i-telekommunikatsii/219529- odin-chelovek-odin-kompyuter-milliony-uchenikov-kak-akadem/.

4. Массовые дистанционные курсы: революция в образовании? https://newtonew.com/tech/massovye-distancionnye-kursy-revoljucija-v-obrazovanii/

5. Roediger, H.L. et al. Ten benefits of testing and their applications to educational practice. Psychology of Learning and Motivation, v.55, 2011, pp.1-36.

6. Distance Learning Has Been Around Since 1892, You Big MOOC, https://www.forbes.com/sites/jamesmarshallcrotty/2012/11/14/distance-learning-has-been-around-since-1892-you-big-mooc/#450998423187/

7. By The Numbers: MOOCS in 2016, https://www.class-central.com/report/mooc-stats-2016/

8. Coursera's 2016: Year in Review, https://www.class-central.com/report/coursera-2016-review/

9. EdX создаёт систему для автоматической проверки эссе. http://www.ed-today.ru/poleznye-stati/217-edx-sozdajot-sistemu-dlya-avtomaticheskoj-proverki-esse/

10. A multi-institutional study of the impact of open textbook adoption on the learning outcomes of post-secondary students. https://link.springer.com/article/10.1007/s12528-015-9101-x/fulltext.html#copyrightInformation

11. Two models of MOOCs education. http://studymooc.org/podrobno-mooc/dve-modeli-mooc-obrazovaniya/

12. Larsen D.P., Butler A.C., Roediger H.L. Repeated testing improves long-term retention relative to repeated study: a randomized controlled trial. Medical Education, pp. 1174-118, nr.43, 2009.

13. Istrate O., Kestens A.. Developing and monitoring a MOOC: the IFRC experience. Proceeding of 11th International Scientific Conference eLearning and software for education. Bucharest, 2015, -pp 576-582.

14. Трансформация онлайн-курсов: главные тренды, что изменилось и почему все будут платить. http://www.hr-portal.ru/article/transformaciya-onlayn-kursov-glavnye-trendy-chto-izmenilos-i-pochemu-vse-budut-platit/

15. Fluid & Future-Proof: How To Create And Distribute A Responsive eLearning Course. https://elearningindustry.com/free-ebooks/create-distribute-responsive-elearning-course-fluid-future-proof/

16. Technology improves higher learning, it doesn't kill it. http://theconversation.com/technology-improves-higher-learning-it-doesnt-kill-it-29657

Design Thinking as an Innovative Approach of Training the Future Leaders of the Digital World

Vasileva Elena, Altukhova Natalia

Financial University of the Russian Federation Government
49, Leningradsky pr., Moscow, 125993, Russia, Tel: +7 (499) 277-21-49
E-mail: evvasileva@fa.ru, nfaltuhova@fa.ru

ABSTRACT

The article discusses the features of implementation of design thinking in academic discipline undergraduate and graduate programs of a direction "Business Informatics". Given a case in which techniques of design thinking (SCAMPER, guerrilla ethnography, participant observation, visualization tools) included in the study customer experience. Presents a case study can also be used in practical classes in the study Lean Startup (part of the methodology, customer development Customer Discovery), in the course "internet marketing" and etc. It describes the problems of teaching students technology entrepreneurship. Selected key participants in the process of training of specialists, whose competence can be claimed in the digital world.

Keywords: design, thinking, education, technology, entrepreneurship, personnel, training

1. INTRODUCTION

Digital transformation is often referred to as the most important condition for the successful development of the organization. Key trends of digital transformation are: an increasing importance of creating customer experience and personal component in brand interaction; transformation of the operating model to enable flexible rebuild to changing market conditions and new breakthrough technologies (informed decision-making, fast execution); the Internet of things as key driver of digital transformation, the introduction of digital thinking into the corporate culture of the organization (Agile format, creating cross-teams and new working principles for the effective and efficient execution of tasks); and also the creation of multi-channel ecosystem with the personal values of clients by analyzing their needs and preferences (analysis of digital traces: big data and data mining).

Entrepreneurial skill and ambitions are in big demand in international markets. The importance of developing team skills and personal development of the person throughout one's life is being empathized. These qualities are soft skills, which are especially needed for large companies that find it the hardest to adapt management and technology platform under the demands of the digital future. To manage the business processes, the companies have introduced a separate position-digital officer, CDO. But how to increase the effectiveness of training future leaders of the digital world? What should be the new education in the University like?

In 2004 David Kelley, founder of IDEO, one of the pioneers in the world of design agencies, where the experience of creating new products was brought into the field of creation of services; and Hasso Plattner, co-founder of SAP, have created a design philosophy of innovative solutions, which combines various novelties in the field of development of creative skills of a person, study of the customer behavior, generation of ideas, visualization. Development tools are actively engaged in Design Thinking at HPI School of Design Thinking in Potsdam and the school of Design Thinking d.school at Stanford. This approach is dedicated to the work of Tom Kelley and David Kelley (2013), Jeanne Liedtka and Tim Ogilvie (2011), Tim Clark, Alexander Osterwalder, Yves Pigneur (2012). On the importance of developing creative methods of creating ideas stated in the works of Edward de Bono (1970), Philip Kotler and Fernando Trias de Bes (2003), Michael Michalko (1998).

Many Western universities and colleges began to include in the curriculum the course Design Thinking (e.g., Babson College), HyperIsland (Sweden). Design approach and other creative techniques in Russia using a business school CAVIAR, Lumiknows, laboratory Wonderfull British school of design.

2. METHODOLOGY: DESIGN THINKING CHANGES THE APPROACH TO CREATING INNOVATION

Design Thinking [1-3] is a tool that will allow one to increase efficiency and to develop creative abilities through development of processes of finding answers, teamwork, game mechanics, visualization and inspiration.

To live in conditions of constant change, it will require person's skills to work in a team, to effectively use one’s competencies to be focused and successful, thinking outside the box and finding original solutions. The near future requires such a man. The ambiguity and uncertainty are the conditions, when Design Thinking is necessary. Design Thinking is a method of innovation (figure 1). Design Thinking is a particular way of thinking, whose development allows to look at the problem from different angles, finding unexpected and creative solutions. It is important for leading companies to identify the underlying needs of customers to develop new client-oriented services in terms of digitization of society and economy, so they have to use innovative techniques and tools. Design Thinking has been already introduced in IBM, General Electric, Procter & Gamble, Philips Electronics, Airbnb. In Russia, the design sessions are held in Sberbank, Raiffeisenbank, the results have been applied on portals of the Moscow Government, in the services of the Moscow metro, the state Corporation "Rosatom", telecommunication company "TELE2", etc.

German Gref, head of Sberbank of Russia in December, has participated in the project on study of customer experience, wearing a special suit Gert, simulating a disability, and visiting one of the branches of the savings Bank, in order to understand how conveniently arranged office and business processes for people with disabilities.

Design Thinking can be used as the basis for organizational innovation to all areas of the business. For the company skills techniques Design Thinking and the holding of regular meetings, sessions, brainstorming is important when creating the project strategy, business models, processes.

The application of the methods of Design Thinking when creating a value proposition or advertising message will make it unexpected, unclear, but attractive and memorable to the consumer. In teaching , Design Thinking opens up even greater prospects. From 2015 we have been introducing the Design Thinking methodology in various courses: "Business modeling", "Internet entrepreneurship", "Marketing", "business Models in digital markets", "decision making Methods", etc. This helped us to maintain interest to science; to re-create business situations by the means of game mechanics; to create team discussions, marketing research and to test the models of solutions. In addition, the students have explored and tested new approaches to create information products.

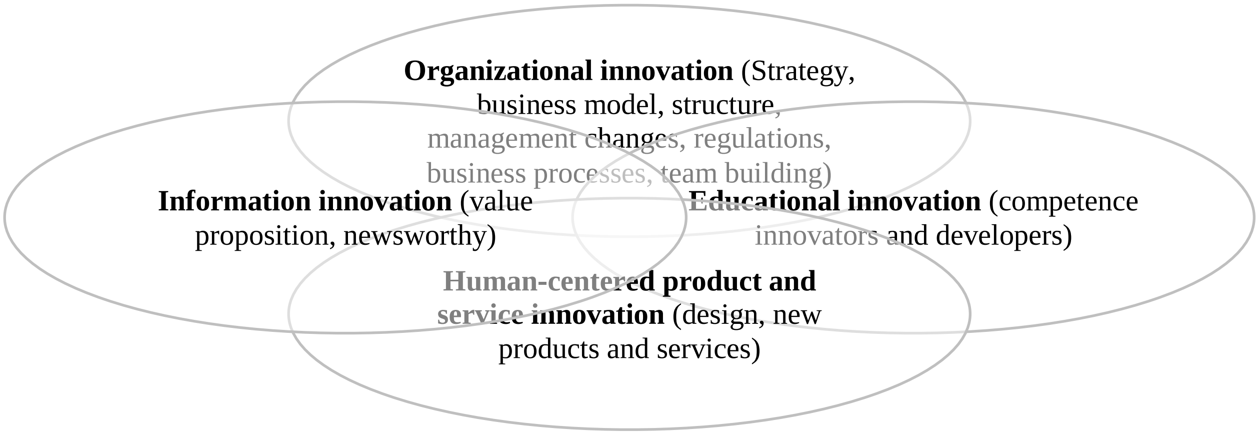

Organizational innovation (Strategy, business model, structure, management changes, regulations, business processes, team building)
Information innovation (value proposition, newsworthy)
Educational innovation (competence innovators and developers)
Human-centered product and service innovation (design, new products and services)

Figure 1. Design Thinking – the method of innovation

The Design Thinking approach includes various heuristic techniques of solving non-trivial problems in the face of uncertainty; the development of creative skills and innovative thinking (out-of-the-box thinking) person; and also game mechanics that allows you to organize communication between different perceptions of the problems involved in the development of innovation. The popularity of the approach is primarily due to its ability to work with tacit knowledge that is important in terms of trend of development of a modern business-oriented person.

The basis of Design Thinking is empathy, understanding of user experience, one’s feelings and sensations; which aims to further develop innovative content of the product, that will aim on the consumer’s emotions. The key steps of the process are empathy, focus, generating, selection, prototyping and testing , are built on the ability to quickly generate many ideas to get away from banality, and the rules on how to choose the best solution to create it, even at the level of the prototype.

The apparent advantage of the method of Design Thinking is changing the approach to the study of the problem. It is based on a search of the answer to the question "how to do something » not "what to do". And the most important is, if a process running into an unexpected result, generates a new one. Generated ideas explored in the intersection of the three spaces of innovation are: the idea, that should be feasible in the foreseeable future from the point of view of technology, and wishes of the user, which are profitable for the business. Example of student work is shown in Figure 2 [4, 5].

3. CASE STUDY"HOW TECHNOLOGICAL INNOVATIONS CAN CHANGE THE EDUCATIONAL ENVIRONMENT OF THE UNIVERSITY?"

Here is an example of one of the developed case studies. Goal: to create a prototype of the classroom of the future. In case study, it is assumed that the creation of hypotheses will examine modern trends Connected learning and Learning-as-a-Service, etc. In addition, it is not limited by technological trends and innovations, and it is necessary to consider other new fashionable models and phenomena (uber-learning, vaping training, spinner-training, patlin-training, HYIP training).

Figure 2. Examples of research of customer experience.

1 step "Empathy". Scoping study starts by identifying the main participants develop solutions. On the Stakeholder Map records the position of all who come in contact or will come into contact with the product or service in order to take into account the interests of each party in the design. There are many versions of the display of the stakeholder map a Stakeholder Map. The map can be constructed in the form of a matrix with two axes, which sometimes is called the "2x2 Matrix", that displays two criteria: the degree of influence of those who are not directly interested in the decision, but can have an impact (positive or negative, indirect or direct)), and the degree of interest or expectations; taking into account both the developers of the solution and its direct consumers (strong and weak). In our opinion, the level of possible cooperation, as well as the degree of possible threat from those who may lose as a result of the successful completion of the project, should be presented on the map (Figure 3).

To understand the process itself, it is useful to build Customer Journey Map (CJM). CJM , which is marketing technology to visualize results of the client research, which simplifies communication with customers and makes communication strategy more effective and complete. CJM helps to take the place of the client and describe his experience. This technique is one of the most popular tools of analysis convenience, mobile app interface, pages of the Internet site. In the study of the experience of the relationship between company and customer, first identify the main groups of buyers (buyer personal), and then determine the questions that can help to analyze each stage of the interaction. The difficulty level can be different and depends on the degree of development of interactions.

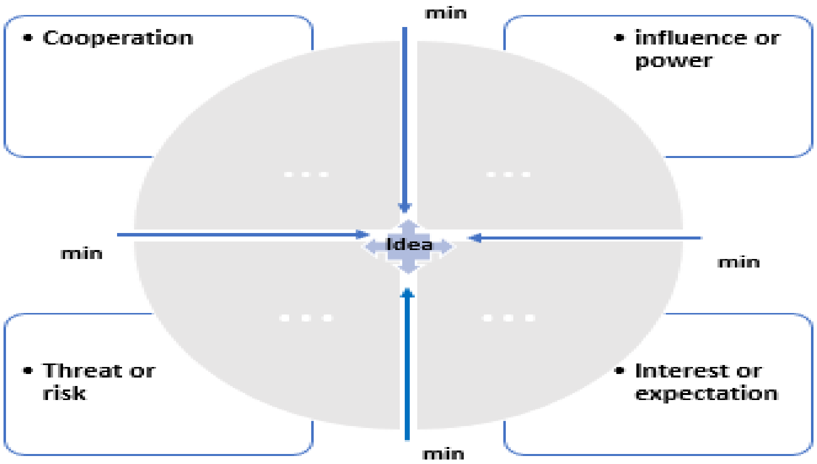


Figure 3. Stakeholder Map.

There is no single technique of creating a custom path, as every draws a map on its own. CJM can be made in the form of a table where horizontally are: past experience of interaction with similar products; reasons for choosing and making purchasing decisions; channels of obtaining product information or methods of delivery; experience of using the product for life cycles, stages or each of its elements (for example, the user's experience of traveling through portal pages); first impressions; and the reasons for rejecting the analyzed product. Vertically are: the user's action; the expected results; problems and barriers; mood; emotions; real users' quotes; their suggestions for product development. The mood of the user is shown by information signs: red sign means the user is unhappy, the yellow sign is the mood of the user, that is indefinite, a green sign informs about the good mood of the user (Table 1). In the future, the map can be added in rows, in which planned activities for product development are recorded: staff actions, improved business processes, resources involved, etc.

Testing of hypotheses derived at the analysis stage, must necessarily be carried out through conducting in-depth interviews of stakeholders in the decision of the parties. The main objective of conducting in-depth interviews is to understand the user experience of a product or service; details of one's interaction with the product or service; and, in the process of analysis, to reach the level of insight. Unlike the interviews, this tool requires additional preparation, that one will need well in advance, and careful plan of not only the issues, but also of the time, which may get needed to demonstrate the Respondent's materials; choosing the location of the interview. The required number of in-depth interviews are between 5 (minimum) and 30.

When conducting an interview, the technique of "Five why?» is used. The technique of "Five why?" can help in the formulation of questions. The secret of technique is to have the question "Why?" raised several times, even if the answers seem obvious. This will allow one to trigger the Respondent's sincerity and reveal tacit knowledge of key research questions; to make the interview effective. So it is possible to get into deep, hidden motives and feelings of the user, to see the other side of the problem, to look at it from a different angle. This technique can be used together with the diagram "Ladder of questions", which, in addition to detailing the problem through the questions «Why?», allows one to apply the "How to do it?" for each of the questions, to suggest what action you can take to solve the problem. As instruments of the survey one can consider social networks Facebook, Vkontakte (Vk), together with the tool Google Forms.

Table 1. Customer journey map

	Actions				
Time					
Expectations					
Problems and barriers					
Emotions, mood, Quotations					
Ideas for improvement (feedback, feedback)					
	Changes				
Staff					
Business processes					
Resources					
Methods / Tools					

2 step "Focusing". To highlight of the many challenges one key there is a method "How can we ...?". The wording of the question: "How can we help?" applied design: a User – Need – Idea. For example, "How can we help [the user] to solve [the problem] as follows: [the idea]", as shown in Table 2. The question serves as a good incentive for finding ideas, start brainstorming. The question is a good stimulus for finding ideas, launching a brainstorm. The real need is well described and allows you to study the phrase "It turns out he needs to" (Table 3) from different angles.

Step 3 of the Generation - SIL and SCAMPER techniques. SIL is a German acronym that stands for "system integration of the elements of the problem." The method consists in consecutive execution of the following actions:

1. Each participant writes their ideas, what competencies they believes are in demand in the future. In this step, ideas are not discussed with other team members. One can immediately prioritize their decisions – from the best ideas to the worst.
2. Ideas are read out loud one at a time. It can be done in the following order: first is the best idea of the beginning player, then second one's worst idea, then the second good idea of the first player and the second worst idea of the second player, and so on.
3. Similar ideas are combined into separate groups (clusters of themes).
4. General ideas during the discussion are ranked from best to worst.

Table 2. Statement of the problem: Point of View (POV)

How we can help	***Personal model:*** The **name** of the potential user***, photo, characteristics, artifacts***
to solve	**"It turns out he needs to"** (the wording of the problem, quotation, metaphor)
this way:	a list of ideas that **may surprise**

Table 3. It turns out he needs ... (assignment: How to maintain a balance between study, work and leisure?»

What does Vasily really need?	**Solution Option**
Reduce travel time	• Teleport • Rent an apartment near the office • Living in the office
Do what you want, not what you need	• Turn a hobby into a job • Score for work and study • Start your own project
Write a diploma	• Buy ready • Write on weekends • Find a service to bypass antiplagiarism • Find a fanatic at work and persuade him to write a diploma
Sleep more	• Previously go to bed • Walk the evening couples • Learn to sleep on super techniques, allowing you to sleep in an hour

Crazy ideas can start the idea generation process. Stupid ideas make the process fun and non-boring and therefore will remove the frame pattern of thinking. The most absurd ideas can be further adapted to the constraints imposed by technology or conditions for the achievement of profitability of the innovative project. Therefore, the task of brainstorming is to fantasize as much as possible and even the most bizarre ideas in a short period of time, and then, in the selection step, to try out thinking and make them real and useful for people, feasible from the point of view of technology and profit.

To generate unconventional solutions to problems, and to approach familiar from differently the SCAMPER technique can be used. SCAMPER is an acronym of the words: Substitute, Replace, Combine, Adapt, Modify, Put to other uses or Use otherwise, Eliminate, Reverse or Turn (Table 3).

Step 4 "Select". To evaluate the hypotheses and to choose the best idea for further development and testing, is made by using different tools. In order to systematize the results of the previous step, one can build a matrix of positive and negative customer experience (Table 4).

Table 4. SCAMPER [3]

Actions	Suggestive or revealing the meaning of the questions
Substitute	Replace with others?
Combine	Is it possible to combine the idea with others, to use in other tasks? What can be combined?
Adapt	What is the solution from another region can solve the problem?
Modify = Magnify	How can I change, improve? How can I increase? How you can bring it to the maximum, to exaggerate, to make a huge? What features can be added? How to add value?
Put to other uses	How can you offer another application? What else?
Eliminate or minify	How to eliminate the problem? What if it was even less? You don't have?
Reverse = Rearrange	How to look at the problem from the other side? How to switch parties (details) of the problem? How to change the sequence, transpose cause and effect (to rearrange items)? What does it mean? How to change the time, pace, place? Is it possible to change positive to negative and Vice versa? Which parties assume the opposite?

To test the idea one can also use the so-called "evaluation matrix". In the sector of the matrix ideas are put, depending on the evaluation of their benefits and costs (Figure 4). Sector are distributed according to the degree of effort or availability of the implementation (the minimum "easy" maximum "hard") as well as the effect of the implementation of ideas ("a very necessary and useful" - "not very necessary and useful"). Spreading all the data and hypotheses on the quadrants of the two-dimensional matrix, we can formulate new hypotheses, to identify new areas for deeper study. Any of object’s characteristics, actions, etc, can be positioned on the axis. Naturally, the best solutions will be those, whose implementation leads to the greatest effect and requires less effort.

Table 5. The matrix of negative and positive customer experience

Top 5 Actions performed by users	Top 5 Actions where there are opportunities for improvement
Top 5 "Needs of the user"	Top 5 "Unmet user needs"

5 step "Prototype". The process of prototyping involves the creation of a sketch, the layout, developed in the process of generating ideas to solve focused problems of the user. This phase checks the idea on the demand of the final consumer.

When prototyping ideas, one can use the technique of "the Wizard of OZ." The method was developed by John F. Jeff Kelly from the research center Thomas J. Watson of IBM in 1980. It is aimed at the study of the human factor, and allows to estimate the reaction of people to the product, in order to understand how users perceive development, and how they will be able to use it.

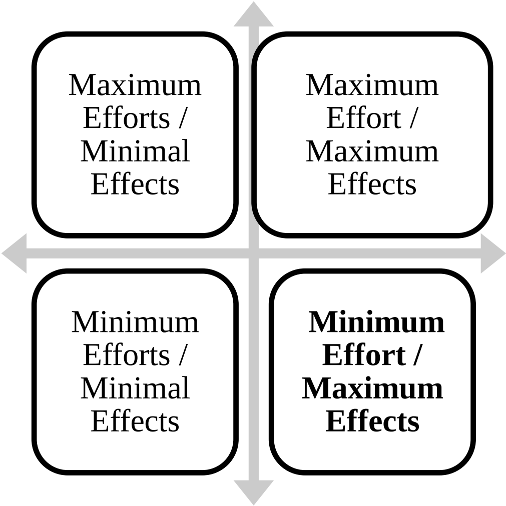

Maximum Efforts / Minimal Effects
Maximum Effort / Maximum Effects
Minimum Efforts / Minimal Effects
Minimum Effort / Maximum Effects

Figure 4. The assessment matrix is "Effort / Effects"

Business origami is created from a paper prototype. Business origami can also be used to describe the interaction between objects (in this case, the connection denoted by arrows above the arrows can be signed scripts or the particular relationship), the display of artifacts in the study of the target audience, the modeling of the situation, the presentation of ideas.

The most affordable and quick way of prototyping is the layout of the sketch. To develop a prototype, one needs to apply the method of gaming simulation using pieces of Lego Serious Play

(LSP). The concept of this method was proposed by the Swiss professors of The International Institute for Management Development , Johan Roos and Bart, in the mid 90-ies. The basis of this method are the principles of play, constructionism and imagination. A serious game should encourage to implement the developed ideas (Figure 5).

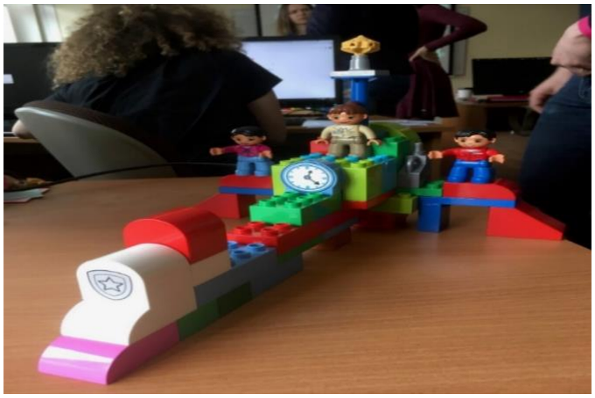


Figure 5. Modeling ideas of the event "Day of students", a group of mA Department of "Business Informatics", 2017

6 step "Test". One of the most interesting things is the technique of "Test user". The method is designed to act the situation by the planned scenario in order to get feedback from the potential user. The user by oneself, without help from developers, has to understand the functioning of the prototype. The researchers actively watch, asking questions during the experiment: "Your impressions?", "What are you thinking about performing this function?", and after testing: "Tell me why it is not convenient (doesn't work as you wanted)?", "Tell us what you felt?", "Why?" "What do you think, what is it?").

7 step Presentation. It is necessary to present the idea, using the Storytelling method. A well-told emotional story with a colorful description of the parts is a great way to communicate ideas. The techniques of making up stories are simplicity (one character in the center and three parts of the story – the action, the conflict and transformation); emotions; disclosure of details; the involvement of the audience. The story can be started from anything-customers, value propositions, resources, or something else.

Storyboard, a series of frames, that shows the sequence of events. The rectangle provides the frame, and the background is the site of action. Men represent the characters of the presented story, and in "bubbles" of speech and thoughts , are where will be written down what they say and think. Also schematically shown, are the actions of the characters.

5. RESULTS

In 2015, the Financial University under the Government of the Russian Federation signed an agreement with the Foundation for Internet development initiatives (Fria) for the inclusion of the course "Internet business" in the educational program in the direction of undergraduate and graduate course "Business-Informatics". In the last two years, FRII has been promoting the idea of introducing

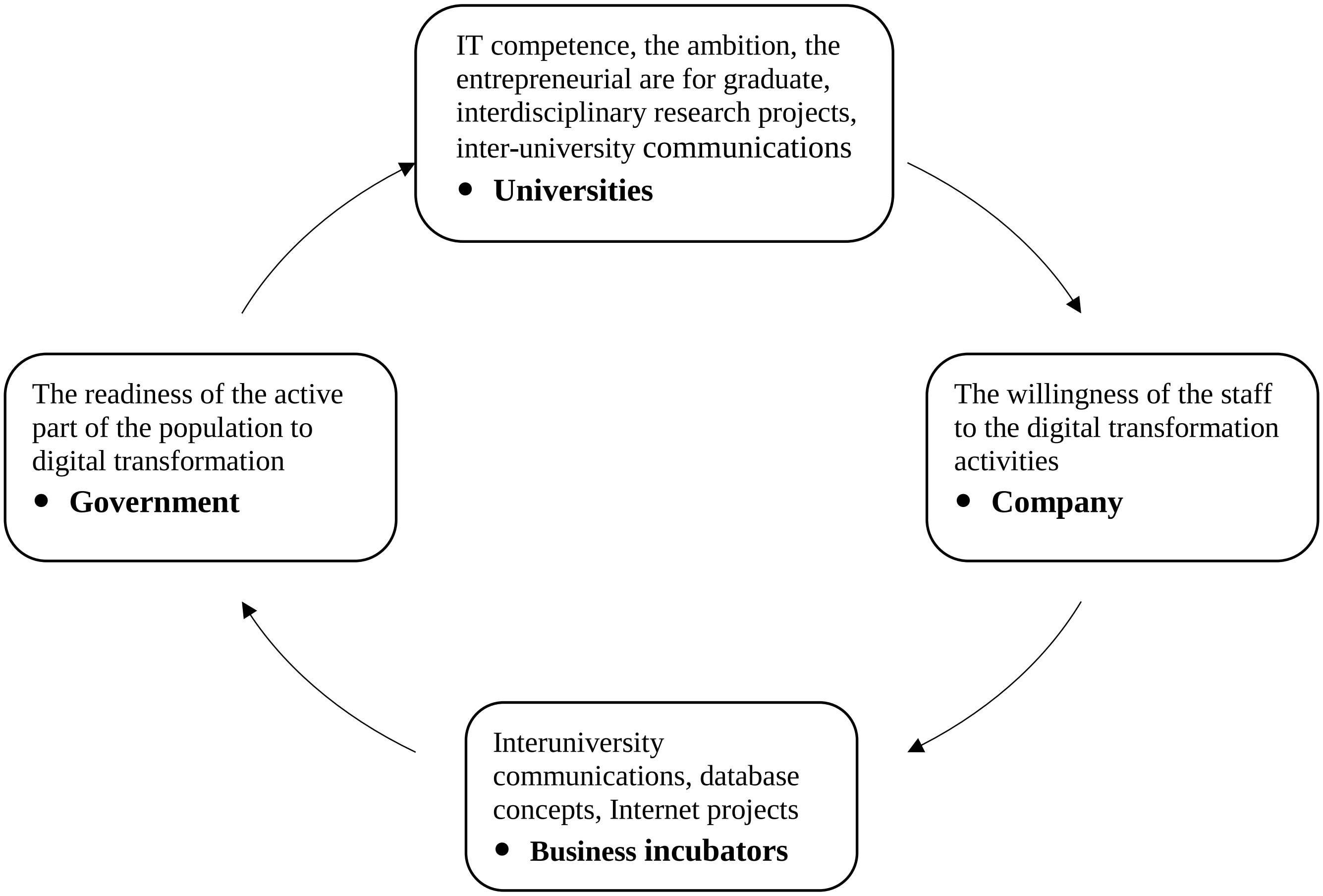

IT competence, the ambition, the entrepreneurial are for graduate, interdisciplinary research projects, inter-university communications
• Universities
The willingness of the staff to the digital transformation activities
• Company
Interuniversity communications, database concepts, Internet projects
• Business incubators
The readiness of the active part of the population to digital transformation
• Government

Figure 6. Ecosystem of training of the graduate and other it areas

this course in educational processes already in more than 100 universities of Russia, Kazakhstan and Belarus. The basis of theoretical and practical materials, we have developed the author's approach to teaching this course was the inclusion of techniques Design Thinking in the Lean Startup approach.

However, we are faced with a problem that is likely relevant to many economic institutions. Innovative ideas created by students, that did not reach the stage of realizing the real product, are not implemented in the online service or mobile app. Having a good background in Economics, and Management, our students are not sufficiently confident in application development, software coding. Thus we have accumulated sufficient useful base unrealized ideas. This would not have happened, if we or other universities, developed ecosystem of support for student it projects (Figure 6).

Participants in such an ecosystem should not only be teachers and students of one University, but also some support members from the University administration. Also it is important to have developed University relations, in which the project can be brought up by the students from different faculties, or areas of training of different universities. Thus, the principle of an interdisciplinary approach to the project was created. The task for universities is to motivate their students to learn from IT leaders the thirst for knowledge, to be innovative, to be ready to share, or to come up with ideas.

In addition, an important role is assigned to IT-leaders, that from the output will not only get interesting and designed decisions, but also specialists prepared to work on the digital markets of their future. It is not for nothing, that the introduction tp the key partners of the principles of Design Thinking is one of the key business technologies of the leading SAP. In the ecosystem of training the future leaders of the digital world, important participants are the applicants and other universities from IT areas. Vocational guidance work with students, is to be carried out, in order to attract to the profession result-oriented people.

6. CONCLUSION

We tested various tools available in Design Thinkig. Today, a year later, came the awareness of what techniques work better at different stages of the project of Internet business. Some methods had to be forgotten, some methods have found successful application in a completely unexpected challenges, and some are yet to be tried out.

The results for students, that we have are the interaction with employers, new knowledge in the field of technological entrepreneurship, the experience of team work, organization of creative competitions, scientific research to perform research activities, ability to present work result. It is easy to teach to encode, to promote their project in the network using known technology Internet marketing, management methods, project management principles, techniques of interviewing potential users to determine the usefulness of even non-existent, but create and almost sale product. Many Internet resources are in no hurry to provide ready-made solutions and advice in any questions regarding the creation and promotion of a startup. It is one thing, though, to talk about already existing methods of analyzing success of product promotion, website, advertising messages on the Internet, which can be checked on ready-made solutions, while quite an another one is to give the opportunity to come up with an idea, analyze its feasibility, assess its competitive advantages, to create a prototype and run it in a test environment.

REFERENCES

1. Community, SAP design thinking. URL: http://scn.sap.com/community/design-thinking
2. Guide to design thinking at d.school. URL: http://dschool.stanford.edu/
3. PI School of Design Thinking. URL: http://hpi.de/school-of-design-thinking.html
4. Natalia Altukhova, Elena Vasilieva, Alla Gromova. (2016). Teaching experience of design thinking in the course of "Internet-business" // Selected Papers of the XI International Scientific-Practical Conference Modern Information Technologies and IT-Education (SITITO). 2016. CEUR-WS. - V. 12 (3-2). - P.100-105.
5. Vasileva E. Techniques of design thinking to the development of team skills and creative abilities of technological entrepreneurs. International Scientific-Practical Conference Modern Information Technologies and IT-Education (SITITO). – 2015. - V. 1 (11). - P.557-561.
6. Michalko, Michael. Cracking Creativity: The Secrets of Creative Genius. Berkeley, CA: Ten Speed Press. (1998).

Remote Laboratory for Servomotor Studying

[1]Vîrlan Petru, [1]Todos Petru, [2]Adăscăliței Adrian

[1]Tehnical University of Moldova
E-mails: petru.virlan@feie.utm.md, petru.todos@adm.utm.md

[2]Tehnical University „Gh. Asachi” Iași, Romania
E-mail: adrian.adascalitei@utiasi.ro

ABSTRACT

This paper presents a way of creating a laboratory work on controlling a remote servomotor. Using LabView, a real experiment is performed, the equipment being remotely controlled, and viewing with a camcorder. The purpose of this paper is to demonstrate the possibility of carrying out laboratory works for students requesting e-learning.

Keywords: virtual, instrument, engineer, servomotor, LabView, remote, laboratory, study

1. INTRODUCTION

An engineer is a person with a technical - theoretical and practical training, obtained in a higher education institution practicing engineering.

Unlike scientists who study the nature and phenomena of nature to establish principles, axioms and theorems, engineers apply the theoretical principles in mathematics and physics to create a concrete product, such as an example, a converter or a mechanism [1].

The laboratory is the subject of the largest financial expenditures in the technical educational institutions, while the rapid development of the technologies and techniques of the contemporary period make it even more difficult to modernize the laboratories. However, because we have the information technologies that provide us with virtual tools to create virtual laboratories that are no more down-to-earth than real laboratories. At the same time, investments are considerably low.

Remote lab - this kind of lab, as shown in Figure 4, is a software application that can be accessed online via the browser, but it allows for a real experiment, the equipment being routed remotely, and visualization done with a video camera [2].

2. REMOTE LAB EQUIPMENT FOR SERVICE CONTROL

To create a "Remote" lab, we will use the LabView application, an Arduino board, communication equipment, a servomotor and a potentiometer. We will also create a control and data acquisition interface to provide distance learning students with the lab by visualizing real physical equipment through a video camera.

Below we present each hardware component of the lab with a small description of it.

The LabView application

LabVIEW is a graphical programming environment based on the G language (graphical language), designed specifically to build applications to control and acquire data, analyze them and present the results. We mention some of the most important features of this environment: - Automatically resolves most of the problems associated with hardware resource management and operating system communication, and in this way the user can focus on the concrete problem he has to solve and not on the operation of the computer . For example, almost all of the nodes (functions), as well as the graphs, adapt to any type of data, whether they are simple real values or data structures;

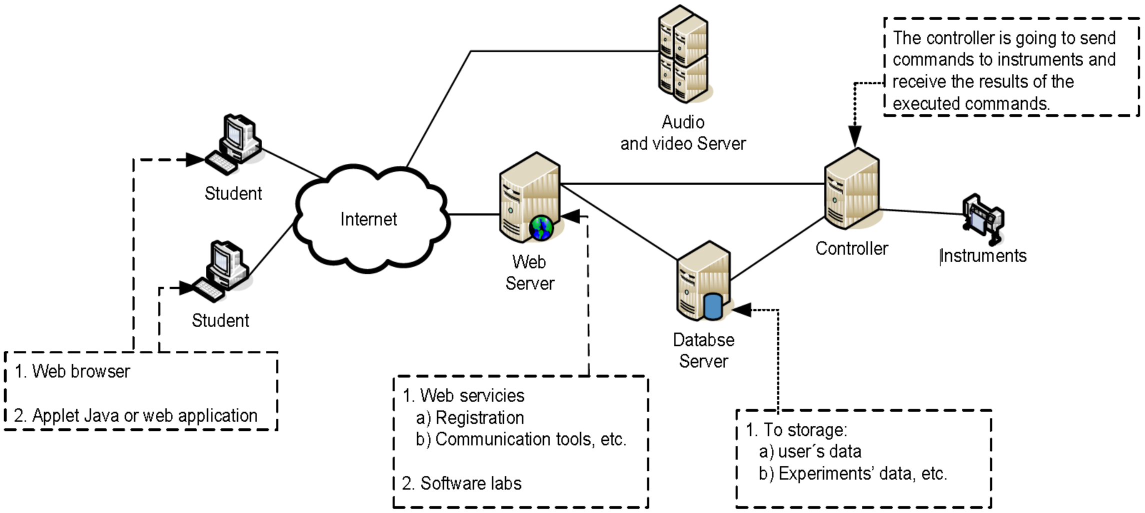

The controller is going to send commands to instruments and receive the results of the executed commands.
Audio and video Server
Student
Internet
Web Server
Controller
Instruments
Student
Databse Server
1. Web browser
2. Applet Java or web application
1. Web servicies
a) Registration
b) Communication tools, etc.
2. Software labs
1. To storage:
a) user´s data
b) Experiments' data, etc.

Figure. 1. Remote lab [2]

- graphical language is more compact, the chart contained in a window contains more information than text, and is easier to read and understand, and drawing a chart is faster than writing an equivalent text;

- in graphical language, parallelism is natural, so writing programs that perform parallel data processing is just as simple as sequential processing;

- allows networking across multiple computers via TCP / IP and UDP, with many functions for working in local area networks or the Internet;

- contains many pre-fabricated applications in various fields, along with the corresponding G code, which can be used directly, can be taken as a teaching example or can be modified by the user to best meet the specific work needs.

All LabVIEW solutions work by default on multithreading without requiring additional programming. In this way, the time needed for the development of applications can be significantly reduced. LabVIEW is available for a wide range of operating systems: Windows 2000 / NT / XP / Me / 9x, Mac OS, Sun Solaris, Linux [3].

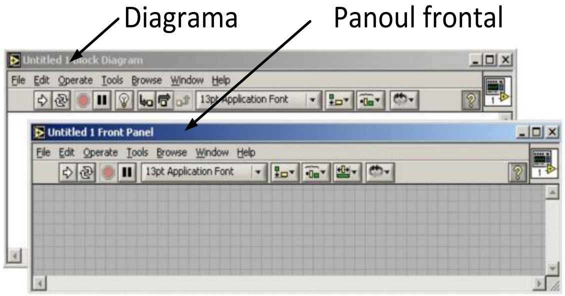


Figure 2. LabVIEW panel and diagram [3]

The Front Panel is the graphical user interface, the window the user will see when they access the application. Using panel elements, the application receives the input data and then displays the output data that resulted from the run.

Block Diagram is the window where the programmer describes the algorithm after which the application will perform the calculations and reasoning required to process the information. In most cases, after the developer has made an application and delivered it to a user, the latter no longer has access to the chart.

Plate arduino Uno

Arduino is a very simple microcontroller platform to use. Arduino can be used to develop interactive applications. In fact, the information is taken from a wide range of input elements (sensors and switches), processed inside the microcontroller and transmitted to an equally wide range of output elements: LEDs, motors, actuators, etc.

The advantages of Arduino over these microcontroller-based systems are:

- reduced acquisition costs;
- can be used on any operating system (Linux, Windows or MacOS). Most development boards are limited to the Windows operating system.
- a simple and easy to learn programming environment.

Arduino Uno is a development board based on the ATmega328P microcontroller, with 6 analog inputs, 14 digital inputs / output pins (6 of which can be used as PWM outputs), a 20 MHz quartz oscillator, a USB connection, a power jack, and a reset button.

Significance of pins:

- VCC - the positive pole of the source (+);
- GND - mass (-);
- PB 0-7 - the 8 input / output pins of port B;
- PC 0-5 - the 6 input / output ports of port C;
- PD 0-7 - the 8 input / output pins of port D;

- ➢ ADC 0-5 - input pins that provide digital analog conversion.

Analog inputs are used to read analog signals from temperature sensors, light sensors, pressure sensors, humidity, etc. An analog input pin can measure a current or voltage signal between 0-5 V. Digital Inputs / Outputs: Allows you to read the state of an input / output element or control elements that have two states: closed ie 0 (LOW values) or open 1 (HIGH); The Pulse Width Modulation (PWM) Pulse Width Modulation (PWM) Pulse Width Modulation (PWM) Pulse Width Modulation (PWM) Pulse Width Modulation Pulse Width Modulation Pulse Width Modulation Pulse Width Modulation The USB port has two roles: to supply the Arduino platform and to provide system data. Power supply of the Arduino platform can be made from an AC-DC power supply with recommended voltage between 7-12 V through the power socket.

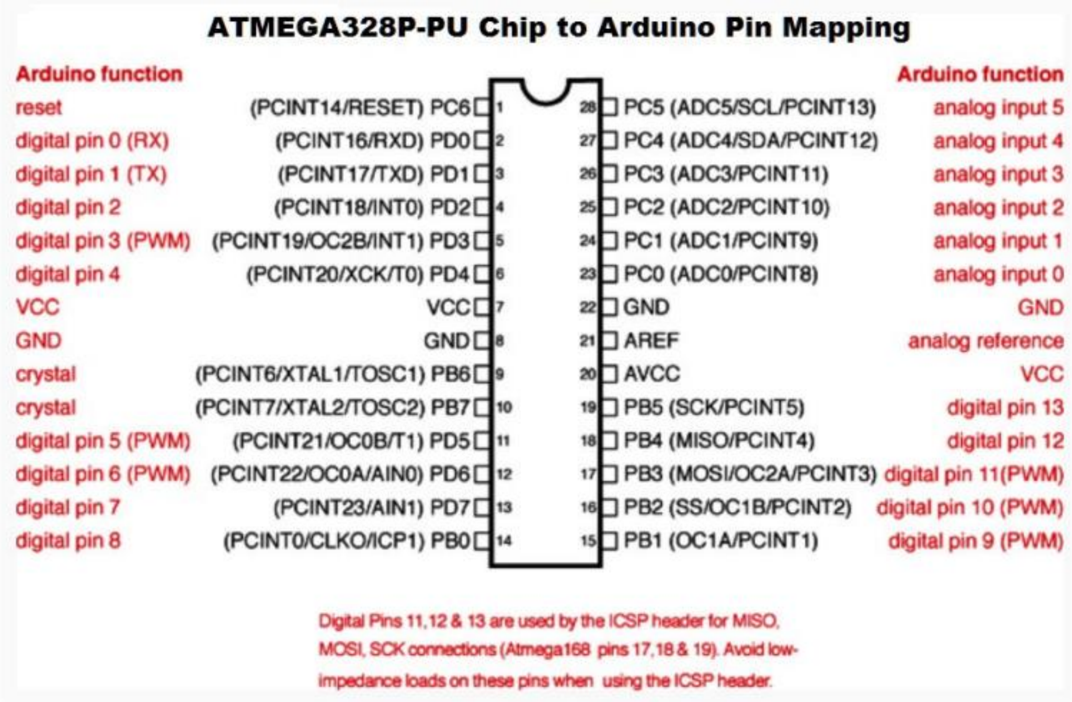

ATMEGA328P-PU Chip to Arduino Pin Mapping
Arduino function
Arduino function
reset (PCINT14/RESET) PC6 1 28 PC5 (ADC5/SCL/PCINT13) analog input 5
digital pin 0 (RX) (PCINT16/RXD) PD0 2 27 PC4 (ADC4/SDA/PCINT12) analog input 4
digital pin 1 (TX) (PCINT17/TXD) PD1 3 26 PC3 (ADC3/PCINT11) analog input 3
digital pin 2 (PCINT18/INT0) PD2 4 25 PC2 (ADC2/PCINT10) analog input 2
digital pin 3 (PWM) (PCINT19/OC2B/INT1) PD3 5 24 PC1 (ADC1/PCINT9) analog input 1
digital pin 4 (PCINT20/XCK/T0) PD4 6 23 PC0 (ADC0/PCINT8) analog input 0
VCC VCC 7 22 GND GND
GND GND 8 21 AREF analog reference
crystal (PCINT6/XTAL1/TOSC1) PB6 9 20 AVCC VCC
crystal (PCINT7/XTAL2/TOSC2) PB7 10 19 PB5 (SCK/PCINT5) digital pin 13
digital pin 5 (PWM) (PCINT21/OC0B/T1) PD5 11 18 PB4 (MISO/PCINT4) digital pin 12
digital pin 6 (PWM) (PCINT22/OC0A/AIN0) PD6 12 17 PB3 (MOSI/OC2A/PCINT3) digital pin 11(PWM)
digital pin 7 (PCINT23/AIN1) PD7 13 16 PB2 (SS/OC1B/PCINT2) digital pin 10 (PWM)
digital pin 8 (PCINT0/CLKO/ICP1) PB0 14 15 PB1 (OC1A/PCINT1) digital pin 9 (PWM)
Digital Pins 11,12 & 13 are used by the ICSP header for MISO, MOSI, SCK connections (Atmega168 pins 17,18 & 19). Avoid low-impedance loads on these pins when using the ICSP header.

Figure 3. Atmega328P microcontroller pins [4]

Requirements for C-program training would seem difficult for beginners, but due to its structure it has a wide range of possibilities.

Several training rules will be enough to be memorized:

- // (unilateral comment) is often used in the content of the program to more explicitly describe one of the program rows. All that is written after the double bar and to the end of the given row will be ignored by the compiler;

- / * * / (multilateral comment) this structure is used if there is a need to explicitly describe the content of several rows in the program, all that is written between these symbols will be ignored by the compiler;
- {} is used to determine the start and end of the control block (used for functions and cycles);
- **;** each command must end with this symbol (the lack of this symbol makes the compilation impossible).

variables:

- int (integer numbers) stores numbers in memory using 2 bits or 16 bits and can include any integer in the range -32768 .... 32767;
- **long** is used when int is not enough, occupies memory from 4 bits up to 32 bits and contains integer numbers in the range -147483684 .... 2147483647;
- **boolean** (true / false), occupies only one bit of memory;
- **float** (decimal numbers) is used to enter the decimal numbers;
- **char** (symbol) holds a symbol using the ASCII encoding system.

Mathematical Operations:

- **=** (assigns) makes an assignment (example: x = 10 * 2, assigns it to variable x number 20);
- **%** (as from the division) 12% 10 result the result 2;
- **+** (assembly);
- **-** (difference);
- ***** (Îmulţire);
- **/** (division).

Symbols for logical comparison:

- **==** (equal);
- **!=** (different);
- < (smaller);
- > (bigger);

By using the programming rules, the program is being developed, which will command the servomotors according to the prescribed algorithm.

Running the "arduino" program from the development environment you just downloaded to the previous step (see the screenshot below). Arduino connects to the PC via a serial port. The first step you have to make is to determine this port. The easiest way is to connect the board, wait about 30 seconds - 1 minute to make sure it was detected by your PC and then open the "Tools -> Serial Port" menu. You should see one or more entries. Memorize them (or write them on a sheet of paper / make a screenshot). Disconnect the Arduino card from the USB port (removes the cable from the PC). Opens the "Tools -> Serial Port" menu again. That port that has disappeared is the port associated with the Arduino board. Reconnect the Arduino board to the PC, wait for it to be recognized by the PC, and then select the port from the "Tools -> Serial Port" menu. The next step is to select the type of plaque you work with. From the "Tools -> Board" menu, select the type of board you are working with (Arduino Uno, Leonardo, Mega, etc.) [4].

3. LIST OF THE ARDUINO PROGRAM FOR DIRECT START AND REVERS OF SERVOMOTOR

The control of the actuator without the LabView application can only be done by programming the Arduino board, this procedure is presented below.

Servo motors allow precise positioning and can be controlled using the Servo Arduino library.

A linear regulator can be used to create a 5V secondary source.

Coding of comments is essential to facilitate debugging and sharing.

Program

```
#include            //Servo library
 Servo servo_test;    //initialize a servo object for the connected servo
int angle = 0;
void setup()
{
  servo_test.attach(9);   // attach the signal pin of servo to pin9 of arduino
}
void loop()
{
  for(angle = 0; angle < 180; angle += 1)  // command to move from 0 degrees to 180 degrees
  {
    servo_test.write(angle);      //command to rotate the servo to the specified angle
    delay(15);
  }
  delay(1000);
  for(angle = 180; angle>=1; angle-=5)    // command to move from 180 degrees to 0 degrees
  {
    servo_test.write(angle);         //command to rotate the servo to the specified angle
    delay(5);
  }
    delay(1000);
}
```

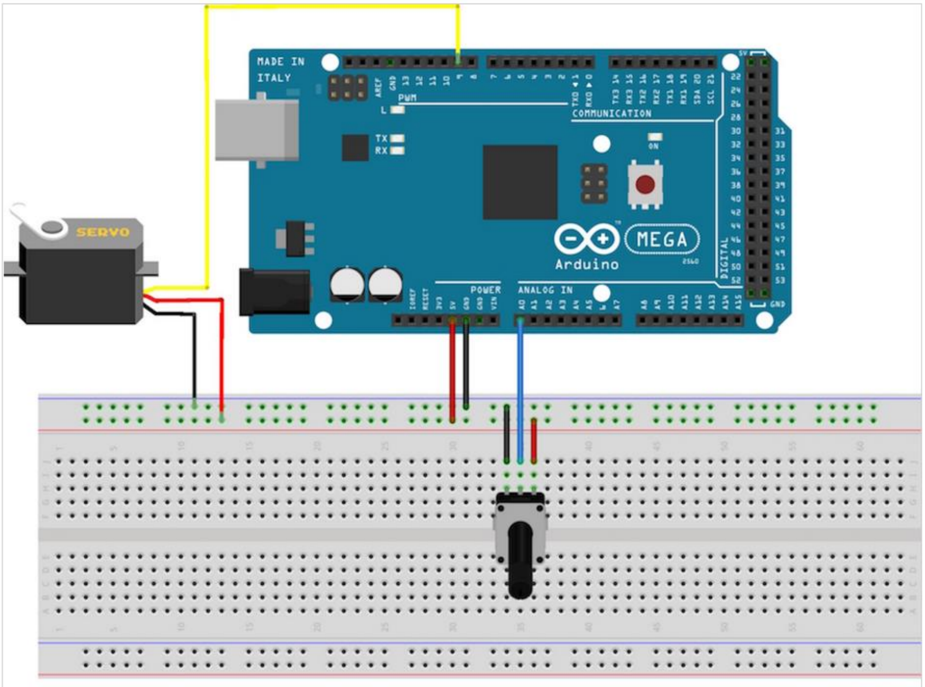


Figure 4. Electrical connection diagram [6]

4. CREATING THE REMOTE LAB FOR DIRECT RUNNING AND REVERSE OF THE SERVOMOTOR

The LabView application allows you to control the remote actuator. So there is no need for the listing of the Arduino program.

In this case, the following steps are taken:

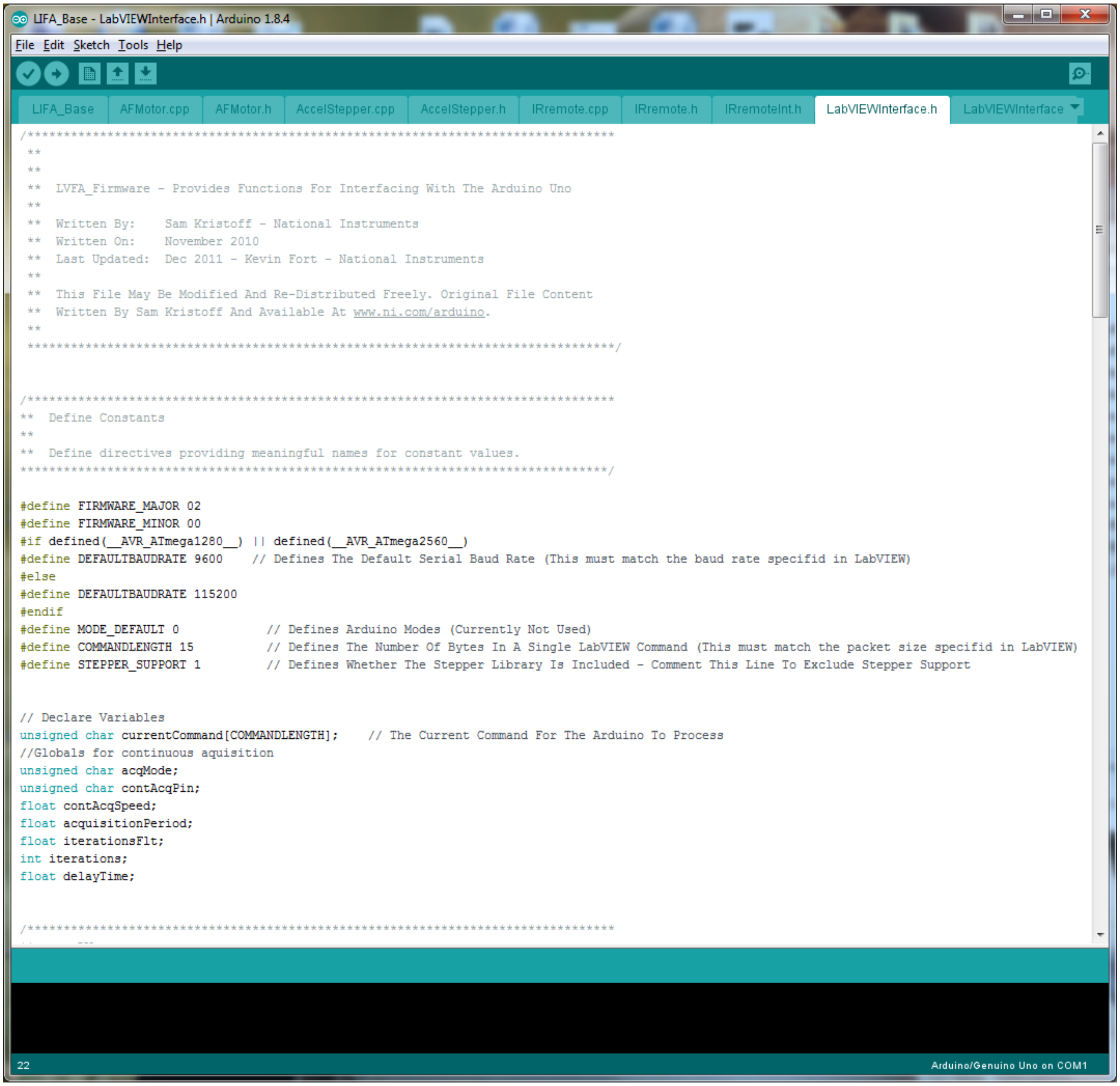
Step 1

We link the LabView application to the Arduino board.

First, we download the "arduino-1.8.4-windows" exe file from the "https://www.arduino.cc/en/ Main / Software" site. Then install it on your computer. At the same time, download and install the "VI Package Manager" software from the "http://www.ni.com/tutorial/ 12397 / en /" website, which contains the program file that provides the LabView interface with arduino (Figure 14).

Step 2

Load the program in Figure 14, in the memory of the Arduino UNO board. This ensures communication between Arduino and LabView.



```
/*********************************************************************************
 **
 **
 **  LVFA_Firmware - Provides Functions For Interfacing With The Arduino Uno
 **
 **  Written By:    Sam Kristoff - National Instruments
 **  Written On:    November 2010
 **  Last Updated:  Dec 2011 - Kevin Fort - National Instruments
 **
 **  This File May Be Modified And Re-Distributed Freely. Original File Content
 **  Written By Sam Kristoff And Available At www.ni.com/arduino.
 **
 *********************************************************************************/


/*********************************************************************************
**  Define Constants
**
**  Define directives providing meaningful names for constant values.
*********************************************************************************/

#define FIRMWARE_MAJOR 02
#define FIRMWARE_MINOR 00
#if defined(__AVR_ATmega1280__) || defined(__AVR_ATmega2560__)
#define DEFAULTBAUDRATE 9600    // Defines The Default Serial Baud Rate (This must match the baud rate specifid in LabVIEW)
#else
#define DEFAULTBAUDRATE 115200
#endif
#define MODE_DEFAULT 0            // Defines Arduino Modes (Currently Not Used)
#define COMMANDLENGTH 15          // Defines The Number Of Bytes In A Single LabVIEW Command (This must match the packet size specifid in LabVIEW)
#define STEPPER_SUPPORT 1         // Defines Whether The Stepper Library Is Included - Comment This Line To Exclude Stepper Support


// Declare Variables
unsigned char currentCommand[COMMANDLENGTH];    // The Current Command For The Arduino To Process
//Globals for continuous aquisition
unsigned char acqMode;
unsigned char contAcqPin;
float contAcqSpeed;
float acquisitionPeriod;
float iterationsFlt;
int iterations;
float delayTime;


/*********************************************************************************
```

Fig. 5. The LabView interface with arduino.

Step 3

The front panel (Figure 15) which contains the control and acquisition part of the laboratory and is visible to the student, as well as the block diagram (Figure 16), which is designed to create control logic of the actuator, is not visible to the student.

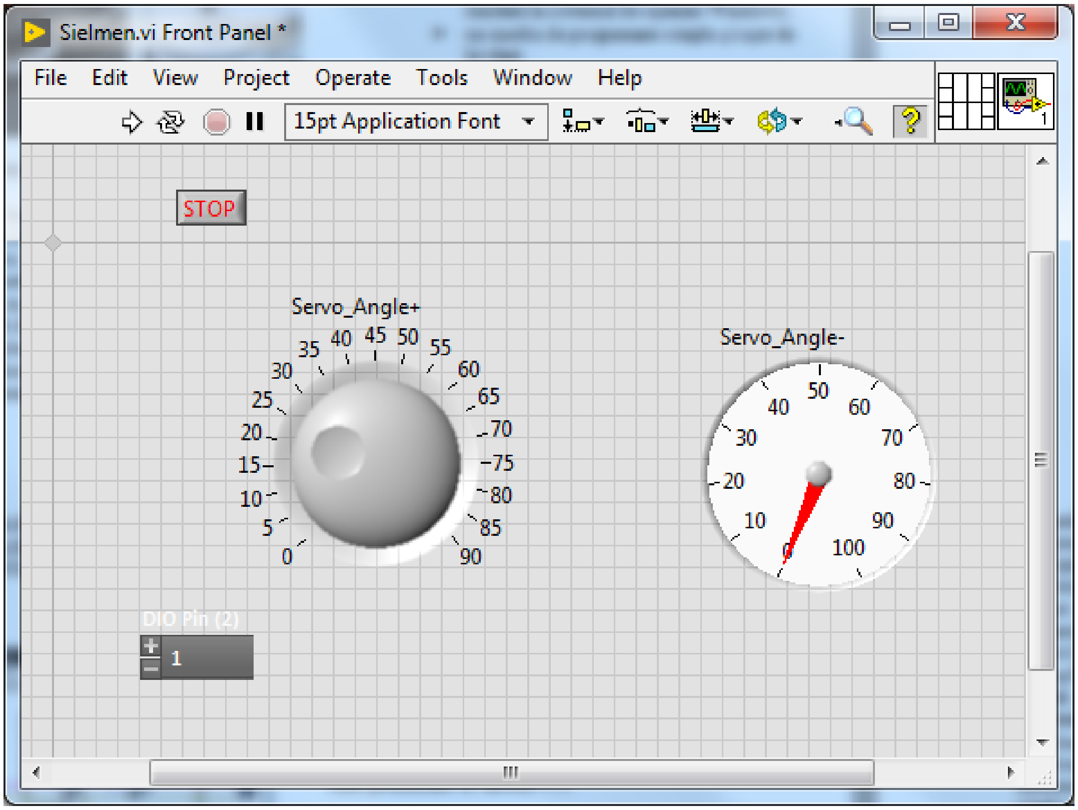


Figure 6. Front panel for servomotor control

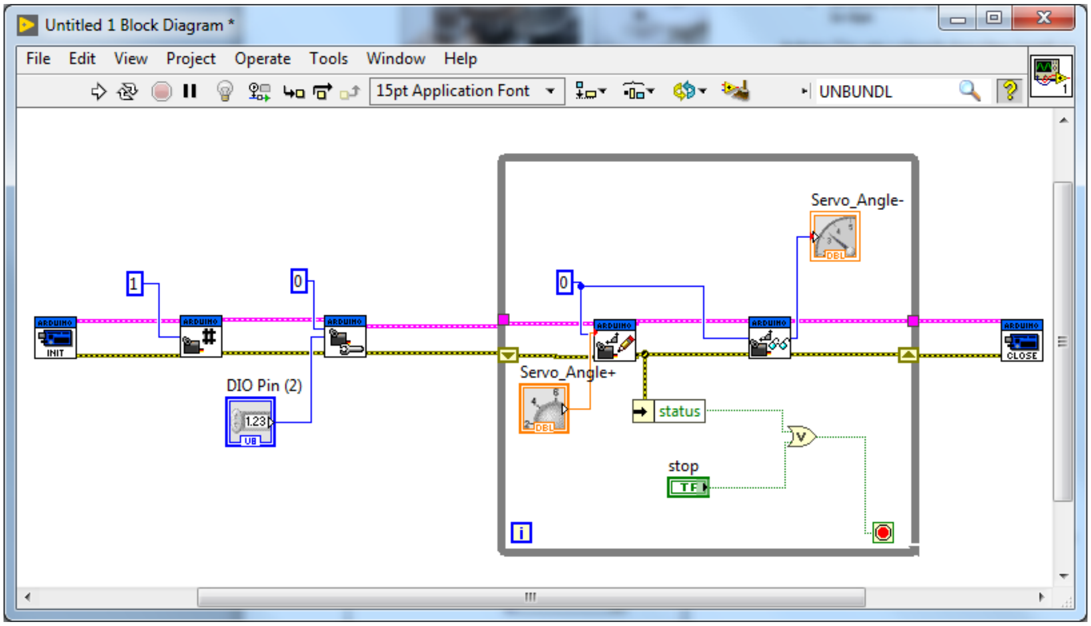


Figure 7. Block diagram for servomotor control

In the front panel for servomotor control, the student can change the direction of rotation of the actuator, the number of steps, the angle of rotation, etc. LabView also allows real physical parameters of the servomotor to be viewed, such as voltage, current, and so on.

In order to pay attention to the laboratory work, each student receives a special task for the study of the servomotor and the results obtained include them in the report and send them to the teacher on the Moodle e-learning platform.

The platform provides online communication between teacher and student. So the student can call on any question at any time. This possibility gives the student the maximum speed to elaborate and present the report of the laboratory work.

5. CONCLUSION

This paper aims to demonstrate the possibility of performing laboratory work at technical disciplines, with the student being at a distance.

Although the control and acquisition of data is virtual, the student can see through a video camera the real physical process that takes place in the laboratory room. Moreover, he can accomplish the work at any time, or may be invited to work with the up-to-date students.

LabView environment allows for any data acquisition and process control. And the arduino plate due to the low cost price makes communication with the physical part of the laboratory work. Therefore, this method of performing laboratory work seems to be the most optimal for the Republic of Moldova.

REFERENCES

1. http://ro.wikipedia.org/wiki/Inginer

2. http://www.researchgate.net/publication/224148635

3. http://www.dpue.energ.pub.ro/Laborator_Informatic/files/info/Laboratorul%206.pdf

4. http://elth.ucv.ro/student1/Cursuri/Bratu%20Cristian/MAP/004%20-%20Curs%20004%20-%20MAP%20-%20Arduino.pdf

5. http://onheli.blogspot.md/2010/02/inside-of-servo.html

6. https://www.allaboutcircuits.com/projects/servo-motor-control-with-an-arduino/

7. Evans Brian W. Arduino Programing Notebook, San Francisco, California, USA 2007

Quality Assurance in On-line Education

[1]Todos Petru, [1]Ghencea Cristina, [1]Vîrlan Petru, [2]Adăscăliței Adrian

[1]Tehnical University of Moldova
E-mails: petru.todos@adm.utm.md, cristina.ghencia@fiu.utm.md, petru.virlan@feie.utm.md

[2]Tehnical University „Gh. Asachi" Iași, Romania
adrian.adascalitei@utiasi.ro

ABSTRACT

Online education constitutes an important component in the continuous growth / development of higher education and adult education. Its quality largely depends on the design rules and the evaluation standards of the programs as a whole as well as the study courses as component parts. The need to ensure the quality of online courses is a current issue. The paper proposes a system of standards, criteria and performance indicators for the design and internal evaluation of on-line courses on e-learning platforms, based on the own experience and good European and world practice.

Keywords: on-line, course, quality, e-learning, evaluation, standards, performance, indicators, distance, learning, Moodle, statistical, analysis, student, perception, assessment.

1. INTRODUCTION

The development of information and communications technology from the last decade has led to fundamental changes in educational practice, leading to the introduction of modern teaching and learning methods. E-learning has emerged in response to the need for learning and refinement in a modern, dynamic world where the information is updated every second, every person, regardless of age and occupation, being obliged to learn and improve continuously. Internet technologies, new Information and Communication Technologies (ICTs) have revolutionized all areas of social and professional life, including learning, education. Due to their massive use in everyday life, new technologies allow an emancipation in the people capacity to learn, favoring a spontaneous tendency towards meta-knowledge and assuming the learning process.

Educational practice has shifted from a closed, teacher-controlled pedagogical approach to an open, transparent, integrated society that supports the student's initiative, facilitating collaboration, personal skills, and lifelong learning. Putting the student at the heart of this new training paradigm, there is a fundamental change in education from content-based learning to context-based learning.

Classical face-to-face education has not lost its actuality or value. It remains for both present and future generations as precious. It should only be updated, supplemented with new tools, special possibilities offered by the information and communication system provided by the Internet, the media, the contemporary ICT tools. Initial training is and will continue to be a priority in the future in the form of presence for young people studying and wanting to learn the fundamentals of science, especially if it is medicine, engineering, philosophy - sciences requiring a multidisciplinary and very profound training before to pursue purely professional training in a narrow field. The foundation is also necessary for a rapid reorientation to new specialties, demanded by the ever-changing market.

Part-time studies and distance learning have emerged as systems dictated by certain economic conditions, first and foremost, the need to continue work and education. This system is constantly developing. Statistical data on the composition of full-time and part-time studies over the last 25 years in TUM speaks explicitly about the importance of this initial training course for specialists with higher education, including for engineering fields. During these years there have been dramatic changes in higher education: there have been major falls in the number of engineers enrolled in the 1990-2000 period, followed by a real explosion with the doubling or even tripling of the quota in 2006-20010, after that, to be reduced to the level of the 90's. However, there was a perfect stability of the share of students enrolled in part-time studies, which within TUM is 28-35 percent.

Master study programs in Moldovan universities are offered now only full-time and can be followed by people who live and work in Chisinau. By remote (part-time) studies, it would be possible to expand the area, to cover the needs of a considerable number of people working outside the capital, including outside the country. The same situation occurs in doctoral schools.

Undoubtedly, there is a need for distance learning for adults, for people who already have a specialty, have jobs, but for the advancement and deepening of knowledge need additional studies, that can be organized more conveniently in the form of distance learning. The person studies at the proper time and at the place where there are necessary conditions and time to do so, without interrupting the basic activity. The person can choose and study the necessary courses and modules corresponding to his or her personal capabilities.

TUM's practice shows us that students enrolled in the engineering programs at the beginning of the second year are starting to look for a job (whether they have financial problems or because of professional reasons). At the four-year study, practically everyone has a job whose program very rarely correlates with the faculty's curriculum. In this context, the mixed form of organization of studies (the concept of blended learning) is a great solution.

Under these circumstances, courses that can be studied online are welcome. These are highly appreciated by students from all cycles and study forms.

The term of online learning is used in many different ways. It generally refers to a method of providing educational information via the Internet [8]. These can range from downloadable content (such as digital textbooks, video or audio) through informal delivery (such as online open courses - MOOCs) to fully structured online courses that include assessments and a qualification. In this work, the online learning will be perceived / understood in this latest form.

Online learning frees the education from the time and space constraints of face-to-face teaching. Nevertheless, learning online and traditional classroom learning are not opposed. Online learning should be seen as a different teaching and learning method that can be used alone (distance and part-time learning) or to complement blended learning [8].

Online learning has many common sides with the "classic" one, but also many specific differences that need to be considered, especially at the design stage.

Study materials for online or part-time education differ from traditional ones, given some key issues [5, 8, 12, 13]: in full-time education, the teacher is the central component of the education system, other learning resources having the secondary role. In online education and part-time education, teaching and, implicitly, direct contact with the teacher are replaced by an individual study with the support of study materials, instructions and the tutoring system. Thus, the teacher is provided with materials designed and tailored to the individual study and by a tutor who systematically provides remote educational support and periodically face to face.

Thus, study materials for online education must fully replace the role of the teacher. They must explicitly: define what is to be learned; provide the necessary information to browse the topics; present examples and explanations, ask questions and introduce individual work tasks; generate student-tutorial interactions and periodically provide self-evaluation with the necessary feedback.

Therefore, designing or converting a traditional course into one online learning is done by considering the following structural elements: learning objectives, study approach recommendations, previous knowledge testing, learning tasks, feedback to study activities, examples, Self-evaluation tests, multimedia elements, and links in hypertext. The content of a course will be divided into subjects / study units that facilitate gradual and structured learning within a defined time unit and end by self-assessment or road mapping.

The success or failure of online learning will depend in a large extent on the quality of its components, primarily on the extent to which the developer of the course has complied with its specific requirements. The quality / performance standards on which the assessment of these courses is based must reflect the above-mentioned requirements.

In appreciating the quality of online courses a special role belongs to students / learners – the central partners of any educational process.

The purpose of this study is to provide creators of educational materials, a system of standards that can effectively guide them in designing or transforming classical study materials into study materials specific to online education as well as a tool for evaluating the quality of online courses by their beneficiaries.

2. BIBLIOGRAPHIC ANALYSIS OF QUALITY ASSURANCE IN ONLINE EDUCATION

From the above, it is clear that when evaluating online programs and courses, the general standards and criteria developed for the evaluation of classical courses and programs will be supplemented with specific standards and indicators reflecting student-platform, student-tutor and student-student aspects of communication / interaction, technical aspects, etc.,

Undoubtedly, online courses have to meet the general requirements defined by the “Standards and Guidelines for Quality Assurance in the European Higher Education Area (ESG)”, adopted at the Bergen Summit (2005) and subsequently presented at the Erevan Summit [1]. This reference document proposes a set of 10 standards and guidelines for internal and external quality assurance in European higher education. ESG does not set quality standards nor imposes how the quality assurance processes should be implemented, but provides guidance, covering dimensions that are vital to the quality of educational supply and learning environments in higher education in general, defines a common framework for quality assurance systems in terms of learning and teaching at European, national and institutional levels.

In another European reference document [2], the ESG requirements are addressed through engineering education. ENAEE (European Network for Engineering Accreditation) standards for accrediting engineer-training programs [2] are described in terms of student workload requirements (in ECTS credits), learning outcomes and training control. It specifies that students' workload requirements and learning outcomes should respect the general framework for qualifications in the European Education Area (CC-EHEA), the competencies being expressed by generic descriptors for each cycle. Training management requirements are in line with standards and guidelines for quality assurance in the European Higher Education Area (ESG).

At national level, each state, adhering to the Bologna process, has committed itself to promoting the requirements of the ESG and CC-EHEA general framework, adopting its own standards systems for the evaluation and accreditation of study programs. Thus, the National Agency for Quality Assurance in Vocational Education in the Republic of Moldova (NAQAVE) [3] has developed a system of standards, criteria and performance indicators for the internal evaluation of study programs as a whole, with separate headings for initial professional training and adults' training. In the fifth part of the RAQAHE Guide (Romanian Agency for Quality Assurance in Higher Education) [4] there are nominated standards, criteria and specific performance indicators for the external evaluation of study programs in distance learning. A separate chapter of this heading is dedicated to the requirements of e-learning platforms used as support for distance learning programs.

