ISSN 2522-9052

Національний технічний університет
“Харківський політехнічний інститут”

National Technical University
“Kharkiv Polytechnic Institute”

Сучасні інформаційні системи

Advanced Information Systems

Том 1, № 1

Volume 1, No. 1

Щоквартальний науково-технічний журнал

Заснований у березні 2015 року

У журналі публікуються результати досліджень з експлуатації та розробки сучасних інформаційних систем у різних проблемних галузях. Журнал призначений для наукових працівників, викладачів, докторантів, аспірантів, а також студентів старших курсів відповідних спеціальностей.

Засновник і видавець:
Національний технічний університет
“Харківський політехнічний інститут”

Кафедра “Обчислювальна техніка та програмування”, вул. Кирпичова, 2, 61002, м. Харків, Україна

Телефон:
+38 (057) 707-61-65

E-mail редколегії:
kuchuk56@ukr.net

Інформаційний сайт:
www.journals.uran.ua

Quarterly scientific and technical journal

Founded in March 2015

The journal publishes the research study from the usage and development of advanced information systems in various problem areas. The journal is intended for researchers, lecturers, doctoral students, postgraduate students, and for senior students of the corresponding specialties.

Founder and publisher:
National Technical University
"Kharkiv Polytechnic Institute"

Department of Computer Science and Programming, 61002, Ukraine, Kharkiv, Kyrpychova str., 2

Phone:
+38 (057) 707-61-65

E-mail of the editorial board:
kuchuk56@ukr.net

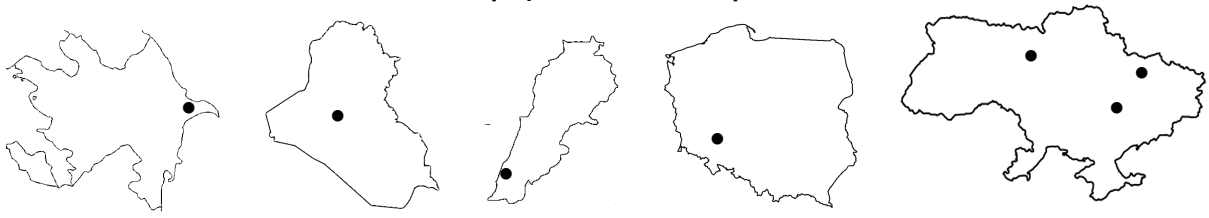
Information site:
www.journals.uran.ua

Затверджений до друку Вченою Радою Національного технічного університету “Харківський політехнічний інститут” (протокол від 07 липня 2017 року № 6).

Свідоцтво про державну реєстрацію КВ № 22522-12422Р від 13.01.2017 р.

Харків • 2017

Географія статей номера



Азербайджан *Ірак* *Ліван* *Польща* *Україна*

ЗМІСТ

TABLE OF CONTENTS

Вступне слово

головного редактора журналу
лауреата премії НАН України
імені С.О. Лебедєва,
член-кореспондента
Національної академії наук України,
доктора технічних наук, професора,
ректора
Національного технічного університету
“Харківський політехнічний інститут”
Євгена Івановича СОКОЛА

Шановні читачі (колеги)!

Сьогодні ми є свідками стрімкого розвитку інформаційних технологій і систем, повсюдного їх використання практично у всіх сферах життєдіяльності сучасного суспільства, підвищення інтересу до цієї тематики практично всіх фахівців різних галузей і напрямків. Все це стало можливим завдяки новим досягненням наукової думки, революційним ідеям наших фахівців, інтересу з боку IT-індустрії. Ці досягнення реалізуються в принципово нових технічних, технологічних і математичних підходах, які потребують висококваліфікованих фахівців в різних галузях IT-напрямків.

В таких умовах для всіх нас особливо важливо мати можливість донести свою точку зору до громадськості, обґрунтувати власну позицію, взяти участь в дискусії, ознайомитися з іншими думками, і найголовніше – зробити це в доступному середовищі.

Упевнений, що журнал «Сучасні інформаційні системи» стане відкритою трибуною як для відомих вчених, так і для представників молодих поколінь науковців.

Побажаємо нашому виданню знайти свою вагому нішу в науково-технічній періодиці нашої країни, щоб відбір тем, їх діапазон, проблематика публікацій були багатогранними і різнопланові, на піку актуальності і читацького інтересу, а всім авторам журналу – невичерпного творчого натхнення і успіхів.

Introduction

Chief editor of the journal
Laureate of NAS of Ukraine
named after S.O. Lebedev
Corresponding Member
of the National Academy of Sciences of
Ukraine, Doctor of Technical Sciences,
Professor, Rector
of National Technical University
"Kharkiv Polytechnic Institute"
Yevgen Ivanovych SOKOL

Dear readers (colleagues)!

Today, we are witnessing the rapid development of information technologies and systems, their widespread use in virtually all in modern society, interest in this subject in practically all professionals of various industries and areas. All of this became possible thanks to the new achievements of scientific thought, the revolutionary ideas of our specialists, interest from the IT industry.

These achievements are realized in fundamentally new technical, technological and mathematical approaches that require highly skilled specialists in various fields of IT.

In such circumstances, it is especially important for all of us to have the opportunity to convey our point of view to the public, to justify our own position, to participate in the discussion, to get acquainted with other thoughts, and most importantly - to do so in an accessible environment.

I am convinced that the journal "Advanced Information Systems" will become an open platform for both prominent scientists and representatives of younger generations of scholars.

I wish to find a significant niche in the scientific and technical publications, that the selection of themes, their range, issues of publications were multifaceted and diverse, at the peak of relevance and readership interest, and to all authors of the journal – inexhaustible creative inspiration and success.

Modeling of information systems

UDC 623.451 **doi: 10.20998/2522-9052.2017.1.01**

A. Kovtun, V. Tabunenko

National Academy of the National Guard of Ukraine, Kharkiv, Ukraine

MODELING OF THE HIGH-SPEED PUNCHING DRUMMER BARRIERSAS A SET OF HOLLOW CYLINDERS

Were analyzed the characteristics of damaging elements of artillery systems and small arms. Were analyzed the characteristics and structures of personal Armor protection. Modern protection has layered structure. The main blow of high speed sub munitions takes the hard plate. They can be made of metal or high-strength double-layer panels. At a meeting with the panel the toe of bullet was destroyed. As a result of growing area of interaction between the bullet and the panel, there is a deflection and uncoupling ceramic bullet while destruction. When you hit the drummer in the obstacle created several types of wave perturbations that propagate with different velocities. These effects cause is a complex stress state structure, whose intensity decreases rapidly with time. **The aim of the article** is to investigate the interaction of high-striker with a protective barrier in the form of a set of hollow cylinders. The **methods** that are used: Improving personal armor protection can be achieved by applying the optimum combination of new materials and advanced structural and circuit design. Character penetration drummer an obstacle may change if the obstacle is to imagine a structure that consists of a set of hollow cylinders. Considered the process of interaction, of high-speed impactor, with a protective barrier, in the form of a set of hollow cylinders. In contact with the surface layer drummer obstacles by having an expanded, drummer enters the hollow cylinder, which closely hugs the side surface of the impactor, creating resistance to motion. When moving drummer in the cylinder is converting kinetic energy into energy impactor cylinder and deformation work to overcome friction. Thus, the energy of drummer extinguished intermediate layer and redistributed to the power frame inner layer. following **results** are obtained. The proposed a model to determine the depth of penetration drummer an obstacle in the form of a set of hollow cylinders. There are results of the calculations. It is proposed to further improve the protection of personal Armor achieve by applying the optimum combination of new materials and advanced structural and circuit design.

Keywords: body armor, high-speed hammer, striking element, threat levels, protective barrier, plastic deformation, a hollow cylinder, penetrating power.

Formulation of the problem

Despite the rapid development of modern methods of warfare and the development of weapons based on new physical principles, armed with modern armies are improved traditional means of destruction. Therefore, urgent tasks are the development of modern means of personal body armor.

When conducting modern military operations there are different types of weapons and ammunition, each of which has its own set of characteristics (mass, shape, hardness, speed, etc.), which complicates the solution of the problem of protection against them. The main striking elements are the following:

1) fragments of artillery and rockets, grenades, mines;

2) high-speed bullet;

3) low-velocity bullets.

Fragmental weapons can produce thousands of pieces of small sizes of various shapes, most of which has a mass of about 1 gram. Fragments have an initial speed of 1000-2000 m/s, but with an irregular shape, quickly losing it. They are a source of injury in a large area.

High-speed bullets have greater penetration than fragments [1]. On penetration bullet affects its structure. Bullet with a round toe, the core and the shell of a soft alloy more amenable to deformation in a collision with a protective barrier than steel shards. However, elongated shape still increases its penetration. Heavier bullets with low-speed weighing up to 15 grams of reaching speeds of up to 400 meter per second. Therefore, they have almost the same level of penetration into the protective barrier that of high-speed low mass fragments. With this in mind, personal body armor must meet various requirements for protective characteristics corresponding to different levels of threat. In turn, the threat level is determined by the nature of the fighting, weapons and views used in accordance with this dictates the need for the degree of security of the personnel.

It is known that the armor penetration [2] of bullets of small arms is defined as the maximum thickness for penetration of armor steel, and on the ability of penetration through the protective clothing of various classes of protection while maintaining after-penetration effect action sufficient to guarantee the decommissioning of the enemy. In various countries the necessary residual energy of a bullet or bullet fragments after the breaking of protective clothing is estimated between 80J and more. In general, it is known that, as used in armor-piercing bullets sorts cores after breaking barriers have a sufficient lethal effect caliber core only at least 7.6 mm, and its residual rate of at least 200 meter per second.

Modern protective equipment (Fig. 1) has a layered structure [3]. The basic personal protective equipment material is resistant to high-energy shock fabric fibers made of synthetic, special composition and structure. This fabric is used in the form of a package of several layers, delays and low-speed bullet splinters. To keep the high-speed sub munitions used rigid plate. Furthermore, for cushioning, the cushion layer is applied.

The main hit of high submunitions perceives rigid plate. They can be made of high strength metal or double-layer panels. Upon impact with the panel, bullet sock destroyed. This increases the area of interaction of the bullet and the panel comes deflection and splitting ceramics while fracture the bullet.

Fig. 1. Types of body armor

In the scientific literature, most attention is paid to the definition of required thickness barrier, depending on the impact velocity [4–7]. It is noted that the reaction of the hammer with the barrier with low speed inertial forces are negligible compared to the strength characteristics of the elements. Deformation covers the entire structure and has is mainly elastic character. At medium speeds the hit force of inertia can be impact comparable with the static penetration resistance, deformation is local and is characterized by high values of the plastic deformation and its speed. At high speeds, the hit becomes more prevalent inertial forces within the material interacting elements close to hydrodynamic.

Different researchers have produced a variety of empirical formulas which take into account the basic parameters of the impact [4, 5] (formula by Petri, Nobile, Saatchi and Kruppov, Havre, Thompson, Davies, Berezanskaya and ets.), based on experimental data obtained during shelling of armor plates at different conditions, which narrows their field of application.

However, most studies have paid attention to the mechanical characteristics of materials, much less design parameters evaluated barriers. Common to the known studies is that the protective barrier provided in a plate (kit plate), while one of the components of firearms is a mechanical system consisting of a striker (bullet) and barrel (sheath).

Thus, these data suggest that the theory of the mechanical interaction of projectiles from obstacles [8] of various kinds has not received its completion, the processes occurring in hit interaction of elements of mechanical systems is not fully understood, and applied models and methods of calculation depend on the necessary the accuracy of the results, while not measured structural parameters barriers. It is suggested that further improvement of personal body armor can be achieved by applying the optimum combination of new materials and modern design-circuit design.

Processes occurring in the punching of barriers are very diverse and depend on many factors. The main ones are: the speed and direction of impact, size and shape of drummers, the design and manufacturing technology of protective equipment, the physical and mechanical properties of materials and drummers protective barriers.

The reliability of the forecast of the results of impact interaction drummer barrier rises comparing the results of the analytical and numerical modeling, and data field tests. A comprehensive experimental- design study features of the interaction of projectiles with targets is essential for a reliable forecast of the results of the interaction of the elements and can significantly improve the efficiency of development of constructive solutions. This research scheme (the study of the behavior of structural elements under real conditions of dynamic loading, numerical and experimental modeling) allows you to create a basis for the development and justification of recommendations for the rational design and selection of materials and their structural condition, to enhance the effectiveness of their use in designs.

The scientific basis for studying the process of breaking down barriers by high-speed strikers are theory of elasticity, ductility and strength of materials, theoretical framework for ensuring the survivability of personnel departments in the conduct of hostilities, the theory of reliability models, mathematical modeling, mathematical design of experiments.

The aim of the article is to investigate the interaction of high-striker with a protective barrier in the form of a set of hollow cylinders.

The Main material

The process of penetration of the striker in the traditional protection barrier which is integrates several physical mechanisms. In this case, there is a stage associated with apart of the target material and the stage of knockout plugs (scabbing).

When you hit striker on the barrier there are several types of perturbation waves traveling at different speeds. These disturbances cause design complex stress state, the intensity of which decreases rapidly in time.

The initial stage of penetration of the striker in the barrier [9, 10] is determined by the point in time during which the drummer penetrate the barrier at a depth of about two of it diameters. During this period, for the non-deformable drummer with conical warhead changes the character of the movement and the stress-strain state of the target material, and the penetration force reaches a steady state value other than efforts in the surface layers. (In the case of interaction between striker with a relatively strong barrier at the initial stage of an intensive deformation of the head of the striker and the formation of its new form).

After reaching a certain critical penetration depth of the crater size ceases stop change and starts to form the main channel of the cavity. The final stage of penetration

barrier is considered part of the process, which starts with the approach striker to the back surface of the barriers to a certain critical distance, and ends with the release of the striker obstructions. Achieving the specified distance associated with access to the back surface of the plastic zone, it causes a change in the stress-strain state of the interacting elements.

When approaching striker to the back surface of the barrier, there arises the tensile zone of radial and tangential stresses and σ_r and σ_φ as expanding conical funnel. As a result of these stresses in the material can be damaged or cracked. Further movement of striker leads to mechanical damage of the target material.

The nature of striker penetration into the target may change if the barrier will be a structure consisting of a set of hollow cylinders (Fig. 2).

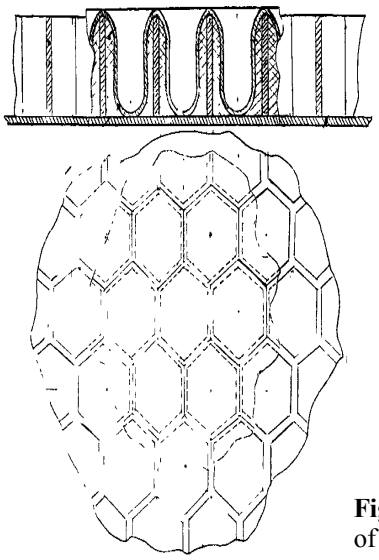


Fig. 2. The construction of the barriers

Structurally, the protective barrier of this type may comprise outer, intermediate and inner layers [11]. Wherein the outer layer is made as a set of interconnected hollow cylinder with a closed bottom and a top part which extending and made of materials possessing ductility property. The inner layer is a frame structure in the form of spatial lattice consisting of a plate connected to the placed perpendicular to the reinforcement ribs, the distance between which is greater than the outer diameter of the cylinder of the outer layer. The outer and inner layers are interconnected by means of an intermediate layer of adherently-elastic material. The construction of outer protective barrier layer can convert the kinetic energy of striker to the work by plastic deformation of the cylinder. Application of the inner layer as the power frame, allows striker to redistribute energy over a larger area. The use of an intermediate layer of adherently-elastic material can reduce the energy transmitted by drummer to inner layer of protective barriers.

Upon contact with striker outer barrier layer, by having the divergent upper part, the hammer falls in a hollow cylinder that fits tightly the lateral surface of the moving striker, which creates a resistance to its movement. When moving striker in the cylinder of the kinetic energy is converted into energy of striker cylinder and a deformation work to overcome the friction force. In this case, part of the energy striker is extinguished intermediate layer and redistributed on the frame structure of the inner layer.

Consider the process of interaction between the hammer (bullet) with thick-walled hollow cylinder (tube) (Fig. 3), using the elements of the theory of plastic deformation of thick-walled pipes which are under internal pressure pi created penetrated into the cylinder drummer. At the same time, ri - the inner radius of the cylinder, ro - the outer radius of the cylinder.

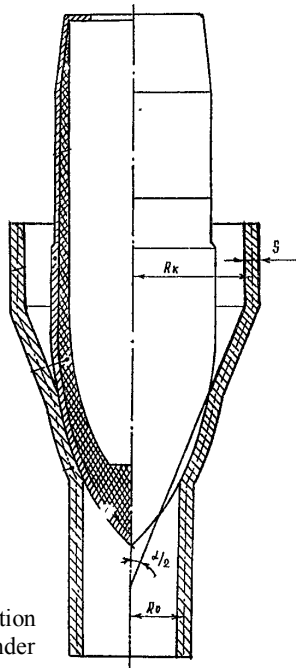


Fig. 3. Scheme of the interaction of the bullets with a hollow cylinder

Of the three principal stressesσ_θ, $\sigma_я$, σ_r, occurred at the same time in the cylinder design according to the results given in this article [12], the most important is the voltage σ_θ, and the smallest σ_r. In this case, the plasticity of the condition can be written as:

$$\sigma_\theta - \sigma_r = 2\,k, \qquad (1)$$

where $k = 0.5\,\sigma_t$ – the criterion of plasticity of Saint-Venant.

From the analysis of the expression for σ_θ in solving elastic problems for thick-walled pipes [12] that the greatest tension will be in the interior of the pipe. With increasing internal pressure p_v in the plastic state will go first inner layer. In order to determine the value p_v, where plastic deformations appear in the inner layer, substitute the plasticity condition (1) and the expression for σ_θ and σ_r, obtained by solving the plane problem of elasticity theory, denoting the internal pressure corresponding to the start of plastic deformation of p_t:

$$\frac{r_v^2 \cdot p_t}{r_n^2 - r_v^2} \cdot \left(r_n^2 / r_v^2 + 1 \right) + p_t = 2 \cdot k.$$

hereof

$$p_t = \frac{r_n^2 - r_v^2}{r_n^2} \cdot k.$$

Consider a case in which the internal pressure $p_v > p_t$. The internal portion of tube section will be in a plastic state, and external - in the elastic. The boundary between the plastic and elastic zones is a cylindrical surface of radius r_t. On the border of this layer is radial stresses σ_r, which is denoted by q. Thus, it is determined by the formulas [10] to the outer layer of the pipe with an inner radius ri, pressure q and an outer radius r_o of voltage σ_r and σ_θ :

$$\sigma_r = -\frac{r_t^2 \cdot q}{r_n^2 - r_t^2} \cdot \left(r_n^2 / r^2 - 1\right);$$

$$\sigma_\theta = \frac{r_t^2 \cdot q}{r_n^2 - r_t^2} \cdot \left(r_n^2 / r^2 + 1\right).$$

To determine these values, consider the inner layer of the pipe is a pipe under internal p_v and external p_n pressures. The inner radius r_v of the pipe and the outer r_t. This pipe is entirely in the plastic state. Therefore, in addition to her equilibrium differential equation:

$$\frac{\partial \sigma_r}{\partial r} + \frac{\sigma_r - \sigma_\theta}{r} = 0. \quad (2)$$

Have plasticity condition (1).

After substituting this condition in (2) we get:

$$\frac{\partial \sigma_r}{\partial r} = \frac{2k}{r}.$$

After integrating this equation we obtain:

$$\sigma_r = 2k \cdot (\ln r + C). \quad (3)$$

The integration constant C we find the condition that at $r = r_{vn}$, $\sigma_r = - p_v$, then $2k \cdot (\ln r_{vn} + C) = - p_v$, where

$$C = -(\ln r_{vn} + p_v / 2k).$$

After substituting the integrating for C (3)

$$\sigma_r = 2k \cdot \ln\left(r / r_B\right) - p_B. \quad (4)$$

From plasticity conditions

$$\sigma_\theta = 2k(\ln\left(r_t / r_v\right) + 1) - p_v. \quad (5)$$

Thus, for plastic (internal) stress area defined by the formulas (4, 5). At the boundary between the elastic and plastic zones, i.e. at $r = r_т$, voltage σ_r and σ_θ, defined by the formulas for the elastic (σ^y_r ,σ^y_θ) and plastic ($\sigma^п_r$,$\sigma^п_\theta$) zones should be the same, that is, to determine the unknown q and $r_т$ are the following conditions: when

$$r = r_т \sigma^п_r = - q, \quad \sigma^п_\theta = \sigma^y_\theta,$$

the first condition:

$$q = -(2k \ln\left(r_t / r_v\right) - p_{‰}),$$

from the second condition, we obtain:

$$2k \cdot \left(\ln\left(r_t / r_v\right) + 1\right) - p_v =$$

$$= \left(p_v - 2k \ln\left(r_t / r_v\right)\right) \cdot \left(r_n^{2,} + r_t^2\right) / \left(r_n^{2,} - r_t^2\right).$$

From whence

$$p_v = k \cdot \left(2 \ln\left(r_t / r_v\right) - r_t^2 / r_n^2 + 1\right).$$

If the plastic zone will occupy all the cross-section, the bearing capacity of thick-walled tube is exhausted. The value of the internal pressure limit is determined by the formula:

$$p_{пр.} = 2\, k \ln\left(r / r_v\right). \quad (6)$$

The force P acting on the annular element unit width of thick-walled pipes is determined by the expression:

$$P = 2\pi \, r \, p_{пр.}. \quad (7)$$

The force causing the tangential stresses in the cylinder, with the proviso that the plastic zone will occupy all of the cylinder section and carrying capacity is exhausted:

$$P = 2\pi \, r_k \, \delta \, \sigma_\Theta, \quad (8)$$

where r_k – final (after deformation) radius of the cylinder;

δ – the thickness of the cylinder.

The force pulling the striker within the cylinder defined by the formula:

$$P_1 = f_1 \cdot P, \quad (9)$$

where f_1 is effective coefficient of friction.

Drummer energy expended on overcoming the forces of friction and deformation of the cylinder:

$$E_\Sigma = \Delta E_{тр.} + \Delta E_{деф.}.$$

The path traveled by the striker inside the cylinder, by the formula:

$$E_\Sigma = P_1 \, h, \quad (10)$$

where we find h

$$h = \frac{E_\Sigma}{P_1}. \quad (11)$$

Determine the magnitude of the penetration depth of BSC-43 bullet weighing 7.9 g, and the initial speed of 715 meters per second with a steel core Kalashnikov (AKM) in a steel cylinder, provided that the plastic zone will occupy all of the cylinder section and carrying capacity is exhausted.

Substituting in the formula (6)–(11) the following parameters:

$r_k = 0{,}0038$ m;

$\delta = 0{,}01$ m;

$\sigma_\Theta = 1{,}22 \text{x} 10^9$ H/ m^2;

$f_1 = 1{,}2$; bullet energy

$E_\Sigma = 2019$ J.

As a result, the calculations we get: $h = 0{,}007$ m.

Results of field experiments confirm the fundamental possibility of stopping bullets barrier of a set of hollow cylinders (Fig. 4).

Calculation of breaking the plate thickness of the same material from the formula by Thomson gives the following result.

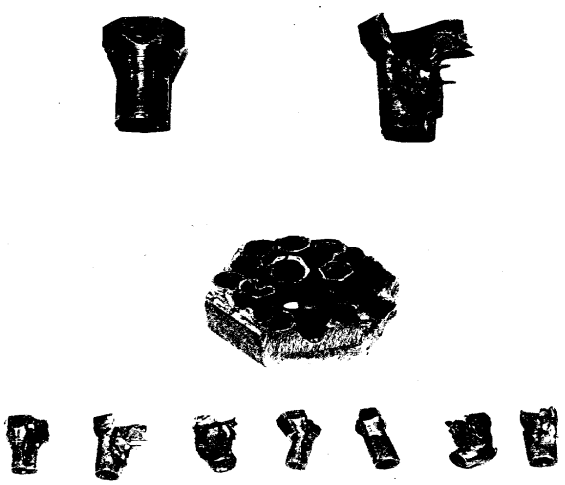


Fig. 4. Experimental results

The total energy absorbed by the plate during its plastic deformation during expansion hole is defined as follows:

$$E_{\Sigma} = \pi R^2 h \cdot \left[\sigma/2 + \rho \cdot uR/L\right],$$

where R – caliber of the bullets, m;

h – thickness of a punched layer barrier, m;

σ – limiting stress for the environment, MPa;

ρ – density of the fluid kg / m^3;

u – bullet speed, m/s;

L – length of the bullet head, m.

For steel barriers with parameters

σ = 1200 MPa; ρ = 7800 kg/m^3;

characteristics bullet

u = 715 m / s; R = 0.00762 m; L = 0.012 m,

the energy

$$E_{\Sigma} = 2019 \text{ J}$$

the thickness of the punched of barrier layer

$$h = 0{,}018 \text{ m}.$$

Dependence of thickness of the broken through layer of barrier of h on the thickness of cylinder δ, presented on a Fig. 5.

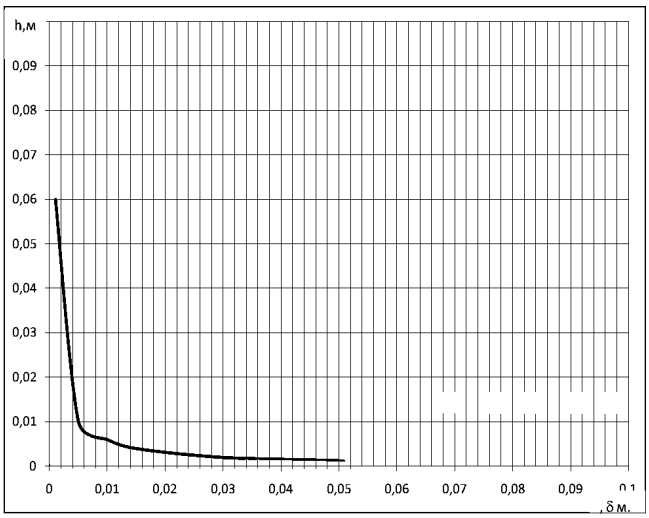


Fig. 5. Dependence of thickness of the broken through layer of barrier on the thickness of cylinder

Conclusions

1. Investigated the process of the interaction of high-drummer (bullet) with a protective barrier in the form of a set of hollow cylinders.

2. Propose a model for determining the depth of penetration of high-speed drummer into the hollow cylinder.

3. The calculation of the depth of penetration of bullets of BSC-43 weight of 7.9 grams and an initial velocity of 715 m/s with steel core from a Kalashnikov (AKM) in a steel cylinder, provided that the plastic zone will occupy all the section and bearing capacity of the cylinder is exhausted.

3. The calculation of the depth of penetration of the BSC-43 bullets from a Kalashnikov (AKM) in a plate of the same material from the formula Thomson.

4. Further studies are related to taking into account the violation of the structural integrity of the bullet with steel core and a lead jacket, the possibility of which must be considered when designing the protective armor constructions.

REFERENCES

1. Raygorodetskiy, A. Sverkhskorostnyye strelkovyye boyepripasy [Super-speed sagittaric ammunition], available at: http://www.dogswar.ru/armii-mira/vooryjenie/4430-sverhskorostnye-stre.html (last accessed January 23, 2017).
2. Kak rabotayet broneprobivayemost [How armor breakability works], available at: https://ru.wargaming.net/support/kb/articles/50 (last accessed January 23, 2017).
3. Bronezhilety [Flak jackets], available at: http://ohrana.ru/equipment/special/2345/ (last accessed January 23, 2017).
4. Popov N.N., Rastorguyev B.S. and Zabegayev A.V. (1992), Raschet konstruktsiy na dinamicheskiye i spetsial'nyye nagruzki [Calculation of Structures for Dynamic and Special Loads], Vysshaya shkola, Moskva, 320 p.
5. Kalashnikov V.V. and Aleksentseva S.Ye. (2009), "Issledovaniye vliyaniya konstruktsii puli na protsess probivaniya stal'noy pregrady" [Investigation of the effect of ballet construction on steelarmour punching process], *Vestnik Samarskogo Gosudarstvennogo Tekhnicheskogo Universiteta* [Bulletin of the Samara State Technical University], No 2 (24), pp. 60–68.
6. Aptukov V.N. (1990), "Pronikaniye: mekhanicheskiye aspekty i matematicheskoye modelirovaniye" [Penetration: Mechanical Aspects and Mathematical Modeling], *Problemy prochnosti* [Strength problems], No 2, pp. 60–68.
7. Astanin V.V. Galiyev Sh.U. and Ivashchenko K.V. (1988), Osobennosti deformirovaniya i razrusheniya pregrad pri vzaimodeystvii po normali so stal'nym udarnikom [Specific features of deformation and fracture of obstacles in normal interaction with a steel striker], *Problemy prochnosti* [Strength problems], No 12, pp. 52–57.
8. Yefremov, A. K. (2013), "Osobennosti rascheta kontaktnykh datchikov tseli vzryvateley" [Peculiarities of the calculation of contact sensors for fuses], *Science & education*, No 8, available at: http://technomag.bmstu.ru/doc/605972.html (last accessed January 23, 2017), **doi**: 10.7463/0813.0605972.

9. Mechanics of penetration of metal armor [Mechanics of penetration of metal armor], available at: http://materialy-bronirovaniya.ru/metallicheskaya-bronya/mekhanika-protsessa-probivaniya-metallicheskogo-broneelementa (last accessed January 23, 2017).
10. Fedorov, S.V., Veldanov, V.A., Gladkov, N.A. and Smirnov, V.E. (2016) "Numerical Analysis of Penetration of Segmented and Telescoic Projectiles of High Density Alloy into the Steel Target", *Bulletin of Bauman Moscow State Technical University. Series: machine-building*, No 3(108), pp. 100–117, available at: http://elibrary.ru/item.asp?id=26202542 (last accessed January 23, 2017).
11. Grekov, V.F., Kovtun, A.V., Nesterenko, S.I. and Nedelko V.A. (1998), *Protective clothing for outdoor use*, Patent UA, No 20386.
12. Terebushko, O.I. (1984), *Osnovy teorii uprugosti i plastichnosti* [Fundamentals of the theory of elasticity and plasticity], Nauka, Moskva, 320 p.

Надійшла (received) 31.01.2017
Прийнята до друку (accepted for publication) 18.04.2017

Моделювання процесу пробивання високошвидкісним ударником перепони у вигляді набору порожнистих циліндрів

А. В. Ковтун, В. О. Табуненко

Проаналізовані характеристики вражаючих елементів артилерійських систем і стрілецької зброї Проаналізовані характеристики и конструкції індивідуальних засобів броне захисту. Основний удар високо швидкісних вражаючих елементів приймають жорсткі пластини. Вони можуть бути виконані з високоміцних металів або двошарових панелей. При зустрічі з такою панеллю, носок кулі руйнується. В результаті зростає площа взаємодії кулі і панелі, виникає прогин і розчеплення кераміки при одночасному руйнуванні кулі. При ударі ударника по перешкоді в ній виникає декілька типів хвиль збурювань, які поширюються с різними швидкостями. Ці впливи викликають в конструкції складний напружений стан, інтенсивність якого швидко знижується в часі. **Мета статті** – досліджувати процес взаємодії високошвидкісного ударника із захисною перешкодою у вигляді набору пустотілих циліндрів. **Методи дослідження.** Удосконалення засобів індивідуального броне захисту може бути досягнуто шляхом застосування оптимального поєднання нових матеріалів і сучасних конструктивно-схемних рішень. Характер проникнення ударника в перешкоду може змінитися, якщо перешкода буде уявляти собою конструкцію, яка складається з набору пустотілих циліндрів. Розглянуто процес взаємодії високо швидкісного ударника з захисною перешкодою у вигляді набору пустотілих циліндрів. При контакті ударника з поверхневим шаром перешкоди, за рахунок наявності розширеної верхньої частини, ударник попадає в пустотілий циліндр, який щільно обіймає бокову поверхню ударника, що створює супротив його руху. При русі ударника в циліндрі проходить перетворення кінетичної енергії ударника в енергію деформування циліндра і роботу по переборенню сили тертя. При цьому частина енергії ударника гаситься проміжним шаром і перерозподіляється на силовий каркас внутрішнього шару. **Результати.** Запропонована модель визначення глибини проникнення ударника в перешкоду у вигляді набору пустотілих циліндрів. Наведені результати розрахунків. Пропонується подальше удосконалення засобів індивідуального бронезахисту досягати шляхом застосування оптимального поєднання нових матеріалів і сучасних конструктивно-схемних рішень.

Ключові слова: бронезахист, високошвидкісний ударник, що вражає елемент, рівні загрози, перешкода, пластична деформація, порожнистий циліндр.

Моделирование процесса пробивания высокоскоростным ударником преграды в виде набора полых цилиндров

А. В. Ковтун, В. А. Табуненко

Проанализированы характеристики поражающих элементов артиллерийских систем и стрелкового оружия проанализированы характеристики и конструкции индивидуальных средств броне защиты. Основной удар высоко скоростных поражающих элементов принимают жесткие пластины. Они могут быть выполнены из высокопрочных металлов или двухслойных панелей. При встрече с такой панелью, носок шара разрушается. В результате растет площадь взаимодействия шара и панели, возникает прогиб и расцепления керамики при одновременном разрушении шара. При ударе ударника по препятствиям в ней возникает несколько типов волн возмущений, которые распространяются с разными скоростями. Эти воздействия вызывают в конструкции сложное напряженное состояние, интенсивность которого быстро снижается во времени. **Цель статьи** - исследовать процесс взаимодействия высокоскоростного ударника с защитной преградой в виде набора пустотелых цилиндров. **Методы исследования.** Совершенствование средств индивидуальной броне защиты может быть достигнуто путем применения оптимального сочетания новых материалов и современных конструктивно-схемных решений. Характер проникновения ударника в препятствие может измениться, если препятствие будет представлять собой конструкцию, состоящую из набора пустотелых цилиндров. Рассмотрен процесс взаимодействия высоко скоростного ударника с защитным препятствием в виде набора пустотелых цилиндров. При контакте ударника с поверхностным слоем препятствия, за счет наличия расширенной верхней части, ударник попадает в пустотелый цилиндр, плотно занимает боковую поверхность ударника, что создает сопротивление его движения. При движении ударника в цилиндре проходит преобразования кинетической энергии ударника в энергию деформации цилиндра и работу по преодолении силы трения. При этом часть энергии ударника гасится промежуточным слоем и перераспределяется на силовой каркас внутреннего слоя. **Результаты.** Предложенная модель определения глубины проникновения ударника в препятствие в виде набора пустотелых цилиндров. Приведенные результаты расчетов. Предлагается дальнейшее совершенствование средств индивидуальной бронезащиты достигать путем применения оптимального сочетания новых материалов и современных конструктивно-схемных решений.

Ключевые слова: бронезащита, высокоскоростной ударник, поражающий элемент, уровни угрозы, препятствие, пластическая деформация, полый цилиндр.

Methods of information systems synthesis

УДК 62-50 **doi: 10.20998/2522-9052.2017.1.02**

В. І. Носков, М. В. Ліпчанський, Г. В. Гейко

Національний технічний університет «Харківський політехнічний інститут», Харків, Україна

СИНТЕЗ СИСТЕМИ УПРАВЛІННЯ АСИНХРОННИМ ТЯГОВИМ ПРИВОДОМ МЕТОДОМ АКУР

Предметом вивчення в статті є аналіз методів синтезу систем автоматичного управління (САУ) для рухомого складу з асинхронним тяговим приводом (АТП). **Мета** – забезпечення якості динаміки процесів, точності приведення об'єктів в задану точку фазового простору та мінімізація енергетичних витрат на процеси керування в умовах детермінованих і випадкових збурень. **Задача –** вибір метода синтезу оптимальних САУ, що дозволяє забезпечити необхідні показники якості роботи АТП. Аналіз проблем оптимального управління тяговим приводом рухомого складу показав, що найбільш перспективно використовувати для синтезу систем управління об'єктами, які описуються системами нелінійних диференціальних рівнянь, метод аналітичного конструювання регуляторів за критерієм узагальненої роботи (АКУР). Метод АКУР дозволяє синтезувати регулятори, які оптимізують процеси управління не тільки при детермінованих, але й при випадкових збуреннях. Але використання цього методу можливо для об'єктів, математична модель яких описується системою диференціальних рівнянь, в яких управління входять лінійно. У зв'язку з тим, що в АТП управління входять нелінійно, для використання методу АКУР була виконана його адаптація та були отримані вирази для управлінь, які визначають структуру оптимального регулятора. **Висновки:** запропоновано підхід для синтезу САУ асинхронного тягового приводу з використанням метода АКУР. Була виконана адаптація цього методу з урахуванням нелінійних управлінь.

Ключові слова: система автоматичного управління, асинхронний тяговий привід, метод аналітичного конструювання регуляторів за критерієм узагальненої роботи.

Вступ

Одним з найважливіших напрямків технічного розвитку рухомого складу з високими економічними показниками є впровадження тягових приводів з асинхронними двигунами, які мають ряд переваг у порівнянні з двигунами постійного струму. Широке впровадження асинхронного приводу на залізницях України затрималося з кількох причин, основною з яких є необхідність створення надійної та економічної САУ тяговим приводом. У той же час випробування і досвід експлуатації перших українських дизель-поїздів ДЕЛ-01 та ДЕЛ-02 з АТП показують, що ця складність подолана, а накопичений досвід у галузі математичного моделювання, застосування сучасних методів теорії автоматичного управління і прогресивних інформаційних технологій, можуть бути використані при створенні сучасного рухомого складу.

Аналіз проблеми та постановка задачі

На даний час відома низка методів для синтезу оптимальних систем управління. Проте, найбільшого поширення набули тільки деякі з них: класичне варіаційне числення, динамічне програмування, принцип максимуму Понтрягіна, метод функцій Ляпунова, методи аналітичного конструювання регуляторів Лєтова-Калмана та О.А. Красовського, машинно-орієнтовані методи термінального управління з використанням алгоритмів випадкового пошуку [1–4]. Багато авторів займалися питаннями синтезу регуляторів для деяких видів математичних моделей, в яких управління входять нелінійно [5–7]. Аналіз проблем оптимального управління тяговим приводом рухомого складу показав, що найбільш перспективно використовувати для синтезу систем управління об'єктами, які описуються системами нелінійних диференційних рівнянь, метод аналітичного конструювання регуляторів за критерієм узагальненої роботи. Метод АКУР дозволяє синтезувати регулятори, які оптимізують процеси управління не тільки при детермінованих, але і при випадкових збуреннях. Критерій оптимальності в методі АКУР дає можливість враховувати як вимоги до якості динамічних процесів, точності переведення об'єкта в задану точку фазового простору, так і мінімізувати енергетичні витрати на процеси управління.

Загальне формулювання основної теореми методу АКУР таке [8–10]. Нехай об'єкт описується системою нелінійних диференційних рівнянь:

$$\frac{dx_i}{dt} + f_i(x_1, ..., x_n, t) = \sum_{j=1}^{m} \phi_{ij}(x_1, ..., x_n, t)u_j + \\ + \sum_{k=1}^{n} \eta_{ik}(x_1, \dots, x_n, t)\xi_k(t), \quad (1)$$

тоді управліннями, оптимальними в сенсі мінімуму функціонала

$$I = M\left[V_3\left(x_1(t_2), ..., x_n(t_2), t_2\right)\right] + M \times \\ \times\left[\int_{t_1}^{t_2} Q(x_1, ..., x_n, t)dt\right] + M\left[\frac{1}{q}\sum_{j=1}^{m}\int_{t_1}^{t_2}\left(u_j/k_j\right)^q dt\right] + \quad (2)$$

$$+M\left[\frac{1}{p}\sum_{j=1}^{m}\int_{t_1}^{t_2}\left(k_j\sum_{i=1}^{n}\phi_{ij}\frac{\partial V}{\partial x_i}\right)^p dt\right]$$

є управління

$$u_j=-k_j^p\left(\sum_{i=1}^{n}\varphi_{ij}\frac{\partial V}{\partial x_i}\right)^{p-1}, \qquad (3)$$

де V – рішення лінійного диференційного рівняння в частинних похідних

$$\frac{\partial V}{\partial t}-\sum_{i=1}^{n}\frac{\partial V}{\partial x_i}f_i=-Q \qquad (4)$$

за граничною умовою

$$V\left[x_1(t_2),...,x_n(t_2),t_2\right]=V_3\left[x_1(t_2),...,x_n(t_2),t_2\right]. \qquad (5)$$

У співвідношеннях (1) – (5) прийняті наступні позначення: x_i $(i=1,\,2,\,...,\,n)$ – фазові координати об'єкта; f_i, φ_{ij}, η_{ik} $(i=1,\,2,\,...,\,n;\,j=1,\,2,\,...,\,m;$ $k=1,2,\,...,r)$ – безперервні задані функції; $\xi_k(t)$ – білі шуми (послідовності статистично незалежних δ-імпульсів, випадкових за площею і розділених як завгодно малими, але кінцевими проміжками часу); M – символ математичного сподівання; $V_3[x_1(t_2),\,...,\,x_n(t_2),\,t_2]$ – позитивно визначена безперервна функція, що задає точність переведення об'єкта в момент часу t_2 в задану точку фазового простору; $Q(x_1,\,...,\,x_n,\,t)$ – позитивно визначена безперервна функція, що задає вимоги до якості перехідних процесів об'єкту за фазовими координатами в інтервалі часу управління $[t_1,\,t_2]$; p, q – позитивні числа, що задовольняють умовам: $1/p+1/q=1$ та x^p, x^q – парні функції x; k_j $(j=\overline{1,m})$ – задані числа; u_j $(j=\overline{1,m})$ – сигнали управління на входах виконуючих пристроїв.

У тому випадку, коли функції f_i, Q, V_3 можна задати у вигляді ступеневих рядів:

$$f_i=\sum_{g=1}^{n}a_{ig}x_g+\sum_{g,h=1}^{n}a_{igh}x_gx_h+\sum_{g,h,q=1}^{n}a_{ighq}x_gx_hx_q+..., \qquad (6)$$

$$Q=\frac{1}{2}\sum_{g,h=1}^{n}\beta_{gh}x_gx_h+\frac{1}{3}\sum_{g,h,q=1}^{n}\beta_{ghq}x_gx_hx_q+\frac{1}{4}\sum_{g,h,q,l=1}^{n}\beta_{ghql}x_gx_hx_qx_l+..., \qquad (7)$$

$$V_3=\frac{1}{2}\sum_{g,h=1}^{n}\rho_{gh}x_gx_h+\frac{1}{3}\sum_{g,h,q=1}^{n}\rho_{ghq}x_gx_hx_q+\frac{1}{4}\sum_{g,h,q,l=1}^{n}\rho_{ghql}x_gx_hx_qx_l+..., \qquad (8)$$

де $a_{ig}, a_{igh}, a_{ighl}$, … – коефіцієнти, які є в загальному випадку функціями часу, що не змінюються при перестановці індексів, починаючи з другого; $\beta_{gh}, \beta_{ghq}, \beta_{ghql}$, … – коефіцієнти, які є в загальному випадку функціями часу, що не змінюються при перестановці індексів; $\rho_{gh}, \rho_{ghq}, \rho_{ghql}$, … – постійні коефіцієнти, які не змінюються при перестановці індексів, рішення рівняння (4) можна шукати у вигляді

$$V=\frac{1}{2}\sum_{g,h=1}^{n}A_{gh}x_gx_h+\frac{1}{3}\sum_{g,h,q=1}^{n}A_{ghq}x_gx_hx_q+\frac{1}{4}\sum_{g,h,q,l=1}^{n}A_{ghql}x_gx_hx_qx_l+..., \qquad (9)$$

де A_{gh}, A_{ghq}, A_{ghql} – коефіцієнти, які є в загальному випадку функціями часу, можуть бути визначені з системи звичайних диференційних рівнянь:

$$\frac{dA_{ij}}{dt}-\sum_{p=1}^{n}(\alpha_{pi}A_{pj}+\alpha_{pj}A_{pi})=-\beta_{ij};$$

$$\frac{dA_{ijk}}{dt}-\sum_{p=1}^{n}(\alpha_{pi}A_{pjk}+\alpha_{pj}A_{pik}+\alpha_{pk}A_{pij})=-\beta_{ijk}+\sum_{p=1}^{n}\left(A_{pi}\alpha_{pjk}+A_{pj}\alpha_{pik}+A_{pk}\alpha_{pij}\right). \qquad (10)$$

З урахуванням співвідношення (9) вираз для управління (3) можна представити у вигляді:

$$u_j=-k_j^p\left(\sum_{i=1}^{n}\varphi_{ij}\left(\sum_{k=1}^{n}A_{jk}x_k+\sum_{k,l=1}^{n}A_{ikl}x_kx_l+...\right)\right)^{p-1}. \qquad (11)$$

Це співвідношення і визначає структуру оптимального, в сенсі мінімуму функціоналу узагальненої роботи (2), регулятора для початкового об'єкта управління (1).

Таким чином, для синтезу оптимальної системи управління методом АКУР необхідно, щоб математична модель об'єкта мала вигляд (1).

Адаптація методу АКУР для об'єктів, в які управління входять нелінійно

З вигляду рівнянь (1) випливає, що метод АКУР можна використовувати для об'єктів, що описуються за допомогою систем звичайних нелінійних диференційних рівнянь, в які управління u_j входять лінійно. Це накладає певні обмеження на область застосування методу, оскільки існує широкий клас об'єктів, математичні моделі яких описуються системами звичайних диференційних рівнянь, в які управляючі впливи входять нелінійно.

Прикладом є асинхронний тяговий привід [11]. В цьому випадку у праву частину системи рівнянь (1) входять співвідношення виду $u_1\sin(\alpha u_2+\gamma)$, де u_1 і u_2 – управління; α, γ – константи, або в більш загальному випадку – у вигляді добутку функцій, кожна з яких залежить від одного управління: $\psi_1(u_1)$, $\psi_2(u_2)$. У зв'язку з необхідністю вирішувати завдання для об'єкта, математична модель якого містить керуючі впливи під знаками функцій, або у вигляді добутку двох функцій, кожна з яких залежить від одного управління, пропонується нова модифікація методу аналітичного конструювання регуляторів за критерієм узагальненої роботи, яка ґрунтується на такій теоремі [12].