As far as the fundamental requirements regarding the quality of education, the policy of the state and of the tendering institutions are concerned, the education services will be the same regardless of the type of programs and the way of delivery - full-time, part-time, online or blended learning. At the same time, as mentioned above, there are significant differences between e-learning and campus education. To address these differences were required adjustments to the design and evaluation methods of these programs and courses. For example, in 2006, the Swedish National Higher Education Assessment Agency [5], initiating the evaluation of distance learning programs, identifies five aspects of high quality of e-learning: information and communication technology, structure planning, teachers' skills, adjusting students' needs, infrastructure and organization. In the coming years, we see an explosive development of standards-based systems specializing in designing and evaluating online programs and courses for both distance and blended education [7-11].

Ensuring the quality of the study courses - the basic components of the curriculum for both full-time, distance, or blended-learning education, as well as continuous training, is the responsibility of the educational service providers [1].

Most universities have developed their own standards systems, guides to good practice on designing and evaluating courses for online education [7, 9, 10, 11]. In [7] we find an exemplary model of standards' systems designed to evaluate online courses provided by Penn State University (USA) for distance learning. These standards place a strong emphasis on accessibility, utility, ease of navigation within the course, information security. One of the most complicated issues in distance learning - competency assessment; it is widely addressed in the Good Practice Guide, developed at the command of the Academic Patented Consortium of Texas State (USA) [8]. The same interest represents the system of standards [9], property of the consortium mentioned. Similar systems of specialized standards apply to universities in the UK, Canada, Australia [10], South Africa [11] and many other countries that have developed distance learning or blended-education courses.

As far as the education system in the Republic of Moldova is concerned, the Education Code provides for the organization of full-time, part-time and distance studies for all three cycles of higher education. By the order of the Minister of Education of May 2016, it was adopted the Framework

Regulation on Organization and Deployment of Distance Higher Education in the first cycle I - Bachelor's and cycle II - Master's Degree and Adult Formation in Higher Education Institutions [12]. This specifies concrete requirements, including the provision of students with teaching materials, delineation of study activities that can be offered online (individual study, self-evaluation, planned tutorial) and activities taking place in the university campus with attendance (seminars, laboratory works, final assessment of the competences of the students accumulated at the units of course). The study process is based on methodological and didactic materials that are especially adapted to the specifics of distance learning: information guides, multimedia interactive courses, electronic courses, self-test systems, special teaching materials that can be disseminated through both E-learning platforms and Internet, and intranet networks, accessible on different terminals (computer, tablet, smartphone, etc.). It will also be mentioned that the ANACIP Guidelines for External Evaluation of Bachelor, Higher Education Programs [3] specify within the "Teaching-Learning Process" standard, criterion 3.1.3, the importance of using ICT (2 out of 100 points are awarded), but without specifying the relevant indicators and evidence to be considered to meet this standard. Good practice guides, developed by Moldovan universities, focus on practical recommendations on course design, the use of the various tools provided by the Moodle e-learning platform, and only a limited number of prescriptions on the assessment of the courses developed. For example, [13] includes an evaluation list comprising 17 questions, which in most of them are related to the structure of the course developed. The current study comes to fill this shortcoming.

3. SYSTEM OF THE ONLINE COURSES EVALUATION

During an institutional research project, using the practical experience of the project team in the field of teacher training on the design of e-learning courses accumulated over more than 7 years and the good practices mentioned in Chapter I, it has been developed an academic system of standards, criteria and performance indicators (SICP) that has as its fields of use:

- Online courses design for online and blended education
- To define the requirements regarding the content of didactic materials in teacher training programs - course creators and tutors;
- Evaluation of e-learning courses in order to accept their placement on TUM learning platforms,
- Evaluating modules in order to recognize them as study units relevant to adult learning programs,
- Evaluation of the pretending courses at "TUM Quality Label", the TUM Senate Award, and the recognition of the status of the published methodical work.

The SCIP TUM system comprises three types of standards and indicators (fig.1):

- Educational, which defines the scientific content of the material presented,
- Structural, which are specific to the online course,
- Providing online course support.

The eight evaluation standards (STEs) included in the SCIP TUM system have common descriptors with those defined by NAQAVE / ESG / EURO-ACE standards for evaluating study programs (Figure 2). At the same time, it should be mentioned that the NAQAVE standards "Student social insurance" and "External program quality assurance" from the SCIP TUM list were omitted as little relevant for the evaluation of courses or modules. These include indicators that are only appreciable at program or institution level.

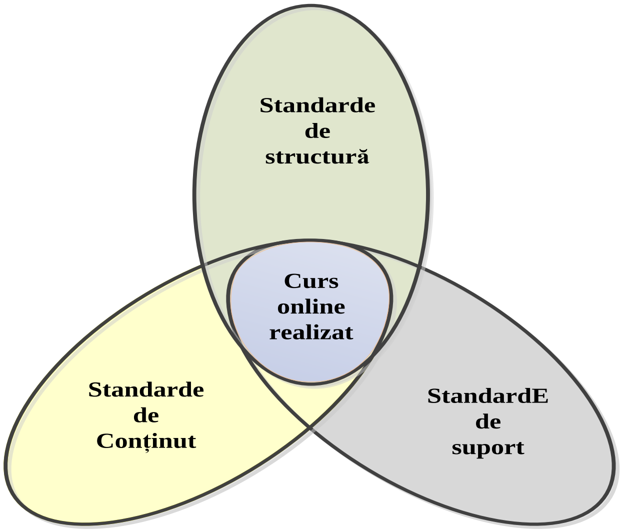


Figure 1. Quality Assessment Standards of the online courses

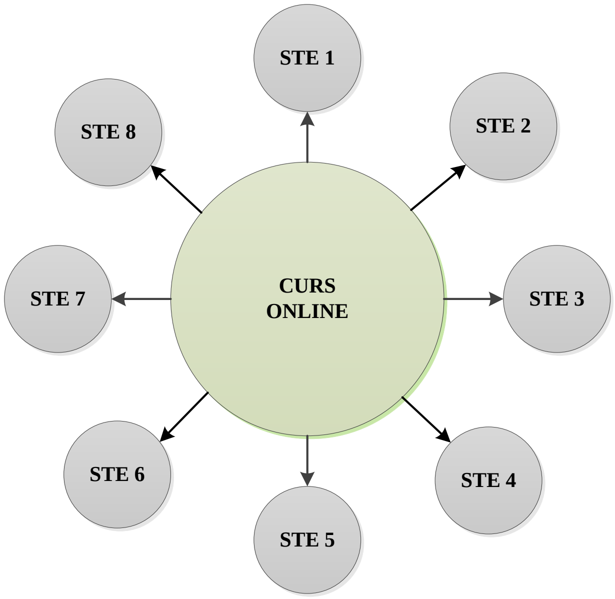


Figure. 2 Standards for assessing the quality of online courses: STE 1 – Policies for quality assurance, STE 2 - Course design, STE 3 – Teaching-learning - student-centered assessment, STE 4 - Admission, course, certification, STE 5 – Academic staff, STE 6 - Learning Resources and Students'

Support, STE 7 - Information Management, STE 8 - Continuous Monitoring and Periodic Evaluation of the Course

For each of the 8 standards there were defined from 1 to 5 evaluation criteria (in general 19) and performance indicators: from 1 to 5 for each criterion, in general 46 indicators.

The overall structure of the SCIP TUM system is shown in Figure 3. Performance indicators have been defined based on two basic principles: significance (importance) for course quality increasing and measurability – to be measurable quantitatively or qualitatively and documented.

Below, as an example, is presented the list of evaluation criteria in the "Course design" standard, which also includes the criteria descriptors:

- Course Description: The course overview is made clear to students at the beginning of the course,
- Analytical program: Students have easy access to the analytical curriculum,
- Learning objectives and purposes: Learning objectives and purposes describe what students can do after successful completion of the course,
- Training materials: Training materials enable students to achieve the declared learning skills.
- Course Technologies: The course technologies support student achievement of course objectives, achievement of declared competencies.

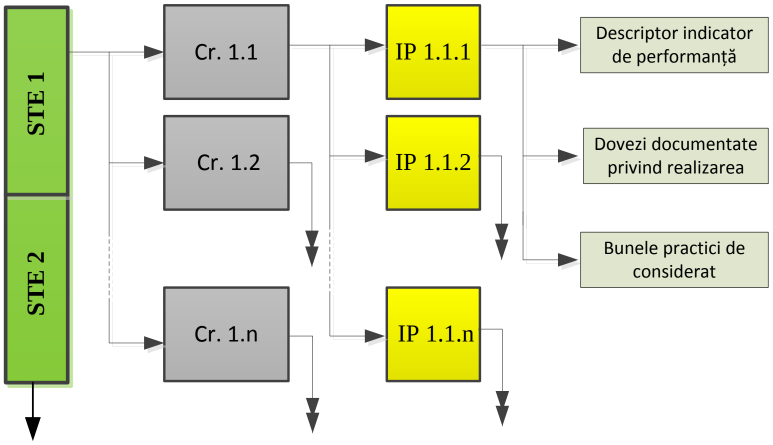

STE 1
STE 2
Cr. 1.1
Cr. 1.2
Cr. 1.n
IP 1.1.1
IP 1.1.2
IP 1.1.n
Descriptor indicator de performanță
Dovezi documentate privind realizarea
Bunele practici de considerat

Figure.3 SCIP UTM structure: ST-standard, Cr - evaluation criterion, IP - performance indicator

Each standard is accompanied by a descriptor that coincides with the description of that NAQAVE standard. Criteria and performance indicators, in turn, are accompanied by a description of the evidence of achievement, which must be presented to the assessor. An example of structure for the "Training Materials" criterion is shown in Table 1. In order to increase the utility of SCIP useful tips and good practice references for that chapter accompany each criterion.

The SCIP standards in that way were discussed and approved by the TUM Senate, after which the electronic learning platform www.http://elearning.utm.md/moodle was placed on the university's website for use as university rules.

The system was tested by evaluating a set of 14 e-learning courses developed during the 2013-2016 period and taught in the TUM electrical engineering and metrology programs, as well as selective questioning of the students enrolled in the courses as well as of the teachers from Training courses for Tutor Creators within TUM. Most of the detected inconsistencies are related to the lack or incompleteness of information for students.

4. THE QUALITY OF ONLINE COURSES IN THE STUDENTS PERCEPTION

Of the eight online quality assessment standards included in SCIP UTM, three are directly related to students: teaching / learning, course structure and student support. There are many factors that can influence students' online learning experiences. These factors can only be defined experimentally, based on a statistical analysis of the questioning of students participating in the process.

Table 1. Structure of the "training materials" evaluation criterion of SCIP TUM

Cr.2.4 Training materials: Training materials allow students to reach learning skills declared.		
2.4.1 The training materials contribute to the objectives and skills of the course. 2.4.2 Both the purpose of instructional materials and the way materials are to be used for learning activities are clearly explained. 2.4.3 Instructive materials are current and varied. 2.4.4 The distinction between obligatory and optional materials is clearly explained. 2.4.5 All the training materials used in the course are properly quoted in the university policy.	Complete course in electronic format. University policy regarding the use of third-party materials. Appropriate evidence is provided for the use of copyrighted material, as appropriate.	The course respects the University's policies for the use of third-party copyrighted material. It is the responsibility of course developers to ensure that the use of these materials follows university policy.

In order to identify students' perception of the quality of online courses, the (research) team turned to qualitative research, analyzing the views of students who participated in the online courses on Moodle's platform. In this study, 65 students enrolled in the online courses took part. Qualitative research provides an understanding of circumstances or a phenomenon that describes the situation rather than determines the cause and effect [14] [15].

The data collection was based on a questionnaire [16] distributed through the Moodle platform of the Technical University of Moldova in January – July 2017. The questionnaire contains closed questions with easy ticking. Answers to the questions were evaluated using a Likert-type scale in five points, with 5 points awarded to the rating – totally agree, 4 – agreement, 3 – indefinite, 2 – disagreement, 1 – total disagreement. Also, open questions were included, the role of these questions is to provide the possibility of improving response variants. To ensure the veracity of the answers, the questionnaire was anonymous. For this type of survey, the questions are used, short, simple. And this criterion has been met.

The questionnaire is grouped around seven major dimensions: 1. personal data, 2. educational aspects, 3. technical and ergonomic aspects, 4. graphics and multimedia, 5. the activity of the teachers / tutors in the training process, 6. the overall appreciation of the course and on-line training, 7. general online course evaluation.

To make sure that the data collection tool meets our objectives and that questions are not a source of confusion, a pre-investigation was carried out on a sample of 15 people. This has made it possible to make significant improvements in rephrasing questions, identifying words that can confuse or correcting the final questionnaire format so that it becomes a more effective tool.

The sample for this study was made up of 65 students enrolled in online learning courses. The students participated in the online survey on the Moodle platform of the Technical University of Moldova [16]. At the end, 65 questionnaires were completed. The data were analyzed to respond to research questions and cross the similarities and differences between participants.

To analyze the answers given during the study, we adapted the grounded theory method. Specifically, in this study, we proceed as follows:

- First we identify the codes by collecting the terms used by participants to describe the criteria for assessing the quality of online courses. Thus, we obtain a list of terms that include different views expressed in different ways.

- Secondly, we group similar content terms to find common concepts. Therefore, we have gathered them to create the categories – spontaneous entities proposed by participants as important for assessing the quality of online courses. For each category, the most representative view was found.

Each participant chose his current status. Finally, the following groups of participants were obtained:

students (with daily frequency studies); students (low frequency study); masters.

Thus, in the end, the following groups were obtained:

master students – 35 persons; low-frequency students – 10 people; students in the day education form – 20 persons; 46 participants also studied / completed other training courses through the UTM e-Learning platform; 19 participants did not study / have completed other training courses through UTM e-Learning platform.

The results of the categorization and finding the criteria for evaluating the quality of the online courses in the perception of the students

The sample the data were collected in a table whose lines make up the status of the participant and whose columns are the answers to the questions in the questionnaire.

Answers to questions were analyzed using the Correspondence Analysis method that describes the relationship between two categories variables and the relationships between their categories (association relationships).

Correspondence Analysis (CA) is based on contingency table analysis through row and column profiles [17]. The line profiles correspond to the relative frequencies of the different criteria mentioned by each group of participants with different status.

Dimensions are graphically represented to visualize relationships between variables. The CA results were generated using the following code in the RStudio program [18]:

```
data <- read.table("C:/Users/user/Desktop/Sondaj_UTM.txt ", header=TRUE,sep="\t",
na.strings="NA", dec=",", strip.white=TRUE)
summary(data)
library(FactoMineR)
res = textual (data,num.text=4,contingence.by=1)
res$nb.words
descfreq(res$cont.table,proba=0.2)
res = CA(res$cont.table)
plot.CA(res,invisible="col")
```

After the correspondence analysis a geometric visual representation (perceptual map) of the complex relation between the categorical variables occurred, in which the categories with similar distributions occupy close positions, and the categories with different distributions are placed in distant positions.

Below are the results of the Correspondence Analysis (CA) and the observations for each question in the survey:

Question 1: “What I appreciate most of this course”

Masters have appreciated the structure of the online course, accessibility of information, useful information, online evaluation of the possibility of working at distance and the knowledge obtained at the end of the course.

Students with low-frequency studies appreciated the most useful information, teacher activity and the convenience of working at a distance. According to the graphical representation in figure 1, convenience was highly appreciated by this group of students, less by master students and with students daily frequency.

Students with full-time studies have appreciated the teacher, teaching, course content and accessibility of information.

Question 2: “What I dislike in this course”

According to the statistical analysis made by the master students they dislike the platform interface, the large amount of information, a little interactivity, the feeling of isolation.

Students with low-frequency studies deprive the platform interface and repeat recording errors

Most students with daily frequency do not dislike anything but a very small number mentioned that there are few practical lessons.

Question 3: "What were the main technical difficulties that I faced"

Among the main technical difficulties, the master students mentioned the low speed of navigation, the platform sometimes did not work. For students with distance learning it was difficult to create a new account after losing their password, the platform did not work sometimes, the low speed of navigation. Full-time learning students have encountered difficulties uploading high volume files, and they also mentioned that the platform did not work sometimes.

Question 4: "Proposals to improve the course from a technical point of view"

Most Masters have proposed increasing navigation speed and a more attractive interface to the site.

Students with low frequency have the same proposals. While students with daily frequency are proposing to improve the method of uploading high volume files and a more attractive interface to the site.

Question 5: "Objections / proposals to teachers / tutors in the online training process"

The Master's objections are delayed feedback from the teacher and little interaction in the online environment. They would like to have more online communication between course participants and teachers.

Graduate students need more practical lessons, online communication, and teacher feedback.

Students with daily frequency point out that their online course teacher is excellent and would like more online interaction.

When asked if distance learning provides better assimilation of knowledge, 78% master students confirmed the fact, and 22% denied it. The same answers are also found in low-frequency students. 75% of students with daily frequency responded affirmatively.

General course evaluation

Students with daily frequency appreciated the on-line course they graduated with a maximum mark of 10, most of the masters rated 9 and a large proportion of low-frequency students rated it with a grade 8 (Figure 6). The lowest appreciation was the grade 7 that was given by a very small number of survey participants.

The results obtained were examined, then grouped into two major areas. These areas have been positive experiences and negative experiences with online education.

Positive experiences included: easy access to information, online assessment methods, the convenience of learning distance. Negative experiences included: platform interface, high volume of information, low navigation speed, heavy upload of high volume files, delayed instructor feedback, technical support unavailable from the instructor, and a sense of isolation.

The factors that attributed to the positive experiences of the participants were: easy access to computers and the Internet, structure of well-designed course, spontaneous records after evaluations and flexible time for online courses. The factors that attributed to the negative experiences of the participants were: insufficient time to assimilate information or lack of feedback from the instructor; Monotonous training methods, lack of technical support, lack of interpersonal communication, and poorly designed course interface.

The data collection and analysis provided answers to the following research questions: (1) What is the experience of students receiving online education? (2) How do students perceive the quality of online courses in their experiences? (3) What factors have formed the students' online education? (4) How do these factors contribute to the quality of online education?

5. CONCLUSIONS AND RECOMMENDATIONS

1. Online education is an important component in the continuous growth / development of higher education and adult learning.

2. The quality of online courses is determined by a number of specific factors, such as the presence of multiple student teaching materials, solved problems with detailed explanations, individual papers with clear indications on how to present, self-evaluation activities, to get advice, help, and consultation in synchronous and asynchronous terms from the tutor or teacher.

3. A system with 8 standards, 19 criteria and 46 performance indicators was developed for the evaluation and design of e-learning courses in the frame of distance learning, law-frequency or blended learning programs. The developed system of standards meets the SEG, EURO-ACE as well as specific quality requirements specified in p.2

4. The system was tested by evaluating a set of 14 e-learning courses developed and taught in TUM's electrical engineering and metrology programs as well as selective questioning of students enrolled in courses and of teachers from training courses of course makers at TUM.

5. The result of questioning a sample of 65 students from different categories (students with low-frequency studies, students with daily frequency, masters) found that students would want more online communication and feedback from the teacher. Many respondents also mentioned the amount of information on the course, and it is recommended to review the information in online courses. However, this does not mean that the platform administrator should be reserved to ensure the quality of online education. More importantly, the Administrator must provide enough support for participants, improve platform layout, and provide permanent access to the Moodle platform. The findings of this study will allow institutions offering online courses to evaluate their programs and to provide an effective online teaching.

REFERENCES

1. Standards and Guidelines for Quality Assurance in the European Higher Education Area (ESG). (2015). Brussels, Belgium.
2. EUR-ACE. Framework Standards and Guidelines (ENAEE). 2015. www.enaee.eu

3. Ghid de evaluare externă a programelor de studii de licență. Învățământ superior. ANACIP. 2016 Tipogr. “Bons Offices”. – 52p. ISBN 978 9975-67-124-2.
4. ARACIS. Ghid Evaluare Externa, partea a ***v-a*** - evaluarea externă a programelor de studii oferite prin învățământ la distanță. http://www.aracis.ro/fileadmin/ARACIS/Legislatie_-_Proceduri/Partea_a_V-a.
5. Hansso Henrik, Johansson M., Westman P., Åström E. E -learning quality. Aspects and criteria for evaluation of e-learning in higher education. Published by the Swedish National Agency for Higher Education 2008. https://www.researchgate.net/publication/270158432.
6. Blieck Yves, Ooghe Ilse, Chang Zhu, Koen De Pryck, Hilde Van Laer. Framework for quality assurance and improvement in Adult education for online and blended learning: a Qualitative study – preliminary results. *Proceedings of ICERI2015 Conference 16th-18th November 2015, Seville, Spain. -pp. 6401-6411. ISBN: 978-84-608-2657-6*
7. Penn State Quality Assurance e-Learning Design Standards. https://weblearning.psu.edu/resources/penn-state-online-resources/qualityassurance/
8. Stamenka Uvalić-Trumbić, John Daniel. A Guide to Quality in Online Learning. Academic Partnerships. 2013. http://www.chea.org/userfiles/uploads/A%20Guide%20to%20Quality%20in%20Online%20Learning.pdf
9. Non-annotated Standards from the QM Higher Education Rubric, Fifth Edition. Ed.: Quality Matters Rubric. 2014. www.qualitymatters.org.
10. Practice Standards for Online Learning at Griffith University. 2015. https://www.griffith.edu.au/__data/assets/pdf_file/0005/773033/Practice-Standards-for-Online-Learning_v.3-_approved-by-L-and-T-Committee_2.pdf.
11. The NADEOSA Quality Criteria for Distance Education in South Africa. http://www.saide.org.za/resources/Reports/NADEOSA%20QC%20Section%202.pdf
12. Regulamentul – cadru privind organizarea și desfășurarea învățământului superior la distanță.Aprobat prin ordinul ME nr. 474 din 24.05.2016. http://www.edu.gov.md/sites/default/files/ordin_474_din_24.05.2016.pdf
13. Todos P., Ghencea C. Ghid de bune practici: *Elaborarea și evaluarea cursurilor online . UTM, 2014. -33p.*
14. Fraenkel J.R. and N.E. Wallen. How to design and evaluate research in education. 2003: McGraw-Hill Higher Education.
15. Glesne C., Becoming qualitative researchers: An introduction. 2015: Pearson.
16. Chestionar de evaluare a cursului online. Available from: http://elearning.utm.md/moodle/mod/questionnaire/view.php?id=29387.
17. Glaser B. and Strauss A. The discovery of grounded theory: strategies for qualitative research Aldine Publishing Company. New York, 1967.
18. Husson F.O., Lê S.B., and Pagès J.R.M. Analyse de données avec R. 2016.

3. INFORMATION and CYBER SECURITY

The General Aspects of the Information Technical Protection

Rusnac Andrei
Information security expert, Republic of Moldova
E-mail: rusnacandrei79@gmail.com

ABSTRACT

The article describes the general aspects of attack with technical methods against information and communication systems, information, as well as against information infrastructure facilities.

Keywords: *information, security, technical, protection, attack, weapons, critical, infrastructure.*

1. THE TECHNICAL ATTACK

The technical attack – is an action directed by using technical and / or program means on the objects, carried out in order to affect the integrity, availability and / or confidentiality of the information systems, by using electromagnetic induction principles and technical channels (electromagnetic, audio and visual) critical infrastructure facilities and electronic communications to ensure their interaction as well as information that is stored, processed, or transmitted.

2. THE TECHNICAL INFORMATION LEAKAGE CHANNELS

2.1 The channels

Along with technical facilities and information processing systems, as a rule, other technical facilities and systems are located in the premises where they are installed. These include:

1) systems and means of urban telecommunications;
2) systems and means of data transmission in a radio communication system;
3) systems and means of security and fire alarm;
4) warning and signaling systems and means;
5) control and measuring equipment;
6) systems and air conditioning;
7) systems and means of a wired radio network and the reception of radio and television programs;
8) means of electronic office equipment.

Natural information leakage channels are formed due to spurious electromagnetic emissions arising during the information processing (electromagnetic information leakage channels), as well as due to induction of informative signals in power and connecting lines, foreign conductors (electrical leakage channels).

Special information leakage channels include channels created by the introduction of electronic devices for information interception and by "high-frequency irradiation".

2.2 The electromagnetic information leakage channels

In electromagnetic information leakage channels, the carrier of information is the electromagnetic radiation that occurs when information is processing by technical means. The main reasons of appearance of electromagnetic leakage channels are:

1) secondary electromagnetic radiation;
2) modulation by an informative signal of spurious electromagnetic emissions of high-frequency generators of technical means;
3) modulation by an informative signal of parasitic electromagnetic radiation of technical means.

Secondary electromagnetic radiation of technical means is an undesirable radio emission that results from nonlinear processes in technical equipment blocks with the following information processing modes:

1) the output of information to the monitor screen;
2) the input of data from the keyboard;
3) writing of the information to the media devices;
4) reading of the information from the media devices;
5) the data transmission to communication channels;
6) the data output to peripheral devices.

This channel is most widely used for listening to telephone conversations, conducted by radiotelephones, cellular phones or by radio relay and satellite communication lines.

2.3 The electrical information leakage channels

The electrical channel for interception of information transmitted by cable communication lines implies the contact connection of the interception equipment to the cable communication lines.

The easiest way is the direct connection to the line in parallel. However, this fact is easily detected, because it leads to a change in the characteristics of the communication line due to voltage drop. Therefore, the interception means are connected to the communication line or through a matching device that slightly reduces the voltage drop, or through a special voltage drop compensation device.

The contact method is used mainly to remove information from coaxial and low-frequency communication cables. For cables in which high air pressure is maintained, devices that exclude its reduction are used, as a result of which a special alarm is prevented.

The electrical channel is more often used to intercept telephone conversations.

2.4 The induction information leakage channels

In the induction channel, which does not require a contact connection, the effect of the appearance is used around an electromagnetic field of the communication cable when electric signals are transmitted through it, which are intercepted by special induction sensors.

Modern induction sensors are capable to register information from cables protected not only by insulation, but also by double armor made of steel tape and steel wire tightly wrapping the cable.

Some means of contactless information retrieval can be combined with radio transmitters to transfer it to the interception control point.

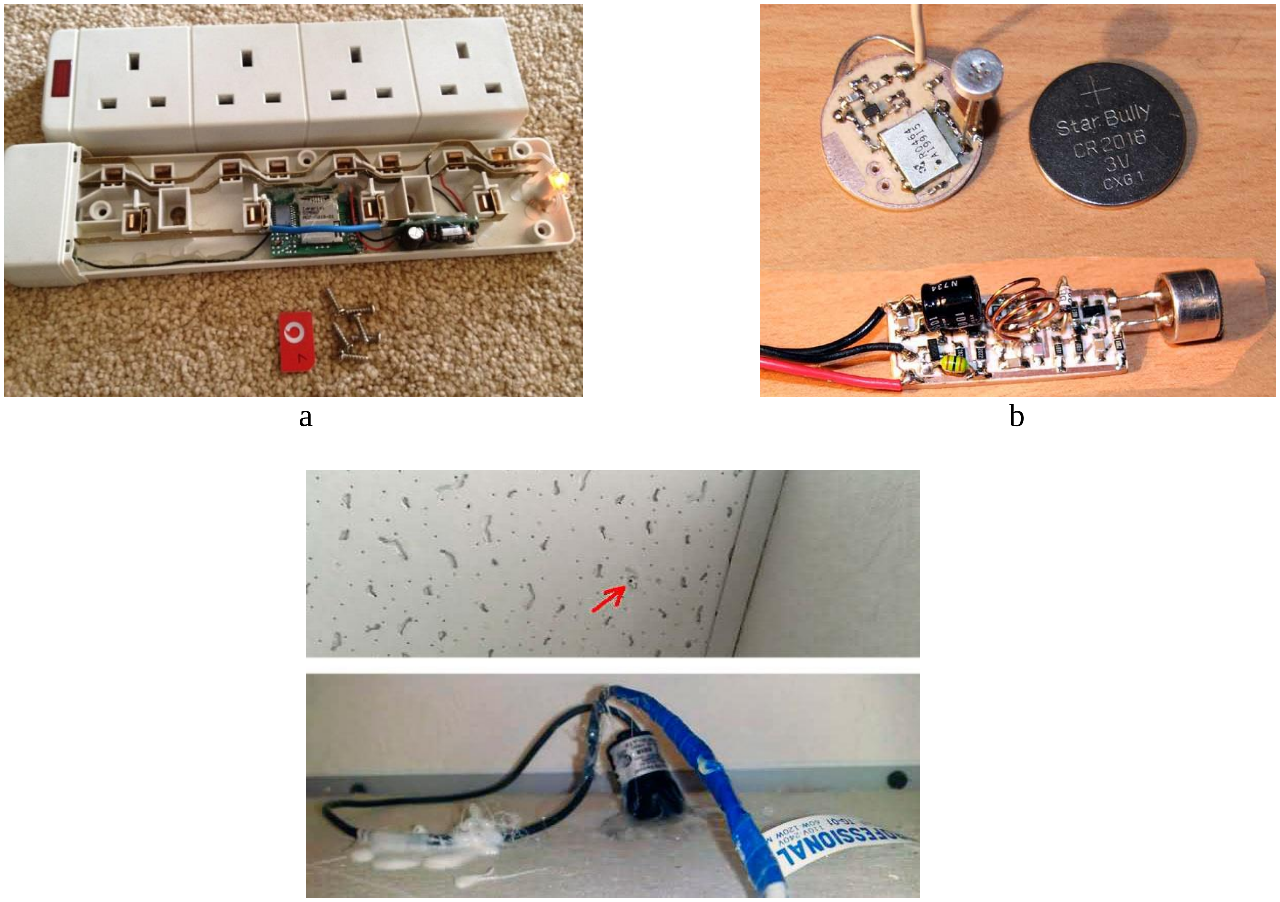
2.5 The specially created information leakage technical channels

Along with passive methods of information interception, it is possible to use also active methods, in particular, the method of "high-frequency irradiation".

To intercept information, it is also possible to use electronic interception devices that are hidden introduced into technical facilities and systems.

The intercepted information is direct transmitted by the communication channel to the receiving point, or it is recorded in a special storage device and transmitted only by the control command.

To transmit information to the receiver the radio station, the optical (infrared) channel or the lines of the transmitter can be used.



a

b

c

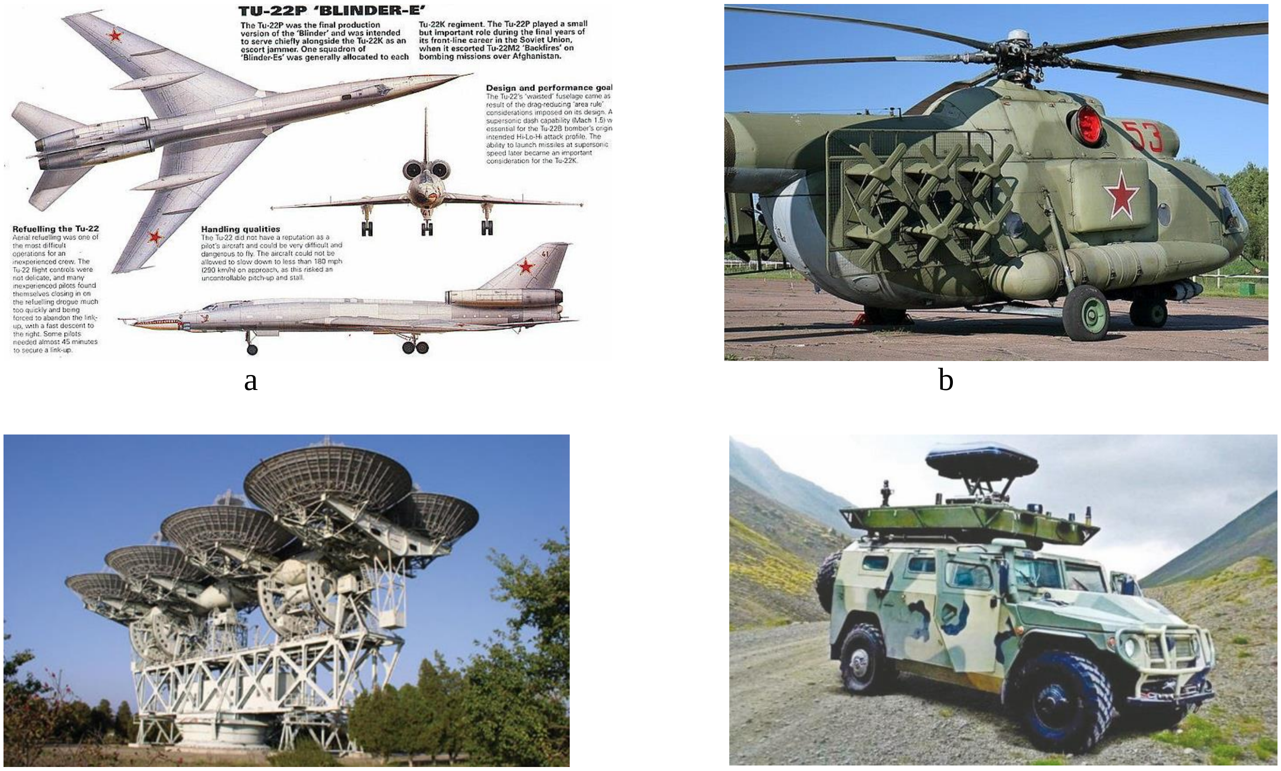
Figure 1. Examples of specially created information leakage technical channels

3. THE TECHNICAL ATTACK AS A WEAPON

The task of the radio electronic warfare is the disorganization of the radio-electronic equipment resulted by exposure to electromagnetic radiation. In the modern warfare, such means of participation can have a huge impact on the course of military warfare. In the main, radiobroadcasts are used for broadcasting radio means of the enemy, such as radiobroadcasting, radiobroadcasting and anti-aircraft defense.

The radio stations are active and passive. Activation - the extraction of a special device, such as special devices, and the recording of reflections in the radio broadcasting means of a different subject.

Active interference is the electromagnetic radiation created by special devices and passive interference is created by reflecting the signals of radio electronic means of different objects. Active interference is divided into noise masking, and imitation. The imitation interference is intended for the creation of false purposes for the radar stations or the distortion information about the aim. For this, the electronic warfare station receives the radar signal and reflects it with the changed characteristics (power, phase, frequency, etc.). This leads to the fact that one or more false marks appear on the radar screen with the changed parameters of range, altitude, heading, etc. Therefore, if you "issue" a large series of impulses, this will lead to the fact that on the screen of radar stations these false marks merge into one large line that completely "smears" the real mark.



TU-22P 'BLINDER-E'

The Tu-22P was the final production version of the 'Blinder' and was intended to serve chiefly alongside the Tu-22K as an escort jammer. One squadron of 'Blinder-Es' was generally allocated to each Tu-22K regiment. The Tu-22P played a small but important role during the final years of its front-line career in the Soviet Union, when it escorted Tu-22M2 'Backfires' on bombing missions over Afghanistan.

Design and performance goal

The Tu-22's 'waisted' fuselage came as result of the drag-reducing 'area rule' considerations imposed on its design. A supersonic dash capability (Mach 1.5) w essential for the Tu-22B bomber's origin intended Hi-Lo-Hi attack profile. The ability to launch missiles at supersonic speed later became an important consideration for the Tu-22K.

Refuelling the Tu-22

Aerial refuelling was one of the most difficult operations for an inexperienced crew. The Tu-22 flight controls were not delicate, and many inexperienced pilots found themselves closing in on the refuelling drogue much too quickly and being forced to abandon the link-up, with a fast descent to the right. Some pilots needed almost 45 minutes to secure a link-up.

Handling qualities

The Tu-22 did not have a reputation as a pilot's aircraft and could be very difficult and dangerous to fly. The aircraft could not be allowed to slow down to less than 180 mph (290 km/h) on approach, as this risked an uncontrollable pitch-up and stall.

a

b

c

d

Figure 2. Examples of military electromagnetic radiation systems.

4. THE TECHNICAL PROTECTION

Technical protection of the critical infrastructure facilities is any activity that aims to ensure the functionality, continuity and integrity of the critical infrastructure, to neutralize a threat or risk. This protection includes the sequential activities on risk assessment and analysis, ensuring the security of objects. Technical protection is aimed at securing information by providing technical measures, preventing leakage, destroying and blocking information, affecting integrity and access to information. The purpose of ensuring the technical security of critical infrastructure is its stable, secure and continuous functionality.

The security system ensures:

1) the prevention of unauthorized access, destruction, modification, blocking, copying, providing, disseminating of the information, and committing of other illegal acts;
2) the prevention of the impact on the technical means of information processing, which could disrupt or block the functionality of the critical infrastructure;
3) the responsibility for security incidents;
4) the possibility of immediate recovery of the integrity and functioning of the critical infrastructure facilities;
5) the reservation of technological data and processes.

5. CONCLUSION

Successful technical attack causes the critical infrastructure object to be broken or shut down. The disruption and / or cessation of the operation of a critical infrastructure object of a system located on the territory of the Republic of Moldova, which is essential for maintaining the vital functions of the society, health, safety, social or economic welfare of individuals, would have a significant impact at national level and will lead to the state's inability to maintain government, defense, security and law enforcement functions.

In connection with the entry of humanity in the era of globalization, the introduction of new science-intensive technologies and total informatization of all fields of activity, the scope and extent of the negative impact of technical threats and attacks on the state of international and national security will increase. However, this problem does not have an exceptionally technical solution.

REFERENCES

1. Antiterror equipment: catalog. - Germany: PKI Electronic Intelligence, 2008. - 116p.: http://www.pki-electronic.com;
2. Computer Keyboard Monitoring: product range. - Italy, Torino, B.E.A. S.R.L., 2007. -P. 35-37;
3. Key Devil Keylogger.: http://www.keydevil.com/secure-purchase.html;
4. Kuhn Markus G. Compromising emanations: eavesdropping risks of computer displays.: http://www.cl.cam.ac.uk/techreports/UCAM-CL-TR-577.html;
5. Security and surveillance products.: http://endoacustica.com;
6. Wireless controlled keylogger.: http://www.keyear.com;

Problem of the Boundaries Determining in the Information Space

Pilyugin Pavel

Moscow Technical University of Communications and Informatics
8A, Aviamotornaya Str., Moscow, 111024, Russian Federation
E-mail: paul.pilyugin@gmail.com.

ABSTRACT

The article deals with the problem of defining areas of cyberspace where the state has the right to apply various methods of protection. The "digital border" is a key concept for ensuring "digital sovereignty". The "digital border" is also a necessary condition for ensuring "digital sovereignty".

Different definitions of the "digital boundary" are considered in the article. For each type of "digital boundaries", the reasons for their occurrence, the technical and technological methods for their construction, and the effectiveness for ensuring "digital sovereignty" are described.

Providing "digital sovereignty" involves using of authentication, authorization and audition. All these functions are used differently for various types of "digital" boundaries. A model of a distributed multi-level digital boundary is proposed. This model supposes the control of information flows at all levels of cyberspace. Technical and economic constraints are proposed to be solved through the distribution of information flow control functions over the network.

Technological basis of such digital boundary can be made by software-defined networks, which allow to concentrate all tasks of analysis and network management in one center. Moreover, information collected in that center can be used during investigations of various incidents if they fall within the sphere of state responsibility.

Keywords: digital, sovereignty, border, autonomous, system, distributed, multi-level, boundary

1. CYBERSPACE AND NATIONAL SECURITY

The solution to the problems of international information security should not only ensure the harmonization of national legislation and international rules, but to comply with the national interests, to agree on the rules of engagement States [1]. Recently, in international information security, there has been significant progress and commitment to responsible behavior of States in cyberspace [2]. However, still remain unresolved a number of issues related to the definition of areas of responsibility and authority of different States in cyberspace [3].

The unavailability of regulators and fiscal authorities control over economic activities in cyberspace, international cybercrime, identifying the initiators of the cyberattacks and state responsibility – all this is connected with the concepts of "cross border traffic", sovereignty and borders in cyberspace[4].

Thus, involvement in the information space of an increasing number of States it is necessary to divide their areas of responsibility and determine the possibility of use of protection mechanisms to ensure national and international information security. The tasks of the state in this case is to identify the source of the threat (his or someone else's area of responsibility) and protection from these threats.

2. THE DEFINITION OF CYBERSPACE BORDERS

We need to identify cyberspace area in which state can apply its legislation.. There are different approaches to determining the boundaries in the information space.[5].

2.1. BR - Border of Reality.

"Cyberspace is another place" – this approach is based on the assumption that the technical and technological basis of the information space – cyberspace "radically subverts a system of rule making based on borders between physical spaces", that is denying the claim that cyberspace should naturally be governed by territorially defined rules[6]. Thus, the boundary passes through different terminal devices: computers, smartphones, etc. – the device interaction with the real world. Then everything that happens in cyberspace is not governed by national legislation, therefore the state controls only a terminal device.

Control terminal devices is technically possible, moreover, today almost every device (computer or smartphone) automatically updates its software and reports its status to the centre, that is, they can become managed elements of the "digital border". Often the authentication to access the network via public Wi-Fi access point is implemented through sending SMS. It is also a mechanism of control terminal devices and the element digital boundaries.

You can also implement different methods of access control and logging. However, in this case the costs of global control comparable to the cost of creating and maintaining the Internet.

2.2. PB – Physical border.

Another approach is to attempt to establish control over electronic communications in the place of crossing physical boundaries. When people criticize this approach, talking about various ways to bypass such controls in China [7]. This is true, as no border is not absolute – there will always be loopholes and enthusiasts to use them.

However, the "Convention on cybercrime," linking state responsibility with the territory [2], and the means of such control in fact it is widely firewall, which is considered an indispensable tool to ensure network security. The Chinese experience of development and using "the Great Firewall of China", showed the effectiveness (socialnoy efficiency) this protection mechanism[7]. However, a simple copy of the experience require a considerable investment of resources in the reorganization of computer networks and in the development of the industry of production of national content.

RB and PB are based on the management of the real objects of the physical world. Technical means and communication lines on the territory of the state subject to control. We can assume that the combination of these two approaches will effectively control traffic (to determine where and where the information is sent). It is also possible to determine the origin (recipient) of this information within a state-controlled zone.

2.3. VB - virtual border.

The task of identifying the source of traffic inside or outside the controlled zone, or determining which country should do this, was proposed to address the responsibility of countries for the IP address groups of the providers of these countries (geographical routing).

This approach, in fact, draws a boundary in the IP address space. Groups of such addresses are allocated to providers (sometimes transnational ones) that manage them independently. Because of the limited address space (sometimes for reasons of convenience and economy), providers use address translation techniques-in this case, the "device-network address" relationship exists only during network interaction.

Despite the simplicity and attractiveness, this approach has a number of difficulties. These difficulties can be overcome by moving to a new IPv6 protocol and geographic allocation of addresses. It is also necessary to protect IP addresses from forgery.

3. THE BORDERS OF AUTONOMUS SYSTEMS.

3.1. Autonomous systems.

Initially the Internet was created as a Federation of networks, therefore, the principles of the Federal structure and the concept of borders inherent in it initially. The Internet as a Federation of networks consists of Autonomous systems (AS). Under the Autonomous system isre understood as large network of provider or group of providers using a network management common policy. Each Autonomous system has its own identification number. Legal entity (group of entities) that form a Autonomous system, has a territorial identity and falls under the jurisdiction of a particular state.

All this logically leads to the possibility of defining boundaries on autonomous systems, which is the development of the approach of the division of spheres in the space of IP-addresses. This allows us to eliminate a number of emerging uncertainties and makes the division of cyberspace into areas of responsibility "tied" to the territorial borders of the state.

3.2. Border Gateway Protocol.

The interaction between the AS is based on the Border Gateway Protocol (BGP). All the configured BGP policy in relation to the external/neighboring Autonomous systems, that is, describes the rules of interaction with them. So providers, exchanging traffic, in fact, conclude with each other (peering) agreements that provide the physical connection of their networks and technical cooperation – exchange of routing information. The routing information is a list of AS, and each AS spreading this list, may add information about the preference for routes traffic.

Violations in routing information can lead to the inaccessibility of entire network segments, "leakage" or "hacking" traffic (https://bgpstream.com/ or https://bgpmon.net/).

There are cases when large amounts of traffic go to distant regions. For example, in Russia there were cases of internal routing through China Telecom in Frankfurt. A similar situation in US occurred when large amounts of internal traffic were sent through Chinese, Belarusian or Icelandic providers. Each state can control internal traffic and formulate its policy on cross-border exchange. In this case, the "digital border" will be tied to stand-alone systems. You can represent the boundary not as a line, but as a point or set of points of connections (contact) between different autonomous systems of different states (Figure 1).

Typically the points of such cross-border transport are Internet Exchange Points (IXPs). It is important to note that AS can control traffic according to different characteristics, and therefore cross-border exchange can be monitored AS, even if they are not points of cross-border transition.

3.3. Development of Border Gateway Protocol.

The current version of the BGP-4 protocol was created more than 20 years ago. Today, the Internet Engineering Task Force (IETF) is developing a new, more secure version of the protocol. There are two main modifications (https://www.ietf.org/archive/id/draft-ymbk-idr-bgp-open-policy-03.txt). The first modification is related to the expansion of the set of AS roles and their attributes, which allows to identify the "leakage" of routes as a result of errors. The second modification is aimed at expanding the concept of "confederation of AS". Such a confederation allows the implementation of a unified policy of the Union of the AU. This allows us to consider the unified policy of the state and its digital border.

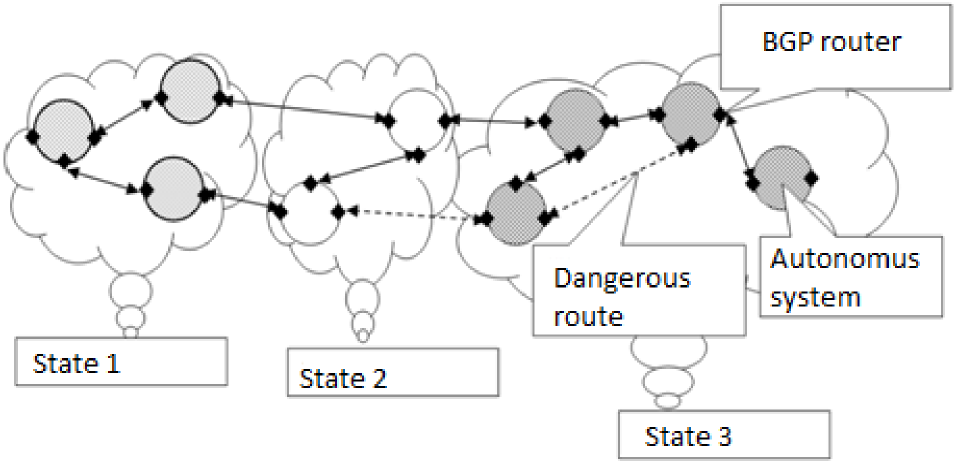


Figure 1. Diagram of the digital border.

4. DISTRIBUTED DIGITAL BOUNDARY.

4.1. Technological and organizational contradictions.

At the technological level controls cross-border traffic is similar to traffic control with firewall that solve the problem of protection against various external attacks. Controls cross-border traffic should ensure control not only incoming but also outgoing traffic (e.g. preventing hacker attacks from the state-controlled sphere of cyberspace). However, a deep analysis of the traffic increases the computational complexity, which is contrary to the requirements of high performance for cross-border transitions.

Another important property of the control of information flows should be realized when we transform the "line of defense" into a "digital boundary". In addition, that the control of information flows must be bi-directional, it should enable the investigation of identified incidents. Investigations require information about the source of the attack and the fact of a cross-border crossing. The registration of the facts of cross-border traffic should be "transparent" for all parties involved in the investigation. The registration of incoming traffic is important for making claims to the adverse party, and registration of outgoing traffic is necessary to confirm the justification of the claims. Here there is one more contradiction - to register the source more simply at the place of its connection, but this registration is less "transparent", since it can be quite "far" from the point of trans-boundary transition.

4.2. The elimination of technological and institutional contradictions.

Controversies resolutions are possible in a distributed control system and with a single routing policy.

The requirement for significant computational resources for the tasks of traffic control is contrary to the requirements of high throughput at the traffic exchange cross-border points. In this case it is advantageous in the traffic exchange cross-border points to place a simple traffic filtering means. For more resource-intensive monitoring tools, you can use other less-loaded network nodes through which traffic flows.

For nodes far from the digital border reducing the "transparency" controls can be resolved by distribution of the registration function, maintaining the chain connectivity of the registration information.

The distribution of control functions for autonomous systems allows you to distribute costs to all participants of the telecommunications market, since they should not be excessive for them.

4.3. SDN as the technological basis of the digital boundary.

Today Route Server (RS) is used to provide routing, the main function of which is storing routes and sending all BGP announcements of peers connected to it. There are more than 50,000 autonomous systems and 300 IXPs in the world. Their bandwidth is more than 5 petabytes / sec, and the total number of routes is more than 500,000 [8]. All this complicates the tasks of managing and configuring networks. Overcoming these difficulties is possible with the transition to the technology of software-defined networks (SDN) [9]. SDN is not only the next level of abstraction of the network description. SDN allows you to concentrate all tasks of network management (group of networks) in one center - the controller (or a group of controllers) of the network.

This ideology can be used for a local area network, a corporate network, an Autonomous system or group of Autonomous systems. General routing policy, more precise traffic control and a single management center significantly expands the possibilities of building a digital border..

First, networks built using this technology actually have a firewall distributed over the network, managed from a single center. This is what can allow implementing filtering functions for all national fragments of the SDN network, based on a unified security policy.

Second, the SDN switches by sending routing information to the controller to allow it to analyze information flows and to identify possible violations of security policy.

And finally, thirdly, because SDN allows you to manage the routing, filtering and traffic control almost at all technological levels, the use of this method in the traffic exchange points will significantly increase their capabilities. Such Internet exchange point (IXP) using SDN, called software-defined exchange points (SDX) [8].

Indeed, SDX does not just distribute RS information, but it allows you to more accurately and flexibly configure traffic exchange, without requiring classical BGP tricks. In fact, the SDX controller acts as a compiler for translating the policies of different autonomous systems into routing rules for the network switch. Therefore, there is a potential opportunity to efficiently exchange traffic between the AS and manage routing.

5. CONCLUSION

The above approaches to the definition of the digital boundary and the methods for implementing these approaches determine the scope of state control over a part of the information space. However, the "digital border" thus established must be recognized by other countries. And although the states within the group of government experts at the UN recognized the need for "responsible behavior in cyberspace," but the process of adapting and improving international law may not be easy, as different states pursue their own interests first of all [1,2].

It seems that the approaches described above to the definition of boundaries in the information space can become a subject of discussion for the development of international law. And their implementation in practice can determine the "digital border" of the state "de facto". However, the introduction of any restrictive measures must be carefully weighed and thought out, taking into account political, social and economic consequences.

REFERENCES

1. Convention on cybercrime (Budapest, 23.XI.2001) https://rm.coe.int/1680081580

2. Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security. 22 July 2015. A/70/174

3. Pilyugin P.L., Salnikov A.A. Prospects of application of international legal norms in cyberspace. Ninth International Forum«Partnership of State Authorities, Civil Society and the Business Community in Ensuring International Information Security» and Eleventh Scientific Conference of the International Information Security Research Consortium April 20–23, 2015. Garmisch-Partenkirchen, Munich, Germany, 2015.
M.: Moscow University press, 2015. -pp.20 -140

4. Streltsov A.A., Pilyugin P.L. About digital sovereignty. “Informatization and communication” – 2016. – №2. – pp.25-30

5. Kasenova M.B. Problemy pravovogo regulirovaniya transgranichnogo ispol'zovaniya interneta. Moscow. MGIMO University 2015. – 429p.

6. Johnson D.R., Post D.G. «Law and Borders – the Rise of Law in Cyberspace», Stanford Law Review, № 48, 1996. https://cyber.harvard.edu/is02/readings/johnson-post.html

7. Marczak B., Weaver N., Dalek J. at all. “China’s Great Cannon.” http://citizenlab.org/2015/04/chinas-great-cannon/

8. Conran M. SDX: Software Defined Internet Exchange. 02.feb.2016. «Network, Security, and Cloud» http://network-insight.net/2016/02/sdx-software-defined-internet-exchange/

Modern Security Issues in Software-Defined Networking

[1]Smeliansky Ruslan, [2]Pilyugin Pavel

[1]Lomonosov Moscow State University
GSP-1, 1-52, Leninskiye Gory, Moscow, 119991, Russian Federation
E-mail: cmc@cs.msu.su

[2]Moscow Technical University of Communications and Informatics
8A, Aviamotornaya Str., Moscow, 111024, Russian Federation
E-mail: paul.pilyugin@gmail.com

ABSTRACT

This paper discusses the problems of information security definition - software-defined networking (SDN). Although the separation of control plane and data plane levels relieves a number of network security threats but they also change the capabilities of existing protection methods and new threats emerge in relation to a control loop. There are two main groups of tasks: the first is to provide data security in the SDN networking (data plane) and the second is due to the need to protect the control circuit (control plane). Moreover, the information security implementation affects the SDN-based development of virtualized network services (NFV).

Keywords: software, defined, networking, data, plane, security, control, virtual, functions, firewall.

1. SDN SECURITY

As the most obvious successor to the traditional network architecture with combined control and data planes, the Software Defined Network (SDN) is considered with the possibility of logically centralized control. Further growth of cloud services, increased requirements for bandwidth, the complexity of network scaling and vendor dependency has led to a stable global trend - the development of SDN technologies. In fact, this is a method of administering computer networks that allows you to manage network services when the control plane is separated from the underlying data plane. According to the SDN concept, all control logic is transferred to controllers that are able to monitor the operation of the entire network and manage network switches. Planning of the network and traffic management at the same time occurs programmatically through the introduction of new applications. These applications can perform a variety of functions in the interests of business tasks (for example, control access, manage bandwidth, etc.). Thus, the network becomes "programmable", created from available resources for specific applications and more open [1].

That is why in the developed telecommunications markets they put first fundamentally new opportunities that give operators SDN and NFV technologies (virtualization of network element functions). Among the most famous foreign practitioners are Google, Amazon, Verizon, PayPal, Telefonica, Ebay, Telecom Italy, AT & T, NTT, TW telecom, SK Telecom. According to VMware, today in Europe more than 30 pilot implementations of NFV have been successfully carried out. For example, the initiative of the largest

European operator Telefonica called Unica implies the virtualization of 30% of the functions of all new network equipment Telefonica.

Despite the fact that SDN ideology is now moving from the research stage to the industrial implementation stage, the SDN security objectives continue to be actively studied and developed (in accordance with Gardner forecast 2015 \ 2016 curve) [2].

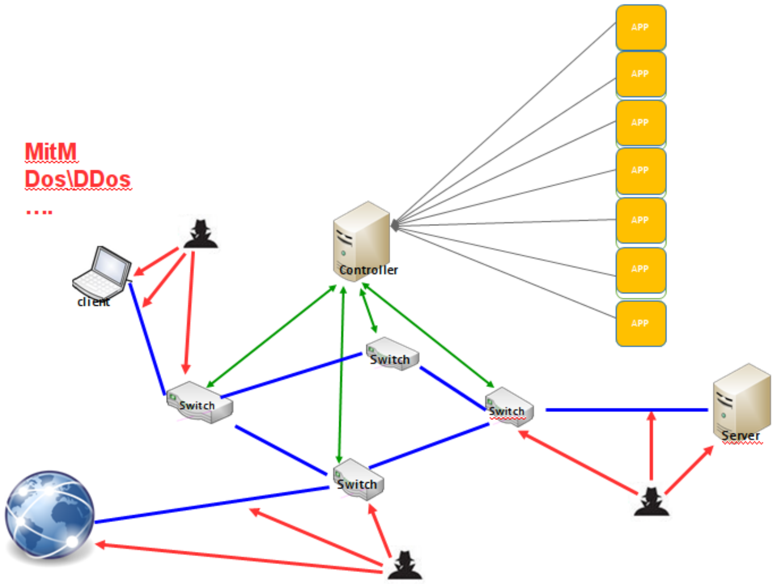


Figure 1. Threats to the data plane.

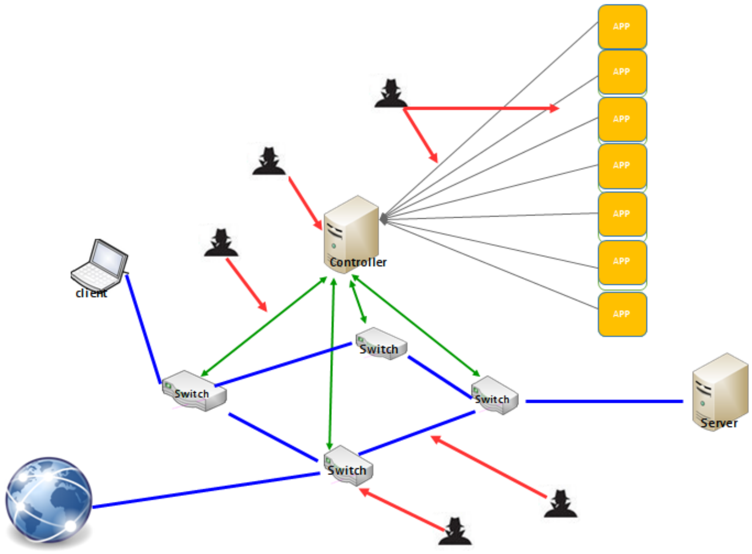


Figure 2. Threats to the control plane.

And while the separation of management layers and the data layer removes a number of threats to network security, the capabilities of existing protection methods change and new threats arise regarding the control loop.

Two main groups of solved problems can be distinguished: the first is connected with
ensuring the operability of networks and the security of data in them (data plane, Figure 1)), and the
second is caused by the need to protect the control circuit SDN (control plane, Figure 2) [3,4].

2. DATA PLANE SECURITY

To ensure the security in the data plane (confidentiality, integrity and availability of data transmitted in the data networks) a whole arsenal of various security mechanisms has already been created.

These mechanisms are aimed at countering threats on the communication line, communication equipment and network nodes (VLAN, firewall, VPN, IDS, IPS, etc).

SDN with OpenFlow control protocol has a number of properties that are well suited for building a secure and managed computing environment:

- The flow paradigm (and not the packet paradigm) is not associated with traditional routing restrictions.
- Centralized management is more effective for protection and monitoring.
- Granular management of security policy can be based on tasks being solved, used services, organizational and geographical criteria, and not on physical configuration.
- A flexible security policy, focused on resources: from a complex firewall to simple access devices.
- The transition to control via programming provides flexible control.
  The transition to SDN allows you to transfer to the control loop a number of functions currently performed by individual specialized devices. For example, the use of switches to delineate access according to IEEE 802.1x in the SDN has maximum flexibility as the ascription to a particular virtual subnet can be based on the L1-L4 layer headers, that is not available to conventional switches.

a. Firewall capabilities in SDN
   The main task of the firewall is to filter traffic passing through it. The basis of filtering rules is the template tables that define the actions for skipping or repelling traffic. SDN switches will perform routing functions that contain similar template tables and can perform the simplest functions. However, there are a number of differences between SDN switches from routers.

- The switch can extract the heading information of L1-L4 levels from the packet headings.
- The switch is capable of performing even more complex operations except for skipping and repelling traffic; it is possible to mirror the traffic or change the headings of the transmitted packets.
- The switch is able to send headings packet or packets entirely to the network controller for a more complex analysis.

- SDN switches are capable of supporting counters which allows you to analyze the quantitative characteristics of the traffic passing through.
- SDN switches can perform filtering functions at all points of connection of network equipment, also protecting against internal attacks.
- ME functions can be performed in the SDN without the use of additional specialized equipment. Thus the functions of the firewall can be implemented at any point in the network.

b. SDN Intrusion Detection System (IDS)

Using SDN for intrusion detection allows you to monitor not only any network point (network sensors) but any host connected to the network as host sensors.

Since SDN allows mirroring any flows passing through the switch, the stream from any point of the network data plane can be sent to the IDS server. In order to avoid losing part of the information (L1 level) available to the switch, the SDN controller can act as an integrated sensor.

The SDN controller can also perform some of the IDS functions, which will detect attacks in the control plane, use quantitative flow estimates and automatically respond to detected intrusions.

c. Virtualization of security functions in SDN & NFV

Providing virtual security functions instead of hardware ones allow you to build security systems according to customer requirements flexibly configure their functionality and promptly make the necessary changes.

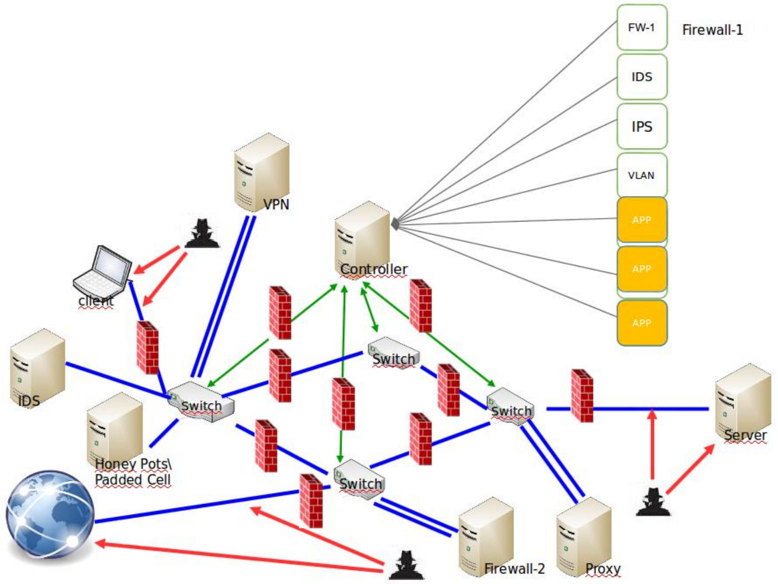


Figure 3. Virtual security functions.

3. CONTROL PLANE SECURITY

The centralization of management functions in the SDN increases the security risks for these networks associated with attacks on the control circuit SDN. Separating the control loop from the data loop provided in the SDN, on the one hand, increases the safety of the network, and on the other, requires the creation and maintenance of mechanisms for separating these circuits.

a. SDN controller

The SDN controller is the crucial element of the whole network, the compromise of which can lead to denial of service and to various negative consequences.

Attacks on the controller are possible as "from above" from the side of compromised applications, and from below from the side of compromised switches. In this regard, to ensure the safety of the controller, the following tasks must be solved:

- ensuring the security of the initial load and administrative functions;
- Control applications for undocumented functions;
- isolation and control of application access to controller resources;
- monitoring of controller status;
- Control the propriety of external communications.

b. Switches and communications

Compromised communications and SDN switches can be used to conduct attacks on the controller, to disrupt the network or to compromise the security of data transmitted over the network.

To solve the above tasks, it is necessary to develop mechanisms for ensuring network security, taking into accounts the features and capabilities of SDN: IDS \ IPS; VLAN and VPN (for control plane isolation); Auth (for network devices authentication); Center (centralized control) and Spec (special network mechanisms) [5].

Protection of the control plane must be multi-level since only a combination of different mechanisms will ensure the safety of the control loop.

On the basis of the third version of the SDN controller in Applied Research Center for Computer Networks (ARCCN) - RuNOS [6], which is openly accessible, all interested researchers and organizations can participate in this work. In the new version 0.6 of the RUNOS controller, a graphical web interface has been added and it has become possible for third-party applications to interact with the controller via an external REST interface.

REFERENCES

1. Smelyanskiy R.L. «SDN: is it a solution for network security?». Seventh International Forum «Partnership of State Authorities, Civil Society and the Business Community in Ensuring International Information Security» April 22–25, 2013 Garmisch-Partenkirchen, Munich, Germany – V: 1 – pp 300-309. –MSU. – Moscow – 2013.

2. 2017 SDx Infrastructure Security Report The Rise of Software-Defined Security (SDS) https://www.sdxcentral.com/reports/2017/sdx-infrastructure-security/.

3. Coughlin M. A Survey of SDN Security Research University of Colorado Boulder 2013 http://lordofzoobs.tv/coughlin/doc/a_survey_of_sdn_security_research.pdf.

4. Scott-Hayward S., Callaghan G., Sezer S. SDN security: a survey. DOI: 10.1109/SDN4FNS.2013.6702553 Conference: Future Networks and Services (SDN4FNS), 2013 IEEE SDN.

5. Jakob Spooner J., Zhu S.Y. A Review of Solutions for SDN-Exclusive Security Issues. University of Derby Derby, England. (IJACSA) International Journal of Advanced Computer Science and Applications, Vol. 7, No. 8, 2016.

“New Harvard” Architecture – Computer with “Viral Immunity”

Konyavsky Valeriy

Moscow Institute of Physics and Technology
9 Institutskiy per., Dolgoprudny, Moscow Region, 141701, Russian Federation
Tel: +7(495)4084554, e-mail info@mipt.ru

ABSTRACT

Alongside with huge advantages, computers bring challenges. And almost all of these challenges are connected with the possibility to interfere with the operation of your computer from the outside. Fighting hackers has become a "pain in the neck" for many people, and the word "virus" is often associated with a computer rather than medicine. The failure to fight hackers makes us look for the reasons not in the software as it is done today, but in something more deep. Computers are designed to run programs - various algorithms written in programming languages. The word “various” means almost “all” here. The computer runs any program. Predefined functions can be performed not only by computers - for example, finite-state machines can perform them too. The difference is that the computer executes "any" program. The computer is incomparably more flexible and versatile compared to the finite-state machine.

Keywords: computer, architecture, Neumann, Harvard, viral, immunity, vulnerability, hacker, attack

1. INTRODUCTION

Considers problems of protection of information when using computers with classical architectures: von Neumann and Harvard. These architectures are discussed in the article as untrusted, but despite this they are widely used to solve important tasks. As a result, there are conditions for virus attacks. Imperfect architecture of computers makes them an almost ideal environment for the uncontrolled spread of computer viruses.

In the article the analysis of the vulnerability of architectures: von Neumann and Harvard. It is shown that the architectural vulnerability inherent in each of the classic architectures that is associated with the ability to change the sequence of commands and data. This organization architectures creates the conditions for carrying out hacker attacks. Covers the typical phases of penetration of viruses in the computing environment, and methods of blocking viruses due to changes in computer architecture.

2. ARCHITECTURAL VULNERABILITY TURING MACHINE

Any computer is (more or less exact) implementation of the idea of a "Turing machine" [1]. The concepts "Turing machine" and "algorithm", computability are inseparably linked, defined by one another. The mere existence of an abstract “executor” such as the Turing machine makes us feel confident about human omnipotence. Indeed, any problem (or rather, recursive one, i.e. almost any) can be solved if there are enough resources (memory and time).

Perhaps it was amazing simplicity of wordings that provoked the development of general-purpose computers (universal computers, computer equipment, personal computers, PC), which partially (with finite memory) simulate the Turing machine, giving us pseudo-unlimited possibilities and pushing us into the way of extensive development. If the memory is insufficient - no problem – we’ll add some. If the time is insufficient – we’ll increase the clock frequency, the number of cores, or virtualize the resources.

For many years, this position has dragged the development of information technology behind it like a "locomotive". For example, the capacity of common local disks has grown from tens of kilobytes to hundreds of gigabytes over the last two decades, and is often measured by terabytes, but the memory still lacks. Beginning from kilohertz, clock frequencies have reached gigahertz, but the performance still lacks. However, the IT industry has become one of the industries determining the current level of economic development. Huge amounts of investments are the payment for technological progress and universality of solutions.

Using the Turing machine, one can [1] model any other computer (any "executor"), so they say about the completeness of the Turing machine. In its turn, taking into account the above-mentioned restrictions (finiteness of the memory), the Turing machine can be modeled on an general-purpose computer. Such general-purpose computers are called Turing complete.

Thus, Turing complete general-purpose computers should at least perform elementary operations peculiar to the Turing machine, namely, to move the control unit (read-write head) to the left or to the right along the tape, to read and to write characters of a finite alphabet in cells. Linearity of the memory and consistency of operations are the basic characteristics of the Turing machine.

General-purpose computers are potentially capable of self-learning, reaching a level at which a discoursing person will not be able to guess whom he is speaking to - a man or a computer (the Turing test). Of course, these are splendid prospects, the very existence of which makes the sphere of computer technology very attractive!

But is the ability of self-learning always a plus? For example, serious concerns can emerge if controllers of automated process control system at nuclear power plants, in railway transport or continuous production will uncontrolledly learn. It is unlikely that these controllers should be intelligent, and not accurately perform their functions. Apparently, therefore finite-state machines are usually used to solve such problems. Finite-state machines, context-free grammars, primitive recursive functions are examples of Turing incomplete formalisms.

Thus, there are many problems that can be solved not by a general-purpose “executor”. Moreover, there are many problems that should be solved not by a general-purpose, but by a specialized “executor”. Thus, the inalienable opportunity “to read and to write”, which makes the copy operation in the computer immanent, totally contradicts, at least, the tasks of information security. The property, which is required for “general-purposefulness” gets unacceptable in specific circumstances.

Trying to protect itself from malicious hacker programs, the humanity has (for more than 60 years) been developing programs that are traditionally attributed to the sphere of information security - means of identification, authentication, authorization, integrity control, anti-virus software, cryptographic tools and so on. Use of such means brings some positive effect, but very poor one. Acting within a universal, but a formal model, we will inevitably face its incompleteness - in full accordance with the Gödel's incompleteness theorem.

It becomes obvious that searching for vulnerabilities only in software is not enough. Indeed, **if a general-purpose computer runs any program, it will obviously run a malware.** It does not depend on its software; it is defined by its architecture. General-purposefulness of a computer is ensured by its architecture, the very “construction” of the Turing machine, both, in the abstract form and in practice. The ability to run malicious programs is a basic, systemic, architectural vulnerability of all computers built like the Turing machine. Vulnerability is the reverse side of general-purposefulness. The Turing machine is vulnerable in its architecture. All kinds of computers used are vulnerable because they have been designed to be as general-purposeful, as possible. This vulnerability is a price for general-purposefulness of our computers. We exploit computers, and hackers exploit this vulnerability.

3. THE VON NEUMANN ARCHITECTURE, HARVARD ARCHITECTURE AND THEIR VULNERABILITY

Since the architecture cannot be changed by software, no software will help us to ensure reliable defense against hackers. The “tug of war” has been going on for many years, giving jobs to hundreds of thousands of information security experts, but not saving us from losses.
What should we do?

If vulnerability lies in the architecture, we need to improve the architecture.
There are two classic architectures – the Von Neumann architecture [2] and the Harvard architecture [3]. Almost all personal computers can serve as examples of the former one, and almost all tablet computers and phones can serve as examples of the latter one.

The computer described below is a computer whose architecture differs from both the von Neumann architecture and the Harvard architecture. However, the computer described below, or rather, a new or changed or modified architecture, is not the first deviation from classics. Let’s consider some of them.
We know [4] the von Neumann principles of computing process organization, namely:

P1. Use of the binary system in computers.
P2. Operation control of the computer with the help of a **sequence** of commands (programs).

P3. Use of the computer memory to store both data and programs. The **data and the programs are stored in a single memory** in the same form, and the same operation can be performed in relation to commands as to the data.

P4. Serial numbering (addressing) of all computer storage locations, and the possibility to randomly access any storage location using its address. In other words, the **entire memory of the computer is located in the same address space**.

P5. Provision of a conditional branch to **any** part of the code while running a program, despite the fact that the commands are executed one by one.

Note that P4 and P5 are not new principles, but in fact it is a partial description of the Turing machine.

The analysis of the computer development history shows that some of these principles have been repeatedly violated, which often led to unexpectedly positive results. Some historical examples are summarized in Table 1.