Теорема. Нехай об'єкт описується системою:

$$\frac{dx_i}{dt} + f_i(x_i, ..., x_n, t) = \sum_{k=1}^{n} \eta_{ik}(x_1,\ldots,x_n,t)o_k(t) + \\ + \sum_{j=1}^{m} \phi_{ij}(x_1, ..., x_n, t)\psi_{1ij}(u_{1ij})\psi_{2ij}(u_{2ij}), \quad (12)$$

тоді оптимальними в сенсі мінімуму функціоналу

$$I = M[V_3(x_1(t_2), ..., x_n(t_2), t_2)] + M\left[\int_{t_1}^{t_2} Q dt\right] + \\ + M\left[\sum_{j=1}^{m}\sum_{i=1}^{n}\int_{t_1}^{t_2}\left(u_{1ij}^2 / k_{1ij}^2 + u_{2ij}^2 / k_{2ij}^2\right) dt\right] \quad (13)$$

є управління:

$$u_{1ij} = -k_{1ij}^2 \frac{\partial V}{\partial x_i}\varphi_{ij}\psi_{1ij}\psi_{2ij} / 2u_{1ij}; \quad (14)$$

$$u_{2ij} = -k_{2ij}^2 \frac{\partial V}{\partial x_i}\varphi_{ij}\psi_{1ij}\psi_{2ij} / 2u_{2ij}, \quad (15)$$

де V – рішення рівняння (4) за граничною умовою (5).

Доказ. Повна похідна функції V в силу рівнянь об'єкта (12) і рівняння (4) дорівнює

$$\frac{dV}{dt} = \frac{\partial V}{\partial t} + \sum_{i=1}^{n}\frac{\partial V}{\partial x_i}\frac{dx_i}{dt} = \\ = \frac{\partial V}{\partial t} + \sum_{i=1}^{n}\frac{\partial V}{\partial x_i}\left(\sum_{j=1}^{m}\varphi_{ij}\psi_{ij}^1\psi_{ij}^2 + \sum_{k=1}^{r}\eta_{ik}\xi_k(t) - f_i\right) = (16)$$

$$= -Q + \sum_{i=1}^{n}\frac{\partial V}{\partial x_i}\sum_{j=1}^{\mathrm{m}}\varphi_{ij}\psi_{ij}^1\psi_{ij}^2 + \sum_{i=1}^{n}\frac{\partial V}{\partial x_i}\sum_{k=1}^{r}\eta_{ik}\xi_k(t).$$

Інтегруємо вираз (16) в інтервалі часу $[t_1, t_2]$:

$$V[x_1(t_2), \ldots, x_n(t_2), t_2] - V[x_1(t_1), \ldots, x_n(t_1), t_1] = \\ = -\int_{t_1}^{t_2} Q dt + \sum_{i=1}^{n}\sum_{j=1}^{m}\int_{t_1}^{t_2}\frac{\partial V}{\partial x_i}\varphi_{ij}\psi_{ij}^1\psi_{ij}^2 dt + \quad (17)$$

$$+ \sum_{i=1}^{n}\sum_{k=1}^{r}\int_{t_1}^{t_2}\frac{\partial V}{\partial x_i}\eta_{ik}\xi_k(t)dt.$$

Враховуючи, що за умовою

$$V[x_1(t_2), \ldots, x_n(t_2), t_2] = V_3[x_1(t_2), \ldots, x_n(t_2), t_2],$$

із (17) можна отримати

$$M\left[V_3\left(x_1(t_2), \ldots, x_n(t_2), t_2\right)\right] + M\left[\int_{t_1}^{t_2} Q dt\right] = \\ = M\left[V\left(x_1(t_1), \ldots, x_n(t_1), t_1\right)\right] + \quad (18)$$

$$+ M\left[\sum_{i=1}^{n}\sum_{j=1}^{m}\int_{t_1}^{t_2}\frac{\partial V}{\partial x_i}\varphi_{ij}\psi_{ij}^1\psi_{ij}^2 dt\right] + M\left[\sum_{i=1}^{n}\sum_{k=1}^{r}\int_{t_1}^{t_2}\frac{\partial V}{\partial x_i}\eta_{ik}\xi_k(t)dt\right].$$

Використовуючи методику О.А. Красовського [9] покажемо, що останній член у (18) не залежить від управлінь (14), (15). З огляду на прийняту модель білих шумів в (1) і (12), можна записати

$$\xi_k(t) = \sum_d B_{kd}\delta(t - \tau_d), \quad (19)$$

де $\xi_k(t)$ – узагальнений стаціонарний випадковий процес; B_{kd} – незалежні випадкові центровані величини; $\tau_1, \tau_2, \ldots$ – випадкові моменти часу, яким відповідають "імпульси" δ-функції.

Згідно співвідношенню (19) останній член виразу (18) можна перетворити до вигляду

$$R = M\left[\sum_{i=1}^{n}\sum_{j=1}^{m}\sum_{d}\left(B_{kd}\int_{\tau_d - 0}^{\tau_d + 0}\frac{\partial V}{\partial x_i}\eta_{ik}\delta(t - \tau_d)dt\right)\right]. \quad (20)$$

Внаслідок впливу δ-функцій $\delta(t - \tau_d)$ $(d = const)$ фазові координати об'єкта управління (12) на інтервалі часу від $\tau_d - 0$ до $\tau_d + 0$ отримують прирощення

$$\Delta x_{id} = \int_{\tau_d - 0}^{\tau_d + 0}\eta_{ik}B_{kd}\delta(t - \tau_d)dt, \quad i = \overline{1,n}.$$

З точністю до нескінченно малих величин більш високого порядку прирощення Δx_{id} не залежить від управлінь u_{1ij} та u_{2ij} $(i = \overline{1,n},\ j = \overline{1,m})$. Таким чином, зміни фазових координат, викликані впливом збурень у вигляді δ-функцій, з точністю до нескінченно малих величин вищого порядку не залежать від управлінь u_{1ij} и u_{2ij}, а це означає, що і збурення функцій

$$V[x_1, \ldots, x_n, t],\ \frac{\partial V}{\partial x_i},\ \eta_{ik}(x_1, \ldots, x_n, t),$$

викликані впливом збурень у вигляді δ-функцій з точністю до нескінченно малих більш вищого порядку, не залежать від управлінь u_{1ij} и u_{2ij} $(i = \overline{1,n},\ j = \overline{1,m})$. Тому і R з точністю до нескінченно малих величин не залежить від управлінь.

Функціонал (13) з урахуванням виразів (17) і (20) перетворимо до виду

$$I = M\left[V(x_1(t_1), \ldots, x_n(t_1), t_1)\right] + \\ + M\left[\sum_{i=1}^{n}\sum_{j=1}^{m}\int_{t_1}^{t_2}\frac{\partial V}{\partial x_i}\varphi_{ij}\psi_{ij}^1\psi_{ij}^2 dt\right] + \quad (21)$$

$$+ M\left[\sum_{j=1}^{m}\sum_{i=1}^{n}\int_{t_1}^{t_2}\left(u_{1ij}^2 / k_{1ij}^2 + u_{2ij}^2 / k_{2ij}^2\right)dt\right] + R.$$

Оскільки маємо таке:

$$\sum_{j=1}^{m}\sum_{i=1}^{n}\left[\frac{u_{1ij}}{k_{1ij}} + k_{1ij}\frac{\partial V}{\partial x_i}\varphi_{ij}\psi_{1ij}\psi_{2ij} / 2u_{1ij}\right]^2 = \\ = \sum_{j=1}^{m}\sum_{i=1}^{n}\left[\frac{u_{1ij}^2}{k_{1ij}^2} + \frac{\partial V}{\partial x_i}\varphi_{ij}\psi_{1ij}\psi_{2ij} + \frac{u_{1ij}^2}{k_{1ij}^2}\right] = \\ = 2\sum_{j=1}^{m}\sum_{i=1}^{n}\frac{u_{1ij}^2}{k_{1ij}^2} + \sum_{j=1}^{m}\sum_{i=1}^{n}\frac{\partial V}{\partial x_i}\varphi_{ij}\psi_{1ij}\psi_{2ij};$$

$$\sum_{j=1}^{m}\sum_{i=1}^{n}\left[\frac{u_{2ij}}{k_{2ij}} + k_{2ij}\frac{\partial V}{\partial x_i}\varphi_{ij}\psi_{1ij}\psi_{2ij} / 2u_{2ij}\right]^2 =$$

$$= 2\sum_{j=1}^{m}\sum_{i=1}^{n}\frac{u_{2ij}^2}{k_{2ij}^2} + \sum_{j=1}^{m}\sum_{i=1}^{n}\frac{\partial V}{\partial x_i}\varphi_{ij}\psi_{1ij}\psi_{2ij},$$

то функціонал (21) можна записати у вигляді

$$I = M\left[V(x_1(t_1),\ ...,\ x_n(t_1),t_1)\right] + M \times$$

$$\times\left[\frac{1}{2}\int_{t_1}^{t_2}\sum_{j=1}^{m}\sum_{i=1}^{n}[\frac{u_{1ij}}{k_{1ij}} + k_{1ij}\frac{\partial V}{\partial x_i}\phi_{ij}\psi_{1ij}\psi_{2ij} / 2u_{1ij}]^2 dt\right] + M \times \quad (22)$$

$$\times\left[\frac{1}{2}\int_{t_1}^{t_2}\sum_{j=1}^{m}\sum_{i=1}^{n}[\frac{u_{2ij}}{k_{2ij}} + k_{2ij}\frac{\partial V}{\partial x_i}\phi_{ij}\psi_{1ij}\psi_{2ij} / 2u_{2ij}]^2 dt\right] + R.$$

Якщо управління u_{1ij}, u_{2ij} визначаються відповідно співвідношеннями (14) і (15), то підінтегральний вираз в функціоналі (22) обертається в нуль, і він приймає мінімальне значення.

Отже, теорема доведена. Вона доведена для випадку $p = q = 2$, тобто для квадратичного критерію якості щодо управлінь, критерію, що має ясний фізичний сенс і широко застосовується при оптимізації електропривода. Зауважимо, що вигляд оптимальних управлінь (14) і (15) при випадкових збуреннях описаного типу однаковий для детермінованих і стохастичних систем. При цьому величини управлінь як і в найбільш загальних теоремах по АКУР О.А. Красовського [8] не залежать від рівня шумів.

Якщо функції f_i, Q, V_3 можна представити у вигляді степеневих рядів (6), (7), (8), то рішення рівняння (4) матиме вигляд (9), а коефіцієнти цього рівняння визначаються з системи рівнянь (10). З урахуванням співвідношення (9) рівняння (14) і (15) можна представити у вигляді

$$u_{1ij} = -k_{1ij}^2\frac{\phi_{ij}\cdot\psi_{1ij}\cdot\psi_{2ij}}{2u_{1ij}}\left(\sum_{k=1}^{n}A_{jk}x_k + \sum_{k,l=1}^{n}A_{ikl}x_k x_l + ...\right), \quad (23)$$

$$u_{2ij} = -k_{2ij}^2\frac{\phi_{ij}\cdot\psi_{1ij}\cdot\psi_{2ij}}{2u_{2ij}}\left(\sum_{k=1}^{n}A_{jk}x_k + \sum_{k,l=1}^{n}A_{ikl}x_k x_l + ...\right). \quad (24)$$

Ці співвідношення і визначають структуру оптимального регулятора.

Висновок

Запропоновано підхід для синтезу САУ асинхронного тягового приводу з використанням метода АКУР. Була виконана адаптація цього методу з урахуванням нелінійних управлінь. Отримані співвідношення, котрі визначають структуру оптимального регулятора

СПИСОК ЛІТЕРАТУРИ

1. Варіаційне числення та методи оптимізації / М.О. Перестюк, О.М. Станжицький, О.В. Капустян, Ю.В. Ловейкін. Навч. посібник. – Київ: КНУ ім. Т.Шевченка, 2010. – 121 с.
2. Милютин А.А. Принцип максимума в оптимальном управлении / А.А. Милютин, А.В. Дмитрук, Н.П. Осмоловский – М.: МГУ им. М.В. Ломоносова, 2004. – 167 с.
3. Летов А.М. Аналитическое конструирование регуляторов / А.М. Летов // М.: Автоматика и телемеханика. – 1960. – Т. 21, вып. 4. – С. 436–441.
4. Сурков В.В. Аналитическое конструирование регуляторов, оптимальных по точности и быстродействию / В.В. Сурков, Б.В. Сухинин, В.И. Ловчаков, А.Э. Соловьев. – Тула: Тул. гос. ун-т, 2005. – 300 с.
5. Дмитриенко В.Д. Синтез оптимальных регуляторов для дизель-поезда методом аналитического конструирования по критерию обобщенной работы / В.Д. Дмитриенко, Н.И. Заполовский, Н.В. Мезенцев // Вісник НТУ «ХПІ». – Харків: НТУ «ХПІ», 2010. – Вип. 31. – С. 87–94.
6. Эволюционные методы компьютерного моделирования / А.Ф. Верлань, В.Д. Дмитриенко, Н.И. Корсунов, В.А. Шорох. – К.: Наук. думка, 1992. – 256 с.
7. Дмитриенко В.Д. Оптимизация функционала обобщенной работы при нелинейно входящих управлениях / В.Д. Дмитриенко, В.И. Носков, Н.В. Мезенцев // Праці Луганського відділення Міжнародної Академії Автоматизації. – Луганськ: МАН, 2005. – № 1. – С. 17 – 22.
8. Моделирование и оптимизация систем управления и контроля локомотивов / В.И. Носков, В.Д. Дмитриенко, Н.И. Заполовский, С.Ю. Леонов. – Х.: ХФИ «Транспорт Украины», 2003. – 248 с.
9. Красовский А.А. Системы автоматического управления полетом и их аналитическое конструирование / А.А. Красовский . – М.: Наука, 1973. – 560 с.
10. Дмитриенко В.Д. Синтез регуляторов методом АКОР А.А. Красовского при нелинейно входящих управлениях и случайных возмущающих воздействиях / В.Д. Дмитриенко, В.И. Носков, Н.В. Мезенцев // Вісник НТУ «ХПІ», 2009. – Харків: НТУ «ХПІ», 2010. – Вип. 12. – С. 53 – 60.
11. Носков В.И. Математическая модель электропривода на основе метода АКУР. / В.И. Носков, А.И. Баленко, Н.И. Заполовский // Функционально-ориентированные вычислительные системы: Межд. НТК. – Киев, 1993. – С. 20.
12. Дмитриенко В.Д. Решение задачи оптимизации критерия обобщенной работы при нелинейно входящих управлениях / В.Д. Дмитриенко, В.И. Носков, Н.В. Мезенцев // Системи обробки інформації. – 2004. – Вип. 12 (40) – С. 52 – 59.

REFERENCES

1. Perestyuk, M.O., Stanzhits'kiy, O.M., Kapustyan, O.V. and Loveykín YU.V. (2010), *Variatsiyne chyslennya ta metody optymizatsiyi* [Variation calculus and optimization methods], KNU im. T. Shevchenka, Київ, 121 p.
2. Milyutin, A.A., Dmitruk, A.V. and Osmolovskiy N.P. (2004), *Printsip maksimuma v optimal'nom upravlenii* [The maximum principle in optimal control], MGU im. M.V. Lomonosova, Moskva, 167 p.
3. Letov A.M. (1960), "*Analiticheskoye konstruirovaniye regulyatorov*" [Analytical Design of Controllers, Avtomatika i telemekhanika], t. 21, vyp. 4, pp. 436–441.

4. Surkov V.V., Sukhynyn, B.V., Lovchakov, V.Y. and Solovev, A.É. (2005), Analytycheskoe konstruyrovanye rehulyatorov, optymalnykh po tochnosty y bystrodeystvyyu [Analytical design of regulators optimal in accuracy and speed], Tul. hos. un-t, Tula, 300 p.
5. Dmitriyenko, V.D., Zapolovskyy, N.Y. and Mezentsev, N.V. (2010), Syntez optymalnykh rehulyatorov dlya dyzel-poezda metodom analytycheskoho konstruyrovanyya po kryteryyu obobshchennoy raboty [Synthesis of optimal regulators for a diesel train by the method of analytical construction according to the criterion of generalized work], *Visnyk NTU «KHPI»*, Kharkiv, vyp. 31, pp. 87–94.
6. Verlan, A.F., Dmytryenko, V.D., Korsunov, N.Y. and Shorokh, V.A. (1992), Évolyutsyonnye metody kompyuternoho modelyrovanyya [Evolutionary methods of computer modeling], Nauk. dumka, Kyev, 256 p.
7. Dmitriyenko, V.D., Noskov, V.I. and Mezentsev, N.V. (2005), Optymyzatsyya funktsyonala obobshchennoy raboty pry nelyneyno vkhodyashchykh upravlenyyakh [Optimization of the function of generalized work under non-linearly incoming control], *Pratsi Luhanskoho viddilennya Mizhnarodnoyi Akademiyi Avtomatyzatsiyi*, No. 1, pp. 17–22.
8. Noskov V.Y., Dmitriyenko, V.D. and Leonov, S.YU. (2003), *Modelyrovanye y optymyzatsyya system upravlenyya y kontrolya lokomotyvov* [Modeling and Optimization of Locomotive Control and Control Systems], KHFY «Transport Ukrayny», Kharkov, 248 p.
9. Krasovskyy A.A. (1973), *Systemy avtomatycheskoho upravlenyya poletom y ykh analytycheskoe konstruyrovanye* [Systems for Automatic Flight Control and their Analytical Design], Nauka, Moskva, 560 p.
10. Dmitriyenko, V.D., Noskov, V.I. and Mezentsev, N.V. (2009), Syntez rehulyatorov metodom AKOR A.A. Krasovskoho pry nelyneyno vkhodyashchykh upravlenyyakh y sluchaynykh vozmushchayushchykh vozdeystvyyakh, *Visnyk NTU «KHPI»*, Vyp. 12, pp 53–60.
11. Noskov, V.Y., Balenko, A.Y. and Zapolovskyy, N.Y. (1993), Matematycheskaya model élektropryvoda na osnove metoda AKUR, *Funktsyonalno-oryentyrovannye vychyslytelnye systemy*: Mezhd. NTK, Kyev, p. 20.
12. Dmitriyenko, V.D., Noskov, V.I. and Mezentsev, N.V. (2004), Resheniye zadachi optimizatsii kriteriya obobshchennoy raboty pri nelineyno vkhodyashchikh upravleniyakh [Solution of the problem of optimization of the criterion of generalized work for nonlinearly incoming controls], *Sistemi obrobki informatsíi*, vip. 12 (40), pp. 52–59.

Надійшла (received) 07.02.2017
Прийнята до друку (accepted for publication) 16.05.2017

Синтез системы управления асинхронным тяговым приводом методом АКОР

В. И. Носков, М. В. Липчанский, Г. В. Гейко

Предметом изучения в статье является анализ методов синтеза систем автоматического управления (САУ) для подвижного состава с асинхронным тяговым приводом (АТП). **Цель** – обеспечение качества динамики процессов, точности приведения объектов в заданную точку фазового пространства и минимизация энергетических затрат на процессы управления в условиях детерминированных и случайных возмущений. **Задача** – выбор метода синтеза оптимальных САУ, позволяющий обеспечить требуемые показатели качества работы АТП. Анализ проблем оптимального управления тяговым приводом движущегося состава показал, что наиболее перспективно использовать для синтеза систем управления объектами, которые описываются системами нелинейных дифференциальных уравнений, метод аналитического конструирования регуляторов по критерию обобщенной работы (АКОР). Метод АКОР позволяет синтезировать регуляторы, которые оптимизируют процессы управления не только при детерминированных, но и при случайных возмущениях. Однако, использование этого метода возможно для объектов, математическая модель которых описывается системой дифференциальных уравнений, в которых управления входят линейно. В связи с тем, что в АТП управления входят нелинейно, для использования метода АКОР была выполнена его адаптация и были получены выражения для управлений, которые определяют структуру оптимального регулятора. **Выводы:** предложен подход для синтеза САУ асинхронного тягового привода с использованием метода АКОР. Была выполнена адаптация этого метода с учётом нелинейных управлений.

Ключевые слова: система автоматического управления, асинхронный тяговый привод, метод аналитического конструирования регуляторов по критерию обобщенной работы.

Synthesis of the asynchronous traction drive control system by the ACOR method

V. Noskov, M. Lipchansky, G. Geiko

The **subject** of the study in the article is the analysis of methods for the synthesis of automatic control systems (ACS) for rolling stock with an asynchronous traction drive (ATD). **The goal** is assurance the quality of the processes dynamics, the accuracy of bringing objects to a specified point in the phase space, and minimizing energy costs for control processes in conditions of deterministic and random perturbations. **The task** is selection the method of optimal ACS synthesis, which allows providing the required indicators of ATD work quality. Analysis of the problems of optimal control of moving train traction drive showed that it is most promisingly to use the method of analytic construction of regulators by the criterion of generalized work (ACOR) for the synthesis of object management systems, which are described by systems of nonlinear differential equations. AKOR method allows to synthesize regulators that optimize control processes not only for deterministic, but also for random perturbations. However, the use of this method is possible for objects whose mathematical model is described by a system of differential equations in which control enters linearly. In connection with the fact that controls are non-linear in the ATD, to use the AKOR method, its adaptation was performed and expressions were obtained for the controls that determine the structure of the optimal regulator. **Conclusions:** an approach for the synthesis of the asynchronous traction drive ACS using the AKOR method is proposed. Adaptation of this method was carried out taking into account nonlinear controls.

Keywords: automatic control system, asynchronous traction drive, method of analytic construction of the regulators by the criterion of generalized work.

УДК 004.7 **doi: 10.20998/2522-9052.2017.1.03**

И. В. Шостак, А. П. Собчак, О. И. Попова, М. А. Мищенко

Национальный аэрокосмический университет имени Н.Е. Жуковского “ХАИ”, Харьков, Украина

МЕТОД СИНТЕЗА МУЛЬТИАГЕНТНОЙ ВЕБ-ОРИЕНТИРОВАННОЙ СРЕДЫ НА ОСНОВЕ ИНФОРМАЦИОННЫХ СПУТНИКОВ

Цель. Создание благоприятной веб-ориентированной среды за счет продуцирования агентов – спутников в виде дорвеев, что дает возможность повысить информативность объекта производства виртуального приборостроительного предприятия. **Результаты.** В статье рассмотрен метод повышения информативности продукции виртуального приборостроительного предприятия с использованием информационных спутников, на основе синтеза мультиагентной веб-ориентированной среды за счет продуцирования агентов – спутников в виде дорвеев. Раскрыт подробный поэтапный алгоритм создания таких информационных спутников в виде сайтов дорвеев, с основным уклоном на информативность. Представлена основная проблема, связанная с утратой производственного потенциала, а также её решение с применением предложенного метода. **Вывод.** Метод позволяет не только приспособить оборудование к рынку путем его своевременной модернизации, а также позволяет с минимальными затратами денежных ресурсов обеспечить конъюнктуру рынка, конкурентоспособность изделий и их сбыт, который определяет востребованность производства и формирует портфель заказов.

Ключевые слова: информативность, веб-ориентированная среда, конкурентоспособность, востребованность.

Введение

Внедрение в производство научных достижений, а также постепенная замена человеческих ресурсов машинами, что рассматривалось как более выгодное решение с точки зрения экономики (повышение производительности и качества), способствовало более высокой прибыли предприятия. Однако, такие меры повлекли за собой сокращение числа занятых людей в производстве, что привело к постиндустриальному обществу, в экономике которого преобладает инновационный сектор экономики с высокопроизводительной промышленностью, индустрией знаний, а также более высокой долей населения, занятого в сфере услуг, чем в промышленном производстве.

Сегодня все больше предприятий направлено на предоставление услуг, что в свою очередь уменьшает производственную деятельность. Все большую популярность приобретает специальный вид производства на базе виртуального предприятия (ВП), состоящего из географически разделенных исполнителей, которые взаимодействуют в процессе производства, используя преимущественно электронные средства коммуникаций. Существенным преимуществом такого предприятия является отсутствие общих производственных площадей, высокая гибкость производства в зависимости от потребности рынка, а также, значительно меньший начальный капитал для организации такого предприятия.

Основное направление работы ВП состоит в изучении существующего спроса на рынке, в создании такого спроса, а также в повышении информативности продукта, что является одним из ключевых путей к сохранению производственного потенциала и получению прибыли.

В условиях современного рынка, непрерывно наполняющегося все большим разнообразием товаров, которые активно модернизируются, все сложнее обеспечить уникальность и конкурентоспособность своего продукта, так как даже самый особый и уникальный из всех продуктов, может упустить свой шанс на должное признание. В большинстве случаев, так происходит из-за недостаточного представления продукта и обеспечения его информативности.

Поэтому важной задачей является обеспечение должной информативности продукта, так как от того, насколько широко и качественно она распространится, зависит конкурентоспособность товара и формирование спроса на него.

Одним из методов формирования информативности, является метод повышения информативности продукции с использованием информационных спутников, благодаря которому можно приспособить оборудование к рынку не только путем его своевременной модернизации, но и путем достижения желаемой информативности с помощью информационных спутников.

Основываясь на том, что при возникновении потребности в покупке какого-либо ресурса, потенциальный клиент чаще всего обращается к поиску нужной для него информации в просторах интернета, предлагается в этой среде организовать формирование информативности, поскольку такая среда предоставляет стремительный процесс распространения информации, а также обладает более лучшим и качественным описанием оборудования.

Цель работы: создание благоприятной веб-ориентированной среды за счет продуцирования агентов – спутников в виде дорвеев, что даст возможность повысить информативность объекта производства виртуального приборостроительного предприятия (ВПП).

В качестве рассматриваемого примера объекта выбран продукт отечественного производителя, научно-производственного предприятия «КИАТОН», которое является лидером упаковки в Украине за последние годы, а также может рассматриваться как типовой представитель виртуального приборостроительного предприятия [4].

1. Метод повышения информативности продукции ВППд

Исходными данными, которые будут использоваться при проверке метода, являются:

1) www.KIATON.com.ua – исходный многостраничный веб-ресурс;

2) Mark InJet-II – мелкосимвольный каплеструйный промышленно маркировочный принтер;

3) конструкторы сайтов, хостинги – веб-среда для продуцирования информационных спутников.

Для реализации метода необходимо выбрать технологию, с помощью которой будет определена информативность в результате реализации метода. Так как целью является повышение экономических показателей, то можно применить формулу определения информативности в экономическом смысле – увеличение товарооборота в результате проведения мер по повышению информативности объекта рынка.

Дополнительный товарооборот под воздействием рекламы определяется следующим образом:

$$T_д = T_c \cdot П \cdot Д / 100, \quad (1)$$

где $T_д$ – дополнительный товарооборот, вызванный рекламным мероприятием, денежных едини.;

T_c – среднедневной товарооборот, вызванный рекламным мероприятием, денежных едини.;

$Д$ – количество дней учета товарооборота в рекламный и после рекламные периоды;

$П$ – относительный прирост среднедневного товарооборота за рекламный период по сравнению с до рекламным, % [4].

В основе метода повышения информативности продукции виртуального приборостроительного предприятия лежит синтез мультиагентной веб-ориентированной среды, где агентами, несущими в себе программную сущность, способную действовать в интересах достижения целей, поставленных перед ним владельцем или пользователем [3], являются информационные спутники.

Предлагаемым способом повышения информативности продукции производственного предприятия, является привлечение информационных спутников с использованием такого ресурса, как дорвей.

Дорвей (от англ. *doorway* — входная дверь, портал) или входная страница — вид поискового спама, веб-страница, специально оптимизированная под один или несколько поисковых запросов с целью её попадания на высокие места в результатах поиска по этим запросам и дальнейшего перенаправления посетителей на другой сайт или страницу. Иногда дорвеем называют и целый веб-сайт, состоящий из таких страниц. Как правило, содержимое дорвея не представляет никакой информационной ценности для посетителя страницы, и содержит в себе ссылку или автоматическую переадресацию (редирект) на некоторую другую целевую страницу или сайт, раскручивающийся при помощи таких дорвейев.

С точки зрения пользователя, который часто даже не имеет возможности рассмотреть страницу дорвея, – сайт бесполезен. Сайты-дорвеи часто регистрируют на бесплатных хостингах.

Текстовое содержимое дорвея часто бессмысленное, состоит из обрывков предложений с огромным количеством ключевых слов. Такие сайты только засоряют сеть Интернет. Основная цель дорвея – проиндексироваться и попасть в результаты выдачи.

Дорвей, как и другие виды поискового спама, относятся к так называемой «чёрной оптимизации», и поэтому поисковые системы стремятся автоматически и вручную исключать их из своих индексов, как сайты, не имеющие никакой смысловой нагрузки для людей [1].

Среди дорвеев можно условно выделить следующие типы:

1. **Белые дорвеи** – законопослушные сайты, на которых может присутствовать авторский контент и качественная графика. Оказавшись на таком сайте, пользователь может по ссылкам попасть на продвигаемый ресурс.

2. **Серые дорвеи** – это сайты, основная задача которых заключается в передаче ссылочного сайта, поэтому текстовые материалы на таких сайтах – уникальные и понятные, а ссылки вставляются в текстовое окружение. Заручившись поддержкой таких дорвеев, главный сайт может увеличить свой ссылочный вес.

3. **Черные дорвеи** – сайты, основной задачей которых является автоматическая переадресация, или редирект, на сторонний ресурс, что не приветствуется поисковиками. Для реализации этой задачи настраиваются мета-теги или java-скрипты. На черных дорвеях размещаются бессмысленные тексты ввиду того, что у пользователя все равно не будет времени их прочитать.

Основной целью дорвея является продвижение главного сайта вверх в поисковой выдаче.

В создании дорвеев посильный вклад вносят так называемые доргены, которые «придумывают» тексты с требуемыми запросами.

В данном случае, предлагается использовать дорвей максимальной информативности и смысловой нагрузки, что в свою очередь поможет избавиться от «черной оптимизации», т.е., рассматривается создание так называемых «белых дорвеев». Это поможет пользователю избавиться от бесполезной информации, а виртуальному производственному предприятию предоставить возможность информационного продвижения своей продукции и создания спроса.

При достижении информативности данным способом, затрачивается минимальное количество времени и финансов, а также создается презентация продукции для более широкой аудитории.

Рассмотрим на примере классификации видов маркировочного оборудования научно-производственного объединения «КИАТОН» (рис. 1) процесс построения спецификации агентов в виде web-ресурсов – дерева белых дорвеев (рис. 2), построенного в соответствии с представленными разновидностями изделий .

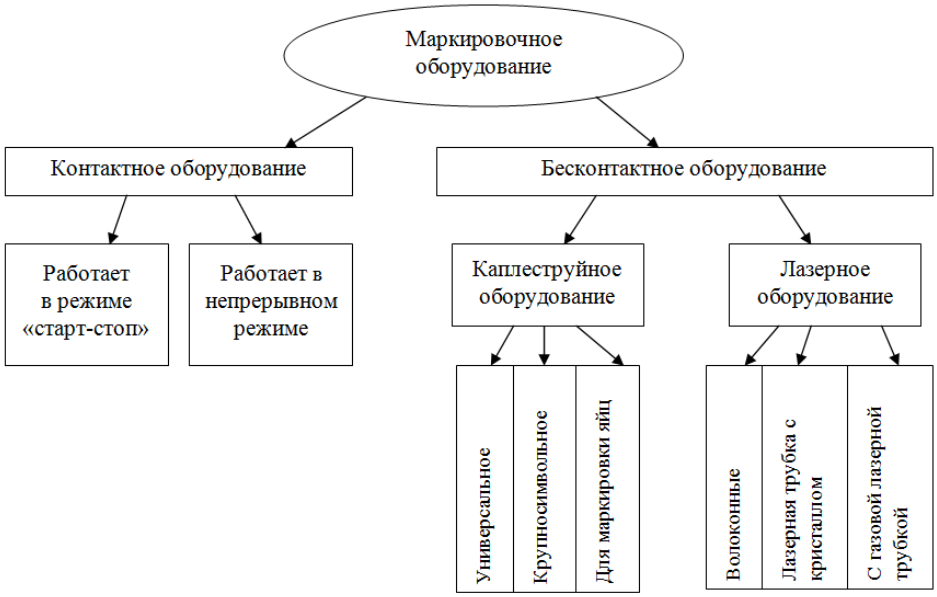


Рис. 1. Классификация видов приборостроительных изделий на примере маркировочного оборудования научно – производственного предприятия «КИАТОН»

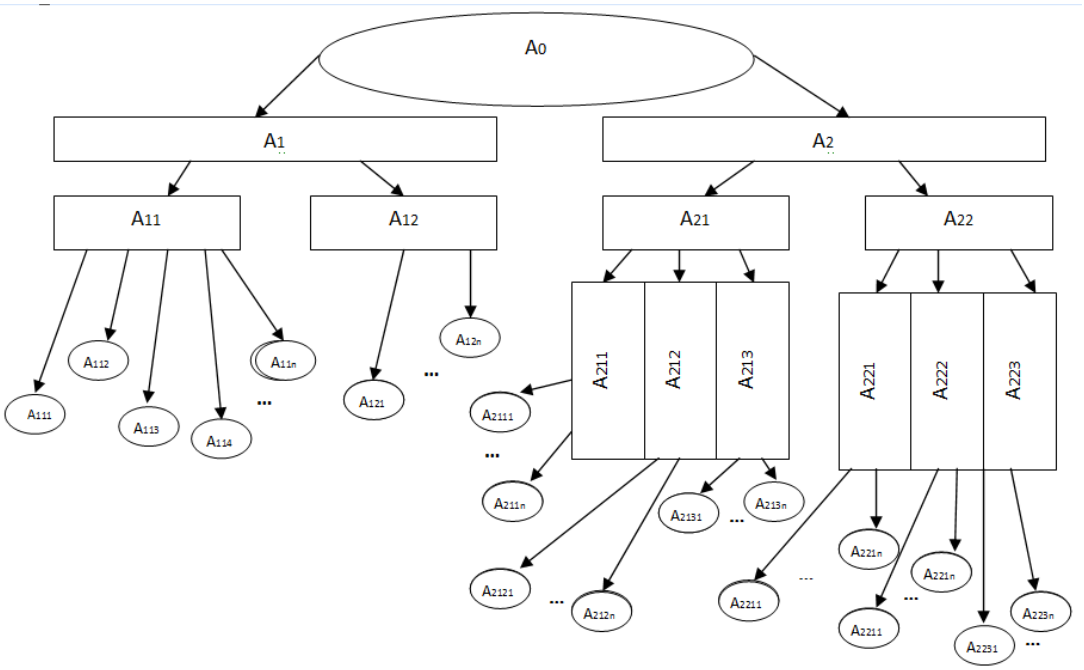


Рис. 2. Спецификация агентов в виде дорвеев

Сущность предлагаемого метода заключается в повышении информативности продукции ВПП путем разработки и развертывания в гипермедийной среде с мультиагентной технологией набора информационных спутников (белых дорвеев), представляющих собой сообщество рефлексивных агентов, миссией которых является ориентирование потенциальных заказчиков на продукцию ВПП. В результате применения метода будет создана информационная система, которая размещена в интернет-среде и ориентирует потенциального заказчика на продукцию соответствующего ВПП.

Исходными данными для разработки метода послужила совокупность следующих показателей:

$$A = < P, O, SS, K, K_d, g, f >, \qquad (2)$$

где P – номенклатура выпускаемой продукции ВПП; O – объем выпуска каждого изделия в номенклатуре ВПП; SS - коэффициент сезонности; K – количество посещений интернет-магазина, K_d – множество посетителей интернет-магазина, которые заключили с ВПП договор о поставке продукции; g – функция, отображающая посещения интернет-магазина ВПП потенциальным клиентом,

$$g : A \rightarrow K; \qquad (3)$$

f – функция, которая отражает заключения договора потенциального клиента с ВПП.

Обобщенное описание метода включает четыре этапа, три из которых реализуются при создании мультиагентной веб-ориентированной среды, а четвертый – в процессе его функционирования.

1. *Разработка интернет-магазина по реализации продукции ВПП*:

а) реализация многоязычного интерфейса;

б) реализация модуля анализа рынка на основе статистики объема продаж по каждому виду продукции *P*;

в) реализация модуля диалога с пользователями *K*, для ответов на запросы об объемах выпуска продукции *O*;

г) разработка модуля реализации продукции.

2. *Разработка основного сайта ВПП* с реализацией функций информирования пользователей *K* о следующем: структуре ВПП, дополнительных характеристиках выпускаемой продукции, системе скидок, сервисном обслуживании.

3. *Разработка набора рефлексивных агентов в форме сайтов-дорвеев*, количество которых совпадает с номенклатурой P продукции, произведенной виртуальным приборостроительным предприятием. Кроме информации о конкретном виде продукции, агент несет информацию (например, номер мобильного телефона) ВПП.

4. *Формирование плана выпуска продукции ВПП по результатам анализа рынка* (данный этап реализуется в процессе функционирования мультиагентной веб-ориентированной среды). [4]

2. Алгоритм синтеза информационного спутника

Большинство дорвеев создаются с помощью «доргенов», которые по своей сути содержат в себе весьма малую часть полезной информации для пользователя, и чаще всего служат для перенаправления информации на другие источники.

При устранении этих недостатков, а именно наличие бесполезной информации, – с данного вебресурса можно получить качественный информационный ресурс, основанный на построении детального и пошагового алгоритма.

Предлагаемый алгоритм (рис. 3) был построен на основе создания нескольких десятков информационных спутников, содержащих в себе основной

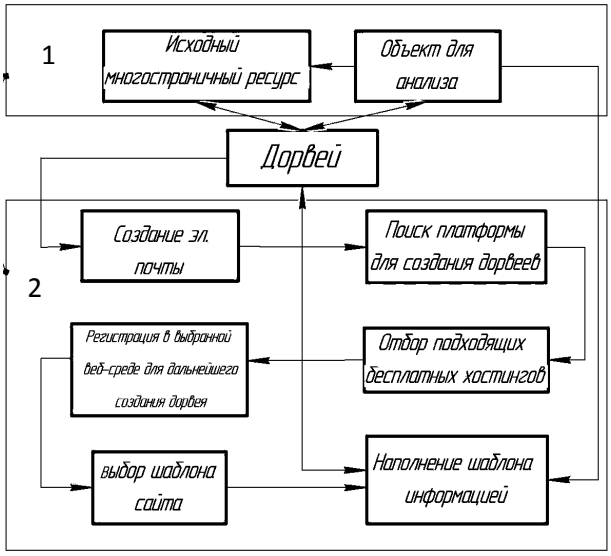


Рис. 3. Алгоритм создания дорвея

уклон на повышение информативности продукции ВПП.

В качестве примера производства ВПП для реализации алгоритма как объект был принят мелкосимвольный каплеструйный принтер **Mark InJet-II**, на основе которого были построены сайты с информационным уклоном [5 – 9].

2.1. Создание электронной почты

Важным шагом в подготовке к созданию дорвея в среде конструкторов сайтов является наличие электронного адреса, поэтому перед тем как приступить к непосредственной работе, необходимым и обязательным условием является процесс авторизации в выбранной платформе. Создание электронной почты можно отнести к обязательным исходным данным, входящим в список предоставляемых ресурсов, созданных самим пользователем. Тем не менее, для полной автоматизации мультиагентной среды необходим последовательный алгоритм.

Начальным этапом является выбор среды для создания электронного адреса почты. Среди наиболее распространенных и общеизвестных электронных адресов была выбрана среда Ukr.net, для создания адреса в которой необходимо:

1) ввести в поисковой строке запроса «почта Ukr.net»;

2) перейти по ссылке результата поиска;

3) выбрать раздел «регистрация»;

4) заполнить поля, которые обязательны при создании адреса. Отображение электронной почты предлагается заполнить сгенерированными вариантами таких слов: markirofka, Infomark, Infoagent, myltiagent, virtualpredpriyatie. Пароль составляется генератором из латинских букв и цифр. В поле имени пользователя вводим «Admin». Также, произвольно заполняем поля «день рождения» и «пол». В качестве адреса резервной почты для восстановления указывается любой другой адрес, действительный, с возможностью воспользоваться им. Последним этапом для регистрации является указание актуального номера мобильного телефона, на который приходит подтверждающая комбинация цифр.

5) завершается регистрация кликом на поле «зарегистрироваться».

2.2. Поиск платформы для создания дорвея

Основным расположением сайтов-дорвеев являются бесплатные хостинги (хостинг — услуга по предоставлению места для размещения информации на сервере, постоянно подключенном к интернету). Основным преимуществом этого интернет-ресурса является отсутствие финансовых затрат, т.е. возможность создания на бесплатной основе. Одним из явных недостатков является ограниченная функциональность. Алгоритм поиска бесплатной платформы состоит из таких этапов:

1) ввод в поисковой строке браузера запроса «Бесплатные конструкторы сайтов»;

2) осуществление выбора, среди множества вариантов предлагается воспользоваться рейтингом лучших на сегодняшнее время сайтов конструкторов.

2.3. Отбор бесплатных хостингов

Чтобы исключить из списка неподходящие хостинги предлагается рассматривать выбор таких ресурсов по следующим критериям:

- доступность – использование бесплатных хостингов;
- долгосрочность - время существование. В жизни дорвеев присутствует прямая зависимость от времени, поэтому, в первую очередь рассматриваются те платформы, на которых это время существование будет максимальным.
- примитивность – простота строения подобных дорвеев.

После отбора по представленным критериям в общем списке оказывается конечное значение подходящих хостингов для создания информационных спутников, которые в дальнейшем будут работать в синтезируемой мультиагентной среде.

Критерии оценивания и отбора в зависимости от потребности могут корректироваться.

В процессе создания сайтов, были рассмотрены самые популярные платформы для комфортной работы и выбраны хостинги с наибольшим циклом жизни, например, платформа «Wix».

2.4. Регистрация в выбранной веб-среде для дальнейшего создания

Одним из обязательных требований для создания сайтов является регистрация в выбранном конструкторе, для которой необходимо наличие электронного почтового адреса, созданного на первом этапе.

Процесс регистрации состоит из нижеперечисленных этапов:

– создание сайта, с дальнейшим переходом к окну регистрации;

– создание нового пользователя;

– заполнение полей с электронным адресом, созданным в первом разделе и генерирование пароля, аналогично такому же принципу, что и при регистрации электронной почты.

2.5. Выбор шаблона сайта

Пройдя этап авторизации в среде построения сайтов, открываются возможности воспользоваться шаблонами, которые в дальнейшем определят структуру и вид дорвея.

Выбор шаблона происходит по следующему алгоритмы:

1) переход по ссылке «Создать сайт»;
2) выбор типа шаблона сайта, принимается раздел «пустые»;
3) выбор одностраничного шаблона сайта;
4) перейти по ссылке «Редактировать» - переход в режим создание сайта.

2.6. Наполнение шаблона информацией

Процесс создания информационных спутников должен осуществляться в кратчайшие сроки и, как было указано выше, работать в автономном режиме, что позволяет мгновенно, без вмешательства со стороны своего владельца, выполнять требуемые функции.

Чаще всего они используют такие статистические методы как марковские цепи [1], для создания множества страниц на основе списка ключевых слов и коллекции тематических текстов. Такой подход позволяет без участия человека (что было бы трудозатратно) создавать страницы с уникальным содержимым, не определяющиеся поисковыми системами как дубликаты других страниц.

Самым важным этапом в создании информационных носителей является наполнение сайта полезной информацией, так как все предыдущее были подготовительными этапами.

Алгоритм наполнение сайта полезной информацией состоит из следующих шагов:

- ссылаясь на исходные данные, а именно на продукт с которым работаем, заполняем строку с названием сайта, выбрав «редактировать» и ввести название «In Jet-2»;

- перед выбором и загрузкой фотографии с продуктом необходимо произвести запрос на исходном многостраничном ресурсе [11]. Попав по ссылке на исходный сайт, в поисковой строке вводится запрос «мелкосимвольная маркировка». В результате предоставляется доступ к описанию, характеристикам, фото и видео по маркировочному оборудованию.

- выбор фото или картинки с указанным продуктом, которая будет отображаться на сайте;

- сопровождение визуализации объекта несколькими ключевыми фразами, описывающие маркировочное оборудование;

- заполнение сайта описанием о способе нанесения маркировки из исходного многостраничного ресурса;

- загрузка фотографии продукции, с которой может работать каплеструйный принтер;

- представление основных параметром и возможностей промышленного каплеструйного маркировочного принтера Mark InJet-II .

- указание самых основных и ключевых качеств модели в сравнении с существующими прототипами;

- размещение на сайте контактного мобильного номера телефона для связи с виртуальным приборостроительным предприятием;

- переход по ссылке «Опубликовать», что в свою очередь является заключающим этапом в создании дорвея.

Вывод

Правильное применение рассмотренного в данной статье метода с привлечением веб-ориентированных информационных спутников, которые совместно с основным веб-ресурсом образуют мультиагентную среду, позволяет с минимальными затратами денежных ресурсов обеспечить конъюнктуру рынка, конкурентоспособность изделий и их сбыт, который определяет востребованность производства и формирует портфель заказов виртуального предприятия.