Table 1. Some computers deviating from the Von Neumann principles

Principle	Example of violation	Peculiarity
P1	Computer “Setun” [5]	Ternary number system
P2	V.M. Glushkov’s macroconveyor computer [6] Computer “B5000” produced by Burroughs Corporation [7]	Independent command flows
P3	Computer “MIR”-1 [5] Computer “B5000” produced by Burroughs Corporation [7] All computers built based on the Harvard architecture [3]	Computer language High-level commands and data are stored separately

These and many other examples show that computing process organization principles of Von Neumann (at least P1 - P3) are not dogmas, and they have been repeatedly questioned by leading global developers, and an open-minded approach has yielded positive results, although the experiments have been rather expensive. The contrary thereof is also true - focusing on general-purposefulness (computing process organization in accordance with the Von Neumann principles) at the previous stage of technological development gave a powerful impetus to information technology, but at the same time stopped productive research in the field of computer architectures for a long time. It should be also noted that the principles that go back to the ideas of the Turing machine (P4 and P5) have never been violated, or we just could not find examples thereof.

Technology has made a huge breakthrough over the recent years, but it has not almost affected the computer architecture. The most outstanding change here is the outrunning growth of solutions based on the Harvard architecture. While a few years ago, the ratio of x86 and ARM processors sold was

80:20, today it is 50:50, and this trend is increasing[1]. There are now conditions to reflect on improving the architecture.

While developing a computer, one must understand what functions are to be performed by hardware, and what functions are to be performed by software. The correct choice of this ratio has allowed PCs built on the von Neumann architecture to occupy a leading position during many years. However, the maximum effectiveness of this technical solution has been already reached; extensive development (increase of productivity, memory, reduction of dimensions, etc.) does not meet social needs any longer. A computer deprived of the vulnerabilities that hamper the development of information exchange may become a driver for the development. When developing a new computer, one must include in the hardware things that reduce its cost, rarely change, expand its capabilities and are always used. Moreover, it does not seem impossible now that the computer structure can dynamically change in the process of operation. Or, for example, at first the structure may be as that of a finite-state machine, and then at the next stage it can become a Turing "general-purpose" machine. Let's analyze existing architectures.

A distinctive feature of the von Neumann architecture is that commands and data are not divided, they are transferred through a single common channel.

The Harvard architecture provides for availability of separate channels for commands and data.

Such a scheme requires a more complex organization of the processor, but ensures greater performance, since flows of commands and data are not consecutive, but parallel, independent.

However, both in the case of a Von Neumann computer and in the case of a computer with Harvard architecture the organization of command and data flows is such that both computers are vulnerable in their architecture. The flexibility and the general-purposefulness in both cases are ensured by the possibility to change the sequence of commands and data (double-headed arrows from the processor to the memory), irrespective of whether they are stored in a single or separate memories. In its turn, the possibility to change the sequence of commands and data creates a possibility of unauthorized interference of malicious software - this is the main architectural vulnerability.

4. THE USE OF ARCHITECTURAL VULNERABILITIES BY HACKERS

Such vulnerability is a basis for almost all modern hacker attacks which mostly boil down to the "takeover" attack. The attack usually looks like as follows:
s1) malicious software is introduced and installed in the main memory;
s2) a malicious interrupt handler is introduced and installed in the main memory;
s3) the malicious software and the interrupt handler are recorded in the long-term memory;
s4) an interrupt is caused using any available mechanism such as a DDOS attack;

[1] The assessment was provided by academician B.A. Babayan (INTEL) in his conversation with the author, June 2015

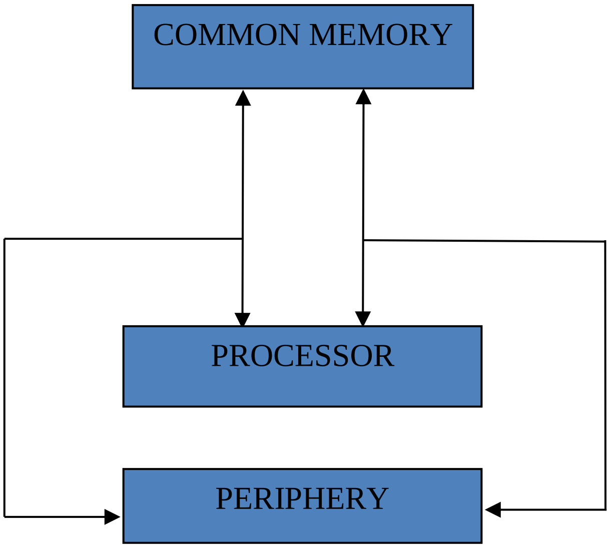


Figure 1. Von Neumann architecture

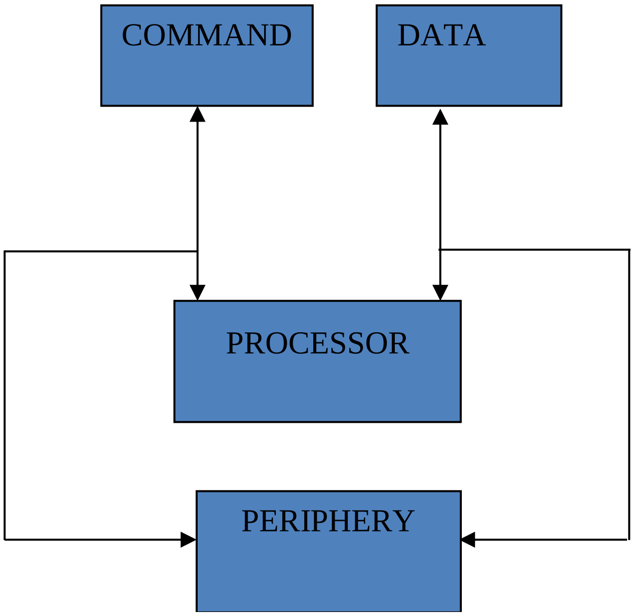


Figure 2. Harvard architecture

s5) the preinstalled interrupt handler gets activated and passes control to the malicious software;
s6) the malicious software performs its function, for example, destroys information.

The steps s1 - s3 – are here steps to prepare for an attack, s4 is initiating the attack, s5 and s6 are the very use of architectural vulnerability.

To neutralize s1 and s2 steps antivirus programs are usually used. Sometimes it is useful, but only sometimes, because it is impossible to detect all malware with the help of anti-virus software.

Moreover, experts know some strictures of the malware that cannot be detected at all. One could even say that computer viruses and generally malware can be detected only because of their defects. In general, you can always develop a malware that cannot be detected by signature search anti-virus software, heuristic analyzers and behavior blockers.

Step s3 cannot be prevented in standard architectures. One can only block the aftereffects. One can block the aftereffects of s3 while starting the system using integrity control mechanisms, which are in fact auditors determining whether there is a change in data composition or not. Sometimes this test is performed using the same sets of anti-virus software, but it is a poor solution, because the test should be performed prior to start of the OS, but programs, including antivirus ones run under the OS control.

Event generation at s4 is partially blocked with the help of special traffic analysis tools installed both in the network and on client computers. It is important that there are no means yet to *certainly* block this vulnerability.

Negative effects of s5 and s6 steps are blocked using task (process, flow) initiation control tools. These are very effective mechanisms, but tools implementing them are quite expensive, and to set them one needs to be an expert in computer technology and information security.

Since some of these security functions should be performed before starting the operating system, they cannot be implemented by software, but only with the help of a complex device.

5. BLOCKING ARCHITECTURAL VULNERABILITIES IN COMPUTERS VON NEUMANN ARCHITECTURE

Data security tool protecting from unauthorized access (DST PUA) "Accord" is an example of such a device [8].

This is a trusted startup hardware module with a software complex of access control. It performs all the necessary control functions, and its software part controls, in particular, tasks initiation. Accord is designed to work on x86-processor computers. Note that the architecture of such computers is very similar to the classical Von Neumann architecture.

The effectiveness of DST PUA Accord is connected with the fact that it blocks vulnerabilities associated with integrity violation, and creates a trusted environment to run software that protects your computer at s1 - s6 steps.

Despite its popularity, the price of DST PUA Accord is quite high, and its setting can be done only by professionals. Of course, it is the best solution for companies, but apparently it is too complex for private use. Its complexity is due to the von Neumann architecture of the computer protected - you need to add a read-only memory, divide the flows of commands and data, carry out control procedures in a trusted environment before starting the operating system, and so on.

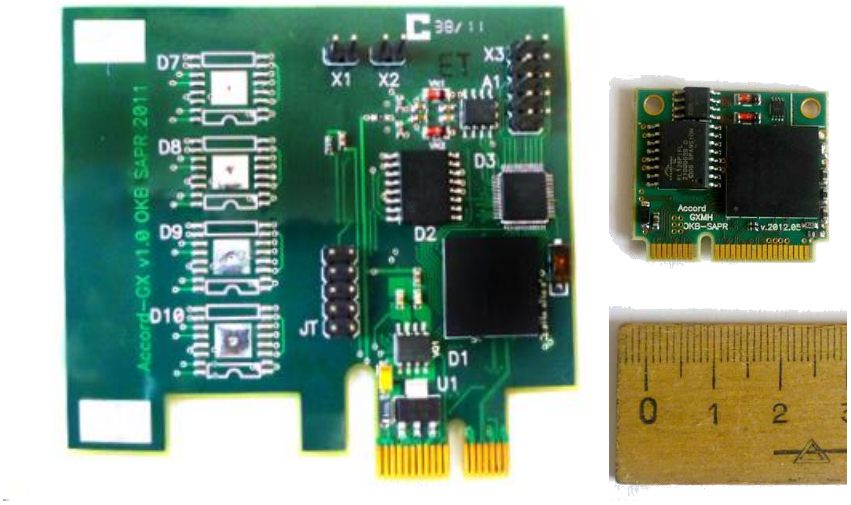


Figure 3. DST PUA Accord

However, computers built on the Harvard architecture already have separated flows of commands and data. If so, is it possible to use this fact to simplify and reduce the cost of security mechanisms? It is only necessary to make the memory read-only (then there would be no need to use complex mechanisms to monitor programs and data integrity before the start of the operating system), and in this case control procedures can run under a trusted and read-only operating system.

These functions can be easily performed if one ensures movement of commands and data only in one direction - from the memory to the processor as shown in figure 4. Obviously, this architecture will ensure invariability of the OS, programs and data.

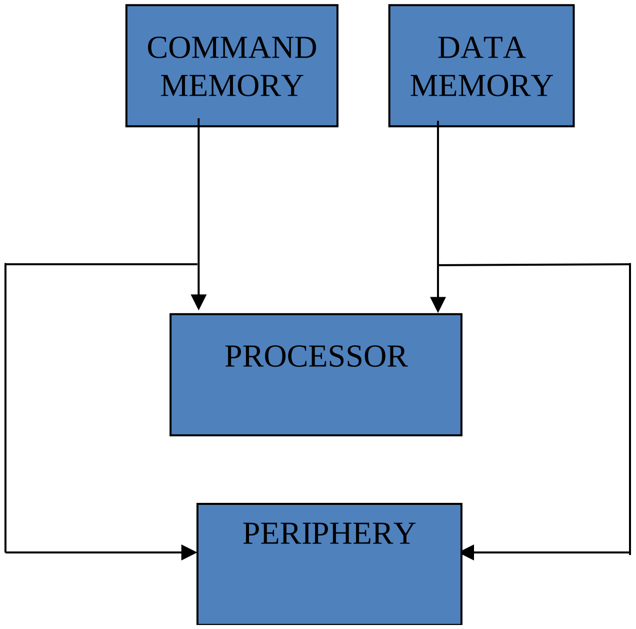


Figure 4. Harvard architecture with RO

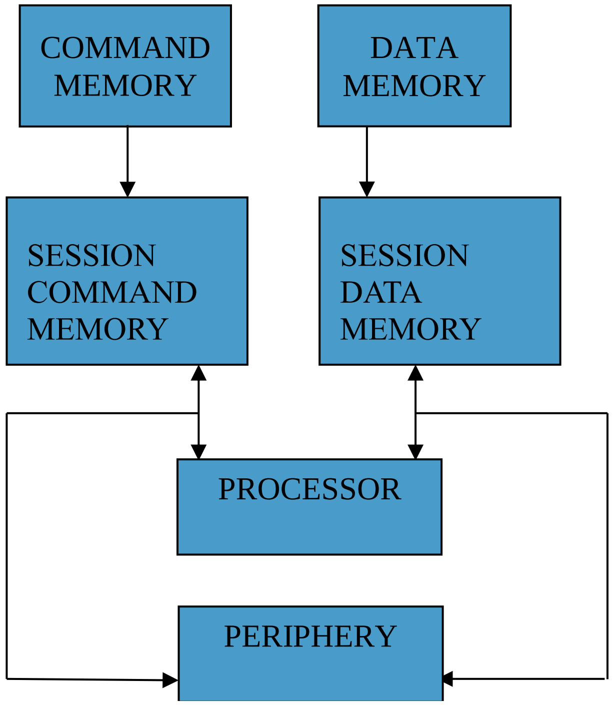


Figure 5. Harvard architecture with session memory

If we return to the above attack scheme, we see that s3 step cannot be executed, so the attack itself (s5 and s6 steps) cannot be executed too. Such a computer will acquire a significant “viral immunity” as malware will not be recorded on the computer.

A disadvantage of this is that you will have to improve almost all the software, because developers of existing software widely use the memory write operations. To run, almost all programs need the possibility to write.

To be able to use all previously developed software without any modifications, the proposed architecture should be supplemented with session memory[2] blocks, in which programs will run as shown in figure 6.

6. THE NEW HARVARD ARCHITECTURE

Thus, the computer architecture will differ at various stages – at first, it will be as shown in figure 5, and then it will be as shown in figure 6. In fact, the architecture changes from the start-up to the operation stage. Combining two figures, we will get a variable architecture of the Harvard type as shown in figure 7.

The proposed architecture has been named “new Harvard” architecture. It differs from others by its read-only memory. At the start-up stage commands and data are located in the session memory, where they are executed. The initial start-up and copying of codes to the session memory may be performed both, consecutively or in parallel – the essence of separation does not change. Similar changes can be entered by using a common session memory (Fig. 7) as the von Neumann architecture.

Of course, this scheme is just theoretical, and it is much more complex in real computers. However, we can say for sure that owners of such computers feel much more protected from hacker attacks.

The new architecture is characterized by dynamic variability, which maintains effectiveness and at the same time ensures sufficient security, invariability of the operating system, “viral immunity”, use of adapted standard operating systems and all the software developed for them.

[2] The notion “session memory” was proposed by A.V. Babanin while discussing this architecture with the author, March 2015

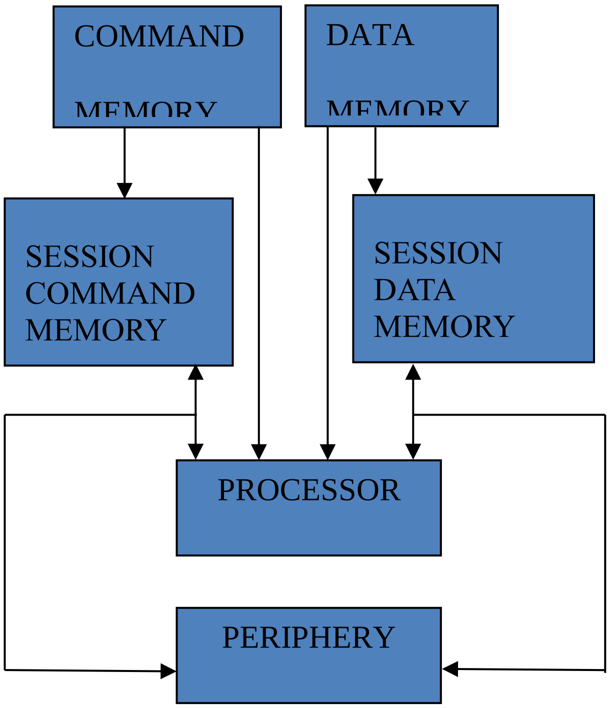


Figure 6. New Harvard architecture

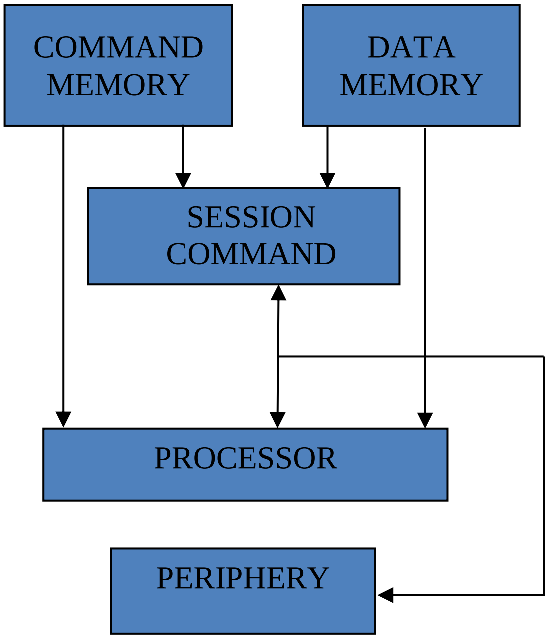


Figure 7. New Harvard architecture with a common session memory

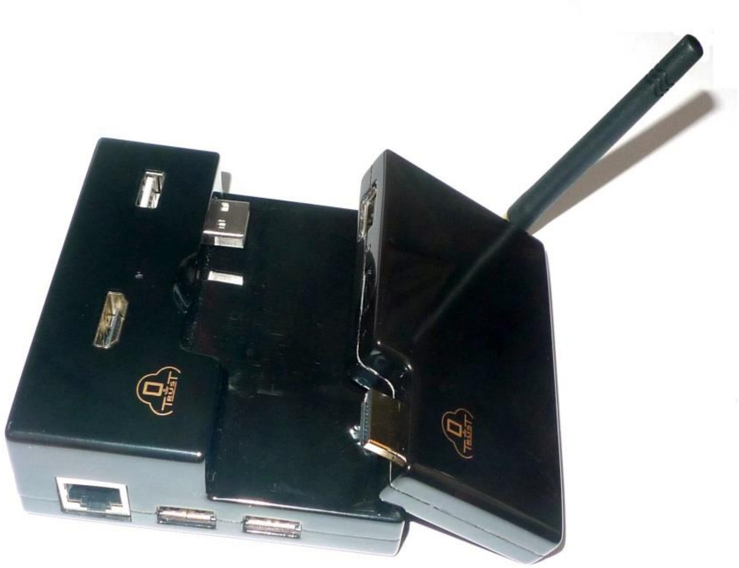


Figure 8. A modular computer MKT card, New Harvard architecture

7. CONCLUSION

Developing the architecture of this computer, we have violated several von Neumann principles, and first of all - P4 and P5. Indeed, P4 is violated, since the command memory and the data memory are not available for writing, and numbering of the cells of this memory and the session memory cannot be considered “consecutive”. And, of course, a conditional branch is possible within the session memory and impossible in the protected memory, so P5 is also violated. And what do we get in return?

There are two main advantages - a high level of “viral immunity” and a possibility to create and maintain a trusted environment and to use all previously developed and tested software.

It is important that the above architecture can be used to create computers for all kinds of information exchange where the trusted environment and security are important - from remote banking (RB) [9] and secure “clouds” [10,11] to the "Internet of Things". 7 types of computers are now serially produced on the basis of the above architecture - MKT, MKT+ MKTrusT, MKcard, MKcard-long, AQ-MK, TrusTPAD.

Their features are described in [12-18], and the computers themselves are described in [19]. New types of computers are being developed now.

REFERENCES

1. https://ru.wikipedia.org/wiki/Машина_Тьюринга.
2. https://ru.wikipedia.org/wiki/Архитектура_фон_Неймана.
3. https://ru.wikipedia.org/wiki/Гарвардская_архитектура.
4. http://www.inf1.info/machineneumann.
5. Malinovsky A. History of computer engineering in persons. – К.: “KIT”, PTOO “A.S.K.”, 1995. – 384 p.
6. Glushkov V.M., Ignatyev M.B., Myasnikov V.A., Torgashev V.A. Recursive Machines and Computing Technology. IFIP Congress 1974: 65-70
7. https://ru.wikipedia.org/wiki/Burroughs_Corporation
8. Konyavsky V.A. Data security management using DST PUA Accord. – M.: Radio i Svyaz, 1999. – 325 p.
9. Konyavsky V.A. Secure microcomputer МК-TRUST — a new solution for remote banking. National banking journal. M., 2014. No. 3 (March).
10. Konyavsky V.A., Akatkin Yu.M. Do not we trust the cloud or it does not trust us? Information Security. M., 2014. No. 1.
11. Akatkin Yu.M., Konyavsky V.A. Secure access to corporate cloud applications. Information Security. M., 2014. No. 1.
12. Konyavsky V.A., Stepanov V.B. Thin client computer with hardware data security tools: utility model patent No. 118773. 27.07.12, bul. No. 21.
13. Konyavsky V.A. Computer with hardware data protection from unauthorized change: utility model patent No. 137626. 20.02.2014, bul. No. 5.
14. Konyavsky V.A. Mobile computer with hardware protection of the trusted operating system: utility model patent No. 138562. 20.03.2014, bul. No. 8.
15. Konyavsky V.A. Mobile computer with hardware protection of the trusted operating system from unauthorized change: utility model patent No. 139532. 20.04.2014, bul. No. 11.
16. Konyavsky V.A. Mobile computer with hardware protection of the trusted operating system: utility model patent No. 147527. 10.11.2014, bul. No. 31.
17. Akatkin Yu.M., Konyavsky V.A. Mobile computer with hardware protection of the trusted operating system from unauthorized change: utility model patent No. 151264. 27.03.2015, bul. No. 9.
18. Konyavsky V.A. Workstation with hardware data security tools for computer networks with client server or terminal architecture: utility model patent No. 153044. 27.06.2015, bul. No. 18.
19. Trusted Cloud Computers [electronic resource]: http://www.trustedcloudcomputers.ru.

Network Attacks Detection based on Cluster Analysis

Nikolskaia Kseniia

South Ural State University
76, Lenin Prospekt, Chelyabinsk, Russian Federation
Tel: 89995897237, e-mail: nikolskaya174@gmail.com

ABSTRACT

In this paper, a method for detecting network attacks on a computer system is considered. The possibility of using artificial neural networks for the analysis of network traffic was investigated. A method for solving a problem based on the clustering of the space of vectors describing the information interaction of the nodes of the computer network of the information system is described.

Keywords: cybersecurity, neural, network, clustering, traffic, data, mining, attack, computer, system

1. INTRODUCTION

The network security is an important issue in the process of the protecting information. At the moment there are many expert systems that provide information protection. However, not yet developed a system that fully provides protection from the computer attacks. All expert systems are built on various algorithms, for example, clustering algorithms. This is one of the recent trends in research. About him written quite a few works. The task of clustering is as follows. There are many objects that need to be investigated. Each of the objects is characterized by a set of certain variables. Each variable takes a value from some dataset. The essence of the problem is to break up the dataset into groups (clusters).

The initial data for research should be IP-packets (or packet headers). They gather at the observation points. The unit of consideration is the flow. The stream consists of a sequence of IP packets. IP packets must be aggregated according to certain rules. For example, a bidirectional or unidirectional sequence of packets between two IP addresses, a full TCP session, or a unidirectional sequence of IP packets. The sequence of IP packets is determined based on five header fields <src_ip, src_port, dst_ip, dst_port, protocol >, as well as the rules of formation. Under the rules of formation, the completion of the flow will be determined. In this case, only information that is contained in the packet headers is available for the classifier.

To determine the traffic category is necessary to fixate a set of variables (attributes). Attributes are based on static characteristics. For example, the size of the packets, the interval between packets, and the characteristics that are extracted from the packet headers (the size of the TCP segments or the number of retransmissions). A stream is assigned a set of attribute values according to which clustering is performed. As a result, you should get clusters. Each cluster must correspond to a dominant category.

2. CLUSTERING TRAFFIC BASED ON VARIOUS ALGORITHMS

One of the first papers devoted to the classification of traffic using machine-learning techniques is the work [1]. In this paper, a methodology was presented for dividing traffic flows into groups with one type of behavior in relation to the load on the network. For example, the transfer of large amounts of data, one transaction in the exchange process, several transactions, etc. The task of identifying specific applications was not set. Since different types of behavior can be traced in one application, and vice versa, different protocols, for example, HTTP and FTP, can have similar characteristics.

Complete bidirectional flows are investigated. They are limited only by observation time and are formed on the basis of the publicly available sets of packets waikato Internet traffic storage (WITS). The following attributes of the stream are considered: packet size statistics (minimum, maximum, quartiles, ratio of minimum to maximum, first five modes); statistics of time intervals between packets; number of bytes; duration of interaction; the number of transactions between the transaction mode and the transmission mode (more than three packets in one direction and none in the opposite direction); the idle time as a sum of intervals of more than 2 seconds, when no packets are sent in either direction for transaction modes or for transferring large amounts of traffic.

An approach of nondeterministic, so-called soft, clustering is used: one and the same flow can belong to several clusters with a certain probability. Such a statistical approach is applied in practical situations, for example, in the case when training data is not enough to make an exact decision. The task is to find the most plausible set of clusters, having a set of training data and a priori expectation. At the base lies a model called the “finite mixture”. A mixture is a set of probability distributions that is unique for each cluster, simulating attribute values for cluster members. To evaluate the parameters that ensure the maximum likelihood of a mixed model, the EM (expectation-maximization) algorithm is used, which has the necessary statistical basis.

The number of clusters that is a parameter of the implementation of the EM algorithm can be determined by selection, but in this paper we propose a method of cross-validation, which provides an automatic determination of the number of clusters. This method gives a generalized estimate of the model obtained, for example, the question of the behavior of the model on data other than training ones is investigated. For visualization of clusters it is suggested to use kiviat-graphs (radar, star chart) - two-dimensional graphs, in which numerical attributes correspond to axes emerging from one point. The algorithm implementation proposed by the Waikato University Machine Learning Group is used. As a result of clustering, six clusters were obtained. One of the clusters contained 59% of all threads and related to the HTTP protocol with a behavior pattern typical for the extraction of small and medium-sized objects. One cluster contained mostly threads related to the TCP DNS. The remaining clusters contained streams corresponding to different protocols.

As one of the validation options, clusters obtained at half of the training data were considered. It turned out the same basic number of clusters. However, it was not possible to obtain clusters, each of which would correspond to a dominant application.

In works [2, 3] for classifying traffic, the classifier AutoClass [4] is used, which is an implementation of the EM-algorithm. The AutoClass algorithm is designed to find a set of clusters (classes in the terminology of AutoClass), which is as plausible as possible in relation to the data and model. The number of clusters can be determined automatically, if it is not specified. To determine the number of clusters and the best separation of data from clusters, the EM algorithm is used iteratively. The method of improving the quality of clusters has allowed to achieve good results in the separation of various applications.

Three publicly available data sets Auckland-VI, NZIX-II (WITS), and Leipzig-II were collected at different points at different times. Consider bidirectional flows defined by the five <src_ip, src_port, dst_ip, dst_port, protocol> and a timeout of 60 s. Flow attributes are considered average and deviations for the intervals between packets and for packet sizes, the size of the stream in bytes, and the length of the stream. All parameters, except duration, are calculated separately for each direction of traffic. Attributes are considered independent and modeled using a log-normal distribution. The proposed classification technique includes the following steps.

1. Transformation of input data: the organization of packets into streams, the calculation of the characteristics of flows and the preliminary classification of flows using a opensourse system for NetMate network measurements.

2. Using the received stream characteristics and the attribute model for uncontrolled learning on test data using AutoClass. Because training is a lengthy process, 1000 randomly selected streams with TCP / UDP ports corresponding to FTP, Telnet, SMTP, DNS, AOL Messenger, Napster, Half-Life (of 8000 streams corresponding to these applications) are taken as samples.

3. Evaluation of combinations of attributes and improving the quality of clusters. To find the most contrast clustering, the best combination of attributes is searched. The search process is an iterative process consisting of three phases: selection of a subset of attributes; study of the obtained clusters; evaluation of the structure of clusters. To find the best subset of attributes, use the sequential forward selection technique. The process starts with one attribute, the ones that show themselves best in the attributes are placed in the SEL(1) set. Then, a set of two attributes is checked, one of which is in SEL(1), and the other is not in SEL(1). Showing themselves from the best side sets of two attributes are placed in SEL (2). The process continues until there is an improvement in the structure of the clusters.

The methodology was tested on three sets of data or with the separation of one set into two parts. It turned out that for different data sets, the different sets of attributes turned out to be the best relative to the measure of homogeneity, and their number varies from 4 to 6. For the data sets examined, the most effective were the attributes constructed on the basis of the statistics of the deviation of the packet sizes in the streams. The indicators for the various applications were also different. Thus, a certain success in the separation of applications is achieved with the correct selection of attributes. The most homogeneous were the clusters, corresponding to the application of Half-Life. On average, for different test data, the uniformity is 85%. As an indicator of incorrect classification for an application, the ratio of incorrectly classified flows to the flows of this application to which classes are assigned is considered. The lowest recognition rates are available for FTP, Web and Telnet traffic.

It should be noted that the analysis did not consider flows containing fewer than three packets, since it is impossible to compute for such packets some characteristics. For TCP streams, abnormal streams discarded (TCP requires at least three packets to be sent in each direction), and for UDP traffic, normal traffic can be dropped, for example DNS-request. As a result of the study of traffic related to eight applications, about 50 clusters were obtained. It is not clear which interpretation corresponds to clusters for which a dominant application is not defined.

In research [5], the results of clustering of network traffic were compared using the algorithms K-Means [6], DBSCAN [7] and AutoClass [4]. At the same time, for the first two algorithms during the research there was no information on the application of network traffic to clustering. The study was carried out for these algorithms, since it is known that they work faster than AutoClass. The algorithms were compared from the point of view of the ability to generate clusters, which could be more attributed to one application, which in the end is of the greatest interest for researchers developing an effective and accurate classification mechanism.

The studies were carried out on two data blocks: the public daily Auckland IV block (WITS) and its own Calgary data block, consisting of traffic at the Calgary exit point to the global network and containing complete packets. In this case, the stream is bi-directional traffic corresponding to a complete TCP session, starting with the connection establishment before the break or until the idle is detected for 90 seconds. The choice of attributes is largely due to work [3]. There is a consistent and non-redundant list of attributes. The following thread attributes were considered: the number of packets, the average packet size, the average payload size of the packet (in each direction and the total), and the average interval between packets. Logarithmic transformation of attribute values is performed, since many characteristics have distributions with "heavy tails" and as a metric Euclidean distance between vectors attributes is used [8, 9].

Traffic categories were determined based on the study of port numbers, since the Auckland IV block contains only packet headers. The block is represented by categories DNS, FTP, HTTP, IRC, LIMEWIRE (P2P), NNTP, POP3 and SOCKS. The second block was investigated by searching in the full content of the template packets corresponding to the protocols under investigation, and consisted of the following traffic by protocols: HTTP, P2P, SMTP, and POP3. In both blocks of data, HTTP was the dominant traffic. Therefore, the blocks were transformed: in the Auckland IV block, 1000 samples of each traffic category were randomly selected, and in the Calgary block, 2000 samples of each category were selected. As a measure of the proximity of the vectors of attributes x and y of dimension n, the Euclidean distance was used.

As a measure of the effectiveness of algorithms, the overall accuracy is used - the total accuracy for all clusters. It characterizes the ability to create clustering, in which each cluster belongs to only one category of traffic. In this case, the cluster is marked with a category if most of the streams belong to this category. Full correctness is defined as ΣT P - the number of threads that are being examined.

Studies have shown that the results essentially depend on the choice of the parameters of the algorithms. In this respect, the AutoClass algorithm, which has no parameters, is preferable. The dependence of the results of the study on the selected data samples remains unknown.

3. APPROACHES TO CREATING SYSTEMS FOR CLASSIFYING NETWORK TRAFFIC

When considering the classification should be based on the works [10,11]. In these papers it is proposed to use the method of partial control of clustering. It has a number of advantages. A small number of tagged streams are required (belonging to the class). It will be mixed with a lot of untagged streams.

However, marking samples creates a certain difficulty, and a small amount of samples used in training can lead to incorrect results.

Another advantage is the ability to track new applications and the new behavior of already encountered applications. If it is necessary to conduct a controlled classification, then it will be necessary to assign a certain class to each type of flow. The last advantage is that the approach can be used within the system of collecting traffic statistics, functioning both at the points of exit from the local network to the global network, and within the core network.

A stream is a bidirectional sequence of packets, taking into account the transport layer protocol and port numbers. The end of the stream is determined after the connection is completed or after a timeout. As above, only the most common TCP traffic is considered. A separate classifier is required for each transport protocol. The attributes of the stream are: total number of packets, average packet size, total number of bytes, total number of bytes in headers, number of packets from active to passive, number of bytes from active side, number of payload bytes from active party, total number of bytes in headers from the active side. To select a subset of attributes was used the technology backward greedy search [12].

When marking the training data to establish the "absolute" truth, a combined approach was applied. This approach is based on some categories: on automatic investigation of signatures; comparison of traffic that contains encrypted data, with traffic related to the same IP addresses and containing open text; In the case of HTTPS (port 443), a manual check of the presence of calls to real web servers was carried out.

The proposed method, which combines a controlled and uncontrolled approach, involves two stages. Suppose a fixed set of desired categories of applications Y = {Y1, . . . , Yq}. At the first stage, the clustering algorithm is applied to the training set of tagged and unmarked threads. In this case, the K-

Means algorithm is used. Further, tagged streams are used to compose clusters and known categories. The cluster receives the application label to which the maximum of the tagged streams belongs. All untagged threads that fall into this cluster receive the application label of the cluster. In this case, some clusters can not be assigned a category if they do not include tagged streams. Such clusters are marked with the Unknown label.

The possibility of clustering without the use of tagged streams was studied. As a result of experiments it was established that it is possible to not mark flows. For a sufficiently large number of clusters (k = 400), can first cluster, then mark only a few arbitrarily chosen flows from the cluster and get a correctness equal to 94%. The experiment was conducted on a block consisting of 64,000 streams. The next series of experiments was performed to determine the number of tagged flows necessary for qualitative clustering. It was found that with a fixed number of marked training streams, an increase in the number of untagged flows leads to an increase in the correctness. This is important, since the marking of the flows is complex, in addition, one should take into account the possibility of errors.

Classification in real time implies the fastest possible identification of the category to which the considered stream belongs. Unlike the autonomous classification, when all information about flows is available, only part of the information about the statistical parameters of the flows is available in real time. To overcome this difficulty, a layered classification system was developed. Levels are based on the notion of a packet milestone. The boundary is reached when the number of packets sent or received reaches a certain value (SYNACK packages are included in the review). Each level is an independent classification model. The model is obtained by training on samples that have reached the appropriate size, defined by packet milestone. You can define layers based on the transport protocol. The first layer defines only the transport protocol and ports. For TCP traffic, the flow goes to the second layer when the first data packet is received, and so on.

A multi-level approach can potentially improve classification. At each level, the same set of thread attributes is considered. The statistics are collected as the packets of this stream are collected. When the first boundary is reached, the partial flow is classified according to the first-level model. When the next boundary is reached, the flow is again classified according to the model of the given level, i.e., there is a revision. The correctness of real time is calculated at each level relative to bytes - the fraction of bytes that received the correct label. The final classification of the flow occurs at the level where the flow ends. Such a multilevel approach is implemented in the real-time classifier used in the Bro system to protect against unauthorized access [13].

When testing a multi-level methodology, a block of data consisting of 966,000 streams was examined. At each level, the model was built on the basis of 8000 streams at k = 400. Thirteen layers were considered, the boundaries were distributed exponentially: 8, 16, 32, ... Eleven or more layers have reached only 5% of threads larger than 4096 bytes. At the first stage 40% of bytes were correctly evaluated, on the fifth - 50%, on the thirteenth - 78%. The last meta received by the flow turned out to be correct in 82% of cases. It is noted that some layers that do not increase the correctness can be excluded.

The experiments showed that the approaches considered make it possible to obtain classifiers that can be used for sufficiently long periods of time, re-training is necessary only with significant changes in network behavior, for example, when new applications appear.

4. HYBRID REAL-TIME CLASSIFIER FOR DETECTING P2P INTERACTION

In research [14], a hybrid classifier was used to classify traffic in real time. It consisted of a hardware classifier and a software classifier. The hardware classifier was implemented at the level of port numbers and application layer signatures. The software classifier was built on the basis of a neural network of a special type.

The hardware classifier must be based on a processor that can provide high speed. This is necessary for the maintenance of hybrid lines and programmability. Also, the processor must provide access to memory and network interfaces. In processors, the architecture of high-speed parallel processing must be implemented. They must be able to implement complex algorithms. Since researching the contents of packets, investigating traffic and redirecting traffic at high speeds requires high power. When recognizing P2P traffic, the packet is transferred to the level of the program classifier. This means that the hardware classifier works as a filter. Another task of the hardware classifier is the formation of traffic attribute values. These attributes will be used by the software classifier.

The software classifier uses statistical traffic parameters. To identify P2P traffic, it is necessary to study the behavioral characteristics of the participants in the exchange at the transport level. Such identification is given in [15]. Behavioral characteristics: simultaneous use of TCP and UDP protocols in traffic between two IP addresses; rare access to the domain name service; the practically identical number of source addresses and port numbers when accessing some IP destination address (typical for P2P exchange due to random choice of port numbers); use a small number of source port numbers when accessing different addresses and destination ports under UDP exchange.

The P2P software classifier is based on a neural network of a special type - flexible neuron tree (FNT) [16]. The neural network has the appearance of a tree with two hidden layers. A feature of the network is the use of different activation functions for different nodes, the optional connectivity of the elements of layer i with all elements of layer i + 1 and the intersection of layers, i.e. On the input of the layer i + 1, not only the elements of the layer i, but also the elements of the layers whose numbers are less than arrive i. The inputs x0, x1, x2, x3 use the attributes fpro, fIP −fort, fuPort, fDNS, and they can be used in hidden layers, but at the output, at the root, there must be only one element y. By its value, it is determined whether it belongs to P2P traffic. The activation function is a sigmoid function of the form f (a, b, x). When testing the classifier, the attributes for the IP address were counted every 5 minutes. The output element y is a real number between 0 and 1. If the value of y lies in the range [0; 0,5], then the IP-address takes part in P2P-exchange with high probability, otherwise it is not P2P-traffic.

The possibilities of P2P traffic identification are considered in the example of training a neural network on the BitTottent and Edonkey traffic detected using a hardware classifier with the subsequent identification of a P2P hybrid traffic classifier corresponding to the BitTottent, Edonkey Kazaa, PPlive, and Skype protocols. About 1675 Mbytes was examined, of which about 885 Mbytes corresponded to P2P traffic. At the same time, the correctness was approximately 95%.

Secondly, it is possible to replenish the rules of the hardware classifier by examining the traffic identified by the software classifier, as well as the possibility of re-learning the real-time neural tree based on previous results.

5. CONCLUSION

In this paper, methods for analyzing IP traffic using clustering algorithms are presented. The analysis was carried out on the basis of information contained in the headers of IP packets. The main problems that arise in the solution of the problem by the clustering method were identified. For example, choice the right characteristics that classify the data; choice of clustering method; choice the number of clusters and interpret the results. Clustering algorithms of various complexity that are designed for passive analysis and real-time analysis are considered.

Comparison of clustering algorithms was carried out. The main factors that influence the quality of the analysis were identified: the importance of selecting a set of consistent and non-redundant attributes and the dependence of this set on data samples; dependence on parameters of algorithms, for example, from the choice of thresholds and the number of clusters; the susceptibility of the assumed parameters for distributing attribute values within a class or cluster to the first choice; the ability to apply to unidirectional traffic; the effect of the sizes of blocks of data samples on the quality of the algorithm.

The solution to the traffic classification problem is very complex, especially in real time. This is due to the fact that small data is easy to process. And consequently come to the final decision. But this decision is questionable. On large data, it is very difficult to analyze, since very large computing powers are needed.

Thus, despite a large number of works, the problem of classification of IP-traffic is not solved in full. Hybrid classifiers are promising. They apply several techniques simultaneously.

ACKNOWLEDGMENTS

The work was partially supported by the Government of the Russian Federation according to Act 211 (contract No. 02.A03.21.0011.)

REFERENCES

1. McGregor A., Hall M., Lorier P., Brunskill J. Flow clustering using machine learning techniques // Passive and active measurement workshop (PAM 2004): Proc. Lecture Notes in Computer Science. V. 3015, Antibes Juan-les-Pins (France), Apr. 2004. N. Y.: Springer, 2004. P. 205–214.

2. Zander S., Nguyen T., Armitage G. Self-learning IP traffic classification based on statistical flow characteristics // Passive and active measurement workshop (PAM 2005): Proc. Lecture Notes in Computer Science. V. 3431, Boston, USA, March — Apr. 2005. N. Y.: Springer, 2005. P. 325–328.

3. Zander S., Nguyen T., Armitage G. Automated traffic classification and application identifi- cation using machine learning // 30th Annual IEEE conf. on local computer networks (LCN 2005): Proc. IEEE Computer Soc., Sydney (Australia), Nov. 2005. Washington: IEEE Computer Soc., 2005. P. 250–257.

4. Cheeseman P., Stutz J. Bayesian classification (AutoClass): theory and results // Advances in knowledge discovery and data mining. Palo Alto (CA, USA): AAAI/MIT Press, 1996. P. 61–68.

5. Erman J., Arlitt M., Mahanti A. Traffic classification using clustering algorithms // Special interest group on data communication (SIGCOMM) 2006 workshops: Proc. of the 2006 SIGCOMM workshop on Mining network data, Pisa (Italy), Sept. 11–15, 2006. N. Y.: ACM, 2006. P. 281–286.

6. Барсегян А. А. Технологии анализа данных: Data Mining, Visual Mining, Text Mining, Olap / А. А. Барсегян, М. С. Куприянов, В. В. Степаненко, И. И. Холод. СПб.: БХВ-Петербург, 2007.

7. Ester M., Kriegel H., Sander J., Xu X. A density-based algorithm for discovering clusters in large spatial databases with noise // Proc. of the 2nd Intern. conf. on knowledge discovery and data mining (KDD-96), Portland (USA), 1996. Palo Alto: AAAI/MIT Press, 1996. P. 226–231.

8. Witten I. H. Data mining: practical machine learning tools and techniques / I. H. Witten,
E. Frank. San Francisco: Morgan Kaufmann, 2005. P. 560.

9. Paxson V. Empirically-derived analytic models of wide-area TCP connections // IEEE/ACM Trans. Network. 1994. V. 2, N 4. P. 316–336.

10. Erman J., Mahanti A., Arlitt M., et al. Semi-supervised network traffic classification // Proc. of the Intern. conf. on measurement and modeling of computer systems (SIGMETRICS'07), San Diego (USA), June 12–16, 2007. N. Y.: ACM, 2007. P. 369–370.
11. Mahanti A., Arlitt M., Cohen I., Williamson C. Offline/realtime traffic classification using semi-supervised learning: Tech. rep. Univ. of Calgary. 2007. V. 64. P. 1194–1213.

12. Guyon I., Elisseeff A. An introduction to variable and feature selection // J. Machine Learn. Res. 2003. V. 3. P. 1157–1182.

13. Paxson V. Bro: a system for detecting network intruders in real-time // Computer Networks. 1999. V. 31, iss. 23/24. P. 2435–2463.

14. Chen Z., Yang B., Chen Y., et al. Online hybrid traffic classifier for Peer-to-Peer systems based on network processors // Appl. Soft Comput. 2009. V. 9, N 2. P. 685–694.

15. Karagiannis T., Broido A., Faloutsos M., Mc Claffy. Transport layer identification of P2P traffic // Proc. of the 4th ACM SIGCOMM conf. on Internet measurement (IMC'04), Taormina (Sicily, Italy), Oct. 25–27, 2004. N. Y.: ACM, 2004. P. 121–134.

16. Chen Y., Yang B., Dong J. Nonlinear systems modelling via optimal design of neural tree // Intern. J. Neural Systems. 2004. V. 14. P. 125–138.

Web Users' Activities Tracking based on the Beacons Implementation

Asyaev Grigorii, Medvedev Maxim, Mursalimov Ainur, Sinkov Anton

South Ural State University
76, Lenin Prospekt, Chelyabinsk, Russian Federation
Tel: 79617930538, E-mails: asyaev1996@mail.ru, own77d@gmail.com, mursalimovainur@mail.ru, sinkov_96@mail.ru

ABSTRACT

The article considers the concept of web beacons, the purpose and principles of embedding web beacons into websites, the ways of the manual and automated detection of them and minimizing the effectiveness of tracking user’s activities in the Internet. The results of a study on the use of web beacons on the most popular websites are presented.

Keywords: web, beacons, cookies, activity, tracking, user, privacy, advertisement, browser fingerprint

1. INTRODUCTION

The interaction between the Internet users and website owners (in the broadest sense) is associated with a global age-old problem – on the one hand, the owners (particularly, the advertisers) declare that they want to constantly progress in understanding and predicting user interests and requests, on the other hand, users accuse the websites owners of collecting their personal information, which is essential for advertisers in order to show the content that depends on what pages the users visit.

Tracking is important, for example, for social networks to exclude the need for users to authenticate once more when logging after starting another session, and online stores that collect information about user purchases, the current content of their virtual shopping cart and their preferences. Usually, the so-called cookies are used for this. There are 1st party cookies hosted on the domain where the user is located at the moment (which is needed to exclude the need to re-authenticate during a second session) and 3rd party cookies hosted on a third-party domain (used by advertisers to collect data on user’s actions and user's computer statistics). Users can disable the cookies (3rd party in most cases). This, in turn, is an obstacle for advertisers and malefactor who collect statistics.

Thus, the creators of websites came to a simple but effective solution to the problem – the use of the so-called web beacons (clear GIFs, cleardots, web bugs [1], tracking pixels, tracking bugs etc.) allowing to monitor the activity of users on the network. In turn, malefactors that use web beacons can compromise the privacy of victims by sending them spam and phishing e-mails. Since the principles of operation of web beacons are based on the basic principles of HTTP functioning, and their implementation doesn’t require any additional software and is done through the simplest HTML tags, user tracking technology being carried out by web beacons on the one hand is simple, on the other hand is very resistant to tracking itself by third-party software. The most important thing is that it is impossible to disable beacons like it is with cookies, which can lead to violations of the privacy of the Internet users, but it is possible to limit the functioning of web beacons.

2. DESCRIPTION OF THE WEB BEACON

A web beacon is an image or an inline frame that is placed on a web page and, when loaded as the user visits this page or as an e-mail is opened, sends the information necessary for tracking user activities to the "owner" of the beacon [2].

The scenarios of using web beacons are most often limited by using them to collect statistics on website visits, to collect web analytics in order to optimize the display of content on the webpages, and to display targeted advertisements. Attackers are used to find out whether the e-mail address to which the beacon is sent is valid, for the purpose of sending to spam and phishing e-mails. When sending a GET request to the server, the address on which the request is sent can be converted by the server so as to transfer information about the user to the server (discussed later).

Beacons most often work in conjunction with cookies: the server while sending responses to the web browser, adds a Set-Cookie header to it, and the web browser creates a cookie file while downloading the beacon [2].

3. THE IMPLEMENTATION OF THE WEB BEACONS IN WEBPAGES

Depending on the implementation method, web beacons can be classified as follows.

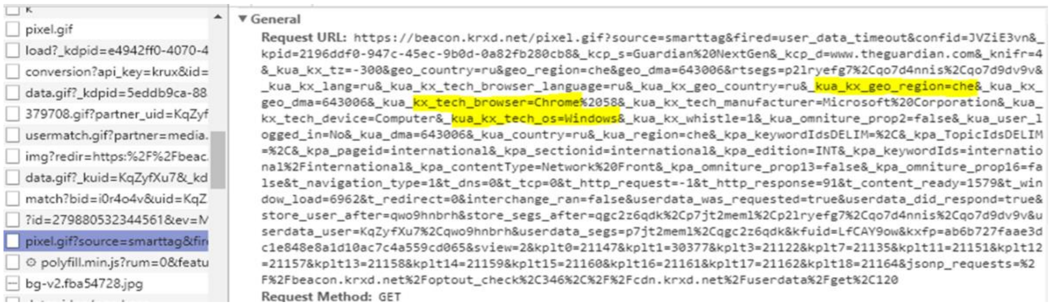
1. In the simplest case, the web beacon is an ordinary image in JPG, PNG, GIF format with a size of 1x1 pixels. This provides imperceptibility, complemented most often with setting the style attribute of style sheet language CSS for the HTML <img> tag, and also it provides beacon's fast loading that does not affect page load speed.

In general, the format of such a web beacon in HTML looks as follows:
<img src= "https://beaconurl.com/beacon.jpg" width="1" height="1">, or
<img src= "https://beaconurl.com/beacon.png" style= "position:absolute; visibility:hidden">, or
<img src= "https://beaconurl.com/beacon.gif" style= "display:none"> and so on.

Being a simple picture, such a beacon is downloaded by the browser, and the server (1st party or 3rd party server, as it is with cookies) that posted the image on the page gets information that a web beacon has been downloaded to a computer having a certain IP address. Such beacons are imperceptible to the user, but theoretically it is not necessary – the beacon can be any image of any format and size.

Having limited functionality, web beacons-images are usually used to keep statistics of visiting different webpages by an individual user, in order to find out his interests by the contents of visited pages, because within a single session of work the user's IP address is constant.

Figure 1 shows an example of a web beacon that is located on the https://www.theguardian.com/international page and sends data about the user software to a third party server: the version and type of OS, the location data (country, region), user's system language, as well as other information. The web beacons function in conjunction with cookies.


pixel.gif
load?_kdpid=e4942ff0-4070-4
conversion?api_key=krux&id=
data.gif?_kdpid=5eddb9ca-88
379708.gif?partner_uid=KqZyf
usermatch.gif?partner=media.
img?redir=https:%2F%2Fbeac.
data.gif?_kuid=KqZyfXu7&_kd
match?bid=i0r4o4v&uid=KqZ
?id=279880532344561&ev=M
pixel.gif?source=smarttag&fir
polyfill.min.js?rum=0&featu
bg-v2.fba54728.jpg

▼ General

```
Request URL: https://beacon.krxd.net/pixel.gif?source=smarttag&fired=user_data_timeout&confid=JVZiE3vn&_
kpid=2196ddf0-947c-45ec-9b0d-0a82fb280cb8&_kcp_s=Guardian%20NextGen&_kcp_d=www.theguardian.com&_knifr=4
&_kua_kx_tz=-300&geo_country=ru&geo_region=che&geo_dma=643006&rtsegs=p21ryefg7%2Cqo7d4nnis%2Cqo7d9dv9v&
_kua_kx_lang=ru&_kua_kx_tech_browser_language=ru&_kua_kx_geo_country=ru&_kua_kx_geo_region=che&_kua_kx_
geo_dma=643006&_kua_kx_tech_browser=Chrome%2058&_kua_kx_tech_manufacturer=Microsoft%20Corporation&_kua_
kx_tech_device=Computer&_kua_kx_tech_os=Windows&_kua_kx_whistle=1&_kua_omniture_prop2=false&_kua_user_l
ogged_in=No&_kua_dma=643006&_kua_country=ru&_kua_region=che&_kpa_keywordIdsDELIM=%2C&_kpa_TopicIdsDELIM
=%2C&_kpa_pageid=international&_kpa_sectionid=international&_kpa_edition=INT&_kpa_keywordIds=internatio
nal%2Finternational&_kpa_contentType=Network%20Front&_kpa_omniture_prop13=false&_kpa_omniture_prop16=fa
lse&t_navigation_type=1&t_dns=0&t_tcp=0&t_http_request=-1&t_http_response=91&t_content_ready=1579&t_win
dow_load=6962&t_redirect=0&interchange_ran=false&userdata_was_requested=true&userdata_did_respond=true&
store_user_after=qwo9hnbrh&store_segs_after=qgc2z6qdk%2Cp7jt2meml%2Cp21ryefg7%2Cqo7d4nnis%2Cqo7d9dv9v&u
serdata_user=KqZyfXu7%2Cqwo9hnbrh&userdata_segs=p7jt2meml%2Cqgc2z6qdk&kfuid=LfCAY9ow&kxfp=ab6b727faae3d
c1e848e8a1d10ac7c4a559cd065&sview=2&kplt0=21147&kplt1=30377&kplt3=21122&kplt7=21135&kplt11=21151&kplt12
=21157&kplt13=21158&kplt14=21159&kplt15=21160&kplt16=21161&kplt17=21162&kplt18=21164&jsonp_requests=%2
F%2Fbeacon.krxd.net%2Foptout_check%2C346%2C%2F%2Fcdn.krxd.net%2Fuserdata%2Fget%2C120
Request Method: GET
```

Figure 1. Web beacon put in a GIF file collecting user’s software details, geolocation data and using cookies.

Ironically, the information collected about the user is actually sent to the third-party server by the user himself : while the browser is downloading the web beacon it is also sending the GET request to the web beacon's URL. The information collected by the server is encoded in the URL's query string. For example: let the web beacon that is further downloaded by the browser be located at "https://beaconurl.com/beacon.gif". Accordingly, the GET request sent by the browser to the server will look, for example, like this:
GET https://beaconurl.com/beacon.gif?devicetype=PC&datetime=20170912195151&ostype=microsoft&osmane=win10&screenresolution=1920x1080&country=en&region=chelyabinsk HTTP / 1.0

The parameters of the query string (stored after a "?" symbol) do not affect the display of the content and are ignored by the server, but the URL from the request is stored in the log files of the server for analysis. Here, after the "?" symbol, a structure is sent as parameters of the query string, which after being parsed by the server is converted to a list consisting of key-value pairs [3].

2. Web beacons implemented as a link to an executable script. In the HTML language they look the same as web beacons-images, but the src attribute of the <img> tag contains the path to the executable script (for this type of beacon - the PHP script mostly). Usually, a different approach, called 301-redirect, is used. For example, let there be some server "beaconurl.com" and in the directory beaconurl.com/path the following files are stored: "beacon.jpg", "beacon.php".
The HTML page displays the following:
<img src = "https://beaconurl.com/path/beacon.jpg" width = "1" height = "1">.

As soon as the browser makes a request to the address "https://beaconurl.com/path/beacon.jpg", the request is redirected with the HTTP code 30x (x = 1,2,3,5 or 7) to the address "https://beaconurl.com/path/beacon.php", which contains a script that allows the server to obtain the necessary information. The script is executed, in the address bar the user sees not the source link, but a link to the script. Such web beacons are not common and are replaced by more simple and reliable ones.

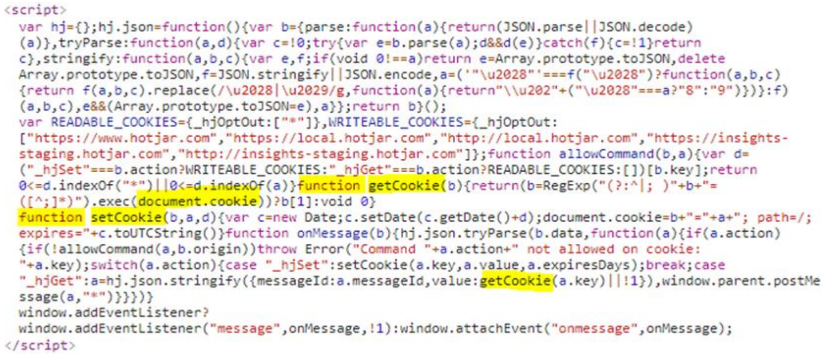
3. Iframe-beacons. They are the most "harmless" among all the others. They are to make sure that the user has viewed some content. Most of these beacons do not send information about the user to third-party servers. Used wherever a reliable collection of information is required. Web beacons-images are easily detected and disabled, since in most cases they are formatted in HTML-code according to some templates. To solve this problem, advertisers use Iframes inline frames [3]. The simplest examples of using Iframes are built-in web pages of audio/video players from third-party hosting websites. An inline frame is a certain area of a web page within which another webpage or its fragment is loaded, specified in the attributes of the <iframe> </iframe> paired tag. Navigation through this webpage (its fragment) is carried out regardless of navigation through the main webpage. A web beacon made in the form of the inline frame is an 1x1 pixel area imperceptible for the user, often with CSS style attributes that prevent it from being displayed, for example:

```
<iframe src="https://beaconurl.com/beacon.html" style="display: none; width: 1px; height: 1px; opacity: 0;"></iframe>
```

The beacon.html document contains executable JavaScript code.

Inline frames in the vast majority of cases contain an executable JavaScript code, which, among other things, contains instructions for creating and analyzing cookie files. It is relatively easy and efficient to use the inline frames for cross-domain tracking – to monitor the activity of a single user on several different domains, just one single inline frame is used. Cookies are different for different domains, even if they contain the same data.

The owner of several domains can track single user’s activities by analyzing his unique identifier stored inside different cookies saved by different websites but referred to the single domain that analyzes user activity, thus collecting any analytics necessary. A single frame can contain a script responsible for processing the transitions of the user across multiple domains - thus the script is responsible processing different cookies, which is impossible when using web beacons-images that do not execute any scripts and that belong to the single server on which each single of them is stored, regarding to the collecting of analytics. Figure 2 shows an example of a script placed in an Iframe-beacon.



```
<script>
  var hj={};hj.json=function(){var b={parse:function(a){return(JSON.parse||JSON.decode)
  (a)},tryParse:function(a,d){var c=!0;try{var e=b.parse(a);d&&d(e)}catch(f){c=!1}return
  c},stringify:function(a,b,c){var e,f;if(void 0!==a)return e=Array.prototype.toJSON,delete
  Array.prototype.toJSON,f=JSON.stringify||JSON.encode,a=('"\u2028"'===f("\u2028")?function(a,b,c)
  {return f(a,b,c).replace(/\u2028|\u2029/g,function(a){return"\\u202"+("\u2028"===a?"8":"9")})}:f)
  (a,b,c),e&&(Array.prototype.toJSON=e),a}};return b}();
  var READABLE_COOKIES={_hjOptOut:["*"]},WRITEABLE_COOKIES={_hjOptOut:
  ["https://www.hotjar.com","https://local.hotjar.com","http://local.hotjar.com","https://insights-
  staging.hotjar.com","http://insights-staging.hotjar.com"]};function allowCommand(b,a){var d=
  ("_hjSet"===b.action?WRITEABLE_COOKIES:"_hjGet"===b.action?READABLE_COOKIES:[])[b.key];return
  0<=d.indexOf("*")||0<=d.indexOf(a)}function getCookie(b){return(b=RegExp("(?:^|; )"+b+"=
  ([^;]*)").exec(document.cookie))?b[1]:void 0}
  function setCookie(b,a,d){var c=new Date;c.setDate(c.getDate()+d);document.cookie=b+"="+a+"; path=/;
  expires="+c.toUTCString()}function onMessage(b){hj.json.tryParse(b.data,function(a){if(a.action)
  {if(!allowCommand(a,b.origin))throw Error("Command "+a.action+" not allowed on cookie:
  "+a.key);switch(a.action){case "_hjSet":setCookie(a.key,a.value,a.expiresDays);break;case
  "_hjGet":a=hj.json.stringify({messageId:a.messageId,value:getCookie(a.key)||!1}),window.parent.postMe
  ssage(a,"*")}}})}
  window.addEventListener?
  window.addEventListener("message",onMessage,!1):window.attachEvent("onmessage",onMessage);
</script>
```

Figure 2. A JavaScript script that is executed once an iframe-beacon is uploaded. A document.cookie object if responsible for creating cookies even when they are disabled by a user through his browser settings.

4. DETECTING THE WEB BEACONS

In order to detect the built-in web beacon, the following distinctive features and features that indicate their essence were distinguished[3]:

1. The URL of the element differs from the URL of the webpage that contains the element. If the element embedded in the page has a URL that is different from the address of the current webpage, then most likely this element was implemented from the outside to collect information about the user.

2. The inline element has a tiny size that is 7 or fewer pixels. The presence of images, almost invisible to a user, and therefore not intended to convey any information to the user, means the intention to covertly carry out actions, including malicious.

3. The host named in element's URL is third party regarding to the URL of the page containing the element. Specically, this means that their two TLD(top-level domains), i.e., rightmost two dot-separated components, differ.

4. A list of all element's URLs contains either one URL that is longer than 100 characters, or several URLs each having a length greater than mu + 0.75sigma, where mu and sigma are the average and standard deviation of row sizes, which is not typical for conventional element(image) URLs. The presence of such an address indicates that the element does not belong to traditional image stores, but most likely to intruders.

5. The image URL appears once in the list of URLs of all images. If the set of addresses of all images on the page contains repeated URLs, this indicates that the page owner stores the images in one or more places. The presence of URLs that occur once in the entire set means that there are extraneous images that can be web beacons.

6. In the URL of the image, there are several substrings from the set "http", "https", "ftp", etc., denoting the URL scheme. For example, an image with the URL "http://pic.base.com/log/https://www.image.com" indicates that it may contain a web beacon, since this form of URL-address representation is atypical for most elements, which indicates the unnatural formation of this address, i.e. interference of intruders who introduced a web beacon.

5. THE MINIMIZATION OF THE WEB BEACONS TRACKING ACTIVITY

To identify a person, 33 bits of entropy are enough [4]. Peter Eckersley believes that information such as a city of residence, a person's sex, DOB is equal to 33 bits. Such an amount is enough to recognize the user. At present, there is a service called Panopticlick, which provides a numerical estimate of the degree of human identification from statistics collected using its web browser.

The outcome of the service's functioning in a Google Chrome 60 browser without applying any web beacon protection measures showed an entropy equal to 28.89, which is close to the value of 33 bits. This shows that to protect the user's privacy on the Internet, protection against invisible tracking is mandatory.

The following defense methods against the web beacons’ functioning were tested:

1. Blocking third-party cookies.

Effective against: web beacons that create cookies.

Ineffective against: web beacons that do not create cookies, regardless of their type.

Even after deleting cookies, the server is able to identify the user. This is possible thanks to the browser fingerprints technique. Based on parameters such as language settings, time zone, installed extensions, a dossier is created for a specific user.

And the more inventive the settings for the protection of the user, the more he will be recognized compared to users whose settings are set by default [5]. "Browser fingerprint" marks an Internet connection with a special label, which is equal to a certain hash sum, calculated using an algorithm, depending on the user's settings. Using this technique, you can not only restore deleted cookies, but also identify the user using a previously computed hash sum without leaving any traces. Filtering the incoming traffic through the firewall settings can be useful to prevent "browser fingerprints" collecting.

2. Using several web browsers.

Effective against: any kinds of web beacons.

The user uses, for example, two web browsers: one for social networks, everyday purposes, another for searching information on the Internet. As a result, the browser that is used by the user will not display targeted advertisements.

3. Surfing the Internet in the Incognito mode.
Effective against: some beacons that create cookies, iframe-beacons and a small amount of web beacons that collect several types of statistics.
Ineffective against: the majority of beacons that redirect requests, simple web beacons-images and script-beacons.

It is noteworthy that even in the incognito mode, the overall statistics of the browser (OS type, screen resolution and so on) are sent in HTTP requests to servers. The study showed that when working in incognito modes of web browsers, cookies are still created and stored on the user's computer, but they are deleted when the session is over in the browser. Disabling cookies in the browser’s settings does not give any result either.

The study consisted of visiting a web page with a newly installed browser with cookies enabled. After that, all the cookies were deleted and disabled in the browser's settings. Then again, the same web page was visited until it's complete loading. Table 1 shows that despite the cookies were formally disabled, they are still preserved, but in a much smaller amount.

Table 1 – Studying efficiency of disabling cookies while surfing the Internet

Blocking cookies disabled	Blocking cookies enabled
Cookie files saved on user’s PC (domains only) after visiting aliexpress.com	
aliexpress.com criteo.com facebook.com itao.com mc.yandex.ru ru.aliexpress.com ru.itao.com yandex.ru mmstat.com vk.com g.alicdn.com openx.net	aliexpress.com google.ru

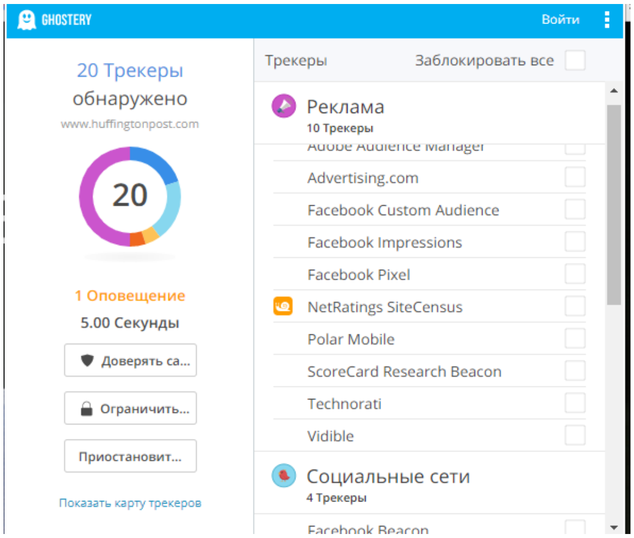
4. Disabling the execution of JavaScript code [6].
Effective against: iframe-beacons that contain scripts within themselves.
Ineffective against: all types of beacons, except iframe-beacons.
This can be useful against trackers that use the API to gain access to a third-party program. The API allows you to access any service. In addition, if the user is tracked using scripts written in JavaScript (as implemented, for example, in Google Analytics – when the website is loaded, some code is executed that loads a library from the Google Analytics website that performs user activity monitoring functions).

Disabling JavaScript prevents the execution of these scripts and, as a consequence, tracking the user. However, by blocking the execution of JavaScript scripts, there is a chance not to access some resources that use it for functioning.

5. Using browser extensions that allow to detect and block web beacons of different target orientation (advertising, tracking activity, and so on).

Effective against: the vast majority of web beacons-images, script-beacons, many iframe-beacons.
Ineffective against: unique varieties of web beacons that cannot be evaluated and identified.
One such extension is Ghostery. It to some extent emulates the Do Not Track standard developed by the World Wide Web Consortium and supported by most popular web browsers. According to the standard, a DNT header is added to HTTP requests, blocking the execution of all tracking technologies used by the server.

However, adding a header performs only a recommendatory function, the server does not have to adhere to the standard and may continue to use the tracking functionality. The extension detects and blocks most of the existing web beacons, including embedded in advertisements, subscription buttons, registration through social networks. For example, when visiting the website http://www.huffingtonpost.com, the extension showed 20 trackers found during the checking (Fig.3), the 5 among which are Facebook Beacons.



20 Трекеры
обнаружено
www.huffingtonpost.com

20

1 Оповещение
5.00 Секунды

Трекеры Заблокировать все □

Реклама
10 Трекеры

Adobe Audience Manager □
Advertising.com □
Facebook Custom Audience □
Facebook Impressions □
Facebook Pixel □
NetRatings SiteCensus □
Polar Mobile □
ScoreCard Research Beacon □
Technorati □
Vidible □

Социальные сети
4 Трекеры

Facebook Beacon □

Figure 3. An example of how the Ghostery extension for Google Chrome functions.

6. Using e-mail clients and servers that prohibit automatic downloading of images when opening a message [7].

Effective against: web beacons-images (it is impossible to estimate the inefficiency of a method, since only web beacons-images are exploited in e-mail).

For example, the e-mail service Gmail. A few years ago, most e-mail services assumed automatic downloading of images when opening letters, which allowed using web beacons in them. At this time, all images that appear in Gmail e-mails are pre-cached on Google servers. On the one hand, this excludes the downloading of malicious programs, and on the other hand this excludes the distribution of web beacons, as the publishers do not receive reliable information about who opened the letter. In web browsers, it is possible to disable the downloading of images without the user's prior consent, which, on the one hand, excludes the operation of image beacons, but at the same time affects the user's perception of websites.

7. Adding domains to the hosts file whose servers are tracking the user's activities.
Effective against: any web beacons whose URLs are blocked by the user.
Ineffective against: iframe-beacons containing scripts, and script beacons.
The most complicated and slow way, because firstly all the domain names of the servers which are tracking the user must be found, and then the hosts file must be edited manually. The same logic is applicable when configuring the firewall. Any beacons containing scripts are almost impossible to track up to the URL manually, as this requires proper skills and knowledge in programming languages and debugging web pages.

6. RESEARCHING THE QUANTITATIVE CHARACTERISTICS OF THE WEB BEACONS IMPLEMENTATION IN THE WEBSITES

6.1. Description of the method of data collecting

The 1000 most popular domains all over the world among the list called "The Majestic Million" were chosen for analysis. To process the list, a script was written in Python 3.6, which creates a proxy server by executing the methods and functions of the submodule "Server" of the Python module "browsermobproxy" and the submodule "webmodel" of the "selenium" Python module.

The script then launches a Mozilla Firefox 54 web browser through a special web driver and loads the requested webpage inside it. The data downloaded through the browser's running page, as well as all HTTP requests sent by the browser, together with the responses received from the servers, pass through a proxy server that collects them in the JSON format. The resulting JSON file is processed as follows:

- from the entire file using the "filter_entries()" method of the "HarPage" submodule of the Python module "haralyzer", the objects which describe images of any format and size are selected;
- each image found is downloaded by its URL, and its size is checked;
- if an image size equals to 1x1 pixels, its web address is stored, as well as other statistical information necessary for further processing.
- the domain of the web beacon found is additionally checked. If it coincides with the domain of the website on which it is located, it does not participate in the further consideration, since the 1st party web beacons are not usually designed to collect statistics about users. Only 3rd party beacons that are stored on 3rd party servers are taken into account.

Thus, the script processes all domains from the list. It is worth noting that the websites inaccessible in the territory of the Russian Federation were not processed and did not participate in the statistics. The browser, however, was specifically installed solely for data collection, additional settings or parameter changes were not made.

6.2. Data processing

The obtained data were processed, after which the graphs shown in Figures 4 and 5 were drawn.
First of all, web beacons-images were researched, as they make up the overwhelming majority among all other web beacons.

General statistics on the processed domains:

- amount of domains: 1000;
- amount of domains not containing web beacons: 193;
- amount of domains containing more than 10 web beacons: 238;
- total amount of processed images regardless of their properties: 41547;
- amount of 1st party web beacons-images: 350;
- amount of 3rd party web beacons-images: 12444;
- amount of providers of image beacons: 456.

At the same time there were web beacons of various formats. Most of them are in GIF format – 12125 pcs. Also PNG beacons – 297, JPEG beacons – 22 and BMP beacons – 4 were discovered. Information about the type of elements being downloaded is contained in the "Content-Type" header of server's response to HTTP GET-request from the browser. In the log files of the browser itself, information about the type of elements is stored in the "mimeType" field of statistics about all network requests made on this domain.

The server does not always respond to a browser request without errors or warnings. The HTTP status codes are responsible for showing this kind of information. The most common code is 200, which is shown after the item is loaded without any problems. Servers that implement script-beacons and beacons that masquerade as beacons-images are forced to send a response to the browser's request with codes from the series of 30x, where x = 1,2,3,4,5 or 7. This means that when the browser tries to load an item, the request is redirected to another element, which is typical only for beacons that masquerade as picture beacons, but ultimately execute PHP scripts. Therefore, the status codes for HTTP requests were also examined, based on which the following percentages were obtained:

- 200 «OK» – The request has succeeded – 95.14% – the situation inherent in beacons-images and iframe-beacons;
- 202 «Accepted» – The request has been accepted for processing, but the processing has not been completed – 0.03% – this code also means successful browser-server interaction;
- 302 «Found» – URI of requested resource has been changed temporarily – 4.77%;
- 303 «See Other» – Server sent this response to directing client to get requested resource to another URI with an GET request – 0.03%;
- 304 «Not Modified» – This is used for caching content – 0.03%.

It can be seen that the elements that sent responses with codes 302,303,304 to the browser's requests were found. These are beacons associated with the execution of scripts (except iframe beacons).

Let's draw a graph (Fig. 4) showing websites from among the investigated ones, which host the largest number of third-party web beacons. The ordinates mark the URLs of the sites studied, along the abscissa – the number of beacons relative to their total number.

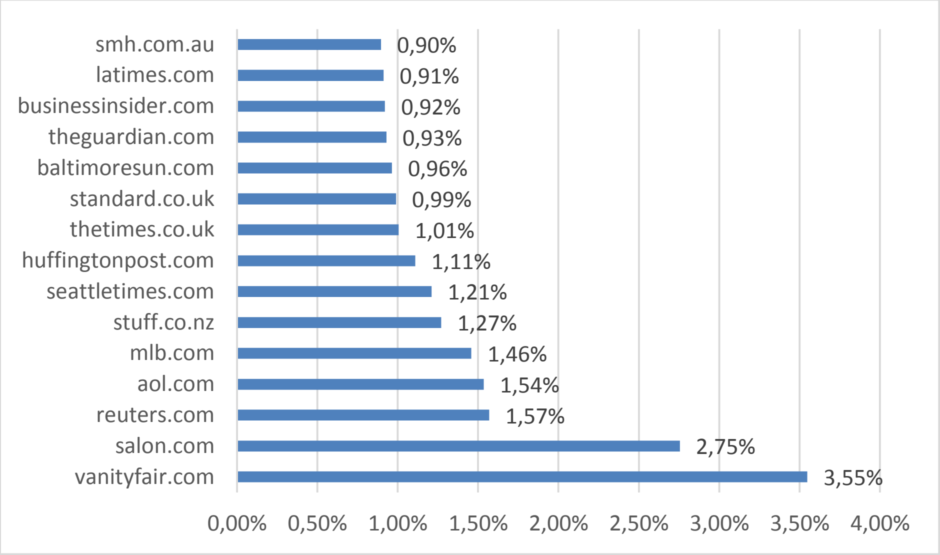


Figure 4. Websites containing the largest amount of web beacons.

The following graph (Fig. 5) shows the names of the providers whose number of beacons is the largest among all those considered. It is these providers that embed the largest number of beacons. The ordinates mark the domain names, and the abscissa axis marks the percentage of web beacons of the domain (aggregated) found on the studied websites (1000), relative to their total number (12444).

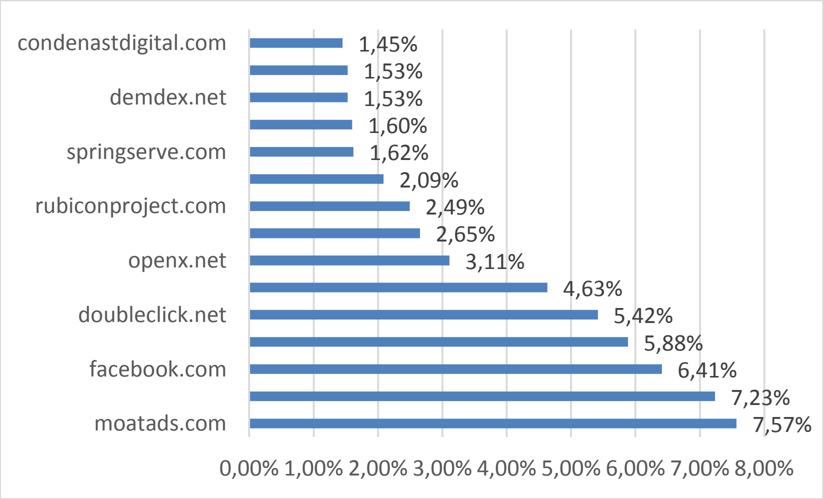
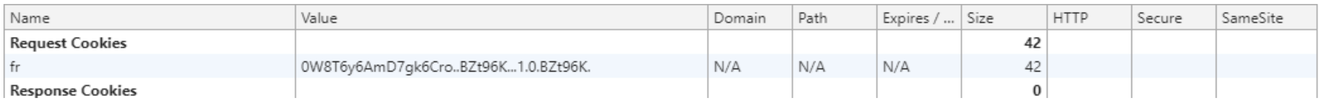


Figure 5. Providers that host the largest amounts of web beacons on websites.

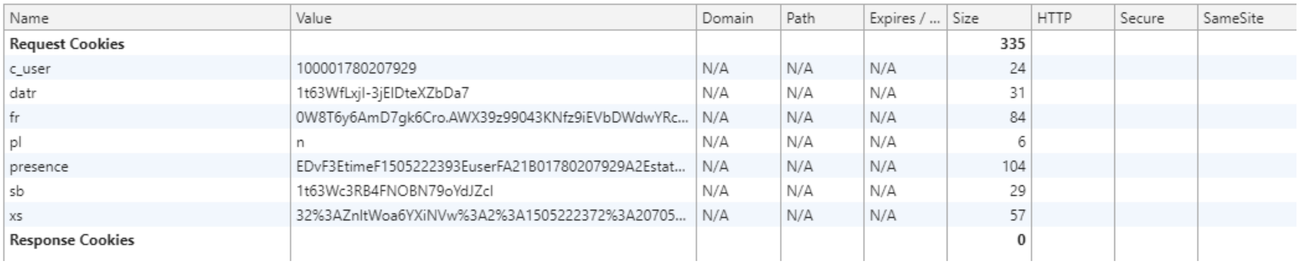
As can be seen in Figure 5, most providers are advertising or web analytics services. However, much of the web beacons are implemented by various social networks, in particular Facebook. These beacons represent the greatest danger if anonymity on the Internet is necessary, since if the user is authorized, then along with the beacon his personal information is transmitted.

Let's consider web beacons from Facebook more. As can be seen in Figure 5, their beacons occupy the third place among the total number. Facebook Beacons are used for cross-analytics, and every Facebook user can create his own beacon free of charge. When visiting a website having the Facebook Beacon, for example, https://vimeo.com, without authentification on Facebook, then a cookie with a single "key-value" field is created (Figure 6), after authentification, a cookie file with seven fields is created, among which is a user ID value (c_user key).



Name	Value	Domain	Path	Expires / ...	Size	HTTP	Secure	SameSite
Request Cookies					**42**			
fr	0W8T6y6AmD7gk6Cro..BZt96K...1.0.BZt96K.	N/A	N/A	N/A	42			
Response Cookies					**0**			

Figure 6. Cookies requested by Facebook Beacon without authorization on Facebook.



Name	Value	Domain	Path	Expires / ...	Size	HTTP	Secure	SameSite
Request Cookies					**335**			
c_user	100001780207929	N/A	N/A	N/A	24			
datr	1t63WfLxjl-3jEIDteXZbDa7	N/A	N/A	N/A	31			
fr	0W8T6y6AmD7gk6Cro.AWX39z99043KNfz9iEVbDWdwYRc...	N/A	N/A	N/A	84			
pl	n	N/A	N/A	N/A	6			
presence	EDvF3EtimeF1505222393EuserFA21B01780207929A2Estat...	N/A	N/A	N/A	104			
sb	1t63Wc3RB4FNOBN79oYdJZcl	N/A	N/A	N/A	29			
xs	32%3AZnltWoa6YXiNVw%3A2%3A1505222372%3A20705...	N/A	N/A	N/A	57			
Response Cookies					**0**			

Figure 7. Cookies requested by Facebook Beacon with authorization on Facebook.

In addition to Facebook, Google's beacons also collect data about users visiting different sites. In particular, DoubleClick.net also belongs to Google. After authorization on one of the Google services, DoubleClick beacons transmit DSID and IDE, which can identify the user. In this case, if there is no authorization, then the cookies are not transmitted at all.

8. CONCLUSION

Web beacons are a powerful tool for monitoring the activity of users on the Internet. Complementing and largely replacing cookies, web beacons can be elusive for both the users and for software that is intended to block them.

There is no one-size-fits-all approach that makes it possible to block all web beacons present on whatever resource, as well as there is no method that prevents the collection of the basic information provided by web browsers. Only 19% of the researched websites do not contain web beacons in the form in which they are usually embedded on websites, and on average one domain contains more than 10 elements that can be certainly recognized as the web beacons of various providers.

This shows the scale of tracking users on the Internet and explains the amount of the targeted advertisement shown on the most of the websites a common web user visits every day.

REFERENCES

1. Walther H., Santry P. CYA: Securing Exchange Server 2003 and Outlook Web Access, Proc. Syngress - 2004. PP.166-168.

2. Alsaid A., Martin D. "Detecting Web Bugs With Bugnosis: Privacy Advocacy Through Education", in: Lecture Notes in Computer Science. Dingledine R., Syverson P., Editors, Proc. LNCS Vol. 2482.

3. Fonseca F., Pinto R., Meira Jr. W. "Increasing User's Privacy Control Through Flexible Web Bug Detection", in: Third Latin American Web Congress (LA-WEB'2005), Proc. LA-WEB. - 2005. pp.1-13.

4. Eckersley P. "How unique is your web browser?" in Proceedings of the 10th International Conference on Privacy Enhancing Technologies, Proc. PETS'10. - 2010, pp. 2-3.

5. Negrini F. Who follows you on the Internet? https://www.kaspersky.ru/blog/web-tracking-in-numbers/11849/. Viewed: 2017, August.

6. Flanagan D. JavaScript: The Definitive Guide, 6th Edition, Proc. O'Reilly Media - 2011. PP. 1096

7. Frew J. How Advertisers Use Web Beacons to Track You on the Web and in Emails. http://www.makeuseof.com/tag/how-web-beacons-track-web/. Viewed: 2017, August.

Document Object Model Cross Site Scripting Vulnerability Testing

Kovalenko Oleksandr, Smirnov Oleksii, Smirnov Sergii, Kovalenko Anna

Central Ukrainian National Technical University
8, Universytetskyi, Kropyvnytskyi, Ukraine
Tel: +380502840472, e-mails: clashav@gmail.com, dr.smirnovoa@gmail.com,
smirnov.ser.81@gmail.com, annasun911@gmail.com

ABSTRACT

The paper presents research results and vulnerability testing algorithms for one of the most common types of attacks on Web-based applications - cross site scripting - XSS (Cross Site Scripting) - DOM XSS. Cross-site scripting is an error of validating user data, which allows to pass JavaScript code for execution in the user's browser. Attacks of this kind are often also called HTML injections, because the implementation mechanism is very similar to SQL injections, but unlike the latter, the implemented code is executed in the user's browser. The approach of mathematical modeling based on GERT-networks is chosen. The research has shown that GERT (Graphical Evaluation and Review Technique) is a method of studying and analyzing stochastic networks used to describe the logical relationship between parts of a project or process steps. The main goal of GERT is to evaluate the logic of the network and the duration of activity and to make a conclusion concerning the need to perform certain activities. A method for testing Web-applications and a corresponding set of mathematical models has been developed. The mathematical modeling is based on the GERT-network synthesis approach. As a result, mathematical models of the DOM XSS vulnerability testing method have been developed. The mathematical model of the DOM XSS vulnerability testing method differs from the known by taking into account the execution or analysis of the DOM structure. The developed method can be used when testing the vulnerability of a Web application.

Keywords: testing, vulnerability, network, security, attack, Web, application, stochastic, modeling

1. INTRODUCTION

At present, the high demand for Web-applications and Web-services causes a great interest of attackers in their possible vulnerabilities. At the same time, the main threats towards server components are transformed into attacks directed against ordinary users.

The analysis of the materials of the Open Web Application Security Project (OWASP TOP-10) showed that one of the most dangerous types of attacks (vulnerabilities) is cross-site scripting - XSS (Cross Site Scripting).

Analysis of the literature showed that cross-site scripting is an error in validating user data which allows to pass JavaScript code for execution in the user's browser. Attacks of this kind are often also called HTML injections, because the implementation mechanism is very similar to SQL injections, but unlike the latter, the implemented code is executed in the user's browser.

From works [1-8, 15-20] it is known that XSS usually means instant and deferred cross-site scripting. In case of instant XSS malicious code (Javascript) is returned by the attacked server immediately as a response to the HTTP request. Deferred XSS means that malicious code is stored on the attacked system and can later be embedded in the HTML page of the vulnerable system. This classification assumes that the fundamental property of XSS is that malicious code is sent from the browser to the server and returned to the same browser (instant XSS) or any other browser (deferred XSS).

A number of online articles give a detailed description of the main mechanisms of the emergence of this kind of threats, as well as ways of their possible blocking. However, in order to identify these threats and the possible consequences of their spread in the process of safe management of IT projects, and also to offer the best ways to solve this problem, there is a need for a mathematical formalization of the process of their initialization and distribution.

A particularly urgent task in this direction is the modeling of the DOM (Document Object Model) XSS vulnerability. This is due to the fact that the vulnerability of DOM XSS is a subtype of XSS, in case of which the result of the attack is not in the server's response and, therefore, not in the HTML code, but in the DOM structure of the HTML page. The results of such vulnerability attacks can be detected only when executing or analysing the DOM structure. The very mechanism of the attack, namely the injection of Javascript code into the vulnerable segment, remains unchanged.

The aim of this work is to create a vulnerability testing method for one of the most common types of attacks on Web applications - DOM XSS.

2. THE DOM XSS VULNERABILITY ANALYSIS ALGORITHM

For mathematical formalization of the algorithm of the DOM XSS vulnerability analysis we will use the main provisions of network GERT-modeling, described in detail in [9-12].

The algorithm for analyzing DOM XSS vulnerability can be described as follows:

1) All the <script> tags are extracted from the code of the analyzed page and then a list of tags for analysis is generated.

2) The contents of the tag are analyzed. If the tags do not contain code, but refer to a remote file, the file is accessed and the code is obtained from it. The contents of the file contain potentially unsafe parts of the code (sink) that use the client's input data (source).

Examples of sources may be:

- document.URL
- document.documentURI
- location.href
- location.search
- location.*
- window.name
- document.referrer

Examples of sink:

- document.write

- (element).innerHTML
- eval
- setTimout / setInterval
- execScript

3) If the tag code uses source, an attack with a certain marker is performed, which can be traced in the DOM page structure after the code execution (for example, injection of certain text content into the DOM) .

4) The contents of the DOM are checked. If there is a marker in the DOM as a result of the attack, it can be concluded that there is a DOM vulnerability.

5) Steps 2 - 4 are performed for each script tag on the page

To construct a formal model for the analysis algorithm of Web applications vulnerability to DOM XSS, a stochastic GERT network has been chosen

Studies have shown that GERT (Graphical Evaluation and Review Technique) is a method of studying and analyzing stochastic networks used to describe the logical relationship between parts of a project or process steps [9-12]. The main goal of GERT is to evaluate the logic of the network and the duration of activity and to make a conclusion about the need to perform certain activities.

GERT networks consist of nodes of type AND, INCLUSIVE-OR and EXCLUSIVE-OR, and arrows with two or more parameters. An arrow has a direction, it has a start node and an end node.

Arrow parameters contain:

1) the probability of completing an arrow (Pa), provided that the node which is the source of the arrow has been implemented;

2) the time (ta) of an arrow completion, if it is completed.

Time ta can be a random variable. If an arrow is not part of the network implementation, that is, during the process, the activity associated with the arrow does not occur, then ta = 0.

A node in a stochastic GERT network consists of an input function (a contributive function) and an exit function (a distributive function). Each of the functions is described by a certain logical relation to the connected arrows.

In general, the conducted studies have shown that GERT-modeling is an effective way of determining previously unknown laws and functions of random variables distribution under the known algorithm of functioning (process). That is why, GERT-modeling has been chosen as a tool for mathematical modeling.

3. GERT-MODEL OF THE METHOD OF DOM XSS VULNERABILITY TESTING

According to the presented description let us construct the GERT-model network of the method of testing DOM XSS vulnerability. A graphic representation of the GERT model is shown in Figure 1.

In the presented network, the nodes of the graph are interpreted by the states of the computer system during the functioning of the DOM structure, and the arrows of the graph are the probabilistic-temporal characteristics of the transitions between states. In particular, arrow (1, 2) characterizes the time of obtaining and analyzing the contents of the tag. The arrow (2,3) displays the time characteristics of the attack in case of availability of "source" structure. The arrow (2,4) specifies the random access time to the content of the remote file (search for "sink"). The arrow (4,2) characterizes the return to the execution of the attack. The arrow (3.5) describes the continuation of the attack, in particular, checking the contents of the DOM. Further, the arrow (5.6) characterizes the decision time for the vulnerability, while the arrow (5.1) displays the time characteristics of the transition to the new tag.

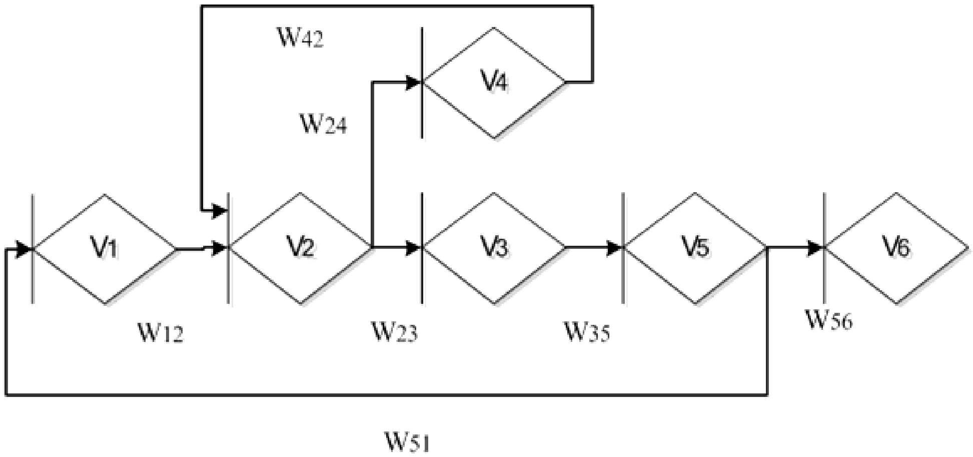


Figure 1. The GERT-model of the DOM XSS testing method

The characteristics of the arrows of the model are presented in Table. 1

Table 1 - Characteristics of the Model Arrows

№ п/п	Arrow	W-function	Probability	The moments generating function
	(1,2)	W_{12}	p1	$\lambda_1/(\lambda_1 - s)$
	(2,3)	W_{23}	p2	$\lambda_2/(\lambda_2 - s)$
	(2,4)	W_{24}	p3	$\lambda_3/(\lambda_3 - s)$
	(3,5)	W_{35}	p2	$\lambda_2/(\lambda_2 - s)$
	(5,6)	W_{56}	p4	$\lambda_4/(\lambda_4 - s)$
	(5,1)	W_{51}	1 – p4	$\lambda_5/(\lambda_5 - s)$
	(4,2)	W_{42}	p3	$\lambda_3/(\lambda_3 - s)$

The equivalent W-function of the execution time of the DOM XSS vulnerability testing method is:

$$W_E(s) = \frac{W_{12}W_{23}W_{35}W_{56} + W_{12}W_{24}W_{42}W_{23}W_{35}W_{56}}{1 - W_{12}W_{23}W_{35}W_{51} - W_{12}W_{24}W_{42}W_{23}W_{35}W_{51}} =$$

$$= \frac{p_1 p_2^2 \lambda_1 \lambda_2^2 \left(p_4 \lambda_4 (\lambda_3 - s)^2 (\lambda_5 - s) + p_3^2 q_1 \lambda_3^2 \lambda_5 (\lambda_4 - s)\right)}{(\lambda_4 - s)\begin{pmatrix} (\lambda_1 - s)(\lambda_2 - s)^2 (\lambda_3 - s)^2 (\lambda_5 - s) - \\ - p_1 \lambda_1 p_2^2 \lambda_2^2 q_1 \lambda_5 (\lambda_3 - s)^2 - p_1 p_2^2 p_3^2 \lambda_1 \lambda_2^2 q_1 \lambda_3^2 \lambda_5 \end{pmatrix}}, \qquad (1)$$

where $1 - p_4 = q_1$.

The peculiarity of the process under consideration lies in the heterogeneity of the analyzed and processed data. In this case, different cases of feedback organization are possible. In Fig. 1 these cycles are fixed in the form of transitions, $W_{12} \to W_{24} \to W_{42}$, $W_{12} \to W_{23} \to W_{35} \to W_{51}$.

For GERT-networks with loops there are no simple methods for finding singular points of the function $\Phi_{\text{Å}}(z)$ of replacing real variables $(z = -i\varsigma)$, where ς is a real variable. This is due to the fact that in order to find singular points it is necessary to solve nonlinear equations, and the more complex the structure of the GERT-network, the more complex the initial equation. Therefore, during the modelling, it is proposed to resort to such a replacement.

Performing a complex transformation $z = -s$, we get

$$\Phi(z) = \frac{uz^3 + vz^2 + bz + k}{(\lambda_4 + z)(z^6 + cz^5 + dz^4 + gz^3 + hz^2 + wz + m)}, \tag{2}$$

where:

$u = -p_1 p_2^2 p_4 \lambda_1 \lambda_2^2 \lambda_4$,

$v = p_1 p_2^2 p_4 \lambda_1 \lambda_2^2 \lambda_4 (\lambda_5 + 2\lambda_3)$,

$b = -p_1 p_2^2 p_4 \lambda_1 \lambda_2^2 \lambda_4 \lambda_3 (2\lambda_5 - \lambda_3)$,

$k = -p_1 p_2^2 \lambda_1 \lambda_2^2 \lambda_3^2 \lambda_4 \lambda_5 (p_4 + p_3^2 q_1)$,

$\tilde{n} = \lambda_1 + 2\lambda_2 + 2\lambda_3 + \lambda_5$,

$$d = -(2\lambda_3\lambda_5 + \lambda_1\lambda_5 + 2\lambda_2\lambda_5 + \lambda_3^2 + \\ + 2\lambda_1\lambda_3 + 4\lambda_2\lambda_3 + 2\lambda_1\lambda_2 + \lambda_2^2),$$

$$g = \lambda_3^2\lambda_5 + 4\lambda_1\lambda_2\lambda_5 + 4\lambda_2\lambda_3\lambda_5 + \lambda_2^2 + \lambda_3^2\lambda_1 + \\ + 2\lambda_3^2\lambda_2 + 4\lambda_1\lambda_2\lambda_3 + 2\lambda_2^2\lambda_3 + \lambda_2^2\lambda_1,$$

$$h = -(\lambda_1\lambda_3^2\lambda_5 + 2\lambda_2\lambda_3^2\lambda_5 + 4\lambda_1\lambda_2\lambda_3\lambda_5 + 2\lambda_2^2\lambda_3\lambda_5 + \\ + \lambda_2^2\lambda_3^2 + 2\lambda_1\lambda_2^2\lambda_3 - p_1 p_2^2 q_1 \lambda_1 \lambda_2 \lambda_5),$$

$$w = \lambda_1\lambda_2\lambda_3^2\lambda_5 + \lambda_2^2\lambda_3^2\lambda_5 + 2\lambda_1\lambda_2^2\lambda_3\lambda_5 + \\ + \lambda_1\lambda_2^2\lambda_3 - 2p_1 p_2^2 q_1 \lambda_1 \lambda_2 \lambda_3 \lambda_5,$$

$m = p_1 p_2^2 q_1 \lambda_1 \lambda_2 \lambda_3^2 \lambda_5 + p_1 p_2^2 p_3 q_1 \lambda_1 \lambda_2^2 \lambda_3^2 \lambda_5 - \lambda_1 \lambda_2^2 \lambda_3 \lambda_5$.

The distribution density of the time probabilities of the execution of the DOM XSS vulnerability analysis algorithm:

$$\varphi(x) = \frac{1}{2\pi i} \int_{-i\infty}^{i\infty} e^{zx} \frac{uz^3 + vz^2 + bz + k}{(\lambda_4 + z)\begin{pmatrix} z^6 + cz^5 + dz^4 + \\ + gz^3 + hz^2 + wz + m \end{pmatrix}} dz, \tag{3}$$

where the integration operation is performed using the Bromwich-Wagner integral [13] The method of integration depends on whether the function $\Phi(z)$ has only simple poles, or poles of some order. In the case when the function $\Phi(z)$ has only simple poles, the expression $\mathring{a}^{zx}\Phi(z)$ can be represented as follows:

$$e^{zx}\Phi(z) = \frac{e^{zx}\left(\mathrm{u}z^3 + vz^2 + bz + k\right)}{z^7 + \gamma_6 z^6 + \gamma_5 z^5 + \gamma_4 z^4 + \gamma_3 z^3 + \gamma_2 z^2 + \gamma_1 z + \gamma_0} = \frac{\mu(z)}{\psi(z)}, \tag{4}$$

where:

$\gamma_6 = \lambda_4 + c$,

$\gamma_5 = c\lambda_4 + d$,

$\gamma_4 = d\lambda_4 + g$,

$\gamma_3 = g\lambda_4 + h$,

$\gamma_2 = h\lambda_4 + w$,

$\gamma_1 = w\lambda_4 + m$,

$\gamma_0 = m\lambda_4$.

Then the density of the execution time distribution of the DOM XSS vulnerability analysis algorithm is:

$$\begin{aligned} \varphi(x) &= \sum_{k=1}^{7} \operatorname{Re}s\left[e^{zx}\Phi(z)\right] = \sum_{k=1}^{7} \frac{\mu(z_k)}{\psi(z_k)} = \\ &= \sum_{k=1}^{7} \frac{e^{zx}\left(\mathrm{u}z^3 + vz^2 + bz + k\right)}{7z_k^6 + 6\gamma_6 z_k^5 + 5\gamma_5 z_k^4 + 4\gamma_4 z_k^3 + 3\gamma_3 z_k^2 + 2\gamma_2 z_k + \gamma_1}. \end{aligned} \tag{5}$$

The function $\Phi(z)$, in addition to the solutions determined by the roots of the equation $z^6 + cz^5 + dz^4 + gz^3 + hz^2 + wz + m = 0$, may have a second- or third-order pole in those cases where the value λ_4 is equal to the value of the roots z_2, z_3, z_4, z_5, z_6, z_7. In these cases, the distribution density of the message transmission time $\varphi(x)$ is found by the formula for finding the residues r_{-1} from the poles z_k of the order n:

$$r_{-1} = \frac{1}{(n-1)!} \lim_{z \to z_k} \frac{d^{n-1}\left((z - z_k)^n e^{zx}\Phi(z)\right)}{dz^{n-1}}. \tag{6}$$

Expression (6) is a fractional-rational function relative to z with the degree of the denominator greater than the degree of the numerator. Therefore, the conditions of the Jordan lemma are satisfied for it [13]. The function $\Phi(z)$ has poles at points $z_1 = -\lambda_4$.

The polynomial: $z^6 + cz^5 + dz^4 + gz^3 + hz^2 + wz + m$ generates seven more poles. The solution of equation:

$$z^6 + cz^5 + dz^4 + gz^3 + hz^2 + wz + m = 0 \tag{7}$$

can be found by any method, for example, according to the formulas of Viet [13]. As a result, special points z_2, z_3, z_4, z_5, z_6, z_7 are calculated.

Thus, based on the exponential GERT network, a mathematical model for the analysis algorithm of DOM XSS vulnerability has been developed. This model differs from the known by taking into account the execution or analysis of DOM structure.

The model can be used to study processes in computerized systems, when developing new data protection tools and protocols.

The use of exponential stochastic GERT models will make it possible to use the results obtained in analytical form (functions, distribution densities) for comparative analysis and research of more complex computer systems by mathematical methods.

4. CONCLUSION

In this research a set of mathematical models of the method for testing WEB-applications has been developed. The basis of the mathematical modeling is the GERT-network synthesis approach. As a result, mathematical models of the DOM XSS vulnerability testing method have been developed.

The mathematical model of the DOM XSS vulnerability testing method differs from the known by taking into account the execution or analysis of DOM structure, which makes it possible to carry out an analytical assessment of the time spent on testing this vulnerability in the context of implementing strategies of development of secure software

In the course of the study of the presented models, it was found that the random value of the execution time of the test methods in question generally corresponds to the gamma distribution. Verification of this hypothesis is based on Pearson's criterion χ^2.

REFERENCES

1. About The Open Web Application Security Project – OWASP: [Електронний ресурс]. – Режим доступу: https://www.owasp.org/index.php/About_ The_Open_Web_Application_ Security_Project.

2. OWASP Top 10 – 2017 RC1: [Електронний ресурс]. – Режим доступу: https://github.com/OWASP/Top10/blob/master/2017/OWASP%20Top%2010%20-%202017%20RC1-English.pdf.

3. Positive Research 2016: [Електронний ресурс]. – Режим доступу: https://www.ptsecurity.com/upload/ptru/analytics/Positive-Research-2016-rus.pdf.

4. OSSTMM 3 – The Open Source Security Testing Methodology Manual. Contemporary Security Testing And Analysis: [Електронний ресурс]. –Режим доступу: http://www.isecom.org/mirror/OSSTMM.3.pdf.

5. Testing for DOM-based Cross-site scripting (OTG-CLIENT-001) – OWASP: [Електронний ресурс]. – Режим доступу: https://www.owasp.org/index.php/Testing_for_DOM-based_Cross_site_scripting_(OTG-CLIENT-001).

6. Testing for SQL Injection (OTG-INPVAL-005) – OWASP: [Електронний ресурс]. – Режим доступу: https://www.owasp.org/index.php/103 Testing_for_SQL_Injection_(OTG-INPVAL-005).

7. Cohen W., Ravikumar P., Fienberg S. A Comparison of String Metrics for Matching Names and Records [Электронный ресурс] / William W. Cohen, Pradeep Ravikumar, Stephen E. Fienberg.

Режим доступа: https://www.cs.cmu.edu/afs/cs/Web/People/wcohen/postscript/kdd-2003-match-ws.pdf.

8. Kevin Dreßler A., Axel-Cyrille Ngonga Ngomo On the Efficient Execution of Bounded Jaro-Winkler Distances / Semantic Web – Interoperability, Usability, Applicability an IOS Press Journal Электронный ресурс http://www.semantic-web-journal.net/system/files/swj944.pdf

9. Pritsker A. A. B. GERT: Graphical Evaluation and Review Technique. Part I. Fundamentals / Pritsker A. A. B., Happ W. W. // The Journal of Industrial Engineering (May 1966). pp. 267-274.

10. Pritsker, A. A. B. Modeling and analysis using Q-GERT networks / Pritsker, A. A. B. – New York: Wiley : Distributed by Halsted Press, 1979 – 435 p.

11. Семенов С.Г. Gert-модель прогнозування параметрів функціональної безпеки технічних систем / С.Г.Семенов, Гавриленко С.Ю., Кассем Халіфе // Зб. наукових праць. Системи обробки інформації. – Х.: ХУ ПС, 2016. – Вип. 2(139) С.50-52.

12. Semenov S.G., Zmiyevskaya V N., Kassem Khalife Development of Gert model of management system by using test cases // Journal of Qafqaz university-mathematics and computer science 2016, Vol.(4), № 1 С. 52-59

13. Эдвардс Г. Последняя теорема Ферма. Генетическое введение в алгебраическую теорию чисел / Г. Эдвардс. – М.: Мир, 1980. – 486 с.

14. Гмурман В.Е. Теория вероятностей и математическая статистика / В.Е. Гмурман. – М.: Высшая школа, 2003. – 479 с.

15. Коваленко А.В. Методы качественного анализа и количественной оценки рисков разработки программного обеспечения / А.А. Смирнов, А.В. Коваленко // Збірник наукових праць "Системи обробки інформації". – Випуск 5(142). – Х.: ХУПС – 2016. – С. 153-157.

16. Коваленко А.В. Проблемы анализа и оценки рисков информационной деятельности / А.А. Смирнов, А.В. Коваленко, Н.Н. Якименко, А.П. Доренский // Збірник наукових праць "Системи обробки інформації". – Випуск 3(140). – Х.: ХУПС – 2016. – С. 40-42.

17. Коваленко А.В. Метод качественного анализа рисков разработки программного обеспечения / А.А. Смирнов, А.В. Коваленко, Н.Н. Якименко, А.П. Доренский // Наука і техніка Повітряних Сил Збройних Сил України. – Випуск 2(23). – Харків: ХУПС. – 2016. – С. 150-158.

18. Коваленко А.В. Метод количественной оценки рисков разработки программного обеспечения / А.А. Смирнов, А.В. Коваленко, Н.Н. Якименко, А.П. Доренский // Збірник наукових праць Харківського університету Повітряних Сил. Випуск 2 (47). – Харків: ХУПС. – 2016. – С. 128-133.

19. Коваленко А.В. Использование псевдобулевых методов бивалентного программирования для управления рисками разработки программного обеспечения / А.А. Смирнов, А.В. Коваленко // Системи управління, навігації та зв’язку. – Випуск 1 (37). – Полтава: ПолтНТУ. – 2016. – С. 98-103.

20. Коваленко А.В. Метод управления рисками разработки программного обеспечения / А.В. Коваленко // Системи управління, навігації та зв’язку. – Випуск 2 (38). – Полтава: ПолтНТУ. – 2016. – С. 93-100.

Using the Multidimensional Matrices in Cryptography

Zgureanu Aureliu

Academy of Economic Studies of Moldova
61, Banulescu-Bodoni str., Chisinau, MD-2005, Republic of Moldova
Tel: 37379234829, e-mail: aurelzgureanu@gmail.com

ABSTRACT

This paper contains a synthesis of researches in the field of multidimensional matrices and multi-ary relations. These researches have led to the development of a large prime number generator and proving a series of properties of Boolean functions represented by the subsets of column which have permitted to develop some information encryption algorithms based on the multidimensional matrices. A more detailed explanation of these algorithms can be found in the following works: [5], [6], [8], [9], [10].

Keywords: multidimensional, matrix, n-ary relation, prime, number, encryption, system, key, generation.

1. MULTIDIMENSIONAL MATRICES

1.1. Relations on the sets

Let two finite sets $X=\{x_1,x_2,...,x_m\}$ and $Y=\{y_1,y_2,...,y_n\}$.

Definition 1. *A binary relation* on *X* and *Y* (denoted by R_{XY} or $X \to Y$) is called a subset of the Cartesian product $X \times Y=\{(x_1,y_1),(x_1,y_2),...,(x_m,y_n)\}$.
The relationship can be represented by a two-dimensional matrix

$$A=(a_{ij})_{m\times n}=\begin{array}{c|ccccc|} & 1 & \cdots & j & \cdots & n \\ \hline 1 & a_{11} & \cdots & a_{1j} & \cdots & a_{1n} \\ \vdots & \vdots & & \vdots & & \vdots \\ i & a_{i1} & \cdots & a_{ij} & \cdots & a_{in} \\ \vdots & \vdots & & \vdots & & \vdots \\ m & a_{m1} & \cdots & a_{mj} & \cdots & a_{mn} \\ \hline \end{array}, \text{ where } a_{ij}=\begin{cases} 1, \mathit{if}\ (x_i,y_j)\in R_{XY}, \\ 0, \mathit{if}\ (x_i,y_j)\notin R_{XY}. \end{cases}$$

Lines and columns are associated only with the indices of elements, often with the elements themselves. This matrix can also be written in another form:

$$A=\begin{array}{|c|c|} \hline XY & a_{ij} \\ \hline 11 & a_{11} \\ \vdots & \vdots \\ ij & a_{ij} \\ \vdots & \vdots \\ mn & a_{mn} \\ \hline \end{array}$$

By analogy with the definition of common two-dimensional matrices we define the multidimensional matrix.

Definition 2. A system *A* of $N_A = n_1 n_2 n_3 \cdot ... \cdot n_p$ elements $a_{i_1 i_2 i_3 ... i_p}$ ($i_\alpha = 1,2,3,..., n_\alpha$; $\alpha = 1,2,3,..., p$) that belong to the set Ω and are placed in the points of *p*-dimensional space of coordinates $i_1, i_2, ..., i_p$, is called a multidimensional matrix over the set **Ω**. The number *p* is called the size of the matrix and shows the number of indexes in the notation of the matrix elements. Size N_A shows the total number of elements in this matrix. Size n_α of the index i_α shows how many values (from 1 to i_α) this index runs. So in this paper, a multidimensional matrix is a direct generalization of the usual two-dimensional matrix.

By analogy with binary relation the *n*-ary relation on *n* sets $X_1 = \{x_{11}, x_{12}, ..., x_{1m_1}\}, \ldots,$ $X_2 = \{x_{21}, x_{22}, ..., x_{2m_2}\}$, ..., $X_n = \{x_{n1}, x_{n2}, ..., x_{nm_n}\}$ is a subset of the Cartesian product $X_1 \times X_2 \times ... \times X_n$, denoted by $R_{X_1 X_2 ... X_n}$ [7], [8]. So $R_{X_1 X_2 ... X_n} \subseteq X_1 \times X_2 \times ... \times X_n$, and the elements of $R_{X_1 X_2 ... X_n}$ represent some corteges $(x_{j_1}, x_{j_2}, ..., x_{j_n})$ of size *n* where $x_{j_i} \in X_i$, $i = \overline{1, n}$. The matrix od this relation is an *n*-dimensional matrix which have the form:

$$A = (a_{j_1 j_2 \cdots j_n})_{m_1 \times .. \times m_n} = \begin{array}{cccc|c} X_1 & X_2 & \cdots & X_n & a_{j_1 j_2 \cdots j_n} \\ \hline 1 & 1 & \cdots & 1 & a_{11...1} \\ \vdots & \vdots & \cdots & \vdots & \vdots \\ j_1 & j_2 & \cdots & j_n & a_{j_1 j_2 \cdots j_n} \\ \vdots & \vdots & \cdots & \vdots & \vdots \\ m_1 & m_2 & \cdots & m_n & a_{m_1 m_2 ... m_n} \\ \hline \end{array},$$

where $a_{j_1 j_2 \cdots j_n} = \begin{cases} 1, \ if \ (x_{j_1}, x_{j_2}, ..., x_{j_n}) \in R_{X_1 X_2 ... X_n} \\ 0, \ if \ (x_{j_1}, x_{j_2}, ..., x_{j_n}) \notin R_{X_1 X_2 ... X_n} \end{cases}$, $j_1 \in \{1, ..., m_1\}, ..., j_n \in \{1, ..., m_n\}$.

This matrix can also be written as a two-dimensional matrix:

$$A = \begin{bmatrix} a_{11\ldots1} & a_{11\ldots2} & \cdots & a_{1m_2\ldots m_n} \\ a_{21\ldots1} & a_{21\ldots2} & \cdots & a_{2m_2\ldots m_n} \\ . & . & . & . \\ a_{m_11\ldots1} & a_{m_11\ldots2} & \cdots & a_{m_1m_2\ldots m_n} \end{bmatrix}.$$

In general, elements of matrix A may be of arbitrary origin and $\Omega = \{\omega_1, \omega_2,.., \omega_m\}$, where ω_i can be other than 0 or 1. A particular case of this matrix represents the three-dimensional matrices which can be represented geometrically in the space $\mathbf{R}^3$ as is shown in the Figure 1. This matrix represents the relation $R_{X_1X_2X_3}$ on the sets $X_1 = \{x_{11}, x_{12}, x_{13}, x_{14}\}$, $X_2 = \{x_{21}, x_{22}\}$ and $X_3 = \{x_{31}, x_{32}, x_{33}\}$ with elements which belong to $\Omega = \{M, O, T\}$. It corresponds to the matrix which is represented in the Figure 2.

1.2. Sets of relations

Using the multidimensional matrices we can represent the subsets of relations [2], [7], [8], [24]. Let a family of sets $X = \{X_1,..., X_n\}$ and the set $\Omega = \{\omega_1, \omega_2,.., \omega_m\}$, where all ω_i are arbitrary elements. On this family are defined k relations:

$$R_j = R_{X_{j_1},...,X_{jd_j}},\ 2 \le d_j \le n,\ j = \overline{1,k},\ j_1, j_2,..., j_d \in \{1,2,...,n\}.$$

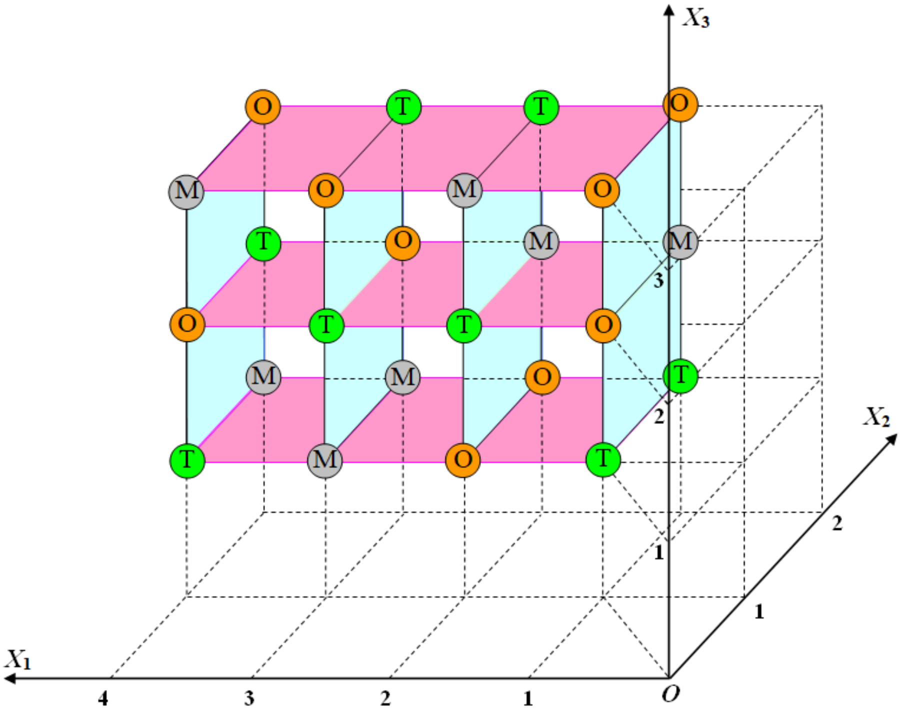


Figure 1. A sample of a three-dimensional matrix

The elements of the matrices of these relations belong to Ω. Denote by $\vec{R}$ the vector (cortege) with the coordinates $R_j : \vec{R} = (R_1,...,R_j,..,R_k)$. To this vector we associate an *n*-dimensional matrix

$$A_R = \Phi(\vec{R}),$$

according to the rule shown in Figure 3 [7], [8], [9], [11].

$A =$

		X_3		
X_1	X_2	1	2	3
1	1	T	O	M
1	2	M	T	O
2	1	O	T	M
2	2	O	M	T
3	1	M	T	O
3	2	M	O	T
4	1	T	O	M
4	2	M	T	O

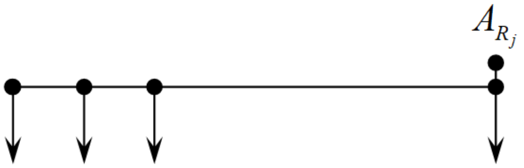
Figure 2. The representations of a three-dimensional matrix

In figure 3 the matrix A_{R_j} of the relations $R_j = R_{X_b X_c X_a}$ from the set of relations is presented and $r_{ij} = r_{i_b i_c i_a}$ is an element of this matrix. Thus the elements of the *n*-dimensional matrix representing the set of relations are the vectors $\vec{r}_i = (r_{i1},..., r_{ij},..., r_{ik}),\ i = \overline{1,u}$ whose coordinates are elements of the matrices of the relations on the sets from *X*. At the same time the coordinates of these vectors are also elements of the set $\Omega = \{\omega_1,...,\omega_m\}$. We denote the elements of this set according to the substitution $\begin{pmatrix} \omega_1 & \omega_2 & \cdots & \omega_m \\ 0 & 1 & \cdots & m-1 \end{pmatrix}$. As a result of this substitution to the vector $\vec{r}_i$ corresponds a number $a_{i_1...i_n}$ in the base *m*. Converting it to base 10 we get

$$a_{i_1...i_n} = \sum_{j=1}^{k} r_{ij} \cdot m^{k-j},\ i = \overline{1,u}.$$

Thus, the transformation $A_R = \Phi(\vec{R})$ puts into correspondence to set $\vec{R}$ a vector $\vec{A} = (a_{11...1},...,a_{m_1...m_n})$ [7], [8], [9]:

$$\vec{A} = \Phi(\vec{R})$$



$$A_R = \begin{array}{ccc} \begin{array}{cccccccc} & X_1 & \cdots & X_a & X_b & X_c & \cdots & X_n \end{array} & \begin{array}{ccccc} 1 & \cdots & j & \cdots & k \end{array} & a_{i_1 \ldots i_n} \\ \begin{pmatrix} 1 & 1 & \cdots & 1 & 1 & 1 & \cdots & 1 \\ \vdots & . & . & . & . & . & . & . \\ i & i_1 & \cdots & i_a & i_b & i_c & \cdots & i_n \\ \vdots & . & . & . & . & . & . & . \\ u & u_1 & \cdots & u_a & u_b & u_c & \cdots & u_n \end{pmatrix} & \begin{pmatrix} r_{11} & \cdots & r_{1j} & \cdots & r_{1k} \\ & & \ddots & & \\ r_{i1} & \cdots & r_{ij} & \cdots & r_{ik} \\ & & \ddots & & \\ r_{u1} & \cdots & r_{uj} & \cdots & r_{uk} \end{pmatrix} & \begin{pmatrix} a_{1\ldots1} \\ \vdots \\ a_{i_1 \ldots i_n} \\ \vdots \\ a_{u_1 \ldots u_n} \end{pmatrix} \end{array}$$

Figure 3. A correspondence rule $A_R = \Phi(\vec{R})$

The representation of the sets of relations by the multi-dimensional matrices allows us to try solving the issue of compressing information and to efficiently performing operations with large-scale systems [3]. Depending on the elements of the matrices of these relations [1] and of the set Ω we obtain different corteges $\vec{A}$. Inverse transformation $\vec{R} = \Phi^{-1}(\vec{A})$ is not unambiguous and, because of this, knowing only the cortege $\vec{A}$ is difficult to find the cortege $\vec{R}$. There are particular cases where the problem is solved and this involves some practical applications [4].

2. APPLICATIONS OF THE MULTIDIMENSIONAL MATRICES

2.1. Generating of the large prime numbers

The large prime numbers are widely used in cryptography, for example in public key encryption algorithms or in the digital signature generation. At the same time, these numbers are generated using probabilistic algorithms (considered, however, sufficiently secure for such purposes). However, the multidimensional matrices allowed the development of a deterministic algorithm (non-probabilistic) for large prime number generating [5]. The algorithm is based on a particular case in which inverse transformation can be calculated unequivocally. As a result a multidimensional matrix is obtained and it can be projected on a two-dimensional matrix:

$$A = \begin{array}{c} K_0 \\ K_1 \\ K_2 \\ \vdots \\ K_{m-1} \end{array} \begin{bmatrix} 0 & m+0 & 2m+0 & \cdots & m^n-(m-0) \\ 1 & m+1 & 2m+1 & \cdots & m^n-(m-1) \\ 2 & m+2 & 2m+2 & \cdots & m^n-(m-2) \\ \vdots & \vdots & \vdots & \cdots & \vdots \\ m-1 & m+(m-1) & 2m+(m-1) & \cdots & m^n-1 \end{bmatrix}$$

In this two-dimensional matrix according to Legendre's theorem, prime numbers are distributed only in some of the rows and have an increased density on these rows. This allows us to build prime numbers with certain useful properties for cryptography [5].

Let the number *m* represented in canonical form as the product of primes factors $m = p_1^{\lambda_1} p_2^{\lambda_2} \dots p_k^{\lambda_k}$, where p_i are prime numbers, $i = \overline{1,k}$ and λ_i – the multiplicity of the factor p_i. According to Legendre's theorem, the line contains an infinite number of prime numbers only if *m* and *i* are mutually prime. The number of these lines equals Euler's function $\varphi(m)$.

The prime numbers are unevenly distributed in the set of the natural number. We often encounter the problem of determining intervals with a higher "density" of prime numbers. By modifying the vector $\vec{R}$ we can modify the contents of the rows and the number of their elements remains the same. To solve this and some other problems are used Boolean functions in the context of the relations on sets.

2.2. The representing of the Boolean functions by the subsets of column

Boolean functions are also an important element in the development of the encryption systems. Especially interesting is the so-called bent functions, which differ from other Boolean functions in that they are far from linearity. Researching bent functions in traditional form (canonical or algebraic) is often quite difficult. The representation of the Boolean functions by the subsets of column can help us to simplify this research. This representation of Boolean function is based on multi-ary relations.

Let a Boolean function $F(x_1,...,x_\tau,...,x_n)$ where the function F and the variables $x_1,...,x_\tau,...,x_n$ can take only two values: 0 or 1. This function is an *n*-ary relation R_{X^n}, where $X = \Omega = \{0,1\}$.

In accordance with [10] on the set $X = \{x_1,...,x_n\}$ we build the partition $\{\tilde{X}_1, \tilde{X}_2\} = \{\{x_1,...,x_\tau\}, \{x_{\tau+1},...,x_n\}\}$. We build others two sets: $Y = \{y_0, y_1,.., y_{2^\tau-1}\}$ (consisting of the binary states corresponding to the variables from $\tilde{X}_1$) and $Z = \{z_0, z_1,...,z_{2^{n-\tau}-1}\}$ (consisting of the binary states corresponding to the variables from $\tilde{X}_2$). Then the Boolean function can be considered a binary relation between the sets *Y* and *Z* which has the matrix

$$R_{YZ}=\begin{array}{c|ccccc|} & z_0 & \cdots & z_j & \cdots & z_p \\ y_0 & a_{00} & \cdots & a_{0j} & \cdots & a_{0p} \\ \vdots & & & \ddots & & \\ y_i & a_{i0} & \cdots & a_{ij} & \cdots & a_{ip} \\ \vdots & & & \ddots & & \\ y_m & a_{m0} & \cdots & a_{mj} & \cdots & a_{mp} \end{array},$$

$$m=2^{\tau}-1,\ p=2^{n-\tau}-1,\ \forall i,j\ \ a_{ij}=\begin{cases}1, if\ F(y_i,z_j)=1,\\ 0, if\ F(y_i,z_j)=0.\end{cases}$$

Definition 3. The subset $S_{F^{\varepsilon}}^{z_j}$ of the set Y

$$S_{F^{\varepsilon}}^{z_j}=\{y_i:\forall y_i\in Y, F(y_i,z_j)=\varepsilon, \varepsilon\in\{0,1\}\}$$

Is called a *subset of column* of the function $F(x_1,...,x_n)$ for the column z_j.

The Boolean function can be represented by the *table of the subsets of column* (table 1):

Table 1. The table of the subsets of column of a Boolean function

	z_0	$\ldots$	z_j	$\ldots$	z_p
F^1	$S_{F^1}^{z_0}$	$\ldots$	$S_{F^1}^{z_j}$	$\ldots$	$S_{F^1}^{z_p}$

In [10] have proved a number of theorems for an easy calculation of the subsets of column of the functions represented in the conjunctive or disjunctive normal forms or in algebraic form (the theorems 1-8).

Theorem 1. If $F(x_1,...,x_{\tau},x_{\tau+1},...,x_n)=F_1\vee...\vee F_i\vee...\vee F_k$, then

$$S_{F^1}^{z_j}=\bigcup_{i=1}^{k}S_{F_i^1}^{z_j},\ \forall j\in\{0,...,2^{n-\tau}-1\}$$

Theorem 2. If $F(x_1,...,x_{\tau},x_{\tau+1},...,x_n)=F_1\wedge...\wedge F_i\wedge...\wedge F_k$, then

$$S_{F^1}^{z_j}=\bigcap_{i=1}^{k}S_{F_i^1}^{z_j},\ \forall j\in\{0,...,2^{n-\tau}-1\}$$

Theorem 3. If $F(x_1,...,x_{\tau},x_{\tau+1},...,x_n)=F_1\oplus...\oplus F_i\oplus...\oplus F_k$, then

$$S_{F^1}^{z_j}=\mathop{\Delta}\limits_{i=1}^{k}\ S_{F_i^1}^{z_j},\quad \forall j\in\{0,...,2^{n-\tau}-1\},$$

where Δ is the symmetric difference of the subsets of column.

Theorem 4. If $F(x_1,...,x_\tau, x_{\tau+1},...,x_n) = F_1 \to F_2$, then

$$S^{z_j}_{F^1} = S^{z_j}_{F_1^0} \bigcup S^{z_j}_{F_2^1}.$$

Theorem 5. If $U_i = x_{j_1}^{\sigma_{j_1}} \wedge ... \wedge x_{j_q}^{\sigma_{j_q}}$, $x_{j_1},...,x_{j_q} \in \tilde{X}_2$, then

$$S^{z_j}_{U_i^1} = \begin{cases} \{0,...,2^\tau - 1\}, \, if \;\; \forall a \in \{1,...,q\}: x_{j_a} = \sigma_{j_a}, \\ \varnothing, \quad if \;\; \exists a \in \{1,...,q\}: x_{j_a} \neq \sigma_{j_a}. \end{cases}$$

Theorem 6. If $U_i = x_{i_1}^{\sigma_{i_1}} \wedge ... \wedge x_{i_s}^{\sigma_{i_s}}$, $x_{i_1},...,x_{i_s} \in \tilde{X}_1$. then

$$S^{z_j}_{u_i^1} = \overline{m} \begin{matrix} \sigma_{i_1} & \cdots & \sigma_{i_s} \\ i_1 & \cdots & i_s \end{matrix}, \;\; \forall j \in \{0,1,...,2^{n-\tau} - 1\}.$$

Theorem 7. If $U_i = x_{i_1}^{\sigma_{i_1}} \wedge ... \wedge x_{i_c}^{\sigma_{i_c}} \wedge x_{j_1}^{\sigma_{j_1}} \wedge ... \wedge x_{j_q}^{\sigma_{j_q}}$, where $x_{i_1},...,x_{i_c} \in \{x_1,...,x_\tau\}$, $x_{j_1},...,x_{j_q} \in \{x_{\tau+1},...,x_n\}$, then

$$S^{z_j}_{U_i^1} = \begin{cases} \varnothing, \, if \;\; \exists a \in \{1,...,q\}: x_{j_a} \neq \sigma_{j_a} \\ m \begin{matrix} \sigma_{i_1} \cdots \sigma_{i_c} \\ i_1 \cdots i_c \end{matrix}, if \;\; \forall a \in \{1,...,q\}: x_{j_a} = \sigma_{j_a} \end{cases}.$$

Moreover, have been demonstrated some theorems which allow us to calculate the subsets of columns of the partial derivatives of Boolean functions. Thereby we can readily calculate the coefficients of the Zhegalkin polynomial and represent the Boolean function in the algebraic form.

Theorem 8. In the Zhegalkin polynomial of the Boolean function $F(x_1,...x_\tau, x_{\tau+1},...,x_n)$ the coefficients satisfy the relations

$$C_0 = F(0,...,0), \; C_{i_1,i_2,...,i_k} = \begin{cases} 0, \text{ dacă } 0 \notin S^{z_0}_{\left(\frac{\partial^k F}{\partial x_{i_1} \partial x_{i_2} ... \partial x_{i_k}}\right)^1} \\ 1, \text{ dacă } 0 \in S^{z_0}_{\left(\frac{\partial^k F}{\partial x_{i_1} \partial x_{i_2} ... \partial x_{i_k}}\right)^1} \end{cases}, \quad \forall i_1,...,i_k \in \{1,...,n\}.$$

The inverse problem, i.e. calculating an antiderivative function knowing only a few partial derivatives is a complex problem that can be used for key generation in symmetric encryption systems.

2. ENCTYPTION SYSTEMS BASED ON THE MULTIDIMENSIONAL MATRICES

3.1. A symmetric algorithm based on the polynomial decomposition of the numbers

A symmetric cryptographic algorithm (called Cripto 2) based on large prime numbers, multidimensional matrices, and polynomial decomposition of the numbers was developed in [10]. For this algorithm we select a matrix $A_R = \Phi(\vec{R})$ for which the inverse transformation $\overline{R} = \Phi^{-1}(\vec{c})$ is difficult enough.

Let we have to encrypt the coordinates of the cortege $\vec{m} = (m_1, m_2, ..., m_t)$ which represents the numerical coding of the given clear text. We consider the coordinates of this cortex as elements of the set Ω. In this case these coordinates must be also elements of the matrix R_j. If the coordinates of the vector do not repeat according to some rule then all matrices A_{R_j} must be of the order n [9]. Let $t = a \cdot b$. Then the matrix A_R will have the form represented in figure 4 where $n = \lceil \log_2 a \rceil$, $k = b$ and the coordinates of the cortege $\overline{c}$ are calculated by the formula:

$$c_i = \sum_{j=1}^{b} m_{(i-1)b+j} \cdot y_i^{b-j},\ i = \overline{1,a},\ y_i > \max \omega_h,\ h = \overline{1,t},$$

where $y_1, y_2, ..., y_a$ are large prime numbers (to increase the security), which represent the private keys. In particular the algorithm can work with only one private key *y*.

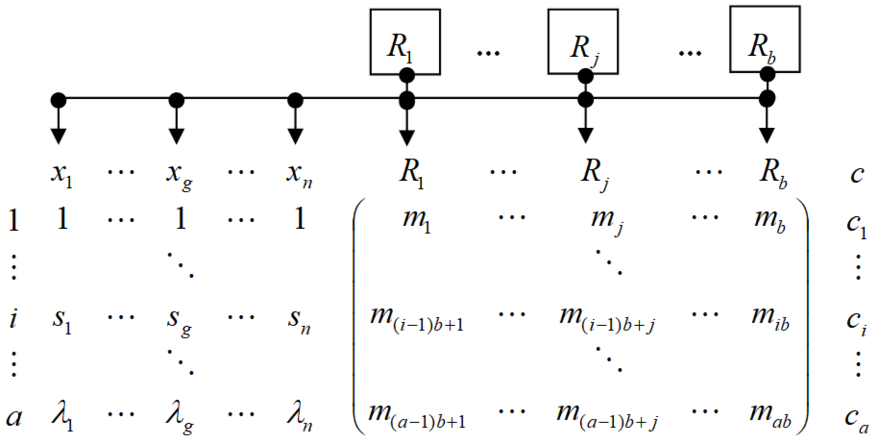


Figure 4. The matrix A_R for the encryption system Cripto 1

3.2. Encryption system based on Boolean function

Boolean functions and their properties are widely applied in cryptography. Operations with Boolean functions are very fast, and this allows developing cryptographic algorithms with increased work speed. Such an algorithm is proposed in this paragraph. The algorithm is based on the properties of multi-ary relations, multidimensional matrices (as a tool for working with Boolean functions) and on the representation of Boolean functions by subsets of column [8].

Consider a particular case for the family of sets $X = \{X_1, X_2, ..., X_n\}$:

$$X_1 = X_2 = ... = X_n = \Omega = \{0,1\}.$$

We denote the relations defined on these sets with $M_j = M_{X_{j_1} ,...X_{j d_j}}$ where $(2 \le d_j \le n,\ j = \overline{1, k},$ $j_1,\ j_2\ ,...,\ j_{d_j} \in \{1, 2, ..., n\})$ and obtain the cortege

$$\overline{M} = (M_1,...,M_j,..,M_k).$$

We put in correspondence to this cortege an n-dimensional matrix $A_M = \Phi(\vec{M}),\ \ i = \overline{0,u},\ \ j = \overline{1,k}$ (figure 5) [8]. In this matrix $M_j = M_{X_\tau ,...X_n}$ and $m_{ij} = m_{\sigma_\tau ...\sigma_n} \in \{0,1\}$.

$$A_M = \begin{array}{c} \\ 0 \\ \vdots \\ i \\ \vdots \\ u \end{array} \begin{array}{c} \begin{array}{ccccc} x_1 & \cdots & x_\tau & \cdots & x_n \end{array} \\ \begin{pmatrix} 0 & \cdots & 0 & \cdots & 0 \\ & & \ddots & & \\ \sigma_1 & \cdots & \sigma_\tau & \cdots & \sigma_n \\ & & \ddots & & \\ 1 & \cdots & 1 & \cdots & 1 \end{pmatrix} \end{array} \begin{array}{c} \begin{array}{ccccc} M_1 & \cdots & M_j & \cdots & M_k \end{array} \\ \begin{pmatrix} m_{01} & \cdots & m_{0j} & \cdots & m_{0k} \\ & & \ddots & & \\ m_{i1} & \cdots & m_{ij} & \cdots & m_{ik} \\ & & \ddots & & \\ m_{u1} & \cdots & m_{uj} & \cdots & m_{uk} \end{pmatrix} \end{array} \begin{array}{c} m \\ \begin{pmatrix} m_0 \\ \vdots \\ m_i \\ \vdots \\ m_u \end{pmatrix} \end{array}$$

Figure 5. The representation of the matrix A_M

Therefore, this matrix represents a system of k Boolean function of the variables $x_1,...,x_n$. We put in correspondence to this matrix a cortege of numbers:

$$\overline{m} = (m_0,...,m_i,...,m_t), t \le u\ ,\ m_i = \sum_{j=1}^{k} m_{ij} \cdot 2^{k-j}, i = \overline{0,t},\ n = \lceil \log_2 t \rceil,\ k = \lceil \log_2 \max m_i \rceil.$$

By analogy we build another matrix A_D to which we put in correspondence a cortege of numbers $\overline{d}$:

$$\overline{d} = (d_0,...,d_i,...,d_t),\ t \le u\ ,\ d_i = \sum_{j=1}^{k} d_{ij} \cdot 2^{k-j}, i = \overline{0,t}.$$

With these two matrices we can perform logical operations such as $A_M \wedge A_D,\ A_M \vee A_D,\ A_M \oplus A_D$ etc. resulting in other matrices of the same size. One of these operations ($\oplus$) has the following property

$$A_M \oplus A_D = A_C\ ,\ A_C \oplus A_D = A_M\ ,$$

which allows to use the matrix A_D as a private key for encryption and decryption the cortege $\overline{m}$ (which represents the digital code of the plane text *M*). The encrypted message is represented by the cortege $\bar{c}$:

$$\bar{c} = (c_0,...,c_i...,c_t),\ t \le u\ ,\ c_i = \sum_{j=1}^{k} c_{ij} \cdot 2^{k-j}, i = \overline{0,t},\ c_{ij} = m_{ij} \oplus d_{ij}\ .$$

The private key in this algorithm is generated using the subsets of column of the Boolean functions $F_1,...,F_j,...,F_k$ which correspond to the relations $D_1,...,D_j,...,D_k$.

3.3. Encryption keys generation

As was shown in [6], suppose we have a family of bent Boolean functions $\Phi = \{F_1,\ F_2,\ ...,\ F_g\}$, where *g* is a quite large number (the size of *g* depends on many factors, one of them is the number of variables of *F*). The representation of one of the function $F = F_i$ by the subsets of column of partial derivatives is shown in the Table 2.

In addition to this, these functions satisfy the condition: the subsets of column of derivatives must contain a minimum number of elements with the same minimal number of units in their binary representation [3].

The *key generator* randomly choose *t* triples of numbers (n_1, n_2, n_3), which represent the public key, where

- n_1 – index of the function from the set Φ;
- n_2 – its binary firm defines the variables for the derivative calculations;
- n_3 – index *z* - number of subset of column.

Based on these triples we built the vector $\bar{d} = (d_0,...,d_t)$ which represents the secret key. One triplet generates one subset of column which is calculated without calculation of the entire matrix form table 2.

Table 2. Table of the partial derivatives of a Boolean function

	$x_{\tau+1}...x_n$				
	z_0	...	z_j	...	z_p
F^1	$S^{z_0}_{F^1}$	...	$S^{z_j}_{F^1}$	...	$S^{z_p}_{F^1}$
$\left(\frac{\partial F}{\partial x_1}\right)^1$	$S^{z_0}_{\left(\frac{\partial F}{\partial x_1}\right)^1}$	...	$S^{z_j}_{\left(\frac{\partial F}{\partial x_1}\right)^1}$	...	$S^{z_p}_{\left(\frac{\partial F}{\partial x_1}\right)^1}$
$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$
$\left(\frac{\partial F}{\partial x_n}\right)^1$	$S^{z_0}_{\left(\frac{\partial F}{\partial x_n}\right)^1}$	...	$S^{z_j}_{\left(\frac{\partial F}{\partial x_n}\right)^1}$	...	$S^{z_p}_{\left(\frac{\partial F}{\partial x_n}\right)^1}$

$\left(\frac{\partial^2 F}{\partial x_1 \partial x_2}\right)^1$	$S^{z_0}\left(\frac{\partial^2 F}{\partial x_1 \partial x_2}\right)^1$	...	$S^{z_j}\left(\frac{\partial^2 F}{\partial x_1 \partial x_2}\right)^1$	...	$S^{z_p}\left(\frac{\partial^2 F}{\partial x_1 \partial x_2}\right)^1$
$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$
$\left(\frac{\partial^n F}{\partial x_1 \partial x_2 ... \partial x_n}\right)^1$	$S^{z_0}\left(\frac{\partial^n F}{\partial x_1 \partial x_2 ... \partial x_n}\right)^1$	...	$S^{z_j}\left(\frac{\partial^n F}{\partial x_1 \partial x_2 ... \partial x_n}\right)^1$	...	$S^{z_p}\left(\frac{\partial^n F}{\partial x_1 \partial x_2 ... \partial x_n}\right)^1$

4. CONCLUSION

1. The elaborated algorithms have information processing speed much higher and a problem solving capacity much bigger in comparison to existent encrypting systems. The priorities of the systems have been highlighted during their testing with vectors that contain hundreds, thousands and millions of components.
2. Due to the fact that some of the presented encryption systems can operate with small numbers, it would be easy to implement in software or hardware.
3. The system may be improved using *q*-valent logic functions. Deeper investigations are needed in order to achieve this.
4. On the other side the security of these encryption systems are not completely studied to be sure that them are secured. This also requires additional investigations in order to achieve it.
5. The multidimensional matrices can be used also in many other fields, for example in graph theory, in systems theory, etc. and it would be interested to research this in order to the use the results in cryptography.

REFERENCES

1. Bulat M., Zgureanu A., Ciobanu I., Bivol L., The inverse transformations of multidimensional matrices, in: ASADE Moldova, August 21, 2007, pp. 34-34.

2. Bulat M., Isomorfismo de conjundtos de relaciones, in: Revista de matematica: Teoria y Aplicaciones, 2001, 8(1), pp. 33-46.

3. Bulat M., Isomorfismo de grandes sistemas, in: Acta Academia 2001, Evrica, Chişinau, pp. 161-170.

4. Bulat M., Unele aplicaţii ale matricelor multidimensionale, in: Analele ATIC-2002, v.I (II), pp. 75-82.

5. Bulat M., Zgureanu A., Ciobanu I., Bivol L., Generating of prime numbers based on the multidimensional matrices, in: International Algebraic Conference dedicated to the 100th anniversary of D. K. Faddeev. St Petersburg, Russia, 2007, pp. 98-99.

6. Bulat M., Zgureanu A., Cataranciuc S., Ciobanu Ia., Encryption systems with wandering keys, in: International Conference ITSEC-2012, Chisinau, 2012, pp. 238-246.

7. Zgureanu A., Cataranciuc S., Encryption systems based on multidimensional matrixes, in: „Tiberiu Popoviciu seminar”, Cluj-Napoca 6-7 september, 2010, pp. 99-110.

8. Zgureanu A., Information encryption systems based on Boolean functions. The Computer Science Journal of Moldova, vol.18, no.3(54), 2010, pp. 319-335.

9. Zgureanu A., Sisteme de criptare cu chei variabile. Analele ATIC-2007-2008, vol. I (XII), Chişinău, Evrica, 2009, pp. 92-98.

10. Zgureanu A., Securitatea informaţională şi metode de criptare bazate pe mulţimi de relaţii multi-are. Teza de doctor în ştiinţe fizico-matematice. Chişinău, 2011, 165 p.

11. Булат М. С., Згуряну А. Ф., Чобану Я. И., Бивол Л. Г., Крипто-системы на базе n-арных отношений, in: Системы управления, контроля и измерений (УКИ-08), Российская Конференция с международным участием, Москва ИПУ РАН, 2008: pp. 66-67.

Prospects of the Cybersecurity Development in Digital Economy

Leahovcenco Alexandru

Academy of Economic Studies of Moldova
61, Banulescu-Bodoni Str., MD-2005, Chisinau, Republic of Moldova
Tel: 060255844, e-mail: alexandru.leahovcenco@yandex.com

ABSTRACT

This paper considers the prospects for the development of cybersecurity in the field of digital economy and shows the new areas of vulnerability that may appear in this new field.

Keywords: digital, economy, cybersecurity, threat, economic, system

1. INTRODUCTION

Global interconnectedness facilitated by the internet has created unprecedented opportunities for international commerce and communication, simultaneously with this phenomenon has begun a rapid development of cyber technology which provides many positive benefits, but significant security risks come along with it.

Cyberspace is an unpredictable and boundless domain which grows bigger year by year. A distinctive feature of cyberspace is that are no physical boundaries between users of network. Such situation creates the opportunities to establish a harmful environment by any individual on the planet.

This paper considers the prospects for the development of cybersecurity new features in the digital economy field. The main prerogative of this research was the idea to analyze the threats and the areas which those can affect in the new economic system such like digital economy.

In majority all current cybersecurity developments are aimed to develop tools which can be used for protection in current economic system, like: Real-Time Protection, Active Virus Control, Email Protection, Web Protection, Network Protection, Anti-spam protection, Firewalls etc.

As well this trend it's equal for international cybersecurity standards, as example ISO/IEC 27000 family of standards, it's represents the series of best practice recommendations on information security management and other aspects of cybersecurity. So it represents a variety of tools which can be implemented for better cybersecurity defense. As a result, the most important missed opportunity of all these tools and recommendations consists in the absence of holistic concept of cybersecurity defense prospects that must be developed in the future.

Such concept may have many compartments but in this paper, we will discuss the ***economic aspect*** of „Cybersecurity Concept". For better understanding of idea let's make a remark form history.

In 1997, the important work of American researchers was published *„Bradford De Long J., Froomkin A.M. The Next Economy. April 1997"*[1], in which it was argued that modern technologies are beginning to undermine the properties that make the "Invisible Hand" of the market system an effective tool for organizing production and distribution of products.

The authors studied three classical aspects of the functioning of a market economy and concluded that under the new conditions of establishing a global communication system, they begin to work differently than it was in the days of Adam Smith. The current instruments of market still correspond well to the modern economy, but they will be badly correlated with the future economy (digital).

The most critical factor that is being modified its ***Exclusiveness***, consumers can become buyers. In the new digital economy, the owner of the goods is not in a position to exclude competitors from his segment so easily, i.e. electronic replicability and fast product delivery, destroy the exclusivity that is on the list of the foundations of the market system in the first place"[1].

The paper has the following contents: **Introduction** in which are describe general ideas of cybersecurity prospects in the field of digital economy, **Methodology** which contains the description of a new economic unit „The digital enterprise", Schematic representation of the interaction of agents in the digital economy, Alternatives to the classic mechanisms of the economy in a networked environment, Classification of cyber threats in the digital economy, The main direction of development for cybersecurity and **Conclusions** where are summarizes the findings of research.