СПИСОК ЛИТЕРАТУРЫ

1. Doorway [Электронный ресурс], – Режим доступа: https://ru.wikipedia.org/wiki/ (05.02.2017).
2. Дорвей [Электронный ресурс], – Режим доступа: http://wiki.rookee.ru (05.02.2017).
3. Гаврилова Т. А. Базы знаний интеллектуальных систем / Т. А. Гаврилова, В.Ф. Хорошевский. – С.Пб.: Питер, 2000. – 384 с.
4. Шостак И. В. Информационная технология автоматизации технологической подготовки виртуального производства предприятия / И. В. Шостак, В. Н. Павленко, А. П. Собчак, О. И. Попова // Системи управління, навігації та зв'язку. - 2016. – Вип. 3 (39). – С. 118-125.
5. Панов А. Сайты-сателлиты: угроза или помощь проекту? [Электронный ресурс] / А. Панов. – 2014. – Режим доступа: http://panov-a-w.ru/stati/sajty-satellity-ugroza-ili-pomosch.html (05.02.2017).
6. Printer Mark InJet-II, [Электронный ресурс], – Режим доступа: https://gladiator1994max.wixsite.com/markinjet (05.02.2017).
7. Printer Mark InJet-II, [Электронный ресурс], – Режим доступа: http://markinjet.ukit.me (05.02.2017).
8. Mark InJet-II, [Электронный ресурс], – Режим доступа: http://http://markirovka.ukit.me (05.02.2017).
9. Mark InJet-II [Электронный ресурс], – Режим доступа: http://markprodukt.ukit.me (05.02.2017).
10. Mark InJet-II [Электронный ресурс], – Режим доступа: http://http://marksimwol.ukit.me (05.02.2017).
11. KIATON [Электронный ресурс], – Режим доступа: www.KIATON.com.ua (05.02.2017).

REFERENCES

1. Doorway, available at: https://ru.wikipedia.org/wiki (last accessed February 5, 2017).
2. Dorvej [Doorway], available at: http://wiki.rookee.ru (last accessed February 5, 2017).
3. Gavrilova, T.A. and Khoroshevskiy, V.F. (2000), Bazy znaniy intellektual'nykh *system* [Knowledge bases of intellectual systems], Piter, St. Petersburg, 384 p.
4. Shostak, I.V., Pavlenko, V.N., Sobchak, A.P. and Popova, O.I. (2016), "Informatsionnaya tekhnologiya avtomatizatsii tekhnologicheskoy podgotovki virtual'nogo proizvodstva predpriyatiya" [Information technology automation technology preparation of virtual enterprise], Systemy upravlinnya, navihatsiyi ta zv'yazku, PNTU, Poltava, pp. 118-125.
5. Panov, A. (2014), Sayty-satellity: ugroza ili pomoshch' proyektu? [Satellites: threat or help with the project?], available at: http://panov-a-w.ru/stati/sajty-satellity-ugroza-ili-pomosch.html (last accessed February 5, 2017).
6. Printer Mark InJet-II, available at: https://gladiator1994max.wixsite.com/markinjet (last accessed February 5, 2017).
7. Printer Mark InJet-II, available at: http://markinjet.ukit.me (last accessed February 5, 2017).
8. Mark InJet-II, available at: http://markirovka.ukit.me (last accessed February 5, 2017).
9. Mark InJet-II, available at: http://markprodukt.ukit.me (last accessed February 5, 2017).
10. Mark InJet-II, available at: http://marksimwol.ukit.me (last accessed February 5, 2017).
11. KIATON, available at: http://www.KIATON.com.ua (last accessed February 5, 2017).

Надійшла (Received) 14.02.2017
Прийнята до друку (Accepted for publication) 30.05.2017

Метод синтезу мультиагентного веб-орієнтованого середовища на основі інформаційних супутників

І. В. Шостак, А. П. Собчак, О. І. Попова, М. О. Міщенко

Мета. Створення сприятливої веб-орієнтованого середовища за рахунок продукування агентів - супутників у вигляді дорвеев, що дає можливість підвищити інформативність об'єкта виробництва віртуального приладобудівного підприємства. **Результати.** У статті розглянуто метод підвищення інформативності продукції Віртуального Приладобудівного Підприємства (ВПП) з використанням інформаційних супутників, на основі синтезу мультиагентного веб-орієнтованого середовища за рахунок продукування агентів – супутників у вигляді дорвеїв. Розкрито детальний поетапний алгоритм створення таких інформаційних супутників у вигляді сайтів дорвеїв, з основним ухилом на інформативність. Представлена основна проблема, пов'язана з втратою виробничого потенціалу, а також її рішення із застосуванням запропонованого методу. **Висновки.** Метод дозволяє не тільки пристосувати устаткування до ринку шляхом його своєчасної модернізації, а також дозволяє з мінімальними витратами грошових ресурсів забезпечити кон'юнктуру ринку, конкурентоспроможність виробів та їх збут, який визначає затребуваність виробництва і формує портфель замовлень.

Ключові слова: інформативність, веб-орієнтоване середовище, конкурентоспроможність, затребуваність.

Method of multiagent web-oriented environment synthesis based on information satellites

I. Shostak, A. Sobchak, O. Popova, M. Mishchenko

Purpose. Creation of a favorable web-oriented environment through the production of satellite agents in the form of doorways, which makes it possible to increase the information content of the object of production of a virtual instrument-making enterprise. **Results.** In the article the method of increasing the informative value of the Virtual Instrument Making Enterprise products using information satellites is considered, based on the synthesis of a multi-agent web-based environment through the production of satellite agents in the form of doorways. A detailed step-by-step algorithm for creating such information satellites in the form of doorway sites, with a basic emphasis on informativeness, is disclosed. The main problem related to the loss of production potential, as well as its solution using the proposed method, is presented. **Conclusions.** The method allows not only to adapt equipment to the market by means of its timely modernization, but also allows to provide market conditions, competitiveness of products and their sale with minimum expenses of monetary resources, which determines the demand for production and forms a portfolio of orders.

Keywords: informative, web-oriented environment, competitiveness, demand.

Information systems studying

UDC 621.391 **doi: 10.20998/2522-9052.2017.1.04**

R. Zhyvotovskyi, S. Petruk

Central research Institute of weapons and military equipment of armed forces of Ukraine, Kyiv, Ukraine

JUSTIFICATION OF PERSPECTIVES DIRECTIONS OF UPGRADING RADIOCOMMUNICATION SYSTEMS OF ARMED FORCES UKRAINE

Aim. In the article explore issues and directions of the innovative approach to the development of automated complexes and radio communication facilities for special purposes. During the research it was determined that the effectiveness of the military radio communication system would be improved by facilities of modernization of the latest facilities of radio communication of foreign production or by improving the existing system of military radiocommunication. Presented directions and features of leading research and development works for the improvement and development of channels and systems of military radio communication, the creation of nodes and centers of radio communication, automated complexes and radio communication of special purpose were presented. Was given generalized approach to the construction of the system of automated radio communication, antenna-hardware complexes, software and hardware complexes of radio prediction and planning of use of radio frequency resource. **Conclusions.** According to the results of the conducted researches, conceptual decisions about the system engineering and technological reconfiguration of the existing radio communication system are proposed, which will allow to work in the automated radio networks as part of the radio centers of information and telecommunication units; to unify the facilities and complexes of radio communication with facilities of communication and automation, to provide counter work with the equipment of the old park, as well as to construct a fundamentally new radio communication system with the ability to calculate the planning and forecasting of the radio frequency resource.

Keywords: complex and device of radio communication, antenna-device complex of adaptive radio communication, systems radioprediction and planning radio frequency resource.

Formulation of problem

Analysis of recent research and publications. Improving radio communications have special significance in connection with number of issues that appeared during antiterrorist operation (ATO).

Base of improvement existing radio system should make automated transceiver two-way radio systems and field stationary radio centers of new generation developed on new element base with advanced technology radioaccess that enable creation of sophisticated and flexible structures.

Research perspectives of development of radio communications systems conducted to ensure sustainable, reliable and timely information to different users bring in conditions of natural and artificial destabilizing factors, which is actual scientific task.

Scientific and technological task of research should be resolved within framework of concept of a unified automated digital communication system (UADCS) special purpose, which based on reference model of open systems interconnection OSI (open systems interconnection basic reference model) and modern telecommunication technologies based on using radio with programmable parameters (SDR - Software Defined Radio).

Objective of article is scientific justification for choosing directions of radio communication systems of special purpose taking into account existing and future approaches to construction of radio and reconfigurable automated systems.

Systems of military radio communication should provide the necessary information resource of users for the purpose of their integration into information-control systems of the armed forces, as shown in fig. 1 for the US armed forces. According to recommendations MSE-R for radio with programmable parameters (SDR) include transmitter and/or receiver, which use technology of using software install or change working frequency settings, including in particular frequency range, modulation type or output power except changing operating parameters used in normal course of pre-work preset radio unit, according to particular specification or standard system [1].

Main directions of research, which conducted at creating automated digital radio system:

complex approach in creation, implementation and operation advanced networks, radio systems and radio communications;

realization technology design, which provide, finally, networking, radio channels and radio communications systems that operate consistently in conditions of different kinds of destabilizing factors;

perform not only traditional requirements of creation “set” of technical devices, combined in some information and control network and implementation of main objectives for which creates radio network or radio communication - namely, ensuring reliable, noise-immune, secured and continuous radio 'communication;

development and implementation methods of structural and parametric synthesis channels, receiving, transmitting antenna and hardware adaptive radio communication systems and equipment for radio centers;

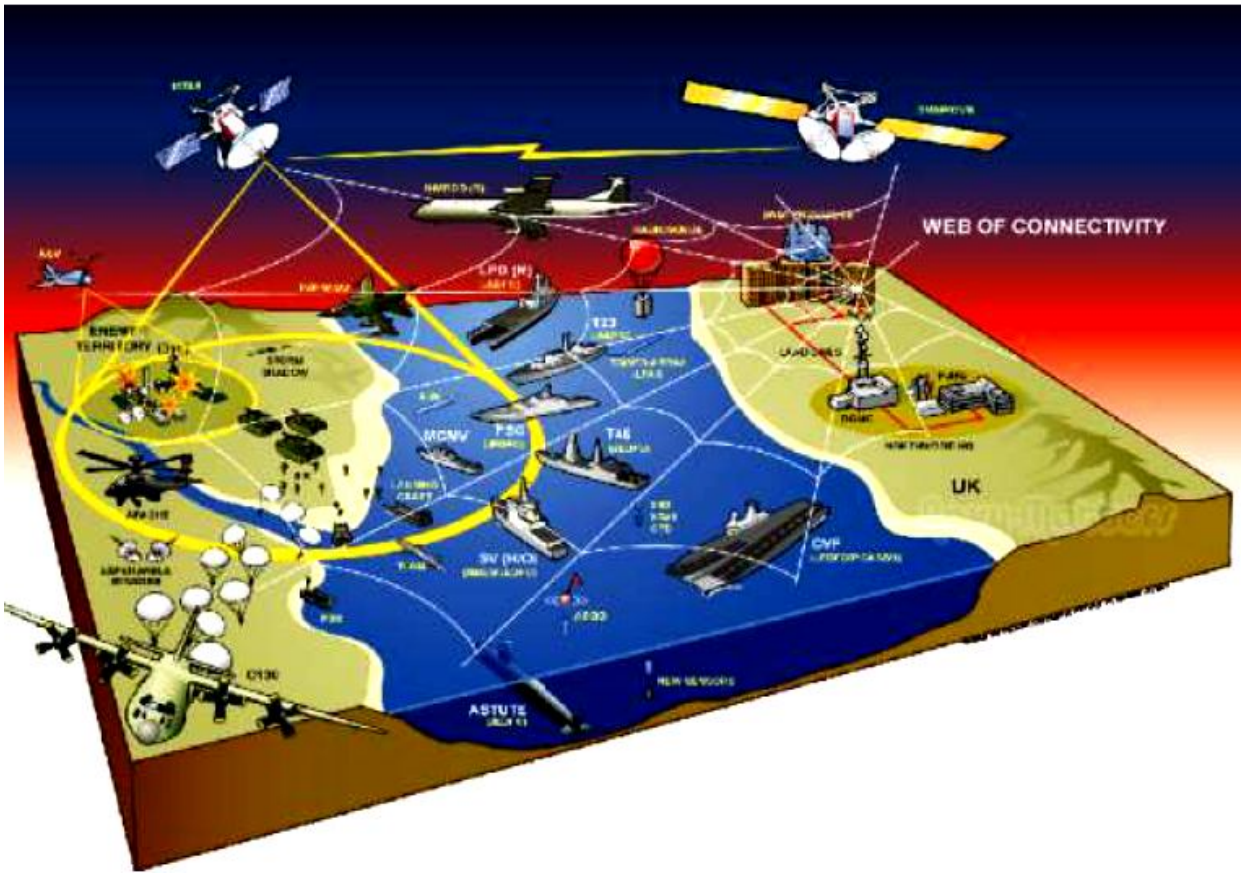


Fig. 1. Structure of the combined information and control system

development and implementation of technology providing necessary tactical and technical characteristics at all stages of life cycle of networks, channels, systems and radio communications.

Task solution

1. Systems (channels) radio communication

Main directions of research in field of radio communications shall including development of principles of construction special purpose radio systems using different levels to ensure structural stability of wireless communication networks to action of enemy countermeasures (REW) and devices of destruction through:

combination of direct and switched radio low and medium lengths that enable transmission of information to bypass nodes have failed and radio lines because of weapons, REW and violation of propagation;

integrated using radio spectrum in HF, UHF bands, which allows to organize radio using different propagation mechanisms - with HF reflection from ionosphere - UHF with display of sporadic layer in conditions of undisturbed environment and terrestrial waves in HF, UHF bands.

Achieving immunity, security and capacity of networks and channels should be based on:

multiparameter adaptation of organization, maintenance and restoration of wireless communication (frequency, speed and transmission mode, spatial orientation of directional diagrams resettlement (antenna feeders antenna-feeder devices);

compensation of powerful natural and intentional interference, and preventing their emission of radio devices;

packing information and dynamic routing packets of information based load and driving conditions [5, 6];

optimal combination of direct and error correction procedures supplementary request ARQ (Automatic Repetition Query) during transmission using effective methods of coding [5, 11];

radio control connectivity and quality radiolines based on cognitive radio (using probing and test signals predicting propagation conditions, employment and evaluation frequency range of signal-interference environment;

Using digital methods for forming and processing of promising optimal signal-code designs that provide high-speed data, without compromising noise immunity parameters [5, 6];

functional independence of radio communication networks of external synchronization (navigation systems) for autonomous functioning in defeat these systems using efficient algorithms entry and support of high-matching-based generators.

While creating radio systems must be provided to develop tactical and technical requirements for radio systems for various purposes, operating in difficult conditions-interference environment, including action REW, which include:

wide requirements for construction and deployment territorial networks, channels and wireless communication systems, including general characteristics and quality indicators of networks and channels;

specifications interoperability of radio communications transport networks, access networks, services, communication services, automated control system of communication, information security and systems (logistics, power supply, network clock synchronization, numbering and addressing), providing taking into account implementation of operational requirements imposed by customer.

Simulation of networks and channels radiocommunication study principles of design and development methods for their implementation should include:

description and typical networking scheme, the complex of radio communication units of various ranks;

complex issues of information security and protection of wireless communication networks of technical devices intelligence;

proposals for uniform joints, protocols and interfaces of network elements network radio.

comparative performance assessment schemes (options) of radio communication;

assessment of probability-time characteristics would bring networks and radio communication channels in terms of destabilizing factors;

development of programs and methods of bench and field tests to verify that parameters of (complex) radio communication requirements of tactical-technical task (TTT) in their development.

2. Creating units and radio communication centers

Implementation of the transition from traditional building radio unit, main task of which was to set pairing devices interconnected via communication devices, to develop promising equipment which incorporates wide functions.

Main directions of research in field of radio communication units and centers should include development of principles of construction of radio centers for various purposes in order to:

Modular building unified radio centers of various ranks, something provide increasing functionality by breeding standard modules;

group using radio in place of their existing assignment radio direction;

digitally automated topology formation and reconfiguration of radio networks;

shuttle spaced elements distributed radio centers based on standard interfaces and advanced telecommunication technologies;

ensure transition of interaction in diverse joints (for data lines and for line management) in unified solution based on one of sheets Ethernet that will greatly simplify task combination of hardware and transfer it from area of software and hardware solutions in area of software problems while increasing it's flexibility and scalability [2-6].

3. Complex and radio communications devices

Main areas of research in field of radio communications systems and should include development of principles of construction radio devices for various purposes in order to:

establishment of receiving, transmitting, antenna and hardware systems and radio frequency systems support;

building complex and radio communications systems based on concept of SDR (Software Defined Radio) and SCR (Software Cognitive Radio), which allow lifecycle framework to develop hardware device functionality and efficient using radio frequency spectrum through improved software that provides different, including new algorithms;

creating complex and radio communications systems, which provide software and hardware platform performance networks, wireless communication features of physical, data link and network levels and management of networks - and transport, session representative and applied levels.

Main tasks that must be addressed in course of research in creating systems and radio communications as part of functions of physical layer are:

formation and spectral energy efficient signals, including signals with extended range ("fast" and "slow" pseudo-restructuring operating frequency) noise signals and their combinations;

provide necessary energy potential of radio channels by varying frequency, speed and power transfer, including by drafting capacity in transmission antenna and hardware;

implementation of spatial configuration diagram orientation of receiving antenna and hardware from direct sources of interference, drawing power transmission antenna and hardware in space;

providing spatial and polarization compensation is not deliberate and intentional interference, and their radiation transmitting means [3, 4,9].

Main scientific and technological challenges in creating systems and radio communications in functions of link layer are:

frequency control and energy resources (adaptation speed, power transmission diagram form directional antennas);

implementation of noise-immune coding signals based on the two-level coding and application turbo coding;

providing multiple access to common time-frequency resource network based on code and the time-frequency separation.

Main objectives of research in creating systems and radio communications as part of functions of network include:

providing connections to network elements of transport network unified automated communications network;

implementation of necessary safety information exchange official radio communications network management procedures on basis of adaptation, routing and signal noise immunity;

integrated management of time-frequency and network energy resources based on active and passive analysis of signal-interference environment, using results of long-term forecasting and operational conditions for radio.

4. Antenna-device complexes

Development of antenna-devise complex, which enable noise-immune receiving information simultaneously on multiple frequencies operating range of specified number of geographically distributed correspondents based on formation of controlled spatial diagram orientation specific forms of implementation required values of sensitivity to electromagnetic field, survivability and reliability in terms of different kinds of destabilizing factors [4-8].

5. Software-devise complexes of radio prediction and planning radio frequency resource

While creating software-device complex of radio prediction and using frequency resources should focus on design:

automated networks operating radio prediction;

models of calculating characteristics of wave propagation in HF range, including using results of probing the ionosphere;

dynamic models of action natural and intentional interference;

software and methodological support for long-term, short-term and operational radio predictable range of usable frequency;

evaluation of statistical parameters obstacle levels in real time.

Was made comparative assessment interference environment in several lists of frequencies from issuing recommendations about frequency with the lowest noise level, and quality control admission on single operating frequency to desired mode.

Implementing radio dispatching functions in information and telecommunication communication centers in appointment operating frequency of radio communications, including:

visual inspection of whole list of backup frequencies in their current state;

frequency assignment reporter considering its usable range of frequencies on current time and noise level;

returning frequency (group of frequency) reserve list;

control radio season transition from one to another;

receiving of given frequency-time program control and marker signals;

receiving and processing results of determine frequency bands usable on their basis for using comparison of noise levels at different frequencies.

Feature software-device complex of radio prediction and planning radio frequency resource, which developed:

providing early assessment and operational characteristics of radio propagation and-interference environment;

recommendations for appointment operating frequencies, as optimal in terms of propagation and minimum level of noise;

planning using radio frequency resource information and telecommunication nodes of communication;

placement equipment should be not result in addition to capital expenditures;

ensuring continuous monitoring and continuous interference environment in several lists of frequencies;

providing automated control over allocation of frequency resources;

delivery in real-time recommendations of choosing operating frequencies on several criterial;

simultaneous using several data stations probing ionosphere.

Ensuring sustainability of channels and radio communications systems:

develop models assess stability of radio communication channels, radio wave propagation characteristics and interference different parts of wavelengths;

study ways and technical solutions to ensure the stability of the antenna feeder devices and protection electronic equipment from electromagnetic radiation of natural and artificial;

development requirements for protection radio equipment and antenna-feeder devices from electromagnetic radiation of natural and artificial:

selection (based on current regulatory and technical documents and literature), analysis and forming initial data on parameters of electromagnetic radiation of natural and artificial origin to develop requirements for safety equipment of radio and antenna-feeder devices from electromagnetic radiation according to the requirements for resistance (survivability) objects using;

development of tactical-technical task on creation equipment of protection radio devices and antenna-feeder devices from electromagnetic radiation of natural and artificial origin.

Assess the stability of settlement radio and antenna-feeder devices to electromagnetic radiation of natural and artificial accordance with their development (without equipment protection against electromagnetic radiation and their use):

calculation of estimates of expected parameters of voltage, current and energy induced in the antenna feeder devices and paths electromagnetic radiation of natural and artificial;

making estimated assessment of stability of radio, antenna and feeder protection equipment and the action of voltage, current and energy that in paths of aerial devices and feeders electromagnetic radiation of natural and artificial;

develop proposals on building schemes equipment protection against electromagnetic radiation of natural and artificial and experimental verification of radio parameters (selection of components used in equipment protection against electromagnetic radiation, allowing for the construction of reception and transmission channels of radio and antenna-feeder and the expected parameters of reduced voltage, current and energy);

develop proposals on building schemes equipment protection against electromagnetic radiation;

experimental verification of conformity of radio parameters (coefficient transmission, coefficient creeping wave amplitude-frequency and phase-frequency characteristics in operating frequency range) of individual units that make up equipment protection against electromagnetic radiation protection equipment and whole set of their development requirements. Development of programs and methods of bench and field tests to verify that parameters of equipment protection against electromagnetic radiation of natural and artificial requirements of tactical-technical task in their development: development of programs and methods of bench and field tests to verify that the parameters of the equipment protection against electromagnetic radiation requirements of TOR their development;

develop programs and methods of bench testing and field verification to ensure necessary resistance to electromagnetic radiation transmit and receiving radio tract;

justification required storage of specific types of control-measure equipment for making bench testing and field equipment protection against electromagnetic radiation;

justification required storage of specific types of control-measure equipment for bench testing and field verification to ensure necessary resistance to electromagnetic radiation transmit and receive radio tract.

Conclusion

In article directions of scientifically based systems (networks, channels), units and centers of radio communication, antenna and hardware, and also recommendations for creating software-device complex of radio prediction and planning of radio frequency resource.

Proposed solutions for system integrators and technology reconfiguration of existing radio system allow to:

1. Ensure working in automated radio networks consisting of stationary radio centers of information and telecommunication units and field information and telecommunications nodes, while providing automatic maintenance provider.
2. Unify devices and complex of radio communication with devices of communications and automation.
3. Ensure common (counter) work with old fleet of radio as stationary and field communication centers of command and control;
4. Ensure functioning and management of receiving and transmitting systems directly from device and remotely.
5. To provide automatic retransmission signal according to the address on choosing optimal correspondent of radio waves passing.
6. Build radically new, distributed type and technologically flexible automated system of radio communications.

Future research should consider development of hybrid information technology to improve efficiency of military radio communications systems.

REFERENCES

1. Text of report MSE-R SM.2152 (2009), available at : http://www.itu.int/publications/R-REP/en (last accessed March 02, 2017).
2. Savitskiy, O.K., Meshalkin, V.A. and Suhotepliy, A.P. (2017), *Technological fundamentals of upgrading networks decameter radio communication special interest of consumers*, available at : http://mashtab.org/company/massmedia/articles/technological_fundamentals_of_upgrading_decametric_radio_networks_for_the_benefits_of_special_users (last accessed March 02, 2017).
3. MIL-STD-188-141B. Interoperability and performance standards for medium and high, frequency radio systems. DOD interface standard. 1 March 1999/ DoD USA (1999), available at : http://hflink.com/standards/MIL_STD_188-141C.pdf (last accessed March 02, 2017).
4. Savitskiy, O.K., Meshalkin, V.A. and Suhotepliy, A.P. (2012), System-technical principles of construction of advanced devices and complexes of radio communication of special networks, available at : http://mashtab.org/company/massmedia/articles/sistemotehnicheskie_principy_postroeniya_perspektivnyh_sredstv_i_kompleksov_radiosvyazi_special_nyh_setej (last accessed March 02, 2017).
5. Kuzmin, B.I. (1993), "Concept of building packet radio networks in range DKMV-MV", *Electrocommunication*, No 5, pp. 11 -13.
6. Kaplin, E.A. (1994), "Principles of construction and operation of packet radio networks in non-stationary messaging environments", *Electrocommunication*. No 10.
7. Gurskyi, T.G., Zhuk O.G., Krivenko O.V. and Shyshatskyi A.V. (2016), "Directions of improvement of facilities of radio communication with pseudorandom reconstruction of the working frequency" *Collection of scientific works of Military*

Institute of Telecommunications and Informatization, Publication 1, pp. 25-34, available at: http://www.viti.edu.ua/index.php?view=coll_2016_1 (last accessed March 02, 2017).

8. Kuvshinov, O.V., Lutov V.V. and Zhuk, O.G. (2017), "Analysis of ways to increase the secrecy of broadband systems of military radiocommunication ", *Collection of scientific works of Kharkiv National Air University Forces*, No. 1, pp. 24-28, available at: http://www.hups.mil.gov.ua/periodic-app/article/17488 (last accessed March 02, 2017).
9. Shyshatskyi, A.V., Lutov V.V. and Zhuk, O.G. (2015), "Analysis of ways of increasing the efficiency of radio communication systems with orthogonal frequency multiplexing", *Arms and military equipment* : Scientific and technical journal, CSIAM AF of Ukraine, Kyiv, No 4(8), pp. 22-26, available at : http://nbuv.gov.ua/UJRN/ovt_2015_4_5 (last accessed March 02, 2017).
10. Slusar, V (2005), "Systems MIMO: principles of construction and signal processing", *Electronics: Science, Technology, Business*, No 8, pp. 52-58, available at: http://www.electronics.ru/files/article_pdf/0/article_974_409.pdf (last accessed March 02, 2017).
11. Shyshatskyi, A.V., Olshanskyi, V.V. and Zhyvotovskyi, R,M. (2016), "Algorithm of the choosing working frequencies for facilities of military radio communication in the conditions of intentional interference", *Systems of armament and military equipment*, No. 2, pp. 62-66, available at: http://www.hups.mil.gov.ua/periodic-app/article/16881 (last accessed March 02, 2017).

Надійшла (received) 16.03.2017
Прийнята до друку (accepted for publication) 23.05.2017

Обґрунтування перспективних напрямків розвитку системи радіозв'язку Збройних Сил України

Р.М. Животовський, С.М. Петрук

Мета. У статті досліджуються питання та напрямку інноваційного підходу до розвитку автоматизованих комплексів і засобів радіозв'язку спеціального призначення. У ході проведених досліджень визначено, що підвищити ефективність системи військовому радіозв'язку можливо шляхом переоснащення новітніми засобами радіозв'язку закордонного виробництва або проведенням удосконалення існуючої системи військовому радіозв'язку. Представлені напрямки й особливості проведення науково-дослідних і дослідно-конструкторських робіт з удосконалення та розробки каналів і систем військовому радіозв'язку, створення вузлів і центрів радіозв'язку, автоматизованих комплексів і засобів радіозв'язку спеціального призначення. Наведений узагальнений підхід до побудови системи автоматизованого радіозв'язку, антенно-апаратних комплексів, програмно-апаратних комплексів радіопрогнозування та планування використання радіочастотного ресурсу. **Висновки**. За підсумками проведених досліджень запропоновані концептуальні рішення по системотехнічній та технологічній реконфігурації існуючої системи радіозв'язку, які дозволять забезпечити роботу в автоматизованих радіомережах у складі радіоцентрів інформаційно-телекомунікаційних вузлів; уніфікувати засоби та комплекси радіозв'язку з засобами зв'язку та автоматизації, забезпечити зустрічну роботу з апаратурою старого парку, а також побудувати принципово нову систему радіозв'язку з можливістю розрахунків планування та прогнозування радіочастотного ресурсу.

Ключові слова: комплекси й засобу радіозв'язку, антенно-апаратні комплекси адаптивного радіозв'язку, комплекси радіопрогнозування та планування використання радіочастотного ресурсу.

Обоснование перспективных направлений развития системы радиосвязи Вооруженных сил Украины

Р.Н. Животовский, С.Н. Петрук

Цель. В статье исследуются вопросы и направления инновационного подхода к развитию автоматизированных комплексов и средств радиосвязи специального назначения. В ходе проведенных исследований определено, что повысит эффективность системы военной радиосвязи возможно путём переоборудования новейшими средствами радиосвязи зарубежного производства либо проведением усовершенствования существующей системы военной радиосвязи. Представлены направления и особенности проведения научно-исследовательских и опытно-конструкторских работ по усовершенствованию и разработке каналов и систем военной радиосвязи, создания узлов и центров радиосвязи, автоматизированных комплексов и средств радиосвязи специального назначения. Приведен обобщенный подход к построению системы автоматизированной радиосвязи, антенно-аппаратных комплексов, программно-аппаратных комплексов радиопрогнозирования и планирования использования радиочастотного ресурса. **Выводы**. По итогам проведённых исследований предложены концептуальные решения по системотехнической и технологической реконфигурации существующей системы радиосвязи, которые позволят обеспечить работу в автоматизированных радиосетях в составе радиоцентров информационно-телекоммуникационных узлов; унифицировать средства и комплексы радиосвязи со средствами связи и автоматизации, обеспечить встречную работу с аппаратурой старого парка, а также построить принципиально новую систему радиосвязи с возможностью расчёта планирования и прогнозирования радиочастотного ресурса.

Ключевые слова: комплексы и средства радиосвязи, антенно-аппаратные комплексы адаптивного радиосвязи, комплексы радиопрогнозирования и планирования использования радиочастотного ресурса.

UDC 621.391 **doi: 10.20998/2522-9052.2017.1.05**

I. Romanenko, A. Shyshatskyi

Central research Institute of weapons and military equipment of armed forces of Ukraine, Kyiv, Ukraine

ANALYSIS OF MODERN CONDITION OF MILITARY RADIOCOMMUNICATION SYSTEM

Aim of the article is to conduct an analysis of military communications systems that were used in the area of conducting antiterrorist operation in the Donetsk and Lugansk regions. The article analyzes the modern facilities of military communication, namely: military radiocommunication systems, military satellite communication systems, military systems of radio relay and tropospheric communication. The advantages and disadvantages of each type of communication are considered, the causes of their occurrence were considered, and the ways of solving these reasons in the future were substantiated. An analysis of the main technical characteristics of military communication systems, opportunities, advantages and disadvantages has been conducted. The perspectives for the development of military communication systems have been determined on the basis of the analysis of the military facilities of communication used in the article, which are used in the region of the antiterrorist operation in the Donetsk and Lugansk regions. To eliminate the problematic issues mentioned in the article, the authors of the article are proposing to launch their own military satellite for the needs of the Armed Forces of Ukraine; To develop new models of military communication; To conduct deep modernization of the existing radio stations, command-staff cars, radio relay and tropospheric stations; To integrate telecommunications equipment adopted in the last years into a single information space of the Armed Forces of Ukraine, as well as to reach agreement with representatives of leading telecommunication equipment manufacturers regarding the transfer of technologies and deployment of production in the territory of Ukraine.

Keywords: radiocommunication system, radiocommunication, radio-electronic suppression, intentional interference.

Introduction

Since beginning of armed aggression against Ukraine in beginning 2014 as Armed Forces of Ukraine in general, and forces of connection were are not ready due to effective warfare. Principles of building communication systems, laid in Soviet Union, were outdated and mostly involved using analog equipment.

Because of that, for providing effective control by anti-terrorist operation (ATO) was necessary to modernize communication systems, including radiocommunication systems [1]. Then in article to radiocommunication classified all types of communication, in which data transmission carried by using radio waves, that is actually radio (HF and UHF) and trunking, radio relay, tropospheric, satellite.

So *purpose of the article* is analysis of modern condition of systems and military radiocommunication, determination way of upgrading and perspectives of development.

Presentation of main material research

1. UHF radiocommunacation

Radio communication old park have large dimensions and weight, easy monitored and supersession by device of electronic warfare (EW) enemy. It's UHF radio stations R-159, R-105, R-111, R-123, and others. After beginning of ATO for providing communication directly on battlefield priority task was providing portable radio for forces with support digital mode and classifying (masking) language.

Domestic UHF radio stations produced by "Telecard-device", which was taken into armament (P-002, P-005, P-030, with power 2, 5 and 30 W) [2], a number of reasons absent in forces. They work in range of working frequencies 30-110 MHz, support the ability to disguise information and mode of frequency hopping spread spectrum (FHSS) at speed 312.5 h/sec (maximum number of nominal operating frequency in FHSS mode - 256), can transmit data at speeds 16 kbit/sec. Main disadvantages stations "Telecard-device" based on these characteristics: lack of cryptographic information protection; limited number of frequencies in FHSS mode, which make SRC more vulnerable to devices of radio technical intelligence (RTI) and enemy devices of electronic low warfare; data rate. Typical plan of communication organization in area of realization ATO exampled on fig. 1. Using mobile phones as it has shown and experience of carrying ATO is dangerous due to high probability of interception by enemy, determine locating forces, and potentially incoherent withdraw mobile communication systems down if it's use for command and control forces [1].

Based on lack of modern small portable radio stations, was decided to use trunking communication equipment "Mototrbro" production company "Motorola", which characterized by high quality and functionality, support digital mode and provide cryptographic information protection.

Trunking communication is major link in tactical management. It allows to provide link in motion directly on battlefield.

Main equipment "Mototrbo": DP 4800 portable radios (with screen and keyboard), DP 4400 (without screen and keyboard), car radios DM 4600, repeaters DR 3000 [4].

It should be noted that National Guard of Ukraine also uses trunking communication equipment "Mototrbo", but in the higher frequency range (403-470 MHz) [1]. Interaction organized by several radio stations commanders to units that perform tasks together or by creating a gateway with two car stations [1, 3].

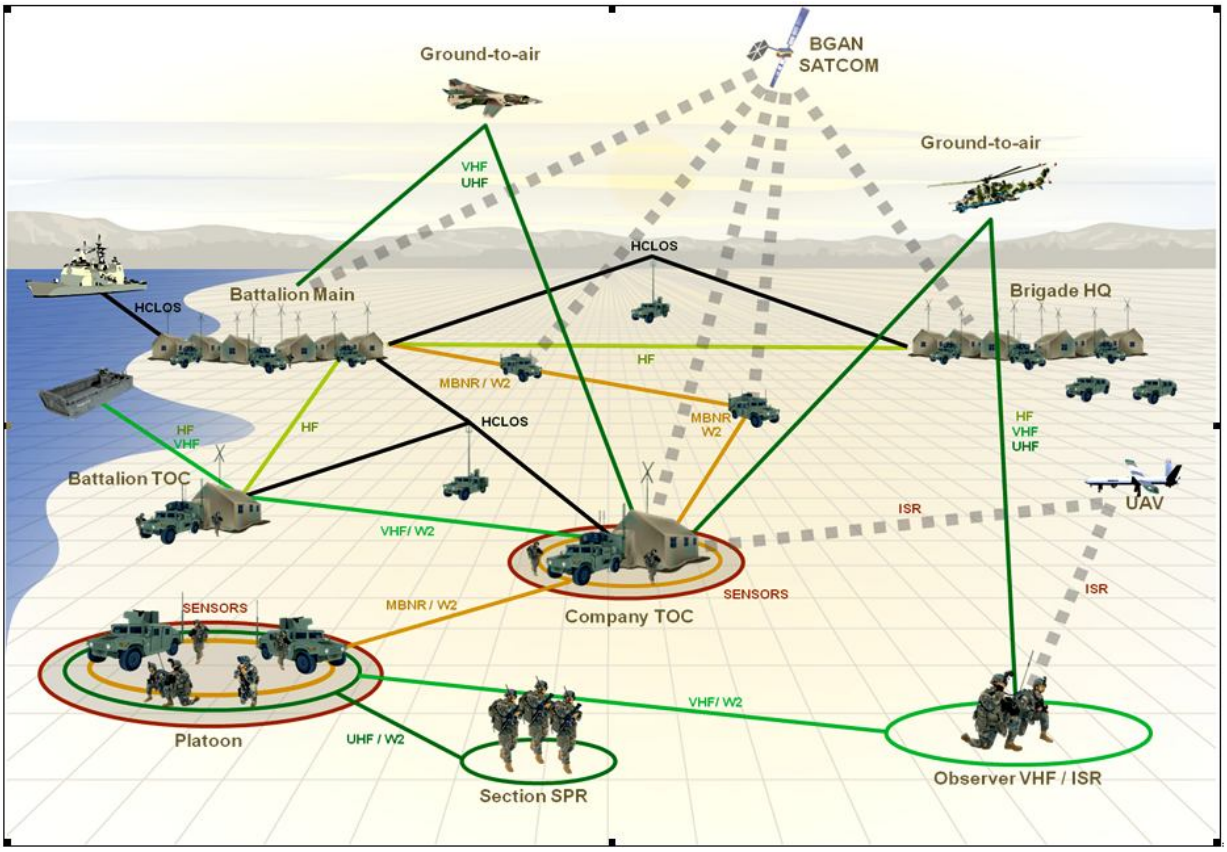


Fig. 1. Typical plan of communication organization in area of realization ATO

Radio stations, depending on configuration of the channel can work through the repeater, and directly among themselves (in the mode of direct communication). Repeater network simultaneously transmits two information channels by dividing the time of distribution channels.

Presence of transponder enables following approximate values communication range [1, 3] between portable stations 15-20 km and more, by car stations - up to 30-40 km and more. At the same time, direct communication channels for portable stations, range is usually no more than 5-7 km. It should be noted, that the communication range is determined by terrain, lifting height repeater antennas, antenna type. When repeater place site in air, such as in an airplane, communication range can be up several hundred kilometers. Well proven in planning trunking communications program that can be used to calculate coverage repeater, posted on the website of Canadian Institute of Telecommunications [4].

Mode of working system "Mototrbo", which used in Armed Forces: direct communication; because of one independent relay (conventional mode);

IP site connect, which provides up to 15 repeaters combined into single network using IP network. Communication range is determined by topology of IP network can theoretically be arbitrarily large.

Also it used in some cases, in single situation, mode Capacity Plus, which provides for increasing channel capacity convertive mode through using multiple (up to 8 voice) repeaters placed along and interconnected through the switcher (switch). As one repeater provides 2 channels, the 8 transponders – 16 channels. Now state of field-communication center in mechanized battalion includes following equipment: Repeater DR 3000 - 1; DM 4600 - 7; DP 4800 - 10; DP 4400 - 70.

Repeater can work on 2 antennas (spaced antenna reception and transmission) or one antenna (via duplexer connected to relay). For the first option should be to provide spatial diversity antennas (primarily vertically - at least 2 meters, with the reception antenna is located above and horizontally - as far as conditions permit areas, existing poles and feeder length). Disadvantage of scheme with duplexer is reducing cover (10%) due to additional losses in the filters of the duplexer. In addition, duplexer filters are narrowband (bandwidth about 50 kHz), so change frequency transmission and reception transponder can only be within ± 18.75 kHz the central frequency. Generally, duplexer filters can recustomize in the frequency range with of about 5 MHz, but in the field, this procedure is quite problematic. It need using HF-signal generator and digital spectrum analyzer. These operations are usually carried out before delivery to the troops. Antennas that can be used for repeaters: probe various modifications (usual pin, J-shaped, collinear etc.). And directed type "wave channel". When more larger antenna gain, the narrower working bandwidth which it overlaps.

To deploy antenna masts used hardware from old park storage (P-409, P-419, P-414, P-142N, R-161A-2M et al.) or existing local infrastructure. In addition, to increase communication range of recovery options repeater (or antennas) balloon on unmanned

aerial vehicles, aircraft. The last option is planned for using after leaving district. Debaltseve [1] for communication while moving units and parts, when standard antenna-mast devices are repeaters in collapsed state.

To create appropriate usually use company radio channels of direct communication, battalion and brigade radio network should be created to channel repeater. Brigadier network can be created in several ways:

in IP site connection mode;

through repeater MP brigade in case of radio visibility with car radio stations COP battalions;

organization radio direction separate car radio with highly elevated directional antennas type "wave channel" on battalions repeaters, each time slot which is used for organization radio crews;

Combination of two or even three above mentioned methods, it is possible without increasing the number of radio stations by scanning mode channels.

Repeater in battalion is peer system IP-site connect teams (provided its creation). 1st battalion channel repeater is released under the radio network brigade in IP-site connect, on the 2nd channel organized radio network battalion commander.

Radio Network a lower level as radio interactions, it is advisable to organize channels of direct communication.

Based on the experience of combat employment system "Mototrbo" its benefits to provide radio communication in the background are the following: digital mode;

built-standard encryption key length of 40 bits and possibility of replacing (at extra cost) to 256 bits. Standards ARC-4 and AES-256 can not be used for transmission of confidential information is disadvantage, and at the same time advantage due to lack of strict requirements for using equipment, key documents, in particular, such as for equipment classification;

transponder availability; scan mode channels (radio station can control up to 16 radio while in another mode of reception);

high enough mechanical (impact resistance), moisture and dust (protection class IP 57, portable stations allow immersion in water to depth of 1 m); high speed connection (less than 300 ms).

Main disadvantages equipment "Mototrbo":

obstacle security lack of modes, including FHSS mode. Because of that channels "Mototrbo" can easily be suppressed by instruments of electronic warfare opponent.

Measures that increase the resistance slightly REW are: maximum dispersal of the various radio channels all over range of operating frequencies, creating a "false" radio work using directional antennas;

hardware configuration is only possible using PC, keyboard user station can modify channels;

low speed of transmission data (less 2 kbit/s).

Perspectives UHF radio. Task of providing communications on move, directly on battlefield, generally resolved by trunking communication system "Mototrbo", which has potential to remain in service as backup device of communication and/or at level of junior officers and soldiers. Main device of UHF radio communication must be professional military radio. Examples of such stations is devices of production "Harris", including: RF-7800S in link-division squad, RF-7800V-HH or RF-7850M-HH link platoon-mouth; link battalion, brigade stations should complement external power amplifier and install on the car (armored) basis [5] (applicable, that it will be special command post vehicles (CSV), or retrofitted, modernized CSV of old park).

Today station type RF-7850M-HH in service in limited quantities and using mainly for benefit of Special Operations units and highly mobile airborne troops (AF) [1]. Because of high cost of Harris radios acceptable solution can be procured radios from other manufacturers optimal criterion of "price-quality" such as radio production company "Aselsan" (Turkey) [6].

Watching on high cost of foreign professional military UHF and need of UHF radio in TC, and obviously, in the long term is necessary to establish domestic production VHF radio.

2. UHF radiocommunication

Radiocommunication in range of short waves (HF) has special place in military communication. Main advantage of HF communication is ability to provide radio communication for hundreds and thousands of kilometers without relay signal. This is possible due to ability of radio waves in this range distributed by reflection from the ionosphere towards Earth and vice versa.

Main feature of HF radio line, regardless of the distance between correspondents is that the conditions of propagation of radio waves of certain frequency band by reflection from ionosphere, determined by time of day, season and solar activity.

Disadvantages of HF radio communication are, firstly, low bandwidth communication channels is caused by transience Ionosphere and low frequency HF range capacity, second, dependence on reliability of radio communications on the correct choice of operating frequencies.

Using analog HF radio stations that were and are represented on arms (P-130, P-134, P-140, P-161A-2M) provide reliable, obstacle security and communication closed considerably difficult.

Because HF radio in ATU organized using radio production "Harris": RF-7800H capacity of 20, 150 or 400 watts (Falcon III) and MPR-9600 (Falcon II) power of 20 W and 125 [7, 8].

Backpack (20 watts) radio station replaced P-130m from command post storage (CSV) Soviet production station with external power amplifiers - medium power radio station R-161A or R-140-2M (P-140-0,5). Usually CSV and medium power stations upgraded by installing radio "Harris".

HF radio stations "Harris" brought to battalion (division) inclusive. Because of this, the lowest level of HF radio - radio crews.

Main tasks of HF radio communication: operational organization of communication channels

with senior staff, communication with units that operate in isolation from main forces, relationship with deep intelligence units, backup key information areas on which channels formed lines snap (wired or radio relay) to transport networks or satellite stations.

Analysis of operating HF radio Harris conducted in [9], which systematically issues and suggests possible ways to solve them. One of major shortcomings that complicates HF radio communications is lack of frequency control service.

3. Perspectives of HF radio

Given large number of HF radios Falcon-III and Falcon-II, it is clear that system of military HF radio communication Armed Forces of Ukraine should be built precisely based on equipment.

If decision will take on adoption of HF radio other (including domestic) manufacturers, they should be compatible with existing radio stations “Harris”.

Stations with an external amplifier, and in many cases stations capacity of 20 watts, should be installed as part of CSV upgraded or new CSV own production.

4. Satellite communications

Satellite communications at start of anti-terrorist operation (ATO) was used to limited extent, mostly to link with peacekeeping contingents through leased lines of business, including "Iridium", "Inmarsat". Experience of communication during ATO showed special significance of satellite communications where is no ability to deploy fully functional field communication system. Equipment used in satellite communications link from GS AF of Ukraine to separate (unit block post) including [1].

Detailed full subsystem of satellite communications connected (Fig. 1) ensures stable connection between control point (CP) of all levels of management of Armed Forces of Ukraine and brought to some of company tactical groups and block posts. In absence of own telecommunications satellite subsystems on existing satellite stations make satellite communication terminals and portable satellite communications for commercial purpose (“Tooway”).

Satellite Internet “Tooway” - service provided by Eutelsat throughout Europe via satellite Ka-Sat, positioned in geostationary orbit at position 9 ° SD (83 Ka-band transponders, amount of resource - 20 000 MHz), operating in the Ka-band (20/30 GHz). Ka-Sat satellite is unique because it is designed solely to provide satellite internet “Tooway” satellite using small diameter antennas.

Provider of service “two-way satellite Internet Tooway” SkyLogic company, which provides VSAT Internet access in 26 European countries, including Ukraine. Headquarters is located SkyLogic operator in Italy in Turin. The owner of satellite Ka-Sat 9E is company Eutelsat, France.

According characteristics maximum speed while ensuring access to the Internet on line “up” can be up to 5 Mbit/s on line “down” - up to 20 Mbit/s. Speed that can be achieved in one terminal for military purposes can be up to 5 Mbit/s.

Terminals “Tooway” installed in headquarters machine P-142, P-145 connection and integrated hardware P-258-60K (P-238TK) and used separately. Satellite channels of communication, in first queue created with using modern equipment IP-encryption of domestic production, as well as open, enabled single information environment for benefit of units that carry out tasks in area of ATO [10].

Main advantages of using system Tooway in system of military communications are:

cost of satellite channels in range Ka significantly lower than in lower ranges, in particular, Ku;

comfortable to use and customize terminals, much smaller than in Ku.

Main disadvantages of terminal are:

dependence on communication quality (bit rate) on weather conditions. In Ku band that would not be virtually;

difficult scheme of signal routing (all calls go through main station in Italy and Ukraine get fiber optic lines). Calls from terminal to terminal twojumps because signal delay between subscribers only through propagation of more than 0.5 seconds, which reduces reliability of communication by increasing likelihood of failures in different parts of channel;

inability to use equipment in field (especially low - satellite modem, routers, gateways, telephones, cables and connectors, etc.).

Last disadvantage to some extent remedied by making sets of Mobile Satellite Communications (MSC 1.1), more adapted to using in field, providing reliable operation at temperatures from -10 °C to + 30 °C [11]. Modem, router, VoIP-penstock gateways and battery as backup power source installed in special container with high mechanical and vibration resistance.

Total weight of 24.5 kg kit. 1.1 MSC transported personnel serving his knapsack with two backpacks. In addition, antenna gain MSC both transmission higher by about 1 dB.

Perspectives of satellite communications. Towards development of satellite communications include:

deployment HUB station “Tooway” in Ukraine, which will provide connection simplify and reduce likelihood of failures (increasing reliability of communication);

launch their own satellites and development their own satellite terminals military purposes.

5. Radiorelay and tropospheric communication

Main purpose and tropospheric radio relay stations in system of military communications - creating lines binding to stationary communication centers telephone network, creating line of communication between control points. Number of local digital radio-relay stations (RRS) R-450 produced by “Telecard-device” in service, with capacity of up to 8 Mbit/s is extremely limited. Given high cost and relatively low bandwidth and their subsequent manufacture and supply troops unnecessary.

Recently was adopted by radio relay station R-425S3 (code "Mars") production Ltd. “JSC Olympus’s” (Svetlovodks) which provides transfer rates up to 155 Mbit/s in range of 6,4-7,1 MHz. With using of RRS built backbone communication line along contact line, which is under commissioning. In addition, upgraded hardware of P-414 (P-414MU), which has also entered service includes RRS R-425 with two-way radio equipment 6,4-7,1 MHz band to build transmission lines and 14,4 -15,4 MHz (throughput up to 50 Mbit/s) for construction of transmission lines linking.

Widely spread way to build lines linking using modern equipment wireless (access point Wi-Fi) [1] with directional antennas, such as production of “Ubiquity Networks” with capacity of up to 300 Mbit/s.

At armed forces of communication have also analog PPS type R-409, R-419, R-414, R-410, R-412, in addition, digital TRS P-417MU and P-423-2.

One of the modernization and TRS analog RRS old park is using modems M-Eth-2DSLbis domestic production of "Crocus" [12], which form Ethernet-flow as possible for given width and channel speed. Modem replaces analog hardware interconnect stations and includes inlet tract intermediate frequency (for modulator / demodulator station). Using such modems allow to turn in radio highway bypassing analog to digital equipment channel formation reach speeds of up to several (5-8) Mbit/s.

6. Perspectives of relay and tropospheric communication

Perspectives areas of troposphere communication are:

development of modern RRS and TRS on experience of leading countries, including establishment of small radio relay, tropospheric stations [1, 13] at speed at least 2 Mbit/s over distance of 100 km (with possibility of creating retranslators), analogues of which are armed with advanced countries [14];

modernization analog RRS, TRS by installing digital modems as SHDSL, and specially designed.

7. Other perspectives of radio communication systems

In [15] proposed variant of communication system in background with wide application in conjunction with professional military hardware tools for civil use (such as Wi-Fi, Wi-MAX, etc.).

Main idea of proposed scheme - construction of telecommunication network with ability to transfer and processing of heterogeneous traffic with providing many routes passing information of individual users on basis of purely civilian network equipment and communication facilities existing Armed Forces, with gradual build-up of professional military component equipment.

Conclusion

Because of this, modern Armed Forces radio communication system used in area of anti-terrorist operations, generally provides tasks of communication for benefit of command.

Main directions of development of systems and radio communications are:

launch own satellite telecommunications Ukraine of resources allocated for using by Armed Forces of Ukraine;

development and production own military devices digital radio (satellite terminals HF and UHF radios, microwave and tropospheric stations, command post vehicles);

modernization old hardware park (command post vehicles, tropospheric and radio relay stations);

integration new domestic and foreign devices of radio communications in communication system of Armed Forces of Ukraine.

Future research directed to develop methods of selecting options means military radio.

REFERENCES

1. Shyshatskiy, A.V., Bashkirov, O.M. and Kostina, O.M. (2015), “Development of integrated systems and data for Armed Forces”, Arms and military equipment, No 1(5), pp. 35-40, available at : http://journals.uran.ua/index.php/2414-0651/issue/view/1%285%29%202015 (last accessed March 01, 2017).
2. Official site of "Telecard-device". Products for power structures (2017), available at : mil.telecard.odessa.ua (last accessed March 01, 2017).
3. Borisov, I.V., Gritsenok K.M., Gurskiy T.G. and Pomin A.G. (2015), Methodical recommendations for setting up and operation of trunking communication Mototrbo, MITI, Kyiv, 112 p.
4. Site for calculating radio coverage zone, available at : http://lrcov.crc.ca (last accessed March 01, 2017).
5. Gurskyi, T.G., Zhuk O.G., Krivenko O.V. and Shyshatskyi A.V. (2016), “Directions of improvement of facilities of radio communication with pseudorandom reconstruction of the working frequency” *Collection of scientific works of Military Institute of Telecommunications and Informatization*, Publication 1, pp. 25-34, available at: http://www.viti.edu.ua/index.php?view=coll_2016_1 (last accessed March 02, 2017).
6. Official website of company „Aselsan” (2017), available at : www.aselsan.com.tr/en-us/Pages/default.aspx (last accessed March 01, 2017).
7. Gurskiy, T.G. ,Ilinov, M.D. and Makarchuk O.M. (2015), Methodical recomendations with using shortwaves backpack radio stations Harris RF-7800H-MP, MITI, Kyiv, 68 p.
8. MPR-9600. Tactical shortwaves radio stations. Operating Instructions (2011), Translated editions of Ukrainian language from publication number 10515-0228-4200, Rev. D, 185 p.

9. Gurskiy, T.G., Ilinov, M.D. and Esaulov, M.U. (2016), “More efficient using HF radio communication in Armed Forces of Ukraine”, Priority directions of development telecommunication systems and networks for special purposes. Using units, facilities, communications and automation in ATO, IX scientific and practical conference MITI, Kyiv, November 2016, pp. 27-33, available at : http://www.viti.edu.ua/files/zbk/2016/c_2016.pdf (last accessed March 01, 2017).
10. Gurskiy, T.G., Kiselov, R.V. and Makarchuk O.M. (2015), Methodical recommendations for setting up and operation of satellite communication Tooway, MITI, Kyiv, 32 p.
11. Mobile complex of satellite communication 1.1. (2017), available at : www.datagroup.ua/uk/uslugi/mobilnyie-kompleksyi/mobile-komplekt-sputnikovoj-svyazi-11 (last accessed March 01, 2017).
12. Official website of company „KROCUS-COM” (2017), available at : www.crocuscom.com/ru/products.php?cid=19 (last accessed March 15, 2017).
13. Ilchenko, M.E., Naritnik, T.N. and Slusar, V.I. (2014), "New generation Creation direction of new tropospheric stations”, *Digital technologies*, No 16, pp. 8-18, available at : http://www.slyusar.kiev.ua/DIGITAL_Technologies_2014.pdf (last accessed March 01, 2017).
14. Wietgrefe, H., Bastos, L., Deskeuvre, J.-C., Yamamoto, M. and Reddy, P. (2011) “Tactical Troposcatter Terminals for Modern Tactical Networks: Opportunities and Technical Challenge”, *Technical Panel*, IEEE Conference MILCOM, Baltimore, 7–10 November 2011, available at : http://expo.jspargo.com/exhibitor/milcom2011apprul.pdf (last accessed March 01, 2017).
15. Ilevich, S.S., Shcheglov, A.A. and Gurskiy, T.G. (2015), “Variant of telecommunication network deployment in tactical control link”, *Priority directions of development telecommunication systems and networks for special purposes. Using units, facilities, communications and automation in ATO*, VIII scientific and practical conference MITI, Kyiv, October 2015, pp.42-49, available at : http://www.viti.edu.ua/files/zbk/2015/c_2015.pdf (last accessed March 01, 2017).

Надійшла (received) 16.03.2017
Прийнята до друку (accepted for publication) 23.05.2017

Аналіз сучасного стану та перспектив розвитку воєнних систем радіозв’язку

І.О. Романенко, А.В. Шишацький

Метою статті є проведення аналізу військових систем зв’язку, які використовуються в районі проведення антитерористичної операції на території Донецької та Луганської областей. У статті проведений аналіз сучасних засобів військовому зв’язку, а саме: військових систем радіозв’язку, військових систем супутниковому зв’язку, військових систем радіорелейного та тропосферного зв’язку. Розглянуті переваги та недоліки кожного з видів зв’язку, розглянуті причини їх виникнення, а також обґрунтовані шляхи їх вирішення надалі. Проведений аналіз основних технічних характеристик військових систем зв’язку, їх можливостей, переваг та недоліків. На основі проведеного в статті аналізу військових засобів зв’язку, які використовуються в районі проведення антитерористичної операції на території Донецької та Луганської областей визначені перспективи розвитку систем військовому зв'язку. Для усунення зазначених у статті проблемних питань, авторами статті пропонується запустити власний військовий супутник для потреб Збройних Сил України; провести розробку нових зразків військового зв’язку; провести глибоку модернізацію наявних на озброєнні радіостанцій, командно-штабних машин, радіорелейних і тропосферних станцій; провести інтеграцію прийнятого на озброєння за останні роки телекомунікаційного встаткування в єдиний інформаційний простір Збройних Сил України, а також досягти угод із представниками провідних виробників телекомунікаційного устаткування щодо трансферу технологій і розгортання виробництва на території України.

Ключові слова: система радіозв'язку, радіозв'язок, радіоелектронне подавлення, навмисні завади.

Анализ современного состояния и перспектив развития военных систем радиосвязи

И.О. Романенко, А.В. Шишацкий

Целью статьи есть проведение анализа военных систем связи, которые используются в районе проведения антитеррористической операции на территории Донецкой и Луганской областей. В статье проведён анализ современных средств военной связи, а именно: военных систем радиосвязи, военных систем спутниковой связи, военных систем радиорелейной и тропосферной связи. Рассмотрены преимущества и недостатки каждого из видов связи, рассмотрены причины их возникновения, а также обоснованы пути решения указанных причин в дальнейшем. Проведен анализ основных технических характеристик военных систем связи, возможностей, преимуществ и их недостатков. На основе проведённого в статье анализа военных средств связи, которые используются в районе проведения антитеррористической операции на территории Донецкой и Луганской областей определены перспективы развития систем военной связи. Для устранения указанных в статье проблемных вопросов, авторами статьи предлагается запустить собственный военный спутник для нужд Вооруженных Сил Украины; провести разработку новых образцов военной связи; провести глубокую модернизацию имеющихся на вооружении радиостанций, командно-штабных машин, радиорелейных и тропосферных станций; провести интеграцию принятого на вооружение за последние годы телекоммуникационного оборудования в единое информационное пространство Вооруженных Сил Украины, а также достичь соглашений с представителями ведущих производителей телекоммуникационного оборудование относительно трансфера технологий и развёртывания производства на территории Украины.

Ключевые слова: система радиосвязи, радиосвязь, радиоэлектронное подавление, преднамеренные помехи.

Intelligent information systems

UDC 004.94 **doi: 10.20998/2522-9052.2017.1.06**

A. Goriushkina[1], R. Korolev[2]

[1] National Technical University "Kharkiv Polytechnic Institute", Kharkiv, Ukraine
[2] Ivan Kozhedub Kharkiv National Air Force University, Kharkiv, Ukraine

ANALYSIS OF THE CURRENT STATUS OF INTELLIGENT SYSTEM "INTERNET OF THINGS" AND TRENDS IN THE DEVELOPMENT

The **subject** of study in the article is the processes of analysis and evaluation of attack intelligent systems "Internet of Things" (IoT). The goal is to reduce the potential attacks due to the risks of intellectual functioning of the IoT systems, through the timely adoption of security measures. **Objectives:** the classification of attacks on all levels of intelligent systems, IoT, highlighting the main factors and their causes; the following results are obtained. The analysis of the current state of intelligent systems, IoT, analyzed all levels of functioning, and classification of hackers on the factors of their occurrence. The negative consequences negatively affecting the basic characteristics of the functioning of the IoT systems. As a result, a block diagram of attacks at all levels of the IoT. **Conclusions.** The article analyzes the current state of intelligent systems "Internet of Things" (IoT). It is shown that a significant increase in computer network devices connected to the network creates new opportunities for the development of modern society in the field of science and technology. However, the significant development of "Internet of Things" is directly proportional to increases the possibility of attacks in computer networks. Therefore, the scientific direction improvement of existing or development of new algorithms, models, and their implementation to ensure major safety criteria for IoT are relevant.

Keywords: intelligent systems Internet of Things, attacks, security, computer technology.

Introduction

The rapid development of modern society and computer technology offers consumers a wide range of services. To date, the significant growth of networked network devices, systems and services included in the current structure, create new opportunities and advantages for the development of modern society in science, technology and industry.

The devices connected to the Internet allow for high-level communication between users, the network and various types of provided physical services. Such connections are highly effective, and they also open the possibility of using new ways of using the Internet resource. Cloud computing can provide the virtual infrastructure for such utility computing which integrates monitoring devices, storage devices, analytics tools, visualization platforms and client delivery. The cost based model that cloud computing offers will enable end-to-end service provisioning for businesses and users to access applications on demand from anywhere. Smart connectivity with existing networks and context-aware computation using network resources is an indispensable part of Internet of Things.

The analysis of the problem and formulation of the task

"Internet of Things" (IOT) is a global network infrastructure, linking physical and virtual object s through the exploitation of data capture and communication capabilities. It will offer specific object identification, sensor and connection capability as the basis for the development of independent cooperative services and applications. These will be characterized by a high degree of autonomous data capture, event transfer, network connectivity and interoperability.

As recent studies have shown the popularity of different paradigms varies with time. Analysis of trends in the development of the demand for computer resources by users is shown in Fig. 1. As it can be seen, since IoT has come into existence, search volume is consistently increasing with the falling trend for others.

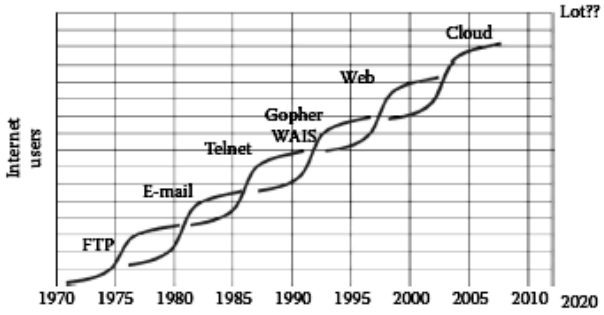


Fig. 1. Analysis of trends in the development of the demand for computer resources by users

In this case, it is shown a schematic of the interconnection of objects is depicted in Fig. 2, where the application domains are chosen based on the scale of the impact of the data generated.

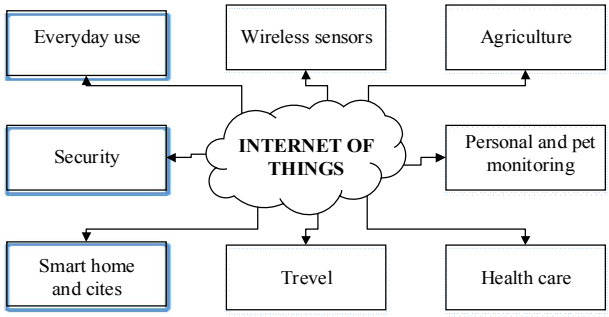


Fig. 2. IoT schematic of end users and application areas based on data

The users span from individual national level organizations addressing wide ranging issues.

According to the research conducted, in connection with the rapidly growing technology Internet of things, over the past 10 years, the tendency of attacks from hackers to different levels of the Internet of Things architecture has significantly increased.

The Fig. 3 shows the statistics of attacks on the Statistics of attacks of the IoT.

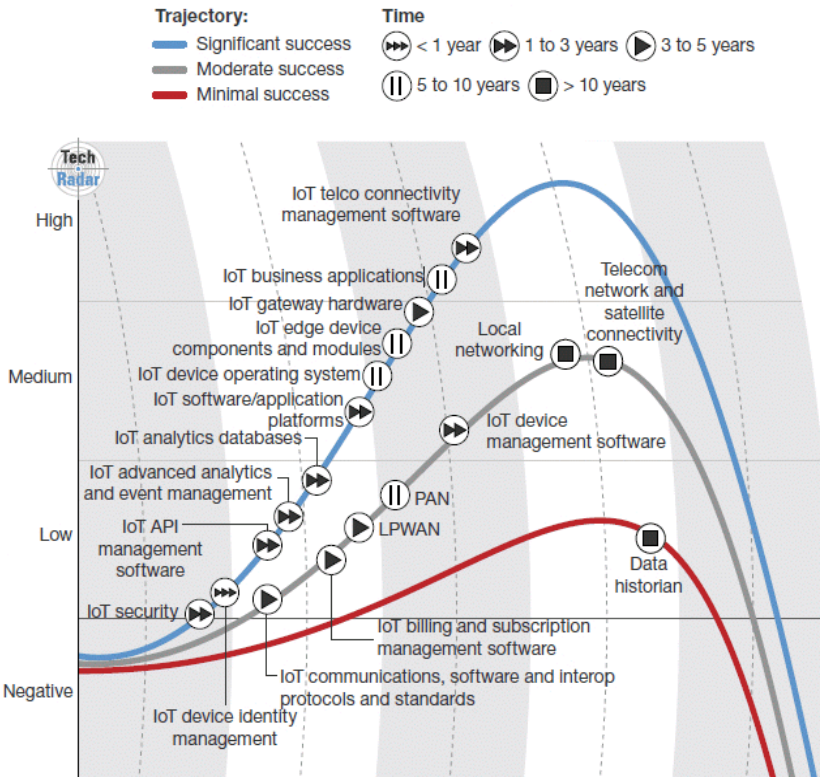


Fig. 3. Statistics of attacks of the IoT

Task solution

IoT combines end-user systems, data centers, digital devices, RFID, sensors and chips, intelligent devices and networks, cloud computing, vehicle networks, and other storage media. These results in the generation of enormous amounts of data which have to be stored processed and presented in a seamless, efficient, and easily interpretable form.

The main levels of IOT architecture are these 3: the perception level, the network level, and the service level, as shown in Fig. 4.

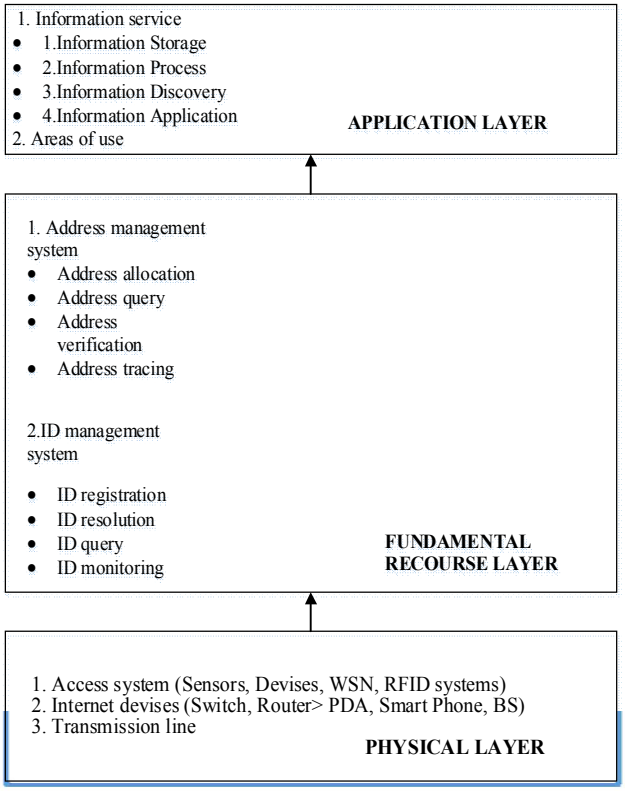


Fig. 4. Internet of Things system architecture

Physical layer. On this level all kinds of information of the physical world used in IOT are perceived and collected in this level, by the technologies of sensors, wireless sensors network (WSN),tags intelligent terminals, electronic data interface (EDI), objects, and so on.

The second layer is Fundamental recourse layer. It consist network level or transport layer and support layer. It's including access network and core network, provides transparent data transmission capability. At the same time, this layer provides an efficient, reliable, trusted network infrastructure platform to upper level and large scale industry application.

Application layer includes data management sub-layer and application service sub-layer. The application service sub-layer transforms information to content and provides good user interface for upper level enterprise application and end users.

There are three IoT components which enables seamless connection:

Hardware—made up of sensors, actuators and embedded communication hardware.

Middleware—on demand storage and computing tools for data analytics.

Presentation—novel easy to understand visualization and interpretation tools which can be widely accessed on different platforms and which can be designed for different applications.

IoT affects the functioning of elements of a heterogeneous structure with a great distance of the control centers from each other. In this regard, the importance of ensuring the quality of service when transferring data in computer networks. It is also obvious that the process of information exchange of IoT data is complicated from the point of view of interaction of various protocols, and its functionality in general.

As studies [1-8] show, an increase in the demand growth by users for these resources in computer networks leads to some undesirable consequences, namely, various attacks on this system, in which existing methods and protection algorithms are not able to ensure the required level of security.

The security of information and network should be equipped with these properties such as identification, confidentiality, integrality and accessibility. Network security and management play an important role in above each level, which was considered.

The analysis showed common security requirements for each level, as shown in Fig. 5.

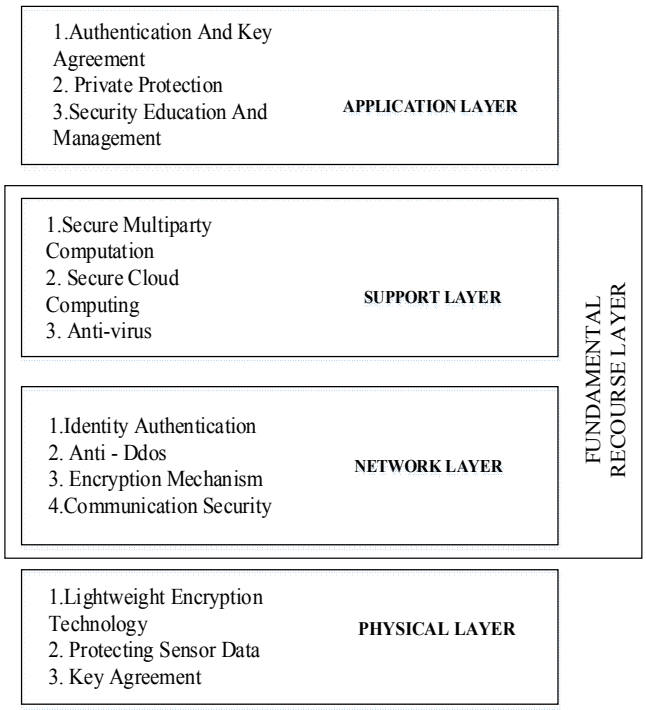


Fig. 5. Security requirements of IoT

Analysis of the literature [1-8] showed that with the increase in the number of interacting IoT objects, the likelihood of attacks in the computer network is also growing proportionally.

For the qualitative work of the intelligent IoT system, it is necessary to carry out a sequence of actions, consisting of five steps, from receiving the initial data to the final delivery of this data to end users. At the same time, at each stage there is a possibility of a threat of attack from hackers.

Let's consider different types of attacks on Internet of Things systems on the example of data transfer in these systems as shown in Fig. 6.

Conclusions

In the last few years, this emerging domain for the IoT has been attracting the significant interest, and will continue for the years to come. In spite of rapid evolution, we are still facing new difficulties and severe challenges. The significant growth of threats and attacks in the field of computer systems and IoT facilities leads to an increase in the measures taken to ensure an appropriate level of security. First of all, effective mechanisms are considered that can identify the attack resistance necessary for the high-quality operation of the IoT intelligent network.

In this article, we consider the at- maturity of research into intelligent systems. The main levels of architecture and security issues at each level are considered. An example of data transmission in the intellectual Internet of things is shown, and atk types of attacks during data transmission. Obviously, under similar circumstances, the issue of the security of intelligent systems is relevant. Therefore, the actual directions are the improvement of existing or development of new algorithms, models and their implementation to provide basic IoT security criteria such as identification, confidentiality, integrity and accessibility.

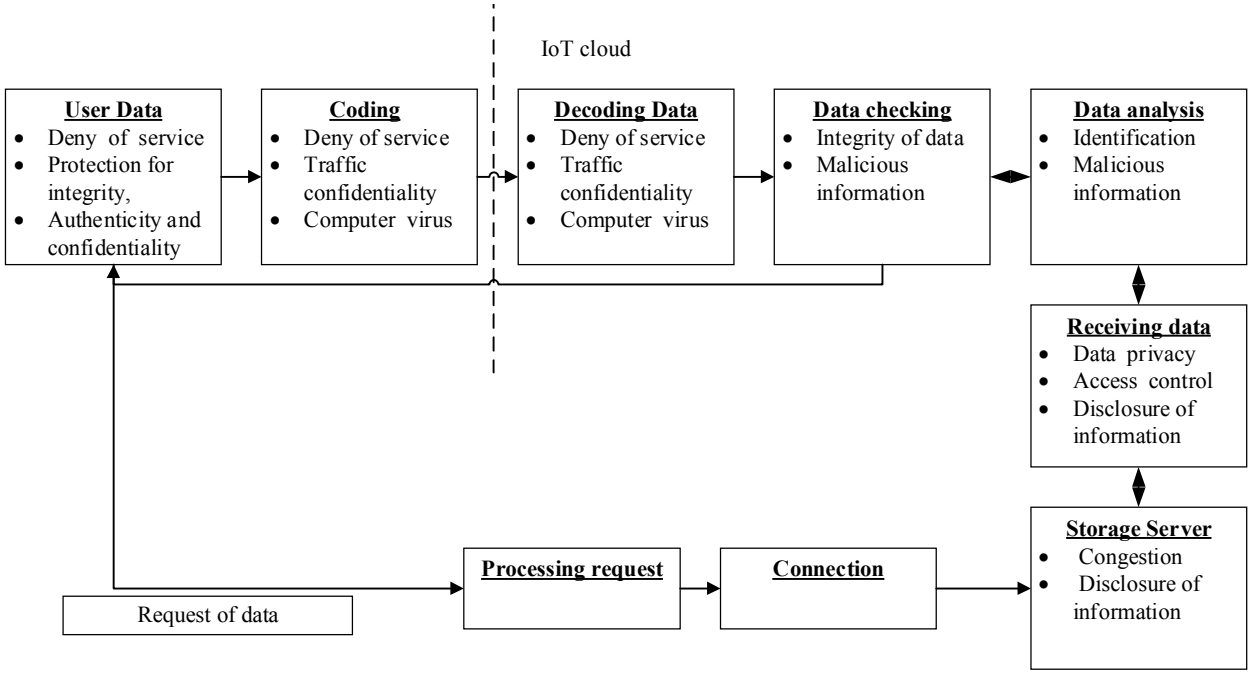


Fig. 6. Different types of data transfer attacks on Internet of Things systems

REFERENCES

1. Chuankun, Wu. (2010), “A preliminary investigation on the security architecture of the Internetof Things”, *Strategy and Policy Decision Research*, 25(4), pp. 411–419.
2. Goldman, Sachs (2014), IoT Primer, The Internet of Things: Making Sense of the Next Mega-Trend, September 3, available at : http://www.goldmansachs.com/our-thinking/outlook/internet-of-things/iot-report.pdf (last accessed March 23, 2017).
3. International Telecommunication Union. ITU Internet reports 2005: The Internet of Things (2005), 212 p.
4. Ibrahim, Mashal, Osama, Alsaryrah, Tein-Yaw, Chung, Cheng-Zen, Yang, Wen-Hsing, Kuo and Dharma, P. Agrawal (2015), “Choices for interaction with things on internet and underlying issues”, *Ad Hoc Networks*, 28, pp. 68–90.
5. Jeyanthi ang N.,N.Ch.S.N. Iyengar. (2013), “Escape-on-sight: An efficient and scalable mechanism for escaping DDoS attacks in cloud computing environment”, *Cybernetics and Information Technologies*, 13(1), pp. 46–60.
6. Kang, Kai, Pang, Zhibo and Wang Cong (2013), “Security and privacy mechanism for health Internet of Things”, *The Journal of China Universities of Posts and Telecommunications*, 20 (Suppl. 2), pp. 64–68.
7. Kim Thuat Nguyen, Maryline Laurent and Nouha Oualha (2015), “Survey on secure communication protocols for the Internet of Things”, *Ad Hoc Networks*, 32, pp. 17–31.
8. Qazi Mamoon Ashraf ang Mohamed Hadi Habaebi (2015), “Autonomic schemes for threat mitigation in Internet of Things”, *Journal of Network and Computer Applications*, 49, pp. 112–127.
9. Jia, X.L., Feng, Q.Y. and Ma, C.Z. (2010) “An efficient anti-collision protocol for RFID tag identification”, *IEEE Communications Letters*, vol. 14, no. 11, pp.1014–1016.
10. Finkenzeller K. (2010), RFID *Handbook: Fundamentals and Applications in Contactless Smart Cards*, Radio Frequency Identification and Near-Field Communication, New York: Wiley. – 478 p.
11. Culler D {2003), “10 Emerging Technologies That Will Change the World”, *Technology Review*, pp. 33–49.
12. Lu, Y.X., Chen, T.B., Meng, Y. (2011), “Evalution guideling system and intelligent evaluation process on the Internet of Things,” *American Journal of Engineering and Technology Research*, vol. 11, no.9, pp.537-541.
13. Bang O., Choi J.H., Lee D. and Lee H. (2009), *Efficient Novel Anti-collision Protocols for Passive RFID Tags*, Auto-ID Labs White Paper WP-HARDWARE-050, MIT, 29 p.

Надійшла (received) 03.04.2017
Прийнята до друку (accepted for publication) 13.06.2017

Аналіз сучасного стану
інтелектуальної системи "Internet of Things" та тенденції її розвитку

А. Е. Горюшкіна, Р. В. Корольов

Предметом вивчення в статті є процеси аналізу та оцінки атак інтелектуальної системи “Internet of Things” (IoT). **Мета** – зниження потенційних атак, зумовлених ризиками функціонування інтелектуальної системи IoT, шляхом своєчасного вжиття заходів безпеки. **Завдання:** класифікація атак на всіх рівнях інтелектуальної системи IoT з виділенням основних факторів і причин їх виникнення; Отримані наступні **результати**. Проведено аналіз сучасного стану інтелектуальної системи IoT, проаналізовано всі рівні функціонування та класифікацію атак хакерів за факторами їх виникнення. Визначено негативні наслідки, що негативно впливають на основні характеристики функціонування IoT. В результаті сформована структурна схема атак на всіх рівнях IoT. **Висновки.** У статті аналізується поточний стан інтелектуальної системи “Internet of Things.” Показано, що значне зростання комп'ютерних мережевих пристроїв, підключених до мережі створює нові можливості для розвитку сучасного суспільства в галузі науки і техніки. Однак, значний розвиток “Internet of Things” прямо пропорційно збільшує можливість атак в комп'ютерній мережі. Тому наукові напрямки вдосконалення існуючих або розробка нових алгоритмів, моделей та їх реалізації для забезпечення основних критеріїв безпеки для IoT є актуальними.

Ключові слова: інтелектуальна система “Internet of Things”, атаки, безпека, комп’ютерні технології.

Анализ современного состояния
интеллектуальной системы "Internet of Things" и тенденции ее развития

А. Э. Горюшкина, Р. В. Королев

Предметом изучения в статье являются процессы анализа и оценки атак интеллектуальной системы “Internet of Things” (IoT). **Цель** – снижение потенциальных атак, обусловленных рисками функционирования интеллектуальной системы IoT, путем своевременного принятия мер безопасности. **Задачи**: классификация атак на всех уровнях интеллектуальной системы IoT с выделением основных факторов и причин их возникновения; Получены следующие результаты. Проведен анализ современного состояния интеллектуальной системы IoT, проанализированы все уровни функционирования и классификацию атак хакеров по факторам их возникновения. Определены негативные последствия, негативно влияющие на основные характеристики функционирования IoT. В результате сформирована структурная схема атак на всех уровнях IoT. **Выводы.** В статье анализируется текущее состояние интеллектуальной системы “Internet of Things”. Показано, что значительный рост компьютерных сетевых устройств, подключенных к сети, создает новые возможности для развития современного общества в области науки и техники. Однако, значительное развитие “Internet of Things” прямо пропорционально увеличивает возможность атак в компьютерной сети. Поэтому, научные направления совершенствования существующих или разработка новых алгоритмов, моделей и их реализации для обеспечения основных критериев безопасности для IoT являются актуальными.

Ключевые слова: интеллектуальная система “Internet of Things”, атаки, безопасность, компьютерные технологии.

UDC 510.635 **doi: 10.20998/2522-9052.2017.1.07**

Khudhair Abed Thamer

Kuliyyah Al-Maaref University College, Republic of Iraq

THE INTELLIGENCE THEORY MATHEMATICAL APPARATUS FORMAL BASE

Purpose. The main task of the theory of intelligence is to describe mathematically the laws governing the intellectual activity of a human. This requires to obtain using physical and objective methods to obtain formal description of the subjective states of a human sufficiently complete for practical purposes. Human thoughts, sensations, perceptions and awareness are all subjective states. This paper is tasked to develop a multidimensional predicate model of comparator identification - the basic experimental method of the intelligence theory and to substantiate the axiomatics of this model. **Methods.** The comparator identification method developed in this paper provides the possibility of obtaining objective knowledge of subjective states of human intelligence. According to the comparator identification method with his behavior the subject realizes some finite predicate, the properties of which are experimentally studied and mathematically described. The comparator identification method is based on the algebra of finite predicates, Boolean algebra and the axiomatic method. **Results.** As a result of the comparator identification method application, we obtain a mathematical description of the studied subjective states of a subject, as well as the form of the function underlying the transformation of physical objects into subjective images generated by them. **Conclusions.** The results of this paper provide a mathematical substantiation of the possibility of using the comparator identification method in human intelligence modeling.

Keywords: theory of intelligence, algebra of finite predicates, comparator identification.

Introduction

In this article some results aimed at developing the mathematical apparatus of the theory of intelligence are obtained.

As a model in the development of the theory of intelligence, we adopt modern Physics, which, like the theory of the intelligence, has two sides - formal and conceptual.

As a formal teaching, Physics is an experienced science that studies the laws of nature and expresses them in the form of equations.

The need to consider the theory of intelligence as a formal teaching is due to the fact that it needs a special mathematical language that is not sufficiently developed in the available sections of mathematics. Therefore, the theory of intelligence, along with a meaningful study of the mind of a human, is also compelled to develop the necessary formal apparatus. Here this theory of intelligence is not unique.

Thus, the needs of celestial mechanics gave rise to mathematical analysis, the doctrine of the logical abilities of a human stimulated the development of the predicate calculus.

The possibility to expound the theory of intellect in a deductive way, proceeding solely from the physically observed facts, is based on the method of the axiomatic description of the mind of a human. This is a comparison method, or a comparator identification method.

The algebra of finite predicates was developed in this article [1]. In [2-4] some aspects of the theory and practice of comparator identification are considered.

In this article, the development of the theory of comparator identification is continued.

A multidimensional predicate model of comparator identification is proposed, and the axiomatics of this model is justified.

1. Comparison method (comparator identification method)

The essence of the method consists in the fact that the subject (the person whose intellect is being investigated) in specially designed experiments by his physical reactions forms the meanings of some predicates $P_1, P_2, ..., P_r$. In these experiments, the properties of predicates are revealed $P_1, P_2, ..., P_r$, Which are formally written in the form of logical equations connecting predicate variables $X_1, X_2, ..., X_r$. Some of these equations are used in the role of axioms or the initial postulates of the theory of intelligence. From axioms, as from equations, there are values of predicate variables $X_1, X_2, ..., X_r$, which are respectively predicates $P_1, P_2, ..., P_r$.

The internal structure of the found predicates characterizes certain details of the mechanism of the human intellect.

The method of comparison was first used by Newton in the physical study of human color vision. Acting as a test subject, he observed on the comparison fields an arbitrary light radiation x_1, x_2 and recorded the equality or inequality of their color. The predicate formed this way $P(x_1, x_2)$ for the first time connected the Grassmann axioms with logical axioms. Based on Grassmann's postulates (laws), Schroedinger first constructed the deductive theory of human color vision.

In the study of human intelligence by comparison, the researcher influences the senses of the subject experienced by physical signals (stimuli) $x_1, x_2, ..., x_n$, generating in his mind certain subjective experiences (states) $y_1, y_2, ..., y_n$. It is assumed that the states $y_1, y_2, ..., y_n$ uniquely depend on the corresponding

incentives $x_1, x_2, ..., x_n$. This means that there are functions $y_1 = f_1(x_1)$, $y_2 = f_2(x_2), \ldots, y_n = f_n(x_n)$. In the experiments on the subject, the stimuli $x_1, x_2, ..., x_n$ are taken from the sets clearly outlined by the researcher $A_1, A_2, ..., A_n$, so it's always $x_1 \in A_1, x_2 \in A_2, ..., x_n \in A_n$.

The sets $A_i, i = \overline{1,n}$ are chosen by the the researcher arbitrarily, at his discretion, proceeding from those scientific tasks that he sets before himself. It is assumed that each of the incentives $x_i \in A_i$ generate a well-defined state y_i. The set of all values of the function $y_i = f_i(x_i)$, given on the set A_i, is denoted by the character B_i.

Thus, each of the functions f_i is a subjection reflecting the set A_i on the set B_i. The functions f_i characterize the subject's ability to react to external objects with their subjective states.

The researcher gives the subject an assignment, which he must perform in the course of the experiment. The task specifies some attitude L, linking the states $y_1 \in B_1, y_2 \in B_2, ..., y_n \in B_n$. In each experiment the researcher forms certain states in the consciousness of the subject $y_1, y_2, ..., y_n$, showing him the appropriate stimuli $x_1, x_2, ..., x_n$. If for these states the ration L is performed the subject must respond with a response $\xi = 1$, if not, with the answer $\xi = 0$. Performing the task, the subject realizes the predicate $\xi = L(y_1, y_2, ..., y_n)$, corresponding the relation L. The predicate L characterizes the action of the mechanism of consciousness of the subject, comparing the state $y_1, y_2, ..., y_n$ in accordance with the received task. It is this comparison operation that gives the name to the method of comparator identification (after the English word "to compare").

The predicate

$$P(x_1, x_2, ..., x_n) = L(f_1(x_1), f_1(x_1), ..., f_n(x_n))$$

characterizes the physically observed behavior of the subject performing the task of the researcher and reacting to the stimuli $x_1, x_2, ..., x_n$ with the response $\xi = P(x_1, x_2, ..., x_n)$.

The problem of the theory of intelligence is from the properties of the predicate P, detected in experiments on the subject, to extract the internal structure of the signals $x_1, x_2, ..., x_n$; $y_1, y_2, ..., y_n$; form of the functions $f_1, f_2, ..., f_n$ and the form of the predicate L.

This problem enables the extension to the case r of the predicates $P_1, P_2, ..., P_n$. In the general case, the subject receives r the tasks that perform alternately for different sets of input signals.

Observable patterns in the behavior of the subject are recorded in the form of a system of logical equations (conditions):

$$\begin{aligned} &P_1(X_1, X_2, ..., X_r) = 1, \\ &P_2(X_1, X_2, ..., X_r) = 1, \\ &\ldots\ldots\ldots\ldots\ldots\ldots \\ &P_l(X_1, X_2, ..., X_r) = 1, \end{aligned} \quad (1)$$

interconnecting the predicate variables $X_1, X_2, ..., X_r$. With the characters $P_1, P_2, ..., P_l$ are denoted the predicates from predicates $X_1, X_2, ..., X_r$. The predicate $X_j(x_1, x_2, ..., x_n), \quad j = \overline{1,r}$ is given on a Cartesian product $A_{1j} \times A_{2j} \times ... \times A_{nj}$. It is meant that the solution $X_1 = P_1, X_2 = P_2, ..., X_r = P_r$ satisfies the system of equations (a).

Values of the arguments $x_1, x_2, ..., x_n$ of the predicates $P_1, P_2, ..., P_r$ appear first in the experiments as the abstract elements, the internal structure of which is unknown. This structure is extracted by deductive methods from conditions (1). From them the internal structure of predicates is extracted $P_1, P_2, ..., P_r$, which consists of the internal structure of the signals $y_{1j}, y_{2j}, ..., y_{nj}$, the functions $f_{1j}, f_{2j}, ..., f_{nj}$ and the predicate L_j for each of the predicates

$$P_j(x_1, x_2, ..., x_n) = L_j(f_{1j}(x_1), f_{1j}(x_1), ..., f_{nj}(x_n)) = L_j(y_{1j}, y_{2j}, ..., y_{nj}).$$

The theory of the intellect as a formal teaching is constructed as follows. There is a universe of elements U, in the role of which a set of all kinds of stimuli is used, which the researcher can present to the subject. From the elements of the universe U the researcher forms sets $A_{1j}, A_{2j}, ..., A_{nj}$, in accordance with the specific task of studying this or that side of the human intellect. On Cartesian products $A_{1j} \times A_{2j} \times ... \times A_{nj}$ the predicates are defined P_j, which are interpreted as the behavior of the subject performing certain tasks of the researcher.

Introducing predicate variables $X_1, X_2, ..., X_r$, we connect them with logical equations (1). Substantially these equations act as initial postulates of the theory of intelligence. Of these, as from axioms, are deductively derived dependencies characterizing the internal structure of the elements of the universe U and the predicates $P_1, P_2, ..., P_r$. The task of the theory of the intellect as a meaningful teaching is the formulation and experimental verification of its postulates in the form of equations (1).

2. Sets

The above-mentioned research program can not be performed without a sufficiently developed mathematical language. First of all, we need a formal language in which it is possible to write down the predicates that the subject realizes in experiments. Next, we need to have a language for writing equations

expressing the properties of these predicates. In addition, it is necessary to have formal means for describing the internal structure of the stimuli presented to the subject and the states experienced by him, as well as the internal structure of the predicates that the subject realizes. Finally, it is necessary to have mathematical means of extraction from the properties of predicates of their internal structure. The foundations for developing the desired formal language are the concepts of set and relation.

Let's assume that $a_1, a_2, ..., a_k$ – are various subjects. Their totality is called a set. We will commonly denote sets by the bold uppercase Latin letters. The subjects $a_1, a_2, ..., a_k$, which are part of the set, are called its elements. As a rule, elements will be denoted by lowercase Latin letters. Sets may differ from each other by a number k and the composition of the elements in them $a_1, a_2, ..., a_k$. To write the set we will use the list of all its elements, enclosed in curly brackets: $\{a_1, a_2, ..., a_k\}$. The sets can be built not only from the elements, but also from the sets, for example $\{\{a_1\}, \{a_1, a_2\}\}$. Such sets are called sets systems.

The elements in the set are unordered, so the order of enumeration of elements in the set record does not matter. In the record of a set, the same elements can be repeated, but the set itself does not change because it does not have the same elements. If the characters a and b denote the same element, it is said that the elements a and b are equal and is written $a = b$. Otherwise, it is written $a \neq b$. If the sets A and B consist of the same elements, then it is said that they are equal and written $A = B$. If it is false that $A = B$, then it is written $A \neq B$.

The sets just considered are named the finite. The number of elements in them can take any natural value $k = 1, 2, ...$. Where $k = 0$ we get an empty set $\varnothing$, which does not contain any elements. Where $k = 1$ we get the singleton sets. Also can be considered the infinite sets for which the value k is not limited to the maximum value. The examples of infinite sets can be a countable set consisting of all natural numbers and the continual set of all real numbers. The power of a continual set is greater than the cardinality of a countable set. There are the sets cardinality of which exceeds the power of the continuum, for example, the set of all real functions.

For an infinite set the role of the number of its elements plays the cardinality of the set. Two sets A and B are named the equipotent, if for each element of the set A can be associated its element of the set B and vice versa. The power of a finite set is the number of its elements. The totality of all objects that are elements of all possible sets that are considered in a particular problem (reasoning, research, theory) is called a universal set or a universe of this problem and is denoted by the character U. It is possible to combine in the same universe, together with elements, also the sets formed from these elements. It is believed that in such a universe the sets differ from the elements, in particular $a \neq \{a\}$.

If the element a is a part of the set A, it is said, that a belongs to A and it is written $a \in A$. The record $a \overline{\in} A$ or $a \notin A$ means that the element a does not belong to the set A. The record $a_1, a_2, ..., a_n \in A$ means that $a_1 \in A, a_2 \in A, ..., a_n \in A$. In the role of elements of a set can be used any elements of the universe U. Each element of any set considered in any problem must be an element of the universe of this problem. The relation $\in$ is named an element belonging to a set.

The relation of belonging of the element to the set and the equality of the elements are related by the law of Leibniz: for all a and b $a = b$ only if $a \in A$ is equally matched $b \in A$ at any A. The relation of an element to a set and the equality of sets are connected by the law of capacity or extensionality: for all A and B $A = B$ only if $a \in A$ is equally matched $a \in B$ at any a.