The main questions of the work are:

1. What alternatives can be found for classic economic mechanism,
2. Which areas of digital economy are most vulnerable,
3. Which vector can be chosen for the development of cybersecurity in the field of digital economy;

2. CONCEPT

Analyzing the state of the economy at current date, can be confidently confirmed that all operations of an economic and social nature are carried out exclusively in a virtual environment. Namely, searching for new partners for business, searching for goods in internet, their purchase, the taxes payments, dating in social networks, work activities. In one word. all important for the existence of humanity, economic relations are being produced in a virtual environment. What does this mean for business, most likely the next, that the former corporate structures will not work efficiently in the new digital economic environment, or even disappear. Considering this fact, can confidently assume that in the near future almost all current economic structures will be transferred in the virtual environment, and in our case these will be enterprises that will be transformed into a new form of a digital enterprise.

The main features of a digital enterprise are as follows:

1. The enterprise exists exclusively in a virtual environment - this means that the enterprise is no longer legally bound to any country and is an independent structure in principle. "The term of **virtual environment** will be considered later".
2. Employees participating in the work of the enterprise and in its business processes can be located absolutely on any spot in the world.

3. Organization of work of employees and all relationships both in the enterprise itself and with other enterprises that are included in a virtual environment are carried out exclusively virtually with the exception of logistics.

Below is a schematic drawing that demonstrates exemplary relationships in a virtual environment. But first for better understanding of it, must be explained the concept of virtual environment.

Virtual Environment - is a collection of network environment, network protocols and communication channels that establish interconnections of any unit that can access the virtual environment and here must be mentioned a fact what this environment can exist like under level of some sort of network like internet or blockchain based network or it can be developed like independent network that can be accessed throw internet or other communications channels.

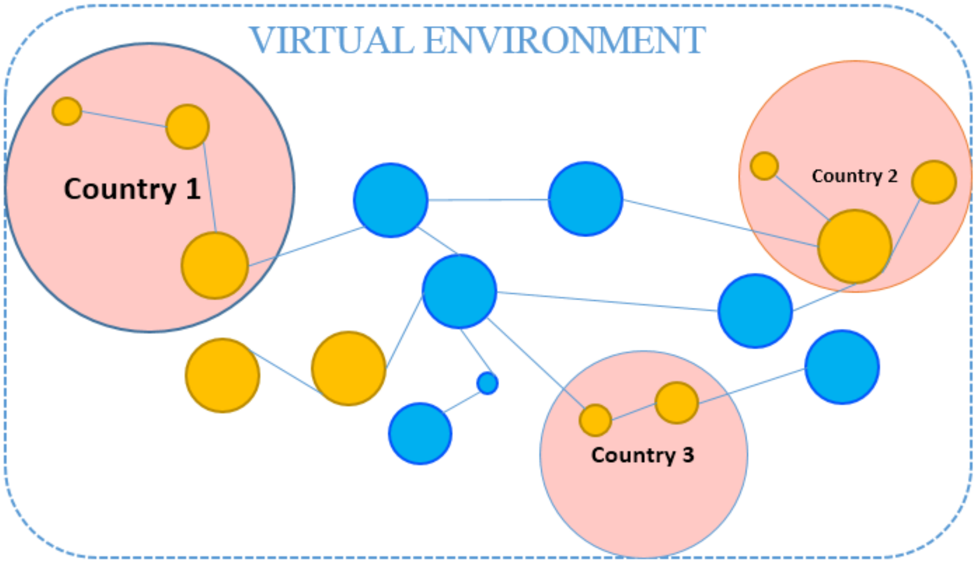


Figure 1. Schematic representation of the interaction of units in the digital economy

As it presents in figure above, red circles represent countries in which state structures (yellow circles) are registered and are managed directly by the government, they correspond with each other inside the country and other units of the environment but not directly. To cooperate, two yellow circles belonging to two different states can use other individuals (digital enterprises - blue circles) as connections nodes. Such structure its similar with block-chain technology so it can be used like a start point for development of digital environment. So the fundamental difference in the structure of the relationship between economic agents in the current economy and digital economy consists in decentralization and the absence of a hierarchical management structure. As a result, the main feature of the digital economy, appear to be what the role of the state as the main regulator in commercial transactions is reduced and is approaching zero, although it will never reach it, since the exchange of goods, services and their payment occur outside the virtual environment. In the case of economic relations in the digital economy, any agent is able to build strong contact with any other agent and begin to conduct economic activities with him without any border restrictions.

But in such case appears some critical questions for cybersecurity such as:

1. How to organize payment of taxes from the activities of the enterprise in such environment?
2. Who will be responsible for control of cybercrimes in such digital environment?

These two questions will take a lot of time to think and discus but for now it's enough to develop a common concept and to choose the correct vector for future developments. In the table below are presented the characteristics of different types of economies to show the main differences of the forms of organization of economic activities.

Table 1. Comparative characteristics of the forms of organization of economic activity

No.	Attribute	Forms of organization of economic activity		
		Socialist	Capitalist	Digital
1.	Priority of the system approach	Regulation by legislative side	Economic agents have equal rights in the environment of the free market	Subordinate to the interests of network organization. (Self-organization)
2.	The distribution of productive forces	Prescriptive	Economic decision-making (more profitable and lucrative)	Social-economic (In the interest of the entire virtual environment)
3.	The circulation of goods and capital	Distributed by the state	Competitive relations (Tough competition)	Aimed at meeting socio-economic needs of the virtual environment participants.
4.	Adaptability to changes in the environment	Stable condition	Strong response to changes in price signals	A high degree of coordination of each virtual unit.
5.	Dynamism of modification and scale	Limited by the interest of the governing authority	Random not predefined change	Easily changeable structure due to the flexibility of building a virtual environment.

As a final argument to confirm that our society are ready to become digital society and to be introduce in a virtual environment could be presented by a table "World Internet Usage and Population Statistics" witch shows distinctively that year by year grows the number of peoples who uses the internet and based on it technologies.

The area of direct communications, which possesses all the power and variety of modern technical means, allows that all agents of economic activity to be placed inside of it. At whatever point on the planet a person is, that individual can easily enter into direct contact with another individual. As a result, appears to be a tendency to virtually materialized, the image of our real world.

Further will be presented the answers to the questions declared in the beginning. First of all, for the first question “What alternatives can be found for classic economic mechanism” must be presented a figure that show the main principle of a new digital economic concept in parallel with old economic concept.

Table 2. World internet usage and population statistics (http://www.internetworldstats.com/stats.htm)

WORLD INTERNET USAGE AND POPULATION STATISTICS JUNE 30, 2017						
World Regions	Population (2017 Est.)	Population % of World	Internet Users 30 June 2017	Penetration Rate (% Pop.)	Growth 2000-2017	Internet Users %
Africa	1,246,504,865	16.6 %	388,376,491	31.2 %	8,503.1%	10.0 %
Asia	4,148,177,672	55.2 %	1,938,075,631	46.7 %	1,595.5%	49.7 %
Europe	822,710,362	10.9 %	659,634,487	80.2 %	527.6%	17.0 %
Latin America / Caribbean	647,604,645	8.6 %	404,269,163	62.4 %	2,137.4%	10.4 %
Middle East	250,327,574	3.3 %	146,972,123	58.7 %	4,374.3%	3.8 %
North America	363,224,006	4.8 %	320,059,368	88.1 %	196.1%	8.2 %
Oceania / Australia	40,479,846	0.5 %	28,180,356	69.6 %	269.8%	0.7 %
WORLD TOTAL	7,519,028,970	100.0 %	3,885,567,619	51.7 %	976.4%	100.0 %

As clearly seen in figure 2 the classical model of the economy has the main goal of making profit, irrespective of the needs of society, which led to irresponsible emission of the currency and the uncontrolled management of the world banks. The only way to smooth out such an economic regime is to return part of earned capital back to society throw “Charity” to stabilize the control regime. That’s why governments must supply form state budget different social programs and business must share it profit with different noncommercial organization, such approach is very unstable and lead to a constant economic crises and recovery. Otherwise is an approach of digital economy that is total opposite because in the area of digital economy, the society and business a close bound to each other that’s mean what every business project which has a goal in making a profit must necessarily have a positive impact on society in the next table will be shown the alternatives for classical economic mechanism. But first a small remark, why it became possible?

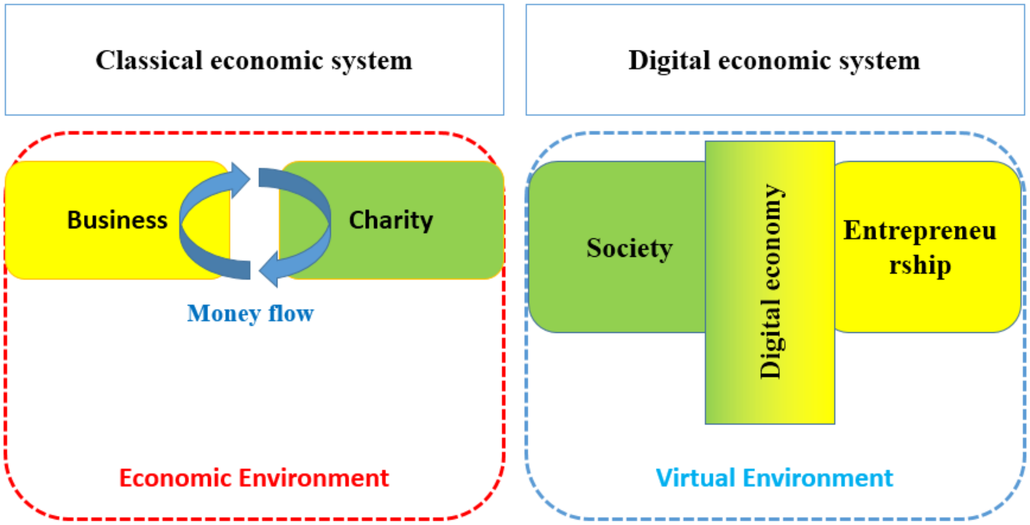


Figure 2. Differences in approaches of classical and digital economy.

Because the fact that prior the Internet channels were poorly developed and were difficult to exchange information and opinions, and therefore it was difficult to find alternatives to the existing systems. A single world wide web has made possible the development of the economy system to unheard of possibilities, the phenomenon of the global network demonstrated that the system itself is organized and evolves in spite of the external environment.

Below are given examples of economic mechanism, the occurrence of which could take place only in the digital economy in comparison with classical economic mechanisms.

Table 3. Alternatives to classical mechanisms of the economy in a network environment

Classical economic mechanisms	Alternatives network Economics
Charity	Impact Investing
Uncontrolled emission of money	Crypto-currency clearing mechanism (Bitcoin, Ethereum, Ripple, Litecoin, NXT)
Microfinance of small enterprises	Peer to Peer Lending & Alternative Investing (https://www.lendingclub.com/)
Costly investment in new and uncertain projects	Crowdfunding (Kickstarter, IndieGoGo, RocketHub)
World Banking Information Environment (SWIFT)	Network environment based on blockchain technology

As can be seen from the information given in Table 2, the society self-organizes itself and chooses which enterprises or projects should be developed by direct financing, and it does so, bypassing the banking monopoly and this is only a small range of opportunities that can develop in a digital environment.

And since such a rapid development of network technologies occurs on its own, and there is no regulatory body that could at least indirectly indicate the right course of development, then it is necessary to think about the security of such a network organization i.e. the **cybersecurity of entrepreneurship**.

Despite the fact that the digital economy is changing, its economic essence remains unchanged, so we can make some predictions about a possible threat to business in the digital environment. If we proceed from the fact that the information itself will in future represent a value that will replace all the values we are familiar with like money, precious metals, mineral oil. Hence the conclusion that information is itself a valuable resource, but how can be it measure its value so that it can be compared with the product?

As a solution may be suggested a mechanism for generating crypto currency based on the computing resources of the earth, because as more and more computers are connected to the world network every day accordingly the cost of information is growing.

As a result, a simple sequence appears that characterizes information as a valuable resource:

Generation of Information → Its retention → Conversion → Transfer

The cyberthreat that will appear in the digital economy will manifest itself in one of these 4 stages. And here can be found the answer for the second question "Which areas of digital economy are most vulnerable".

Table 4. Classification of areas of cyber threats in the digital economy

Steps of converting	Risks
Extraction of information	It is necessary to standardize the process of information formation as value. (Note: To standardize the mechanism of mining the crypto currency in order to avoid it without a control emission)
Its retention	A reliable knowledge bank should be created where the extracted information could be stored. (Note: To create a reliable knowledge bank, where could be stored the extracted information To avoid unauthorized access data to valuable data)
Conversion	Ensure its liquid conversion and exchange avoid speculation when converting and selling it. (Note: To create a legal framework and, better, an inter-state coalition of institutions that could regulate and correlate the fair value of information and other resources in order to avoid speculation in exchange markets)
Transfer	Organize reliable standards and solutions and create secure transmission channels in order to avoid unauthorized stealing. (Note: It is necessary to create a secure network that would guarantee almost 100% transaction protection between any entities of the system)

In conclusion, it should be noted that the generally accepted classification of cyber threats should be clearly analyzed, since this is the most important part of creating a secure virtual economic environment on the basis of which, can be developed cybersecurity standards and can be selected the right vector of elaboration of new economic relations in a digital society.

3. CONCLUSION

As a conclusion of this paper can be answered the last question “Which vector can be chosen for the development of cybersecurity in the field of digital economy?”, as its clear from presented earlier tables the time for changes has come, data presented in table 3 shows the fact that a new structure like digital economy is self-organize mechanism which adapts very quickly against aggressive external environment. This was made possible due to fast data transfer via the network channels this resulted in a quick response to a given request by any unit in the network. It will be very hard to manage such a fast-growing system but at least it can be directed in a right vector. Because in near future the meaning of cyberthreats will be critical changed. That means what cybersecurity standards, protocols, methodologies must have a goal to develop mechanisms that can protect the whole virtual environment and make it safer to use instead to develop particular tools for every individual unit in the system like it is made in our days. What's why establishment of an international regime regulating cybersecurity is important for the future of the international security environment and the security of all states that operate within.

Threats that will appear in virtual environment will affect every nation on earth therefore it’s so important to presume and prevent their dissemination. The threats and challenges associated with the cyber domain will not dissipate on their instead they will continue to evolve. The process will certainly be complicated and time consuming. There will be disagreement between states regarding the specific nature of the threat, levels of state authority and responsibility, and the implications for state sovereignty.

The problem of establishing viable means of verification of compliance will be challenging. Multiple levels of coordination will need to be established, including interagency coordination within states, coordination between allies and partners, and global coordination and cooperation. Despite the difficulties associated with the formation of a global cybersecurity regime, makes to believe that such a regime will ultimately be achieved. International cooperation is not formed overnight, progress may be slow and incremental, but eventually the pieces will come together and the international community will unite in support of a mutually beneficial cybersecurity agreement.

REFERENCES

1. Bradford De Long J., Froomkin A.M. The Next Economy. April 1997, http://www.law.miami.edu/~froomkin/articles/newecon.htm.

2. Akulov V.B., Rudakov M.N. Sposoby izmeneniya struktury organizatsii kompanii. URL: http://www.aup.ru/books/m150/30.htm.

3. Kevin Kelly. New Rules for the New Economy, WIRED September, 1997. URL: http:// www.wired.om/wired/0.09/newrules.html.

4. Siraj Raval, Decentralized Applications, Harnessing Bitcoin's Blockchain Technology, p. 118 (2016).

5. Barlow J. P. Selling Wine Without Bottles: The Economy of Mind on the Global Net: http://lib.ru/COPYRIGHT/barlou.txt

6. Parinov S.I, Yakovleva T.I, Economy of the 21st century based on Internet technologies,

4. SECURITY and DEFENCE

General Aspects of the Information War Preventing and Combating

Rusnac Andrei

Information security expert, Republic of Moldova
E-mail: rusnacandrei79@gmail.com

ABSTRACT

The article describes the general aspects of the information war/warfare, information weapons and propaganda methods using, methods and type of this modern warfare, the principles and methods of detecting, classifying and measures of preventing of this act.

Keywords: war, warfare, information, weapons, propaganda, security, preventing, combating

1. PROPAGANDA

1.1 The phenomenon

Propaganda is an open dissemination of views, facts, arguments and other information, including deliberately distorted and misleading, for the formation of public opinion or other purposes.

A propagandist has a specific goal or set of goals. To achieve them, the propagandist purposely selects facts and arguments and presents them in such a way as to achieve the greatest effect. To enhance the effect, important facts may be overlooked or distorted, with an attempt to divert the attention of the audience from other sources of information.

1.2 The emergence and practical testing of classical propaganda methods

Classical propaganda methods were created, launched and tested during the Second World War. Classical Propaganda has 3 active phases:

1) choosing the operative information channel;
2) emphasizing the "necessary" facts, which are still objective, but will be presented from the "wanted" points of view, maximally simple in order to acquire information (especially in the context when the digital user usually hurries to go to another blog, article, topic, is in transport, writes or posts something else);
3) Creating the "packaging" for the message that draws attention or if the gaining of knowledge is forbidden, it is invisible.

These methods have been successfully tested by preparing and spreading leaflets between soldiers or civilians built on the pyramid model when the conceptual ideas are gradually developed and proven.

1.3 The principle of truthfulness of information

Propaganda formed by this principle is listening as an objective source of information, especially if these rumors are taken over and spread further by those with high positions and functions. They are sources of trust, and attacking / "infecting" these people will allow ideas to spread to others. In this context, the goal of propaganda is to create a discussion environment for problems and contexts that are present from the attacker's point of view.

If people are frankly imposed for someone else's point of view, they are opposed. In this context, propaganda does not give direct answers. Therefore, propaganda pushes people to some conclusions, creates the effect of thinking that they themselves found these answers.

2. INFORMATION WAR

2.1 The phenomenon

According to the Information Security Concept of the Republic of Moldova, the information war is a confrontation between two or more states in the information space in order to damage information systems and networks of electronic communications, processes and resources, national transport, communications, energy, financial and banking systems, taxation, customs , investments, the main sectors of the economy of the Republic of Moldova and its foreign relations, other vital and strategically important for the national economy security of objects, disruption political, economic and social systems, massive psychological treatment of the population for destabilization of society and the state, as well as compulsion to take decisions in the interests of the opposing side.

The phenomenon of information war was manifested and became possible due to a number of factors and conditions, including the development of technical means of dissemination of mass information, the formation of a global information space and the globalization of the world, the changing conditions of the life of the society associated with the increase in the role and importance of public opinion in political processes. In the principles of the information war lies the use of new and innovative technical information dissemination tools that can cover large areas and huge masses of the population. The appearance of the global information network and cellular communications formed the basis for the implementation of ideas of mass impact for manipulating the consciousness of the individual in the process of mediation. The globalization of social processes, the openness of virtual spaces creates the conditions under which ideas, views, any information can seamlessly cross national borders and influence the audience without regard to nationality, social status and ideological preferences. This space is not subjected to any control. Radio, television, mobile communications and the Internet become the main means of information impact on the population of the country's potential adversary, its political and economic elite. At the same time, the distributed mass information acquires a specific, directed character.

In the military aspect, the information war is a kind of military action in which the object of influence is the information stored or circulating in the control, intelligence, combat and other enemy's systems.

The combat effectiveness of the enemy can be affected by violating his information exchange processes or inserting information into the enemy's information systems. From this point of view, the task of the information war is to influence the information of the enemy's in order to undermine his combat capability and protect his information from enemy influence. Information here can act as a target of influence, and as a weapon in the information war.

The advantage of the information war is that it allows you to damage the enemy anonymously and without using any material means of destruction. The enemy is deprived of the right to respond by direct military methods, because in this case he will already look like an aggressor.

Today, the information war is an effective tool for information, political and cultural expansion of the developed countries.

2.2 Components of the information war

Two large groups of events are related to the information war:

4) the impact on the enemy’s military and civilian population in order to introduce mass awareness of certain arrangements;

5) the violation of the enemy’s information, information processes and information and control systems regardless of the means used.

There are main aims in the information war:

1) the control of the information space and ensure the protection of its information from hostile actions;

2) the use of control over the information space for conducting the information attacks on the enemy;

3) the increasing the overall effectiveness of the armed forces through the widespread introduction of military information functions.

The components of the information war include:

1) psychological operations aimed at influencing the motivation of enemy’s militaries;

2) disinformation - giving the enemy false information;

3) radio electronic war, consisting in the "blinding" of enemy’s radio electronic intelligence systems;

4) physical destruction of elements of the enemy's information system;

5) information attack – the destruction or distortion of information without visible damage to the media devices;

6) protecting your information.

There are two types of information attacks:

1) direct (the implementation of actions to introduce and distort information);

2) indirect (the construction of false systems or processes for distortion of the reality).

3. THE INFORMATION WAR VS PROPAGANDA

The detection of the essential characteristics of the information war will require the definition of common and distinctive features of propaganda and counterpropaganda. The propaganda is a one-sided process, unlike an information war in which at least two parties are involved. And only the appearance of counterpropaganda as a counteraction to propaganda makes it possible to conduct their equivalent comparison. Secondly, these two phenomena differ in the degree of intensity. It is the intensity of information exchange that we call one of the criteria that determines the manifestation of an information war. Third, the methods used: despite the fact that information wars, unlike other wars, are not regulated by the international law, nevertheless methods, methods, methods based on deception, lies, disinformation, defamation, etc. dominate in the information war. The enemy's point of view, unlike propaganda, is not weighed and evaluated, but is distorted and used to achieve its goals. Information is used not as an argument, but as a violence. Fourthly, the goal: propaganda seeks to prove, convince and persuade the opponent, but the information war - to deceive, break, and win.

4. THE STYLE OF THE INFORMATION WAR

4.1 The methods of the information war

The information war consists of actions taken to achieve information superiority in providing a national military strategy by influencing information and information systems of the enemy while simultaneously strengthening and protecting their own information, as well as information systems and infrastructure.

The information superiority is defined as the ability to collect, process and distribute a continuous stream of information about the situation, preventing the enemy from doing the same. It can also be defined as the ability to assign and maintain a pace of operation that surpasses any possible enemy pace, allowing it to dominate throughout its conduct, remaining unpredictable, and acting ahead of the adversary in its retaliatory actions.

The information superiority provides an interactive and highly accurate picture of the actions of the enemy and his troops in real time. In addition, it provides the ability to use in widely dispersed operations the widely dispersed construction of diverse forces, the protection of troops and the introduction into the battle of factions, whose composition is as relevant as possible, as well as to carry out flexible and purposeful material and technical support. The information war involves activities directed against control systems (Command & Control Warfare, C2W), and against computer and information networks and systems (Computer Network Attack, CNA).

Destructive impact on management systems is achieved through conducting the psychological operations (Psychological Operations, PSYOP) directed against personnel and decision-makers and affecting their moral sustainability, emotions and motives for decision-making; implementation of measures for operational security (OPSEC), disinformation and physical destruction of critical infrastructure facilities.

Defining the essence of the war is the continuation of politics by other means, by means of information violence (manipulation of people's consciousness, invasion of their psyche and inner peace) with the aim of achieving information, psychological and ideological superiority, inflicting damage on information systems, processes and resources, critical structures and means of communication (information-technical, network-centric and cyberwar), disruption political and social systems, as well as massive psychological processing of the personnel of troops and population (information-psychological war).

The basis for information and psychological war in modern conditions can be the preparation and conduct of large-scale information and psychological operations on specially designed plans for certain purposes.

Information war in peacetime is conducted in the form of information confrontation in all spheres of public life: in economy, politics, in social relations, in the sphere of spiritual life and especially in ideology. In the ideological sphere, the task is to blur the philosophical and methodological foundations of the cognitive activity of the people of the enemy state, sow chaos in his mind, deprive them of confidence in their future, and introduce false economic and moral attitudes.

The ultimate goal of information confrontation is the conquest and retention of information superiority - the advantages over the enemy in the collection, processing, dissemination of information, as well as counteraction to the relevant activities of the enemy.

Disinformation is implemented, as a rule, through all types of media for a long time. The introduction of agents of influence in the media of the opposing state allows manipulating the public consciousness of the people, using special means of its "zombie". The main means of the information war are information and psychological operations.

As a classic example of an information operation, the introduction of the Stuxnet worm into the control systems of Iranian centrifuges for uranium enrichment in 2010 can be cited. The virus was designed in such a way as to gradually create a vibration that was supposed to destroy the rotor and lead to an explosion of the centrifuge.

4.2 The types of war

The most profound definition of the "information war" was suggested by the American Theorist M. Libicki in his work "What Is Information Warfare?" Dated 1995, where he singled out 7 types of information wars:

1) the military confrontation for the mastery of command and control functions;
2) the confrontation between intelligence and counterintelligence;
3) the confrontation in the electronic sphere;
4) the psychological operations;
5) the organized spontaneous hacker attacks on information systems;
6) the information and economic wars for controlling the trade in information products and mastering information necessary to overcome competitors;
7) the cybernetic wars in virtual space.

In a more modern interpretation, the information operation (Info Ops) is understood as an integrated use of the capabilities of electronic weapons, computer network operations (CNO), psychological operations (PSYOP, MISO), operations with military disinformation and disorganization and security operations (OPSEC) to use the possibilities of influencing the human consciousness with the aim of destroying, decomposing, or in general intercepting the influence on the decision-making of the enemy, while defending their own decision.

The forms and methods of information war for a relatively short period of time have undergone qualitative changes. The role of information technologies and mass media has increased significantly - they have become a key means of achieving the military-political goals of states. The destructive power of information-psychological influence in modern conditions is so great that it calls into question not only on the independence of the defeated state, but also the fact of very existence of its peoples as a national community.

At the same time, the information war has its limits of possibilities and is effective not against any opponent. It does not cancel, but rather complements and strengthens traditional means of war.

5. THE INFORMATION WEAPONS

According to the Information Security Concept of the Republic of Moldova, information weapons is information technologies, tools and methods used for information war.

The weapon of the information war is the devices and methods of information processing that are used for large-scale, targeted, rapid and secretive impact on the military and civilian information systems of the enemy in order to disrupt his economy, reduce the degree of combat readiness and combat capability in order to contribute to the achievement of the final victory. At the same time, it means that the information war can be fought as independently, that is, without the use of traditional means and methods of armed struggle, and in combination with other types of combat operations.

In the event of a conflict with any state, a possible first attack is carried out through information networks, during which the critical infrastructure of the state is destroyed, the political and military control system is disrupted, and electronic control equipment is turned off. When the state-victim of aggression becomes practically paralyzed, classical military means are struck.

Information impact can be carried out both against the background of information noise, and in the information vacuum environment. The imposition of alien goals is what makes the information warfare war and distinguishes it from ordinary advertising. Information impact contains distortion of facts or imposes on him an emotional perception that is beneficial to the influencing party.

The information weapons include:

1) malicious code;
2) logical bombs (program bookmarks);
3) means of suppression of information exchange in telecommunication networks;
4) falsification of information in the state and military management channels;
5) means for neutralizing test programs;
6) various kinds of errors deliberately introduced into the software of the object.

One of the great advantages of an information weapon is its relative cheapness compared to another type of weapon. By the criterion of efficiency / cost, it significantly wins any other kind of weapon.

This is because it does not need to invest "energy" to destroy the enemy. Initially, it is assumed that the enemy has all the necessary means for his own destruction. The task of using information weapons is to help the enemy direct the available means, including technical ones, against himself.

Information weapons are aimed directly at changing the behavior of information systems, and in the case of application against people - to change their thinking and behavior accordingly without prior "intimidation".

6. THE CONSEQUENCES OF THE INFORMATION WAR

The information war does not differ from any other war, except for the weapons used, so the signs of defeat must be exactly the same:

1) the death and emigration of a part of the population;
2) the destruction of industry and the payment of indemnities;
3) the loss of a part of the territory;
4) the political dependence on the winner;
5) the destruction (drastic reduction) of the army or the ban on their own army;
6) the export of the most promising and high technology from the country.

7. CONCLUSION

The presence in the life activity of the society of actions emanating from a potential aggressor and simultaneously belonging to a typical information warfare strategy suggests that an information weapon is used against the relevant person, collective, state.

The essential dependence of modern civilization on the information component made it much more vulnerable. The speed and wide dissemination of information networks greatly increased the power of information weapons. The current model of fundamentally open society additionally affects the situation it presupposes a much larger volume of diverse information flows than in the case of a closed society.

In connection with the entry of humanity into the era of globalization and overcoming the obsolete forms of international public relations, the degree and extent of the negative impact of information wars on the state of international and national security will increase. However, this problem does not exclusively have a military solution.

REFERENCES

1. Strategic information warfare: a new face of war / Roger C. Molander, Andrew S. Riddile, Peter A. Wilson: rand.org;
2. Joint Publication 3-13/Information Operations/27 November 1998 Incorporating Change 120 November 2014: dtic.mil;
3. Information Warfare and Security by Dorothy E. Denning Addison-Wesley, December 1998;
4. The Future of Information Warfare / Defining: airpower.maxwell.af.milles;
5. What Is Information Warfare? Strategic Forum Number 28, May 1995 / Martin C. Libicki, Senior Fellow: dodccrp.org;
6. Information Operation Roadmap: nsarchive.gwu.edu;
7. Thomas P. Rona, «Weapon Systems and Information War», Boeing Aerospace Co., Seattle, WA, 1976;
8. Joint Pub 3-13.1 «Command and Control Warfare». DOD US, February 1996;
9. Joint Pub 3-13 «Information Operations», DOD US. December 1998;
10. Cyberwarfare, CRS Report for Congress, RL 30735, Nov. 15, 2000;
11. Караяни А. Г. Теория и практика психологической войны. Организация и проведение информационных операций: psyfactor.org;
12. Лисичкин В. А., Шелепин Л. А. Третья мировая (информационно-психологическая) война: malchish.org;
13. Манойло А. В. Информационно-психологическая война как средство достижения политических целей: psyfactor.org;
14. Власенко И. С., Кирьянов М. В. Информационная война: искажение реальности. — М.: ИД «Канцлер», 2011. - 196 с.;
15. Гриняев С. Н. Поле битвы - киберпространство: Теория, приёмы, средства, методы и системы ведения информационной войны. - Мн.: Харвест, 2004. - 448 с.;
16. Новиков В. К. Информационное оружие - оружие современных и будущих войн. - 2-е изд., испр. - М.: Горячая линия - Телеком, 2013. — 264 с.;

Modern View on Access to Shared Services through Federated Identity Provider

[1]Pocotilenco Valentin, [2]Bogatencov Petru, [3]Sclifos Constantin

[1]Technical University of Moldova
168, Stefan cel Mare Bd., Chisinau, MD-2004, Republic of Moldova
Tel: 37367395240, e-mail: valentin.pocotilenco@adm.utm.md

[2]RENAM Association
Str. Academiei 5, Chisinau, MD-2028, Republic of Moldova
Tel: 37369151334, e-mail: bogatencov@renam.md

[3]Academy of Economic Studies of Moldova
61, Banulescu-Bodoni str., Chișinău, MD-2005, Republic of Moldova
Tel: 37367100878, e-mail: sclifcon@vle.ase.md

ABSTRACT

Modern level of scientific and technical development is due to sharing relevant information and in this case it is very important to organize access to various informational systems with protected informational resources. Implementation of right instruments for interaction with informational systems for research and educational communities is a real necessity and will have essential contribution to increase capacity for knowledge. New instruments for improvement access to protected data resources are actively developing now and in the paper described possible approaches of their realization.

Keywords: federated, identity, services, management, access, provider, information, system, data

1. INTRODUCTION

Contemporary information needs and requirements are permanently growing. The wide set of information sources usually accessed that can be absolutely different from organization or destination point of view. As a result, the user has to use multiple credentials or data protection mechanisms to access them. To simplify the process of using information resources, many different identity management technologies were proposed. Identity management can be done at different levels, for example institutional, national, or international.

Different identity management technologies can be applied at each level. Institutional or national identity management typically employs locally developed implementations which usually comply with a part of identity management practices and fully satisfy local needs. At institutional or national level, SSO (Single Sign On) solutions are a simple way of sharing resources and services, but at international level more widely federated identity mechanisms are used.

2. IDENTITY FEDERATION AND SINGLE SIGN ON

Initially as a service access solution within a project (Figure 1), SSO technology has been expanded to facilitate access to geographically distributed services, evolving into national identity federations.

Figure 1. Microsoft SSO services

Example of SSO access mechanisms at the local level are the resources offered within an educational or research institution is depicted in Figure 2 [3].

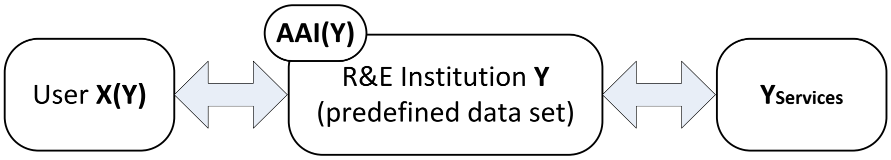


Figure 2. Institutional SSO implementation

Another example of a SSO mechanism is access to national e-resources by applying a single set of access data (Figure 3), as example – IDNO, or different datasets for each service.

Implementation of the models described earlier does not impose restrictions and the need to comply with the implemented AAI, the situation is completely different for the interconnection of national or international institutional resources.

To describe the above situation, we consider that there are two basic components need for federated mechanism functioning: IdM – identity management service; SP – service provider. We will consider that each institution can have at least one IdM and SP element (Figure 4.a). These institutions applying to common agreement will comply with a minimum set of data necessary for the effective operation of AAI. In this situation, each institution retains its data within its own IdM and authenticates/authorizes requests received from other members of the Federation Agreement. Such architecture is called mesh. Another situation can be considered when the IdM is done in a centralized form for shared services (Figure 4.b), the architecture being called Hub&Spoke. Such implementation increases the effectiveness of the authorization mechanism and simplifies the interconnection of resources at regional level.

Another advantage of Hub&Spoke topology is the reduction of costs and risks of maintenance of an IdM. In turn NREN can cooperate with similar organizations complying the AAI requirements for access to regional resources. The process of accession to the agreement for resource sharing is described as the process of establishing of Identity Federation. This process is widely supported within the pan-European GEANT network [1] through the eduGain inter-federation mechanism and disseminated through thematic meetings organized by GEANT Association[5].

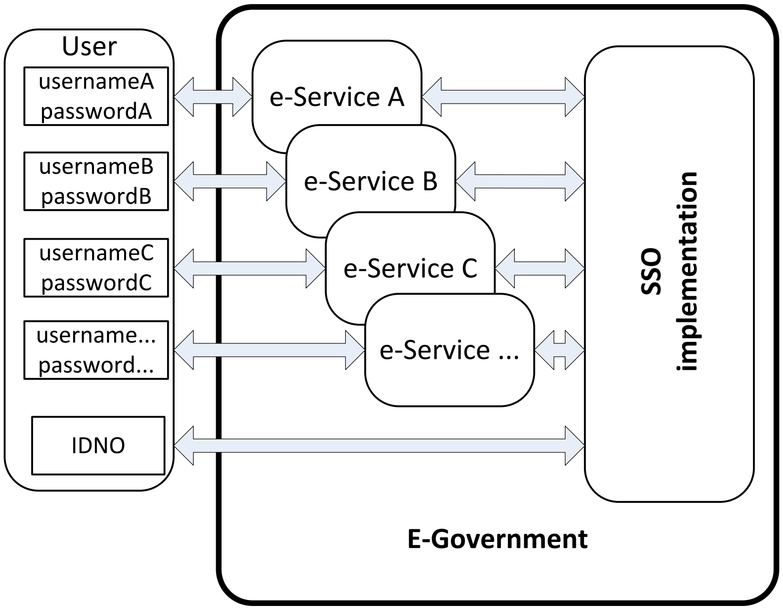


Figure 3. Example of national SSO mechanism

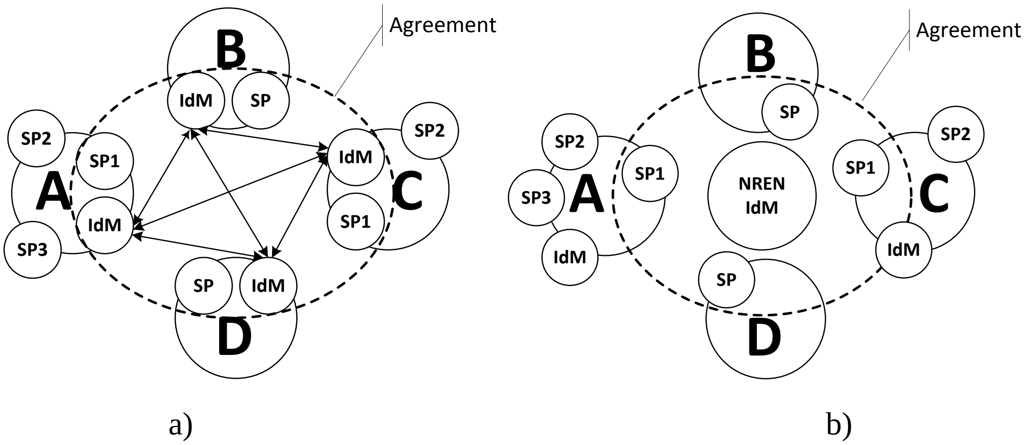


Figure 4. Federation topologies

It is necessary to take into account well-determined methods, requirements and principles, which must be followed by all its members, in order to implement a federated infrastructure for the purpose of resource sharing and access to services shared within eduGain [2]. For interoperation of federations within eduGain currently SAML2.0 is still used, because of large amount of included entities which use a wide range of software solutions based on it. Anyway contemporaneous solutions use more than one protocol for identity management systems, having SAML2.0 only for communication with eduGain, and within the organization network there are possibilities of using different protocols, based on specific data exchange needs (see Figure 5) [4].

An important aspect of security is the point of introducing sensitive data in the process of accessing the selected service. There are two ways to access federated services (as in the Figure 6) [6]. Depending on the SAML data middleware solutions shown in Figure 5, access to the requested service can be obtained by:

- SP initiated login – in this case, the user in institution B will first access the requested service (figure 6a) in institution A. Obviously in the institution A there is no information about the user, so located in the Federation SP will "ask" the IdM instance in institution B if the user is authorized to access the service. Authentication/authorization process will be initialized after redirecting to IdM. As a result, the user will be able to access the service.
- IdP initiated login – in this case, the user will log in to the IdM instance in institution B, thus the user will perform the authentication process. The next step is access to the service, if authentication/authorization process was succeed.

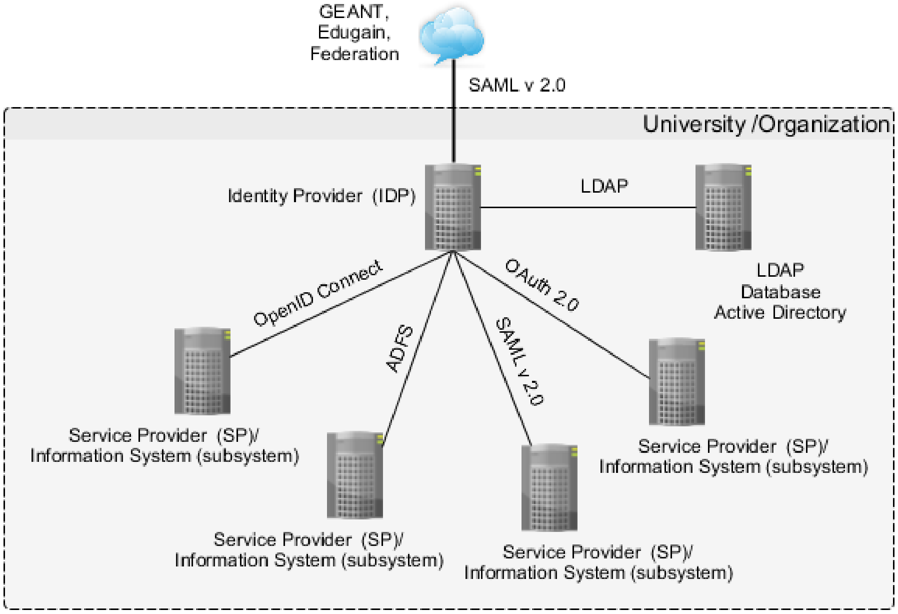


Figure 5. Example of protocols variety

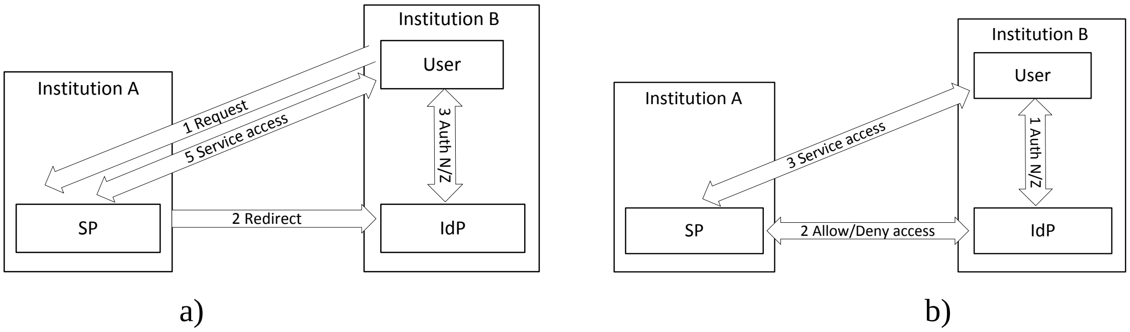


Figure 6. Access to federated services

4. IDENTITY FEDERATION

Access to interinstitutional resources without risk of personal data loss is an important moment in developing fruitful collaborations at national or international levels. In this sense, the operator of the National Research and Education Network RENAM launched identity federation that is named LEAF[7] and continues to improve it operation and used technologies in order to provide a modern service for Research and Educational community of Moldova. LEAF is operating the united internal IdM registered to eduGain, and offering access to three SPs for local purposes. In addition, in order to comply with tendences on identity management marketplace and to follow modern requirements, LEAF team continuously tests and deploying new operational solutions.

REFERENCES

1. www.geant.net, “Federating GN3 Services – Géant”

2. www.geant.net, “Identity Federations”

3. Bogatencov P., Pocotilenco V. Implementation of PKI IDP Management Systems for Access to Resources of European R&E E-Infrastructures. Proceedings of ITSEC-2012 International Conference on Information Technologies and Security, 15-16 October 2012, Chisinau: NCAA, 2013, pp. 227-237. ISBN 978-9975-4172-3

4. Bogatencov P., Pocotilenco V. Implementation of national IdP Management Systems for Access to Resources of European R&E E-Infrastructures. “Networking in Education and Research”, Proceedings of the 11th RoEduNet IEEE International Conference, Sinaia, Romania, January 17-19, 2013, pp. 96-100. ISSN-L 2068-1038.

5. https://tnc2012.terena.org/core/presentation/26, Andreas Åkre Solberg, Roland Hedberg. “GÉANT Federation”, TNC2012

6. http://docs.oasis-open.org, “SAMLV2.0 Technical Overview”

7. http://federations.renam.md, LEAF Federation description

Uncertainty Analysis of Attacker - Defender Interactions in MANET Based on Game GSPN with Intuitionistic Fuzzy Parameters

Guțuleac Emilian, Gîrleanu Ion, Iavorschi Inga, Furtuna Andrei

Technical University of Moldova
168, Stefan cel Mare Bd., MD-2004, Chisinau, Republic of Moldova
Tel: +37322509915, e-mail: emgutul@yahoo.com

ABSTRACT

This paper presents a comprehensive approach to model an expected attacker- defender interaction in a mobile Ad-hoc wireless network (MANET), which combines utilization of theoretical games methods, intuitionistic fuzzy logic and generalized stochastic Petri nets (GSPN), under which it is carried out the security modeling and QoS analysis of MANET with uncertain parameters due to uncontrollable factors. The validity of the proposed model is illustrated by an example with triangular fuzzy intuitionistic numbers using (α, β)- cuts analysis to show how it can be applied to the proposed approach, which better represents both dimensions of uncertainty, stochastic variability and inaccuracy in the shaping of this type systems. To demonstrate the usability of the method in different threat environments, an illustrative example with triangular intuitionistic fuzzy numbers is provided.

Keywords: game, theoretic, approach, intuitionistic, fuzzy, parameter, probability, mobile, ad-hoc, stochastic, Petri, nets, attacker, defender, interaction.

1. INTRODUCTION

Mobile Ad hoc Networks (MANETs) are becoming very attractive and useful in many kinds of communication and networking applications [10, 17, 19, 23]. This is due to their efficiency, relatively low cost, and flexibility provided by their dynamic infrastructure. MANET is a self-organizing computer networks, formed by the cooperation of mobile computer devices, called nodes, that communicate over relatively bandwidth constrained wireless links. Since the nodes are mobile, the MANET topology may change rapidly and unpredictably over time. The network is decentralized; where all network activity including discovering the topology and delivering messages must be executed by the nodes itself. i.e., routing functionality will be incorporated into mobile nodes [19]. However, because of the special characteristics such as wireless communication medium, lack of any infrastructure and mobility of the network nodes, the MANETs are prone to various passive and active security attacks which may be launched by the insider or outsider attackers [4, 17].

An appropriate model of attacker – defender behavior interactions is a key requirement for quantitative security evaluation of MANET nodes. In this context, there is a necessity of describing node's behavior and evaluate the dependability behaviors which is the capacity of a MANET node to complete its mission, in a defined time frame, in the presence of failures and security attacks.

The security community can benefit from the mature dependability modeling techniques, which can provide the operational measures that are so desirable today. On the other hand, by adding hostile actions to the set of possible fault sources, the dependability community will be able to make more realistic models than the ones that are currently in use [4, 7, 11, 14, 16].

Traditional methods for modeling and evaluating the MANET's QoS, nodes parameters and safety behavior are failures tree, attack tree and theoretical game [3, 9, 12, 15, 21, 24]. However, such methods focus upon evaluation of static behaviors of the net while ignoring the dependencies of events or time aspects of failures and attacks. Thus these methods cannot be used to predict in details the behavior of MANET nodes and particularly for real intentional attacks scenarios. Model-based vulnerability analysis of MANET nodes, checks the security properties via state-space exploration is more suitable for accurately describing the states during the operation of protocol and quantitatively analyzing the vulnerability. Automated computational analyses are commonly used in model-based vulnerability analysis of protocol, because this behavior can be translated into the identifiable type model using formal language. Due to the advantage of quick construction and numerical analysis, analytical modeling techniques, such as continuous time Markov chains (CTMC) and generalized stochastic Petri nets (GSPN) [3, 16, 22, 23, 25], have been used for performance analysis of communication, computer and industrial systems [7, 11, 16]. In addition, analytical modeling is a less costly and more efficient method. It generally provides the best insight into the effects of various parameters and their interactions. Hence, analytical modeling is the method of choice for a fast and cost effective evaluation of MANET.

As a combination, the stochastic game-based methods with GSPN contain the advantages of both stochastic model and game theory [12, 13]. Based on the GSPN model, game theory can be introduced to correctly model intentional attacks upon a system and the attacker strategies are regarded as part of the set of transition probabilities between the states [9, 21, 27]. There are increasing numbers of researches involving vulnerability analysis based on stochastic game [21, 27].

These traditional methods, like probabilistic models CTMC and GSPN [7, 11, 14, 23], for quantitative QoS analyze uses data from component parameters (component's failures and repairing rates, security attack rates and defense rates, etc.) which are known with a certain precision and validated via real experiments. However, unfortunately only experiments are not enough for validating with high precision failures parameters, vulnerabilities, and attacks. In addition, because the structure changes dynamically our knowledge about a potential successful attack is minimized. Thus, in order to elaborate adequate security mechanisms, it is necessary to elaborate new approaches in order to understand and describe wireless nodes behavior, to be capable of analyzing their vulnerabilities and estimate quantitatively their QoS parameters.

The classical QoS evaluation methods assume that accurate data is available to determine the best alternatives among the available options. However, in practice, due to the inherent uncertainty and impression of the available data, it is often impossible to obtain accurate information. Therefore, quantitative QoS evaluation under fuzzy environment problem is an interesting research topic, which had received more and more attention from researchers during the last several years.

In order to describe more accurately the expected behavior of attackers interactions with defense of MANET nodes, in this paper it is presented a new approach for modeling and evaluating the quantitative QoS which combines the utilization of theoretical stochastic games method, intuitionistic fuzzy logic [2] and GSPN that extends the work of [12, 13]. Combining these paradigms a new class of GSPN with stochastic games and intuitionistic fuzzy firing rates of timed transitions is defined, called IFGSPN. The advantage of combining these approaches is that IFGSPN models describe in a more realistic way the expected behavior of attackers, the behavior of the security system and dependability being taken into account. Also, the time aspect and intuitionistic fuzzy parameters are introduced in this paper for characterizing the success probabilities of attacker's actions, which most often are ignored. In addition, these models allow to evaluate some QoS parameters and can help to estimate expected losses, associated with different attack and defense strategies. In this context a numerical example is examined to demonstrate the applicability of the IFGSPN approach proposed in this paper.

To our knowledge, there is no analytical uncertainty analysis of attacker-defender interactions in MANET nodes in terms of the end-to-end delay and throughput on game GSPN with fuzzy intuitionistic parameters.

2. ELEMENTS OF STOCHASTIC GAMES THEORY AND INTUITIONISTIC FUZZY LOGIC

To facilitate the description of this work, here we are to introduce first some relevant basic preliminaries, concepts of stochastic game theory (SGT) and intuitionistic fuzzy sets [2].

Basic concepts of SGT. Game theory is the way to handle the problems where multiple conflicting interests' situation exists. In MANET the interactions between the attacker and the defender is taken as two players. So the SGT provides a range of instruments that can be efficiently used for modeling the interaction between independent nodes and intruders in a MANET [21, 27]. In a theoretical stochastic game, players are independent decision factors; their gain depends on other player's actions. In a MANET, nodes have the same behavioral characteristics. This similarity leads to a tight mapping between components of traditional SGT and elements of this network type.

Based on the IFGSPN model we built before and afterwards we introduce stochastic game using the immediate transitions in order to create a generic and sound framework for computing the expected malicious behaviors of attackers. As a consequence, we decide to take advantage of the SGT mentioned in [12, 21] as a mathematical tool. We regard each malicious action, which may cause a transition of the current behavior of MANET node, as an action in a game where the attacker's choices of action are based on consideration of the possible consequences. The interactions between the attacker and the security system itself can then be modeled as a current stochastic game associated with the immediate transitions what they are in conflict in IFGSPN model.

This stochastic game, in the context of security analysis, is usually regarded as a two-player, zero-sum, multistage game where, at each stage, the parameters of the game depend on the current state of the IFGSPN mentioned above. Instantly after a MANET node is attacked, the intruder, after analyzing the vulnerability, seldom has the possibility to select between multiple atomic attack actions. An attack action can be considered successful if these actions produce an undesired transformation to the current system state of MANET node. Considering player *A* (the intruder) with a multitude of actions *A*={ $a_1, a_2, ..., a_m$ } and player *D* (the defense) with a multitude of actions *D*={ $d_1, d_2, ..., d_n$ }, the defense system has as its mixed strategy the probabilistic vector $\vec{q}^2 = (q_1^2, q_2^2, ..., q_n^2)$. Considering the reward matrix $\hat{\rho} = (\rho_{i,j})$, *i*=1, 2,…, *m*, *j*=1, 2, …, *n*, where $\rho_{i,j}$ represents the gain of player A in case he uses the action a_i, and player *D* uses the action d_j. In this paper, we will use a matrix game where a Nash's equilibrium exists and players use mixed strategies [5].

Intuitionistic fuzzy sets (IFS). The theory of fuzzy sets and fuzzy numbers concepts [2, 6] are used because there is a need to quantitatively show imprecise values, where the range of values that is taken by the membership function is not limited by two values, but is extended to the entire range [0,1]. The grade of membership of an element in a fuzzy set is represented by the real value between 0 and l. It does indicate evidence for this element but does not indicate evidence against it. The fuzzy set was extended to develop the IFS [9, 11] by adding an additional *non-membership* degree and degree of *hesitancy*, which may express more abundant and flexible information as compared with the fuzzy set [2]. This degree of hesitancy is nothing but the uncertainty in taking a decision by a decision maker.

Fuzzy numbers are a special case of fuzzy sets and their importance is for more real applications [1, 2, 6]. As a generalization of fuzzy numbers, an intuitionistic fuzzy numbers (IFN) seems to suitably describe an ill-known quantity [2]. Here we are to introduce first some relevant basic preliminaries, notations and definitions of IFS and IFN.

Let a non-fuzzy universal set X be fixed. An IFS A in X is defined as object of the following form $A = \{(x, \mu_A(x), \nu_A(x)) : x \in X\}$, where $\mu_A(x) : X \to [0,1]$ and $\nu_A(x) : X \to [0,1]$ define the degree of *membership* and the degree of *non-membership* of the element $x \in X$ respectively and for every $x \in X$, $0 \le \mu_A(x) + \nu_A(x) \le 1$[??]. The value of $\eta_A(x) = 1 - \mu_A(x) - \nu_A(x)$ is called the degree of *non-determinacy* (or *uncertainty*) of the element $x \in X$ to the intuitionistic fuzzy set A. Obviously, $0 \le \eta_A(x) \le 1$. When $\eta_A(x) = 0$, then an intuitionistic fuzzy set becomes fuzzy set:

$$\{(x, \mu_A(x), 1 - \mu_A(x)) : x \in X\}.$$

An IFN is as an IFS defined over the real axis IR_+. An IFS $A=\{(x,\mu_A(x),\nu_A(x)):x\in IR_+\}$ of a real number is called IFN if: (i) there exists real numbers $x_0 \in IR_+$ such that $\mu_A(x_0)=1$ and $\nu_A(x_0)=0$; (ii) membership μ_A of A is fuzzy convex and non-membership ν_A of A is fuzzy concave; (iii) μ_A is upper semi-continuous and ν_A is lower semi-continuous; (iv) support ($(A)=\overline{(\{x\in IR_+ : \nu_A(x)<1\})}$) is bounded. Therefore, an IFN A is a conjecture of two fuzzy numbers, namely A^+ with a membership function $\mu_{A^+}(x)=\mu_A(x)$ and A^- with a membership function $\mu_{A^-}(x)=\nu_A(x)$.

Two type of IFN are most often encountered in applications: triangular IFN (TIFN) and trapezoidal IFN (TzIFN). In most situations, is recommended to use TIFN for the reason of computational complexity [2]. Thus, a TIFN $\tilde{A}=[a_2;(a_1,a_3);(a_1',a_3')]$ with parameters $a_1'\le a_1\le a_2\le a_3\le a_3'$ is a special IFS on the real number set IR_+, whose membership and non-membership functions are defined as follows:

$$\mu_{\tilde{A}}(x)=\begin{cases}(x-a_1)/(a_2-a_1), & a_1\le x\le a_2\\ (a_3-x)/(a_3-a_2), & a_2\le x\le a_3\\ 0, & \text{otherwise}\end{cases}, \qquad \nu_{\tilde{A}}(x)=\begin{cases}(a_2-x)/(a_2-a_1'), & a_1'\le x\le a_2\\ (x-a_2)/(a_3'-a_2), & a_2\le x\le a_3'\\ 1, & \text{otherwise}\end{cases}.$$

In the application with NFITs of $\tilde{A}$, they are represented as $\tilde{A}=[a_2;(a_1,a_3);(a_1',a_3')]$ or by (α,β)-*cut* sets, denoted $\tilde{A}_{\alpha,\beta}=[\tilde{A}^\alpha;\tilde{A}^\beta]$ with $\tilde{A}^\alpha\cap\tilde{A}^\beta=\varnothing$, that $\tilde{A}_{\alpha,\beta}$ is a crisp subset of IR_+, where $\tilde{A}^\alpha=\{x\in X:\mu_{\tilde{A}}(x)\ge\alpha\}$ and $\tilde{A}^\beta=\{x\in X:\nu_{\tilde{A}}(x)\le\beta\}$ with $0\le\alpha\le1$, $0\le\beta\le1$, and $0\le\alpha+\beta\le1$.

To represent a NFIT, the following closed intervals are often used:

$$\tilde{A}^\alpha=[a_1+\alpha(a_2-a_1),\, a_3-\alpha(a_3-a_2)] \text{ and } \tilde{A}^\beta=[a_2-\beta(a_2-a_1'),\, a_2+\beta(a_3'-a_2)].$$

3. IFGSPN MODELING OF ATTACKER - DEFENDER INTERACTION IN MANET NODES

Analogously to dependability analysis, we regard security breach states of MANET nodes as failure states in the security community. In this paper, a malicious attack toward MANET nodes will therefore result from malicious behaviors which have been successful in exploiting existing vulnerabilities.

While investigating QoS systems, known information about values of component's failure parameters, attack rates, risks and vulnerabilities, etc. are, in general, not perfects [1, 6, 11]. The uncertainty of real values of the quantitative parameters can have two origins. First source of uncertainty comes from the randomness character of the information that has a natural stochastic variability. The second source of epistemic uncertainty is related to imprecise and incomplete character of information, because there is no knowledge about real values of system quantitative parameters, which change dynamically their state. Therefore, in order to make our modeling approach more accurate, realistic, and versatile that describe the behavior of the attacker and defense interactions of the MANET nodes, it is necessary to take into account the probabilistically and fuzzy aspects [12, 22]. This can be implemented by defining a new extension of GSPN, which has quantitative attributes that can have intuitionistic fuzzy values and incorporate the stochastic game, associated with immediate transitions in structural conflict, in way to handle the problems where two conflicting interests situation exist and appears between the attackers and defender. Thus, we use the timed transitions with intuitionistic fuzzy firing rates to determine the intuitionistic fuzzy state probabilities of MANET nod behaviors [1, 6].

Definition 1. A generalized Petri net (GPN), denoted Γ, is a 10-tuple structure of objects: Γ = < *P*, *T*, *Pre*, *Post*, *Test*, *Inh*, K_p , *Pri*, *G*, M_0 >, where: $P \neq \varnothing$, |*P*| = *k*, represents the set of places, which describes the local state of net. Places can contain a positive number of tokens. A place is usually represented as a circle graphically; $T \neq \varnothing, |T|$ = *n* and $P \cap T = \varnothing$, is the set of transitions, which describes the event or the actions and induces the state change. A transition is usually denoted as a rectangle or a line graphically; *Pre*, *Test* and $Inh{:}P \times T \times IN_+^{|P|} \to IN_+$ are forward incident functions relative to transition: *Pre* is the forward incident function, *Test* (and *Inh*) is the promoter (inhibition) function of transition; $Post{:}T \times P \times IN_+^{|P|} \to IN_+$ is the backward incident function relative to transition; $K_p{:}P \times IN_+^{|P|} \to IN$ is the capacity function of places; $Pri{:}T \times IN^{|P|}_+ \to IN_+$ is the dynamical priority function, for firing transitions enabled by current marking; $G: T \times IN_+^{|P|} \to \{true,\ false\}$ it the guard function of transitions; IN_+ is the set of non-negative integers; M_0 is the initial marking.

A place from which an arc originates is considered to be an input place of a transition in which the arc terminates. A place in which an arc terminates is considered to be an output place of a transition from which the arc originates. Token is another important sign, it usually denoted as solid dot and contained in places to represent the state of GSPN. The dynamic behavior of auto modified Γ net is managed and controlled by the firing rules described in [7, 8, 14].

Definition 2. A GSPN with IFN firing rates of timed transitions and stochastic games of immediate transitions, named IFGSPN, is a structure of objects, described by a 7-tuple: $\tilde{\Gamma} =<$ $\hat{N}, \hat{\Gamma}, w, \pi, \hat{\rho}, \tilde{\Lambda}, \mu_\lambda, \nu_\lambda\ U >$, where: $\hat{N} = \{1, 2, ..., \hat{n}\}$ denote the player set; $\hat{\Gamma}$ is a timed stochastic GPN type Γ, where the finite set of transitions T can be divided into two categories, immediate transitions T^0 and timed transitions T^τ, $T = T^0 \cup T^\tau$, $T^0(M) \cap T^\tau(M) = \varnothing$ with $\mathrm{Pr}\,i(T^0) > \mathrm{Pr}\,i(T^\tau)$. The transition $t_k \in T^0$ can be fired randomly and the delay is zero, and they are usually represented as thin bars. T^τ is the set of timed transitions and with each of which is associated a random firing delay time that have an exponential-negative distribution. In its turn $T = \bigcup_{l=1}^{\hat{n}} T_l \bigcup T_r$, $\bigcap_{l=1}^{\hat{n}} T_l \bigcap T_r = \varnothing$ is partitioned so that subset T_l , *l*=1,… $\hat{n}$ is associated with player *l*, and T_r the rest of transitions; $w: T^0 \times IN_+^{|P|} \to IR^+$ is the weight function $0 \leq w(t, M) < +\infty$ which determines the firing probability $q(t, M)$ of immediate transition $t \in T^0(M)$ in current marking *M*, which describes a probabilistic selector; IR^+ is a set of real non-negative numbers; $q^\rho : T_l \to [0, 1]$ is the decision politic, represented by the probability of selecting a particular immediate transition; $\hat{\rho}: T \to (\hat{\rho}_1, ..., \hat{\rho}_l, ..., \hat{\rho}_{\hat{n}})$ is the payoff function,

$\hat{\rho}_l \in (-\infty, +\infty)$; $\widetilde{\Lambda} : T^{\tau} \times IN_{+}^{|P|} \rightarrow IR^{+}$ is the function that determines the intuitionistic fuzzy firing rate $0 < \widetilde{\lambda}(t, M) < +\infty$ of timed transition $t \in T^{\tau}$, that is enabled by current marking M, the parameters of exponential-negative law. In this case IR^{+} is the set with non-negative numbers; $\mu_{\lambda} : \widetilde{\Lambda} \rightarrow [0, 1]$ and $\nu_{\lambda} : \widetilde{\Lambda} \rightarrow [0, 1]$ are the membership degree and the non-membership degree, respectively of $\widetilde{\lambda}(t, M) \in \widetilde{\Lambda}$, which determines the numerical intuitionistic fuzzy values for firing rate of timed transitions; U is the payoff function of attackers of MANET and MANET node security system itself.

With each token in place $p_i^l \in (t_k^{\bullet} \wedge {}^{\bullet}t_j), t_k \in T_l^0, t_j \in T_l^{\tau}$ of player l is assigned a reward $r_j^l(p_i)$ as its property what it is in p_i^l. Players get the reward $r_j^l(p_i)$ after the firing of the transition $t_j \in T_l^{\tau}$, and this reward is recorded in the reward vector of the player *l*. For the sake of simplicity and to fit our attacker-defender model, we assume that our stochastic game is a two-player discounted stochastic game.

The attacker's goal is to compromise functionality of a MANET's node. In figure 1 it is presented the GSPN1 model subjacent of IFGSPN1 that describes interaction between attacker and security system in a MANET node for four strategies.

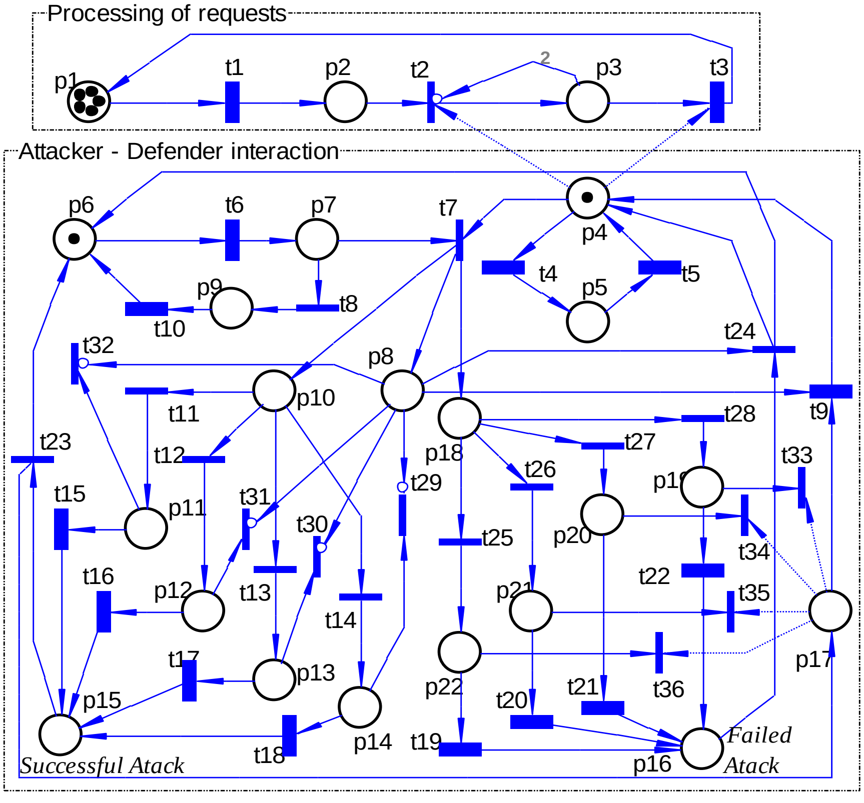


Figure 1. GSPN1 subjacent of IFGSPN1model.

The IFGSPN1 model was built using the methodology described in [7]. In figure 1 the places and transitions are following meaning:

- *places*: p_1- potential number of users using the node; p_2- requests in waiting for processing queue; p_3- request in process; p_4- operating safety state; p_5- failures; p_6- intruder starts the attack; p_7- intruder has attacked; p_8- the attack is detected by security system; p_9- intruder has abandoned the attack; p_{10}- selecting attack strategy; p_{11}, p_{12}, p_{13} and p_{14}- intruder has selected a specific attack strategy a_1, a_2, a_3, a_4; p_{15}- attack has succeeded; p_{16}- attack has failed; p_{17}- security system is damaged (system restore started) ; p_{18}- selecting defense strategy.
- *transitions*: t_1- users requests arriving; t_2- allocation of resources for processing one request; t_3- processing the requests; t_4- occurrence of a failures; t_5- reparation; t_6- analyzing the vulnerabilities and attacking the system; t_7- attack detection; t_8- abandoning the attack; t_9- restoring damaged system after an attack; t_{10}- activities related to abandoning an attack; t_{11}, t_{12}, t_{13} and t_{14}- selecting an respective attack actions: a_1, a_2, a_3 and a_4 (for example: Sybil attack, Selfish attack, RREQ flooding attack and Black hole attack ; t_{15}, t_{16}, t_{17} and t_{18}- attack activities associated with attack action selected by the intruder a_1, a_2, a_3, a_4; t_{19}, t_{20}, t_{21} and t_{22}- respective defense activities d_1, d_2, d_3, d_4 of security system; t_{23}- the start of system restore action; t_{24}- starting the process of processing user requests after attack failed; t_{25}, t_{26}, t_{27} and t_{28}- selecting a respective defense action: d_1, d_2, d_3, d_4; t_{29}, t_{30}, t_{31} and t_{32}- abandoning the attack in case the defense system succeeded; t_{33}, t_{34}, t_{35} and t_{36}- abandoning the defense and start restoring the system in case the attack succeeded.

The firing rates of timed transitions t_i is expressed in form of the TIFN presented as (α,β)- *cuts*, $\alpha \in [0,1]$ and $\beta \in [0,1]$, with respectively trust intervals [2]: $\widetilde{\lambda}_i^{\alpha} = (\lambda_i^{\alpha} + \gamma_i'^{\alpha} \cdot \alpha,\ \lambda_i^{\alpha} - \gamma_i''^{\alpha} \cdot \alpha)$, (resp. $\widetilde{\lambda}_i^{\beta} = (\lambda_i^{\beta} + \gamma_i'^{\beta} \cdot \beta,\ \lambda_i^{\beta} - \gamma_i''^{\beta} \cdot \beta)$, where $\gamma_i'^{\alpha}$ (resp. $\gamma_i'^{\beta}$) and $\gamma_i''^{\alpha}$, (resp. $\gamma_i''^{\beta}$) are coefficients that determine *certainty* $\widetilde{\lambda}_i^{\alpha}$, (resp. *uncertainty* $\widetilde{\lambda}_i^{\beta}$) for left and right intervals, respectively. In case that (α,β)-cut is previously determined and is taking $\gamma_i'^{\alpha} = \gamma_i''^{\alpha} = \gamma_i^{\alpha}$, (resp. $\gamma_i'^{\beta} = \gamma_i''^{\beta} = \gamma_i^{\beta}$) the IFTN $\widetilde{\lambda}_i$ will be expressed by $\widetilde{\lambda}_i = ((\lambda_i^{\alpha}, \gamma_i^{\alpha}); (\lambda_i^{\beta}, \gamma_i^{\beta}))$, which is reduced to calculation.

Intruder’s goal is to maximize his gain by selecting some attack strategies $q_i^1(a_i)$, and the security system will select a respective defense strategy $q_i^2(d_j)$ in order to minimize its losing caused by intruder. The expected intruder’s gain is expressed by the following expression [5, 12]:

$$U^1 = \max_{q_i^1} \min_{q_i^2} \sum_{\forall a_i \in A} \sum_{\forall d_j \in D} q_i^1(a_i) \cdot q_i^2(d_j) \cdot \rho_{i,j} .$$

Some numerical QoS indicators, from a successful attack perspective, in case the intruder and the defense system select the pair of actions (a_i, d_j), associated with post-set immediate transitions of place p_{10} (resp. p_{18}) of model IFGSPN1, can be obtain through stochastic game with provided reward matrix $\hat{\rho} = (\rho_{i,j})_{4\times 4}$, which reflects the reward associated with timed transitions t_{14+i} and t_{18+i}, $i = 1, 2, 3, 4$ and intuitionistic fuzzy firing rates for timed transitions.

The IFGSPN1 model was validated using VPNPTool [8, 18], which is a software tool for visual simulation, verification and performance evaluation of QoS indicators for this type models. The IFGSPN1 has bounded, liveness and reversible properties, and therefore underlying embedded CTMC has ergodic property. This model has been analyzed for different intuitionistic fuzzy firing rates values of timed transitions, allow us to determine QoS indicators specified by the user, one of these indicators is the intuitionistic fuzzy probability that MANET node is in safety state, when $\tilde{\pi}_4 = \Pr(M_k(p_4) = 1)$.

To illustrate this approach, we analyzed the part of IFGSPN1 model that describes the attacker-defender interactions with the following value of the payoff matrix elements:

$$\rho_{1,1} = 20,\ \rho_{1,2} = 30,\ \rho_{1,3} = 50,\ \rho_{1,4} = 20,\ \rho_{2,1} = 40,\ \rho_{2,2} = 10,\ \rho_{2,3} = 20,\ \rho_{2,4} = 50,$$
$$\rho_{3,1} = 30,\ \rho_{3,2} = 50,\ \rho_{3,3} = 40,\ \rho_{3,4} = 20,\ \rho_{4,1} = 10,\ \rho_{4,2} = 30,\ \rho_{4,3} = 30,\ \rho_{4,4} = 40 .$$

For this payoff matrix we get the following strategies: $\vec{q}^{\,1}(A) = (0.061, 0.388, 0.510, 0.041)$ and $\vec{q}^{\,2}(D) = (0.082, 0.143, 0.367, 0.408)$ with expected payoff: $U^1 = 32.45$.

The TIFN values of respective timed transitions firing rates $\tilde{\lambda}_i = [\hat{\lambda}_i^\alpha; \hat{\lambda}_i^\beta]$with$\hat{\lambda}_i^\alpha = (\lambda_i^\alpha, \gamma_i^\alpha)$, $\hat{\lambda}_i^\beta = (\lambda_i^\beta, \gamma_i^\beta)$ and $\tilde{\lambda}_i = \hat{\lambda}_i^* \cdot 10^4 \sec^{-1}$ are the following:

$$\hat{\lambda}_6^* = [(0.1 + 0.9\alpha), (1.1 - 0.1\alpha);\ (1 - 0.95\beta), (1 + 0.2\beta)],\ \hat{\lambda}_4^* = 30,\ \hat{\lambda}_9^* = \hat{\lambda}_{10}^* = [(3 + \alpha, 5 - \alpha); (4 - \beta, 4 + \beta)],$$
$$\hat{\lambda}_{15}^* = \hat{\lambda}_{19}^* = [(4 + \alpha, 6 - \alpha); (5 - \beta, 5 + \beta)],\ \hat{\lambda}_{16}^* = \hat{\lambda}_{20}^* = [(3 + \alpha, 5 - \alpha); (4 - \beta, 4 + \beta)],$$
$$\hat{\lambda}_{17}^* = \hat{\lambda}_{21}^* = [(5 + \alpha, 7 - \alpha); (6 - \beta, 6 + \beta)],\ \hat{\lambda}_{14}^* = \hat{\lambda}_{22}^* = [(7 + \alpha, 9 - \alpha); (8 - \beta, 8 + \beta)].$$

The detailed analysis, for these NFIT firing rates of timed transitions, shows that the confidentiality level of MANET node is NFIT $\tilde{\pi}_{Conf.}(\alpha, \beta) = [\tilde{\pi}_4(\alpha); \tilde{\pi}_4(\beta)]$, where:

$$\tilde{\pi}_4(\alpha) = (0.526317 + 0.073083\alpha,\ 0.661832 - 0.062432\alpha),$$
$$\tilde{\pi}_4(\beta) = (0.5994 - 0.184248\,\beta,\ 0.5994 + 0.091008\,\beta).$$

For these NFIT values, the degree of membership (certainty) $\mu_{\tilde{\pi}_4}(x)$ at $\tilde{\pi}_{Conf.}(\alpha,\beta)$ is:

$$\mu_{\tilde{\pi}_4}(x) = \begin{cases} (x - 0.526317)/0.073083, & 0.52637 \le x \le 0.599400 \\ (0.661832 - x)/0.062432, & 0.599400 \le x \le 0.661832 \\ 0, & \text{otherwise} \end{cases}.$$

Also, the degree of non-membership (uncertainty) at $\mu_{\tilde{\pi}_4}(x)$ at $\tilde{\pi}_{Conf.}(\alpha,\beta)$ is:

$$\nu_{\tilde{\pi}_4}(x) = \begin{cases} (0.599400 - x)/0.184248, & 0.415152 \le x \le 0.599400 \\ (x - 0.599400)/0.091008, & 0.599400 \le x \le 0.690408 \\ 1, & \text{otherwise} \end{cases}.$$

The degree of hesitation at the respective confidence interval of $\tilde{\pi}_{Conf.}(\alpha,\beta) = [\tilde{\pi}_4(\alpha); \tilde{\pi}_4(\beta)]$ is calculated according to the following expression: $\eta_{\tilde{\pi}_0}(x) = 1 - \mu_{\tilde{\pi}_0}(x) - \nu_{\tilde{\pi}_0}(x).$

Figure 2 depicted how the impact of the uncertainty on the attack and defense rates contributes in the degrees of certainty, uncertainty and hesitation on confidentiality MANET node.

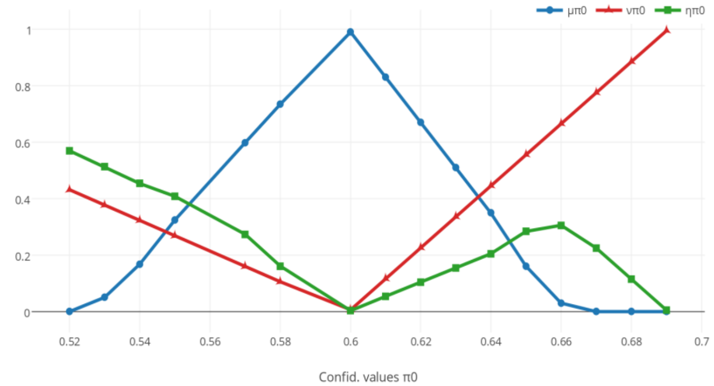


Figure 2. The degrees of certainty, uncertainty and hesitation on confidentiality MANET node $\tilde{\pi}_4(\alpha,\beta)$.

If a performance classification without uncertainty is preferred, it is necessary to either change the set of components or improve the values of parameters used in the security system to reduce its non-uncertainty and hesitation.

5. CONCLUSION

In this papers we present an framework for modeling and evaluating of safety behavior of attacker-defender interaction in MANET nodes using the methods, that we combine the theoretical stochastic games, intuitionistic fuzzy logic and generalized stochastic Petri nets (GSPN), based on which we defined a new class of GSPN with intuitionistic fuzzy firing rates of timed transitions and stochastic games, called IFGSPN. This type of models facilitates the describing expected behavior of the malicious intruder and the behavior of MANET's security system.

In this context, we present a concrete IFGSPN1 model that demonstrate how to describes and analyze the interaction between malicious attacks and defense upon a MANET node, specifying intuitionistic fuzzy parameters and the stochastic game. The validity of the proposed model is illustrated by an example with triangular fuzzy intuitionistic numbers using (α, β) - cuts analysis to show how it can be applied to the proposed approach, which better represents both dimensions of uncertainty, stochastic variability and inaccuracy in the shaping of this type nets in different threat environments.

Moreover, the approach is based on the underlying assumption that the attackers have a complete overview of the security system including states, transition rates, and detection rates, and the game is actually a zero-sum stochastic game; these might not always be valid assumptions. Thus, games of incomplete information and non-zero-sum games will therefore be another focus of our research by applying the intuitionistic fuzzy stochastic game.

REFERENCES

1. Augustin T., Miranda E., Vejnarova J. Imprecise probability models and their applications // International Journal of Approximate Reasoning.- 2009. – V.50 - N4 - P.581 - 582.

2. Atanassov K. T. Intuitionistic fuzzy sets // Fuzzy Sets and Systems. - 1986. - V. 20 - P. 87-96.

3. Azni A.H, Ahmad R., Azri Z., Noh M., Basari A. S., Hussin B. Correlated Node Behavior Model based on Semi Markov Process for MANETS // International Journal of Engineering Science and Innovative Technology (IJESIT). - 2013. -V.2 - N4 - P.50 - 59.

4. Azni A.H, Ahmad R. Noha Z. Survivability Modeling and Analysis of Mobile Ad Hoc Network with Correlated Node Behavior // Procedia Engineering. - 2013. - N53 - P.435 - 440.

5. Chakeri, A., Sadati, N., Sharifian, S. "Fuzzy Nash equilibrium in fuzzy game using ranking fuzzy numbers", in: IEEE International Conference on Fuzzy Systems (FUZZ), pp.1-5 (2010).
6. Costa C., Benjamin, G., Bedregal, C., Doria Neto A. D. "Intuitionistic Fuzzy Probability", in: SBIA 2010, A. C. da Rocha Costa, R. M. Vicari, F. Tonidandel, Editors, Proc. LNAI 6404, Springer-Verlag Heidelberg, pp. 273–282 (2010).

7. Guţuleac E. Descriptive compositional HSPN modeling of computer systems // Annals of the University of Craiova. Series: Atomation, Computers, Electronics and Mechatronics, Ed.: Universitaria, Craiova, România. - 2006. -V.3(30), N.2 , P.82-87.

8. Guţuleac E., Boşneaga C., Reilean A. "VPNP-Software tool for modeling and performance evaluation using generalized stochastic Petri nets", in: The 6-th International Conference on D&AS2002, Proc., Suceava, România, pp. 243-248 (2002).

9. Ibidunmoye E. O., Alese B. K., Ogundele O.S. A Game-theoretic Scenario for Modeling the Attacker-Defender Interaction // J. Comput. Eng. Inf. Technol. - 2013. -V.2 - N1- P.1-8.

10. Jawandhiya P. M., Ghonge M. M., Ali M., Deshpande J. A survey of mobile Ad hoc network attacks // International Journal of Engineering Science and Technology. - 2010 - N2 - P.4063–4071.

11. Kahraman C., Tüysüz, F. "Manufacturing System Modeling Using Petri Nets", in: Prod. Engr. & Manage, C. Kahraman, M. Yavuz, Editors, STUD-FUZZ 252, Springer-Verlag, pp. 95–124 (2010).

12. Lin C., Wang Y. Z., Wang Y. "A Stochastic Game Nets Based Approach for Network Security Analysis", in: The 29th International Conference on Application and Theory of Petri Nets and other Models of Concurrency, Proc., pp.21-33 (2008).

13. Lin C., Wang Y Z., Wang Y. "A Stochastic Game Nets Based Approach for Network Security Analysis", in: The 29 th International Conference on Application and Theory of Petri Nets and other Models of Concurrency, Concurrency Methods: Issues and Applications Workshop, Proc., pp.21-33 (2008).

14. Liu F., Heiner M., Yang M. Fuzzy Stochastic Petri Nets for Modeling Biological Systems with Uncertain Kinetic Parameters. // PLoS ONE. – 2016. –V.11 - N2 - P.1-19.

15. Mattoo M. M, Aziz A. A., Lone S. A. Modeling Malicious Multi-Attacker Node Collusion in MANETs Via Game Theory // Middle-East Journal of Scientific Research. – 2017. – V.25 - N3 - P.568-579.

16. Meng T., Wolter K., Wang Q. “Security and Performance Tradeoff Analysis of Mobile Offloading Systems Under Timing Attacks”, in: Computer Performance Engineering 12th European Workshop, M. Beltran et al., Editors, LNCS 9272, pp. 32–46 (2015).
17. Omar M., Challal Y., Bouabdallah A. Certification-based trust models in mobile ad hoc networks: A survey and taxonomy // Journal of Network and Computer Applications, Elsevier. - 2012.- N35 - P.268-286.

18. Petri Nets Tools Database Quick Overview. https://www.informatik.uni-hamburg.de/TGI/PetriNets/tools/quick.html

19. Prabha C., Kumar S., Khanna R. Wireless Multi-hop Ad-hoc Networks: A Review // IOSR Journal of Computer Engineering (IOSR-JCE). - 2014. V.16 - N2 - P. 54-62.

20. Qazi S., Raad, R., Mu Y., Susilo W. Securing DSR against wormhole attacks in multi rate Ad hoc networks // Journal of Network and Computer Applications. - 2013 - N36 - P.582–592.

21. Raj N. Ann M., Bala P. M. An Attack-defense Stochastic Game Approach for Malicious Nodes in MANETs // Imperial Journal of Interdisciplinary Research, IJIR. - 2016. - V.2 - N4 - P.1035-1040.

22. Sallhammar K., Helvik B. E., Knapskog S. J. On stochastic modeling for integrated security and dependability evaluation // The Journal of Networks. - 2006. - V.1 - N5 - P.31 – 42.

23. Singh S., Singh G., Narasimhan L., Shiwani S. Petri Net Modeling and Analysis of Mobile Communication Protocols UMTS, LTE, GPRS and MANET. International Journal of Engineering Science and Innovative Technology (IJESIT). - 2013. - V.2 - N4 - P.255- 258.

24. Tao M., Shan H. An improved method of the attack tree model for mobile Ad Hoc networks Research // Computer Applications and Software. - 2009. - V. 26 - N4 - P.271 – 273.

25. Yi Z., Dohi T. Survivability Analysis for a Wireless Ad Hoc Network Based on Semi-Markov Model // IEICE Transactions on Information and Systems. - 2012. -V.E95.D - N.12 - P.2844-2851.

26. Yadav P., Gaur M. “A Survey on Formal Modeling for Secure Routing in Mobile Ad hoc Networks”, in: International Conference on Distributed Computing and Internet Technology, ICDCIT, pp.18-23 (2015).

27. Zhuo W., Lin C., Chen X. Quantitative analysis method of network attack and defense based on stochastic game model // Journal of Computers. - 2010. - V.9 - P.1748 – 1762.

Circular Economy – Clarifying the Concept with the CEPS Framework

Taranic Igor

Centre for European Policy Studies, Belgium
E-mail: tsaranik@gmail.com

ABSTRACT

Circular Economy has recently become one of the most important concepts in the sustainable development debate and beyond, becoming an official policy of the European Union starting by 2015. The scale and complexity of this concept require simplification and the applicability of Circular Economy to different types of economic actors requires clarification. The CEPS framework, described in this paper, is addressing those two challenges.

Key words: circular, economy, sustainable, development, policy, population, resources

1. INTRODUCTION

Past two centuries were an era of unprecedented population growth and economic development. It required immense amounts of natural resources, from energy sources and raw materials to land for agricultural purposes. The economic system in the developed countries, guided by a principle of constant growth, has supported the technological progress and contributed to the improvement of the living conditions in many countries. But it came with a price: global warming, deterioration of soil, air pollution and others. Today the population continues to grow faster than ever and is likely to reach about nine billion people in 2015, according to the United Nations estimations [1]. It means that maintaining the population growth and economic development would require even more energy, raw materials, soil and other resources. In order to contain and reduce the environmental pressures on the planet, we would need sustainable development.

The purpose of this paper is to present one of the most important sustainable development concepts of the current decade – the Circular Economy and its application to various groups of stakeholders (industry, cities, etc.).

The first part of the paper presents the historical development of the sustainable development debate, typology of sustainable development concepts and an introduction to the Circular Economy concept.

The second part of the paper presents the CEPS[2] framework – a theoretical intersection between eight Circular Economy building blocks with different types of economic actors.

2. HISTORICAL DEVELOPMENT OF SUSTAINABLE DEVELOPMENT CONCEPTS

The initial idea of the sustainability as interconnection between the environment, social well-being and economic development is attributed to Rachel Carson's book "Silent Spring" [3], a book also coined as a classic that launched the environmental movement. In 1968, "The Population Bomb" was published [4], in which Paul Ehrlich has presented his idea on the connection between human population and resource exploitation, pointing out the environmental challenges of growing population. Those ideas have sparkled institutional response with establishment of numerous influential environmental organizations that shaped the sustainable development debate since the 1970s [5]:

1969 – Friends of the Earth, an advocacy group

1971 – Green Peace, an advocacy group and global movement

1972 – United Nations Environmental Program (UNEP) and many national environmental protection agencies

1982 – World Resources Institute, an influential think-tank

1989 – Stockholm Environment Institute, an influential research institute

And many other organizations throughout the 1990s, 2000s and 2010s.

The idea of sustainable development entered mainstream thinking in the 1990s and since then was referred to under different names and concepts – low carbon economy, sustainable growth, resource efficient economy, sustainable production and consumption, ecological economics etc.[2]. In 2000s, many of these ideas were integrated under the concept of "Green Economy". Figure 1 shows the sustainability concepts family, presenting complementary concepts of sustainable ideas in different domains and disciplines.

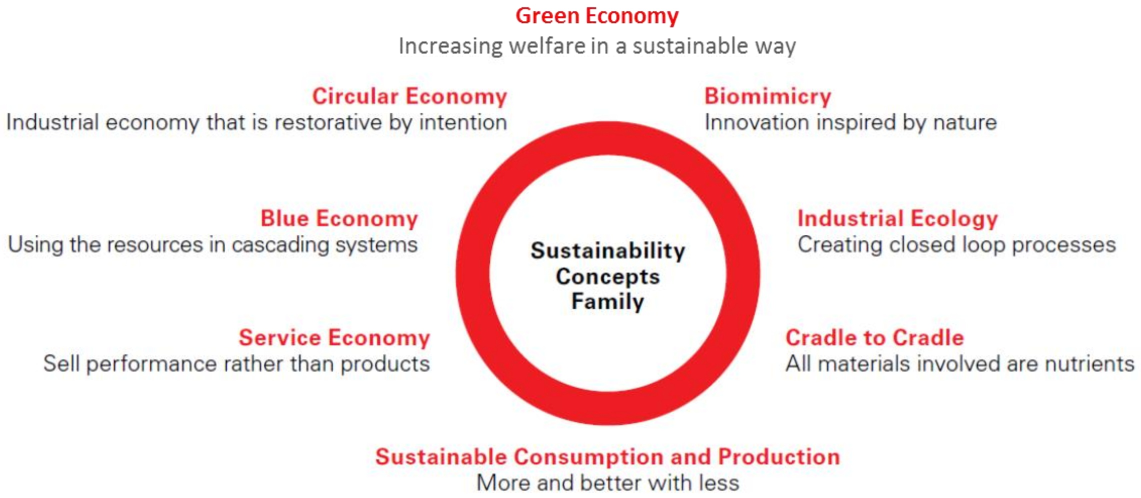

Green Economy
Increasing welfare in a sustainable way
Circular Economy
Industrial economy that is restorative by intention
Biomimicry
Innovation inspired by nature
Blue Economy
Using the resources in cascading systems
Sustainability Concepts Family
Industrial Ecology
Creating closed loop processes
Service Economy
Sell performance rather than products
Cradle to Cradle
All materials involved are nutrients
Sustainable Consumption and Production
More and better with less

Figure 1. Sustainability concepts family (Source: author's adaptation of Lehmann et al. [18])

Circular Economy concept has started developing in the 1970s alongside with industrial ecology, following the principle "everything is an input to everything else" [8]. The concept is challenging the traditional linear industrial process, characterized by low production costs, based on relatively low cost and abundant raw materials. The typical linear lifecycle consists of resource extraction, manufacturing, consuming and disposing the products, also referred to as *take-make-use-dispose*. The circular economy presents an alternative approach, which calls for turning the goods at the end of their lifespan into resource for others through re-use, recycle, re-manufacturing and other practices (Taranic et al. [2]).

Circular Economy became one of the most dominant theoretical and policy concepts in sustainable development in the current decade. Three key reasons stand out:

- Resource scarcity and volatile and increasing energy and materials prices in at the end of 2000s-first part of 2010s
- The idea was popularised by several numerous influential thought leading organisations, including the Club of Rome, Ellen MacArthur Foundation and others
- In 2015, Circular Economy became an official policy of the European Union, making the idea even more widespread

An additional factor explaining the popularity of the Circular Economy concept is that besides environmental benefits, it offers significant micro and macro-economic benefits. The reports prepared by the Ellen MacArthur Foundation and McKinsey, a global management consultancy, show the potential of multi-billion savings in various industries. The Club of Rome points out the positive effects of the Circular Economy on employment [8]. These estimations are important indications for governments and businesses to show their interest and test the concept in practice.

3. The CEPS Framework

There are numerous definitions of Circular Economy in academic and policy literature. Some of them refer to the Circular Economy as a set of practices to make the process of material utilization more efficient. Others see it as a wider concept that should improve the wellbeing of the society. Table 1 provides the summary of the main definitions and interpretations.

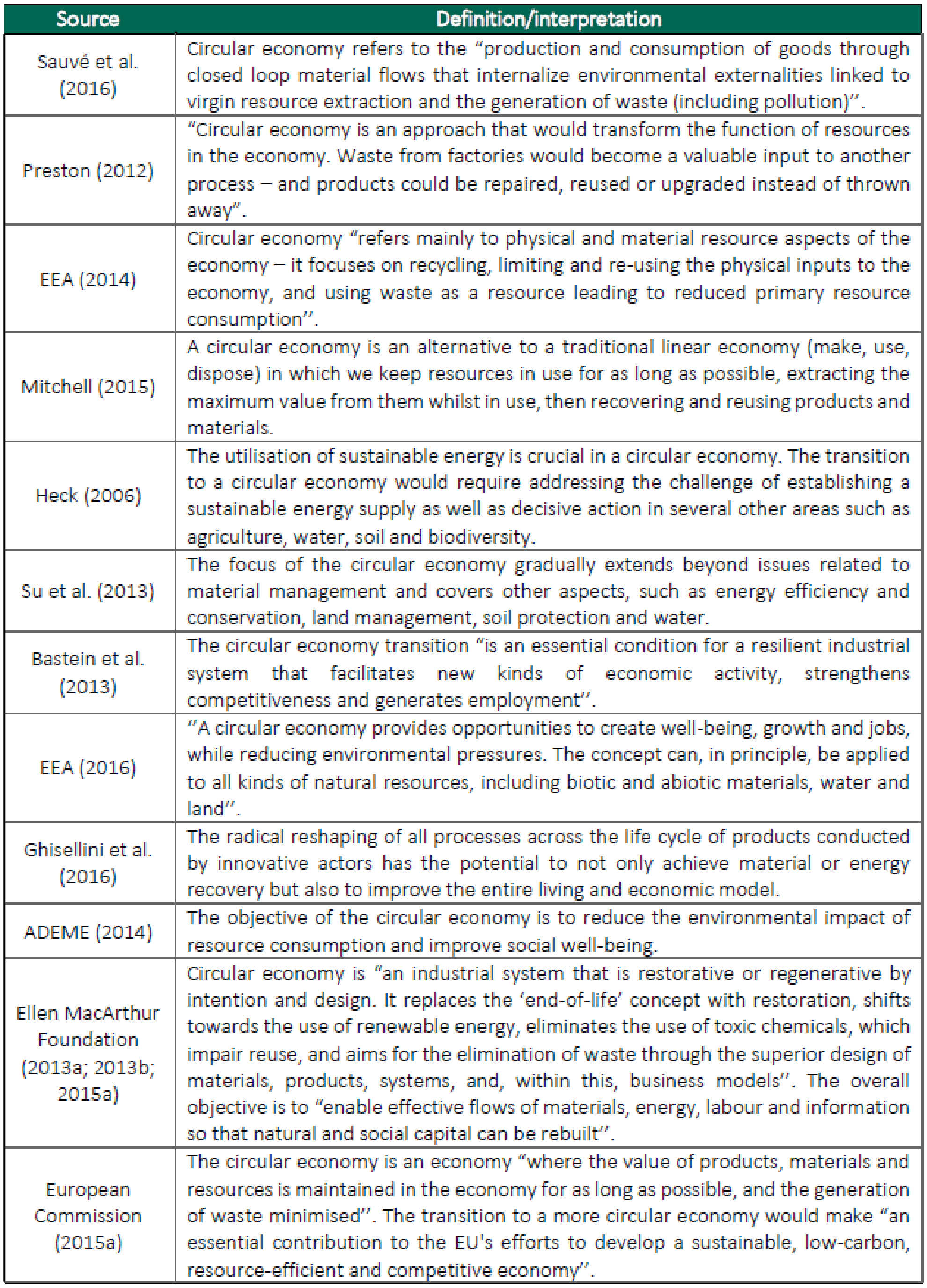
There is also a large number of case studies, demonstrating how various Circular Economy practices were used by different companies. Ellen MacArthur Foundation's website describes dozens of case studies, starting from steel industry, through sustainable food production to textile recycle by fashion brands [9].

But there is a gap in the literature between the theoretical definitions and interpretations of the Circular Economy and specific case studies. It is difficult to turn the definition of the concept into industry's or city's strategy. Taranic et al.[2] aimed to fill that gap by demonstrating how the concept of Circular Economy can be applied by a wider spectrum of stakeholders. Table 2 presents the graphic illustration of their CEPS framework of the interconnection between eight building blocks and five types of stakeholders/economic actors.

3.1. Building blocks

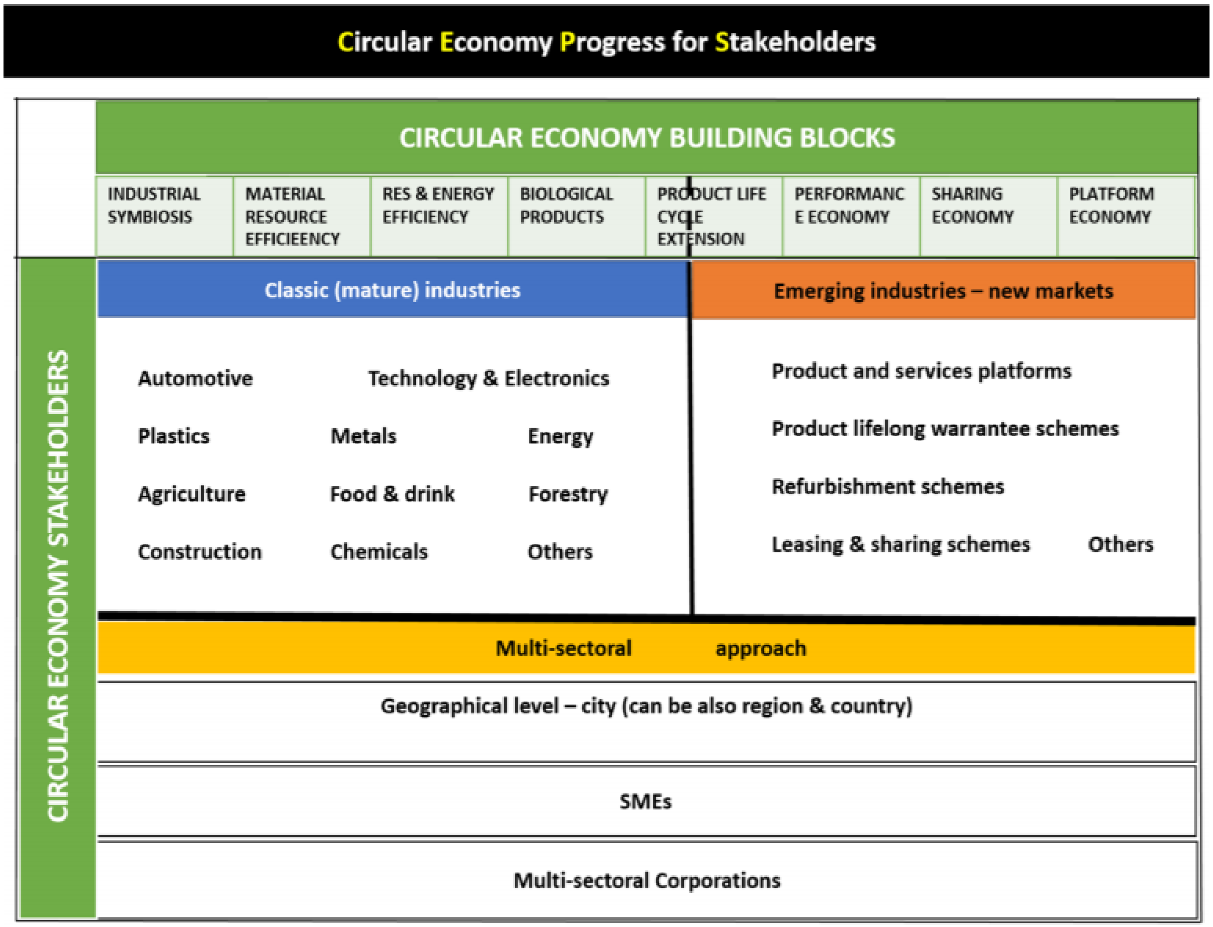
The CEPS framework aims at providing clarity on what factors of the Circular Economy could be applicable to different types of industries and other stakeholders, such as cities and regions, Small and Medium enterprises (SMEs) and multi-sectorial corporations.

Table 1. Circular Economy definitions and interpretations **(**Source: Rizos et al. [7])



Source	Definition/interpretation
Sauvé et al. (2016)	Circular economy refers to the "production and consumption of goods through closed loop material flows that internalize environmental externalities linked to virgin resource extraction and the generation of waste (including pollution)".
Preston (2012)	"Circular economy is an approach that would transform the function of resources in the economy. Waste from factories would become a valuable input to another process – and products could be repaired, reused or upgraded instead of thrown away".
EEA (2014)	Circular economy "refers mainly to physical and material resource aspects of the economy – it focuses on recycling, limiting and re-using the physical inputs to the economy, and using waste as a resource leading to reduced primary resource consumption".
Mitchell (2015)	A circular economy is an alternative to a traditional linear economy (make, use, dispose) in which we keep resources in use for as long as possible, extracting the maximum value from them whilst in use, then recovering and reusing products and materials.
Heck (2006)	The utilisation of sustainable energy is crucial in a circular economy. The transition to a circular economy would require addressing the challenge of establishing a sustainable energy supply as well as decisive action in several other areas such as agriculture, water, soil and biodiversity.
Su et al. (2013)	The focus of the circular economy gradually extends beyond issues related to material management and covers other aspects, such as energy efficiency and conservation, land management, soil protection and water.
Bastein et al. (2013)	The circular economy transition "is an essential condition for a resilient industrial system that facilitates new kinds of economic activity, strengthens competitiveness and generates employment".
EEA (2016)	"A circular economy provides opportunities to create well-being, growth and jobs, while reducing environmental pressures. The concept can, in principle, be applied to all kinds of natural resources, including biotic and abiotic materials, water and land".
Ghisellini et al. (2016)	The radical reshaping of all processes across the life cycle of products conducted by innovative actors has the potential to not only achieve material or energy recovery but also to improve the entire living and economic model.
ADEME (2014)	The objective of the circular economy is to reduce the environmental impact of resource consumption and improve social well-being.
Ellen MacArthur Foundation (2013a; 2013b; 2015a)	Circular economy is "an industrial system that is restorative or regenerative by intention and design. It replaces the 'end-of-life' concept with restoration, shifts towards the use of renewable energy, eliminates the use of toxic chemicals, which impair reuse, and aims for the elimination of waste through the superior design of materials, products, systems, and, within this, business models". The overall objective is to "enable effective flows of materials, energy, labour and information so that natural and social capital can be rebuilt".
European Commission (2015a)	The circular economy is an economy "where the value of products, materials and resources is maintained in the economy for as long as possible, and the generation of waste minimised". The transition to a more circular economy would make "an essential contribution to the EU's efforts to develop a sustainable, low-carbon, resource-efficient and competitive economy".

Table 2: Interconnection between the Circular Economy building blocks and different types of stakeholders (Source: Taranic et al. [2])



Circular Economy Progress for Stakeholders

CIRCULAR ECONOMY BUILDING BLOCKS

INDUSTRIAL SYMBIOSIS	MATERIAL RESOURCE EFFICIEENCY	RES & ENERGY EFFICIENCY	BIOLOGICAL PRODUCTS	PRODUCT LIFE CYCLE EXTENSION	PERFORMANC E ECONOMY	SHARING ECONOMY	PLATFORM ECONOMY

CIRCULAR ECONOMY STAKEHOLDERS

Classic (mature) industries			Emerging industries – new markets	
Automotive	Technology & Electronics		Product and services platforms	
Plastics	Metals	Energy	Product lifelong warrantee schemes	
Agriculture	Food & drink	Forestry	Refurbishment schemes	
Construction	Chemicals	Others	Leasing & sharing schemes	Others

Multi-sectoral approach

Geographical level – city (can be also region & country)

SMEs

Multi-sectoral Corporations

Building block 1 – industrial symbiosis

The origins of the term industrial symbiosis were laid in 1989 by Frosch and Gallopoulos in their “Strategies for manufacturing” article [10]. The essence of their idea was: *“Waste from one industrial process can serve as the raw materials for another, thereby reducing the impact of industry on the environment”* or in other words: *“…a chunk of steel could potentially show up one year in a tin can, the next year in an automobile and 10 years later in the skeleton of a building”.*

Chertow [11] describes industrial symbiosis as a process that involves *“physical exchanges of materials, energy, water, and by-products”* between different co-located industrial facilities, e.g. where waste of one facility is a resource input for another. Industries can share resources for several reasons:

i) increase revenues or reduce costs,

ii) help achieve long-term resource security and
iii) meet regulatory requirements of resource or energy efficiency.

Lombardi and Laybourn [12] claim that industrial symbiosis is not necessarily a physical exchange of materials, but also exchange of knowledge to foster eco-innovation through networks of actors. This interpretation of the industrial symbiosis is very relevant to the current digital age.

Probably the most famous example of an industrial symbiosis is the Kalundborg symbiosis in Denmark, where public and private companies are engaged in exchanging energy, water and materials for more than four decades [13].

One example for eco-innovation networks is European Union's thematic Knowledge and Innovation Communities (KICs) in the domains of energy, climate, raw materials and food. The KICs aim at facilitating the contact between different actors in their thematic value chains, support start-ups and provide educational activities in their domains [14].

Building block 2 – Material resource efficiency

Material resource efficiency refers to reduction of the amounts of material resources and their life cycle environmental impact in production processes [15].

Building block 3 – Renewable Energy Sources (RES) and Energy Efficiency

The concept of the Circular Economy goes hand in hand with energy savings and reducing the use of the fossil fuels and GHG emissions to fight the climate change [2].

Building block 4 – biological products

Modern agriculture was able to keep up with population growth in the last two centuries, but did so in an unsustainable way, partly deteriorating soil and contributing to climate change [16]. While global population continues to grows, the whole value chain of food needs a sustainable transformation.

These are only some of today's challenges: food producers are dependent on pesticides and synthetic fertilizers; distributors of food make excessive use of materials for packaging and consumers generate millions of tones of food waste in the EU alone [16].

There are solutions. An interesting example is an Israeli start-up HomeBiogas developed a small domestic system that converts food waste and animal manure into cooking gas and liquid fertilizers (HomeBiogas.com, 2016) [17]. But it needs to be brought to a larger scale.

Building block 5 – product life cycle extension

Product lifecycle extension aims at designing products with prolonged life spans. For instance, products can be designed to serve longer, easily repairable or upgradable, and finally re-usable and recyclable at later stages of the life cycle (Taranic et al. [2]).

Building blocks 5,7 & 8 – performance, sharing and platform economies

These are three interrelated concepts. Performance economy means providing products as services through renting, leasing and sharing business models. Performance economy refers mainly to Business to Business and Business to Consumers economic activities, such as car leasing, for example (Taranic et al. [2]).

Sharing economy refers to a peer-to-peer activity model of providing access and sharing the access to goods and services. This is a concept that existed for thousands of years. The recent novelty is that digital platforms enable the development of the sharing economy on a larger economic and geographic scale than ever before (Taranic et al. [2]).

3.2. Stakeholders/Economic actors

The CEPS framework identifies several main types of stakeholders in the Circular Economy. The first type is the classic (or mature) industries, such as automotive, chemicals, agriculture, etc.

The second type is the emerging industries, such as companies active in digital platforms (e.g. UBER) and sharing economy (e,g, Airbnb).

The third type is the multi-sectorial approach:

- Cities and regions can have their Circular Economy strategies, depending on the nature of their economic activities. For example, industrial cities and regions could endorse the industrial symbiosis activities, while service oriented cities could facilitate the development of the sharing economy business models
- SMEs are part of every value chain of industry and service provision activities
- Multi-sectorial corporations that are active in different industry types (Taranic et al. [2]).

4. CONCLUSION

This paper has briefly presented the following:

- Historical development of the sustainable development debate, since the end of 1960s till nowadays
- The CEPS framework for the Circular Economy, including:
    - Eight building blocks
    - Five types of main stakeholders/economic actors, active in the circular economy

The CEPS framework is simplifying and clarifying the Circular Economy concept in order to support businesses and policy makers. Further research and practical application are required to assess the effectiveness of the CEPS framework.

REFERENCES

1. UNEP (2004): World population to 2300 http://www.un.org/ esa/population/publications/ longrange2/WorldPop2300final.pdf.
2. Taranic I., Behrens A. and Topi C. (2016): Understanding the Circular Economy in Europe, from resource efficiency to sharing platforms, CEPS special report No. 143.
3. .https://www.ceps.eu/system/files/SR%20No143%20Circular%20Economy_0.pdf.
4. Carson R. (1962): *Silent Spring*, Riverside Press, Boston.
5. Ehrlich P.R. (1968): *The population bomb*, Balantine Books, New York.
6. Sustainable development timeline http://www.iisd.org/pdf/2012/sd_timeline_2012.pdf.
7. Circular Economy. Improving the management of natural resources https://www.satw.ch/fileadmin/user_upload/documents/02_Themen/06_Rohstoffe/circulareconomy_EN.pdf.
8. Rizos V., Tuokko K. and Behrens A. (2017): Circular Economy. A review of definitions, processes and impacts, CEPS research report https://www.ceps.eu/system/files/RR2017-08_CircularEconomy_0.pdf.
9. Wijkman A. and Skånberg K. (2015): The Circular Economy and benefits for society. Jobs and Climate Clear Winners in an Economy Based on Renewable Energy and Resource Efficiency https://www.clubofrome.org/wp-content/uploads/2016/03/The-Circular-Economy-and-Benefits-for-Society.pdf.
10. Ellen MacArthur Foundation (2017): Circular Economy Case studies https://www.ellenmacarthurfoundation.org/case-studies.
11. Frosch R. A. and N. E. Gallopoulos (1989), "Strategies for manufacturing'', Scientific American, Vol. 261, No.3, pp. 144-152.
12. Chertow M.R. (2007), "'Uncovering' Industrial Symbiosis", Journal of Industrial Ecology 11 (1), (http://is4ie.org/resources/Documents/uncovering%20IE.pdf).
13. Lombardi D.R. and P. Laybourn (2012), "Redefining Industrial Symbiosis", Journal of Industrial Ecology 16 (1).
14. http://www.symbiosis.dk/en/.
15. https://eit.europa.eu/activities/innovation-communities.
16. European Environment Agency (2016): Resource efficiency and the low carbon economy https://www.eea.europa.eu/soer-2015/synthesis/report/4-resourceefficiency.
17. European Commission (2015): Average EU consumer wastes 16% of food, most of which could be avoided. https://ec.europa.eu/jrc /en/news/ average-eu-consumer-wastes- 16-food-most-which-could-be-avoided.
18. HomeBiogas.com (2016), "The Ultimate Family Size Biogas System" (https://homebiogas.com/).
19. Lehmann M., de Leeuw B., Fehr E. and Wong A. (2014) Circular Economy. Improving the management of natural resources, Swiss Academy of engineering sciences. https://www.satw.ch/fileadmin/user_upload/documents/02_Themen/06_Rohstoffe/circulareconomy_EN.pdf.

Estimating the Scale of Shadow Economics in IT

Ohrimenco Serghei, Borta Grigori

Academy of Economic Studies of Moldova
E-mails: osa@ase.md, grigori.borta@gmail.com

ABSTRACT

This paper analyzes the approaches to defining a new category – shadow information (digital) economics and its structure. The methods of measuring and level estimation for this domain of economics are analyzed. A set of actions directed towards estimating the scale of shadow information (digital) economics is defined.

Keywords: shadow, information, digital, economics, cognitive, modeling, level, estimation, measuring

1. INTRODUCTION

The recent years show a significant growth of research aimed at shadow economics phenomenon. This includes works related to detailing the contents of the category, analysis of statistical data of shadow activity in general and its components in particular, estimating the scale of this activity, and a search for ways of struggle against it. All of this research is closely related to the "classical" shadow economics, as well as a relatively new phenomenon in economics – shadow information (digital) economics. The research performed by the authors, and publications by many leading experts in the domain allow underlining the following problems, requiring a solution:

- Discussion of the definition of shadow information economics, and the criteria of relating economic activity to it;
- Structure of SIE;
- Factors of SIE development;
- Effects of its existence and functioning;
- Scientific approaches and methods of estimation the scale of SIE;
- Measures of its reduction in the best interest of national security.

Within this paper, the authors analyze the following directions:

- Detailing the definition of SIE;
- The structure of SIE;
- Methods of SIE estimation;

- Definition of SIE.

It is important to note that the term of “shadow economics” is very ambiguous in its understanding and is defined in many different ways by different researchers. Because of this, several approaches are used: from legal point of view, from the socioeconomic point of view, from the technological point of view, etc. Almost all the specialists note the lack of a single universal notion of “shadow” economics, which in the theoretical sense means the refusal of market subjects to use legal norms and the replacement with an alternative mechanism of resolving debates between national and private interests, and in the applied aspect – hidden and prohibited activities.

The main, most widely used definitions of “shadow economics” are as follows:

- “Shadow economics” is defined as the prohibited types of economic and non-economic activities;
- “Shadow economics” is defined only as hidden production;
- “Shadow economics” is comprised all the economic activity, not accounted for by the official statistics or that evades taxation, but is necessary to be calculated and included in GDP.
- “Shadow economics” is the economic activity being that is hidden or forbidden performed within the boundaries of both official (legal) and informal economics.

Further, we analyze one of the approaches in more details from SIE point of view. In the boundaries of the first approach, “shadow economics” is defined as forbidden, underground activity. Indeed, all the activity related to offering goods and services in the boundaries of SIE is defined as illegal and forbidden. Moreover, in this case “shadow economics” should also include non-economic (non-production) types of illegal activity, such as organized crime, extortion, racket, etc. Even though this type of activity are not related to production, forming of prime income, assets, they lead to redistribution of income and assets, and can, therefore, be viewed as economic problems.

In the second case, the notion of “shadow economics” is limited only to hidden production, including legal economic activity. However, this activity is either partially or fully hidden aiming at evading taxes and other duties. A typical example of this kind of activity is freelancing, whose activity cannot be fully overseen.

The third approach reflects all the systematically unregistered economic processes: both legal and illegal.

The correct approach from the economic point of view is the fourth one, though, because in this case the domain in question is the observable one, particularly its “shadow economics” part.

Contemporary international standards on statistics when building the most important macroeconomic indicators as one of the main points include the requirement to account for hidden and informal economics.

2. APPROACHES TO SIE DEFINITION

While studying SIE, it is important to use at least three conceptual approaches to understanding the phenomenon: legal approach, economic approach, economic-legal approach. In order to detail all the criminal activity, one should also use organizational, technical, technological and some of the other approaches along with the economic and legal ones.

Previously conducted research allowed to offer a couple definitions of SIE, the conceptual bases of which are the following:

1. Shadow information economics is a specific sphere of economic activity with according structure and the system of economic relationships. The specificity is defined by illegality, unofficial and criminal character of economic activity and profit concealment.
2. Shadow information economics is the sector of economic relationships, encompassing all the types of production and economic activities, that contradict applicable law by their nature, direction, character, form, composition and are performed contrary to state regulations and bypassing applicable controls.
3. Shadow information economics is all the individual and collective activity that is illegal, related to design, development, distribution, support, and use of components of information and communication technologies hidden from the society. The likeness between shadow economics and shadow information economics is defined by the similarity of characteristics, functions, and descriptions.
4. Thus, shadow information economics is all the illegal and hidden goods and services that use and are based on information technologies. The most important economic elements of this domain are the following: illegal economic relationships, illegal activity, related to production, distribution, and use of illegal goods and services. This domain of activity is also characterized as being parasitic.

3. METHODS OF SIE ESTIMATION

An overwhelming number of researchers separate methods of “classical” shadow economics estimation into two main categories: direct and indirect. Direct methods are the ones that are based on the information gathered from questionnaires and observations over participants (at least in the role of the user) of shadow economics processes. The indirect ones are based on the analysis of summary economic indicators in official statistics, financial institutions, and tax offices.

When estimating the scale of “classical” shadow economics, the goals of statistics are different from the ones posed by law enforcement and taxation authorities: the former try to estimate the scale unregulated economics in order to adjust macroeconomic indicators and to minimize possible errors; the latter aim to estimate the amount of evaded tax in order to persecute the offenders.

In case the necessary statistics are missing, which is typical for shadow information economics, it is preferable to make an estimation based upon certain assumptions, rather than just altogether ignore the existence of shadow economic activity in the sector. This is exactly why macroeconomic estimations of unregistered economics bear an approximate, probability-based character and cannot be used to estimate the shadow economics on the micro level.

One of the difficulties in the research of SIE is the development of an estimation apparatus that will provide its quantitative parameters, because the possibilities of scale estimation are very limited due to the character of the phenomenon that presumes full enclosure. As a result, different methods are being used in order to estimate, their precision depending on many factors, including initial data.

The report outlines the results of analysis of “classical” shadow economics estimation methods, which include the following ones: method of specific indicators, structural method, method of soft modelling, expert estimation methods, combined methods, method of accounting analysis, method of document analysis, methods of economic analysis. Each of the abovementioned methods is analyzed from the conceptual point of view, their benefits and drawbacks, and their optimal applicability criteria. For example, the method of specific indicators uses one index, indicating the level of economic activity and obtained by direct or indirect method, having both benefits and drawbacks. Optimal conditions formation is required in order for this method to be applicable to goods and services estimation in the SIE domain. Furthermore, some methods are specifically tailored to work with specific subjects (e.g. software producing companies), others are tailored to work on macroeconomic level. Abovementioned features allow drawing a conclusion that estimation of SIE, no matter what method is chosen, bears stochastic character and is for the most part subjective.

One of the promising approaches to improve existing methods of SIE scale estimation is, in our opinion, is the use of cognitive modelling, because of its proven effectiveness in research of unstructured systems and processes. In this case, SIE is represented as a set of factors, processes, and phenomena described by a cognitive map. The map reflects subjective representation of a certain phenomenon, regularities inherent to a certain domain by a group of experts.

Conducted research using cognitive maps allowed proposing an estimation of SIE influence over economic and information security of individuals, society, and state. First, shadow economy in general and SIE in particular, directly influences social-economic processes in a country and reduces security level.

It is recommended to perform cognitive analysis and modelling of SIE influence in the following order:

1. Outlining the main threats and their influence over security of the state;
2. Building a cognitive map of SIE influence, describing the main factors characterizing subject area, outlining target factors, and cause-and-effect relationships;
3. Building a cognitive map describing the power of effect and relationship with according model tests for stability and adequacy;
4. Scenario modelling with definition of possible factor, scenario, and situation change;
5. Choice of directions and measures leading to optimal scenario realization.

Authors propose a cognitive map of macroeconomic factors influence upon the level of economic security. The main proposed factors are described below, considering two possible sides of view on the problem: victim and attacker.

- Level of income per capita. Availability of cheap labor due to low average wage, high level of unemployment in developing countries with the condition of high potential profit in the countries that are targets of the attacks (developed countries). This factor may serve as an important component of high attraction and final profit.
- Level of society technology penetration, developed infrastructure – in general this means availability, level, and quality of access to information resources, technologies, and systems. From the attacker's point of view, the better developed is the infrastructure, the easier it is to perform an attack using different attack vector, having wide variety of technological, technical, and information resources available. From the victim's point of view, very often well-developed infrastructure usually means that the country is a developed one, and, therefore, its citizens have more income available, and, thus, are more attractive as an attack target.
- Education level. For the attacker's point of view, high education level means better and deeper understanding of software and hardware, and, consequentially, a possibility to perform more complex and sophisticated attacks. On the other hand, from the victims' perspective, a high level of education means that more complex defense measure are in place. Furthermore, better education should mean better understanding of how to behave in digital world, more responsible attitude towards personal and corporate data.
- Crime level in the country. The higher is the crime level in a certain country, the higher is the probability to find a person willing to commit crime.

The abovementioned factors are intertwined, for the most part, but the following assumption has to be made: in general, the attacker tries to choose the best possible combination of factors, the one that will bring maximal profit. Thus, in a perfect case scenario for the attacker, the executor will be from a country with well-developed infrastructure, but low average wage, and high level of crime; the victim will be from a country with stable economics and high income.

The following factors are characteristic of SIE:

1. The risk of being caught and punished for a crime in SIE domain, is much lower compared to “classical” shadow economics.
2. Initial entrance level is low from both financial and temporal points of view. To start working in SIE, only an Internet-connected computer is required. Furthermore, to start profiting in SIE, deep understanding of technologies in general, and online commerce in particular is not required. Many tools are readily and freely available. Interfaces of many tools are quite easy to understand and begin using. Personal data and credit card data are easily available for sale with no technical skills required.
3. It is much easier to find a client, an executor, or a seller due to how global the Internet has become.
4. Compared to “classical” money transfers, digital transactions are performed much faster and much more secure, and can be performed anonymously.
5. Information goods and services bear much lower risks compared to, for example, selling weapons, drugs, while the amount of profit may be on a similar level.
6. Lower risks of liabilities, including criminal one.

4. CONCLUSION

In authors’ opinion, further research of the phenomenon should be directed at outlining reasons and parameters in its segments.

In conclusion, it is important to note that defining the volume of SIE and certain economic activity (e.g. production and sale of malware, DDoS attacks, etc.) is currently not performed. This can partially be explained not only by the lack of corresponding methods, but also by the lack of an information base, that could serve as a basis for this kind of calculations.

REFRENCES

1. Ohrimenco S., & Borta G. (2012). *Shadow information ecnonomics.* Санкт-Перебург: Партнерство кафедр ЮНЕСКО в области применения ИКТ в образовании. Конференция Института ЮНЕСКО по информационным технологиям в образовании. XIII Международный форум: Формирование современного информационного общества – проблемы, перспективы, инновационные.

2. Ohrimenco S., & Borta G. (2013). *The Structure of Shadow Information Economics.* Chisinau: Internationall Conference on Information Technologies and Security 2012.
3. Ohrimenco S., Sarkisian A., & Borta G. (2012). *Price policy model at the modern shadow market of information technologies.* Sofia: UNWE.

4. Schneider F. (2017). *Implausible Large Differences of the Size of the Underground Economies in Highly Developed European Countries?* Linz: Johannes Kepler Universitet.

5. Schneider F., Buehn A., & Montenegro C. E. (07 2010 г.). *Shadow Economies All over the World.* Получено 06 10 2015 г., из worldbank.org: https://openknowledge.worldbank.org/bitstream/handle/10986/3928/WPS5356.pdf?sequence=1

6. Бирюков Е. (2010). *Альтернативные подходы к оценке теневого сектора экономики.* Челябинск: Вестник Челябинского государственного университета.

7. Красавина Л., & Валенцева Н. (2005). *аучные подходы к оценке масштабов «теневой» экономики в финансово-кредитной сферы и меры по их снижению.* Финансы и кредит.

8. Чурилова Э. (2003). *О методических подходах органов государственной статистики к оценке масштабов "теневой экономики".* Вестник Ф.А.

A Directory Service for City Video Surveillance Systems

Ajiboye Sola O., Chatwin Christopher, Birch Philip, Young Rupert

University of Sussex
Falmer-Brighton, United Kingdom
E-mail: r.c.d.young@sussex.ac.uk

ABSTRACT

A city Resource Directory (CRD) for the smart video surveillance system offers enhanced security for citizens. With a growing need for public security and safety, video enabled devices are a common sight in private and public locations around the world. They are however isolated systems, and unless owned by the government, there is no means to intelligently confirm their existence or benefit from their activities, at the public level. We propose a citywide surveillance directory system to support and facilitate the cataloguing, accessing, managing and administration of the video surveillance networks. To demonstrate the our work, we developed a simulation project in which resource directories designated for specific cities were used to administer local surveillance systems and we demonstrate how a surveillance system registers with only the appropriate CRD in its local city. We demonstrated how our solution manages failed nodes during the registration process of cameras joining the CRD.

Keywords: Video, Surveillance, Systems, Discovery, Service, Resource, Directory, Service, Self-Awareness, Lookup Protocols.

1. INTRODUCTION

By definition, a resource directory (RD) is a network service (typically, a software component) that holds information about services and resources hosted on other network objects, with a view to lookup and discovery of the resource or service in response to a network request [1] [2]. It does not contribute to the performance of the resource it describes in any way but seeks to provide location and availability information about the resource by modeling the request/response elements, using the concepts of the Internet Protocol (IP) and web properties such as the URI and Internet media type. The activities of an automated RD will normally rely on the use of a service discovery protocol, which describes the procedures that a request uses to learn the endpoints exposed by the RD. We further discuss some notable RD systems and their relevance in section 2.

Since the early days of self-aware systems (or smart systems), several terminologies have been coined to describe it including self-adaptive software, and autonomic computing and machine-to-machine platforms – they are systems comprising several interacting devices but ideally require little or no human intervention to initiate the interactions. The concept has been at the center of active research in the technology community in the last two decades [3] [4]. In an early proposition by Laddaga [5], self-adaptive software was expected to possess the following properties: it is supposed to understand 'what it does', 'how it does it', 'how to evaluate its own performance', hence 'how to respond to changing conditions'. It was conceived that the proposed properties of self-adaptive software influenced both DARPA's publication of a broad agency announcement of self-adaptive software [5] and IBM's autonomic computing [3]. IBM's vision for autonomic computing implies that a self-managing system should be self-configuring, self-healing, self-optimizing, and self-protecting and exhibits self-awareness, self-situation, self-monitoring, and self-adjustment [4].

The early propositions and the recent works on the IoT are directly influencing the perception of the systems for the near future. The ability to self-manage is opening up a new set of challenges in managing these systems. For example, automatic re-configuration (that is, with little or no human intervention) of the network following the addition of a newly deployed object with a robust and standardized approach has been noted as a major problem of the large smart network (such as the massive IoT paradigm) [1]. This was observed to directly impair the longevity and resilience of smart networks towards future changes such as availability, resource description, and mobility of the member objects. However the current practice requires an individual or an organization to install and to manually configure their own surveillance systems with an ambition to protect the system and data. As with all manual configurations, there is a likelihood of human error or deliberate setting up of the network with an incompatible system approach.

Terminologies

In this paper, we refer to a camera or a 'group of cameras', used to capture surveillance data by an individual or organization as a 'camera network' or CamNet for short. The rest of this paper will refer to both a camera and a 'camera network' as a 'CamNet' – a CamNet comprise of one or more cameras. We refer to a collection of CamNets in the same city as the City Surveillance System (CiSS), where all the CamNets in a city are registered in the City Resource Directory (CRD).

Contributions and Scope

The contributions and goals of this paper are to introduce the CRD with a view to demonstrating the feasibility of their operations. We present a demonstration of the operations of a city Resource Directory (CRD), showing its capability to administer all 'known' CamNets in a smart city, which is presented in section 3. However the detailed system architecture is presented in [6] while the experiments for generating metadata, and computing the topology-aware networks, the CamNet and City FVSN are being published elsewhere. The rest of this paper describes the features of the proposed resource directory and suggestions for future work based on our findings.

2. RELATED WORK

The importance of resource directories servers (RDS) is already established, with implementation techniques published in various notable works that included proposed standards and several experimental and pilot works [1], [2], [7], [8], [9], [10]. The works found that the anticipated interaction between smart objects in the internet-like structure (which is one of the key concepts of the IoT) could only be efficient, if the registration of new objects, discovery and resolution of the objects are automated. We predict that once each smart object acquires a unique identification on the Internet, for example using IPv6, a directory-like ideology could act as a low cost but effective system concept for initiating multidimensional unification among the heterogeneous smart objects and networks in the IoT. The existing works we found, as discussed below, have proposed self-managing systems as a solution to managing the internal configuration, administration and management of the elements and processes of local networks. This work provides a self-managing mechanism to support the government and the public safety departments in decision making, auditing and monitoring of the resources within their jurisdiction.

The early IBM vision for autonomic computing implies that a self-managing system should be self-configuring, self-healing, self-optimizing, and self-protecting and should exhibit self-aware-ness, self-situation, self-monitoring, and self-adjustment [11], [4]. The vision was birthed from the autonomic operation of the body's nervous system, which was found to oversee the operations of the heart rate and the body temperature without external intervention [11]. To achieve this biologically inspired goal, the proposed architecture configures a node as the autonomic manager, which serves as the nervous system for the other non-autonomic nodes on the network. The autonomic manager identifies the non-autonomic elements under its influence and monitors both its external environment and executes actions based on the received information. The non-autonomic elements are perceived to be any computer or resources used within the computer system. In other words, the autonomic managers are perceived to relieve the humans of some of the computer administrative tasks. The approach employed in autonomic computing, with the concept of an autonomic manager is not compliant with our approach in this work since we aim at a completely decentralized solution.

The literature suggests that IBM is introducing a research-based project into the industry, called the IBM Smart Surveillance Analytics (SSA) [12]. The overall system architecture, which was depicted in Figure 1, was described as "an open framework for event integration and correlation, highly specialized searches based on multiple object attributes, and advanced real-time alerts". It was reported that the SSA provides capability and an approach to generating metadata for achieving both real-time analytics and post-event investigation.

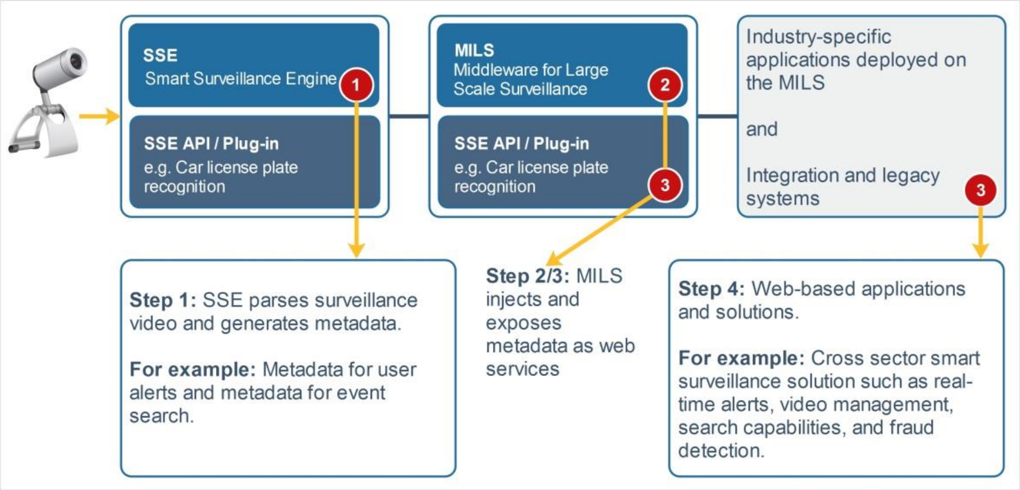

SSE
Smart Surveillance Engine
1
SSE API / Plug-in
e.g. Car license plate recognition
MILS
Middleware for Large Scale Surveillance
2
SSE API / Plug-in
e.g. Car license plate recognition
3
Industry-specific applications deployed on the MILS
and
Integration and legacy systems
3
Step 1: SSE parses surveillance video and generates metadata.
For example: Metadata for user alerts and metadata for event search.
Step 2/3: MILS injects and exposes metadata as web services
Step 4: Web-based applications and solutions.
For example: Cross sector smart surveillance solution such as real-time alerts, video management, search capabilities, and fraud detection.

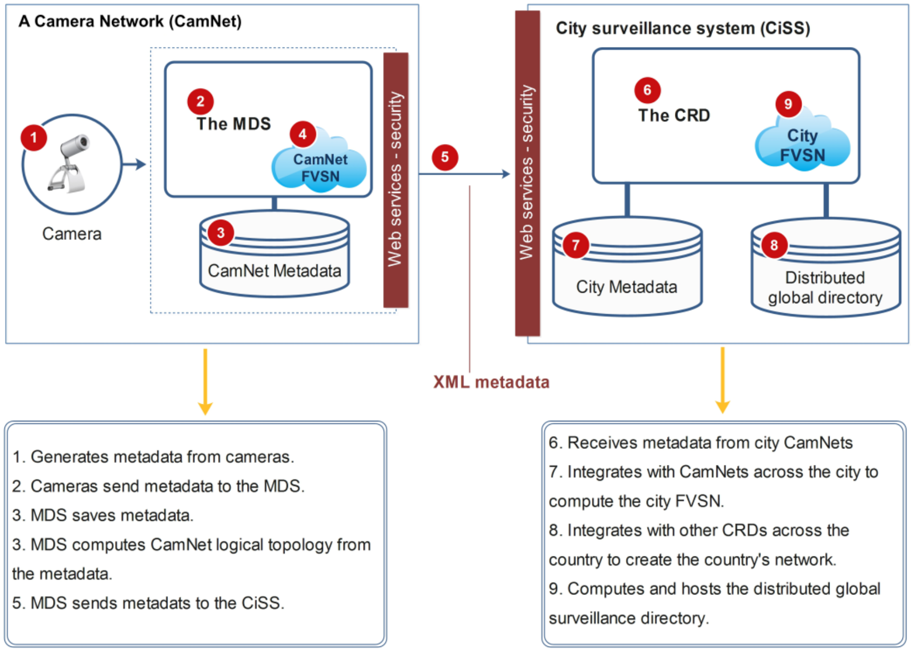
Figure 1. IBM Smart Surveillance Analytics (SSA) [12]

A real-time analytics monitors small spatial areas plus specific event detection such as identification of threat, alert generation and object tracking. While post-event investigation involves large spatial areas such as a city for the purpose of investigation and historical pattern discovery [13]. In Figure 1, the block diagram of the components in the architecture shows that the SSA employs a software stack (that is, SSE, MILS, Middleware etc.), mostly written in a C++ framework, to achieve the solutions, including event detection in metadata and real time alert generation. Publication suggested that this solution has been deployed in the retail environments for achieving business intelligence and intrusion alert [14].

It was noted above that the IBM SSA was designed to facilitate analytics of both real-time and post event analytics - it is however presented as a standalone system for a specific business environment. Based on our knowledge from the evidence in the literature (which includes the academic and commercial community), we found that all the existing research and literature has considered video surveillance systems as isolated systems, based on the system boundaries of the independent owner. However, we provide a unique and novel perspective into solving these problems. We identified the opportunities of unifying and integrating the independent systems and explored the feasibility of public-level exploration of the unified video surveillance systems.

3. DESIGN APPROACH AND ARCHITECTURE

Figure 2 depicts the high-level conceptual overview of the global surveillance system suggested in this research (showing a CamNet and a CRD). It shows the flow of metadata from the CamNet to the city’s CRD. The components presented in the CamNet shows the high-level process/information flow within the CamNet. The camera captures data and sends it to the metadata server (MDS). The MDS generates metadata from the video captured by the cameras, persists the metadata locally but also sends a copy to the CRD, where the unified metadata is used for city-level analytics. The design of the CRD is the focus of this paper.



1. Generates metadata from cameras.
2. Cameras send metadata to the MDS.
3. MDS saves metadata.
3. MDS computes CamNet logical topology from the metadata.
5. MDS sends metadats to the CiSS.

6. Receives metadata from city CamNets
7. Integrates with CamNets across the city to compute the city FVSN.
8. Integrates with other CRDs across the country to create the country's network.
9. Computes and hosts the distributed global surveillance directory.

Figure 2. The high level conceptual view of the city surveillance system showing process flow

The System Overview of a City

The CiSS system overview, which is depicted in Figure3, is the client-server network of the CamNets in a city. Each CamNet joins the city's CiSS upon successful registration and sends metadata to the CRD, based on its configuration. A CamNet only has knowledge of its own existence and the CRD - and does not have the knowledge of any other CamNet or a camera outside its own network. The only connectivity information a CamNet has about the CiSS is the URI for making web method calls to the CRD.

The City Resource Directory Server (CRD)

The city resource directory server is a self-managing discoverable service, which is depicted in Figure 4. It shows 2 subdirectories – the first is the directory of CamNets, which is used to administer the entire CamNets in the city – that is, the CiSS. It uses the database to save the configuration, contact, and ownership information about each CamNet in the city. And depending on the level of access granted by the CamNet administrator, the CRD holds detailed information about each camera in the CamNet, this information is obtained when the CamNet registers with the CRD. The registration process is described in section 4. The second (G-DHT) is the directory of the other CRDs - it is used to acquire knowledge about other CRDs around with the aim of knowing which CRD is more appropriate to administer a CamNet, this is further discussed in section 3.4, the G-DHT.

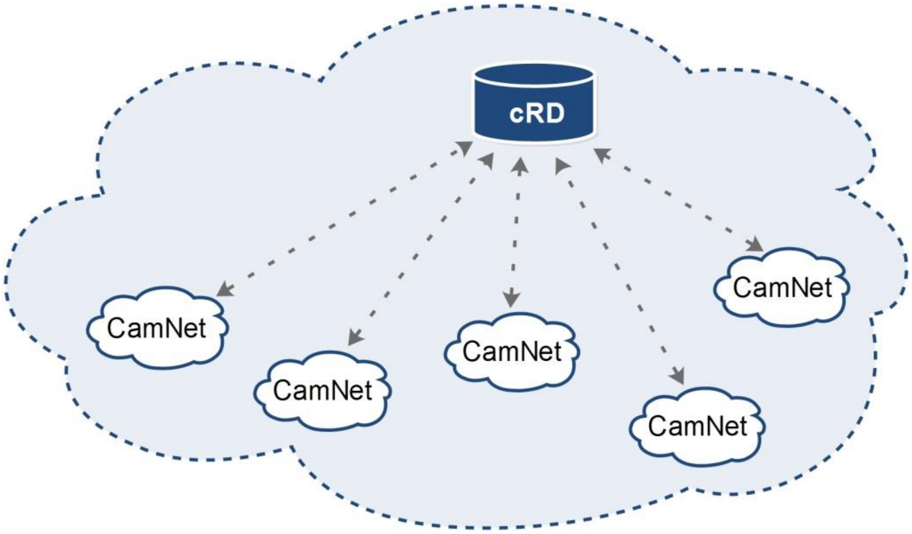


Figure 3. The system overview of the CiSS

The Directory of CamNets (CamNets)
This serves as the application support to all the CamNets in the city. The CRD observes whether each member CamNet has sent data in a configurable timeframe. If data has not been received from a CamNet within the set period, the CRD will assume a failed node and mark the CamNet inactive. However if the CamNet transmits data again, the registration process is reactivated to validate it and confirm its suitability as a local CamNet. The CRD comprise of components and processes, that includes:

Open directory service - The directory service is 'open' to any CamNet that has the URI information of the CRD. A CamNet may call the services of the CRD to register, send metadata, or update its own identity information, which the CRD holds. The CRD is equipped with a layer of web methods, which it uses to access underlying database functions for creating, reading, updating and deleting records. When a CamNet sends a request, it sends along authentication credentials, which the CRD uses to verify and either accept or reject the request. If the sending CamNet is valid, the request is accepted and processed accordingly. If the sending CamNet is unknown, the CRD will first attempt to register it as described in section 3.5. However if the registration is unsuccessful, the request will not be processed. The fundamental purpose of the CRD is the cataloguing of the cameras in the city and also to store and administer metadata it receives from CamNets within the city.

The Query engine - The metadata repository is only accessible to authorized officers in the city, who can run queries to obtain information on the metadata repository and CamNet directory. For example, a police office that is interested in the location of the cameras within an area may run a query to retrieve the location information and contact information for the CamNets in the area. The query engine is also responsible for generating alerts and can be used to query the metadata database to establish trends and patterns with a view to predicting future events.

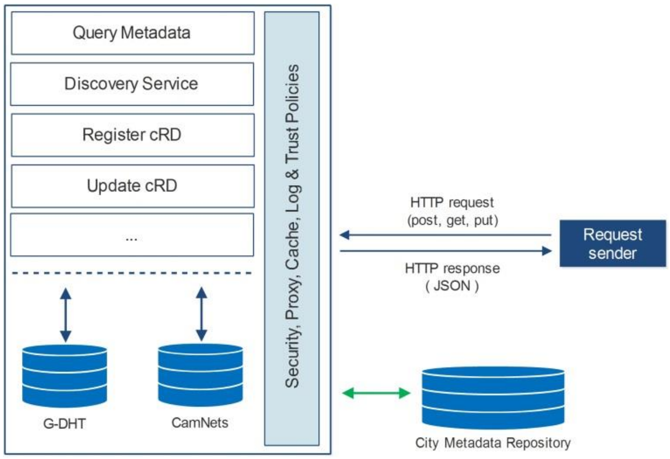


Figure 4. Internal architecture of the CRD.

Security - The security and privacy of surveillance data is vital to the credibility and reliability of the system and the data it produces. This is especially important for an IoT enabled service, which is open to requests/response from anywhere. Each sending device sends authentication credentials with each request for verification and validation - it does not process a message that is missing the security credentials. The CRD is equipped with a role-based access routine, which it uses to decide the level of access available to a logged in user. For example, a police office in the city may have access to query the location of cameras while a more senior officer may have access to achieve more sensitive tasks such as retrieval of metadata from the CamNets.

In addition, although Denial of Service attacks requires specialist firewall implementation, which sits as a layer between the requests and the object being protected, the CRD is equipped with a local version of a firewall in that it blocks any device that sends multiple requests in a configurable period of time. It adds the device's IP address to its 'blocked' list so that any message originating from the device will be dropped.

The Directory of CRDs (G-DHT)

The G-DHT is distributed dynamic hash table (DHT) that keeps information for looking up and discovering other CRDs. The table is used to forward a registration request to other CRDs, if the original CRD is not the correct CRD for the city of the CamNet. Table 1 is a cut-down version of the simple DHT-like implementation in the experiments. The Globally Unique Identity Number (GUIDN) field is unique – it is used to identify each CRD.

The GUIDN field represents the unique DHT's hash for CRD. The field is used to uniquely identify each known CRD – it is also used to index the database table. The naming convention of the GUIDN allows for human readability. For example, the GUID for the Brighton city in the UK could be 'gb.east-sussex.brighton' – as seen in Table 1. The first part, 'gb' represents the name of the country's locale, the second part, and 'east-sussex' represents the county, the third part, and 'brighton1' represents the first CRD configured for the city of Brighton. Incidentally, if a CRD receives a registration request originating from a different city, it uses the GUIDN to locate the appropriate CRD and forwards the registration request.

Table 3. An example DHT table on a CRD.

ID	GUIDN	URL
1	gb-east-sussex-london	https://rd.brighton.co.uk/london
2	gb-east-sussex-brighton	https://rd.london.co.uk/brighton
3	gb-east-sussex-worthing	https://rd.crawley.co.uk/worthing
4	gb-east-sussex-crawley	https://rd.washington.com/crawley
5	gb-east-sussex-hasting	https://rd.boston.com/hasting
6	gb-east-sussex-bristol	https://rd.brisbane.com.auk/bristol
7	gb-east-sussex-leeds	https://rd.melbourne.com.au/leeds
8	gb-east-sussex-reading	https://rd.beijing.cn/reading

CamNet Registration

With regards to the algorithms that operate these experiments, we evaluate a use case to demonstrate and validate our approach - the registration of a new CamNet. That is, the addition of a new CamNet, which aims to join the relevant CRD in the city of its location. The experiment aims to ascertain how the availability of the CRDs affects the registration algorithm, which is presented in ALGORITHM 1. The registration process ensures that the appropriate CRD is located and accepts the CamNet, if it meets the registration requirements. The success of the algorithm to locate the appropriate CRD is aided by the GUIDN naming convention discussed in section 3.4 above. Based on the operation of the algorithm, if a CRD receives a request destined for a different CRD, it simply forwards the request to the appropriate CRD, using the G-DHT to lookup the forwarding URI of the recipient CRD.

ALGORITHM 1: CamNet to CRD Registration

Input: A request sent by CamNet d, CamNet's identity e.

Process: Lookup suitable CRD for request f, add CamNet to own directory g, send response to CamNet h,

Condition: CamNet is located in own city i, CamNet in the same country as self j, CRD is found for address k.

Response: SUCCESS, FAIL, NO_RESPONSE

```
Begin
        Begin
        init count_HOP = 0;
        if get d == TRUE AND get e == TRUE then
              do f
        if i == TRUE AND j == TRUE
          do g
          do h = SUCCESS
        else
          do count_HOP++
        if j == FALSE then
          do tag d = SEND FAILED_INTERNATIONAL
          else if i == FALSE AND j == TRUE then
            do forward d to k
            else if i == TRUE AND k == FALSE then
              do h == FAIL
            endif
          endif
        endif
        END
End
```

4. EXPERIMENTATION AND EVALUATION

Experiment Setup

To demonstrate the registration process, we develop an experimental project to evaluate and assess the feasibility of the approach in relation to the success rate of CamNets registering with their own local CRD. We further investigate how the end of life of a CRD could affect the reliability of the system with a view to providing answers to the following research question: “To what degree of accuracy is the registration process for a new CamNet in respect to locating its own CRD achieved?”. In particular, we investigate these parameters under the condition that the city CRD used the G-DHT to acquire knowledge about other CRDs.