The set A is called a subset or part of the set B, and the set B – the superset of the set A, if every element of the set A belongs also to the set B. In this case it is said that the set A is included in the set B and is written $A \subseteq B$. In the role of sets of elements, can be used any subset of the universe U. Each set, considered in any problem, must be a subset of the universe of this problem:

$$A \subseteq U \tag{2}$$

for any A. Each element that appears in the problem must belong to the universe of this problem:

$$a \subseteq U \tag{3}$$

for any a. The empty set is a subset of any set:

$$\varnothing \subseteq A \tag{4}$$

for any A.

The relation $\subseteq$ is called the inclusion of sets. It is reflexive:

$$A \subseteq A \tag{5}$$

for any A; anti-symmetrically: $A \subseteq B$ and $B \subseteq A$ is equally matched $A = B$ for any A and B; transitively: $A \subseteq B$ and $B \subseteq C$ entails $A \subseteq C$ for any A, B, C. If $A \subseteq B$ and $A \neq B$, then A are called proper subsets or regular parts of the set B an is written $A \subset B$. The relation $\subset$ is called a strict inclusion of sets. The sets $\varnothing$ and A re called improper subsets of the set A, all other subsets of the set A – its own subsets.

The totality or the sum $A \cup B$ of sets A and B is set consisting of all elements of the set A and all elements of the set B. The predicating $A \cup B$ is equally matched to the predicating $a \in A$ or $a \in A$ at any a, A, B. Intersection or common part $A \cap B$ of the sets A and B A set consisting of all such elements, each of which is contained both in the set A, and in the set B. The predicating $a \in A \cap B$ is equally matched to the predicating $a \in A$ and $a \in A$ at any a, A, B.

The operations of union and intersection of sets are idempotent:

$$A \cup A = A, \quad (6)$$

$$A \cap A = A \quad (7)$$

for any A; commutative:

$$A \cup B = B \cup A, \quad (8)$$

$$A \cap B = B \cap A \quad (9)$$

for any A and B; associative:

$$(A \cup B) \cup C = A \cup (B \cup C), \quad (10)$$

$$(A \cap B) \cap C = A \cap (B \cap C), \quad (11)$$

and distributive:

$$(A \cup B) \cap C = (A \cap C) \cup (B \cap C), \quad (12)$$

$$(A \cap B) \cup C = (A \cup B) \cap (B \cup C) \quad (13)$$

for any A, B, C.

The unification and the intersections of sets obey the laws of absorption or elimination:

$$(A \cup (A \cap B) = A, \quad (14)$$

$$(A \cap (A \cup B) = A \quad (15)$$

for any A and B.

In combination with the universal and empty sets, the operations of union and intersection of sets have the following properties:

$$A \cup \varnothing = A, \quad (16)$$

$$A \cap U = A, \quad (17)$$

$$A \cup U = U, \quad (18)$$

$$A \cap \varnothing = \varnothing \quad (19)$$

at any A.

The sets A and B are called disjoint if $A \cap B = \varnothing$; otherwise these sets are called intersect. A set of B is called the complement of the set A, if $A \cap B = \varnothing$ and $A \cup B = U$. For every set A there is a single complement $\overline{A}$. at any a and A $a \in \overline{A}$ is equally matched $a \notin A$.

The operation of addition $\overline{A}$ of the set A obeys the double complement law:

$$\overline{\overline{A}} = A \quad (20)$$

for any A; the Morgan de:

$$\overline{A \cup B} = \overline{A} \cap \overline{B}, \quad (21)$$

$$\overline{A \cap B} = \overline{A} \cup \overline{B} \quad (22)$$

for any A and B. In combination with the universal and empty sets, the operations of union, intersection, and complement of sets have the following properties:

$$A \cup \overline{A} = U, \quad (23)$$

$$A \cap \overline{A} = \varnothing \quad (24)$$

for any A;

$$\overline{\varnothing} = U, \quad (25)$$

$$\overline{U} = \varnothing. \quad (26)$$

At any A and B the equality $A \cup B = B$ is equally matched to the inclusion $A \subseteq B$, the following inclusions are valid:

$$A \subseteq A \cup B, \quad (27)$$

$$A \subseteq A \cap B. \quad (28)$$

The difference of sets A and B is called the set

$$A \setminus B = A \cap \overline{B}. \quad (29)$$

The system of all subsets of the universe U together with the operations of addition, union, and intersection of sets is called the algebra of sets. The relations (6)–(29) are called the basic identities of the algebra of sets.

Any set M, containing elements 0 and 1, on which two double operations + and $\cdot$ and one single ', satisfying at any $a,b,c \in M$ equalities:

$$a + a = a, \quad (30)$$

$$a \cdot a = a, \quad (31)$$

$$a + b = b + a, \quad (32)$$

$$a \cdot b = b \cdot a, \quad (33)$$

$$(a + b) + c = a + (b + c), \quad (34)$$

$$(a \cdot b) \cdot c = a \cdot (b \cdot c), \quad (35)$$

$$(a + b) \cdot c = (a \cdot c) + (b \cdot c), \quad (36)$$

$$(a \cdot b) + c = (a + c) \cdot (b + c), \quad (37)$$

$$a + (a \cdot b) = a, \quad (38)$$

$$a \cdot (a + b) = a, \quad (39)$$

$$a + 0 = a, \quad (40)$$

$$a \cdot 1 = a, \quad (41)$$

$$a + 1 = 1, \quad (42)$$

$$a \cdot 0 = 0, \quad (43)$$

$$(a')' = a, \quad (44)$$

$$(a + b)' = a' \cdot b', \quad (45)$$

$$(a \cdot b)' = a' + b', \quad (46)$$

$$a + a' = 1, \quad (47)$$

$$a \cdot a' = 0, \quad (48)$$

$$\overline{0} = 1, \quad (49)$$

$$\overline{1} = 0 \quad (50)$$

is called a Boolean algebra. Relations (30)–(50) are called basic identities of a Boolean algebra.

Not all basic identities of Boolean algebra are independent of each other. Some of them can be derived from the totality of the others.

Thus, from the identities:

$$a + a = a,$$

$$a + b = b + a,$$

$$(a + b) + c = a + (b + c),$$

$$\begin{gathered}(a+b)\cdot c=(a\cdot c)+(b\cdot c),\\ (a')'=a,\\ (a+b)'=a'\cdot b',\\ a+(b\cdot b')=a\end{gathered}\qquad(51)$$

all the other basic identities of Boolean algebra are derived. The identity (51), which is absent in the list of basic identities of a Boolean algebra, follows from the identities $a+0=a$ and $a\cdot a'=0$.

The recently given seven identities (51) are logically independent from each other, they are called axioms of Boolean algebra.

Any non-empty set M, on which the operations + are given $\cdot$ and ', subordinate to these axioms, is a Boolean algebra. From the axioms of Boolean algebra follows the existence and uniqueness of zero $0=a\cdot a'$ and a figure $1=a+a'$.

If 0 is taken as a set $\varnothing$, 1 is taken as a set U, + is taken as an operation, $\cdot$, ' – correspondingly the operations $\cup$, $\cap$, $\bar{}$ over the sets of a set U, then the Boolean algebra turns into one of its varieties - the algebra of sets. Operations $\cup$, $\cap$, $\bar{}$ are called Boolean operations over sets. The axioms of Boolean algebra now play the role of axioms of algebra of sets, which can be written in the form of identities:

$$\begin{gathered}A\cup B=B\cup A,\\ (A\cup B)\cup C=A\cup(B\cup C),\\ (A\cup B)\cap C=(A\cap C)\cup(B\cap C),\\ \bar{\bar{A}}=A,\\ \overline{A\cup B}=\bar{A}\cap\bar{B},\\ A\cup(B\cap\bar{B})=A.\end{gathered}\qquad(52)$$

Conclusions

From an applied point of view, the language of finite mathematics seems quite acceptable for the theory of intelligence, since any artificial intelligence systems have a finite complexity. With their help, you can practically reproduce only those intellectual processes that allow a mathematical description in the language of finite mathematics.

So, let's focus on the final mathematics in the role of the universal language of the theory of intelligence. But in which specific form of an algebraic system should it be used in the theory of intelligence. For this purpose, can be used the algebra of finite predicates.

This recommendation is based on the completeness of the algebra of finite predicates.

In the language of the algebra of finite predicates, can be written any finite relation and any finite function.

This means that in the language of the algebra of finite predicates, any law of intelligence and any intellectual activity realized on a computer can be expressed.

All that can be expressed in the language of the algebra of finite predicates can also be practically reproduced on a computer. And on the contrary, everything that can be implemented on a computer can also be written in the language of the algebra of finite predicates.

Thus, there is an exact correspondence between the descriptive possibilities of the algebra of finite predicates and the capabilities of computers to actually implement the descriptions of this algebra. The conclusion about the admissibility of the algebra of finite predicates for the theory of intelligence is also reinforced by the fact that literally all paths lead to the algebra of finite predicates.

So, if the language of graph theory is supplemented with a formal apparatus, then as a result it is obtained the algebra of finite predicates.

If the algebra of logic is generalized and go from binary to alphabetic ones, it is also obtained the algebra of finite predicates.

If a multivalued logic is supplemented with a language for writing relations, we again come to the algebra of finite predicates. Finally, if we take a finite fragment of the logic of predicates and algebraize it, then in this case we are led to the same algebra of finite predicates.

It is very important that the algebra of finite predicates serves for the theory of intellect not only as a formal language for describing the laws of the intellect and intellectual activity of man. Its role is much more significant. Without exaggeration, we can say that the algebra of finite predicates in action is actually the intellect.

The structures of the algebra of finite predicates express the very essence of intellectual processes and phenomena, allowing the direct interpretation in psychological terms.

REFERENCES

1. Bondarenko, M.F. and Shabanov-Kushnarenko, Yu.P. (2007), *Teoriya intellekta* [Intelligence theory], SMIT, Kharkiv, 576 p.
2. Shabanov-Kushnarenko, S.Yu. and Khudhair Abed Thamer (2015), “Postroenie predikatnyh prototipov strukturiruemyh objektov na osnove ponyatiynogo podhoda” [Construction of structured objects predicate prototypes on the conceptual approach basis], *Uralskiy Nauchnyi Vestnik* [Bulletin of the Ukraine HAC], № 15 (146), pp. 5-12.
3. Shabanov-Kushnarenko, S.Yu. and Kalinichenko, O.V. and Kovalenko, A.I. and Shmatko, A.A. (2015), “O formalizacii znaniy na baze akgebry konechnyh predikatov” [About the finite predicates algebra knowledge based formalization] // *Zbirnyk Harkivskogo nacionalnogo universytetu Povitryanyh Syl* [Collected papers of the Air Force Kharkov National University] [Bulletin of the Ukraine HAC], № 3 (44), pp. 70-73.
4. Kalinichenko, O.V. and Shabanov-Kushnarenko, S.Yu. and Yarmak, A.V. (2015), “O predikatnyh modelyah neyavnyh znaniy v zadachah analiza informacionyh processov” [On implicit knowledge predicate models in problems of information processes analysis] // *Zbirnyk Harkivskogo nacionalnogo universytetu Povitryanyh Syl* [Collected papers of the Air Force Kharkov National University] [Bulletin of the Ukraine HAC], № 2 (43). pp. 46-49.

5. Shabanov-Kushnarenko, S.Yu. and Khudhair Abed Thamer and Leshchynska, I.O. (2013), “Razrabotka predikatnyh modeley logicheskih svyazey ponyatiy” [Development of logical connections concepts predicate models], *Zbirnyk Harkivskogo nacionalnogo universytetu Povitryanyh Syl* [Collected papers of the Air Force Kharkov National University] [Bulletin of the Ukraine HAC], № 4 (37). pp. 72-75.
6. Shabanova-Kushnarenko, L.V. “Postroenie struktury lineynogo prostranstva dlya predikatnoy modeli metriki” [Construction of the structure of a linear space for the predicate model of a metric], *Systemy obrobky informacii* [Information processing systems] [Bulletin of the Ukraine HAC], № 1 (138). pp. 118-121.
7. Kalynychenko, O. and Chalyi, S. and Shabanov-Kushnarenko, S. and Golyan, V. Discriminative Approach to Discovery Implicit Knowledge / *Computational Models for Business and Engineering Domains (7th International Conference on Intelligent Information and Engineering Systems)*, Rzeszow, Poland. 16-20.09.2014, pp. 96-108.
8. Shabanov-Kushnarenko, S.Yu. and Polyakov, D.A. and Petrova, L.G. (2011), “O postroenii bazovoy algebro-logicheskoy modeli obrazovaniya narechiy russkogo yazyka” [About the basic algebra-logical model construction of the russian language adverbs formation], *Systemy obrobky informacii* [Information processing systems] [Bulletin of the Ukraine HAC], № 5 (95). pp. 143-146.
9. Bondarenko, M.F. and Shabanov-Kushnarenko, Yu.P. and Shabanov-Kushnarenko, S.Yu. (2011), “Modeli komparatornoy identifikatsii v vide semeystv integral'nykh odno- i dvukhparametricheskikh operatorov” [Models of comparative identification in the form of families of integral one- and two-parameter operators], *Bionika intellekta* [Intelligence Bionics], № 2. pp. 86-97.
10. Bondarenko M.F. and Shabanov-Kushnarenko Yu.P. and Shabanov-Kushnarenko S.Yu. (2009), “Prakticheskiye prilozheniya komparatornoy identifikatsii lineynykh konechnomernykh obyektov” [Practical applications of comparative identification of linear finite-dimensional objects], *Bionika intellekta* [Intelligence Bionics], № 2 (71). pp. 5-12.
11. Bondarenko, M.F. and Shabanov-Kushnarenko, Yu.P. and Shabanov-Kushnarenko, S.Yu. (2009), “Metody identifikatsii mekhanizma sub"yektivnykh sotsial'no-ekonomicheskikh otsenok” [Methods for identifying the mechanism of subjective socio-economic assessments], *Bionika intellekta* [Intelligence Bionics], № 2 (71). pp. 24-30.
12. Shabanov-Kushnarenko, S.Yu. (2015), *Comparatornaya identifikaciya processov mnogomernoy kolichestvennoy ocenki* [Multidimensional quantitative estimation processes comparative identification] Saarbrucken, Deutschland: Palmarium Academic Publishing, 217 p.

Надійшла (received) 14.02.2017
Прийнята до друку (accepted for publication) 16.05.2017

Формальна база математичного апарату теорії інтелекту

Кудхаір Абед Тамер

Мета Головне завдання теорії інтелекту - математично описати закони, що регулюють інтелектуальну діяльність людини. Для цього необхідно отримати фізичні та об'єктивні методи отримання формального опису суб'єктивних станів людини, достатньо повних для практичних цілей. Людські думки, відчуття, сприйняття та усвідомлення - це всі суб'єктивні стани. У цій статті поставлено завдання розробити багатовимірну предикатну модель компараторної ідентифікації - основного експериментального методу теорії інтелекту, і обґрунтувати аксіоматику цієї моделі. **Методи.** Метод компараторної ідентифікації, розроблений в даній статті, дає можливість отримати об'єктивне знання суб'єктивних станів людського інтелекту. За методом компараторної ідентифікації з його поведінкою суб'єкт реалізує деякий кінцевий предикат, властивості якого експериментально вивчені та математично описані. Метод компараторної ідентифікації заснований на методах алгебри скінченних предикатів, булевої алгебри і аксіоматичному методі. **Результати**. Застосування методу компараторної ідентифікації дає математичний опис досліджуваних суб'єктивних станів людини, а також вид функції, що лежить в основі перетворення фізичних предметів в породжувані нею суб'єктивні образи. **Висновки.** Результати роботи математично обґрунтовують можливості застосування методу компараторної ідентифікації при моделюванні інтелекту людини.

Ключові слова: теорія інтелекту, алгебра скінченних предикатів, компараторна ідентифікація.

Формальная база математического аппарата теории интеллекта

Кудхаир Абед Тамер

Цель Главная задача теории интеллекта – математически описать законы, регулирующие интеллектуальную деятельность человека. Для этого необходимо получить физические и объективные методы получения формального описания субъективных состояний человека, достаточно полных для практических целей. Человеческие мысли, чувства, восприятие и осознание - это все субъективные состояния. В этой статье поставлена задача разработать многомерную предикатную модель компараторной идентификации – основного экспериментального метода теории интеллекта, и обосновать аксиоматику этой модели. **Методы.** Метод компараторной идентификации, разработанный в данной статье, дает возможность получить объективное знание субъективных состояний человеческого интеллекта. По методу компараторной идентификации с его поведением субъект реализует некоторое конечное предикат, свойства которого экспериментально изучены и математически описаны. Метод компараторной идентификации основан на методах алгебры конечных предикатов, булевой алгебры и аксиоматическом методе. **Результаты.** Применение метода компараторной идентификации дает математическое описание исследуемых субъективных состояний человека, а также вид функции, лежащий в основе преобразования физических предметов в порождаемые ей субъективные образы. **Выводы.** Результаты работы математически обосновывают возможности применения метода компараторной идентификации при моделировании интеллекта человека.

Ключевые слова: теория интеллекта, алгебра конечных предикатов, компараторная идентификация.

Methods of information systems protection

UDC 004.492.34 **doi: 10.20998/2522-9052.2017.1.08**

S. Gavrilenko, D. Saenko

National Technical University "Kharkiv Polytechnic Institute", Kharkiv, Ukraine

DEVELOPMENT OF THE METHOD AND PROGRAM MODEL OF THE STATIC ANALYZER OF HARMFUL FILES

The **subject** of research in this article is the methods of analyzing malicious software. The **goal** is to improve the secure functioning of computer systems (CS) and protect them from the effects of computer viruses. **Research target**: the research of modern means of software antivirus protection; analysis of the methods of creating a file signature; the development of a software model for static file detection, based on the analysis of the PE structure; the generation of tables of features that are inherent to families of viruses such as Worms, Backdor, Trojan; the obtainment binary signatures of malicious and secure software. The **methods** used are: analysis of the code in a Hex file, file hashing algorithms. The following **results** are obtained. The PE-structure of the file has been analyzed; sections have been selected for further analysis. A software model of static file detection has been developed and the analysis of secure and malicious files has been performed. Features in the form of strings and API functions have been selected; a bitmask has been formed for further file analysis. 3500 files of malicious and safe software has been scanned, their analysis has been performed. Signatures of each malicious file have been encoded and stored in the signature database. Using the developed software model, a study has been made of the possibility of detecting modifications to malicious software. **Conclusions**. A method and software model of static detection of malicious files has been developed, which allow automatic obtainment of a set of file features and draw a conclusion about the severity of the file.

Keywords: malicious software, signature, Python, portable execute, malicious application, API functions, harmful files.

Introduction

The times when the information security was reduced to the policies and protection of all devices in the corporate network are a thing of the past. Today this is clearly not enough. Cyber threats are developing rapidly, and the understanding of which direction this development is taking place plays a key role in ensuring the effective protection of enterprises [1]. If the viruses were not detected at an early stage, the recovery cost after an attack increases more than twofold. For example, the total recovery cost after a cyber attack lasting a week or more is over 1 million dollars. At the same time, the immediate reaction to the malfunction costs the company an average of 400 thousand dollars.

To date, there is a great number of anti-virus programs, but they are not capable of completely protecting the information stored on the computer, so a timely detection of malicious software is a crucial task.

Analysis of the problem and formulation of the research target

The analysis of the literature [2-8] has proven that many specialized anti-virus programs are used as protection from cyber attacks, whose work is most often based on the technologies of signature and heuristic analysis. One of the components of suspicious software analysis is static detection – according to the file analysis conducted in binary format and dynamic detection – according to their behavior in the system [9, 10].

Threat data is collected from a variety of sources, including cloud infrastructure, web crawlers, botnet monitoring services, spam traps. New cyber threats are determined by checking URLs, domains, IP addresses, file checksums, timestamps, file names, DNS data, and other features that are inherent to the programs. The received information is thoroughly checked, systematized, cleaned and analyzed both by technical means and by company analysts that are developing the antivirus software.

At the same time, to date, there are no automated systems of decision-making on the account of file severity and the building of a signature for newly detected malicious software.

The solution for the research target

For the analysis of files, two types of searches are used for detecting anomalies: static and dynamic [12-16]. Static code analysis is based on the analysis of the frequency of using the processor's commands and on the basis of this information a conclusion is made concerning the file's virus infection.

The main demerit of this method is that there is a number of complex polymorphic viruses that use almost all the processor commands and from copy to copy the set of used commands varies greatly, therefore, according to the constructed frequency table it is not possible to detect the virus.

The method of dynamic code analysis consists in analyzing the executable code in a special "environment", called the emulation buffer or "sandbox". The result of this analysis is a summary of objects that were active during the execution of the file. A modern dynamic method can check not only the

processor's commands, but also the activation of the operating system. The task of writing a full-fledged dynamic analyzer is quite laborious, not to mention the fact it requires constant monitoring of the actions of each command. This is necessary in order to not accidentally activate the destructive components of the virus algorithm.

In this paper, a program model for the static detection of files in binary format has been developed according to the analysis of the PE-structure of executable files in order to obtain features that are characteristic for malicious files [10,12,14]. The analyzed files are a family of viruses such as Worms, Backdor, Trojan. The developed software allows the analysis of the import and export sections of the file's structure and receives the names of functions and dynamic libraries, as well as information about function arguments: the names of the services used, the names of the processes to be deleted or created, various network peculiarities (IP addresses, ports, resource addresses, email addresses). The analysis of the PE-structure of the file made it possible to identify a number of parameters for further investigation. As a further study, it was decided to use the following parameters:

- Shannon's entropy of the data section; ($H = \sum_{i=0}^{N} (N_i/N) \cdot \log(N_i/N)$);
- a compiler or /packager;
- number of sections;
- availability of a certificate;
- the presence of a record during boot up;
- list of used API functions that cause suspicions in the executable file.

These parameters characterize:

- file compression;
- a packed file may raise more suspicion;
- a large number of sections can cause suspicion;
- the availibility of a certificate reduces the likelihood of file damage;
- the presence of a record during bootup causes increased attention;

As an example, 290 files of Worm type, 1050 files of Trojan type, 1153 files of Backdoor type, 1000 safe files have been analyzed in this paper. The application is written in Python with the use of pefile libraries and sqlite3 database.

The first stage of the study is the removal of information from the PE-structure of malicious software: and the search for API functions from the import and strings table (Hex-sequences of a given length, Fig. 1).

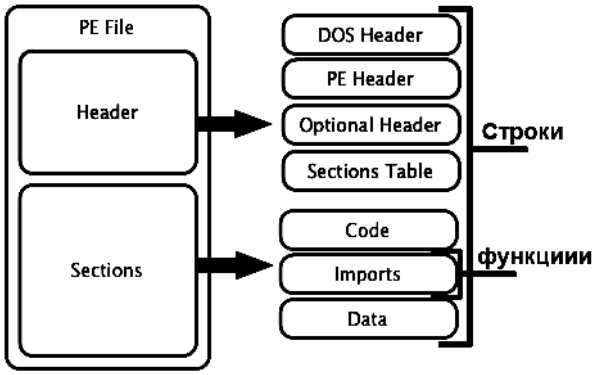


Fig. 1. PE structure of executed file

In Fig. 2 an example is shown of a PE file structure with highlighted areas of analysis.

Offset(h)	00	01	02	03	04	05	06	07	08	09	0A	0B	0C	0D	0E	0F	
00000000	4D	5A	90	00	03	00	00	00	04	00	00	00	FF	FF	00	00	
00000010	B8	00	00	00	00	00	00	00	40	00	00	00	00	00	00	00	DOS header
00000020	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	
00000030	00	00	00	00	00	00	00	00	00	00	00	00	80	00	00	00	
00000040	0E	1F	BA	0E	00	B4	09	CD	21	B8	01	4C	CD	21	54	68	
00000050	69	73	20	70	72	6F	67	72	61	6D	20	63	61	6E	6E	6F	DOS stub
00000060	74	20	62	65	20	72	75	6E	20	69	6E	20	44	4F	53	20	
00000070	6D	6F	64	65	2E	0D	0D	0A	24	00	00	00	00	00	00	00	
00000080	50	45	00	00	4C	01	03	00	8D	FA	81	4D	00	00	00	00	PE signature, PE file header
00000090	00	00	00	00	E0	00	02	01	0B	01	08	00	00	0A	00	00	PE standard fields
000000A0	00	08	00	00	00	00	00	00	9E	28	00	00	00	20	00	00	
000000B0	00	40	00	00	00	00	40	00	00	20	00	00	00	02	00	00	
000000C0	04	00	00	00	00	00	00	00	04	00	00	00	00	00	00	00	PE NT fields
000000D0	00	80	00	00	00	02	00	00	01	82	00	00	03	00	40	85	
000000E0	00	00	10	00	00	10	00	00	00	00	10	00	00	10	00	00	
000000F0	00	00	00	00	10	00	00	00	00	00	00	00	00	00	00	00	
00000100	4C	28	00	00	4F	00	00	00	00	40	00	00	A8	05	00	00	
00000110	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	Data directories
00000120	00	60	00	00	0C	00	00	00	A4	27	00	00	1C	00	00	00	
00000130	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	
00000140	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	
00000150	00	00	00	00	00	00	00	00	00	20	00	00	08	00	00	00	
00000160	00	00	00	00	00	00	00	00	08	20	00	00	48	00	00	00	
00000170	00	00	00	00	00	00	00	00	2E	74	65	78	74	00	00	00	
00000180	A4	08	00	00	00	20	00	00	00	0A	00	00	00	02	00	00	.text section header
00000190	00	00	00	00	00	00	00	00	00	00	00	00	20	00	00	60	
000001A0	2E	72	73	72	63	00	00	00	A8	05	00	00	00	40	00	00	.rsrc section header
000001B0	00	06	00	00	00	0C	00	00	00	00	00	00	00	00	00	00	
000001C0	00	00	00	00	40	00	00	40	2E	72	65	6C	6F	63	00	00	
000001D0	0C	00	00	00	00	60	00	00	00	02	00	00	00	12	00	00	.reloc section header
000001E0	00	00	00	00	00	00	00	00	00	00	00	00	40	00	00	42	
000001F0	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	
00000200	80	28	00	00	00	00	00	00	48	00	00	00	02	00	05	00	.text section
00000210	E4	20	00	00	C0	06	00	00	09	00	00	00	01	00	00	06	
00000220	00	00	00	00	00	00	00	00	50	20	00	00	80	00	00	00	
00000230	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	

Fig. 2. Example of a PE file structure

The result of the analysis of the PE malicious files structure being investigated is presented in two tables:

- a table with API-functions and libraries, in which they are included. A total of 24,945 entries were received (Fig. 3).

- table with strings (Fig. 4). A total of 175651 strings were found, the length of which varied from 6 to 70 characters.

In a similar manner, the testing of secure software has been performed. A fragment of the test results is shown in Fig. 5.

TABLE import | Поиск | Показать всё | Добавить | Дублировать | Изменить | Удалить

rowid	id	id_file	libf	funcf
1	1	1	msvbvm60.dll	_cicos
2	1	1	msvbvm60.dll	_adj_fptan
3	1	1	msvbvm60.dll	__vbafreevar
4	1	1	msvbvm60.dll	__vbaarymove
5	1	1	msvbvm60.dll	__vbastrvarmove
6	1	1	msvbvm60.dll	__vbalenbstr
7	1	1	msvbvm60.dll	__vbaend

Fig. 3. Table of found libraries and API-functions

TABLE stringl | Поиск | Показать всё | Добавить | Дублировать | Изменить | Удалить

rowid	id	id_file	strline	srtc
1	1	1	!this program cannot be run i...	44
2	1	1	`.data	6
3	1	1	msvbvm60.dll	12
4	1	1	systemmonitor	13
5	1	1	sysmon	6
6	1	1	task manager	12

Fig. 4. Table of found strings

	Функции	Количество	%
2	GetProcessHeap	277	40
3	_onexit	281	40
4	WriteFile	285	41
5	WideCharMultiByte	291	42
6	DeleteCriticalSection	296	42
7	SetlastError	298	43
8	GetModuleA	306	44
9	HeapAlloc	314	45
10	MultiByteToWideChar	315	45

Fig. 5. Fragment of the results of safe software testing

The analysis of the received data of the harmful and secure software, has allowed the allocation of the most frequently meeting functions and strings that are inherent to each family of the considered viruses and the generation of the feature table. It was decided to use 50 features for further analysis. Fig. 6 depicts a table of features that are characteristic for viruses such as Worms.

These features were later used as bit masks for file analysis. As a result of searching for selected features in files, binary vectors of malicious files and safe software were obtained (Fig. 7).

To avoid accidental errors in the transmission of data and to detect intentional changes to the file by attackers, the binary vectors of the malicious software are encoded using one of the MD5, SHA-1, or CRC algorithms.

These algorithms are widely used to obtain file signatures. Fig. 8 demonstrates examples of signatures obtained using various methods.

funcf	count(funcf)
getmodulefilenamea	219
writefile	219
getprocaddress	206
regclosekey	194
closehandle	190
getstdhandle	180
getlasterror	177
exitprocess	175
virtualalloc	171
setfilepointer	168
localalloc	167
createfilea	157
freelibrary	155

strline	count(strline)
tobject	799
integer	709
sender	687
kernel32.dll	685
jpht'@	648
graphics	550
jxht'@	486
xx.cpp	432
boolean	428
classes	395
user32.dll	376
controls	324
closehandle	309
getmodulehandlea	287
advapi32.dll	283

Fig. 6. Tables of the most common functions and strings encountered in malicious files such as Worms

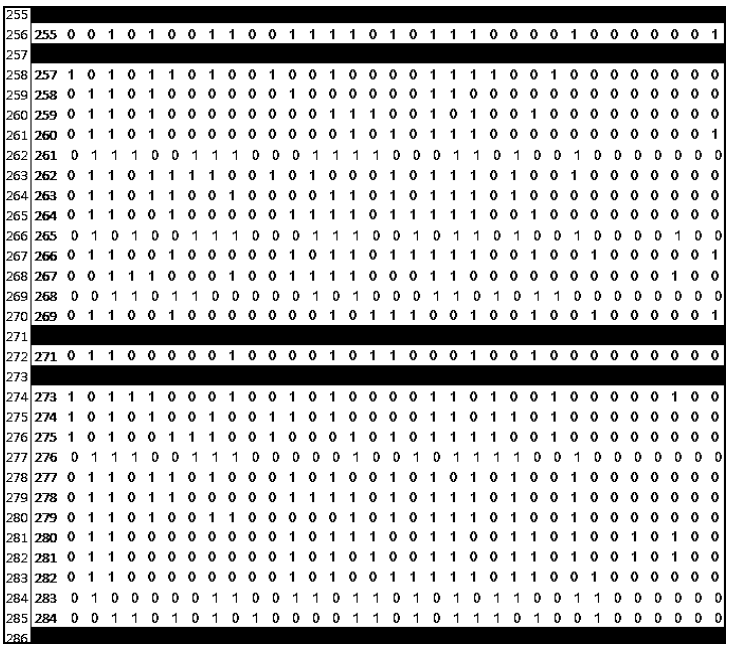


Fig. 7. An example of a malicious files and secure software scan

The received signatures allowed the formation of a signature database for the examined malicious software.

Further analysis of the software is performed by using a developed code analyzer consisting of an analysis block of the input file's PE structure, a decision-making system, a virus signature base, an output unit.

The decision-making system allows you to set the received signature coefficient of coincidence of the analyzed software with signatures that are stored in the database.

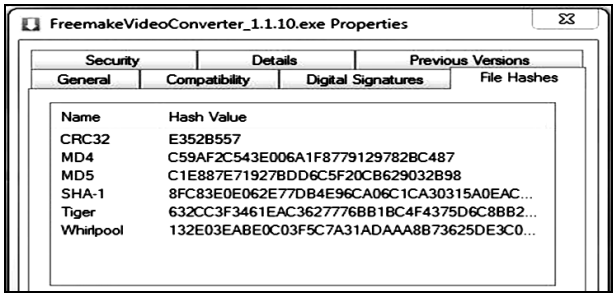


Fig. 8. Examples of file signatures

The results of testing the developed parser showed the possibility of using it to detect modified malware at 92% coincidence with the signatures that are stored in the database. With a decrease in the coefficient of coincidence, false positives appear which require additional investigation of the analyzed file, for example, by introducing a PRL block based on a nerve network.

Conclusions

In this paper, we propose a software model of static file detection, based on the analysis of the PE file structure. 3500 malicious files (such as Worms, Backdor, Trojan) and safe software have been scanned; sections of file structure import and export have been analyzed. Features in the form of strings and API functions inherent in these families of viruses have been selected; virus signatures have been generated and stored in the signature database. Using the developed software model, a static parser of malicious files has been tested to detect modifications of malicious software.

The test results revealed the possibility of using the developed automatic static parser of malicious files in the general system of anti-virus data protection. At the same time, the coefficient of coincidence of the received signatures of files with the masks template is high enough, and its reduction leads to false positives. This disadvantage can be eliminated by introducing into the decision-making system an additional analysis block, for example, based on a nerve network.

REFERENCES

1. Polugodovoy otchet po IB ot Cisco [Semi-annual report on information security from Cisco], available at: http://www.securitylab.ru/blog/personal/ Informacionnaya_bezopasnost_v_detalyah/316275.php (last accessed February 28, 2017).
2. Shelukhin, O.I., Sakalema, D.Zh. and Filinov, A.S. (2013), Obnaruzhenie vtorzheniy v kompyuternyie seti [Intrusion Detection into Computer Networks], Moskva : Hot line-Telecom, 220 p.
3. Semenov. S.G., Davydov, V.V., and Gavrilenko, S.Yu (2014), Zaschita dannyih v kompyuterizirovannyih upravlyayuschih sistemah (monografiya) [Data Protection in Computer-Aided Control Systems (monograph)] , "LAP LAMBERT ACADEMIC PUBLISHING" Germany, 236 p.
4. Igray, kak "Laboratoriya Kasperskogo" [Play as "Kaspersky Lab"], available at: http://www.kaspersky.ru/about/news/product/2017/kompaniya-otkryvayet-dostup-k-svoyey-baze-znaniy-o-kiberugrozakh-v-ramkakh-novogo-biznes-servisa (last accessed February 28, 2017).

5. Lukatsky, A.V. (2001), *Obnaruzhenie atak* [Attack Detection], St. Petersburg : VHV-Petersburg, 624 p.
6. Kaspersky, K. (2006), *Zapiski issledovatelya kompyuternyih virusov* [Notes of a researcher of computer viruses], St. Petersburg: Peter, 316 p.
7. Goshko, S.V. (2009) *Tehnologii borbyi s kompyuternyimi virusam*i [Technologies to combat computer viruses], Moscow: Solon-Press, 352 p.
8. Semenov, S., Gavrilenko, S. and Chelak V. (2016), "Developing parametrical criterion for registering abnormal behavior in computer and telecommunication systems on the basis of economic test", *Actual problems of economics*, Kiev, Vol 4 (178), pp. 451–459.
9. Tolstikhin I.O. (2009), *Razrabotka metodov klassifikatsii zlovrednyih ispolnyaemyih faylov* [Development of classification methods for malicious executable files], available at: http://www.machinelearning.ru/wiki/images/ 5/58/Tolst09techrep.pdf (last accessed February 28, 2017).
10. Ero Carrera (2007), *Win32 Static Analysis in Python*, available at: http://2006.recon.cx/en/f/lightning-ecarrera-win32-static-analysis-in-python.pdf (last accessed February 28, 2017).
11. Sikorski, M. (2012) A. *Honig Practical Malware Analysis: The Hands-On Guide to Dissecting Malicious Software*: San Francisco, 802 p.
12. AntivIrusnI tehnologIyi: v poshukah panatseyi [Antivirus technologies: in search of a panacea], available at: http://zillya.ua/antivirusni-tekhnologi%D1%97-v-poshukakh-panatse%D1%97 (last accessed February 28, 2017)
13. John Snow (2016), S*ozdaem PE-virus №1* [Create PE-virus No.1], available at: https://xakep.ru/2007/04/23/37880/ (last accessed February 28, 2017).
14. Obnaruzhenie, osnovannoe na signaturah [Signature-based detection], available at: http://mind-control.wikia.com/wiki (last accessed February 28, 2017).
15. PE Detective, available at: http://ntcore.com/pedetective.php (last accessed February 28, 2017).
16. Antivirusnyie dvizhki [Antivirus engines], available at: https://fcenter.ru/online/ softarticles/utilities/12214 (last accessed February 28, 2017).

Надійшла (received) 31.03.2017
Прийнята до друку (accepted for publication) 13.06.2017

Розробка методу і програмної моделі статичного аналізатора шкідливих файлів

С. Ю. Гавриленко, Д. М. Саєнко

Предметом дослідження в даній статті є методи аналізу шкідливого програмного забезпечення. **Мета** статті полягає в підвищенні безпеки функціонування комп'ютерних систем (КС) і захисту їх від впливу комп'ютерних вірусів. **Завдання:** дослідження сучасних засобів антивірусного захисту програмного забезпечення; аналіз методів формування сигнатури файлів; розробка програмної моделі статичного детектування файлів, що базується на аналізі PE-структури; формування таблиць ознак, притаманних родин вірусів типу Worms, Backdor, Trojan; отримання довічних сигнатур шкідливого і безпечного програмного забезпечення. Використовуваними **методами** є: аналіз коду в Hex-файлі, алгоритми хешування файлів. Отримані наступні **результати**. Проаналізовано PE-структуру файлу, обрані секції для подальшого аналізу. Розроблена програмна модель статичного детектування файлів і виконано аналіз безпечних і шкідливих файлів. Обрані ознаки у вигляді рядків і API функцій, сформована бітова маска для подальшого аналізу файлів. Виконано сканування 3500 файлів шкідливого і безпечного програмного забезпечення, проведено їх аналіз. Сигнатури кожного шкідливого файлу закодовані і збережені в базі сигнатур, За допомогою розробленої програмної моделі виконано дослідження можливості виявлення модифікацій шкідливого програмного забезпечення. **Висновок**. Розроблено метод і програмну модель статичного детектування шкідливих файлів, що дозволяє отримати набір ознак файлу в автоматичному режимі і зробити висновок про шкідливість файлу.

Ключові слова: шкідливе програмне забезпечення, сигнатура, Python, портативний запуск, шкідливий додаток, API-функції, шкідливі файли.

Разработка метода и программной модели статического анализатора вредоносных файлов

С. Ю. Гавриленко, Д. Н. Саенко

Предметом исследования в данной статье являются методы анализа вредоносного программного обеспечения. **Цель** – повышении безопасности функционирования компьютерных систем (КС) и защита их от воздействия компьютерных вирусов. **Задачи**: исследование современных средств антивирусной защиты программного обеспечения; анализ методов формирования сигнатуры файлов; разработка программной модели статического детектирования файлов, базирующаяся на анализе PE-структуры; формирование таблиц признаков, присущих семействам вирусов типа Worms, Backdor, Trojan; получение двоичных сигнатур вредоносного и безопасного программного обеспечения. Используемыми **методами** являются: анализ кода в Hex-файле, алгоритмы хеширования файлов. Получены следующие **результаты**. Проанализирована PE-структура файла, выбраны секции для последующего анализа. Разработана программная модель статического детектирования файлов и выполнен анализ безопасных и вредоносных файлов. Выбраны признаки в виде строк и API функций, сформирована битовая маска для дальнейшего анализа файлов. Выполнено сканирование 3500 файлов вредоносного и безопасного программного обеспечения, проведен их анализ. Сигнатуры каждого вредоносного файла закодированы и сохранены в базе сигнатур, С помощью разработанной программной модели выполнено исследование возможности обнаружения модификаций вредоносного программного обеспечения. **Выводы**. Разработан метод и программная модель статического детектирования вредоносных файлов, позволяющая получить набор признаков файла в автоматическом режиме и сделать вывод о вредоносности файла.

Ключевые слова: вредоносное программное обеспечение, сигнатура, Python, портативний запуск, вредоносное приложение, API-функции, вредоносные файлы.

UDC 004.94 **doi: 10.20998/2522-9052.2017.1.09**

V. Kosenko[1], O. Malyeyeva[2], E. Persiyanova[3], A. Rogovyi[4]

[1] SE "Kharkiv Scientific-Research Institute of Mechanical Engineering Technology", Kharkiv, Ukraine
[2] National Aerospace University – Kharkiv Aviation Institute, Kharkiv, Ukraine
[3] SE "Southern National Design & Research Institute of Aerospace Industries", Kharkiv, Ukraine
[4] National Technical University "Kharkiv Polytechnic Institute", Kharkiv, Ukraine

ANALYSIS OF INFORMATION-TELECOMMUNICATION NETWORK RISK BASED ON COGNITIVE MAPS AND CAUSE-EFFECT DIAGRAM

The **subject matter** of the article is the processes of analysis and risk assessment of information and telecommunications networks. The **aim** is to reduce the potential losses caused by the risks of information and telecommunications network (ITN) functioning by taking timely risk management measures. The **objectives** are: classification of ITN risks, highlighting the main factors and causes of their occurrence; formation of a systematic presentation of risks to identify their manifestation and consequences; development of the method for assessing the influence of the risk and private risk on probable consequences; obtaining a quantitative risk assessment of ITN. The **methods** used are: system analysis of risks, method of cognitive maps, cause-and-effect analysis. The following **results** are obtained: classification of private risks of ITN according to the reasons and the factors of their occurrence is made; the negative consequences affecting the basic characteristics of the operation of ITN are defined; as a result, the structural system model of ITN risks is formed, in which the relationships between the elements of the main aspects of risk are shown; the method based on the theory of causal analysis is suggested in order to quantify the risk impact on ITN functioning. The risk model is based on the construction and analysis of probabilistic or fuzzy cognitive maps. Experts estimate the level of influence of private risks on the characteristics of the network in order to make decisions on risk management. The generalized structure of the cause-effect diagram of the risk factors, manifestation and consequences is developed; on ITN basis the method for quantifying the probability of risk consequences is suggested. The quantitative assessment of probable malfunctioning of the network that is determined by a specific effect (taking into account ITN probability), which is caused by private risks is also made. **Conclusion.** The suggested approach for quantitative assessment of ITN risk is based on the method of cause-and-effect analysis and enables taking into account both the factors causing it and probable consequences. The obtained results can be used to determine probable failures and losses in ITN functioning on the basis of the information about the degree of risk factors effects, risk events and consequences, and the cause-effect relationships between them. Thus, potential losses can be identified; measures to manage the risks of ITN functioning can be taken.

Keywords: information-telecommunication network, risk factors, consequences, cause-effect diagram, influence factors.

Introduction

Under continuously improving concepts of developing information and telecommunication networks (ITN), creating new network technologies and growing demand for services, there is a trend of their "convergence", i.e. combining into more complex structures and technologies. There is an interpenetration of information environments different in occurrence and principles of the work.

The European Commission defined the convergence in telecommunications as the ability of various network platforms to provide the same set of services or the combination of end devices, such as a telephone, a personal computer and a TV receiver in the form of a single terminal [1].

This term includes all the changes in telecommunications that relate to the development and integration of services and networks, the replacement of old technologies with new ones, and so on. Information and telecommunication components are connected on the basis of a multiservice platform.

Therefore, to provide high-quality transport services while transferring information is becoming increasingly difficult. In order to solve this problem system analysis and risk assessment of information and telecommunication networks (ITN) for further evaluation of damage and decision-making as for risk counter should be performed.

The analysis of the problem and formulation of the task

The information security of telecommunication systems is subjected to a wide range of threats: from virus infection, which can be handled locally, to regulatory collisions that require the work of legislative and law enforcement authorities. Hence, there are risks that can have a negative impact on ITN performance.

Today, ITN protection is regulated by the standards of the Technical Laboratory of Information (ITL) at the National Institute of Standards and Technology (NIST) [2].

The work of Ross R. [3] and Paulsen S. [4] is devoted to the analysis of vulnerability and risk assessment of ITN. The problems of information security and methods of protecting information activity are considered by such authors as Zadirak V. [5], Gornitnkaya D. [6], Buryachok V. [7], Furmanov A. [8], Boyarchuk A. [9]. The classification of network attacks, threats to information security [10] has been made and methods for their detection have been determined [11] so far. The issues of decision-making as for the management of information security of networks are considered in the works of Voropaev V. [10], Sklyar V. [12].

Currently, the majority of scientific developments are conducted in the field of information risk (IR) assessment without system accounting of ITN causes,

factors and interaction with other types of ITN risks. In addition, there is no classification of the causes and risk factors identified as threats.

Therefore, this article deals with the development of a systematic presentation of the ITN risks to identify the relationship between the factors that cause risks, risks manifestation and their consequences as well as with the development of the approach that enables assessing the impact of risks on ITN functioning.

Task solution

In the systemic risk model, we define the basic categories to identify the relationships between their elements (Fig. 1).

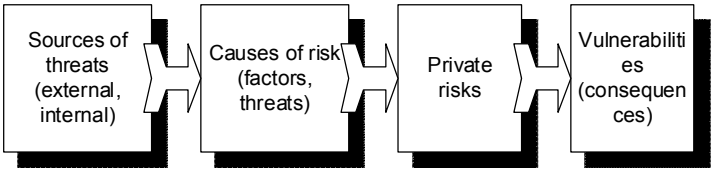


Fig. 1. Main categories of risk analysis

The procedure of analysis and risk assessment presupposes the following stages:

- analysis of risk factors (potential sources of threats),
- listing ITN key risks, which can significantly affect ITN functioning,
- analysis of the consequences of of risk events,
- analysis of cause-effect relationships between elements of the categories of the system risk model,
- assessment of the probability and cost of ITN risk.

To analyze risk factors the types of ITN risks should be classified. According to the reasons of their occurrence, the ITN risks can be divided into two main categories:

- objective risks arising as a result of disruptions in the operation of information transmission channels,
- subjective risks caused by the loss of information and ITN misuse.