Note that our evaluation did not have to account for the underlying performance issues based on the end-to-end attributes of network conditions. This is because our interest in the research is in the outcome at the application level and our setup does not include the network load variables in typical network-oriented experiments since all our CRDs are located on the same machine as database objects.

Using the Rapid Application Software development methodology, we completed a prototype, based on the client-server architecture presented in section 3.1. The programming aspects of the experiment were achieved using the ‘Hypertext Pre-processor, PHP’ (version 5.6.10), supported by the ‘MySql database community server’ (version 5.5.47). The project was built using the community version of the Zend framework version 2. Although the project could be implemented in other programming environments such as Java/Oracle, or .NET/MSSQL, the PHP/MySQL combination was chosen for the experiment for the following reasons:

1. Ability to build a web-based user interface for setting up and configuring the components in the experiments.
2. They are open-source and community driven software, ease of modification and adaptability to the research implementation.
3. Ability to complete the setup with the tools and resources mentioned above.

Simulation

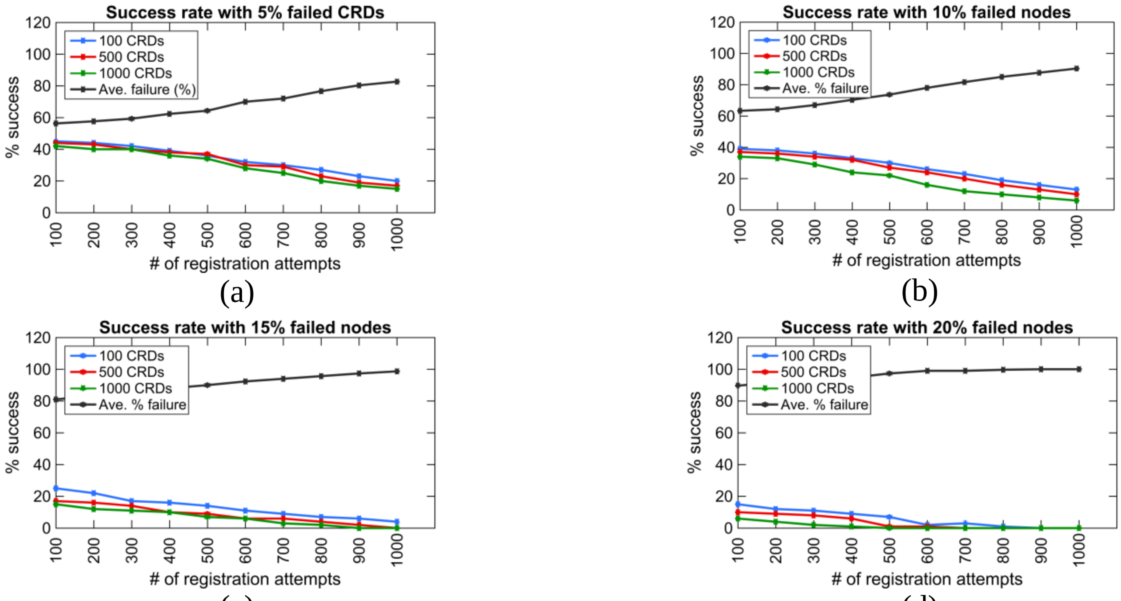
The CamNet chooses a CRD at random from the total n CRDs (where n can be any positive integer – we experiment with n = 100, 500, and 1000), and submit each registration request to the randomly chosen CRD. To ensure that the CamNet registration is valid for one of the n CRDs, we provide a list of n IP addresses where an IP address is valid for a CRD. When submitting the registration, the CamNet assigns itself one of the n IP addresses, which the receiving CRD uses to check whether the request is valid for itself.

5. RESULTS

The simulation implements a flat network – that is, a server does not control the registration process. In the first set of experiments, all the nodes were active and accessible. Once this is achieved, we carry out more experiments with a view to investigating the ability of our solution to register CamNets in their local CRD when a known CRD failed. We introduce a level of uncertainty to the network by making some nodes unreachable. To make a CRD unreachable, we set its status 'disabled' in the experimental database, while the disabled node still remains in the G-DHT of the active CamNets.

We initially introduced 5% failed CRDs, then we increased the failure in increments of 5% up to 20% - the results are presented in Figures 5 (a) to (d). For each set of experiment, we carry out 10 simulations – in the first simulation, we sent 100 requests then, we increased the number of requests in increments of 100 until we reached 1000 requests in the last simulation. Figure 5 (a) shows the result of 5% failed nodes – it can be observed that the failure rate rises with the increase in the number of registration attempts, for any number of all the simulations. It is also observed that reliability (that is, registration success rate) decreases as the number of request grows tending towards 0 reliability but it did not reach 0 with 1000 requests. The trend of the results for 10%, 15%, and 20% failed CRDs are similar to those observed with the 5% failed CRDs, except that the success rate reached 0% for the 20% failed CRDs simulation when registration reached about 600 attempts.

Based on our observation of 0% reliability, we decided to add a routine to the registration process so that the CRDs first check the availability of a known CRD before it forwards a message to it. If the recipient CRD acknowledges the request, then the message forwarding proceeds. However if the CRD is not found, a failed registration message is sent back to the CamNet and the CRD is removed from the G-DHT. The results are presented in Figures 6 (a) and (b).



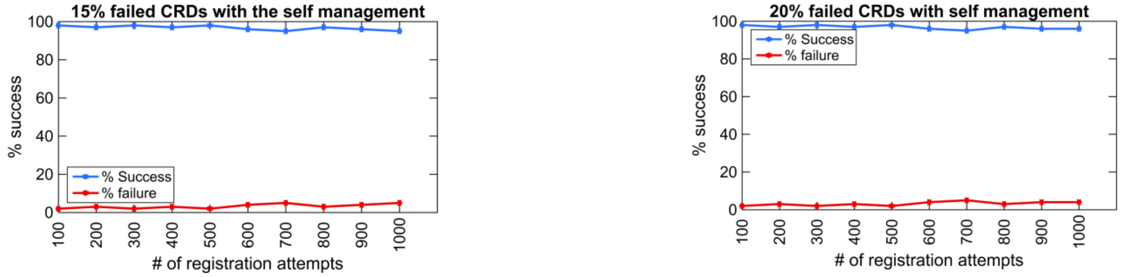
(a) (b)

(c) (d)

Figure 5. Success rate of the system when varying the percentage of unavailable CRDs.

Improved Reliability with Self-Management

To resolve the problem of the network crashing due to the failed CRDs, as observed above, we apply a level of self-management to the registration algorithm (see algorithm 1 above), such that the requesting CRD first checks the reachability of the destination CRD before sending a request. If a CRD is not reachable, then CRD sends the failure notice to the requesting CamNet instead. With this solution in place, we are able to prevent a network crash where the worst-case reliability achieved was at 96% with 20% failed nodes. Figures 6 (a) and (b) both showed a similar level of success varying between 96% and 99% for both 15% and 20% failed CRDs.



(a) (b)

Figure 6: Success rate of the system under when varying percentage of the CRDs are not available.

It is observed that the achieved reliability is higher than the probability score of the system. For example, in the 20% failed node, the maximum success rate will be 80%, based on probability score. However, the achieved success rate is an average of 97%. This is because failed CRDs are removed and the CamNet does not make further attempts to register disabled CRDs.

6.CONCLUSION

A city CRD is capable of providing information about any surveillance network in the city, through the local membership of the city's CamNets. In practice this schema can support the public safety departments in identifying and locating surveillance networks across the city without the need for physical street inspection – this could potentially improve the efficiency and success of police investigations. In practice, we envisage that the size and number of cameras in the city will change erratically over time as CamNets are added, transferred and migrated from place to place. The directory server must provide a means for self-update and management for each CamNet. Providing a historic record for each CamNet and how to access it, should the need arise.

The experiment equally demonstrated that an unreachable cRD could result in inconsistent behavior and outcome so it is imperative to provide a solution to the change in device status. For example, when 90% of the total numbers of CRDs are accessible as in our experiment, the accuracy of registration is low (64% in our experiment). However with the introduction of the self-management solution, we recorded significant improvement of about 97%. We will further explore the possibility of perpetual 100% success rate in our future work by improving our self-management procedure.

The results from this research indicate that this schema has great potential in solving security and surveillance problems. Although there is still a great deal of work needed to develop and test the different components and how they inter-relate, this is work in progress and we will present further findings in subsequent publications.

REFERENCES

1. Cirani S., Davoli L., Ferrari G. at all. "A Scalable and Self-Configuring Architecture for Service Discovery in the Internet of Things," *IEEE Internet Things J.*, vol. 1, no. 5, pp. 508–521, Oct. 2014.

2. Shelby Z., Hartke K., Bormann C. "The Constrained Application Protocol (CoAP)," *RFC 7252 (Proposed Standard), Internet Engineering Task Force*, 2014. [Online]. Available: http://tools.ietf.org/html/rfc7252. [Accessed: 29-Jan-2016].

3. Dutt N., Jantsch A., Sarma S. "Self-aware Cyber-Physical Systems-on-Chip," in *2015 IEEE/ACM International Conference on Computer-Aided Design (ICCAD)*, 2015, pp. 46–50.

4. Dobson S., Sterritt R., Nixon P., and Hinchey M. "Fulfilling the Vision of Autonomic Computing," *Computer (Long. Beach. Calif).*, vol. 43, no. 1, pp. 35–41, Jan. 2010.

5. Laddaga R., "Active Software," P. Robertson, H. Shrobe, and R. Laddaga, Eds. Berlin, Heidelberg: Springer Berlin Heidelberg, 2000, pp. 11–26.

6. Ajiboye S.O., Birch P., Chatwin C., and Young R. “Hierarchical Video Surveillance Architecture - A Chassis for Video Big Data Analytics and Exploration,” in *Proc. SPIE 9407*, 2015, vol. 9407, pp. 1–10.

7. Yachir A., Amirat Y., Chibani A., Badache N. “Event-Aware Framework for Dynamic Services Discovery and Selection in the Context of Ambient Intelligence and Internet of Things,” *IEEE Trans. Autom. Sci. Eng.*, vol. 13, no. 1, pp. 85–102, Jan. 2016.

8. Carballido Villaverde B., Alberola R.D.P., Jara A.J., Fedor S., Das S.K., and Pesch D. “Service discovery protocols for constrained machine-to-machine communications,” *IEEE Commun. Surv. Tutorials*, vol. 16, no. 1, pp. 41–60, 2014.

9. Zisman A., Spanoudakis G., Dooley J., and Siveroni I. “Proactive and Reactive Runtime Service Discovery: A Framework and Its Evaluation,” *IEEE Trans. Softw. Eng.*, vol. 39, no. 7, pp. 954–974, Jul. 2013.

10. Demers S., Fecko M.A., Lin Y.J., Shur D., Samtani S., Sinkar K., and Chapin J. “Scalable Registration and Discovery of Devices in Low-Bandwidth Tactical Networks,” in *MILCOM 2013 - 2013 IEEE Military Communications Conference*, 2013, pp. 550–555.

11. Kephart J.O. and Chess D.M. “The vision of autonomic computing,” *Computer (Long. Beach. Calif).*, vol. 36, no. 1, pp. 41–50, Jan. 2003.

12. IBM, “IBM Smart Surveillance Research - Publications,” 2013. [Online]. Available: http://researcher.watson.ibm.com/researcher/view_grouppubs.php?grp=1394.

13. Feris R.S., Siddiquie B., Petterson J., Zhai Y., Datta A., Brown L.M., and Pankanti S. “Large-Scale Vehicle Detection, Indexing, and Search in Urban Surveillance Videos,” *IEEE Trans. Multimed.*, vol. 14, no. 1, pp. 28–42, Feb. 2012.

14. Connell J., Fan Q., Gabbur P., Haas N., Pankanti S., and Trinh H. “Retail video analytics: an overview and survey,” *Proc. SPIE - Int. Soc. Opt. Eng.*, vol. 8663, no. March, p. 86630X, 2013.

High Speed Targets Recognition Systems Design Based on Optimal Combination of the Optical and Electronic Processors

[1]Perju Veacheslav, [2]Sofronescu Igor

[1]Institute of Advanced Information Technologies, FIUM
52, Vlaicu Pircalab Str., Chisinau, MD-2012, Republic of Moldova
Tel: (373)79431225, e-mail: vlperju@yahoo.com

[2]Armed Forces Military Academy
23, Haltei Str., Chisinau, Republic of Moldova
E-mail: igor.sofronescu@academy.army.md

ABSTRACT

The theory of the high speed targets recognition systems design based on the optimal combination of the optical and electronic processors has been presented. Is described the general task of targets recognition, is presented the classification of the targets recognition systems and main requirements to them. A model of parallel image processing have been considered and the generalized structure of parallel target recognition system is presented. There are described the factors which define the utilization of optical or electronic processing devices during different steps of the conveyor system. It is mentioned that optical processors are characterized by higher processing speed and have good perspectives. It is analyzed the possibility to realize different image processing operations by the optical and electronic processors. There are described the features of the target' image forming units and of the buffer units necessary to connect processors between them. There have been made time expenditures determination in the target recognition systems and their through-put at the processing of one and series of images, in the dependence on the system conveyor length, relation between optical and electronic processors and the relation of the data processing time in electronic processors to the processing time in the optical processors. There have been presented the method of targets recognition systems design, based on optimal combination of the optical and electronic processors and which permit to obtain maximum through-put of the systems. An example of targets recognition system design is presented.

Keywords: target, recognition, system, design, optical, electronic, processor, image, processing

1. INTRODUCTION

In many civil and military applications are required high speed systems for targets recognition, image processing in real time.

Over the last years a significant progress was achieved in the development of special and general - purpose electronic multiprocessor systems for targets recognition[1-5]. Such systems are characterized by a high productivity (up to hundreds billions operations per second), but are very complex, consume a significant power.

The significant results have been obtained in the construction of the optical and optical-electronic processors with acceptable weight - size characteristics and high through - put [6-9]. High productive processors, which realize operations of Fourier transform, correlation etc. have been developed.

However, the analysis shows that not all of the image processing operations used in target recognition and other applications can be realized at present by the optical processors. Besides, optical processors are characterized by a limited flexibility.

Therefore, the construction of high speed efficient systems for targets recognition, image processing in real time is connected with the development of multiprocessor systems, which are based on the combination of optical and electronic units, optimal distribution of the solving tasks among the processing devices of different type.

In this article is presented a method for design of the high speed optical-electronic target recognition systems. In section 2 is described the general task of targets recognition, is presented the classification of the targets recognition systems and main requirements to them. In section 3 a model of parallel image processing have been considered and the generalized structure of parallel target recognition system is presented. In section 4 are described the factors which define the utilization of optical or electronic processing devices during different steps of the conveyor system. It is mentioned that optical processors are characterized by higher processing speed and have good perspectives. It is analyzed the possibility to realize different image processing operations by the optical and electronic processors. There are described the features of the target' image forming units and of the buffer units necessary to connect processors between them. In section 5 there have been made time expenditures determination in the target recognition systems and their through-put at the processing of one and series of images, in the dependence on the system conveyor length, relation between optical and electronic processors and the relation of the data processing time in electronic processors to the processing time in the optical processors. In section 6 there have been presented the method of targets recognition systems design, based on optimal combination of the optical and electronic processors and which permit to obtain maximum through-put of the systems. An example of targets recognition system design is presented in section 7.

2. GENERAL TASKS OF TARGETS RECOGNITION

In many civil and military applications are required high productive systems for targets recognition, image analysis in real time (Figure 1).

General task of target recognition (TR) can be formulated in the next mode. Let T(x,y) - the target's image which can be arbitrary rotated, scaled, displaced etc. Task of TR consists in the following: to classify the target, to determine the location etc.

Targets recognition systems (TRS) can be of different kind: air-air, air-ground, ground-air and ground-ground; on-board and stationary; electronic, optical etc.

The main requirements to TRS are: real time recognition; high reliability of targets recognition; restrictions to TRS' consuming power, dimensions etc.

Figure 1. Examples of targets

Analysis of existing TRS shows that they have different disadvantages such as: insufficient productivity of data processing, low reliability of TR and flexibility, high consuming power, high weight and dimensions which don't permit effectively to realize the tasks of TR [1-5].

In these conditions appear the necessity to elaborate new approaches to TRS construction and design, which will include electronic and optical processing units in optimal way and will permit to obtain maximal possible throughput of the systems.

3. MODEL AND GENERAL STRUCTUTE OF A SYSTEM FOR PARALLEL TARGETS RECOGNITION

Let the targets recognition task is determined in the following way: W{T(x,y)}→RO, where W - is the function of target recognition; T(x,y) – target's image; RO - the processing result, which can be an image or numerical data.

In this case the most of the targets recognition, image processing problems can be represented in the form of a linear sequence of separate sub problems. The decomposition principle utilization allows to organize parallel processing of two types: in time and in space. Parallel processing in time consists in organization of the sub problems conveyor, which are implemented consecutively.

The spatial concurrency means that on each step of the conveyor processing, the parallel processing of the whole image or its separate fragments is organized. The last type of concurrency is defined by the fact that we can point out some classes of operations while proceeding the image processing. They are executing at each of the image pixels, over separate regions of the image or over the whole image. In other words, to obtain the result we need local (as in the first two cases) or global (as in the last case) initial information. At the working with the local information, the image can be represented as a set of sub images, which are processed by the corresponding set of processor units. The spatial concurrency can be implemented by the help of processor units set of electronic or optical type.

Corresponding with the above-mentioned, the model of the parallel processing of the images can be represented in the following way:

$$RO = C_h\{\underset{i}{U}[\underset{j}{W}{}^{j}_{i}(T_{ij})]\},$$

where C_h - the superposition operation, i - the step number of the conveyor; U - the processing results union operation during one of the conveyor steps; j - the image fragment number; W^j_i- the operation of the processing of the j-th image fragment on i-th step; T_{ij}- the j-th image fragment on i-th step.

This model can be also represented in the form of the operator:

$$T(x,y) \Rightarrow \{W1\}_{M1} \rightarrow \{W2\}_{M2} \rightarrow ... \rightarrow \{Wk\}_{Mk} \Rightarrow RO.$$

The peculiarity of the presented model consists in the maximum level of parallelism of image processing operations that ensure the high productivity of the target recognition system.

According to the proposed model, the generalized structure of parallel target recognition system can be represented as shown in Fig.1, where Y_i - is a device that implements the operation W_i; B_i - buffer device. The device Y_i may be optical or electronic. In the last case it can contain one or a group of processor elements that function in parallel way.

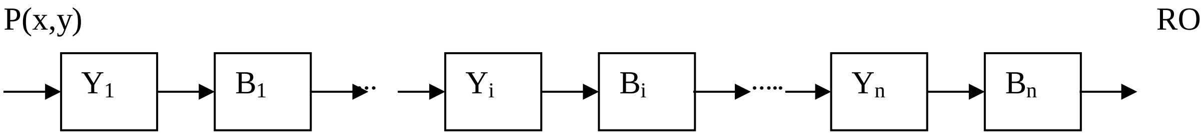


Figure 1. The structure of the target recognition system

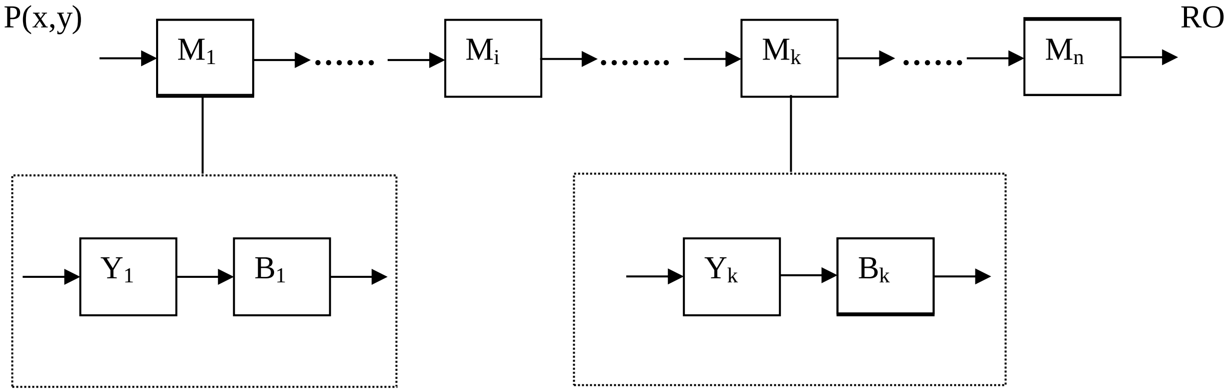


Figure 2. The modular structure of the target recognition system

4. THE POSSIBILITIES TO REALIZE IMAGE PROCESSING OPERATIONS BY OPTICAL AND ELECTRONIC PROCESSORS

In the system described in Section 3, the utilization of optical or electronic processing devices during different steps of the conveyor will be defined by some factors.

For the first, optical processors are characterized by higher processing speed and have good perspectives (Fig.3).

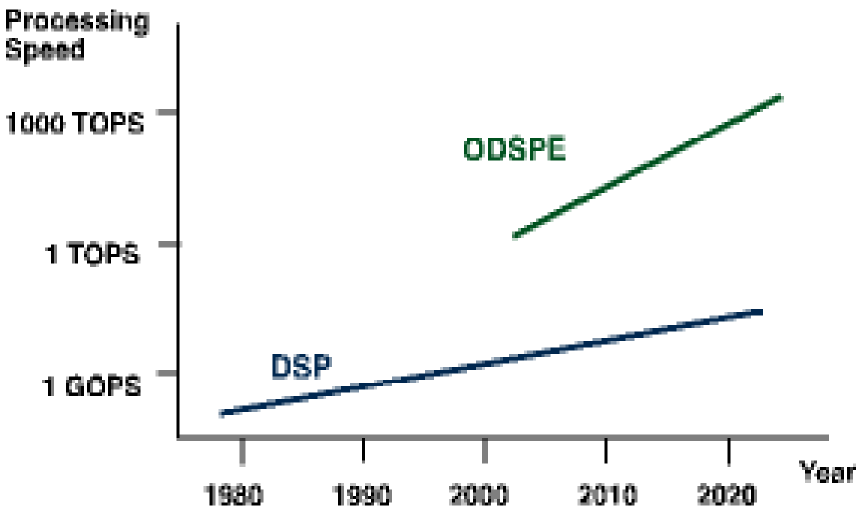


Figure 3. Trends in the development of the electronic (DSP) and optical (ODSPE) signal processors.

At present exist different architectures of the high speed optical processors. For example, optical vector matrix processor (Fig. 4) function at a rate of 125 MHz for a multiplication of a 256 element vector by a 256x256 matrix, or 8000 Giga operations per second.

Some optical processors there were realized as one board plate (Fig. 5), and are characterized by very good parameters (Fig. 6, Table 1).

The next factor is the possibility to realize different image processing operations by the optical processors. In the Table 2 there are presented the respective data. The analysis shows that the significant part of the wide used operations in target recognition, image processing can be implemented optically in 2-10 times faster than by electronic processors. Unfortunately, at present exists some operations, which can't be implemented optically.

Another factor is the way of target' image forming. The image can be formed by an electronic or optical device. The analysis of image forming units (IFU) characteristics showed that electronic and optical IFU provide the identical resolution ability. The difference between them consists in the image forming speed. Optical IFU allow to form images 2-8 times faster.

In the system which consists of the optical and electronic processors, realizing different operations, appear necessity of the processors buffering to convert the signals from one form to other (Figure 6). Let us denote the buffer unit as $B_{m,n}$, where m,n are taking the values 1 or 2. Let us consider that number 1 corresponds to an electronic device, and number 2 - to an optical one. For example, the device $B_{1,2}$ is a buffer storage for connection of electronic and optical processors. The time outlay during the signal buffering of different types is represented in Table 3.

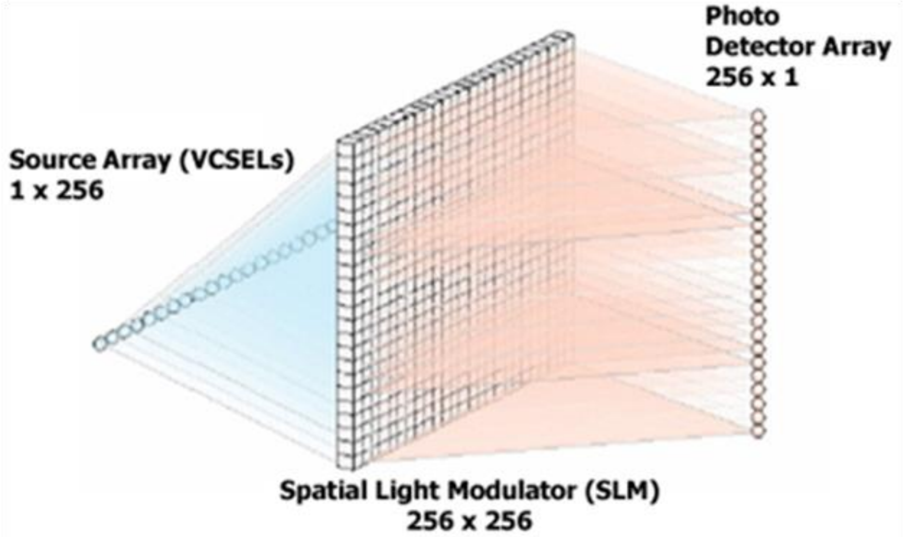


Figure 4. The optical vector matrix multiplier

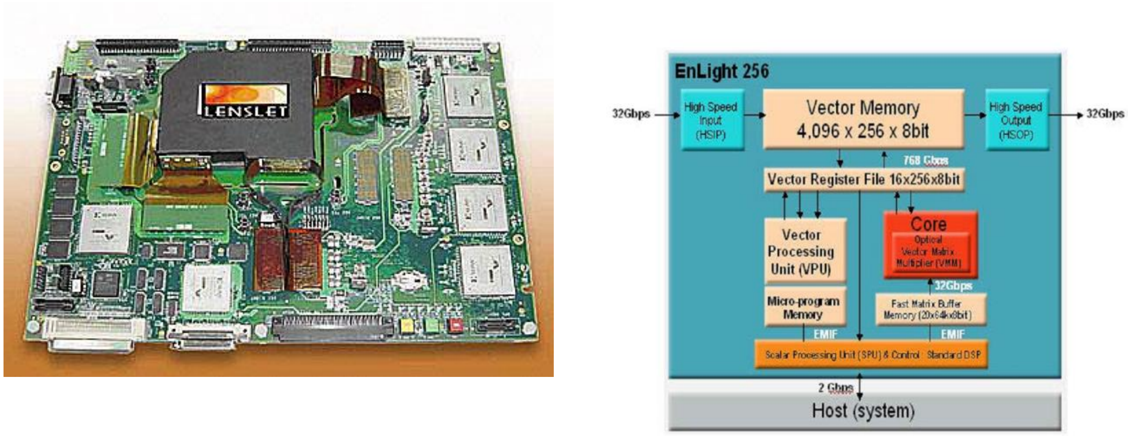
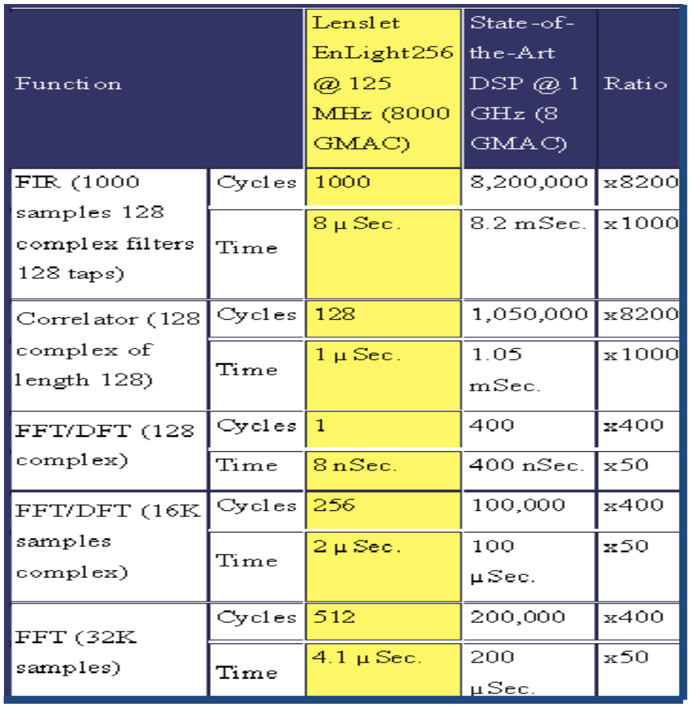

LENSLET
EnLight 256
32Gbps
High Speed Input (HSIP)
Vector Memory 4,096 x 256 x 8bit
High Speed Output (HSOP)
32Gbps
768 Gbps
Vector Register File 16x256x8bit
Vector Processing Unit (VPU)
Core
Optical Vector Matrix Multiplier (VMM)
32Gbps
Micro-program Memory
Fast Matrix Buffer Memory (20x64kx8bit)
EMIF
EMIF
Scalar Processing Unit (SPU) & Control Standard DSP
2 Gbps
Host (system)

Figure 5. Optical processor EnLight 256

Table 1. Comparative data of the optical processor EnLight256 and electronic DSP



Function		Lenslet EnLight256 @ 125 MHz (8000 GMAC)	State-of-the-Art DSP @ 1 GHz (8 GMAC)	Ratio
FIR (1000 samples 128 complex filters 128 taps)	Cycles	1000	8,200,000	x8200
	Time	8 μ Sec.	8.2 mSec.	x1000
Correlator (128 complex of length 128)	Cycles	128	1,050,000	x8200
	Time	1 μ Sec.	1.05 mSec.	x1000
FFT/DFT (128 complex)	Cycles	1	400	x400
	Time	8 nSec.	400 nSec.	x50
FFT/DFT (16K samples complex)	Cycles	256	100,000	x400
	Time	2 μ Sec.	100 μ Sec.	x50
FFT (32K samples)	Cycles	512	200,000	x400
	Time	4.1 μ Sec.	200 μ Sec.	x50

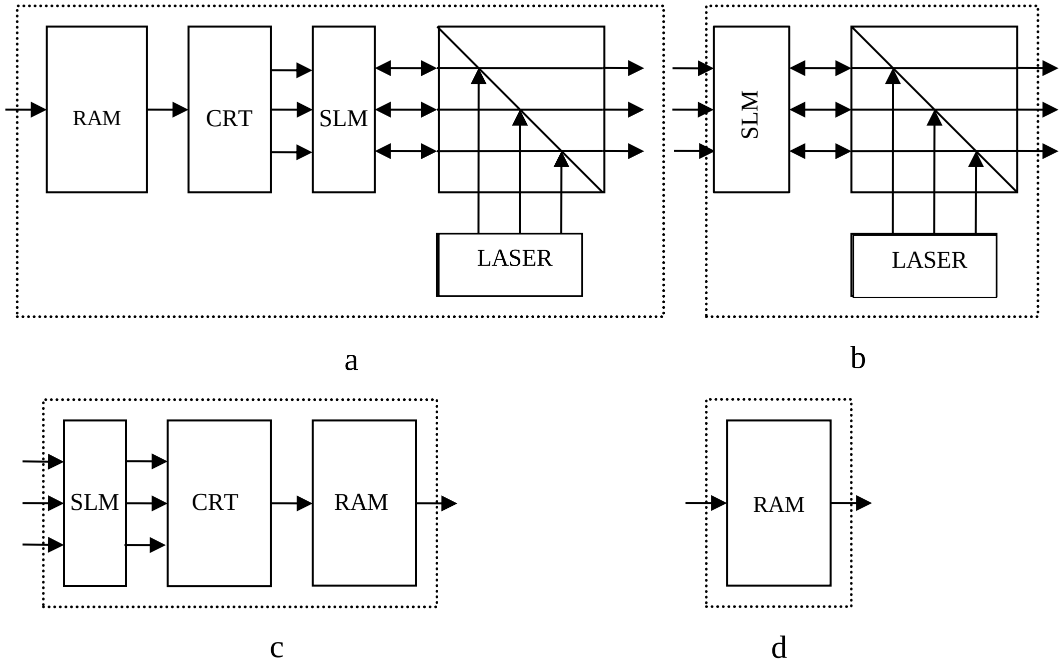


Figure 6. The buffer units: a – electro-optical; b – optical; c – optical-electronic; d – electronic; SLM – spacial light modulator; OC – optical cube; ADC – analog to digital convertor

5. THE THROUGH-PUT OF THE TARGET RECOGNITION SYSTEM

Let us evaluate the time outlay in the system while processing one and series of images. In the structure presented in Fig.1 we can join the consecutively situated optical devices into optical processing modules and electronic devices - into electronic processing modules (Fig.2). Let the system consists of n_o optical and n_e electronic modules ($n_o+n_e=m$), and each module contains accordingly l^o_j optical and l^e_q electronic processing devices. The whole number of optical l^o, electronic l^e devices and the conveyor length l_k will be:

$$l^o=\sum_{J=1}^{n_o} l^o_J, \quad l^e=\sum_{q=1}^{n_e} l^e_q\,, \quad l_k=l^o+l^e.$$

Table 2. The possibilities and the time of the implementation of the image processing operations

Image processing operations	1. Computing means	
	Optical	Electronic
. Image forming	10ms	20(40)ms
2. Noises removal	10ms	172ms
3. Edge detection	10ms	172ms
4. Object extraction	10ms	172ms
5. Image transformation from Cartesian system of coordinates into polar or logarithmic - polar one	10ms	20(40)ms
6. Image rotation and scaling with arbitrary parameters	-	12sec
7. Calculation of two-dimensional Fourier transformation(256x256)	8ms	204.8ms
8. Calculation of two-dimensional correlation and convolution functions	0.512ms	537ms
9. Calculation of geometrical moment features	10ms	0.18sec
10.Calculation of central moment features	-	0.2sec
11.Calculation of invariant moment features	-	0.25sec
12. Chords transformation of the image	10ms	+
13. Image features processing and comparing with a standards	-	50ms
14.Correlation fields analysis, calculation of coordinates maxima	-	20(40)ms
15.Computing process control	-	+

In Table 2: "+" and "-" are a possible and not possible to be realized operations

Table 3. Time outlay during the signal buffering of different types, ms

Kind of the buffer	Image resolution, pixels	
	512x512	256x256
$B_{1,1}$ (electr.-electr.)	40	20
$B_{1,2}$ (electr.-optic.)	50	20
$B_{2,1}$ (optic.-electr.)	40	20
$B_{2,2}$ (optic.-optic.)	10	10

Let us consider the following time characteristics: t^o_{pj} - processing time in j-th optical module; t^e_{pq} - processing time in q-th electronic module; t^o_{kj} - switching time between devices in optical module; t^b_{oo} - buffering time of two neighbor optical processing devices; t^e_{kq}- switching time between devices in electronic module; t^b_{ee}- buffering time of two neighbor electronic processing devices; t^n_{kq}- switching time between the processors in electronic module devices; t^k_{oe} - time of buffering of optical modules with electronic ones; t^k_{eo} - time of buffering of electronic modules with optical ones. These parameters are estimated in the following way:

$$t^o_{pj}=\sum_{z=1}^{l^o_j} t^o_{pjz}, \quad t^e_{pq}=\sum_{f=1}^{l^e_q} t^e_{pqf}, \quad t^o_{kj}=(l^o_j-1)t^b_{oo}, \; t^e_{kq}=(l^e_q-1)t^b_{ee}$$

$$t^n_{kq}=\sum_{f=1}^{l^e_q} t^n_{kqf},$$

$$t^k_{oe}=\sum_{i=1}^{n} t^b_{oei}, \tag{1}$$

$$t^k_{oe}=\sum_{i=1}^{n-1} t^b_{eoi}. \tag{2}$$

The value of n in expressions (1), (2) is defined in the following way:

$$n=\begin{cases} m/2 & \text{if } n_o = n_e \\ n_e & \text{if } n_o > n_e \\ n_o & \text{if } n_o < n_e. \end{cases}$$

The time outlay in optical and electronic modules can be described as following:

$$t^o_j = t^o_{pj} + t^o_{kj} = \sum_{z=1}^{l^o_j} t^o_{pjz} + (l^o_j-1)t^b_{oo},$$

$$t^e_q = t^e_{pq} + t^e_{kq} + t^n_{kq} - \sum_{f=1}^{l^e_q} t^e_{pqf} + (l^e_q-1)t^b_{ee} + \sum_{f=1}^{l^e_q} t^n_{kqf}.$$

The time outlay in optical-electronic computer system while processing one image can be defined as:

$$T = \sum_{j=1}^{n_o} t^o_j + \sum_{q=1}^{n_e} t^e_q + t^k_{oe} + t^k_{eo} =$$

$$= \sum_{j=1}^{n_o} \sum_{z=1}^{l^o_j} t^o_{pjz} + \sum_{q=1}^{n_e} \sum_{f=1}^{l^e_q} t^e_{pqf} + \sum_{j=1}^{n_o}(l^o_j-1)t^b_{oo} + \sum_{q=1}^{n_e} \{\sum_{f=1}^{l^e_q} t^n_{kqf} + (l^e_q-1)t^b_{ee}\} + \sum_{i=1}^{n} \{t^b_{oei} + t^b_{eoi}\}. \tag{3}$$

The analysis shows that the processing time consists of two components - direct processing time and switching time. Switching time is defined by the time of data transfer between conveyor steps (devices buffering time) and the time of processors switching in electronic processing devices.

Let t_{pi} is the time of image processing on i-th step of the conveyor, t_{ki} is the switching time. The whole processing time on the i-th step of the conveyor will be:

$t_i = t_{pi} + t'_{ki}$, where $t'_{ki} = \max\{t_{ki-1}, t_{ki}\}$.

The through-put of a conveyor while processing a series of images is defined as:

$$PS = 1/\max_i\{t_i\} = 1/t'_i. \qquad (4)$$

On the basis of expressions (3), (4) there has been calculated the image processing time and the through-put of the system in the dependence on the conveyor length l_k, relation between optical and electronic processors $k_{oe} = l^o/l_k$ and the relation of the data processing time in electronic processors to the processing time in the optical processors: $a_t = t^e_{pqf} / t^o_{pjz}$.

The analysis shows that the time outlay depends proportionally inverse on the parameter value k_{oe} while having different values of l_k (Figure 7). On decreasing the parameter a_t the maximum time outlay T is observed at $k_{oe}=0.5$ and $l_k <8$. The reason is that on decreasing the parameter a_t, on the time outlay begins to influence substantially the inter modular switching (Figure 8).

Evaluation of the through-put of the system during the processing a series of images shows that on varying the value t'_i from 50 to 240ms the value PS is variable from 20 to 4 images per second.

6. METHOD OF THE TARGETS RECOGNITION SYSTEMS DESIGN

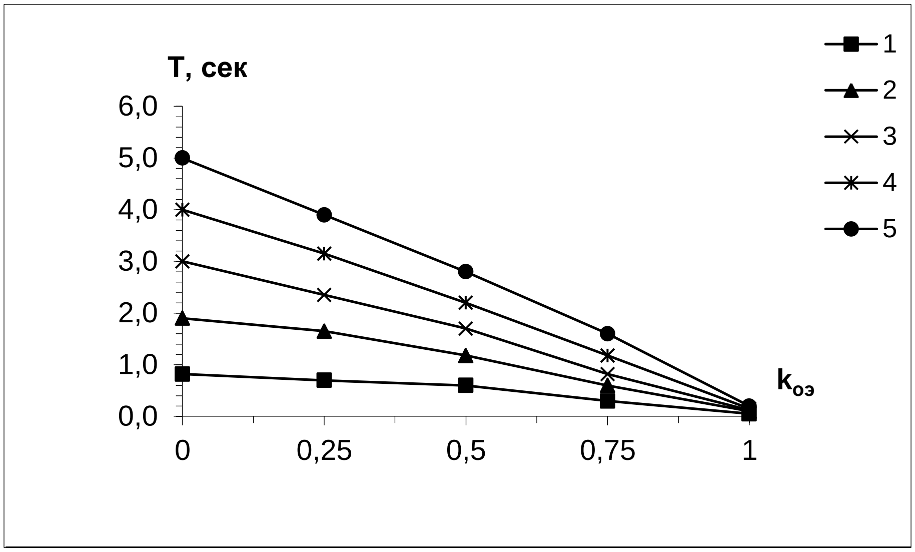
Let us suppose that a large enough sequence of images will be processed, therefore the time of the first step of image loading can be neglected.

The suggested method consists of the following:

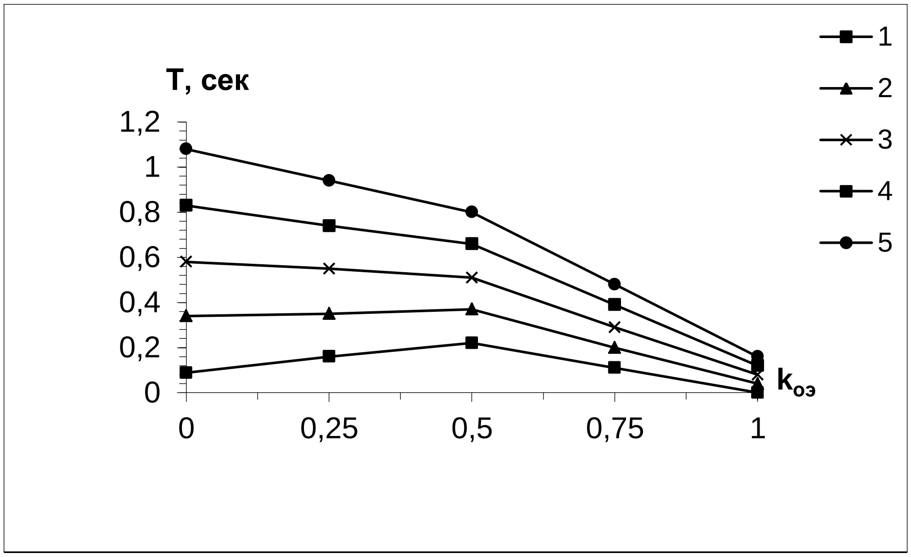
1. The image processing function W is represented as a set of operations $\{W_i\}$ in such a way that its further dividing is impossible or inexpedient. For example, such a function W_i can be indivisible, if its dividing does not lead to following decreasing of the processing time.

2. It is defined a set of operations $\{W_i\}_o$, which can be realized using of optical processors, providing the maximum level of spatial concurrency, speed and compactness. Other operations will be realized using electronic processors.

3. A corresponding switching network is forming which will consists of a set of the optical, electronic buffer devices.



a



b

Figure 7. Dependence of the processing time T from relation of the optical and electronic processors $k_{oe,}$ conveyor length l_k: 1÷5 – at l_k =4; 8; 12; 16; 20, at a_t=10^4 (a) and a_t=10^3 (b).

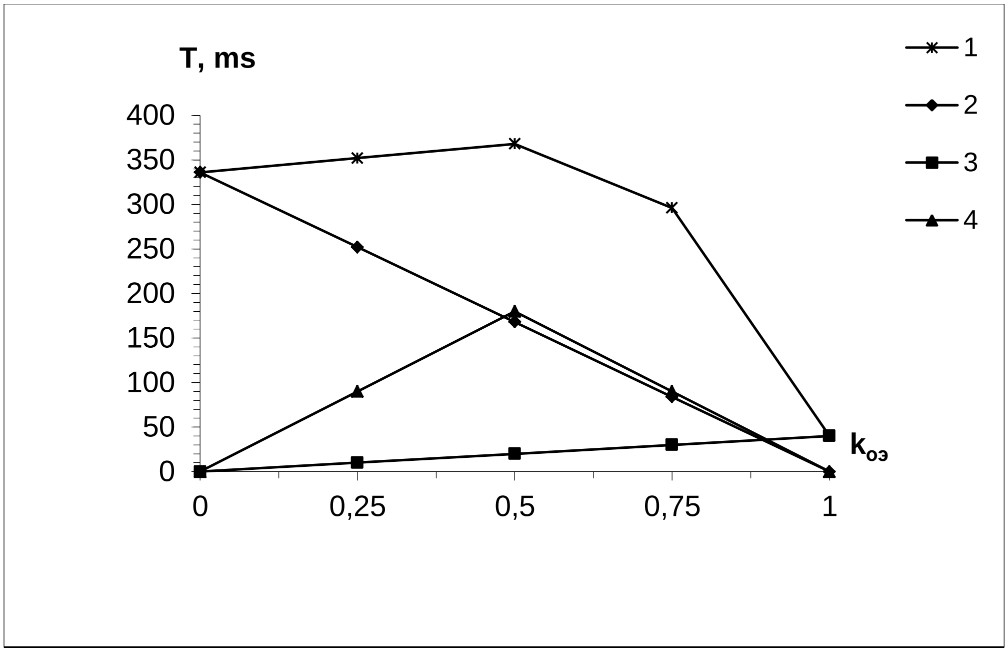


Figure 8. Dependence of the processing time from relation of the optical and electronic processors k_{oe} at l_k =4, a_t=10^3: 1 – total processing time in the system; 2 – in the electronic processing units; 3 – in the optical processing units; 4 – the of the inter modular switching

4. The realization time t_{pi} of different operations W_i and the switching time t_{ki} are defined (Fig.9.a). Basing on the sets of the parameters $\{t_{pi}\}$, $\{t_{ki}\}$, a processing operation W'_i that requires the maximum time outlay is determined out:

$$t'_i = \max_i\{t_i\} = \max_i(t_{pi}+t'_{ki}).$$

5. In the case when the operation W $'_i$ is realized using electronic processor, the possibility of t'_i decreasing up to the level of other values from the set $\{t_i\}$ is examined. For this reason the possibility of introduction of spatial concurrency using a set of processor elements is being analyzed. The image is dividing into separate fragments and for processing of each of them one or several processor elements are being used.

If, however, the function W'_i is being implemented by optical means and there does not exist a possibility to decrease the parameter t'_i, then it is expedient to make the justification of the parameters t_i of electronic modules till the level of t'_i by means of decreasing the number of the used processor elements or by their changing by some less rapid and therefore more inexpensive ones. As a result we shall obtain a balanced set of the parameters $\{t_i\}$ (Fig. 9,b), which provides the maximum through-put of the system.

The described method of the systems design assumes the absence of restrictions on the resources of processor elements in modules. In the case when such limitations take place, the design method will be a.f.

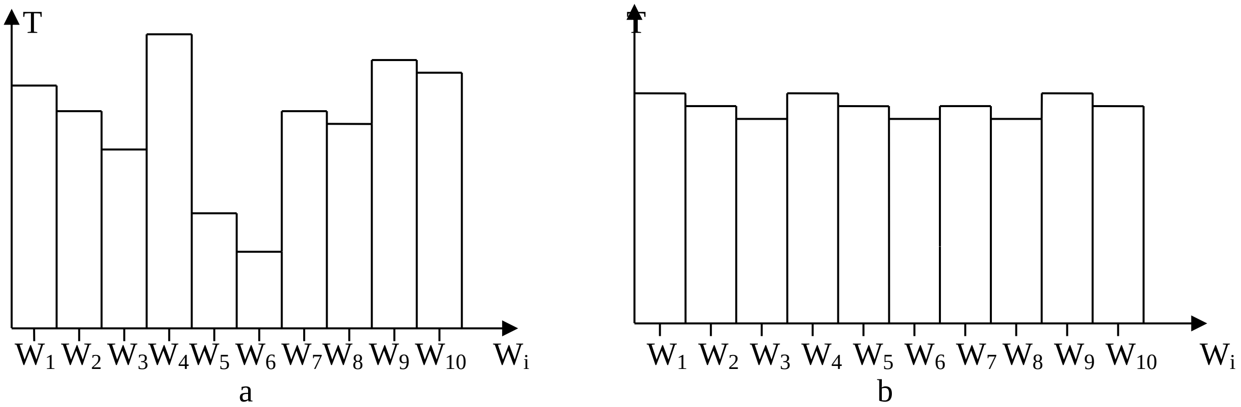


Figure 9. Distribution of the processing time T for different operations W_i in initial (a) and optimized (b) systems.

Let r_o from n functions, which are to be implemented, can be implemented optically and r_e=n-r_o functions are to be implemented by electronic means. Besides, let the resources of electronic processors are M_r and on each step of electronic processing the M_{ri} processors are used.

Having the restrictions on processor elements (PE) resources, the following variants are possible: $r_e>M_{ri}$; $r_e=M_{ri}$; $r_e<M_{ri}$. In the first case, i.e. when $r_e>M_{ri}$ several processing operations are uniting and their realization on one processing device are possible. If a group of operations, which are to be realized, are situated consecutively, then such way of processing is not problematical. If, however such operations are not situated consecutively then the necessity of cycle organization in the conveyor is appears. This leads to increasing of switching time outlay.

In the second and the third cases one or several processing devices can be used for each operation.

7. AN EXAMPLE OF A TARGET RECOGNITION SYSTEM DESIGN

Let us investigate the efficiency of the proposed theory on the example of the design of a system that implements the algorithm of targets recognition based on the invariant moment features.

The algorithm consists of the following:
1. Target’ image forming T(x,y).
2. Noise removing in the image.
3. Target extraction from the image.
4. Target’ moment features calculation.
5. Target identification.

In this way the image processing function W can be represented as a set of five operations W_i, i=1÷5. Each of them will implement a separate step of the algorithm:

$$T(x,y)\rightarrow W_1 \rightarrow W_2\rightarrow W_3\rightarrow W_4\rightarrow W_5\rightarrow RO.$$

The operations W_2, W_3 and W_4 can be implemented by optical means, W_5- only by electronic means and W_1- by optical or electronic means.

The target recognition system structure can be represented as it is shown in Fig.10. In this system the operation W_1 is implemented using image forming unit (IFU), the operations W_2, W_3, W_4 – are realized in the optical processors P_1-P_3, and operation W_5 - in electronic processor P_4. The type of the buffer storage B_1 will depend on the type of IFU. The buffer storages B_2, B_3 are optical, and B_4 is optical-electronic.

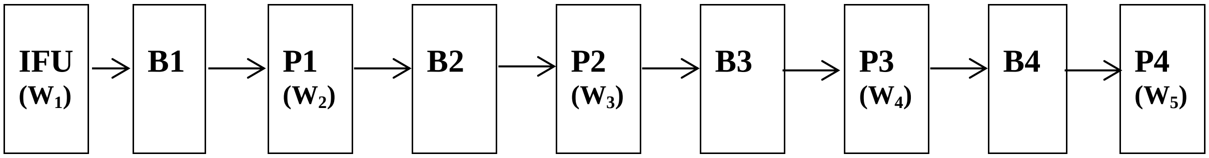


Figure 10. Structure of the target recognition system

The implementation of this algorithm in an electronic system also has been investigated. The operations processing time in the systems are presented in Table 4 and Figure 11.

Table 4. Processing time in optical-electronic and electronic systems, ms

Oper. nr.	Type of operation		Optical-electronic system			Electronic system
			Kind of unit	Time, ms		
				Initial system	Optimized system	Time, ms
1.	W_1	Image forming	Electronic	20.0	20.0	20.0
2.	Buffering B_1		Electr.-Optical	20.0	20.0	20.0
3.	W_2 (in P_1)	Noise removing	Optical	20.0	20.0	170.0
4.	Buffering B_2		Optical	10.0	10.0	20.0
5.	W_3 (in P_2)	Object extraction	Optical	20.0	20.0	170.0
6.	Buffering B_3		Optical	10.0	10.0	20.0
7.	W_4 (in P_3)	Moment features calculation	Optical	20.0	20.0	180.0
8.	Buffering B_4		Optical-Electr.	20.0	20.0	20.0
9.	W_5 (in P_4)	Object identificati on	Electr.	50.0	20.0	50.0
	Total			200	170	670

The analysis shows that the maximum time outlay in initial optical-electronic system will be at realization of the operation W_5: $t'_{W5} = t_8 + t_9 = 70$ms. The through-put of the system in this case will be $P' = 1/t' = 14$ frames/sec. After optimization of the system by decreasing of the processing time at the operation of target identification up to $t'_9 = 20$ms, the processing time $t''_{W5} = t_8 + t'_9 = 40$ms and through-put of the system in this case will increase up to $P'' = 1/t'' = 25$ frames/sec.

The maximum time outlay in an electronic system is defined by the realization of the operation W_4 and is equal to $t'_{W4} = t_6 + t_7 = 200$ms. That defines the through-put of the system is $P = 1/t'_{W4} = 5$ frames/sec.

The comparison of the optimized optical-electronic system and electronic systems shows that the through-put of the first of them is 5 times higher. The total time outlay is 4.8 times lower.

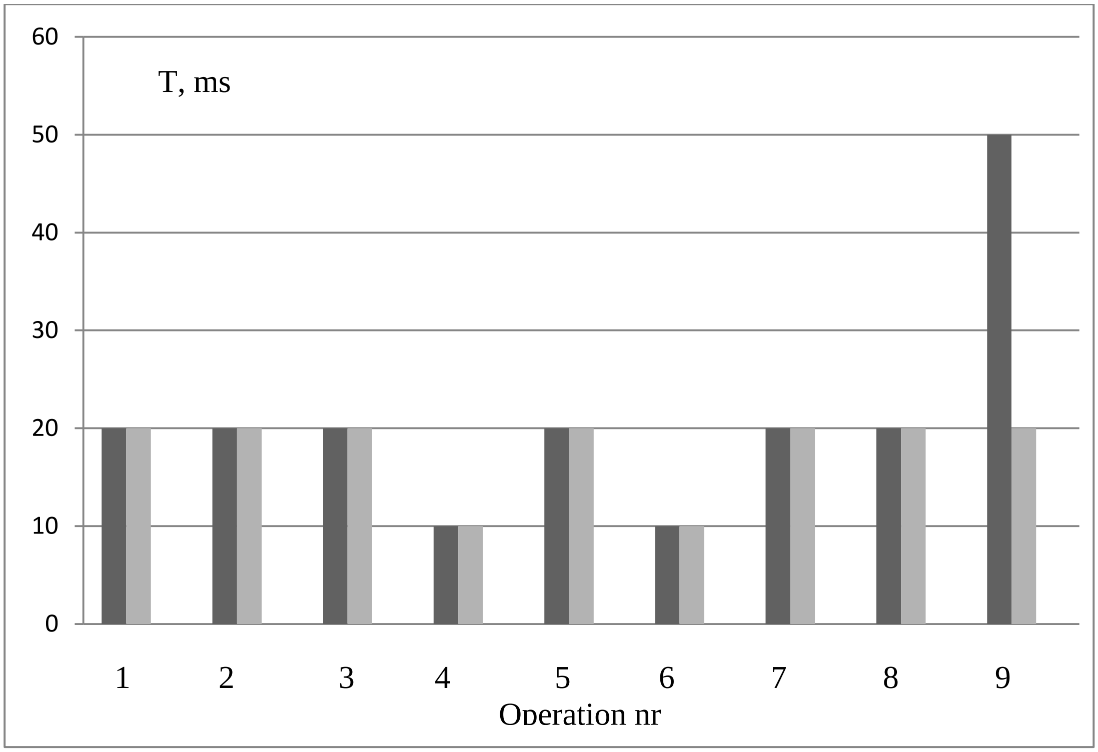


Figure 11. Processing time at different operation in initial (left) and optimized (right) optical-electronic systems

8. CONCLUSION

It is presented the general task of targets recognition, the classification of the targets recognition systems (TRS) and main requirements to them. It is showed that existing TRS have different disadvantages such as: insufficient productivity of data processing, low reliability of TR and flexibility, high consuming power, high weight and dimensions which don't permit effectively to realize the tasks of TR. In these conditions appear the necessity to elaborate new approaches to TRS construction and design, which will include electronic and optical processing units in optimal way and will permit to obtain maximal possible throughput of the systems.

A model of parallel image processing have been described which suppose the presentation of the targets recognition problem in the form of a linear sequence of separate sub problems and which allows to organize parallel processing of two types: in time and in space. Parallel processing in time consists in organization of the sub problems conveyor, which are implemented consecutively. The spatial concurrency means that on each step of the conveyor processing, the parallel processing of the whole image or its separate fragments is organized. At the working with the local information, the image can be represented as a set of sub images, which are processed by the corresponding set of processor units. The spatial concurrency can be implemented by the help of processor units set of electronic or optical type.

According to the proposed model, the generalized structure of parallel target recognition system is presented which include the processing optical or electronic units for realization of the different operations and buffer devices.

It was showed that optical processors are characterized by higher processing speed and have good perspectives. The analysis shows that the significant part of the wide used operations in target recognition, image processing can be implemented optically in 2-10 times faster than by electronic processors. Unfortunately, at present exists some operations, which can't be implemented optically.

The analysis of image forming units (IFU) characteristics showed that electronic and optical IFU provide the identical resolution ability. The difference between them consists in the image forming speed. Optical IFU allow to form images 2-8 times faster.

There are described the structures and parameters of the different kind of the buffer units necessary for connection of the processors: electronic, optical, electronic-optical and optical-electronic.

There have been made time expenditures determination in the target recognition systems and their through-put at the processing of one and series of images, in the dependence on the system conveyor length, relation between optical and electronic processors and the relation of the data processing time in electronic processors to the processing time in the optical processors.

The analysis shows that the time outlay depends proportionally inverse on the relation between optical and electronic processors k_{oe} for different values of conveyor length l_k. On decreasing of the relation of the data processing time in electronic processors to the processing time in the optical processors a_t, the maximum time outlay is observed at $k_{oe}=0.5$ and $l_k<8$. The reason is that on decreasing the parameter a_t, on the time outlay begins to influence substantially the inter modular switching.

Evaluation of the through-put (PS) of the system during the processing a series of images shows that on varying the maximum processing time on the i-th step of the conveyor t'_i from 50 to 240ms, the value PS is variable from 20 to 4 images per second.

There have been presented the method of targets recognition systems design, based on optimal combination of the optical and electronic processors, which permit to obtain maximum through-put of the systems.

The effectiveness of the proposed method was demonstrated at the design of the targets recognition system based on the moment's image features. The analysis shows that the through-put of the optimized optical electronic system is 1.8 times higher than of the initial system, and 5 times higher than of an electronic system.

REFERENCES

1. Marino Giovanni, Tarchi Dario; Kyovtorov Vladimir; Sammartino Pier Francesco. Ground based MIMO SAR and land clutter modelling: Difficulties and guidelines. IEEE 2015 Signal Processing Symposium, 2015, p. 1 – 5.

2. Fei Tai, Kraus Dieter, Zoubir Abdelhak M. Contributions to Automatic Target Recognition Systems for Underwater Mine Classification. IEEE Transactions on Geoscience and Remote Sensing, 2015, Volume: 53, Issue 1, P. 505 – 518.

3. Grimm Christopher; Farhoud Ridha, Fei Tai, Warsitz Ernst; Haeb-Umbach Reinhold. Detection of moving targets in automotive radar with distorted ego-velocity information. 2017 IEEE Microwaves, Radar and Remote Sensing Symposium (MRRS), 2017, P. 111 – 116.

4. Pisane Jonathan, Azarian Sylvain, Lesturgie Marc, Verly Jacques. Automatic Target Recognition for Passive Radar. IEEE Transactions on Aerospace and Electronic Systems, 2014, Volume: 50, Issue 1, P. 371 – 392.

5. Alkanat T., Tunali E., Öz S. Fully-Automatic Target Detection and Tracking for Real-Time, Airborne Imaging Applications. In: Braz J. et al. (Eds) Computer Vision, Imaging and Computer Graphics Theory and Applications. VISIGRAPP 2015. Communications in Computer and Information Science. Vol 598. Springer, 2016.

6. Optical Computing: Light and the Future of Computing. Gillware data recovery. August 27, 2015. https://www.gillware.com/blog/articles/optical-computing-light-and-the-future-of-computing/.

7. Digital signal processors meet Moore's law. Fibre Systems, 7 June 2016. https://www.fibre-systems.com/feature/digital-signal-processors-meet-moore%E2%80%99s-law.

8. Perju V.L. Image processing computer system construction based on optimal optical and electronic means combination. // In: Application of digital image processing. - Andrew G. Tescher, Ed. / Proc. SPIE Vol. 2564, pp.483-494 (1995).

9. EnLight256® 8000 Giga MAC / sec fixed point DSP. http://besho.narod.ru/reviews/newage/EnLight256.pdf.

10. First programmable optical digital signal processor. https://www.controleng.com/single-article/first-programmable-optical-digital-signal-processor /f921dca91f8d5d3ff1a367faa 9477d11. Html.

11. Special light modulators of Hamamatsu Corp.

12. http://search.hamamatsu.com/eu_en/search.x?q=special+light+modulators&page=1

13. Spatial Light Modulators – XY Series of Boulder Nonlinear Systems. http://bnonlinear.com/pdf/XYSeriesDS0909.pdf

Image Quality Improvement based on the Prediction Theory

[1]Zorea Pinchas, [2]Paladi Florentin, [2]Bragaru Tudor

[1]ORT Braude Engineering college, Karmiel, Israel.
Tel: +972-54-2403586. E-mail: pini.zorea@gmail.com

[2]Moldova State University, A. Mateevici str. 60, Chisinau MD.Tel: +373-67-31-55-13
E-mails: fpaladi@usm.md, fpaladi@yahoo.com, theosnume@gmail.com

ABSTRACT

People in all ages worldwide capture photos and immediately upload them to social networks. While the smartphones are the vehicles for these communications and the information transportation through what called social networks websites. Networks websites such as Facebook, Instagram, Twitter, and Snapchat as well as the huge growth of smartphones, have become a significant part of our culture and everyday lives. The huge number of photos and videos in social networks happen regardless to the material image quality. This paper proposes a new real-time image quality improvement process, which is based on the results of research evaluating how smartphones users perceived image quality of smartphones' embedded camera and display. This process is implemented in SW application to be embedded in the social networks websites. That application is one of the outcomes of research on perceived image quality in smartphones.

Keyword: Social network, image, quality, evaluation, human, visual, tests, attribute

1. INTRODUCTION

This paper provides a comprehensive overview of the research work in order to develop the new real-time image quality assessment and image quality improvement in the social networks. The research was based on perceived image quality evaluation experiments, which combined with the software application calibration according to the experiments scores. The perceived image quality evaluation includes human visual tests (HVTs) for subjective image quality assessment. The results of HVTs analysis identifies the most effective image quality attributes for perceived image quality.
The software tool was calibrated according to the HVTs scores. Figure 1 presents the percentage of time spent on social networks in the United States by platform. Most social networks are now mobile first [1].

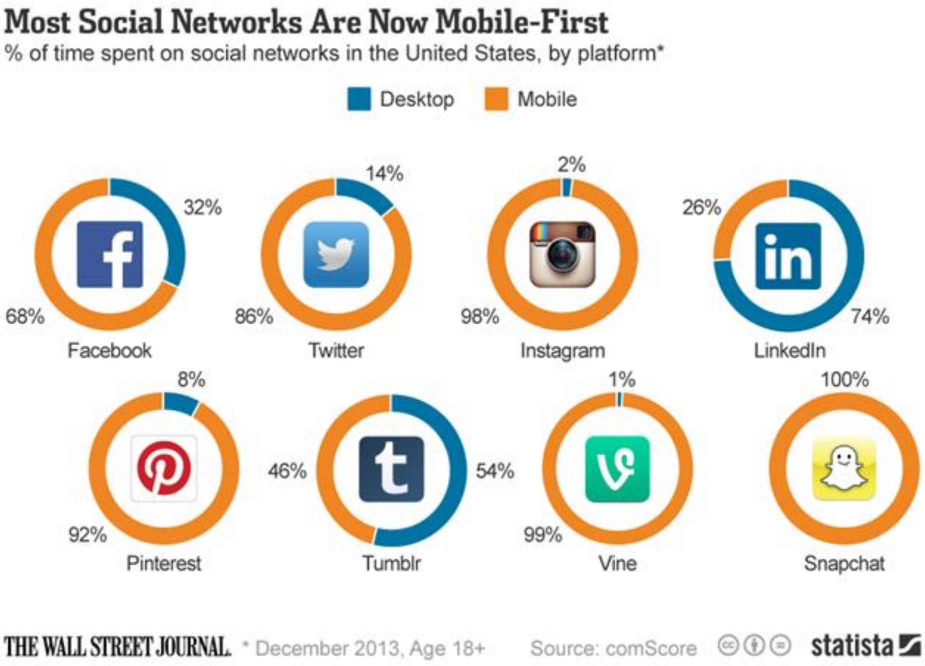


Figure 1. Percentage of spent time in social networks in using mobile [1]

Proposed framework for real time image quality assessment and image quality improvement is presented in Figure 2. Where images captured by smartphones uploaded to the social network website, the image goes first through real time image quality evaluation process and image quality improvement then it is loaded into the server and vice-versa.

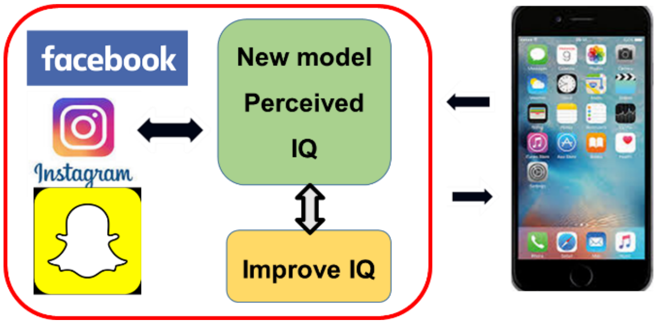


Figure 2. Real time image quality evaluation and improvement

2. IMAGE QUALITY ATTRIBUTES

Firstly, the important IQ attributes must be identified. Most of the standard IQ attributes have been considered by IQ researches as important to IQ assessment. In this work only four standard IQ attributes were selected: brightness, sharpness, contrast and color saturation. With this reduced number of IQ attributes, there are several important issues to consider, such as the relationship of these IQAs to other IQ criteria used in IQ evaluation applications. A long-term goal of this research is to create a link between subjective and objective IQ of smartphone images. With this intention, the IQ attributes should be based on perception and measurement for technological IQ issues. The IQ attributes should be clear enough to be scored by observers. In addition, the standard IQ attributes should be suitable for other IQ metrics using different IQ criteria. The existing groups of standard IQ attributes and IQ assessment models do not fulfill all of these requirements, and therefore a new group of IQ attributes is needed for HVTs and IQ assessment by SW application. Many of the IQ attributes used in research are similar and have common contribution to the perceived IQ.

This enables them to be grouped within more general IQ attributes in order to create a simpler evaluation of perceived IQ. There is usually a compromise between simplicity of IQ assessment procedure and accuracy when it comes to human visual test performance. Reducing most of the standard IQ attributes to four different dimensions, considered as important for the evaluation of perceived IQ. This reduced group of standard IQAs is a reasonable compromise between accuracy and complexity, which meets the statement by P. Engeldrum [3] that observers will not perceive more than five IQ attributes simultaneously. IQ attributes reduced to the following four:

- **Brightness** is considered so perceptually important that it is beneficial to separate it from the color. Brightness will range from “light” to “dark”.
- **Contrast** can be described as the perceived magnitude of visually meaningful differences, global and local, in lightness and chromaticity within the image.
- **Color** contains aspects related to color, such as hue, saturation, and color rendition, except lightness.
- **Sharpness** is related to the clarity of details and definition of edges.

A large number of subjective metrics have been developed for image quality subjective assessment [3]-[5]. Considering this wide range of applications, this research separated the objective research into two main categories: first, the methods that consider statistical or mathematical measurement (i.e., the image features extraction), and, second, methods that consider the human visual system (HVS) characteristics. In this approach, Figure 3 demonstrates the considering VIQET image analyzer measures with incorporation of HVS.

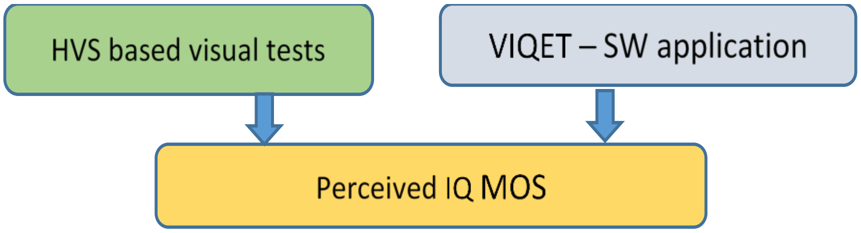


Figure 3. Image quality assessment flow

3. METHODS AND EXPERIMENTS

A large number of images should be used in order to reveal different quality issues. To achieve this, following the recommendations of VQEG, where the images were chosen based on the following criteria: Photos of 10 natural image contents captured by smartphones camera in native resolution of 1920x1200 pixels. These 10 images will be used as a reference. Each original image will be processed by adding the IQ attributes (brightness, contrast, color and sharpness) than the overall test content will be 50 images. Test content was created according to the VQEG recommendations P.913 [4], [7]. Contents were carefully selected to represent a wide range of different situations and demands for pictures. Also, recommendations of Photo-space standards set by I3A were considered when choosing the image contents.

Each original image was processed in order to enhance image quality attributes of: brightness, contrast, sharpness and color saturation. The overall test content for human visual assessment and VIQET analysis includes 50 images (5 images of each scene Figure 4).

1. Outdoor day – landscape, people.
2. Indoor – without backlight.
3. Indoor – with backlight.
4. Outdoor – night.

In order to measure the image quality attributes effect on perceived image quality, preparing 10 sets of natural images and 4 image quality attributes were changed in each original image. A set of images with four different image qualities attributes levels made of each single original image as demonstrated in Figure 5.

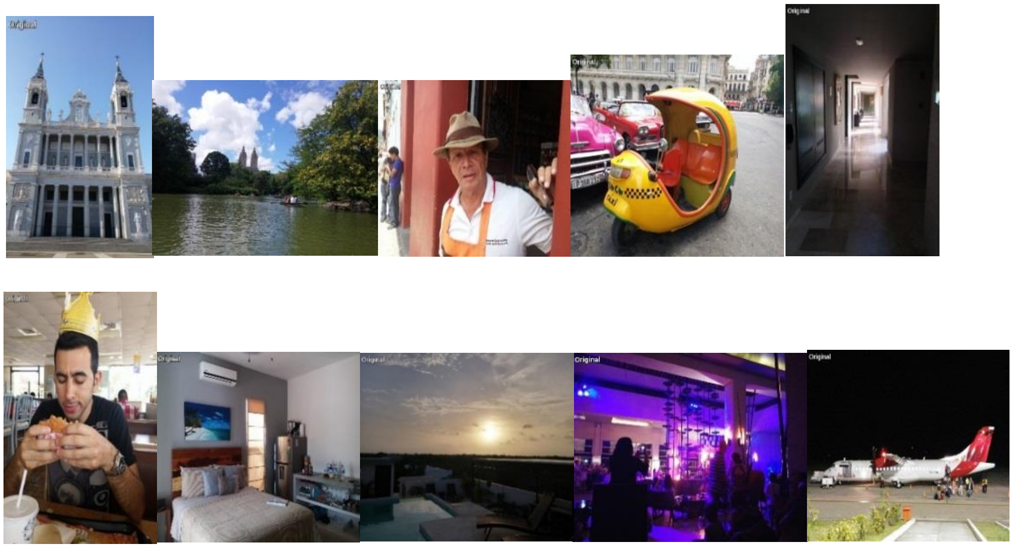


Figure 4. Tests content for image quality assessment

The flow chart in Figure 6, presents the method used in this research, which includes subjective IQ assessment through HVTs and objective IQ assessment with VIQET (VQEG Image Quality Evaluation Tool) which was developed for this purpose.

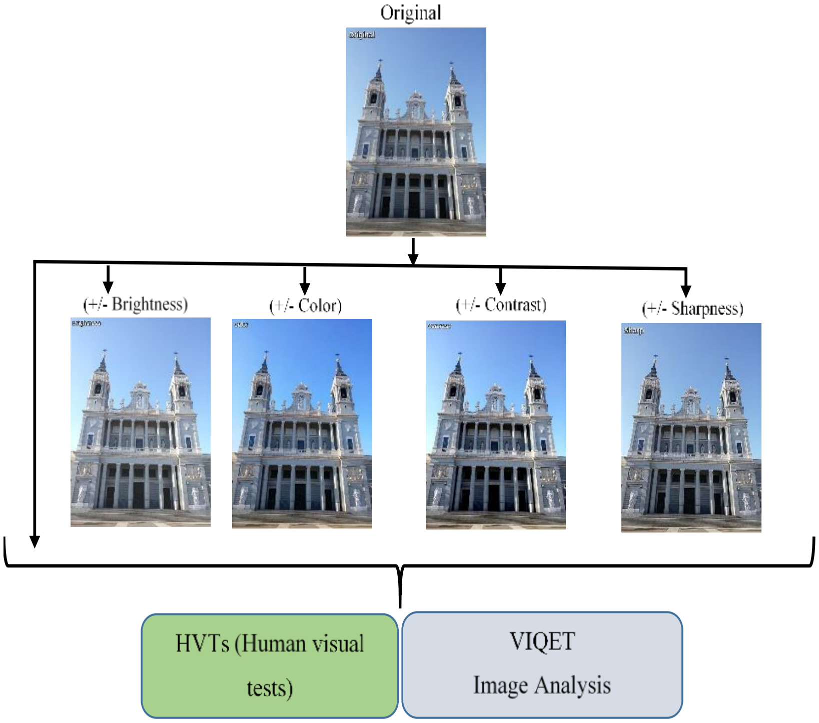


Fig. 5. Test material processing ("building")

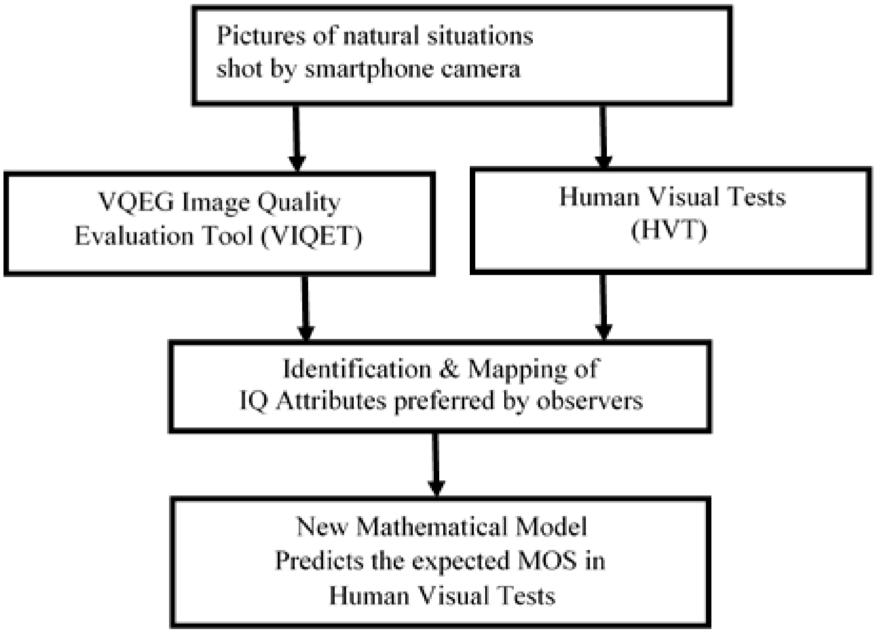

Pictures of natural situations shot by smartphone camera
VQEG Image Quality Evaluation Tool (VIQET)
Human Visual Tests (HVT)
Identification & Mapping of IQ Attributes preferred by observers
New Mathematical Model Predicts the expected MOS in Human Visual Tests

Fig. 6. IQ visual tests and image quality evaluation tool

3.1 Human visual test and VIQET image analysis

This part of study begins with an analysis of the images selected for test content for the HVTs and the VIQET. The process consists of two parts: first, finding how image quality attributes effect observers' preferences through HVTs, then image analysis with the VIQET.

Taking brightness, contrast, color saturation and sharpness as major image quality attributes, because these are the most visible everyday images. Image quality attributes improve or degrade the perceived visual quality of an image. The obtained results indicate that visibility of image quality is strongly depended on the IQ attributes added to the image.

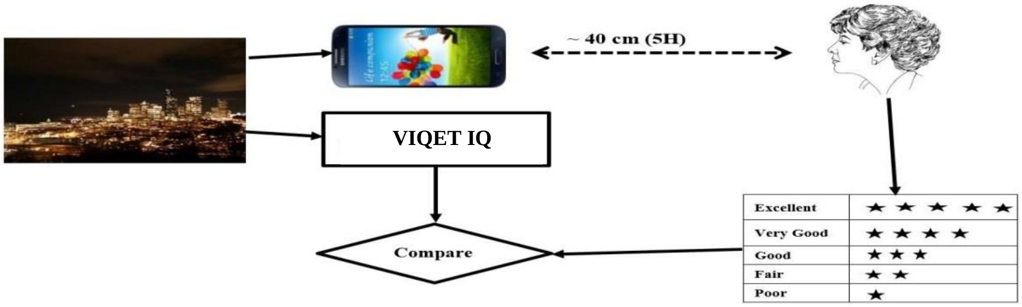


Fig. 7. Model of IQ visual tests and VIQET analysis comparison

The human visual tests (HVTs) test assessed the subjective quality of images material presented on a smartphone display (Samsung Galaxy S5) in a simulated viewing environment. The display resolution, however, was 1920 X 1080 in all tests. Each subjective experiment collected valid data from the participants.

The test material consisted of 50 images, which included the processed images with different IQ attributes. The image samples are presented one at a time, and rated independently using the five-grade image quality scale (1 = poor, 5 = excellent). During the data analysis the ACR (absolute category rating) scores given to the processed versions were subtracted from the ACR scores given to the corresponding reference to obtain a difference mean opinion score (DMOS).

3.2 Image quality evaluation with VIQET

The VIQET is an objective, no-reference photo quality evaluation tool. VIQET is an open source tool designed to evaluate quality of consumer photos. It estimates an overall mean opinion score for a device based on the individual image MOS scores in the set. The VIQET measures the image quality by image analysis based on RGB map (Figure 8) and Sharpness map (Figure 9).

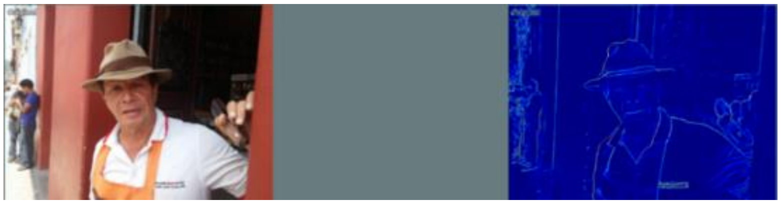


Fig.8. An example of VIQET RGB histogram

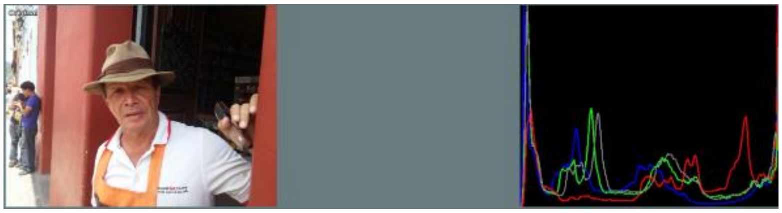


Fig. 9. An example of VIQET Sharpness map

3.3. VIQET image quality attributes and Image quality analysis by VIQET

Table 1 presents an example of VIQET IQ attributes of quantitative image features.

Table 1. VIQET image quality categories

Image feature	Score	Range
MOS	4.5	1 – 5
Multi- scale edge acutance	12.14	Higher is better
Noise signature index	99.39	0 – 589
Saturation	123.41	0 represents B&W image
Illumination	92.00	0 – 255
Dynamic range	106.72	Represents gray levels

- **Multi-scale edge acutance:** refers to how sharp the outline of objects in an image are and how many edges were detected in the scene.
- **Noise signature index:** refers to how noisy or grainy an image is.
- **Saturation:** refers to how vivid and intense a color is.
- **Illumination:** refers to how well-lit an image is.
- **Dynamic Range:** is the range between the lightest and darkest regions in an image.

VIQET is an objective, no reference photo quality. It estimates an overall mean opinion score (MOS) for an image. The estimated MOS for each image is based on a number of image quality features and statistics extracted from the test photo. The mapping from extracted features to MOS is based on psychophysics studies that were conducted to create a large dataset of photos and associated subjective MOS ratings. The studies were used to learn a mapping from quantitative image features to MOS. The estimated MOS by VIQET falls in a range of 1 to 5, where 1 corresponds to a low-quality rating and 5 corresponds to excellent quality.

The same images used for rating IQ by human visual test were required for IQ rating by VIQET to analyze each individual image and get its IQ scores (IQ categories).

3.4. Validation of the IQE results

Next step after the subjective tests, the credibility of assessment results was checked using the linear Pearson correlation coefficient (LPCC) suggested by ITU-T Recommendation P.913 [4].

The Linear Pearson correlation coefficient measures the linear relationship between a VIQET’s performance and the subjective data. Its great virtue is that it is on a standard, comprehensible scale of -1 to 1 and it has been used frequently in similar testing. The CC is calculated as follows:

$$CC = \frac{\sum_{i=1}^{N}(Xi-\overline{X})*(Yi-\overline{Y})}{\sqrt{\sum_{i=1}^{N}(Xi-\overline{X})^2}*\sqrt{\sum_{i=1}^{N}(Yi-\overline{Y})^2}} \qquad (1)$$

Where Xi denotes the subjective score MOS(i) in HVT for processed image (IQ attribute added), X denotes the MOS ("objective") of processed image (IQ attribute added) and Yi denotes the subjective score MOSp(i) in HVT of original image (no IQ attribute added), Y denotes the MOS ("objective") of original image. N in equation (1) represents the total number of images considered in the analysis.

Therefore, in the context of this test, the value of N in equation (3) is: N=10. The sampling distribution of CC is not normally distributed. "Fisher's z transformation" converts CC to the normally distributed variable z. This transformation is given by the following equation:

$$z = 0.5 \cdot \ln\left(\frac{1+R}{1-R}\right) \tag{2}$$

The statistic of z is approximately normally distributed, and its standard deviation is defined by:

$$\sigma_z = \sqrt{\frac{1}{N-3}} \tag{3}$$

The values of LPCC of each subject in HVT (Phase I) were calculated. As a result, the number of the valid subjects (i.e., 35) meets the requirement of the Video Quality Experts Group (VQEG).

Table 2 lists the LPCC of viewer's rating scores on each IQ attribute after the screening process. The perceived image quality of each image was measured in terms of the average score of all valid subjects, also known as the mean opinion score [5], [9], [11].

Table 2. The LPCC of each IQ attributes in HVT

IQ attribute	**Brightness**	**Contrast**	**Original**	**Color Saturation**	**Sharpness**
LPCC	0.22	0.85	0.28	0.72	0.25

The subjects in VIQET analysis were also screened according to the screening result. The perceived image quality difference of all valid subjects, also known as the differential mean opinion score (DMOS) [5], [13-15]. Then, Cronbach's alpha value was computed to measure the internal consistency of the valid scores on each device. The value of alpha of each device is considerably large, which **indicates** that there is a strong internal consistency among the valid subjects.

3.5 Human visual tests results

The perceived image quality on diverse IQ attributes is firstly investigated based on the rated scores, which is, MOS, for the images categories: outdoor day, indoor and outdoor night respectively. Considering the possible influence of the IQ attributes, these images have the same resolution (i.e., 1080P) but in different IQ attributes.

Take the high and low-quality images with ten randomly selected contents as an example, the relationship between the MOS, MSE, PSNR and the IQ attributes of outdoor day images, indoor images and outdoor night images were analyzed and found that there is no significant increase or decrease in the perceived quality, when the brightness is increased.

The viewer's perceived quality is not significantly influenced by the change of brightness during the viewing process. In a general sense, the MOS of the images displayed on all smartphones are used to illustrate the difference of perceived image quality across four IQ attributes (brightness, contrast, color saturation and sharpness).

Illustrate the rates of different IQ attributes defined by VQEG (Video Quality Experts Group) that measured and calculated by VIQET (VQEG image quality Evaluation Tool). Furthermore, a statistical analysis, which is, the one-way analysis of variance (ANOVA), is further performed to check the significance of influence of the IQ attributes on the perceived image quality. The test is firstly implemented on HVT (Human Visual Tests) while observers gave scores to each image displayed on mobile phone display. The analysis is conducted under different IQ attributes.

3.6 Calculating root mean square error

The accuracy of the objective metric is evaluated using the RMSE (Root Mean Square Error) evaluation metric, the calculated values presented in Table 3. The difference between measured and predicted DMOS is defined as the absolute prediction error Perror:

$$Perror(i) = Score(i) - MOSp \tag{4}$$

where the index i denotes the image sample.

While score (i) is the score gave by observer in HVT and MOSp is the predicted MOS (which is the average of all observers' scores). The root-mean-square error of the absolute prediction error Perror is calculated with the formula:

$$RMSE = \sqrt{\left(\frac{1}{N}\sum_{i=1}^{N} Perror(i)^2\right)} \tag{5}$$

where N denotes the total number of images considered in the analysis. (Results of the calculation using RMSE formula in Table 3).

Table 3. Results of the accuracy and signification calculation using RMSE formula

IQ attribute	Brightness	Contrast	Original	Color saturation	Sharpness
Building	0.86	0.72	0.73	0.55	0.53
Lake	0.98	0.69	0.63	0.48	0.54
Man	0.74	0.55	0.61	0.44	0.46
Taxi	0.87	0.59	0.81	0.52	0.47
Room	0.64	0.55	0.68	0.50	0.53
King	0.71	0.60	0.72	0.55	0.49
Hall	0.87	0.65	0.84	0.49	0.58
Bar	0.84	0.61	0.77	0.60	0.52
Sunset	0.81	0.61	0.72	0.55	0.44
Airplane	0.88	0.56	0.72	0.49	0.44

Scores given by the VIQET which based on the four IQAs to the same images that evaluated in the HVT are presented in Table 4.

Table 4. Results of the VIQET image quality analysis

IQ attribute	Multi-scale Edge Acutance	Noise Signature Index	Saturation	Illumination	Dynamic Range
Brightness	13.09	170.33	68.81	81.56	101.19
Contrast	15.71	259.47	115.78	143.20	95.95
Original	13.11	185.46	95.86	112.56	102.32
Saturation	12.23	196.91	112.25	120.26	102.43
Sharpness	27.74	236.84	96.40	173.21	103.28

MOS for the fifty images which evaluated by the observers during the HVT are presented in Table 5.

Table 5. MOS of perceived image quality attributes in HVT

IQ attribute	Brightness	Contrast	Original	Color saturation	Sharpness
MOS	3.46	4.50	3.74	4.62	4.69

3.7 Calculating DMOS Values

The data analysis was performed using the difference mean opinion score (DMOS). DMOS values were calculated for each IQ attribute. DMOS values were calculated using the following formula:

$$DMOS = MOSiq - MOSo \qquad (6)$$

While MOSiq is the average of MOS of IQ attribute and MOSo is the average of MOS of the original image. In using this formula, higher DMOS values indicate better quality. Table 6 presents the DMOS values of ten images with different IQ attributes.

Higher values mean better Image Quality. Sharpness, color saturation and contrast received the highest values respectively.

Table 6. DMOS calculations of IQ attributes

IQ attribute	**Brightness**	**Contrast**	**Color saturation**	**Sharpness**
Building	-0.37	0.75	0.89	1.06
Lake	-0.31	0.66	0.86	0.83
Man	-0.66	0.69	0.83	0.80
Taxi	-0.43	0.86	0.94	0.91
Room	-0.40	0.69	0.80	0.91
King	-0.31	0.74	0.91	0.97
Hall	-0.31	0.86	0.94	1.00
Bar	0.06	0.94	1.00	1.11
Sunset	-0.26	0.83	0.91	1.06
Airplane	-0.31	0.66	0.74	0.86

4.CONCLUSION

This paper proposes a new real-time image quality evaluation and image quality improvement application in real time. Once the application is embedded in the social networks websites. It evaluates the image quality of incoming images in the gateway while images uploaded to the server and improves their image quality in real time.

The same process is done while images downloaded from the website. The image quality evaluation criteria of this application was defined based on the evaluation of perceived image quality in smartphones [6-8], [10[, [12], [14], [15], which are the most popular vehicle in media transportation.

The proposed application brings a benefit to the social networks in image quality improvement of the media content.

REFERENCES

1. Number of smartphone users worldwide from 2014 to 2020. The Statistics Portal, https://www.statista.com/statistics/ 330695/number-of-smartphone-users-worldwide/ (accessed 18.07.2017).
2. Leclaire A., and Moisan L. No-reference image quality Assessment and Blind De-blurring with Sharpness Metrics Exploiting Fourier Phase Information. Journal of Mathematical Imaging and Vision (2014). 45
3. Engeldrum P.G. Image quality modeling: Where are we? Image Processing, Image Quality, Image Capture, Systems Conference (PICS). IS&T, pp 251–255 (1999).
4. Yang F., Wan S. Bitstream-based quality assessment for networked video: a review. IEEE Communications Magazine. 50(11),203–209 (2012). doi: 10.1109/MCOM .2012.6353702.
5. Bhattacharya S., Sukthankar R., and Shah M. A framework for photo-quality assessment and enhancement based on visual aesthetics, in: Proceedings of the International Conference on Multimedia, ACM, 2010, pp. 271–280.
6. Fry E., Triantaphillidou S., Jarvis J., and Gupta G. image quality Optimization, via Application of Contextual Contrast Sensitivity and Discrimination Functions. In image quality and System Performance XII 93960K, Proceedings of Electronic Imaging (San Francisco, CA, USA, Jan. 2015), M.-C. Larabi and S. Triantaphillidou.
7. Methodology for the Subjective Assessment of the Quality of Television Pictures, ITU-R BT.500-11.
8. Eds., International Society for Optics and Photonics, pp. 93960K–93960K–12. 15.
9. Gao Y., J. Tang R. Hong S., Yan Q., Dai N., Zhang T.-S. Chua, Camera constraint-free view-based 3-d object retrieval, IEEE Trans. Image Process. 21 (4) (2012) 2269–2281.
10. Gong R. and Xu H., "Impacts of appearance parameters on perceived image quality for mobile-phone displays," Optik, vol.125, no. 11, pp. 2554–2559, 2014.
11. Zorea P. Prediction of smartphones' perceived image quality using software evaluation tool VIQET. Studia Universitatis Moldaviae. 7(97), 170–180 (2016).
12. Gong R., XU H., Wang B and Luo M., Image quality evaluation for smart-phone displays at lighting levels of indoor and outdoor conditions. Opt. Eng. 0001.51(8):084001-1-084001-6. doi:10.1117/1.OE.51.8.084001.
13. Gao Y., Wang M., Zha Z.J., Tian Q., Dai Q., Zhang N. Less is more: efficient 3-d object retrieval with query view selection, IEEE Trans. Multimedia 13 (5) (2011) 1007–1018.
14. Hyesng J., Choon-W. K., Perceived image quality assessment for color images on mobile displays. Proc. SPIE 9395, Color Imaging XX: Displaying, Processing, Hardcopy, and Applications, 93950U (January 8, 2015), doi:10.1117/12.2083824.
15. Huete J.F., Fernández- Luna J.M., De Campos L.M., Rueda- Morales M.A. Using past-prediction accuracy in recommender systems, Inf.Sci.199(2012)78– 92.

A Comparative Study of Types, Tools and Techniques in Solar Irradiance Forecasting

Sheikh Kanza, Rehman Saad, Abbas Muhammad, Chaudry Qaiser

National University of Sciences and Technology, Islamabad, Pakistan
Rawalpindi-46000, Pakistan, Tel: +923218527037, +923348198705
E-mails: kanza.sheikh@ce.ceme.edu.pk, saadrehman@ceme.nust.edu.pk, m.abbas@ce.ceme.edu.pk, DrQaiserChaudry@gmail.com

ABSTRACT

The existing solar irradiance forecasting methods can be classified, according to the duration of forecast, into three classes: short, medium, and long techniques. The methods are breakdown into three approaches: statistical, physical, and hybrid. The purpose of this classification is to analyze the forecasting techniques that seem to embrace more potential for effectively forecasting a given data. The research evaluates the performances of different tools and techniques for selecting and constructing the most suitable solar irradiance forecasting model. This comparative study clears proper selection and structuring criterion, necessary for getting best results from forecasting model on given dataset. Lastly the paper outlines the future research directions and challenges faced by existing solar irradiance forecasting techniques.

Keywords: artificial, neural, network, solar, photovoltaic, system, irradiance, forecasting

1. INTRODUCTION

Heat and light are the two forms of solar energy. Solar energy is a renewable source because nothing is paid out to consume it on earth. This natural source of energy is also environment friendly with no harmful emissions or waste like other conventional energy sources. Solar energy is economical, with reduced distribution and transmission costs as it is located anywhere where there is sunlight. Even so, use of solar energy is not without its challenges.

The objective of review is to choose an appropriate forecasting technique, depending on a type of load, and then to propose a suitable model whose speculative characteristics are well-matched with the numerical properties of the particular data set. The generalized process is split into three steps: 1) data-preprocessing, 2) estimation, and 3) diagnostic checking. Solar irradiance forecasting is acquiring a lot of attention due to its auspicious applications in multiple fields. It is very costly and hard to install massive infrastructure in residential and industrial sector for communication between different fields as illustrated by **Error! Reference source not found.**. So the use of existing models and techniques is recommended [1]. Comparison between different forecasting types with their durations, strengths and drawbacks are shown in Table 4.Further these types are breakdown into three categories of forecasting approaches as depicted in the following Table 5. These categories of approaches have multiple techniques to facilitate the forecasting process .

The novelty of this paper lies in reviewing and classifying solar irradiance forecasting types, tools and techniques. The research gives the basis for forecast in photovoltaic systems, a concise analysis of forecasting techniques and their performance evaluation as discussed in the literature. It is difficult to rank the performance of all reviewed tools and techniques at this point because these are developed for different environments and scenarios. So, all the techniques are organized under the categories of types and nature of approaches.

All tools, approaches and techniques that are compared in this paper to give a complete understanding of each scheme and their behavior in various environments. This comparison will pave the way for further research of developing different solar irradiance forecasting models. The remainder of the paper is arranged as follows. Section 340 introduces solar irradiance forecasting, including methods and approaches.

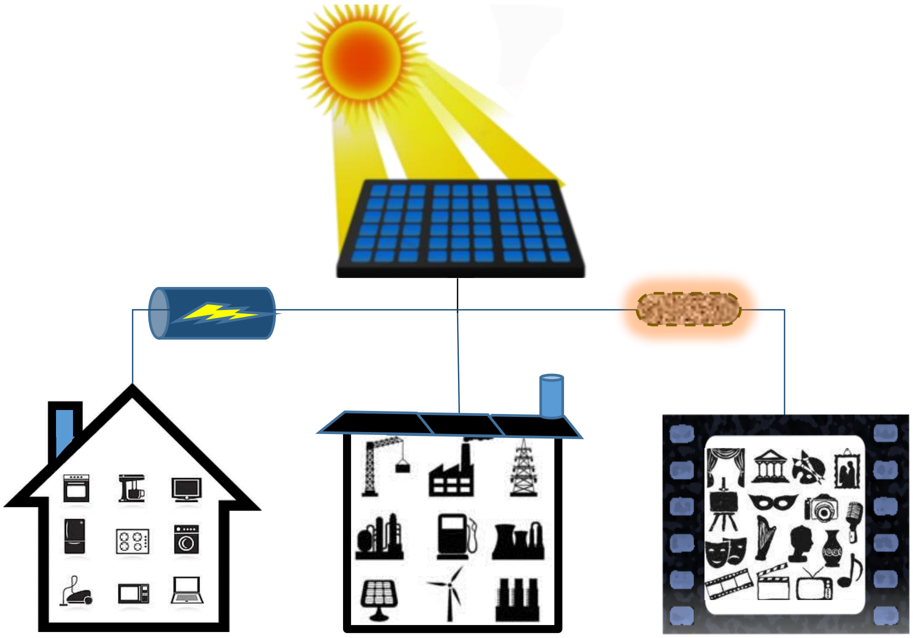


Figure 7 Applications and transmission strategies of solar energy

In section 3, a basic research upon forecasting classification is made. Besides this, forecasting strategies, approaches, classification, advantages, and disadvantages are also analyzed in this section.Then, in section 0, all solar irradiance forecasting tools are reviewed in detail. In this section, the tabulated summaries of existing tools are also presented. Section 0 and 0 enlist the general forecasting steps and research challenges respectively. Finally, section 0 concludes the paper by highlighting findings. The future work and research directions is discussed and suggested in section 0.

2. LITERATURE REVIEW

Global horizontal irradiance (GHI) forecasting gives a more accurate modeling and forecasting for solar power. Several solar irradiance forecast models and approaches are based on the time horizon, and applications. Long term solar irradiation estimation in Morocco by using a three layered and back propagated ANN model [3]. Multi-nonlinear regression neural network to estimate solar radiance in Turkey [4].The spectrum methods like the Autoregressive model (AR) and the Autoregressive moving average model (ARMA) [5], are competent for forecasting the future value of adaptive time series data. The fame of the ARMA method within the scientific research lies in its ability of mining stimulating statistical tools, in accumulation with adoption of the renowned Box-Jenkins method [6].Non-stationary solar irradiance data needs pre-processing. Lauret et al. [7] proposed a benchmarking of several machine learning techniques and an AR model. Bird clear sky model [8] is used to make stationary solar irradiance data. Recently, David et al. [9] extend the same pre-processing work to forecast solar irradiance with recursive ARMA-GARCH models. Many artificial intelligence (AI) techniques including artificial neural networks (ANN), expert systems (ES), genetic algorithms (GA), fuzzy logic (FL) and many hybrid systems were introduced for irradiance forecasting [10]. As the irradiance forecasting techniques including support vector machines, generic algorithms, regression series and all the variations of Artificial Neural Networks (ANN) are well efficient and have the capability to work even more efficiently then before by considering the climate variables (maximum temperature, sunshine duration, relative humidity, cloud cover, longitude, latitude and altitude) while training and producing an output as supported by various studies [11].

3. CLASSIFICATIONS OF SOLAR IRRADIANCE FORECASTING METHODS

Accurate predictions are needed over different time horizons: from very short-term to long-term horizon. There are three different types of irradiance forecasting approaches including statistical, physical and hybrid. Physical models utilize the current atmospheric observations and make future predictions with supercomputers. The statistical models predict the future value by considering the historic trend. Hybrid models (also known as combined models) combine two or more forecasting techniques to increase the forecast accuracy. Hybrid models are meant for overwhelming any insufficiency of using distinct model, such as regression models, to take the benefit of each distinct model and combine them to decrease forecast errors. It is vital to keep in mind that significant concerns like solar irradiance modules, clear sky models, air mass, Linked turbidity and clearness's indices have not been stated at this point because here we deal with Global Horizontal Irradiance (GHI) which is suitable for solar PV systems and do not require direct components of solar irradiance.

The forecasts aid the power system operators in ensuring supply reliability as well as optimal operation planning to allow dispatch of existing renewable generation.

Table 4. Comparison between forecasting types

Forecast Types	Duration	Strengths	Drawbacks	Well-suited Approaches
Short	1h to a week	Best for forecasting Load on holidays	Slow Processing	Statistical
Medium	1 month to an year	Fast to compute, model and trend tracking	Frequent changes in variables like gold price cannot be incorporated easily.	Physical
Long	several years	Minimizes the penalties and ensures the reliable operation	Complex training and forecasting process on Long term historic data	Hybrid

Table 5. Comparison of existing forecasting approaches

Forecasting Approaches	Input Data	Mean Absolute percentage error (MAPE) [12]	Example Technique	Limitation	Strength
Statistical	historical data	8.29% to 10.8% under different weather conditions	AR, MA, ARMA, ARIMA, ANN	Unable to retrieve data in remote areas	Ability of self-organize, learn and adapt
Physical	Environmental description	10% to 12% In case of long term forecasting	(NWP) and satellite cloud imagery	Hard time to provide predictions	More accurate long term planning
Hybrid	Environmental and historical data	7.65%	Fuzzy Logic Cao and Cao	Requires meteorological data even in remote areas	Show good generality capabilities irrespective of environment

3.1 Statistical Methods

Statistical methods additionally incorporate the persistence, which conjectures the future forecasting accepting that it is like past esteem. The perseverance technique is the least complex kind of gauge and is the most widely recognized reference show for brief time skyline conjectures [12].Linear factual models have a place with the class of time-arrangement forecast strategies .They are the most broadly executed and customary strategies exhibit in the writing as contrasting options to the physical techniques. Conventional factual procedures incorporate autoregressive (AR), moving normal (MA), ARMA and different variations of comparative models. The general type of such a model is given by the creators of [14]. In a few examinations, the attention has been on determining the power yield from a PV plant in view of comparative methods for irradiance estimating. In an investigation by Bacher et al. [15], both AR and AR with exogenous info (ARX) models were to anticipate the hourly estimations of sun based power for skylines up to 36 h. Another measurable approach is the Coupled AR and Dynamical System (CARDS) show discussed by [16] to figure out sun oriented radiation time arrangement for one day ahead forecast. Since sunlight based radiation displays regularity, the sun oriented radiation information was utilizing Fourier arrangement and power range examination as exhibited in Boland. Measurable methodologies require noteworthy volume of authentic time arrangement information. ANNs are propelled by the normal insight and the capacity of the human cerebrum to adjust its subjective

Table 6 Comparison of existing techniques

Techniques	Problem Type	Average predictive accuracy	Training speed	Prediction speed	Automatic feature interactions learning?	Parametric
Logistic regression	Classification	High	Fast	Fast	No	Yes
ARIMA	Either	Low	Fast	Fast	Yes	No
ANN	Either	Low	Slow	Moderate	Yes	No
Linear Regression	Regression	Low	Fast	Fast	No	No
SVM	Classification	High	Fast	Fast	Yes	Yes
NWP	Either	Medium	Fast	Fast	Yes	No
GFS	Either	Low	Fast	Moderate	Yes	Yes

procedure to tackle complex issues. The plan of ANNs empowers them to gain as a matter of fact and to exhibit solid summing up the competences. These models are information driven procedures which can speak to a complex non-direct relationship and are fit for extricating the reliance between the information and yield factors through the preparation and learning process. What's more, they have the capacity of self-association, learning and adjustment [17], hence, they are an effective and adaptable tool for forecasting. ANNs are arranged in two structures: encourage forward neural systems (FFNNs) and intermittent neural systems (RNNs) [18]. These systems normally have layers of information and yield neurons with at least one shrouded layers. The hidden neurons in function in innermost layers, to create important associations between the outside sources of info and the system yields. On alternate hand, RNNs are portrayed by the nearness of in reverse associations makes RNNs especially valuable in the demonstrating of dynamic frameworks [19].

3.2 Physical Methods

Physical forecasting techniques can be categorized in two basic groups; those that are satellite based (cloud imagery) and those based on numerical weather prediction (NWP).Various NWP- are typically marketable and are settled and functioned by meteorological stations, utilities and private companies [20]. Almost 14 operating global NWP models can be utilized by solar irradiance forecasting [21]. Integrated Forecast System (IFS) and Global Forest System (GFS) are another important contribution in literature. ECMWF forecasts fifteen day ahead solar irradiance and cloud parameters. The satellites and sky images are related to evaluation of cloud structures and motion from historical as well as current data to forecast their location and size in future and hence directly related to solar irradiance [22].

3.3 Hybrid Methods

Hybrid methods take advantage from different forecasting models. Few solar based forecast methods that exist in the literature are appeared in Table IV. Hybrid models have been executed in three diverse ways; linear, nonlinear and both of them. With the goal to enhance the anticipating exactness, half and half methodologies has been proposed by numerous scientists [23]. Fuzzy Logic includes non-straight mapping of information factors to the yield with persistent scope of participation works in the range [24]. Different investigations have used fuzzy methodologies in the anticipating of based irradiance and PV control generation. The handiness of these models is especially unique in circumstances where the correct model of the framework isn't accessible or deficient, or when the issue definition includes vulnerability or equivocalness. In [25], the creators utilized estimated temperature and irradiance to acquire fuzzy logic models. Interim sort 2 fuzzy models are utilized to represent the vulnerability intrinsic in the sun oriented irradiance expectation. The majority of these strategies required meteorological information as info, which may not be promptly accessible in remote territories. The blunders in the meteorological information influence the nature of sun based irradiance figures. Moreover, climate data is generally illustrative yet not evaluated [27]. Cao and Cao in [28] built up a hybrid model for anticipating arrangements of aggregate every day sun powered irradiance, which joins ANN with wavelet investigation. Ji and Chee [29] utilize a cross breed model [30] of ARMA and TDNN to enhance the forecast precision. They assume that the everyday solar based irradiance arrangement is created by linear and nonlinear methods [31] and utilize the ARMA model to fit the direct segment and the TDNN model to locate the nonlinear pattern lying in the residual. Every single mixture display can possibly outfit the interesting highlights and qualities of blend of models instead of utilizing the models independently [32].

4.SOLAR IRRADIANCE FORECASTING TOOLS

For the comparative analysis of tools some parameters are defined for tool evaluation .Each tool is checked against each parameter and find whether the tool have that feature or not. Only those parameters which are common for all tools like each tool must have some import and export formats and supported parameters (time horizon etc.) are defined. A parameter of release date to find out that how many years of solar irradiance dataset it contains. Other parameters include user how convenient it is for the user to operate the interface (user friendly GUI), either the tool have partially free (for specific time or with certain features). Platform independence or cross platform support (it can run on multiple platforms) is another plus for any tool. Every tool has its unique as well as common parameters for example clear sky index, meteorological factors like temperature and parameters related to solar geometry are common among all. Tools are mentioned below with their reference websites for complete description and help.

Table 7. Comparison of solar irradiance tools

Ref.	Tools	User Friendly GUI	Parameter supported	Import Formats	Export Format	Cost	Cross Plat-form	Release Year
[33]	Area Solar Radiation	Medium	19	.sa	.apk	Full Free	Yes	2000
[34]	Points Solar Radiation	Medium	18	.dbf,.txt	.apk	Full Free	Yes	1999
[35]	Solar Radiation Graphics	Low	20	.dbf, .sa	.pdf,.apk	Partial Free	Yes	1990
[36]	Meteonorm	High	13	.csv	36 formats	Partial Free	Yes	1981
[37]	PVGIS	Medium	24	.MET, *.SIT	.txt, .pdf	Full Free	Yes	1981
[38]	NASA SSE	Medium	58	.txt	.txt,.xml	Full Free	Yes	1983

We have done the analysis on the basis of the above mentioned parameters. The analysis is given in the Table 4. The analysis shows that all the tools are cross platform supported. Majority of the tool convert text (.txt) or database (.csv, .dbf) to text portable (.pdf) or executable (.apk) format. All tools are quite user friendly but Meteonorm is highly user friendly. Both Meteonorm and PVGIS are mature tools as compared to others as they have solar irradiance data since 1981.

5.FORECASTING METHODOLOGY IN GENERAL

This section explains a set of three generic steps of data pre-processing, estimation, and diagnostic checking as shown by Fig. 2

Step 1: Data Pre-Process
This step is meant for data labeling and modification before giving it as input into the forecasting tool. The preprocessing includes: removing nighttime GHI values, detruding, and normalization.

Step 2: Estimation
In this step, the pre-handled information are acquainted with the anticipating tool. The recorded GHI information are sustained to the model as an info and the real GHI is nourished as an objective. The model is set up by the particular data sources as inputs. The chronicled information is prepared utilizing distinctive preparing techniques and the blunder is investigated. The preparation procedure proceeds until the mistake between the determined and the real GHI is limited given the information sources, weights and by utilizing different parameters.

Step 3: Diagnostic Checking
After getting an output from the model, errors are calculated and solution accuracy is determined. Models like NWP require diagnostic checking for modification of systematic deviations; that includes indirect and not standardized parameters delivered by the NWP models as output (e.g., solar surface irradiance); consolidate the yield of various models in an ideal way. The resultant estimated information from organize two speak to the daytime GHI esteems in standardized shape. In this way, organize three is the turnaround of the primary step. Step three incorporates three procedures: denormalization, including evening hours, and figuring the GHI. The handled information is denormalized e.g. through increasing the hourly pinnacle clear sky GHI by the hourly yield GHI from step 2.

6.SOLAR IRRADIANCE FORECASTING CHALLENGES

GHI forecasting is less accurate due to multiple reasons:

- Despite of considerable increase in the size and installed capacity; intermittent (i.e., unavailability) and fluctuating (i.e., constantly change in time) nature of renewable generation is a challenge.

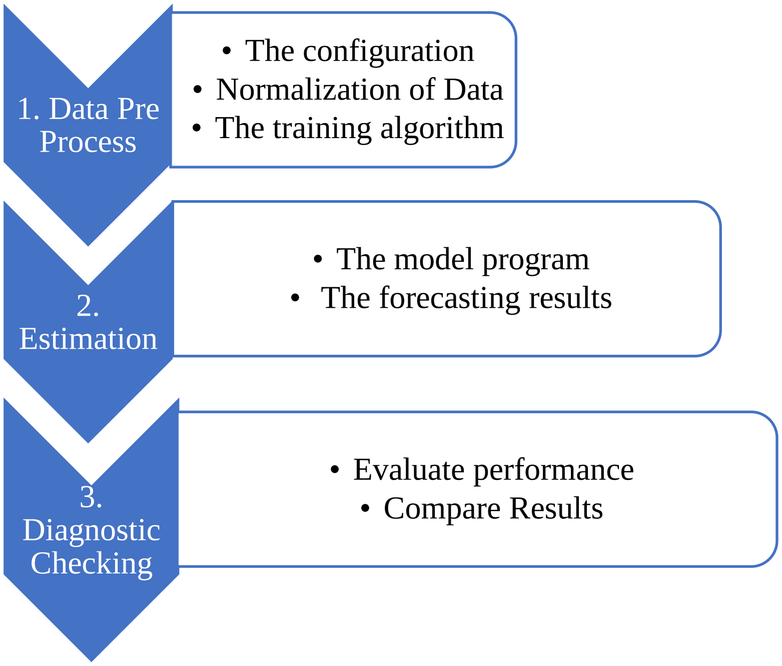


Figure 8 Generalized Forecasting Steps

- Failure to forecast the timing and severity of the fluctuations.
- The irregularity of solar data pattern due to climate change has imposed significant limitations to forecasting models [39]. So, sunny climate has noticeable patterns as compared to foggy climate hence less forecasting error.
- Different times of same day (like the sunset and the sunrise) imposes limitations to forecasting horizon.
- The long-term forecasting usually requires training on long-term historical solar irradiance data to extract patterns of the time series.
- To assure the regulation of supply to demand, providers and managers have to schedule the energy distribution and to guarantee that the generated power meet the consumer's demands plus the electricity cost.

7.CONCLUSION

This paper has offered different forecasting types according to their various selection techniques and principles. An expansive number of existing forecasting techniques have been looked into. Types of solar irradiance forecasting ranges from couple of minutes to a year, has received an immense consideration from industrial and academic scientists. The accuracy of forecasting reduces the energy consumption, distribution and transmission overhead by meeting the future energy demand in an effective manner. The comparison between types, tools and techniques for solar irradiance forecasting is made upon the various parameters of forecasting such as being MAPE, cost, interface type etc. The process of the forecasting routing is divided into three generic step it is not possible to review the performance of every techniques, which are meant for different environments. Therefore, few important techniques are reviewed along with their functionality, performance, strengths, drawbacks and applications in various environments.

FUTURE WORK

Vulnerabilities and intermittent nature of natural resources like solar irradiance to enhance solar irradiance forecasting over temporal and spatial horizons. Sky image techniques will also need to be integrated with the methods like ARIMA and WRF for more accurate forecast product with different time horizons of forecast.

REFERENCES

1. Tuohy J. Zack, Haupt S.E., Sharp J. at all. “Solar Forecasting: Methods, Challenges, and Performance,” *IEEE Power Energy Mag.*, vol. 13, no. 6, pp. 50–59, Nov. 2015.
2. Ela E., Diakov V., Ibanez E. and Heaney M. “Impacts of variability and uncertainty in solar photovoltaic generation at multiple timescales,” *Contract*, vol. 303, pp. 275–3000, 2013.
3. Honeyman S. Kann, Baca J. “U.S. SOLAR MARKET INSIGHT ‘Executive Summary’ 2015 Year in Review.” Solar Energy Industries Association | SEIA and GTM Research, Mar-2016.
4. Chupong and Plangklang B. “Forecasting power output of PV grid connected system in Thailand without using solar radiation measurement,” *Energy Procedia*, vol. 9, pp. 230–237, 2011.
5. Chen S. Duan, Cai T., and Liu B. “Online 24-h solar power forecasting based on weather type classification using artificial neural network,” *Sol. Energy*, vol. 85, no. 11, pp. 2856–2870, Nov. 2011.
6. Watetakarn S., Premrudeepreechacharn S. “Forecasting of solar irradiance for solar power plants by artificial neural network,” I *Smart Grid Technologies-Asia (ISGT ASIA), 2015 IEEE Innovative*, 2015, pp. 1–5.
7. Diagne H.M., Lauret P., David M. “Solar irradiation forecasting: state-of-the-art and proposition for future developments for smallscale insular grids,” in *WREF 2012-World Renewable Energy Forum*, 2012.
8. Stefferud K., Kleissl J., Schoene J. “Solar forecasting and variability analyses using sky camera cloud detection & motion vectors,” in *Power and Energy Society General Meeting, 2012 IEEE,* 2012, pp. 1–6.
9. Kleissl J. *Solar Energy Forecasting and Resource Assessment*. Academic Press, 2013.
10. Diagne M., David M., Lauret P., Boland J., Schmutz N. “Review of solar irradiance forecasting methods and a proposition for smallscale insular grids,” *Renew. Sustain. Energy Rev.*, vol. 27, pp. 65–76, Nov. 2013.
11. Diagne H.M., Lauret P., David M. “Solar irradiation forecasting: state-of-the-art and proposition for future developments for smallscale insular grids,” in *WREF 2012-World Renewable Energy Forum*, 2012.

12. Huang R., Huang T., Gadh R., Li N. “Solar Generation Prediction using the ARMA Model in a Laboratory-level Micro-grid,” in *Smart Grid Communications (SmartGridComm), 2012 IEEE Third International Conference on*, 2012, pp. 528–533.
13. Pillai J. S., Pillai M.J. “An Algorithm for Retrieving Skyline Points based on User Specified Constraints using the Skyline Ordering”, *International Journal of Computer Applications*, vol. 104, no. 11, pp. 24-29, 2014.
14. Zhang Y., Beaudin M., Taheri R., Zareipour H., Wood D. “Day- Ahead Power Output Forecasting for Small-Scale Solar Photovoltaic Electricity Generators,” *IEEE Trans. Smart Grid*, pp. 1–1, 2015.
15. “Solar Data 1991-2010 Site #725650.” [Online]. Available: http://rredc.nrel.gov/solar/old_data/nsrdb/19912010/hourly/siteonthefly.cgi?id=725650. [Accessed: 16-Sep-2014].
16. Webberley A., Wenzhong Gao D. “ Study of Artificial Nectial Network based short term Irradiance forecasting” Power and Energy Socie-ty General Meeting (PES), 21-25 July 2013, 1-4.
17. Hesham K. Alfares and mohammad Nazeeruddin, Electrical Irradiance Forecasting Literature Survey and Classification of Methods, International Journal of Systems Science 33 (1), 2002, 23-24.
18. Ke Li, Tai N., S. Zhang S. “Research and application of climatic sensi-tive short - term irradiance forecasting,” *2015 IEEE Power & Energy Socie-ty General Meeting*, Denver, CO, 2015, pp. 1-5.
19. Farah A., Farah N. “Multi-model approach for electrical irradiance forecasting,” 2015 SAI Intelligent Systems Conference (IntelliSys), London, 2015, pp. 87-92.
20. Munkhammar J., Widén J. "Correlation modeling of instantaneous solar irradiance with applications to solar engineering", Solar Energy, vol. 133, pp. 14-23, 2016.
21. Lim P., Nayar C. "Solar Irradiance and Load Demand Forecasting based on Single Exponential Smoothing Method", International Journal of Engineering and Technology, vol. 4, no. 4, pp. 451-455, 2012.
22. Tofallis C. “A better measure of relative prediction accuracy for model selection and model estimation” Journal of the Operational ResearchSociety vol. 66 no. 8 pp. 1352-1362 Nov 2014.
23. Genyong C., Jingtian S. “Study on the methodology of short-term irradiance forecasting considering the accumulation effect of tempera-ture,”2009 International Conference on Sustainable Power Generation and Supply, Nanjing, 2009, pp. 1-4.
24. Pavan M., Pavan A.M. “A 24-h forecast of solar irradiance using artificial neural network: Application for performance prediction of a grid-connected PV plant at Trieste, Italy,” Sol. Energy, vol. 84, no. 5, pp. 807–821, May 2010.
25. Huang Y., Lu J., Liu C., Xu X., Wang W., Zhou X. “Comparative study of power forecasting methods for PV stations,” in 2010 International Conference on Power System Technology, 2010, pp. 24–28.
26. Zhang Y., Beaudin M., Taheri R., Zareipour H., Wood D. “Day-Ahead Power Output Forecasting for Small-Scale Solar Photovoltaic Electricity Generators,” IEEE Trans. Smart Grid, pp. 1–1, 2015.
27. Marquez R., Coimbra C.F.M. “Forecasting of global and direct solar irradiance using stochastic learning methods, ground experiments and the NWS database,” Sol. Energy, vol. 85, no. 5, pp. 746–756, May 2011.

28. Stefferud K., Kleissl J., Schoene J. “Solar forecasting and variability analyses using sky camera cloud detection & motion vectors,” in Power and Energy Society General Meeting, 2012 IEEE,2012, pp. 1–6.
29. Chupong C., Plangklang B. “Forecasting power output of PV grid connected system in Thailand without using solar radiation measurement,” Energy Procedia, vol. 9, pp. 230–237, 2011.
30. Chen C., Duan S., Cai T., Liu B. “Online 24-h solar power forecasting based on weather type classification using artificial neural network,” Sol. Energy, vol. 85, no. 11, pp. 2856–2870, Nov. 2011.
31. Singh V.P., Vaibhav K., Chaturvedi D.K. “Solar power forecasting modeling using soft computing approach,” in Engineering (NUiCONE), 2012 Nirma University International Conference on,2012, pp. 1–5.
32. Diagne H.M., David M., Lauret P., and Boland J. “Solar irradiation forecasting: state-of-the-art and proposition for future developments for small-scale insular grids,” American Solar Energy Society, 2012.
33. “Area Solar Radiation—Help | ArcGIS for Desktop”, Desktop.arcgis.com, 2017. [Online]. Available: http://desktop.arcgis.com/en/arcmap/10.3/tools/spatial-analyst-toolbox/area-solar-radiation.htm. [Accessed: 12- Oct- 2017].
34. “Points Solar Radiation—Help | ArcGIS for Desktop”, Desktop.arcgis.com, 2017. [Online]. Available: http://desktop.arcgis.com/en/arcmap/10.3/tools/spatial-analyst-toolbox/points-solar-radiation.htm. [Accessed: 12- Oct- 2017].
35. “Solar Radiation Graphics—Help | ArcGIS for Desktop”, Desktop.arcgis.com, 2017. [Online]. Available: http://desktop.arcgis.com/en/arcmap/10.3/tools/spatial-analyst-toolbox/solar-radiation-graphics.htm. [Accessed: 12- Oct- 2017].
36. “Meteonorm: Irradiation data forevery place on Earth”, Meteonorm.com, 2017. [Online]. Available: http://www.meteonorm.com/. [Accessed: 12- Oct- 2017].
37. “JRC's Directorate C: Energy, Transport and Climate - PVGIS - European Commission”, Re.jrc.ec.europa.eu, 2017. [Online]. Available: http://re.jrc.ec.europa.eu/pvgis/. [Accessed: 12- Oct- 2017].
38. “Surface meteorology and Solar Energy”, Eosweb.larc.nasa.gov, 2017. [Online]. Available: https://eosweb.larc.nasa.gov/sse/. [Accessed: 12- Oct- 2017].
39. Lam J., Tang H., Li D. "Seasonal variations in residential and commercial sector electricity consumption in Hong Kong", Energy, vol. 33, no. 3, pp. 513-523, 2008.

Information Security Ensuring of the National Army Computer Networks

Sîrbu Corina, Sîrbu Cristina

Armed Forces Military Academy „Alexandru cel Bun”
23, Haltei Str, or. Chişinău, MD-2017, Republica Moldova
Tel: 37368705210, e-mail: corinasirbu2016@gmail.com

ABSTRACT

he development of society implies the need to build up the information society and the rapid development of modern information and communication technologies, which in turn has a major impact on the social environment, causing essential changes in the cultural, economic and political framework, but also on the life of the military environment. Thus, free access to information and communication technology is one of the conditions for the good functioning of the defense mechanism of the Republic of Moldova, as well as of the modern society.The security of computer systems and networks is a fundamental element for the functioning of the National Army's network of the Republic of Moldova, while allowing it to be transformed from an academic research project into a basic infrastructure of a modern army. Addiction to information technologies has created new categories of vulnerabilities for other components of social infrastructure, and an attack on the Moldovan National Army's IT network will create not only national insecurity but will also have implications for other critical infrastructure (transport, , ect.). Despite some advances in IT security, the vast majority of security-based technology-based solutions have proven to be ineffective, gradually realizing that security in virtual space is essentially a human problem. Such security practices have begun to find their transposition in the military.

Key words: information, communication, technology networks, security, policy infrastructure

1. INTRODUCTION

Information society is a new form of more civilized civilization in which equal and universal access to information, in conjunction with a developed information and communication infrastructure, contributes to sustainable social and economic development, poverty reduction, quality improvement life, integration into the European Union [1]. In the unique global information space, an informational geostrategic confrontation between the great powers was manifested to achieve superiority in the world information space. With the development and increase of the complexity of means, methods and forms of automation of information processing, society's dependence on the security of the information technologies used, which sometimes depends on the well-being and sometimes the lives of many people, [2]

In the previous decade in the information society, there was no formal approach to analyzing requirements for an information system, but programmer specialists simply built the "replica" software of an already existing information system. Gradually, "professional" approaches have evolved, with today's engineering methodologies for designing and building computerized information systems, which are also implemented within the national army where an appropriate level of security is required. The principles underpinning the security of a communications network are expressed in the form of a set of rules and practices, with particular stringency in the structures of force, in the so-called network security policy.

The security policy applies to everyone who in one way or another has access to network resources at any level, starting from the physical one and for whatever purpose (use, administration, maintenance, fraud, attack) of a coherent and complete model of a particular type of activity. The security policy is expressed in the form of a document that includes: the reasons and objectives for its implementation, the competent authority approving it, authors, references, date of preparation, procedures, compatibility measures, consequences of non-application. Unfortunately, there is no 100% secure security system, but defining a security policy is trying to find the best way to avoid the risks to the communications network. Security for an information system can be seen as having multiple layers representing the security levels that surround the subject to be protected. Each level isolates the subject and makes it more difficult to access in a way other than the one in which it was predicted.

Increasing company computerization leads to increased vulnerability. Consequently, ensuring the security of information systems and networks becomes a major concern of all actors involved, especially at the military level where the responsibility for the development and implementation of coherent policies in the field is concentrated. Thus, it is evident the necessity of developing the network security culture of the users of information and communication systems, often insufficiently informed about the potential risks, but also with the solutions for countering them.

The widespread knowledge of the risks and threats to the security of information technology, as well as their prevention and countermeasures, requires effective communication and cooperation among the specific actors in this field.

One important aspect to note is that the information system can only be protected in an IP network when all of the above listed parameters are respected and the security measures are applied on time and without the use of methods other than those required by the system network security.

2. GENERAL PARAMETERS OF THE PROTECTED SYSTEMS OF INFORMATION NETWORKS

The establishment of the informational age is now one of the greatest technical and scientific achievements, having a positive impact on all aspects of the contemporary society. At present, the work of most organizations depends 65% on their own computer system [3]. However, the development and broad implementation of information technologies has generated a number of issues related to ensuring the integrity, confidentiality and availability of information on electronic support.

The information security issue is becoming more acute as more and more sophisticated methods of attacking information are being invented and implemented.

The value of physical equipment is often much less than the value of the data contained. Loss of important national or organization data to competitors or offenders can be very costly. This type of loss can cause a lack of trust in the organization and the dismissal of security personnel. To protect the data, there are several security methods that can be implemented.

Password protection. Password protection can prevent unauthorized access to content. Attackers can gain access to unprotected data from PCs. All PCs should be password protected. 2 password protection levels are recommended:

BIOS - prevents BIOS settings from changing without entering the appropriate password.

Authentication - Prevents unauthorized access to the network.

Network Authentication allows methods for registering network activities as well as enabling or prohibiting access to resources. This determines which resources are being accessed. Normally, the system administrator defines a name convention for user names when deploying network authentication. A common example for a username is the first name followed by the last name. It is recommended to maintain a simple name convention that employees can easily remember. When assigning passwords, security levels must be comparable to the required protection. A good security policy must be strictly implemented and must include, but not be limited to, the following rules:

- ✓ Passwords should expire after a certain amount of time.
- ✓ Passwords should be a combination of letters and numbers so they can not be broken easily.
- ✓ Password standards should prohibit users from writing passwords and leaving them unprotected by visitors' eyes.
- ✓ Rules on password expiration and account lockdown should be defined. Account lock rules apply when an unsuccessful attempt was made to access the system or when a specific change in the system configuration was detected.

To simplify the security management system, a good way is to introduce users into groups and then assign groups some resources. This method ensures that users' rights to access resources on a network are changed only by moving them across groups. This is a useful method when it is necessary to create temporary accounts for visitors or consultants, who can easily limit their access to resources.

Encrypting data. Encryption of data uses codes and ciphers. Traffic between resources and network computers can be protected by attackers who monitor or record transactions by implementing encryption. It is very unlikely that he can decipher captured data in a timely manner for use. Virtual Private Networks (VPNs) use encryption to protect data. A VPN connection allows a remote user to safely access network resources as if they were physically linked to that network.

Port protection. Any communication that uses TCP / IP has a port number associated with it. HTTPS, for example, uses port 443 by default. A firewall is a way to protect an intrusion PC through ports. The user can control the type of data sent to a PC by selecting which ports are open and which are secured. Data transferred to a network is called traffic.

Backup of data. The procedures for making backups of data should be included in a security plan. Data may be lost or damaged in circumstances such as theft, equipment errors or disasters such as fire or floods. Data Backup is one of the most effective ways to protect against data loss.

Passwords. The use of secure, encrypted login information for computers with network access should be the least necessary in any organization. Malicious software monitors the network and can record passwords in clear text. If passwords are encrypted, attackers should decrypt encryption to learn passwords.

Authentication and review. Authentication and event review should be enabled to monitor network activity. The network administrator revises the event authentication file to investigate network access by unauthorized users.

Computer equipment and data can be secured using overlapping protection techniques to prevent unauthorized access to sensitive data. An example of overlap protection is the use of two different techniques to protect a good. When referring to a security program, the cost of implementation must be balanced by the amount of information or equipment to be protected.

Physical security. Use hardware-based hardware hardware to prevent security and information loss or equipment loss.

The security policy should specify the level of security required for the organization. Biometric devices, which measure physical information about a user, are ideal for use in high security areas. However, for smaller organizations, this type of solution would be too expensive.

Data security. You can protect data using data security devices to authenticate employees' access. Two factor identification is a method to increase security. Employees must use both a password and a data security device similar to those listed here to access data:

Smart card - A device that has the ability to store data safely. Internal memory is a built-in chip in an integrated circuit that connects to a reader, either directly or through a wireless connection. Smart cards are used by many applications around the world, such as secure identity cards, online authentication devices, and online credit cards.

Key Fob Security - A small device that resembles an ornament on the key ring. It has a small radio system that establishes communication with the computer over a small radius. The fob is pretty small, so most people attach it to the ring ring. The computer must capture the signal from the key fob before accepting a username and a password.

Biometric device - Measures the physical characteristics of the user, such as fingerprints or iris pattern. The user is given access if these features match those in the database and the correct authentication information is provided.

The security level the customer needs, determines the devices selected to keep the information and equipment safe.

The principles underpinning the security of a communications network are expressed, in the form of a set of rules and practices, in the so-called security policy.

First of all, the needs of each category of users with regard to network resources and access rights, whether inside or outside the network, using the wired structure or wireless access to the network, must be established. It also needs to be established which users really need access to the public Internet. All these aspects are dealt with in the access policy.

The criteria for setting up user groups, the right to have a network access account, the conditions for activating and deactivating accounts, administrators are the network accounts policy [3].

Connecting to the Internet and to the public network in general is a breach in the security of any network because attacks from outside the network act here. Clear principles are needed to protect the interfaces between the public and private networks. The principles under which Internet access and

Internet rights are protected are made up of the Internet-Acceptable Use Policy (I-AUP). Physical and logical access to different network communication equipment must be restricted to their importance in the proper functioning of the network. Measures must be taken to prevent unauthorized access attempts.

Using the login-based and password-based authentication method involves applying passwords for password acceptance, management, and password change policies.

Network access rights must be differentiated in terms of access to and access to documents (reading, writing, editing or deleting). Security policy establishes user rights on access to information and files in general, the strategy to be followed to ensure compliance, security compliance by all users (for example, privacy clauses in contracts signed by users). All these aspects represent the so-called proper use policy of network resources.

The wording of a network security policy must be made clear, with as many details as possible so that different interpretations do not appear. Knowing in detail all the equipment connecting to the network and the guarantees offered by each user is the premise of fair decisions about the privileges or restrictions that are required in each case (connection policy). The denial of network access for those entities for which there is evidence of intent to attack by monitoring traffic is a measure of force majeure necessary to keep the network operating safely.

All default settings must be changed from the moment the equipment is put into operation, and never have to return to it. Periodically, the network equipment's configuration needs to be reviewed to determine whether it meets network security needs at a given time, including passwords, access control lists, MAC addresses, encryption keys.

Encryption of information is required as the ultimate measure of transmission secrecy, when an intruder manages to download packets from the private network. Encryption is also a safety measure with regard to the secrecy of special information that can be attacked by people outside and within the network. The principles of information security are included in the information protection policy.

Specific security policies can be set for each network service (email, file transfer, network user information, etc.). Security rules may be binding or optional, resulting in several categories of security provisions:

The mandatory provisions resulting from agreements, regulations and laws, expressed in detail, with as many specific elements, depending on the field of use, are designed to provide security and trust in a communications network or a particular entity (server, service, program, etc.).

The recommended, so non-binding, provisions are motivated by the serious consequences of not applying them. For best network security, they should be considered as mandatory, although the cost of implementing them is generally high. For example, it is not required to run antivirus programs or install any security patches from operating systems. All of this involves some additional costs (price, system memory, processing time), but in a network, each corresponding insecure node can be an access gate for attackers.

Informative provisions have the role of alerting users to the existence of vulnerabilities (for example, not updating virus lists for antivirus programs), the risks and consequences of security breaches of systems and networks [5].

The security policy is expressed in the form of a document that includes: the reasons and objectives for its implementation, the competent authority approving it, authors, references, date of preparation, procedures, compatibility measures, consequences of non-application. Unfortunately, there is no 100% secure security system, but defining a security policy is trying to find the best way to avoid the risks to the communications network.

European security policy policy.

The Internet is essentially interested in both large and small state institutions. Basically, there are no organizations in a country with at least average growth that does not have webpages that provide information about the services and products offered. Consumers and manufacturers can also communicate instantly through the Net, which gives them the possibility of sharing information and very cheap communications. And yet, they have not "thrown" yet to do large-scale business or administration over the Internet. Why is this restraint? The most commonly cited reasons are related to the security of on-line transactions. Concerns about network and information security have increased in proportion to the increase in network users and the value of transactions. Security has reached a critical point, representing an essential requirement for important businesses and the functioning of an organization's entire system. The combination of several factors has made information and communication security one of the main points on the agenda of the European Union's policy:

- ✓ Governments have realized the dependence of their financial resources and citizens on the proper functioning of their communications networks and have begun to review their security arrangements.
- ✓ The Internet has created a global connection, connecting millions of networks, large and small, millions of personal computers and other devices, such as mobile phones; this significantly reduced the cost of accessing information in case of remote attacks.

Numerous viruses are reported, causing large losses by destroying information and not granting access to networks. These security issues are not specific to a particular country, but a phenomenon that has rapidly spread across EU countries.

While security has become an essential issue for policy-makers, finding an adequate response has become a complex task. Just a few years ago, network security was a state monopoly problem that provided specialized services based on public networks, particularly for telephone networks. The security of IT systems was specific to large organizations and was focused on controlling access to resources. These things have changed considerably due to developments in the context of an enlarged market, including liberalization, convergence and globalization.

Networks are now mainly privately owned and managed by private organizations. Communication services are offered on the basis of competitiveness, security being part of the market offer. However, many customers remain ignorant of security risks when they connect to a network and make decisions based on incomplete information.

3. SCIENTIFIC RULES AND MEASURES IN SCIENCE

Security rules and measures are implemented through the information security policy set out in the SCIAN Regulation Information Management Regulation, which consists of a set of (mandatory) rules and practices that govern how an institution uses, manages, protects and distributes its own sensitive information to be protected. [8]

3.1 Acceptable Use Rules of SCIAN

Use of SCIAN is only in the interest of service. In order to prevent the intentional or unintentional negative influence on the working capacity of the SCIAN components, the likelihood of leakage of information reflected on the screen or in textual form, the access of the visitors to the work rooms is limited. The danger of unauthorized access to SCIAN's information resources increases if the visitor possesses the necessary level of knowledge in the field of information technologies.

Until the beginning of the work, the user is required to carefully examine the SPAD in the presence of unanswered access signs: obvious signs include: destroying the seal, removing the computer block cover, disconnecting the cables between the blocks, etc.; secondary signs include: the presence of external bearers in the base blocks of the computer, the connection of the computer to other communication sources, etc.

With the user suspecting unanswered access, he is required to immediately notify the AS. Until the arrival of the ISS and the establishment of the reasons, it is forbidden to use SPAD. Before entering the user data and password, the Security Memorator will appear on the screen informing the user of the requirements and obligations to connect to SCIAN. If the need to leave the workplace occurs within 10 minutes, the user has to block SPAD (using the Ctrl-Alt-Del buttons and selecting Lock Computer under "Windows Security" mode). In other cases, the user must disconnect SPAD. At the same time, each SPAD connected to SCIAN is automatically protected by the Screen Saver mode, protected by the password that automatically enters 10 minutes from inactivity.

The SCIAN allows the use of only external information carriers registered by the AS. Responsibility for complying with information security measures when working with external information bearers is assigned to the user who uses them. It is necessary to take into account that the term of validity of external information carriers is limited and their very existence poses a potential threat to information security. In addition, incorrect use and storage radically reduces their shelf life and increases the likelihood of data loss. In this connection, it is recommended to use Common Access Maps created in existing or structured networks. External information carriers are kept in special places, in enclosed boxes, metal safes, and it is forbidden to keep external service bosses with personal information. Until the work with external information bearers begins, the user will be convinced of the lack of viruses or other malicious programs. They will not send by e-mail attachments with passwords or data related to SCIAN access systems, as well as bank card data; They will not open messages and will not launch e-mail attachments from an unknown source (as well as dubious sources) They will not access messages announcing winning prizes or asking for personal data, money, etc., they will be treated with suspicion, because most of the time there are phishing attempts.

In the SCIAN, for the protection of transmitted information, Public Key Infrastructure (PKI) public key certificates are used to ensure the authenticity and security of electronic mail, electronic documents and information that are used through electronic cards and card reader. Responsibility for the use, integrity and retention of electronic cards and readers is assigned to the user who uses them and afterwards has been upgraded according to the books of evidence. Upon completion of the work, the devices are kept in special places, in closed boxes, metal safes, and it is forbidden to remove it from the room where SPAD is located to which it is connected without AS permission. Users are required to notify the AS if any problem / breach is noticed in the SCIAN security system and any possible misuse or breach of applicable directive documents.

3.2 SCIAN Monitoring Rules

SCIAN monitoring will be done in such a way that it is possible to detect in a timely manner the computer attacks and the breaches of the Directive documents related to information security. as well as authorized personnel at the Center for Communications and Computer Science of the General Staff for the detection of violations. Any breach of compliance with the Directive documents related to the provision of information security in SCIAN will be documented for the purpose of investigations.

4. INFORMATION SAFETY MODES IN THE COMMUNICATION NETWORKS

The security model for an information system can be seen as having several layers representing the security levels that surround the subject to be protected. Each level isolates the subject and makes it more difficult to access in a way other than the one in which it was predicted.

Physical security is the external level of the security model, and generally consists of the under-key protection of computer equipment in an office or other premises and the provision of security and access control. This physical security deserves special consideration. Another issue of physical security is the safe keeping of the data and software rescue media. Local networks are a great help in this case, and backups can be made over the network on a single machine that can be more easily secured.

Another important problem in the physical security of an information system is simply the evasion of equipment. In addition, other logical security measures (passwords, etc.) become insignificant in the case of unauthorized physical access to equipment. In a system where the processing is distributed, the first physical security measure to be taken into consideration is to prevent access to the equipment.

Logical security consists of those logical (software) methods that ensure control of access to system resources and services. It also has several levels divided into two large groups: Access Security Levels (SAs) and Service Security Levels (SS).

Access Security (SA) includes:

System Access (AS), which is responsible for determining whether and when the network is accessible to users and under what conditions.

Account access (AC) with valid name and password.

Access rights (YES) to files, services, user or group resources.

Service Security (SS), which is under SA, controls access to system services such as queuing, disk I / O, and server management. From this level are:

Service Control (CS) alerts and reports service status;

service rights (DS) how to use a given service.

Access to a perfect security system must be done through these security levels from top to bottom.The security model centered on information or on the subject has several layers that represent security levels. They provide protection for the subject to be secured. Each level isolates the subject and makes it more difficult to access in a way other than the one it was intended to provide and provides extra security with secret information.

Security levels in this model have the following meanings:
SF - Physical security;
SLA - Logical Security of Access;
SLS - Logical Security of Services;
SI - Secretization of information;
II - Integrity of information.

A functional security system must ensure access to resources by verifying access rights on all these levels without the possibility of avoiding them.

The layered security model is best suited to a particular network node. But communication processes involve two or more network nodes and the transmission paths between them. Therefore, security must be tracked at each node of the network, but also on every path or flow of the network.

To model security services in computer systems, the distributed "tree" security model is also used. This model should be applied if distributed resources are accessed across multiple servers on the network. Information is transferred from the source node to the destination node through multiple network nodes and various physical, "wireless or wireless" communication paths. The degree of security offered to a network data transfer process will be given by the weakest segment of the transfer path (node or communication channel). Therefore, to reduce network security risks, it is necessary to secure all segments involved in the communication process to the security level desired for each message.

The client is represented as the root node in the above diagram, the servers as nodes-terminals, and the network communication equipments as intermediate nodes. In each node the first security centered model of the subject can be applied. Connections between the nodes are physical, radio or wired communication paths. In the case of networks with redundant "mesh" topology, it is difficult to identify the "tree" of communication but it can be imposed by strict routing decisions on a certain path in the network.

The arborescent security model is particularly useful for analyzing distributed network attacks from and to multiple nodes to make it more difficult to identify the attacker and increase attack efficiency.

Monitoring of communication processes and security events, along with their classification and hierarchy on multiple degrees of risk on the basis of fuzzy systems, allows the establishment of an optimal security strategy and the application of effective countermeasures using the security tree model.

5.CONCLUSION

Threats to network security have become commonplace in our society. They are becoming more frequent, more diverse and complex, based on the applied technological methods. Ignoring them has become impossible because information has become an absolute and vital benefit, and confrontation in the virtual space with insecurity leads to considerable economic and physical damage.

For the successful countering of threats it is necessary to focus on the following:

- Establishing a conceptual, institutional framework (creating a national information security system, drafting legislation, etc.);
- development of the national program to develop the potential of the national army network (capabilities for preventing, detecting and counteracting attacks on the network, creating specialized structures, raising the level of protection, developing the production of profile products);
- strengthening the information security culture (informing the population, adequate training of managers and technical staff);
- Improving international cooperation (at the level of normative acts, exchange of experience, collective protection against large-scale attacks).

All staff are responsible for how to use the national military network; each user is directly responsible for actions that may affect SCIAN security. Users are non-discriminatory in reporting any suspicion or confirmation of violation of the Regulation on Information Security and the Use of Resources of the National Communi- cations and Computing System.

There is no assurance of personal data privacy or access to information using protocols such as, but not limited to, e-mail, web browsing, phone conversations, fax transmissions and other electronic conversation tools. The use of these electronic communication tools can be monitored for investigations or for the settlement of complaints under the laws in force. Any information used in SCIAN must be kept confidential and safe by users. The fact that information can be stored electronically does not change the obligation to keep it confidential and secure; the type of information or even the information itself is the basis for determining the degree of security required.

Physical and logical access to different network communication equipment must be restricted to their importance in the proper functioning of the network. Measures must be taken to prevent unauthorized access attempts. The use of the user-name and password authentication method involves the application of passwords for accepting, managing, and changing passwords within the password management policy. Network access rights must be differentiated in terms of access to and access to documents.

REFERENCES

1.The National Story of Building the Information Society "Moldova electronica". Government Decision of the Republic of Moldova no. 255 of 09.03.2005.
2. Cisco 2014. Annual Security Report, 80p .
3. http://ro.scribd.com/doc/99927620/Security Information.
4. Silviu Marian Banila, ANALYSIS: The most important security breaches in the recent history. https://ro.stiri.yahoo.com/analiza-cele-mai-importantebrese-securitate-din-istoria-091834763.html.
5. Drăgănescu M. Information Society and Knowledge. The vectors of the knowledge society, Bucharest, Romanian Academy, 95 p .
6. Information security in the context of the globalization process, accessed on http://biblioteca-digitala-online.blogspot.com.
7. Regulation on ensuring the security of information and use of the resources of the National Army communications and information system. Order of the Minister of Defense no.114 of March 12, 2015.
8. Instruction on Shipment of Management Documents through the National Army Communications and Information System (SCIAN). Order of the Minister of Defense no.115 of 12.03.2015.

AUTHOR INDEX