The ITN risks can also be classified as internal and external factors as for their occurrence. Here, the period of ITN life cycle (LC) can be taken into account. Risks arise both at the stage of design (or modernization), and at the stage of operation (while transferring data and controlling processes).

Taking into account the factors of their occurrence, we group the internal risks as:

- risks related to the provision of services (including those with peak loads) that arise during the operation phase,
- risks of fraud, which may be the result of illegal connection, theft of traffic, etc. that arise during the operational phase,

External risks (due to the influence of external environment) include:

- part of the risks of developing and introducing new services that are related to the development of networks and the construction of communication facilities, which can be a consequence of the breakdown of terms by contract organizations, lack of funds, etc., and risks arise at the stage of modernization,
- the risks caused by the legislation imperfection that can arise at any stage of the LC.

Taking into account the categories of factors (technical, process, human, external), we list the possible ITN risks, indicating the causes of their occurrence (Table 1).

Technical factors cause risks associated with improper or unexpected function of ITN technological properties. Factors of the process cause risks associated with the problems of performing internal processes, as a result of which they do not work as expected. The human factor causes risks associated with problems caused by actions (or inaction) of people in certain situations; both insiders and external users of the network may cause problems. External factors are the causes of the risks associated with external, uncontrolled events. In most cases, such events cannot be anticipated and planned [13].

Risks have negative consequences that negatively affect the following main characteristics of ITN functioning:

1. Network performance, which is related to the concepts of reliability and survivability. The differences in these concepts are due to the causes and factors of the risks. Reliability of the communication network covers the influence of the main internal factors – accidental failures of technical means caused by aging processes, defects in manufacturing technology or errors of maintenance personnel. The survivability (stability) of a communication network characterizes ITN ability to maintain full or partial operability under the action of causes that lie outside the network (spontaneous or intentional) and lead to the destruction or significant damage to some of ITN elements.

2. Network performance (or throughput) is related to performance parameters, since the implementation of the required load must be carried out with specified quality parameters.

3. Information security during the storage and transfer of data is associated with violations of confidentiality and the integrity of information. Attempts to violate the privacy and integrity of information can be made by ill-wishers or competitors. In addition, security is affected by failures in the operation of machinery and software systems under the influence of radio electronic signals.

4. The parameter of economic efficiency refers to the ITN characteristics both at the stage of ITN creation, and at the stages of operation and modernization. It is connected with the problems of legal and business risk.

Table 1. **Categories of factors and causes of ITN risks**

Factor category	Risk reasons	Private risks
Internal risks		
Technical factors	P_{11} – lack of capacity; P_{12} – lack of performance; P_{13} – improper maintenance; P_{14} –equipment deterioration	R_1 – Risk of equipment failure
	P_{21} – incompatibility; P_{22} – improper Configuration Management; P_{23} – improper Change Management; P_{24} – incorrect security settings; P_{25} – unsafe programming practices; P_{26} – improper testing	R_2 – Risk of crashing software
	P_{31} – design Problems; P_{32} – specification problems; P_{33} – integration problems; P_{34} – complexity of the system	R_3 – Risk of error in network design
Process factors	P_{41} – Improper workflow; P_{42} - Inadequate documentation of the process; P_{43} – misunderstanding of roles and responsibilities; P_{44} – incorrect information flows; P_{45} – improper escalation of problems; P_{46} – ineffective transfer of tasks	R_4 – Risk of error in network processes (design and execution)
	P_{51} – lack of status monitoring; P_{52} – lack of metrics; P_{53} – lack of periodic analysis; P_{54} – inadequate ownership of the process	R_5 – Risk of process control error
	P_{61} – staffing problems; P_{62} – financing problems; P_{63} – learning and development shortcomings; P_{64} – procurement issues	R_6 – Risk of error in supporting processes
Human factor	P_{71} – random error; P_{72} – ignorance P_{73} –non-observance of instructions	R_7 – Risk of unintentional action
	P_{81} – fraud; P_{82} – sabotage; P_{83} – theft; P_{84} – vandalism	R_8 – Risk of willful acts
	P_{91} – lack of skills; P_{92} – lack of knowledge; P_{93} – absence of instructions; P_{94} – inaccessibility of people	R_9 – Risk of inaction
External risks		
External factors	P_{101} – weather phenomena; P_{102} – fire; P_{103} – flooding; P_{104} – earthquake; P_{105} – riots; P_{106} – quarantine	R_{10} – Disaster risk
	P_{111} – non-compliance with requirements; P_{112} – changes in legislation; P_{113} – litigation	R_{11} – Legal risk
	P_{121} – problems with suppliers; P_{122} – unfavorable market conditions; P_{123} – adverse economic conditions	R_{12} – Business risk
	P_{131} – supply problems with materials; P_{132} – dependence on emergency services; P_{133} – problems with power supply; P_{134} – transport Problems	R_{13} – Risk of substandard services

Risks have a negative impact on the basic properties of information and ITN functioning [14].

Thus, violations in the processes of collecting information, processing it, failures in the technology of data transmission lead to information leakage, unauthorized copying and distortion (forgery). There can happen the blocking of systems and information transfer delay.

Risks due to hardware-software breakdowns and radio electronic disturbances are associated with viruses and "bookmarks" – interception devices. Not only viruses disturb, but also limit the speed of transmission, and can also block the network operation.

As a result of accidents, natural disasters, direct destruction, the breakdown of technical communication systems information carriers can be abducted.

Let's develop a structural system model of ITN risks, in which we will map the interdependence between the elements of the risk main aspects (Fig. 2). With the help of this model, the full set of cause-effect relationships from the causes of risks to their consequences and the impact on the main characteristics of the ITN can be determined.

According to the suggested approach, the risk assessment is carried out in stages. At the first stage, a structural diagram is constructed; private risks that cause the factors and probable consequences of risk occurrence are identified. The interrelationships between these components are presented in the form of a cause-effect diagram [11].

Since the number of relationships between risk factors and risk events is large, for the sake of clarity of the subsequent analysis, the relationship between the risk factors with risk manifestation and consequences is presented in the form of tables (Tables 2, 3), identifying each of the consequences in the form of a variable with the corresponding index.

To quantify the impact of IR on ITN functioning, the method based on the theory of causal analysis is suggested for use [15].

The risk model in the form of a cause-effect network can be based on the construction and analysis of probabilistic or fuzzy cognitive maps [16]. The cognitive map is defined as a tuple of sets:

$$K = (\{P, R, S\}, F, \{B, C\}),$$

where $\{P, R, S\}$ is the finite set of elements, which in this case consists of three subsets (factors, risks, consequences);

F is the finite set of connections between elements;

$\{B, C\}$ is the finite set of weights of these connections.

The cognitive map is transformed into a familiar oriented graph, at the vertices of which the key elements of the modeling object are located, interconnected by arcs that reflect the cause-effect relationships between them. These relationships characterize the degree (influence) of the elements' impact on each other and are set by means of coefficients (determining the probability of risk occurrence as a result of this factor, or consequences due to the risk origin) or by linguistic terms (determining the degree of influence):

$$B=\{b_{i,j}\ i=1..n, j=1..m\},\ C=\{c_{jk}\ j=1..m, k=1..h\}.$$

The values $b_{i,j}$ and c_{jk} can be determined by objective (on the basis of statistical data) or subjective method (by expert assessments) based on past experience.

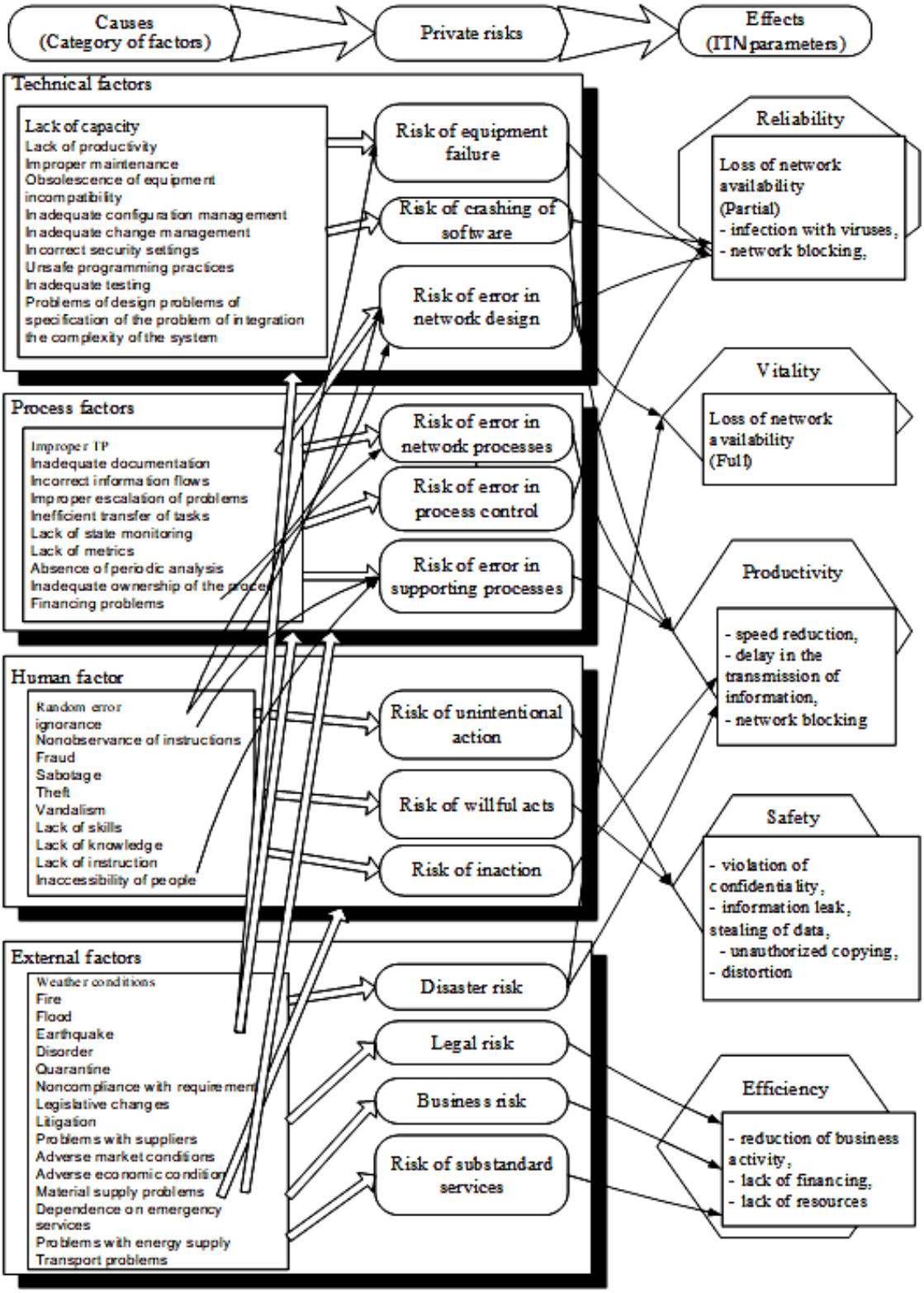


Fig. 2. Systemic risk model of ITN

Table 2. **The matrix of coefficients of factors' influence on private risks of ITN (fragment)**

Risk factors	**Private risks**												
	R_1	R_2	R_3	R_4	R_5	R_6	R_7	R_8	R_9	R_{10}	R_{11}	R_{12}	R_{13}
P_{11}	$b_{11,1}$	$b_{11,2}$	-	-	-	-	-	-	-	-	-	-	-
P_{12}	$b_{12,1}$	$b_{12,21}$	$b_{12,3}$	-	-	-	-	-	-	-	-	-	-
P_{13}	$b_{13,1}$	$b_{13,2}$	-	$b_{13,4}$	-	$b_{13,6}$	$b_{13,7}$	$b_{13,8}$	$b_{13,9}$	-	-	-	-
P_{14}	$b_{14,1}$	-	-	-	-	-	-	-	-	-	-	-	-
P_{21}	-	$b_{21,2}$	-	$b_{21,4}$	-	-	-	-	-	-	-	-	-
P_{22}	-	$b_{22,2}$	-	$b_{22,4}$	-	-	-	-	-	-	-	-	-
P_{23}	-	$b_{23,2}$	-	$b_{23,4}$	-	-	-	-	-	-	-	-	-
P_{24}	-	$b_{24,2}$	-	$b_{24,4}$	-	-	-	-	-	-	-	-	-
P_{25}	-	$b_{25,2}$	-	$b_{25,4}$	-	-	-	-	-	-	-	-	-
P_{26}	-	$b_{26,2}$	-	$b_{26,4}$	-	-	-	-	-	-	-	-	-
.....													
P_{131}	-	-	-	-	-	$b_{131,6}$	$b_{131,7}$	$b_{131,8}$	$b_{131,9}$	-	-	$b_{131,12}$	$b_{131,13}$
P_{132}	-	-	-	-	-	-	$b_{132,7}$	$b_{132,8}$	$b_{132,9}$	-	-		$b_{132,13}$
P_{133}	$b_{133,9}$	-	-	-	-	$b_{133,6}$	$b_{133,7}$	$b_{133,8}$	$b_{133,9}$	$b_{133,9}$	-	$b_{133,12}$	$b_{133,13}$
P_{134}	-	-	-	-	$b_{134,7}$	-	$b_{134,7}$	$b_{134,8}$	$b_{134,,9}$	-	-		$b_{134,13}$

Table 3. **Matrix of risk factors for possible consequences**

Private risks	**Effects**												
	Reliability		**Vitality**	**Performance**			**Security**				**Efficiency**		
	S_1	S_2	S_3	S_4	S_5	S_6	S_7	S_8	S_9	S_{10}	S_{11}	S_{12}	S_{13}
R_1	-	c_{12}	c_{13}	c_{14}	c_{15}	c_{16}	-	-	-	-	-	-	-
R_2	c_{21}	c_{22}	-	c_{24}	c_{25}	c_{26}	-	-	-	-	-	-	-
R_3	-	c_{32}	-	c_{34}	c_{35}	c_{36}	-	-	-	-	-	-	-
R_4	-	c_{42}	-	c_{44}	c_{45}	c_{46}	-	-	-	-	-	-	-
R_5	-	c_{52}	-	-	-	-	-	-	-	c_{510}	-	-	-
R_6	-	-	-	c_{44}	c_{45}	c_{46}	-	-	-	c_{410}	-	-	-
R_7	-	c_{72}	-	c_{74}	c_{75}	c_{76}	c_{77}	c_{78}	c_{79}	c_{710}	-	-	-
R_8	-	c_{82}	c_{83}	c_{84}	c_{85}	c_{86}	c_{87}	c_{88}	c_{89}	c_{810}	-	-	-
R_9	-	-	-	c_{94}	c_{95}	c_{96}	-	-	-	-	-	-	-
R_{10}	-	c_{102}	c_{103}	-	-	-	-	-	-	-	-	-	-
R_{11}	-	-	-	-	-	-	-	-	-	-	c_{1111}	-	-
R_{12}	-	-	-	-	-	-	-	-	-	-	-	c_{1212}	-
R_{13}	-	-	-	-	-	-	-	-	-	-			c_{1313}

The factor of influence of the factor of risk occurrence $b_{i,j}$ is determined on basis of the frequency of occurrence of this type of risk, based on statistical information or based on estimates of forecasting. Recently, the reliability and security indicators of the network are reduced as a result of the following events (which are related to the risks of software failure and deliberate actions):

the selection of keys / passwords (password attacks) - 13.9% of the total;

replacement of IP-address (IP spoofing) - 12,4%;

denial of service (DoS-attacks) - 16.3%;

analysis of traffic (sniffing packages) - 11.2%;

scanning (network intelligence) - 15.9%;

substitution of data transmitted over the network (data and software manipulation) -15.6%;

other methods (viruses and programs "Trojan Horse") - 14.7% [7].

It is necessary to take into account the fact that not all ITN risks can be fully realized or implemented in general in this network; the same type of threat can cause significant or minor damage. Therefore, to make a decision as for ITN risk management, it is necessary to determine the degree of private risk influence on the characteristics of the network function [10]. The level of risk influence c_{jk} can also be determined by experts according to the following scale:

- 0 - the risk does not actually affect the given network characteristic;
- 0.25 - the risk has little impact;
- 0.5 - the risk affects at average degree;
- 0.75 - the risk has a significant impact;
- 1.0 - the risk has a direct impact.

The knowledge of the structure of the causal system can be used to transform the statistical description of inputs into the description of outputs.

To do this, we form a recursive system of equations isomorphic to the structural diagram, the coefficients of which act as coefficients of influence [17]. In our case, we can draw a parallel between the

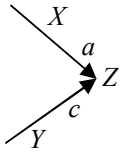
structural coefficients of influence and the probabilities of manifestation of specific events (factors, risks, consequences).

In accordance with the theory of causal analysis the following rules are used for formulating equations:

1. The value of the variable is defined by one input equal to the input value multiplied by the structural coefficient.

$X \xrightarrow{a} Y$ means $Y = aX$.

2. The value of a variable, defined by several input quantities, is equal to the sum of the input values multiplied by their structural coefficients. The order of summation does not matter.



means $Z = aX + cY$

3. The ways that escape from a variable when writing equations for this variable are not taken into account, but each incoming arrow indicates an element that must be considered.

Structural equations describe direct connections. In order to take into account the indirect links, the reduction rules are used: if one variable defines the second variable, and the other determines the third, the value of the third variable can be expressed as the value of the first variable multiplied by the product of the structure coefficients along the chain.

The same principle is applied when a chain has more than two links.

$X \xrightarrow{a} Y \xrightarrow{c} Z$ means $Z = acX$.

The generalized structure of the cause-and-effect diagram of the factors, manifestations and consequences of ITN risks is presented in Fig. 3.

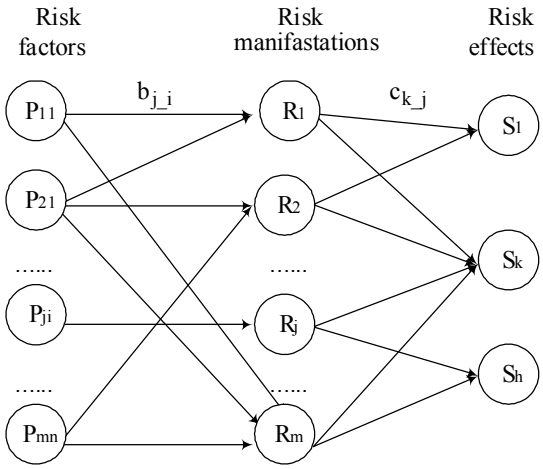


Fig. 3. Structural diagram of the cause-effect diagram

On the diagram $b_{j,i}$, $0 \le b_{j,i} \le 1$ is the coefficient of influence of the i-th factor on the occurrence of the j-th manifestation of risk; c_{kj}, $0 \le c_{kj} \le 1$ is the coefficient of influence of the j-th manifestation of risk on the k-th consequence.

Then the estimation of the probability of occurrence of the k-th consequence is made according to the formula:

$$P(S_k) = \sum_i \sum_j b_{j,i} c_{kj} .$$

For example, in accordance with the systemic representation of risk, the probability of "distortion of information" event is determined in accordance with the causal diagram (Fig. 4) and is calculated by the formula:

$$P(S_{10}) = c_{105}(b_{5,13} + b_{5,1} + b_{5,2} + b_{5,3} + b_{5,4}) +$$
$$+c_{106}(b_{6,13} + b_{6,1} + b_{6,2} + b_{6,3} + b_{6,4} + b_{13,1} + b_{13,2} +$$
$$+b_{13,3} + b_{13,4}) + c_{107}(b_{7,13} + b_{7,1} + b_{7,2} + b_{7,3}) +$$
$$+c_{108}(b_{8,13} + b_{8,1} + b_{8,2} + b_{8,3} + b_{8,4}).$$

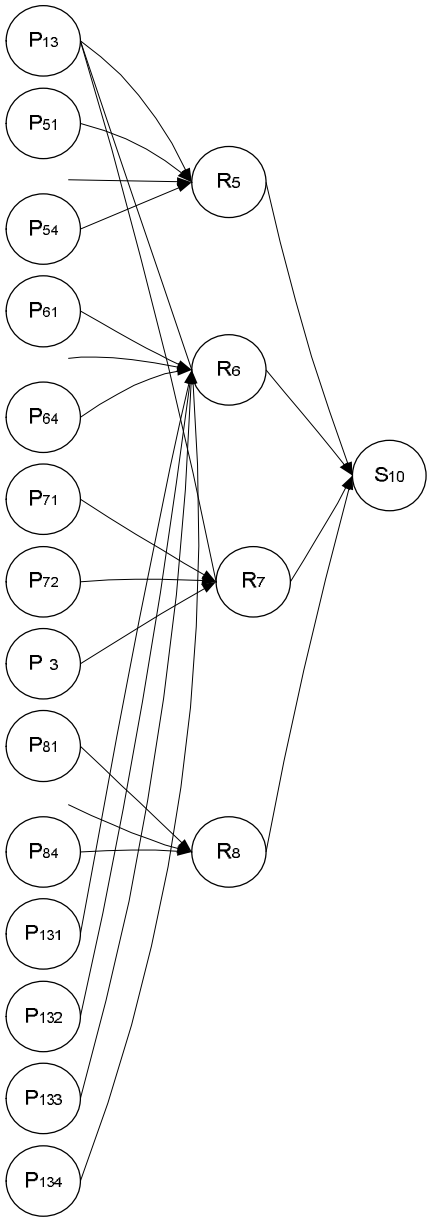


Fig. 4. Example of a cause-effect diagram for "distortion of information" event (consequences)

Thus, knowing the degree of impact (in the form of impact factors) of risk factors, risk events and consequences, as well as cause-effect relationships between them, possible failures and losses in ITN functioning can be determined.

Possible damage to the functioning of the network G_{kj}, determined by the k-th consequence, which is caused by the j-th private risk G_{kj} is calculated according to the relationship [18]:

$$G_{kj} = P(S_k)\, H(R_j \rightarrow S_k) f_k ,$$

where $P(S_k)$ is the probability of k-th consequence;

$H(R_j \rightarrow S_k)$ is the the risk R_j impact on the characteristics S_j,

f_i is the indicator reflecting the value of the k-th characteristic.

Conclusions

The suggested method for quantitative assessment of ITN risk is based on the method of cause-and-effect analysis and enables taking into account both the factors causing it, and probable consequences.

In connection, identifying potential losses can be made, as well as the measures to manage the risks of ITN functioning can be taken.

It should be noted that the main problem in the application of the suggested method is the complexity of obtaining the values of the structural coefficients of the influence of factors, private risks of ITN and their consequences.

REFERENCES

1. Konvergencija setej, tehnologij i uslug [Convergence of networks, technologies and services], available at: http://studopedia.su/6_48249_konvergentsiya-setey-tehnologiy-i-uslug.html (last accessed February 1, 2017).
2. Cichonski, P., Millar, T., Grance, T. and Scarfone, K. (2012), *Computer Security Incident Handling Guide*, National Institute of Standarts and Technology, 79 p.
3. Ross, R. (2012), *Guide for Conducting Risk Assessments,* National Institute of Standards and Technology, 95 p.
4. Paulsen, S. and Boens, J. (2012), *Summary of the Workshop on information and communication technologies supply chain risk management*, National Institute of Standards and Technology, 21 p.
5. Zadiraka, V.K. and Kudin, A.M. (2012), "Osobennosti realizacii kriptograficheskih i steganograficheskih sistem po principu oblachnyh vychislitelnyh tehnologii" [Peculiarities of realization of cryptographic and steganographic systems according to the principle of cloud computing technologies], *Shtuchnyi intelekt* [Artificial Intelligence], No. 3(55), pp. 438–444.
6. Hornytska, D.A., Zakharova, M.V. and Kladnytskiy, A.I. (2012), "Analysis and assessment system of the state of information security, socio-technical resources of attacks", *Information security*, No 2, pp. 70-74.
7. Burachok, V. (2013), "Technology of vulnerabilities using of web-resources in the organization and conducting of network reconnaissance informational telecommunication systems", *Network & Internet security*, Vol. 19, Issue 2, pp. 83-87.
8. Furmanov, A.A., Lahizha, I.N. and Harchenko, V.S. (2009), "[Modeling of guaranteed service-oriented architectures for attacks with using of vulnerabilities", *Radioelectronic and computer systems*, No. 7 (41), pp. 65-69.
9. Boyarchuk, A. (2011*), Safety of critical infrastructures: mathematical and engineering methods of analysis and support,* National Aerospace University "KhAI", Kharkiv, 641 p.
10. Voropaeva, V.Y., Shcherbov, I.L. and Haustova, E.D. (2013), “Upravlenie informacionnoi bezopasnostiu informacionno-telekommunikacionih system na osnove modeli «plan-do-checkact»” [Information Security Management information and telecommunication systems based on the model «PLAN-DO-CHECK-ACT»], *Naukovi pratsi DonNTU. Seriya: ob-chyslyuval'na tekhnika ta avtomatyzatsiya* [Proceedings of Donetsk National Technical University. Series: Computers and Automation], No. 253 (201), pp. 104-110.
11. Prikhodko, T.A. (2011), Issledovanie voprosov bezopasnosti lokal'nyh setej na kanal'nom urovne modeli OSI [Investigation of security issues of local networks on the channel level of the OSI model], available at: http://ea.dgtu.donetsk.ua:8080/handle/123456789/2068 (last accessed February 1, 2017).
12. Sklyar, V.V. (2011), "Methodology of risk analysis of functional safety of information-control systems", in *Safety of critical infrastructures: mathematical and engineering methods of analysis and provision*, Kharchenko, V.S. (Ed.), National Aerospace University "KhAI", Kharkiv, Section 12, pp. 360-408.
13. Nochevnov, E.V. (2016), ["Klassifikacija faktorov riska v upravlenii proektami v oblasti informacionnyh i kommunikacionnyh tehnologij" [Classification of risk factors in project management in the field of information and communication technologies], *Upravlenie proektami i programmami* [Project and Program Management], No. 2, pp. 44-53.
14. Chto takoe informacionnaja bezopasnost' telekommunikacionnyh sistem? [What is the information security of telecommunications systems?], available at: http://camafon.ru/informatsionnaya-bezopasnost/telekommunikatsionnyih-sistem (last accessed February 1, 2017).
15. Hayes, D. (1981), *Causal analysis in statistical studies*, Moscow, Finance and Statistics, 255 p.
16. Kiryanov, V.V. Usovershenstvovanie organizacionnyh osnov sozdanija kompleksnoj sistemy zashhity informacii v informacionno–telekommunikacionnoj sisteme [Improvement of organizational bases for creating a comprehensive information security system in the information and telecommunication system], available at: http://masters.donntu.org/2014/frt/kiryanov/diss/index.htm (last accessed February 1, 2017).
17. Maleeva, O.V. and Sytnik N.I. (2007), "Analysis of the interaction of internal and external risks on the basis of the cause-effect diagram", *Radioelectronic and computer systems*, No. 1, pp. 73-76.

18. Nadezhdin, E.N. and Sheptukhovsky, V.A. Metodika ocenivanija riskov informacionnoj bezopasnosti v vychislitel'nyh setjah obrazovatel'nyh uchrezhdenij [The method of assessing the risks of information security in the computer networks of educational institutions], available at: http://www.masters.donntu.org/2014/frt/vashakidze/library/8.htm (last accessed February 1, 2017).

Received (Надійшла) 10.02.2017
Accepted for publication (Прийнята до друку) 16.05.2017

Аналіз ризиків інформаційно-телекомунікаційної мережі на основі когнітивних карт і причинно-наслідкової діаграми

В. В. Косенко, О. В. Малєєва, О. Ю. Персіянова, А. І. Роговий

Предметом вивчення в статті є процеси аналізу та оцінки ризиків інформаційно-телекомунікаційних мереж. **Мета** - зниження потенційних втрат, зумовлених ризиками функціонування інформаційно-телекомунікаційної мережі (ІТМ), шляхом своєчасного вжиття заходів з управління ризиками. **Завдання:** класифікація ризиків ІТМ з виділенням основних факторів і причин їх виникнення; формування системного уявлення ризиків для виявлення їх проявів і наслідків; розробка методу оцінки ступеня впливу причин на прояв ризику і приватних ризиків на можливі наслідки; отримання кількісної оцінки ризиків ІТМ. Використовуваними **методами** є: системний аналіз ризиків, метод когнітивних карт, причинно-наслідковий аналіз. Отримані такі **результати**. Проведена класифікація приватних ризиків ІТМ з причин та за факторами їх виникнення. Визначено негативні наслідки, що негативно впливають на основні характеристики функціонування ІТМ. В результаті сформована структурна системна модель ризиків ІТМ, в якій відображені взаємозв'язки між елементами основних аспектів ризику. Для кількісної оцінки впливу ризику на функціонування ІТМ запропонований метод, заснований на теорії причинного аналізу. Модель ризиків заснована на побудові та аналізі імовірнісних або нечітких когнітивних карт. Для прийняття рішень з управління ризиками експертами визначається рівень впливу приватних ризиків на характеристики мережі. Розроблено узагальнену структуру причинно-наслідкової діаграми чинників, проявів і наслідків ризиків. На її основі запропоновано спосіб кількісної оцінки можливості виникнення наслідків ризиків. Також проводиться кількісна оцінка можливих збитків для функціонування мережі, що визначається конкретним наслідком (з урахуванням його ймовірності), який викликаний приватними ризиками. **Висновки.** Запропоновано підхід для кількісної оцінки ризику ІТМ заснований на методі причинно-наслідкового аналізу та дозволяє враховувати як чинники, що його викликають, так й можливі наслідки. Отримані результати можна використовувати для визначення можливих збоїв і втрат при функціонуванні ІТМ на основі інформації про ступінь впливу факторів ризику, ризикових подій і наслідків, а також причинно-наслідкових залежностей між ними. Стає можливим визначати потенційні втрати, а також вживати заходів з управління ризиками функціонування ІТМ.

Ключові слова: інформаційно-телекомунікаційна мережа, фактори, ризики, наслідки, причинно-наслідкова діаграма, коефіцієнти впливу.

Анализ рисков информационно-телекоммуникационной сети на основе когнитивных карт и причинно-следственной диаграммы

В. В. Косенко, О. В. Малеева, Е. Ю. Персиянова, А. И. Роговой

Предметом изучения в статье являются процессы анализа и оценки рисков информационно-телекоммуникационных сетей. **Цель** - снижение потенциальных потерь, обусловленных рисками функционирования информационно-телекоммуникационной сети (ИТС), путем своевременного принятия мер по управлению рисками. **Задачи**: классификация рисков ИТС с выделением основных факторов и причин их возникновения; формирование системного представления рисков для выявления их проявлений и последствий; разработка метода оценки степени влияния причин на проявление риска и частных рисков на возможные последствия; получение количественной оценки рисков ИТС. Используемыми **методами** являются**:** системный анализ рисков, метод когнитивных карт, причинно-следственный анализ. Получены следующие **результаты.** Произведена классификация частных рисков ИТС по причинам и по факторам их возникновения. Определены негативные последствия, отрицательно влияющие на основные характеристики функционирования ИТС. В результате сформирована структурная системная модель рисков ИТС, в которой отображены взаимосвязи между элементами основных аспектов риска. Для количественной оценки влияния риска на функционирование ИТС предложен метод, основанный на теории причинного анализа. Модель рисков основана на построении и анализе вероятностных или нечетких когнитивных карт. Для принятия решений по управлению рисками экспертами определяется уровень влияния частных рисков на характеристики сети. Разработана обобщенная структура причинно-следственной диаграммы факторов, проявлений и последствий рисков. На ее основе предложен способ количественной оценки возможности возникновения последствий рисков. Также производится количественная оценка возможного ущерба для функционирования сети, определяемого конкретным последствием (с учетом его вероятности), который вызван частными рисками. **Выводы.** Предложенный подход для количественной оценки риска ИТС основан на методе причинно-следственного анализа и позволяет учитывать, как вызывающие его факторы, так и возможные последствия. Полученные результаты можно использовать для определения возможных сбоев и потерь при функционировании ИТС на основе информации о степени воздействия факторов риска, рисковых событий и последствий, а также причинно-следственных зависимостей между ними. Становится возможным определять потенциальные потери, а также принимать меры по управлению рисками функционирования ИТС.

Ключевые слова: информационно-телекоммуникационная сеть, факторы, риски, последствия, причинно-следственная диаграмма, коэффициенты влияния.

УДК 004.94 **doi: 10.20998/2522-9052.2017.1.10**

V. Oleshchenko, V. Pevnev

National Aerospace University – Kharkiv Aviation Institute, Kharkiv, Ukraine

DEVELOPMENT OF DIGITAL STEGANOGRAPHY TECHNIQUES FOR COPYRIGHT PROTECTION, BASED ON THE WATERMARK

The increasing value of information protection is an important question in our fast-paced world. Especially acute is the question of copyright protection, which is against the backdrop of increasing the number of generated content, has become a real problem. The unauthorized use of foreign Intellectual Property of liability leads to great economic author`s losses. In order to minimize cases of data theft, steganography requires a large number of ways to conceal the fact of the information transfer (in contrast to cryptography, where you actually encrypted the message itself). Steganography is changing the image in a way that only the sender and the intended recipient is able to detect the message sent through it. It is invisible, and thus the detection is not easy. It is a better way of sending secret messages than encoded messages or cryptography as it does not attract attention to itself. Among the already proposed, existing steganography methods, such as: Digital prints (DP), steganography watermark (SW), hidden data (HD), in this work, attention is paid to watermarks (SW). SW implies the presence of the same labels for each container copy. In particular, the SW can be used to confirm the copyright. For example, when you recording video, you can intersperse information about recording time, in each frame, or the camcorder model, or name of your camcorder or the information about operator. If the footage gets into the hands of a rival company, you can try to use the watermark to confirm authorship of the record. If the key is kept secretly by the owner of the camera, then you can use the SW as a confirmation the authenticity of the photo and / or video images. Digital watermarks are used to protect the copyright or proprietary rights to the digital images, digitized photographs or other artwork. The main requirements that apply to this integrated data, are reliability and resistance to distortion. In modern systems, the formation of the digital watermark embedding the principle of label being a narrowband signal over a wide frequency range of the image to be marked. Digital watermarks have a small amount, however, subject to the above requirements for their integration using more sophisticated methods than to embed a message or header. This report is examined the possibility of using methods of steganography, which is based on the use of watermarks to protect and hide information to protect copyright.

Keywords: steganography, cryptography, watermarks, copyrights.

Introduction

Steganography - a method of transmitting or storing information in view of the secrecy the fact of transfer itself. Unlike cryptography, where the enemy can accurately determine whether the transmitted message is encrypted text, steganographic techniques allow embedding secret messages in innocuous message so that it was impossible to suspect the existence of the embedded secret message. Steganography takes its place in security: it does not replace, but rather complements cryptography. Hiding messages by steganography techniques greatly reduces the probability of detection of the fact of transmission of messages. And if message also encrypted, it would have another layer of protection. When combined, steganography and cryptography can provide two levels of security. Computer programs exist which encrypt a message using cryptography, and hide the encryption within an image using steganography. As a rule, a message will appear as something else, such as an image, an article, a shopping list, or a letter Sudoku. [1, 3].

Steganography usually used in conjunction with cryptography techniques, thereby completing it. The advantage of steganography over “clear” cryptography is that messages do not attract attention. Messages which encryption fact is not hidden, is suspicious and may be themselves incriminating in countries where prohibited cryptography [6].

1. Steganographic method`s overview

Currently, due to the rapid development of computer technology and new information channels, new steganographic methods appear, which are based on characteristics of information in computer files. Digital steganography is the most interesting, in terms of information security, it`s a most promising direction of steganography.

Let`s look closer than. The main provisions of steganography are:

- methods of concealment must ensure the authenticity and integrity of the file;
- it is assumed that cryptographer is fully aware of the possible methods of steganography;
- security methods based on the preservation of steganography transformation of the basic properties of open file transfer, when incorporated in it a secret message and some unknown to enemy information – some sort of key. Even if the fact of concealment message has become known to the enemy, the extraction of the secret message is a complex computational task [2].

Steganographic system or stegosystem - a set of tools and techniques that are used to form a secret channel of information transfer.

Stegosystem generalized model shown in Fig. 1.

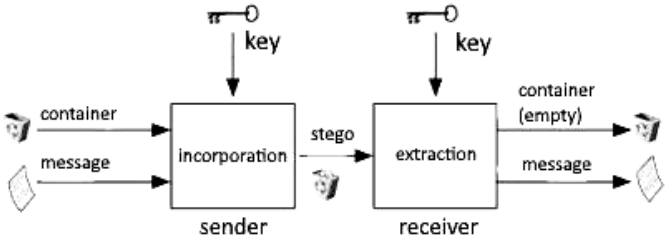


Fig. 1. Stegosystem model

Any information can be used as a data: text, message, image, and so on. In the general case, it is advisable to use the word "message" as the message can be either text or image, and, for example, audio data.

Next to describe hidden information, we'll use the term “message” [2].

There are many algorithms to embed hidden information. All of them can be divided into several subgroups:

- working with the digital signal itself. For example, LSB method;
- “soldering” of hidden information. In this case, there is an imposing concealed of image (sound, sometimes text) over the original. Often used for embedding digital watermarks (DW);
- using the features of the file formats. This includes recording information in metadata or in various other non-reserved fields file.

By way of embedding information stegoalgorithm`s can be divided into linear (additive), and other non-linear. Algorithms of additive introduction of information are concluded in a linear modification of the original image, and its extraction is carried out in the decoder correlation methods. Below is a brief list of stegoalgorithm:

LSB-method (Least Significant Bit) — the essence of this method is to replace the least significant bits in the container (image, audio or video) to the beats of hide messages. The difference between the empty and filled containers should not be perceptible to the human organs of perception.

Echo-methods used in digital audio steganography with irregular intervals and inter-echo sequence to encode values. In imposing a number of restrictions enforced stealth condition for the human perception.

Phase coding — it is also used in digital audio steganography. There is a replacement of the original audio element on the relative phase, which is the secret message.

Method of embedding messages is that a special random sequence is integrated into the container, and then, using a matched filter, the sequence is detected. This method allows to build a large number of messages in a container, and they will not interfere with each other, provided orthogonal sequences used.

Also became popular methods when hidden information transmitted via computer networks using the features of the data transmission protocol. These techniques are called "network steganography." Typical methods of network steganography include changing the properties of one of the network protocols. Furthermore, the relationship can be used between two or more different protocols with a view to better conceal the secret message transmission. Network steganography covers a wide range of techniques, including:

WLAN - Steganography is based on methods that are used to transmit steganogram in wireless networks (Wireless Local Area Networks). A practical example of WLAN steganography - hiccups System (Hidden Communication System for Corrupted Networks).

LACK - steganography - hiding messages during calls using IP-telephony. For example: the use of packages that are delayed or deliberately damaged and ignored by the receiver (this method is referred to as LACK - Lost Audio Packets Steganography) or concealment of information in the header fields that are not used [3, 4].

2. The use of digital watermarking

Hiding information in the media space is usually produced using steganography algorithms. There are several problems, solutions for that use such algorithms, for example:

- ensuring the confidentiality of correspondence (postal privacy);
- communication remote subscribers exchanging digital data arrays;
- communication remote users in an open network structures;
- achieving stealth stored large amounts of information.

One of the most effective methods of protecting multimedia information is embedding the protected object with invisible labels - digital watermark (DW). The name of this method has the known method of protection of securities including money from forgery.

The most important use of a digital watermark found in the copy protection system that seek to prevent or kept from unauthorized copying of digital data. Steganography uses DW when parties exchange secret messages are embedded into a digital signal. It used as tool of protection the documents with a photo - passports, driving licenses, credit cards with photos. Comments to the digital photos with descriptive information - another example of invisible DW. Although some formats of digital data can also carry the additional information, called metadata, DW characterized in that the information is "sewn up" directly in the signal. Multimedia objects in this case will constitute the containers (carriers) of the data. The main advantage is that there is a conditional relationship between the event of substitution of object identification and the presence of the security element - the hidden watermark [7].

Unlike conventional DW watermark can be not only visible, but (usually) invisible. Invisible DW analyzes special decoder, which brings about the correctness of their decision. Stegosystem DW, in particular, should have the task of protection of copyright and property rights for the e-mails with different active intruder attempts distortion or erase the authentication information embedded in them. Formally speaking, the DW system must provide authentication of senders of electronic messages.

Such a problem can be assigned to cryptographic system of electronic digital signature (EDS) data, but unlike stegosystems DW known system electronic signature does not provide protection of authorship is not only digital, but also analog alarms in an environment where the active violator distorts protected message and authentication information.

Other security requirements for stegosystem designed to hide the fact that the transmission of confidential communications from passive offender. It also has its own characteristics to ensure imitoprotection

stegosystems to be put into a hidden channel of transmission of false information [8]. Life cycle of DW can be described like that, on fig. 2:

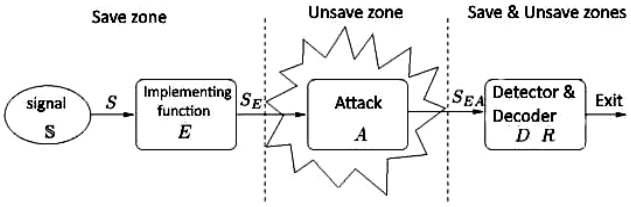


Fig. 2. Stegosystem life cicle

First, in a signal source **S** in a trusted environment embedded watermarks by using the tool **E**. The result is a signal . The next stage - the spread of through a network or any other means. While distributing the signal system can be attacked. In the resulting signal watermarks can potentially be eliminated or changed. The next step is the detection function ***D***. ***D*** tries to detect the watermark ***w***, and pull out of the function ***R*** signal embedded message. This process has the potential to make the attacker. For steganographic systems adopted to determine non-detectability - the probability of missing (ie the lack of detection stegosystem when it was presented for the analysis), and the probability of false detection (when stegosystem falsely detected when its actual absence) [6].

Practical ways stegosystems resistance evaluation based on their resistance to the detection means developed to date steganalysis algorithms.

They are all built on the fact that all the algorithms embedded somehow contribute to distortion relative stegograms used containers.

3. Attack's on stegosystem

By attack on stegosystem mean an attempt to detect, remove, change hidden steganographic message. Such attacks are called steganalysis by analogy with the cryptanalysis cryptography. The following types of attacks:

Subjective attack. Analyst carefully examines the image (listening to audio) in an attempt to determine the "eye", is there a hidden message in it. It is clear that such an attack may be carried out only against the totally unprotected stegosystems. Nevertheless, it is probably the most common in practice, at least at the initial stage of opening stegosystem.

The attack based of the known filled container. In this case the offender has one or more stego. In the latter case, it is assumed that embedding hidden information carried by the sender in the same manner. The analyst's task may consist in detecting the existence stegochanel (basic), as well as in the removal or determination key. Knowing the key, the offender will be able to analyze other stegomessage.

Attack based of the known embedded messages. This type of attack is more characteristic of the intellectual property protection systems, when used in a well-known company logo as a watermark. The objective of the analysis is to obtain a key. If the corresponding hidden messages filled container is unknown, the task is extremely difficult to be solved.

Attack based of the selected hidden message. In this case, the analyst is able to offer the sender to transmit their message and to analyze the resulting stego.

Adaptive attack based on the selected hidden message. This attack is a special case of the previous one. In this case, the analyst has the ability to select messages in order to impose the sender adaptively, depending on the results of previous analysis stego.

Attack based on the selected error filled container. This type of attack is more typical for DWM systems. Steganalyst has stegosystems detector in the form of a "black box" and several stegosystems. Analyzing the detected hidden messages, the intruder tries to open the key. Also steganalyst can apply three attacks, which have no analogues in cryptography.

The attack based of the known empty container. If analyst known about it, he comparing it with the expected stego he can always establish the fact of the stego-channel. Despite the triviality of this case, in many works is its information-theoretical basis. Much more interesting scenario, when the container is known approximately, with some error (as may be the case when you add to it the noise).

Attack based on the selected empty container. In this case, the analyst is able to force the sender to use it proposed container. For example, proposed container may have large homogeneous areas (monochrome image), and then it will be difficult to ensure privacy implementation.

The attack on the based on the known mathematical model of container or part thereof. In this case the attacker attempts to determine the difference between a suspicious message from known model. For example, assume that the bits within the image frame are correlated. Then the lack of such a correlation may be a signal about the existing of hidden message. Message an implementing task is not to break of container statistics. Implement and the attacker may have different patterns of signals, whereas in the information-win confrontation conceals having a better model. [3 , 6].

Conclusions

Currently, computer steganography continues to develop: formed the theoretical basis, is developing new, more persistent messaging integration methods. Among the main reasons observed a surge of interest in steganography can be identified in a number of countries adopted restrictions on the use of strong cryptography, as well as the problem of protecting copyright in artistic works in the digital global networks. For example, for graphics in terms of protection of copyright in their files fundamentally necessary to implement the automatic signing files for the publication of information about the author. It can be a text or other graphic information placed in any (eg, the bottom) of the image, clearly an association with a person by the authors copyright owner. These "tags" are an irrefutable link to the source, provides a particular image file. The introduction of the digital image watermarking, allowing to confirm and verify the developer rights to the media file, is also an effective protective measure for the enforcement of intellectual

property rights. Such tags can be variously positioned as a multimedia file and serve opposition to such unlawful acts, such as the substitution of attribution and repudiation.

REFERENCES

1. Ingemar J., Cox, Matthew L., Miller, Jeffrey A., Bloom, Jessica, Fridrich and Ton, Kalker(2008), *Digital Watermarking and Steganography*, Elsevier Inc., 502 p.
2. Konakhovych, H.F. and Puzyrenko, A.Yu (2006), *Kompyuternaya Stehanohrafyya. Teoryya y Praktyka* [Computer Steganography. Theory and Practice], MK-Press, Kyiv, 288 p., ISBN 966-8806-06-9.
3. Stehanohrafyya [Steganography], available at: https://ru.wikipedia.org/wiki/Стеганография (last accessed January 30, 2017).
4. Osnovy steganografii i tsifrovyye vodyanyye znaki [The Basics of Steganography and Digital Watermarks], available at : http://citforum.ck.ua/internet/securities/stegano.shtml (last accessed January 30, 2017).
5. Steganography and Digital Watermarking, available at : www.lia.deis.unibo.it/Courses/RetiDiCalcolatori/Progetti98/Fortini/ intro.html (last accessed January 30, 2017).
6. Sunchugashev I/ (2008) Stehanohrafyya [Steganography], Dolgoprudnyy, MIFI, available at : http://re.mipt.ru/infsec/2008/ essay/2008_Steganography_Sunchugashev.pdf (last accessed January 30, 2017).
7. Steganography And Digital Watermarking», available at : http://https://www.cs.bham.ac.uk/~mdr/teaching/modules03/security/students/SS5/Steganography.pdf (last accessed January 30, 2017).
8. Tsifrovyye vodyanyye znaki [Digital Watermarks], available at: https://ru.wikipedia.org/wiki/Цифровой_водяной_знак (last accessed January 30, 2017).

Received (надійшла) 07.02.2017
Accepted for publication (прийнята до друку) 16.05.2017

Розробка методів цифрової стеганографії для захисту авторських прав, на основі водяних знаків

В.В. Олещенко, В.Я. Пєвнєв

Все більшого значення в нашому швидко змінюваному світі набуває захист інформації. Особливо гостро стоїть питання захисту авторського права, який на тлі збільшення кількості створюваного контенту, став справжньою проблемою. Несанкціоноване використання чужої інтелектуальної власності призводить до великих економічних втрат автора. Для того що б мінімізувати випадки крадіжки даних, стеганографія передбачає наявність великої кількості способів приховування самого факту передачі даних (на відміну від криптографії, де шифрується саме повідомлення). Серед уже запропонованих, існуючих способів стеганографії таких як: Цифрові відбитки (ЦО), стеганографічні водяні знаки (СВЗ), прихована передача даних (СПД), в даній роботі увага приділена водяним знакам (СВЗ). СВЗ має на увазі наявність однакових міток для кожної копії контейнера. Зокрема СВЗ можна використовувати для підтвердження авторського права. Наприклад, під час запису на відеокамеру можна в кожен кадр вкраплять інформацію про час запису, моделі відеокамери і / або імені оператора відеокамери. У разі якщо відзнятий матеріал потрапить в руки конкуруючої компанії, ви можете спробувати використовувати СВЗ для підтвердження авторства записи. Якщо ключ тримати в секреті від власника камери, то за допомогою СВЗ можна підтверджувати справжність фото та / або відео знімків. Цифрові водяні знаки використовуються для захисту авторських або майнових прав на цифрові зображення, фотографії або інші оцифровані твори мистецтва. Основними вимогами, які пред'являються до таких вбудованим даними, є надійність і стійкість до спотворень. Цифрові водяні знаки мають невеликий обсяг, проте, з урахуванням зазначених вище вимог, для їх вбудовування використовуються більш складні методи, ніж для вбудовування просто повідомлень або заголовків. У цій доповіді розглянута можливість застосування методів стеганографії, заснованих на використанні водяних знаків, для захисту і приховування інформації, для захисту авторського права.

Ключові слова: стеганографія, криптографія, водяні знаки, авторські права.

Разработка методов цифровой стеганографии для защиты авторских прав, на основе водяных знаков

В.В. Олещенко, В.Я. Певнев

Все большее значение в нашем быстро изменяющемся мире приобретает защита информации. Особенно остро стоит вопрос защиты авторского права, который на фоне увеличения количества создаваемого контента, стал настоящей проблемой. Несанкционированное использование чужой интеллектуальной собственности приводит к большим экономическим потерям автора. Для того что бы минимизировать случаи воровства данных, стеганография предполагает наличие большого количества способов сокрытия самого факта передачи данных (в отличии от криптографии, где шифруется само сообщение). Среди уже предложенных, существующих способов стеганографии таких как: Цифровые отпечатки (ЦО), стеганографические водяные знаки (СВЗ), скрытая передача данных (СПД), в данной работе внимание уделено водяным знакам (СВЗ). СВЗ подразумевает наличие одинаковых меток для каждой копии контейнера. В частности СВЗ можно использовать для подтверждения авторского права. Например, при записи на видеокамеру можно в каждый кадр вкраплять информацию о времени записи, модели видеокамеры и/или имени оператора видеокамеры. В случае если отснятый материал попадет в руки конкурирующей компании, вы можете попытаться использовать СВЗ для подтверждения авторства записи. Если ключ держать в секрете от владельца камеры, то с помощью СВЗ можно подтверждать подлинность фото и/или видео снимков. Цифровые водяные знаки используются для защиты авторских или имущественных прав на цифровые изображения, фотографии или другие оцифрованные произведения искусства. Основными требованиями, которые предъявляются к таким встроенным данным, являются надежность и устойчивость к искажениям. Цифровые водяные знаки имеют небольшой объем, однако, с учетом указанных выше требований, для их встраивания используются более сложные методы, чем для встраивания просто сообщений или заголовков. В данном докладе рассмотрена возможность применения методов стеганографии, основанных на использовании водяных знаков, для защиты и скрытия информации, для защиты авторского права.

Ключевые слова: стеганография, криптография, водяные знаки, авторские права.

UDC 004.94 **doi: 10.20998/2522-9052.2017.1.11**

A. Semenova[1], M. Dubrovskyi[2], V. Savitskyi[2]

[1] National Technical University "Kharkiv Polytechnic Institute", Kharkiv, Ukraine
[2] Ivan Kozhedub Kharkiv National Air Force University, Kharkiv, Ukraine

A GERT MODEL OF AN ALGORITHM FOR ANALYZING SECURITY OF A WEB APPLICATION

The **subject** of the study in the article is the mathematical network GERT model algorithm for analyzing the security of web applications, which allows you to find an arbitrary distribution function and the probability density function for the execution time of security of a Web application analysis algorithm. **Objectives:** The analysis of the problem and formulation of the task, task solution, flow chart of security of a Web application analysis, GERT model of security of a Web application analysis algorithm, probability density function for the execution time of security of a Web application analysis algorithm. The **methods** that are used: Methods of graph theory, security testing algorithms, methods of probability theory and mathematical statistics. The following **results** are obtained. An algorithm for testing the security of web applications is developed. A mathematical model of the algorithm for testing Web application security was developed, the model allowed to find an arbitrary distribution function of the statistical value of the vulnerability testing time. The probability distribution function for testing the security of web applications is found. This will make calculations and identify the most likely case of the law of distribution of the random value of the time of testing Web application security. **Conclusion.** A mathematical model of the algorithm security of a Web application analysis has been developed based on an exponential GERT network that is different from known models through taking into account DOM structure execution or analysis. The model can be used to study processes in automated systems as well as to develop new data security tools and protocols. Using exponential stochastic GERT models makes it possible to employ results obtained in an analytical form (functions, distribution densities) for comparative analysis and studies of more complex computer systems using mathematical methods.

Keywords: security of a Web application, a mathematical model, GERT model.

Introduction

Since the demand for web applications as well as web services is high, criminals have developed a keen interest in their potential vulnerabilities. Being originally targeted against server-side components, the key threats eventually turn into attacks on common users.

An analysis of Open Web Application Security Project (OWASP TOP-10) [1, 6] data has shown cross site scripting (hereinafter referred to as XSS) to be one of the most dangerous attack types (vulnerabilities).

An analysis of related literature has demonstrated that XSS is a user data validation error enabling a JavaScript code to be transmitted to the user's browser for execution. Such attacks are also commonly known as HTML injections as they are essentially similar to SQL injections, though the injected code is executed in the user's browser unlike in SQL injections.

The analysis of the problem and formulation of the task

According to [1-3, 6-8, 13], the term XSS generally refers to immediate [1] and deferred [6] cross site scripting. In immediate XSS, the attacked server returns the malicious code (JavaScript) immediately as a response to an HTTP request. Deferred XSS means that the malicious code is stored in the attacked system and can later be injected to an HTML page of the vulnerable system. It follows from this classification that XSS fundamentally consists in the browser sending the malicious code to the server, after which it is returned either to the browser (immediate XSS) or to any other browser (deferred XSS).

A number of articles on the Internet provide a detailed description of the basic mechanisms of such threats as well as potential ways of quenching them. However, to identify the threats and the possible consequences of their spreading within secure IT project management as well as to develop optimal solutions to the problem requires the process of their initialization and spreading to be formalized mathematically.

Simulation of security of a Web application appears to be of special importance in this respect since DOM XSS is an XSS type where the result of the attack is stored not in the server response and thus not in the HTML code but in the DOM structure of the HTML page. The results of attacks made through such vulnerabilities can only be detected when executed or by a DOM structure analysis. The attack mechanism here is still a JavaScript code injection to the vulnerable segment.

Task solution

In order to mathematically formalize the algorithm of security of a Web application analysis, we will refer to the fundamentals of GERT network modeling as described by [9-12].

Fig. 1 presents a flowchart for security of a Web application analysis.

The key stages according to the algorithm are as follows:

1. All <script> tags are retrieved from the code of the page analyzed and a list of tags to be analyzed is made.

2. A tag content analysis performed. In case the tags contain no code and only contain reference to a remote file, the file is accessed and the code is retrieved from it. The file contents is then analyzed for presence

of potentially dangerous sections of code (sinks) that use client input (source).

The following can serve as source examples:

document.URL;
document.documentURI;
location.href;
location.search;
location;
window.name;
document.referrer;
Sink examples;
document.write;
(element).innerHTML;
eval;
setTimout / setInterval;
execScript.

3. If the code uses the source, an attack is executed with a specific marker that can be traced in the page DOM structure after the code has been executed (e.g. an injection of a text content to the DOM).

4. The DOM content is checked for presence of the marker. If the marker is in the DOM following the attack, it indicates a DOM vulnerability.

5. Steps 2–4 are executed for each script tag on the page.

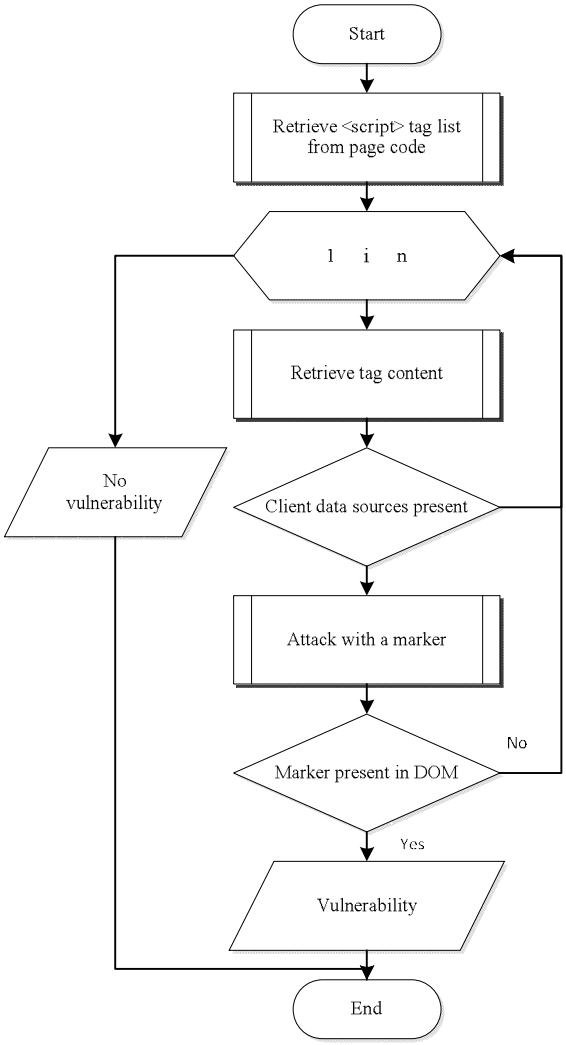


Fig. 1. Flow chart of security of a Web application analysis

Let us build a GERT network model of security of a Web application analysis algorithm according to the description. Fig. 2 provides a graphic presentation of the GERT model.

In the network presented here, graph nodes are interpreted as states of the computer system during DOM structure operation while graph edges are interpreted as probability and timing data for transitions between states. In particular, Edge (1,2) represents the time of tag content retrieval and analysis. Edge (2,3) represents timing characteristics of an attack that is executed in case of a source structure being present in the code. Edge (2,4) sets a random time of accessing the content of the remote file (sink search). Edge (4,2) represents the return to the state of executing the attack. Edge (3,5) describes the continuation of the attack, in particular checking the DOM contents. Edge (5,6) represents the time of decision on vulnerability while Edge (5,1) represents the timing of transition to the next tag.

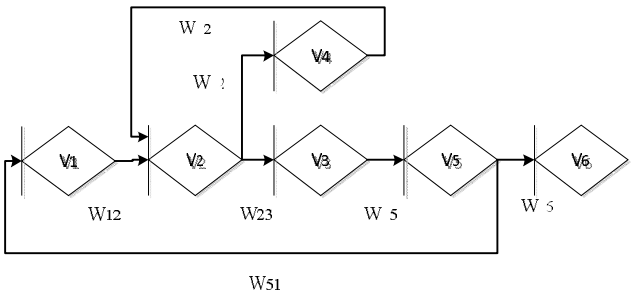


Fig. 2. GERT model of security of a Web application analysis algorithm

Look on a Table 1 for edge characteristics of the model.

The equivalent W function of execution time of security of a Web application analysis algorithm is as follows:

$$W_E(s) = \frac{W_{12}W_{23}W_{35}W_{56} + W_{12}W_{24}W_{42}W_{23}W_{35}W_{56}}{1 - W_{12}W_{23}W_{35}W_{51} - W_{12}W_{24}W_{42}W_{23}W_{35}W_{51}} =$$

$$= \frac{p_1 p_2^2 \lambda_1 \lambda_2^2 \left(p_4 \lambda_4 (\lambda_3 - s)^2 (\lambda_5 - s) + p_3^2 q_1 \lambda_3^2 \lambda_5 (\lambda_4 - s)\right)}{(\lambda_4 - s)\begin{pmatrix}(\lambda_1 - s)(\lambda_2 - s)^2(\lambda_3 - s)^2(\lambda_5 - s) - \\ - p_1 \lambda_1 p_2^2 \lambda_2^2 q_1 \lambda_5 (\lambda_3 - s)^2 - \\ - p_1 p_2^2 p_3^2 \lambda_1 \lambda_2^2 q_1 \lambda_3^2 \lambda_5\end{pmatrix}}, \quad (1)$$

where $1 - p_4 = q_1$.

The point of interest of the process is characterized by high diversity of data analyzed and processed. Feedback can be organized in various ways. Fig. 2 presents the cycles as transitions $W_{12} \to W_{24} \to W_{42}$, $W_{12} \to W_{23} \to W_{35} \to W_{51}$.

No simple methods of finding singular points of function $\Phi_E(z)$ of real variables substitution $(z = -i\varsigma)$, where ς is a real variable, apply to GERT networks with cycles. This is due to the fact that finding singular points requires solving nonlinear equations. The more complex the GERT network structure is, the more complicated is the equation. A substitution is therefore suggested for modelling.

Complex transformation $z = -s$ yields

$$\Phi(z) = \frac{uz^3 + vz^2 + bz + k}{(\lambda_4 + z)(z^6 + cz^5 + dz^4 + gz^3 + hz^2 + wz + m)}, \quad (2)$$

where $u = -p_1 p_2^2 p_4 \lambda_1 \lambda_2^2 \lambda_4$,

$v = p_1 p_2^2 p_4 \lambda_1 \lambda_2^2 \lambda_4 (\lambda_5 + 2\lambda_3)$, $c = \lambda_1 + 2\lambda_2 + 2\lambda_3 + \lambda_5$,

$b = -p_1 p_2^2 p_4 \lambda_1 \lambda_2^2 \lambda_4 \lambda_3 (2\lambda_5 - \lambda_3)$,

$k = -p_1 p_2^2 \lambda_1 \lambda_2^2 \lambda_3^2 \lambda_4 \lambda_5 (p_4 + p_3^2 q_1)$,

$d = -(2\lambda_3\lambda_5 + \lambda_1\lambda_5 + 2\lambda_2\lambda_5 + \lambda_3^2 + 2\lambda_1\lambda_3 + 4\lambda_2\lambda_3 + 2\lambda_1\lambda_2 + \lambda_2^2)$,

$g = (\lambda_3^2\lambda_5 + 4\lambda_1\lambda_2\lambda_5 + 4\lambda_2\lambda_3\lambda_5 + \lambda_2^2 + \lambda_3^2\lambda_1 + 2\lambda_3^2\lambda_2 + 4\lambda_1\lambda_2\lambda_3 + 2\lambda_2^2\lambda_3 + \lambda_2^2\lambda_1)$,

$h = -(\lambda_1\lambda_3^2\lambda_5 + 2\lambda_2\lambda_3^2\lambda_5 + 4\lambda_1\lambda_2\lambda_3\lambda_5 + 2\lambda_2^2\lambda_3\lambda_5 + \lambda_2^2\lambda_3^2 + 2\lambda_1\lambda_2^2\lambda_3 - p_1 p_2^2 q_1 \lambda_1 \lambda_2 \lambda_5)$,

$w = (\lambda_1\lambda_2\lambda_3^2\lambda_5 + \lambda_2^2\lambda_3^2\lambda_5 + 2\lambda_1\lambda_2^2\lambda_3\lambda_5 + \lambda_1\lambda_2^2\lambda_3 - 2p_1p_2^2q_1\lambda_1\lambda_2\lambda_3\lambda_5)$,

$m = (p_1 p_2^2 q_1 \lambda_1 \lambda_2 \lambda_3^2 \lambda_5 + p_1 p_2^2 p_3 q_1 \lambda_1 \lambda_2^2 \lambda_3^2 \lambda_5 - \lambda_1 \lambda_2^2 \lambda_3 \lambda_5)$.

Table 1. **Model Edge Characteristics**

No.	Edge	W function	Probability	Moment generating function
1	(1,2)	W_{12}	p_1	$\lambda_1 / (\lambda_1 - s)$
2	(2,3)	W_{23}	p_2	$\lambda_2 / (\lambda_2 - s)$
3	(2,4)	W_{24}	p_3	$\lambda_3 / (\lambda_3 - s)$
4	(3,5)	W_{35}	p_2	$\lambda_2 / (\lambda_2 - s)$
5	(5,6)	W_{56}	p_4	$\lambda_4 / (\lambda_4 - s)$
6	(5,1)	W_{51}	$1 - p_4$	$\lambda_5 / (\lambda_5 - s)$
7	(4,2)	W_{42}	p_3	$\lambda_3 / (\lambda_3 - s)$

Probability density function for the execution time of security of a Web application analysis algorithm is as follows:

$$\varphi(x) = \frac{1}{2\pi i} \int_{-i\infty}^{i\infty} e^{zx} \frac{uz^3 + vz^2 + bz + k}{(\lambda_4 + z)(z^6 + cz^5 + dz^4 + gz^3 + hz^2 + wz + m)} dz, \quad (3)$$

where integration is carried out with the Bromwich-Wagner integral [4]

The method of integration depends of whether the function $\Phi(z)$ has simple poles only or poles of some order. Where the function $\Phi(z)$ has simple poles only, the expression $e^{zx}\Phi(z)$ can be presented as follows:

$$e^{zx}\Phi(z) = \frac{e^{zx}(uz^3 + vz^2 + bz + k)}{(z^7 + a_6 z^6 + a_5 z^5 + a_4 z^4 + a_3 z^3 + a_2 z^2 + a_1 z + a_0)} = \frac{\mu(z)}{\psi(z)}, \quad (4)$$

where $a_6 = \lambda_4 + c$, $a_5 = c\lambda_4 + d$, $a_4 = d\lambda_4 + g$, $a_3 = g\lambda_4 + h$, $a_2 = h\lambda_4 + w$, $a_1 = w\lambda_4 + m$, $a_0 = m\lambda_4$.

In this case, probability density function for the execution time of security of a Web application analysis algorithm is as follows:

$$\phi(x) = \sum_{k=1}^{6} \mathrm{Res}\left[e^{zx}\Phi(z)\right] = \sum_{k=1}^{7} \frac{\mu(z_k)}{\psi(z_k)} = \sum_{k=1}^{7} \frac{e^{zx}(uz^3 + vz^2 + bz + k)}{(7z_k^6 + 6a_6 z_k^5 + 5a_5 z_k^4 + 4a_4 z_k^3 + 3a_3 z_k^2 + 2a_2 z_k + a_1)}. \quad (5)$$

Apart from the solutions determined by the roots of the equation $z^6 + cz^5 + dz^4 + gz^3 + hz^2 + wz + m = 0$, the function $\Phi(z)$ can have a second or third order pole where the value of λ_4 equals that of the roots z_2, z_3, z_4, z_5, z_6, z_7. In these cases distribution density for message transmission time $\varphi(x)$ can be calculated by the formula for finding the residues r_{-1} of the poles z_k of the order n:

$$r_{-1} = \frac{1}{(n-1)!} \lim_{z \to z_k} \frac{d^{n-1}\left((z - z_k)^n e^{zx}\Phi(z)\right)}{dz^{n-1}}. \quad (6)$$

Expression (5) is a fractional rational function of z with a denominator degree higher than the numerator degree. It therefore meets the conditions of Jordan's lemma [4, 5]. The function $\Phi(z)$ has poles in points $z_1 = -\lambda_4$. The polynomial

$$z^6 + cz^5 + dz^4 + gz^3 + hz^2 + wz + m$$

brings about seven more poles. The equation

$$z^6 + cz^5 + dz^4 + gz^3 + hz^2 + wz + m = 0 \quad (7)$$

can be solved by any method, e.g. Viet's formulas [3, 4]. As the result, singular points z_2, z_3, z_4, z_5, z_6, z_7 are found.

Conclusions

Therefore, a mathematical model of the algorithm security of a Web application analysis has been developed based on an exponential GERT network that is different from known models through taking into account DOM structure execution or analysis.

The model can be used to study processes in automated systems as well as to develop new data security tools and protocols.

Using exponential stochastic GERT models makes it possible to employ results obtained in an analytical form (functions, distribution densities) for comparative analysis and studies of more complex computer systems using mathematical methods.

REFERENCES

1. About The Open Web Application Security Project – OWASP, available at : https://www.owasp.org/index.php/About_The_Open_Web_Application_Security_Project (last accessed December 26, 2016).

2. Babincev, I. and Vuletic, D. (2016), “Web application security analysis using the kali Linux operating system”, *Vojnotehnicki glasnik. Military Technical Courier*, Vol. 64 № 2 available at : https://cyberleninka.ru/article/v/web-application-security-analysis-using-the-kali-linux-operating-system (last accessed December 26, 2016).
3. Baranov, P. and Beybutov E. (2015) “Securing information resources using Web application firewalls”, *Business Informatics*, No. 4 (34). pp. 71-78.
4. Edvards, G. (1980), Poslednyaya teorema Ferma. Geneticheskoye vvedeniye v algebraicheskuyu teoriyu chisel, Moskva : Mir, 486 p.
5. Gmurman, V.Ye. (2003), *Teoriya veroyatnostey i matematicheskaya statistika*, Moskva : Vysshaya shkola, 479 p.
6. Il'yenko, F.V. and Prikhod'ko, T.A. (2013), “Problemy uyazvimosti Web i sredstva dlya analiza bezopasnosti Web-prilozheniy”, *Ínformatsíyní upravlyayuchí sistemi ta komp’yuterniy monítoring*. Materiali III mizhnarodnoí naukovo-tekhnichnoí konferentsií studentiv, aspirantiv ta molodikh vchenikh, Donets'k, DonNTU, available at : http://masters.donntu.org/2013/fknt/ilyenko/library/sredstva_analiza_bezopasnosti_web_ilyenko_prixodko.pdf (last accessed December 26, 2016).
7. Category: OWASP Top Ten Project – OWASP, available at : https://www.owasp.org/index.php/Category:OWASP_Top_Ten_Project. (last accessed December 26, 2016).
8. Cohen, W., Ravikumar, P. and Fienberg S. A Comparison of String Metrics for Matching Names and Records, available at : https://www.cs.cmu.edu/afs/cs/Web/People/wcohen/postscript/kdd-2003-match-ws.pdf (last accessed December 26, 2016).
9. Pritsker, A.A.B. and Happ, W.W. {1966), GERT : “Part I. Fundamentals”, *The Journal of Industrial Engineering*.
10. Pritsker, A.A.B.(1979), *Modeling and analysis using Q-GERT networks*, New York: Wiley : Distributed by Halsted Press.
11. Semenov, S.G., Bos'ko, V.V. and Berezyuk, Í.A. (2012), “Issledovaniya veroyatnostno-vremennykh kharakteristik mul'tiservisnogo kanala svyazi s ispol'zovaniyem matematicheskogo apparata GERT-seti”, *Sistemi obrobki ínformatsíí*, Kharkiv : KHU PS, Vol. 1. Ic. 3 (101). – pp. 139–142.
12. Semenov, S.G. (2012), “Metodika matematicheskogo modelirovaniya zashchishchennoy ITS na osnove mnogosloynoy GERT-seti”, *Vísnik Natsíonal'nogo tekhnichnogo universitetu «KPIt»,* KH.:NTU «Kharkívs'kiy polítekhnichniy ínstitut»,. № 62 (968), pp. 173–181.
13. Sung Gyeong Bae, Hyunghun Cho, Inho Lim and Sukyoung Ryu (2014) “SAFEWAPI: Web API Misuse Detector for Web Applications”, *Proceedings of the 22Nd ACM SIGSOFT International Symposium on Foundations of Software Engineering*, pp. 507–517, available at : https://pdfs.semanticscholar.org/ (last accessed December 26, 2016).

Надійшла (received) 22.01.2017
Прийнята до друку (accepted for publication) 16.05.2017

GERT-модель алгоритму аналізу безпеки web-додатку

А. С. Семенова, М. С. Дубровський, В. В. Савицький

Предметом дослідження в статті є математичний мережевий алгоритм GERT для аналізу безпеки веб-додатків, який дозволяє знайти довільну функцію розподілу і щільність ймовірностей часу виконання алгоритму аналізу безпеки веб-додатків. **Мета:** аналіз проблеми та формулювання завдання, вирішення завдання, розробка блок-схеми аналізу безпеки веб-додатків, розробка GERT моделі алгоритму аналізу безпеки веб-додатків, знаходження розподілу і щільності ймовірностей часу виконання алгоритму аналізу безпеки веб-додатків. **Використовувані методи:** методи теорії графів, алгоритми тестування безпеки, методи теорії ймовірностей і математичної статистики. **Отримані наступні результати.** На основі експоненційної GERT-мережі розроблено математичну модель алгоритму аналізу DOM XSS уразливості, яка відрізняється від відомих, урахуванням виконання або аналізу DOM структури. Модель може бути використана для дослідження процесів в комп'ютеризованих системах, при розробці нових засобів і протоколів захисту даних. Застосування експоненційних стохастичних моделей GERT дасть можливість використання результатів, отриманих в аналітичному вигляді (функції, щільності розподілу) для проведення порівняльного аналізу і досліджень, більш складних комп'ютерних систем математичними методами.

Ключові слова: безпека веб-додатку, математична модель, модель GERT.

GERT-модель алгоритма анализа безопасности web-приложения

А. С. Семенова, М. С. Дубровский, В. В. Савицкий

Предметом исследования в статье является математический сетевой алгоритм GERT для анализа безопасности веб-приложений, который позволяет найти произвольную функцию распределения и плотность вероятностей времени выполнения алгоритма анализа безопасности веб-приложений. **Цель –** анализ проблемы и формулировка задачи, решение задачи, разработка блок-схемы анализа безопасности веб-приложений, разработка GERT модели алгоритма анализа безопасности веб-приложений, нахождение распределения и плотность вероятностей времени выполнения алгоритма анализа безопасности веб-приложений**. Используемые методы:** методы теории графов, алгоритмы тестирования безопасности, методы теории вероятностей и математической статистики. **Получены следующие результаты.** На основе экспоненциальной GERT-сети разработана математическая модель алгоритма анализа DOM XSS уязвимости, которая отличается от известных, учетом выполнения или анализа DOM структуры. Модель может быть использована для исследования процессов в компьютеризированных системах, при разработке новых средств и протоколов защиты данных. Применение экспоненциальных стохастических моделей GERT даст возможность использования результатов, полученных в аналитическом виде (функции, плотности распределения) для проведения сравнительного анализа и исследований, более сложных компьютерных систем математическими методами.

Ключевые слова: безопасность веб-приложения, математическая модель, модель GERT.

Applied problems of information systems operation

UDC 355.47; 912.64 **doi: 10.20998/2522-9052.2017.1.12**

E. G. Hashimov, A. A. Bayramov

War College of Armed Forces of the Azerbaijan Republic, Baku, Azerbaijan

INVESTIGATION OF THE OBSERVATION CONDITIONS ON THE TERRAIN OF WAR OPERATION USING GIS TECHNOLOGY

The modern geoinformation systems (GIS) have been widely applied in Armed Forces for preparation and control of battle operations, for information providing of tactic activities, for improvement of topographic maps etc. In real situations during war activity the Geography information about situation on the terrain can be ofthen changed. So, in this cause the application of usual maps isn't effective. Only the modern automated control systems can provide fast changing information documenting. The observation condition is one of the terrain features for providing information about enemy troops position and facilities. This feature helps to detemine the distance of sight between any observation points, the invisibility factors of terrain. It is depended on nature of relief plant cover, human settlements and other objects, also meteorological conditions, influencing on the visibility. As result of correct organization of observation, the obtained data help commander to estimate completely the military operation area and adopt a reasonable decision. In paper the observation conditions between two points of mountain terrain during battle operation have been investigated using GIS technology. The experiments for estimation of observation situation in mountain terrain has been carried out for one of the chosen region of the Caucasus. The visible and invisible areas have been revealed on the line of sight between two selected oversight points. The invisibility factors have been calculated and studied in depended on camera platform height. The visible and invisivle areas are determined under 0-180° angle in range 17941.16 m. The height profile between observations points and the digital heights model of investigated terrain have been constructed and analysed. At the various heights of camera observation platform the 3D heights models of the visible and invisivle areas have been constructed The invisibility factors between two delected viewpoints have been calculated. It is determined that if the heght of camera platform is increased above-ground level then the invisible area is decreased. ArcGIS software has been used for development and calculation measured results.

Keywords: observation conditions, mountain terrain, GIS, invisibility factor, height profile, ArcGIS software

Background

The modern geoinformation systems (GIS) have been widely applied in Armed Forces for preparation and control of battle operations, for information providing of tactic activities, for improvement of topographic maps, for determination of location on the ground of the land forces etc. [1-4].

In real situations during battle operations the Geography information about situation on the terrain can be ofthen changed. So, in this cause, the application of usual maps isn't effective. Only the modern automated control system can provide fast changing an information documenting. The modern GIS electron maps, video data editing systems, the especial GIS softwear in modern computer-driven control system (Windows 8, 10, 13 etc.) have been developed [5,6]. They provide a creation of the vector, rastr and matrix maps, moreover, and give possibilities efficiently data about terrain updating.

In previously works [7-11] using GIS technology the relief digital model application and the terrain observation conditions were investigated for possibility of planning war operations.

In given paper using GIS technology for one of the chosen region of the Caucasus the observation conditions from one supervision point, the visible and invisible areas have been investigated.

The observation condition is one of the terrain features for providing information about enemy troops position and facilities. This feature helps to detemine the distance of sight between any observation points, the invisibility factors of terrain, and it is depended on nature of relief plant cover, human settlements and other objects, also meteorological conditions, influencing on the visibility. As result of correct organization of observation, the obtained data help commander to estimate completely the military operation area and adopt a reasonable decision.

If there are many ravines, valleys, hills, trees and bushes, various buildings on the terrain then the visibility conditions are such unfavourable. In mountain conditions during supervision it should be select such observation point from out of which it can be possible to see roads, precipices, paths and valleys. The observation conditions help a reconnaissance, organization of fire systems and control of military units, or make worse ones. It help to reveal surroundings terrain and targets, or make worse ones. The observation conditions are characterized by optical (radiolocating) visible distance in one of concrete sector (range) of elevations of the surroundings terrain and targets, also by the sizes of invisible areas and bounds.

As result of carried out and presented experiments, the estimation of observation situation in mountain terrain has been realized. The goal of work is to

determine of visible and invisivle areas between two oversight points. The GIS analysis has been carried out at two stages. At the first stage, the visibility analysis on the line of sight between two oversight points has been carried out, then the visible and invisivle areas under 0-180° angle in range 18000 m are determined, and the terrain profile has been constructed. At the second stage, the terrain elevation 3D model has been constructed. GIS and ArcGIS software have been used for our calculations [5].

Experimental results

Two viewpoints on the topographic map have been selected. The height of first point is 900.8 m, and the height of second point is 901.5 m. The distance between these viewpoints is 17941.16 m.The goal of this work is to study of the influence of relief, trees and bushes, human settlements, various buildings and the height of camera platform on the level of visibility.

I-st experiment. The result of analysis of the line of sight between two viewpoints is shown in fig. 1. The camera platform is located on the surface of ground (the height h = 1 m). The visible areas are marked by the geen lines, the invisible areas are marked by the red lines.

The visibility analysis of the line of sight between two viewpoints has been carried out with taken an account of Earth surface curvature.

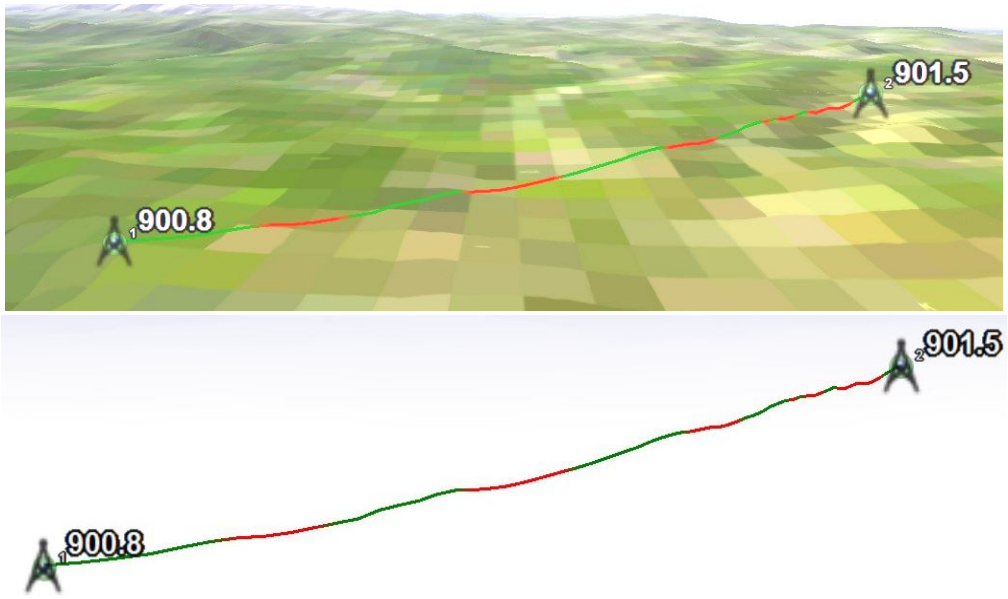


Fig. 1. The visibility analysis of the line of sight between two viewpoints

II-d experiment. The camera platform is lifted on the height h = 10 m above-ground level. Took 1-st viewpoint as basis, the visible and invisivle areas under (0 ÷ 180°) angle in range of 18000 m to direction to 2-nd viewpoint are determined by GIS analysis. The result of analysis of the line of sight between two viewpoints is shown in fig. 2.

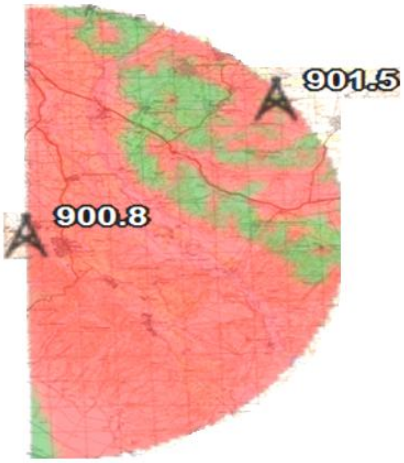


Fig. 2. The visible and invisible areas beween two viewpoints (h=10 m)

The 3D model of visible and invisible areas between two viewpoints (h = 10 m) is shown in fig. 3.

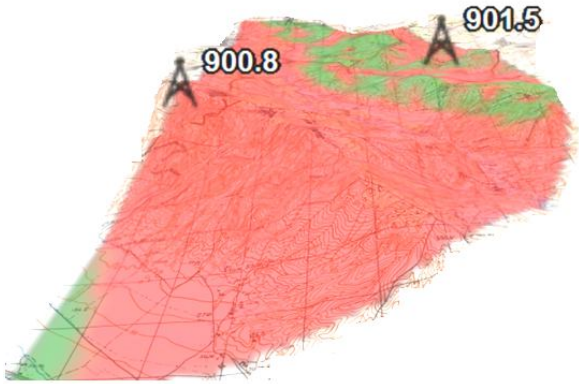


Fig. 3. The 3D model of visible and invisible areas between two viewpoints (h= 10 m

III-rd experiment. The camera platform is lifted on the height h = 20 m above-ground level. Took 1-st viewpoint as basis, the visible and invisivle areas under 0-180° angle in range ≈ 18000 m to direction to 2-nd viewpoint are determined by GIS analysis.The result of analysis of the line of sight between two viewpoints is shown in fig. 4.

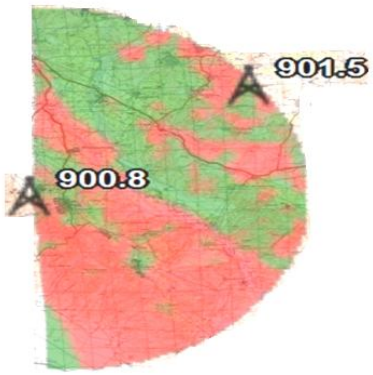


Fig. 4. The visible and invisible areas beween two viewpoints (h = 20 m

The 3D model of visible and invisible areas between two viewpoints (h = 20 m) is shown in fig. 5.

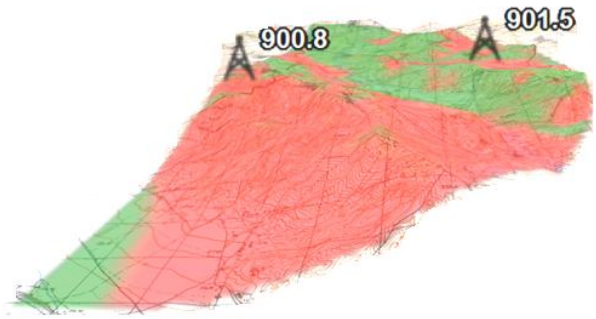


Fig. 5. The 3D model of visible and invisible areas between two viewpoints

IV-th experiment. The camera platform is lifted on the height h = 30 m above-ground level. Took 1-st viewpoint as basis, the visible and invisivle areas under (0 ÷ 180°) angle in range of ≈ 18000 m to direction to 2-nd viewpoint are determined by GIS analysis. The result of analysis of the line of sight between two viewpoints is shown in fig. 6.

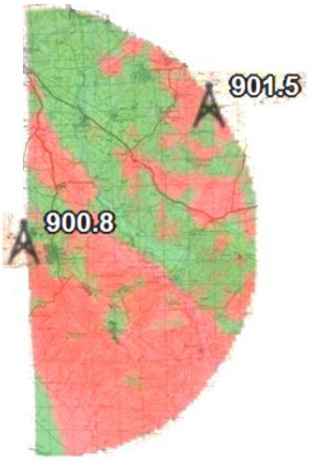


Fig. 6. The visible and invisible areas beween two viewpoints (h = 30 m)

The 3D model of visible and invisible areas between two viewpoints (h = 30 m) is shown in fig. 7.

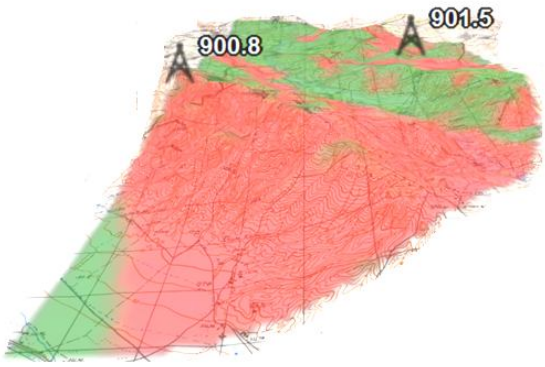


Fig. 7. The 3D model of visible and invisible areas between two viewpoints (h = 30 m)

The investigated terrain were classified on heghts and were divided on 13 zones (fig. 8).

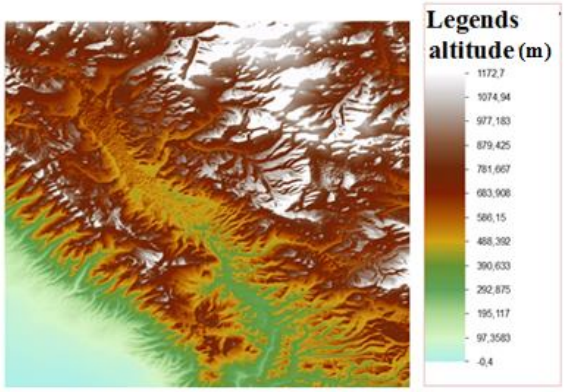


Fig. 8. The digital heights model of terrain

Using GIS softwear the profile on the line of sight between two viewpoints has been constructed (fig. 9). This profile is applicated for determination of double-sided invisible areas between selected viewpoints, for investigation more precisely of terrain profile, for study of terrain slope etc.

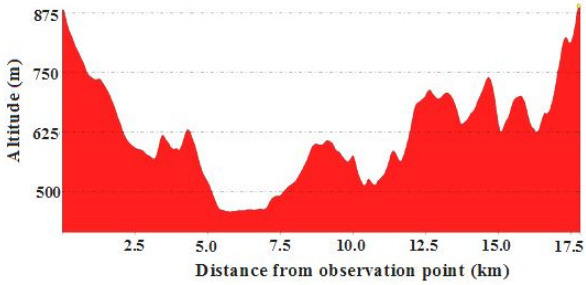


Fig. 9. Constructed profile between two viewpoints

From fig. 9 it is clearly seen, that how the terrain relief is changed step by step by distance and by heights.

Analysis and disscusion

The investigation of observation condition on the war operation region has a goal to determine of visibility and invisibility levels (factors) on the most suitable viewpoint of terrain. By construction of the heights profile of terrain, the visible and invisible areas are determined below method. Let us explaine it using fig. 10.

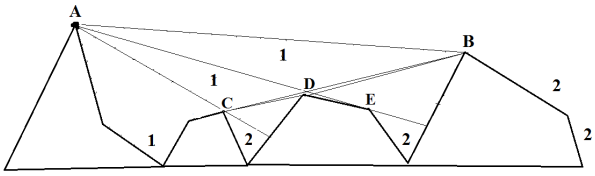


Fig.10. The profile of conditional mountain terrain

The profile of conditional mountain terrain is shown in this figure 10. The two viewpoints are selected on the high posts. Here: ***A*** is the first viewpoint selected on the top of mountain, ***B*** is the second viewpoint (enemy target) selected on the top of another mountain. Between ***A*** and ***B*** viewpoints on the line of sight the heights profile is constructed by use GIS software. As results, visible (1) and invisible (2) areas (figures 10) are determined. From analysis of obtaining information the command staff located in the *A* post make at a decision that the enemy troops and armoured machineries located in areas (2) will be unobserved. On the other hand, if enemy troops will be located in areas (1) then they will be observed from *A* viewpoint.

If *C*, or *D*, or *E* points are selected as viewpoints then, by the same rule, the invisible areas can be determine on *CD*, *DE* or *EB* lines of sight.

Such viewpoints can be selected on the various peaks of the terrain. For the right and correct decision making the commander must to choose such viewpoint that the sum of the invisible areas is minimal. For this, let us apply and use an invisibility factor *P* for various peaks:

$$p = \frac{1}{n-1} \cdot \sum_{i=1}^{n-1} \frac{1}{S_i^0} \cdot \sum_{j=1}^{n-2} S_{ij}^{in} \ . \qquad (1)$$

Here: S_{ij}^{in} is an invisible area between *i* and *j* peaks, S^o is a total area between *A* and *B* peaks; *n* is a number of peaks.

After calculation P_1, P_2,... invisibility factors for various viewpoints to the lines of sights to the enemy post *B*, the minimym of them can be determined::

$$P_{min} = \min \{P_1, P_2, ...\}.$$

So, after calculation of the minimal invisibility factor P_{min} by this method, the cammander can choose a right viewpoint. From this viewpoint (a peak) on the line of sight to ememy point *B* the invisible areas are minimal. Based on this method let us determine an invisibility factor *P* in our experiments.

I-st experiment: the camera platform is located on the ground, then from analysis of data on the fig. 1 we can calculate the invisibility factor P_1 from *A* viewpont on the line sight to *B* post:

$$P_1 \approx 0{,}55 \ \text{ or } \ P_1 \approx 55\ \%.$$

That is, 55% of total area between viewpoints *A* and *B* are invisible.

II-nd experiment: the camera platform is lifted on the height of h = 10 m above-ground level. Then from analysis of data on the figures 2 and 3 we can calculate the invisibility factor P_2 from *A* viewpont on the line sight to *B* post ((h=10 m, figures 2 and 3):

$$P_2 \approx 0{,}42 \ \text{ or } \ P_2 \approx 42\ \%.$$

That is, the camera platform is lifted on the height of h = 10 m above-ground level, then 42 % of total area between viewpoints *A* and *B* are invisible.

III-nd experiment: the camera platform is lifted on the height of h = 20 m above-ground level. Then, from analysis of data on the figures 4 and 5 we can calculate the invisibility factor P_2 from *A* viewpont on the line sight to *B* post ((h=20 m, fig. 4 and 5):

$$P_3 \approx 0{,}36 \ \text{ or } \ P_3 \approx 36\ \%.$$

That is, the camera platform is lifted on the height of h = 20 m above-ground level, then 36 % of total area between viewpoints *A* and *B* are invisible.

IV-th experiment: the camera platform is lifted on the height of h = 30 m above-ground level. Then. from analysis of data on the figures 6 and 7 we can calculate the invisibility factor P_4 from *A* viewpont on the line sight to *B* post ((h=30 m, fig. 6 and 7):

$$P_4 \approx 0{,}22 \ \text{ or } \ P_4 \approx 22\ \%.$$

That is, the camera platform is lifted on the height of h = 20 m above-ground level, then 22 % of total area between viewpoints *A* and *B* are invisible. So, we have

$$P_4 < P_3 < P_2 < P_1.$$

We can conclude that if the heght of camera platform is increased above-ground level then the invisible area is decreased.

Conclusion

The experiments for estimation of observation situation in mountain terrain has been carried out.

Using GIS technology and ArcGIS software the visibility analysis on the line of sight between two selected oversight points has been carried out. The visible and invisivle areas under 0-180° angle in range 17941.16 m are determined. The terrain profile and the digital heights model of investigated terrain have been constructed. At the various heights of camera observation the 3D heights model of the visible and invisivle areas have been constructed. The invisibility factors between two delected viewpoints have been calculated. It is determined that if the heght of camera platform is increased above-ground level then the invisible area is decreased.

REFERENCES

1. Hashimov, E.G. and Bayramov, A.A. (2017), *Application of GIS and seismic location method for detection of invisible military objects*, Monography, Military Press, Baku, 250 p.
2. Sокolov, A.V. Tixonov, M.L. (2008), “GIS military application”, *OBSERVEF*, 5, p 9.37–45.
3. Conrad, Olaf (2010), *SAGA: System for Automated Geoscientific Analyses. Concepts and Basics,* Physical Geography, University Hamburg, GEOSTAT, 33 p.
4. Paul A. Longley, Michael F. Goodchild, David J. Maguire and David W. (2005), *Rhind Geographic information systems and science,* Wiley, UK, London, 536 p.

5. ArcGIS 3D analiz (2008), eğitim dökümanı, İşlem şirketler qrubu, Ankara, 160 p.
6. Karmanov, A.G. (2012), *GIS tutorial. Sankt-Peterburg Naional Reseach Universityof Information Technologies, mechanics and optics*, Sankt-Peterburg. 116 p.
7. Hashimov, E.G., Bayramov, A.A., Nasibov, Ya.A. and Amanov, R.R. (2015), "Application digital model of relief for plannibg military operations", *Herbi Bilik*, No. 4, pp. 63–69.
8. Hashimov, E.G., Bayramov, A.A. and Khalilov, B.M. (2017), "Terrain orthophotomap making and combat control", Proceeding of Internatonal Conf. "*Modern Call of Security and Defence*". I-st vol.19-20 May 2016, War College after G. Rakovski, Sofia, pp. 68–71.
9. Bayramov, A.A., Hashimov, E.G. and Amanov R.R. (2016), "The detection of invisible objects on the terrain on the basis of GIS technology", *Geography and nature sources*, Azerbaijan Geography Society Reports, No. 1, pp. 124–126.
10. Hashimov, E.G., Bayramov, A.A. and Khalilov B.M. (2015), "Operative detection of ground enemy objects", *Herbi Bilik*, No. 1, pp. 33–47.
11. Hashimov, E.G., Bayramov, A.A. and Khalilov B.M. (2016), "Terrain orthophotomap making for detection of military objects", *Milli tehlyukesizlik and herbi elmler* (National Security and Military Sciences), vol. 2, No. 4. pp. 21–28.

Received (Надійшла) 31.03.2017
Accepted for publication (Прийнята до друку) 16.05.2017

Дослідження умов спостереження с використанням ГІС технологій на території військових дій

Е. Г. Гашимов, А. А. Байрамов

Сучасні геоінформаційні системи (ГІС) широко використовуються в Збройних Силах для підготовки і управління бойових операцій, для інформаційного забезпечення тактичних дій, для поліпшення топографічних карт. В реальній ситуації під час військових дій геоінформація про становище на місцевості може часто змінюватися. Тому, в цьому випадку застосування звичайних карт не ефективно. Тільки сучасні автоматизовані системи управління можуть забезпечити швидко мінливу інформаційну документацію. Умова спостереження є одним з властивостей місцевості, що забезпечує інформацією про позицію ворожих військ і військової техніки. Це властивість допомагає визначити відстань спостереження між точками спостереження, фактор невидимості місцевості. Це залежить від природи рельєфу рослинного покриву, поселень і інших об'єктів, а також метеорологічних умов, що впливають на видимість. Як результат правильної організації спостереження, отримані дані допомагають командиру повністю оцінити область військової операції і прийняти прийнятне рішення. У статті, використовуючи ГІС технологію, досліджені умови спостереження між двома точками гірській місцевості під час бойової операції. Експерименти по оцінці ситуації спостереження в гірській місцевості були проведені в одній з обраних регіонів Кавказу. По лінії огляду між двома обраними точками спостереження були виявлені видимі і невидимі області. Були розраховані фактори невидимості і вивчені в залежності від висоти платформи камери. Були визначені видимі і невидимі області в радіусі 17941.16 m під кутами 0-180 °. Був побудований і проаналізовано профіль висот між точками спостереження і цифрова модель висот досліджуваної території. Для різних висот розташування платформи з камерою були побудовані і досліджені 3D моделі висот для видимих і невидимих областей. Були розраховані фактори невидимості між двома обраними точками спостереження. Було встановлено, що чим вище платформа з камерою спостереження, тим менше невидима площа. Для обробки і розрахунку виміряних результатів було використано програмне забезпечення ArcGIS.

Ключові слова: умови спостереження, гірська місцевість, ГІС, фактор невидимості, профіль висот, програмне забезпечення ArcGIS.

Исследование условий наблюдения с использованием ГИС технологий на территории военных действий

Э. Г. Гашимов, А. А. Байрамов

Современные геоинформационные системы (ГИС) широко используются в Вооруженных Силах для подготовки и управления боевых операций, для информационного обеспечения тактических действий, для улучшения топографических карт. В реальной ситуации во время военных действий геоинформация о положении на местности может часто меняться. Поэтому, в этом случае применение обычных карт не эффективно. Только современные автоматизированные системы управления могут обеспечить быстро меняющуюся информационную документацию. Условие наблюдения является одним из свойств местности, обеспечивающее информацией о позиции вражеских войск и военной техники. Это свойство помогает определить расстояние наблюдения между точками наблюдения, фактор невидимости местности. Это зависит от природы рельефа растительного покрова, поселений и других объектов, а также метеорологических условий, влияющих на видимость. Как результат правильной организации наблюдения, полученные данные помогают командиру полностью оценить область военной операции и принять приемлемое решение. В статье, используя ГИС технологию, исследованы условия наблюдения между двумя точками горной местности во время боевой операции. Эксперименты по оценке ситуации наблюдения в горной местности были проведены в одной из выбранных регионов Кавказа. По линии обзора между двумя выбранными точками наблюдения были выявлены видимые и невидимые области. Были рассчитаны факторы невидимости и изучены в зависимости от высоты платформы камеры. Были определены видимые и невидимые области в радиусе 17941.16 m под углами 0-180°. Был построен и проанализирован профиль высот между точками наблюдения и цифровая модель высот исследуемой местности. Для разных высот расположения платформы с камерой были построены и исследованы 3D модели высот для видимых и невидимых областей. Были рассчитаны факторы невидимости между двумя выбранными точками наблюдения. Было установлено, что чем выше платформа с камерой наблюдения, тем меньше невидимая площадь. Для обработки и расчета измеренных результатов было использовано программное обеспечение ArcGIS.

Ключевые слова: условия наблюдения, горная местность, ГИС, фактор невидимости, профиль высот, программное обеспечения ArcGIS.

УДК 678.074.54.6 **doi: 10.20998/2522-9052.2017.1.13**

Н. М. Євдокіменко[1], Л. А. Пісоцька[2], Н. Г. Кучук[3]

[1] ДВНЗ «Український державний хіміко-технологічний університет», Дніпро, Україна
[2] ДЗ «Дніпропетровська медична академія МОЗ України», Дніпро, Україна
[3] Харківський національний університет імені В.Н. Каразіна, Харків, Україна

ПРОГНОЗУВАННЯ ВЛАСТИВОСТЕЙ ЕЛАСТОМЕРНИХ КОМПОЗИЦІЙ ЗА ПЕРКОЛЯЦІЙНИМИ МОДЕЛЯМИ

Наведено результати теоретичних та експериментальних досліджень щодо розробки методики оцінки параметрів геометричної фазової морфології еластомерних композицій, яка базується на результатах аналізу в задачах перколяції та диференційному рівнянні П.Ф. Ферхюльста. Встановлено, що імовірність геометричних фазових переходів**,** при заданому вмісті гетерофази, різко зменшується у випадку зменшення розміру часток гетерофази. За розробленою методикою проведено розрахунки параметрів геометричної фазової морфології гуми з метою оцінки впливу природи та вмісту для усіх інгредієнтів на структуру та властивості гуми. Розроблено принципи побудови оптимального складу еластомерних систем (гуми та блок-поліуретани). Встановлено, що максимальний рівень деформаційно-міцнісних властивостей реалізується у випадку утворення морфологічної будови з мінімальним розміром часток гетерофази. Оптимальною для блок-поліуретанів є морфологія, яка, з одного боку, забезпечує найбільшу імовірність збереження властивостей гетерофази жорстких блоків для забезпечення високої міцності, з іншого боку, – збереження властивостей дисперсійного середовища для забезпечення високої еластичності. Одержані результати, що базуються на аналізі в задачах перколяції добре узгоджені з відомими експериментальними даними: методом світлорозсіювання, методом оптичної та електронної мікроскопії. Запропонований підхід має практичне значення для оптимізації складу еластомерних композицій, а також, для розробки марочного асортименту блок-поліуретанів.

Ключові слова: еластомерні композиції, гума, поліуретанові блок-кополімери, фазова морфологія, перколяційна модель.

Вступ

Сьогодні немає жодної галузі промисловості, де б не застосовувалися еластомерні композити. Ступінь їх використання є важливим критерієм оцінки рівня науково-технічного прогресу в країні. Використання еластомерних композитів забезпечує можливість створення принципово нових конструкцій і різноманітних виробів, сприяє зменшенню їх маси, експлуатаційних і транспортних витрат, підвищенню якості. Характерно, що для конкретних умов експлуатації, як правило, необхідні полімерні матеріали з новим комплексом властивостей, і вирішувати дану проблему найкраще за рахунок пошуку оптимальних комбінацій традиційних полімерів [1].

Багаточисельні дослідження останніх років [2, 4, 5] показали вирішальну роль фазової морфології у забезпеченні високого рівня властивостей еластомерних композицій.

Виходячи з того, що, на відміну від інших матеріалів конструкційного призначення, розвиток технології еластомерів обумовлений не тільки підвищенням рівня міцності (традиційний підхід для всіх матеріалів конструкційного призначення), але і необхідністю збереження основної властивості еластомерів – здатності дисипувати механічну енергію.

З урахуванням принципових відмінностей фізичної природи таких властивостей як міцність і еластичність, геометричну фазову морфологію необхідно визначати як матричну структуру дисперсійне еластичне середовище в якому розповсюджена дисперсна фаза – елемент системи, що забезпечує високий рівень міжмолекулярної взаємодії.

Методика досліджень

Параметри морфологічної будови еластомерних композицій та характер структурних перетворень вивчали як геометричні фазові переходи із застосуванням метода перколяційного аналізу (рис. 1).

Для гетерогенних систем сутність перколяційного моделювання зводиться до такого. Припустимо, що об’єм тривимірного простору заданого розміру поділено на елементарні об’єми (елементи) у кількості L×L×L. Розмір частки гетерофази визначається величиною L. Заповнені квадрати модулюють властивості гетерофази, а незаповнені – властивості дисперсійного середовища.

Результати досліджень та їх обговорення

Аналіз у задачах перколяції дозволяє оцінити вплив морфологічної будови еластомерних композитів на властивості як імовірність геометричного фазового переходу, виходячи із умов зв’язаності.

Імовірність геометричних фазових переходів і термодинамічних фазових переходів якісно подібні, однак аналіз геометричних фазових переходів в порівнянні з термодинамічним, простіший – базується на деяких поняттях геометрії та теорії імовірності [3]. Встановлено, що імовірність геометричних фазових переходів P**,** при заданому вмісті гетерофази $P_{c,}$ різко зменшується у випадку зменшення розміру часток гетерофази (а):

$$P = P_c^L = P_c^{1/a}, \qquad (1)$$

де P – імовірність геометричного фазового переходу; P_c – об’ємна частка гетерофази; L – розмірність перколяційної гратки; a – розмір часток гетерофази.

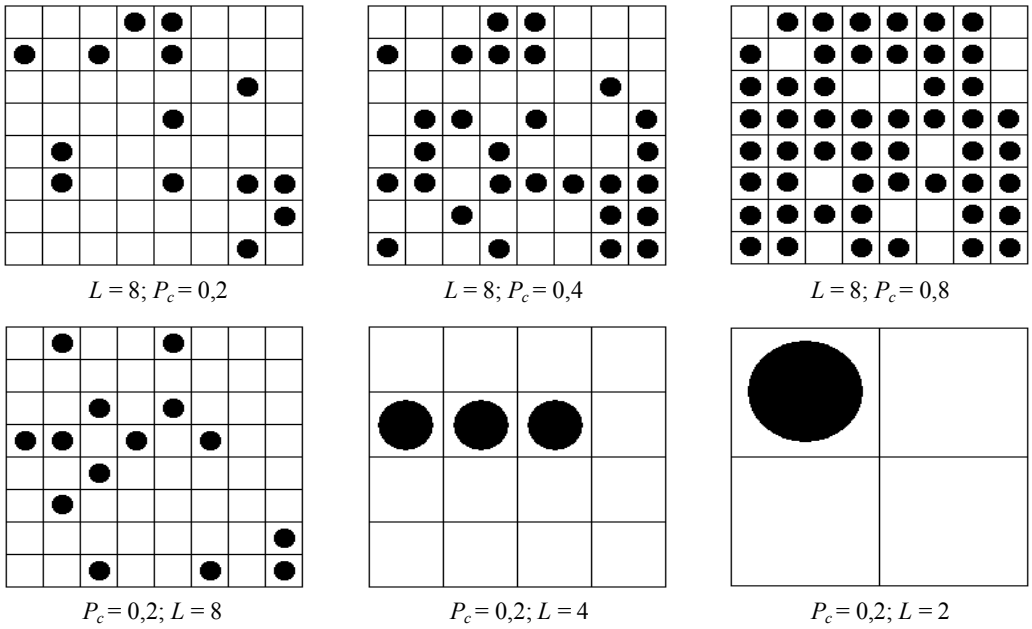
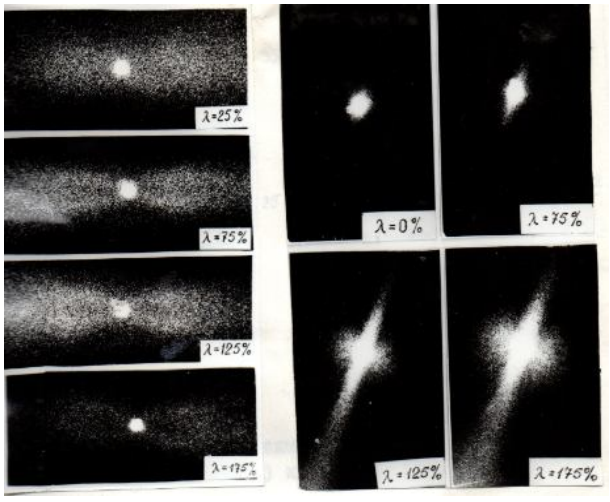


Рис. 1. Приклади перколяційних конфігурацій на квадратній решітці:
L – розмірність решітки, P_c – вміст гетерофази

Тобто, при зменшенні розміру часток гетерофази зменшується імовірність фазового геометричного переходу, отже зростає імовірність збереження властивості матриці – еластичності у випадку гуми. Одержані результати, що базуються на аналізі в задачах перкуляції добре узгоджені з відомими [5] експериментальними даними:

методом світлорозсіювання (рис. 2),

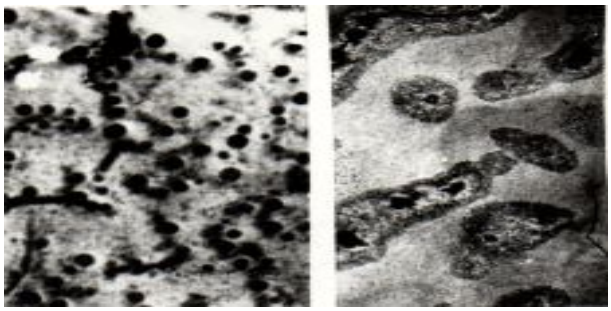
методами оптичної та електронної мікроскопії (рис. 3–5).



а б

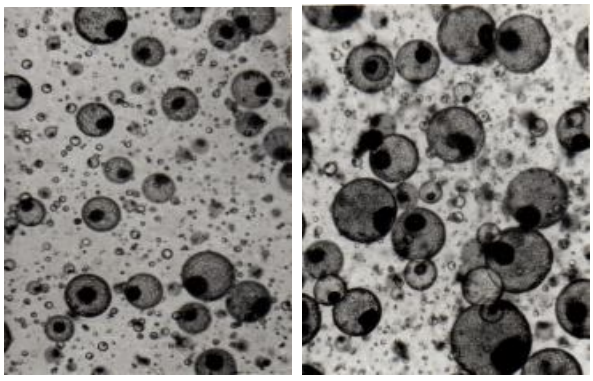
Рис. 2. Методи світлорозсіювання при різному ступеню деформування (λ) для системи:
а – при зменшенні часток гетерофази;
б – при збільшенні часток гетеро фази

Унікальність розробленої методики полягає у тому, що на відміну від усіх сучасних методів дозволяє визначити параметри морфології будь яких зразків, в той час як відомі методи придатні для вивчення прозорих зразків.

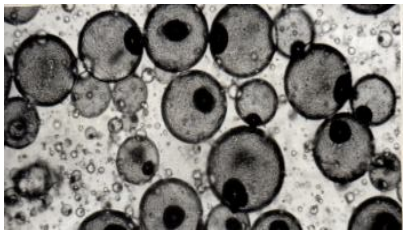


а б

Рис. 3. Електронномікроскопічні фотографії (×30000) системи з різним розміром часток

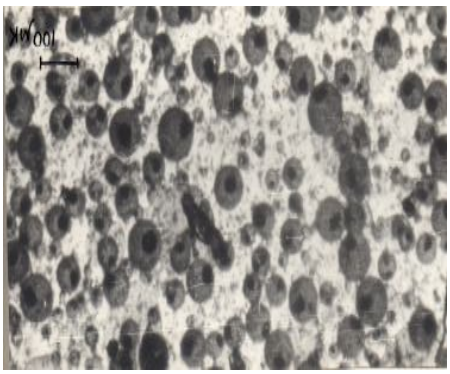


а б

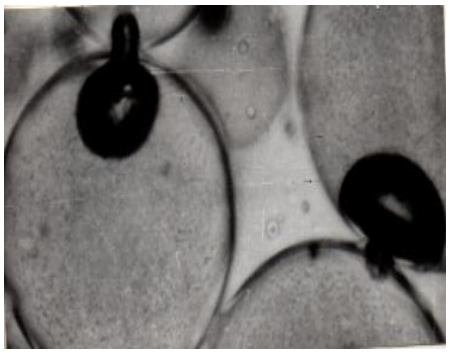


в

Рис. 4. Оптичні мікрофоторгафії (×200) при різному вмісті (P_c) часток гетерофази: а – 0,05; б – 0,2; в – 0,4



а



б

Рис. 5. Оптичні мікрофоторгафії для системи $P_c = 0{,}4$ при різному вмісті збільшенні: а – ×100; б – ×800

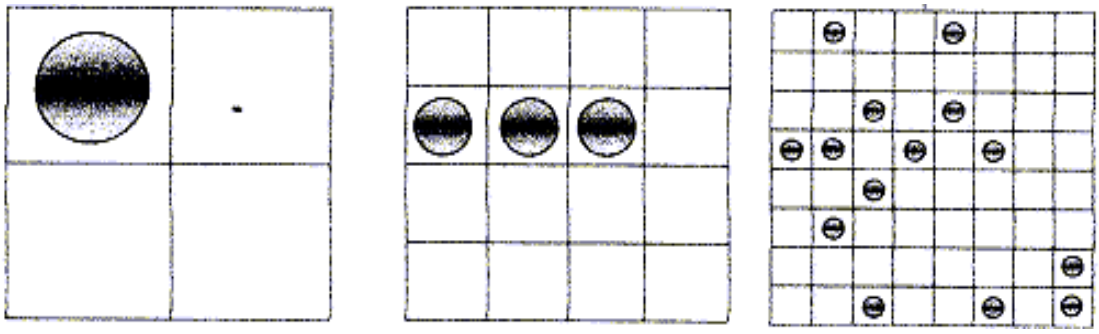
Оптимальною буде структура, при якій найбільша імовірність, з одного боку, щодо реалізації властивостей гетерофази для забезпечення високої міцності, з іншого боку, збереження еластодинамічних властивостей матриці.

На геометричному рівні імовірність збереження властивості гетерофази визначається розміром часток гетерофази (1). Однак якщо розглянути потенціальну міцність матеріалу гетерогенної структури і механізм руйнування такого матеріалу, то розмір впливає на сумарну поверхню часток гетерофази. Одже чим менші розміри часток гетерофази, тим більш зростає міцність.

Потенційну міцність матеріалу визначають за величиною міжмолекулярної взаємодії і кількістю утворених зв'язків. Кількість утворених зв'язків прямо пропорційна сумарній поверхні гетеро фази, тобто при постійному об'ємі гетерофази кількість зв'язків збільшується обернено пропорційно радіусу часток гетеро фази. Отже зменшення розміру часток дозволяє збільшити міцність і еластичність матеріалів.

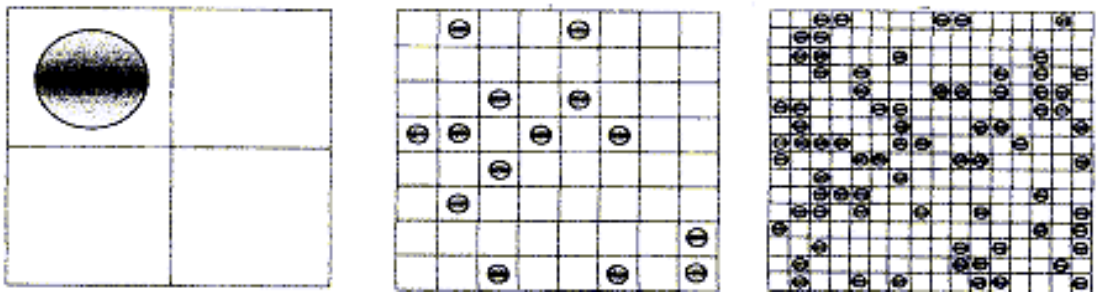
За розробленою методикою проведено розрахунки параметрів геометричної фазової морфології гуми з метою оцінки впливу природи та вмісту для усіх інгредієнтів на структуру та властивості гуми.

Приклади перколяційних моделей для гум наведено на рис. 6, 7.



$C = 0{,}0$ $C = 1{,}0$ $C = 2{,}0$

Рис. 6. Перколяційні моделі для гумових сумішей, що різняться вмістом стеаринової кислоти, мас.ч.



$C = 0{,}0$ $C = 1{,}0$ $C = 5{,}0$

Рис. 7. Перколяційні моделі для гумових сумішей, що різняться вмістом ZnO, мас.ч

Особливий комерційний інтерес мають поліуретанові блок-кополімери (БПУ), для яких, на відміну від гум, характерною є можливість змінюватися в широкому діапазоні деформаційно-міцнісні властивості (від еластомерів до жорстких пластиків).

Важливим є той факт, що використання БПУ із заданими властивостями за рахунок рециклінгу, на відміну від гум, дозволяє суттєво знизити екологічне навантаження [4].

Стосовно досліджених систем БПУ рівняння (2) приймає такий вигляд:

$$P = P_c^{M_{ог}}, \qquad (2)$$

де P – імовірність геометричного фазового переходу в досліджуваних поліуретанах;

P_c – об'ємна частка мікрофази жорстких блоків;

$M_{ог}$ – молекулярна маса олігогліколю у молекулі БПУ.

Приклади перколяційних конфігурацій на квадратній решітці для досліджених у даній роботі БПУ (рис. 8).

Оптимальною є морфологія, яка, з одного боку, забезпечує найбільшу імовірність збереження властивостей гетерофази жорстких блоків для забезпечення високої міцності, з іншого боку, збереження властивостей дисперсійного середовища для високої еластичності.

У випадку розглянутих систем, оптимальною є морфологія БПУ в межах

$$P_{c1} \div P_{c2}=25\div50\% \text{ [5]}.$$

Отримані дані свідчать, що запропонований нами підхід щодо прогнозування рівня властивостей БПУ, який базується на перколяційному аналізі й виявляє принципово важливе значення молекулярної маси олігоестеру у молекули БПУ.

Висновки

На основі проведених теоретичних і експериментальних досліджень морфологічну будову еластомерних композицій (гум та поліуретанових блок-кополімерів) визначено як геометричну фазову морфологію – у високоеластичному дисперсійному середовищі розповсюджена дисперсна фаза (області з підвищеною міжмолекулярною взаємодією).

Встановлено, що максимальний рівень деформаційно-міцнісних властивостей реалізується у випадку утворення морфологічної структури з мінімальним розміром часток гетерофази, при її максимально можливому вмістові (умови геометричних фазових переходів).

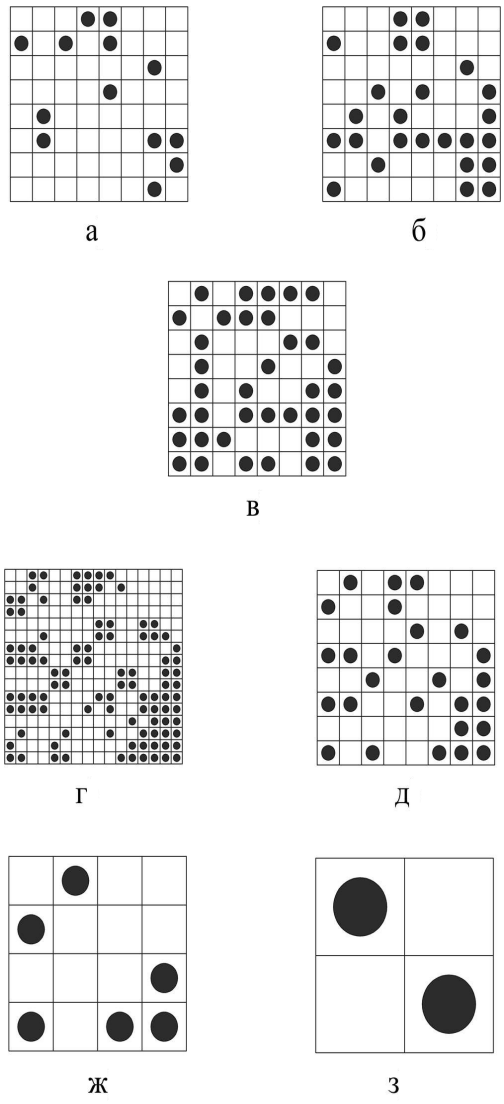


Рис. 8. Приклади перколяційних конфігурації морфології БПУ на квадратній решітці у випадку різного вмісту жорстких блоків P_c та молекулярної маси олігомерних гліколів $M_{ог.}$ (при $M_{ог}$ = 1000: а – P_c = 20%; б – P_c = 40%; в – P_c = 60%, при P_c = 40%: г – $M_{ог}$ = 500; д – $M_{ог}$ = 1000; ж – $M_{ог}$ = 1500; з – $M_{ог}$ = 2000)

СПИСОК ЛІТЕРАТУРИ

1. Пол Д. Полимерные смеси: в 2-х т. / Д. Пол, К. Бакнел; пер. с англ. под ред. В.Н. Кулезнева. – СПб. Научные основы и технологии. – 2009. – Т.1 – 618 с. Т. 2 – 606 с.

2. Кулезнев В.Н. Эластомеры и пластики (от разделения к единству) / В.Н. Кулезнев, Ю.Л. Морозов // Каучук и резина. – 2007. – № 6. – С. 29-33.

3. Гулдах Х. Компьютерное моделирование в физике. Ч. 2 / Х. Гулдах, Я. Табочкин; пер. с англ. – М.: Мир, 1990. – 400 с.

4. Yevdokimenko N.M. Regulating the Morphology and Predicting the Properties of Polyurethane Block Copolymers / N.M. Yevdokimenko, V.N. Anisimov // Polymers of special applications: Polish-Ukrainian conference, abstracts. – Ukraine-Bukovel, 2014. – P. 3.

5. Anisimov V.N. Predicting the Properties of Linear Block-Polyurethanes through Percolation Models / V.N. Anisimov // European Applied Sciences. – 2013. – Vol. 2. – № 3. – P. 4-8.

REFERENCES

1. Pol, D. and Baknel, K. (2009), Polimernyye smesi [Polymer mixtures], Nauchnyye osnovy i tekhnologi, Sankt-Peterburg, Vol. 1. 618 p., Vol. 2. 606 p.

2. Kuleznev, V.N. and Morozov, YU.L. (2007), "Elastomery i plastiki (ot razdeleniya k yedinstvu)" [Elastomers and plastics (from separation to unity)], *Kauchuk i rezina*, No. 6, pp. 29–33.

3. Guldakh, KH. and Tabochkin, YA. (1990), *Komp'yuternoye modelirovaniye v fizike* [Computer Modeling in Physics]. CH.2. Mir, Moskva, 400 p.

4. Yevdokimenko, N.M. and Anisimov, V.N. (2014), "Regulating the Morphology and Predicting the Properties of Polyurethane Block Copolymers", *Polymers of special applications*: Polish-Ukrainian conference, abstracts. Ukraine-Bukovel. – p. 3.

5. Anisimov, V.N. (2013), "Predicting the Properties of Linear Block-Polyurethanes through Percolation Models", *European Applied Sciences*, Vol. 2. No. 3, pp. 4–8.

Надійшла (received) 20.02.2017
Прийнята до друку (accepted for publication) 25.04.2017

Прогнозирование свойств эластомерных композиций по перколяционныи моделям

Н. М. Евдокименко, Л. А. Песоцкая, Н. Г. Кучук

Приведены результаты теоретических и экспериментальных исследований по разработке методики оценки параметров геометрической фазовой морфологии эластомерных композиций, которая базируется на результатах анализа в задачах перколяции и дифференциальном уравнении П.Ф. Ферхюльста. Установлено, что вероятность геометрических фазовых переходов при заданном содержании гетерофазы резко уменьшается в случае уменьшения размера частиц гетерофазы. По разработанной методике проведены расчеты параметров геометрической фазовой морфологии резины с целью оценки влияния природы и содержания для всех ингредиентов на структуру и свойства резины. Разработаны принципы построения оптимального состава эластомерных систем (резины и блок-полиуретаны). Установлено, что максимальный уровень деформационно-прочностных свойств реализуется в случае образования морфологического строения с минимальным размером частиц гетерофазы. Оптимальной для блок-полиуретанов является морфология, которая, с одной стороны, обеспечивает наибольшую вероятность сохранения свойств гетерофазы жестких блоков для обеспечения высокой прочности, с другой – сохранение свойств дисперсионной среды для обеспечения высокой эластичности. Полученные результаты, основанные на анализе в задачах перколяции, хорошо согласованы с известными экспериментальными данными: методом светорассеяния, методом оптической и электронной микроскопии. Предложенный подход имеет практическое значение для оптимизации состава эластомерных композиций, а также для разработки марочного ассортимента блок-полиуретанов.

Ключевые слова: эластомерные композиции, резина, полиуретановые блок-сополимеры, фазовая морфология, перколяционная модель.

Elastomer composition properties forecast using percolation model

N. Yevdokimenko, L. Pesotskaya, N. Kuchuk

The results of theoretical and experimental studies on development of methodology for assessing geometric parameters elastomeric phase morphology compositions based on an analysis of the problems in percolation and Ferhyulsta differential equation. Established that the geometric probability phase transitions, a given content heterophase sharply reduced in case heterophase particle size reduction. With the developed technique Calculations geometric parameters of the rubber phase morphology to assess the impact of the nature and content all ingredients on the structure and properties of rubber. The principles of construction the optimal composition of elastomer (rubber and polyurethane block). Established that maximum deformation-strength properties sold in case formation of morphological structure with a minimum particle size heterophase. The optimal block for polyurethanes morphology is that, on the one hand, provides the highest probability of preservation of properties for heterophase rigid blocks providing high strength, on the other hand - saving properties of variance environment for high elasticity. The results, based on analysis in problems of percolation well aligned with known experimental data, by light scattering, by optical and electron microscopy. The approach has practical value for optimization of elastomeric compositions, as well as to developing brand range block polyurethanes.

Keywords: elastomeric compositions, rubber, polyurethane block copolymers, phase morphology, percolation model.

UDC 004.94 **doi: 10.20998/2522-9052.2017.1.14**

P. Cala, P. Bienkowski

Wroclaw University Of Technology, Wroclaw, Poland

EXPOSURE SYSTEMS USED IN THE ASSESSMENT OF EMF IMPACT ON LIVING ORGANISMS

The **subject** of the study in the article is the processes of analysis and exposure assessment of electromagnetic field on humans. The main goal is to optimize size of the exposure antenna systems, its electrical parameters and generated electromagnetic field (EMF) for different frequency range. **Objectives**: Electromagnetic field (EMF – Electromagnetic Fields) studies on living organisms are one of the important branches of biomedical research. Most of this type of research is conducted using dedicated exposures system with fixed and controlled EMF exposure conditions. The purpose of biomedical research is to determine the influence of electromagnetic fields on living organisms. For this purpose the exposure systems are designed. The main task of the exposure antenna system, is to produce the EMF with known and controlled parameters in a specific EMF area. Depending on the frequency and the component (E or H) of the electromagnetic field used, different types of systems are used. For low frequencies (for instance 50 Hz common frequency) and magnetic fields, Helmholtz solenoids or coils are used, and for electric fields - flat capacitors (E Field). For higher frequencies field E is used for systems with linear antennas or TEM lines. There are also dedicated probes for invasive tissue heating. Each solution has its advantages and limitations and usually there are no universal solutions for all cases. Results: For the generation of a low frequency magnetic field up to several hundred Hz, the Helmholtz solenoid or coil is generally used because of its relatively simple construction, the ability to obtain high intensity and good homogeneity of the field in a relatively large area relative to the dimensions of the whole system. The homogeneous field area can be determined analytically based on system geometry or measurement. Otherwise it looks for exposure system above few MHZ. To create a homogeneous EMF in the field of radio frequencies, the exposure systems - usually the TEM lines (Crawford compartment) or sometimes the GTEM are very likely to be used. In both cases there are frequency and spatial limitations - the homogeneous field is assumed to be maximally present. At 1/3 the height between the plates of the chamber and at the same time the maximum frequency of operation of the TEM chamber can be described by the approximate dependence of fmax [MHz] = 50 / d [m], resulting in a chamber operating at 1 GHz. The work piece does not exceed a height of about 1.5 cm with a diameter of about 4 cm. Larger working areas, but at the same time, a lower homogeneity of the field can be obtained in the GTEM chamber - but at the same time the GTEM chamber has much larger geometric dimensions. Another way is to produce PEM with the parameters in open space - in the vicinity of the antenna. In this case, it is very important to select an antenna so that the expected homogeneous area can be obtained at an acceptable distance from the antenna - in order to maintain high EMF intensity and to reduce the radiation of the antenna beyond the desired area. This can be achieved by limiting the emission area by, for example, shielding or using EMF absorbers. In addition authors simulate novel ablation antenna for ablation treatment. **Conclusions:** Assessing the impact of EMF on biological objects is an interdisciplinary studies that requires the involvement of biological or medical specialists, as well as the EMF standard field and metrology specialist. In this work we have taken the subject of correct selection and description used in the experience of exposure systems. The authors presented the most commonly used EMF emitters in the low frequencies and microwave bands, as well as new model of the ablation treatment antenna.

Keywords*:* antenna, exposure systems, frequency, electromagnetic field.

Introduction

Biomedical research related to the effects of electromagnetic fields (EMF) on organisms carried out since many years and research methods are still improving.

For the purpose of laboratory research is to develop appropriate systems exhibition, enabling to obtain stable and controlled conditions of exposure to the objects. Depending on the anticipated effects and the frequency range are used different solutions, eg. For low frequency magnetic fields are used solenoids or Helmholtz coils [1], for EMF within the higher frequency range such as TEM lines or systems of linear antennas or horn antennas.

The paper presents proposals antennas designed specifically for the exhibition system with popular radio systems - GSM900 / UMTS.

The main goal was to achieve a relatively homogeneous field in the area of approx. 10×10 cm in the smallest possible distance from the antenna - already about 10 cm.

Idea of exposure antenna

The information electromagnetic field of standard and controlled parameters. The key is to control the intensity of EMF, its spectral parameters and foremost to achieve high uniformity. Fig. 1 presents a block diagram of an exemplary exposition system. It includes: microwave power source, antenna operating in the selected frequency band and the system controlling the intensity based on feedback from the EMF probe based on EMF sensors and computer with dedicated software. The antenna is chosen to achieve the desired s to ensure constant, controlled conditions is used EMF control system parameters, usually working with dedicated control software [2]. Instead of measuring the field strength is also possible to monitor the power supply and the matching antenna. To ensure repeatability of biomedical research provide stable conditions of exposure. The most optimal solution would be to standardize testing procedures and as far as possible - exposure systems [3]. Example of that exposure system is presented on Fig. 2.

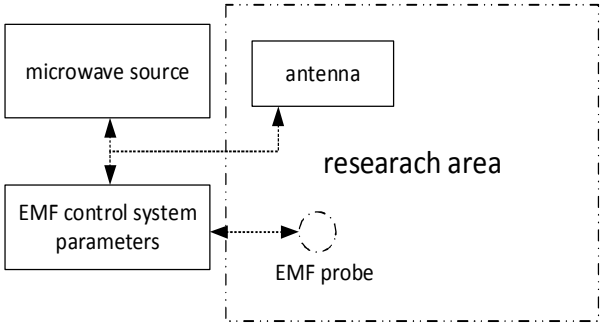


Fig. 1. Exposition block diagram

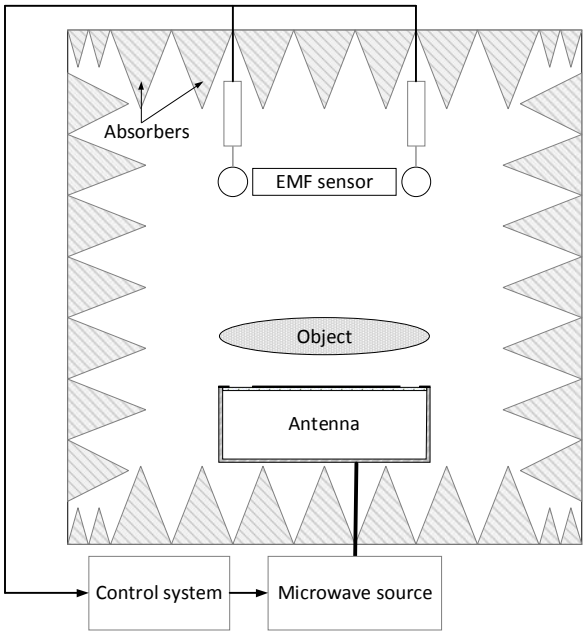


Fig. 2. Exposure system for high freqencies

Prototype antenna

Analyzing the parameters of the antenna used in exposure research were taken into account two main factors: the possibility of obtaining a uniform intensity with wide area above the antenna in order to its geometrical dimensions. Less important was the bandwidth of the antenna and gain. It is assumed that the frequency band of the antenna should coincide with the frequencies of the popular systems such as GSM900/UMTS and advantageous is if it works as a multiband antenna. As the best solution for proposed purposes are microstrip antennas. Although they are characterized by a relatively narrow bandwidth (up to tens of MHz), but it is possible to design a multi-band antenna with relatively small geometrical dimensions.

The primary disadvantage of conventional microstrip antennas is their high sensitivity to coupling with the environment and high levels of back lobe. These disadvantages can be minimized by using a layered antenna cavity, which is a modification of microstrip antenna. By using resonant cavity to reduce the back lobe, minimizes the sensitivity of the antenna and couplings with the environment (which is very desirable in laboratory exposure systems). In additaion it extends the operating band of the antenna. Has been developed several models of antennas, the final results presents dual band cavity microstrip antenna (CMA) for GSM 900 / UMTS band. Fig. 3 shows fabricated antenna.

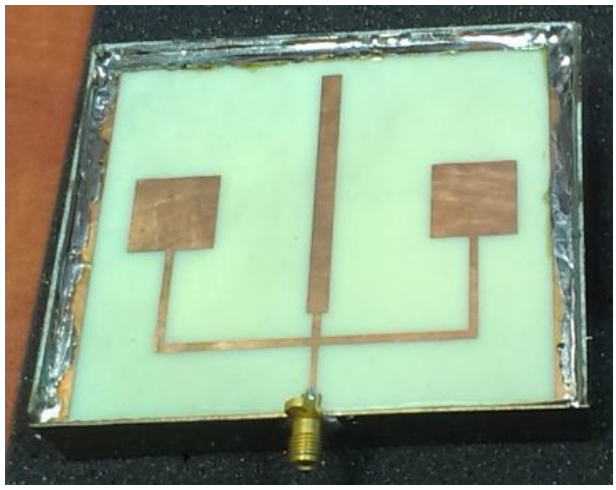


Fig. 3. Exposure system for high freqencies

Dual-band antenna CMA (Fig. 5) is designed as a system of three radiating patches - center patch is responsible for the GSM900 band and the side patches for UMTS. Circuits parameters of fabricated prototype has been tested and results are with the good agreement with the simulated ones. The reflection cooefcient (S11) of the antenna is shown in Fig. 4. The results translate into a VSWR ratio of less than 1.5 for a bandwidth of 8MHz in the range for GSM900 and 64 MHz bandwidth for UMTS. VSWR less than 1.5 provide losses less than 4 % of the reflected power.

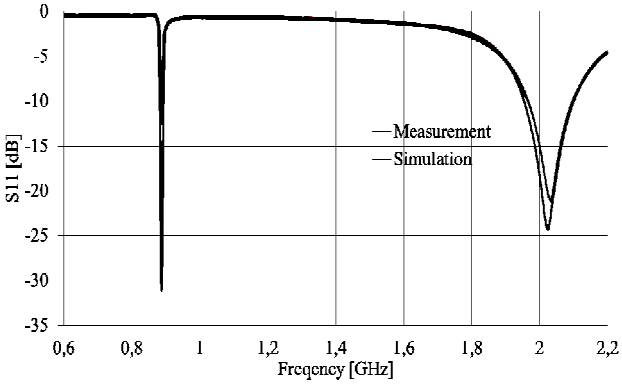


Fig. 4. Reflection coefficient for both, simulated and measurement results respectively

From the perspective of biomedical research , the most important is field distribution in selected area above the antenna in the possible small distance. It reduce the radiating area and achive high intensity field at an acceptable power supply. This results from the test object is often located in near field area or the transition zone between the near field and far field. Analyzed antenna for far-field distance is based on the popular dependence and a far field for CMA GSM900 is 10cm and 20 cm antennas CMA UMTS. Numerical analysis showed that the field uniformity over the antenna is better than ±2dB in the area of 10x10cm and can be obtained at a height of approx. 10cm above the

antennas. EMF distribution experimentally measured for two different height of 5 cm and 10 cm above each of the proposed antennas. The measurements were made using an isotropic probe EMF EP600. The results obtained for the powered antenna by 23 dBm are shown in Table 1.

Table 1. **The results obtained for the powered antenna by 23 dBm**

Antenna	Frequency [MHz]	Inhomogeneity %
CMA_{GSM900}	888	8
CMA_{UMTS}	2034	17

Results

In Fig. 5 it can be seen that the uncertainty generated PEM antenna CMA 5 cm above the antenna is 1.6 dB (± 23 %), while for a 10 cm from the antenna is only 0.6 dB (± 8 %) for the GSM 900 and 1.2 dB (± 17 %) for UMTS . In the case of distribution PEM antenna CBSA obtained 1.5 dB (± 21 %) for 5 cm and 1 dB (± 12 %) for 10 cm. The obtained results provide a satisfactory EMF distribution at 10 cm above the antenna for the area of 10x10cm (Fig. 6).

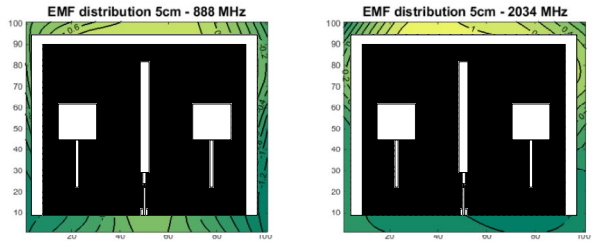


Fig. 5. Measured EMF distribution above 5 cm for both frequencies in dB

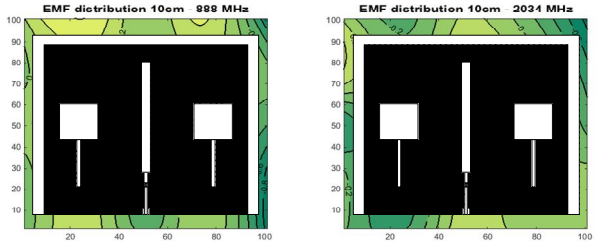


Fig. 6. Measured EMF distribution above 10 cm for both frequencies in dB

Schedules PEM studied two prototypes have a large convergence of results, so it is possible to use both types of antenna systems while maintaining the parameters exhibition field.

Conclusion

Fig. 7 present small microwave anechoic chamber with the proposed novel antenna used in biomedical research.

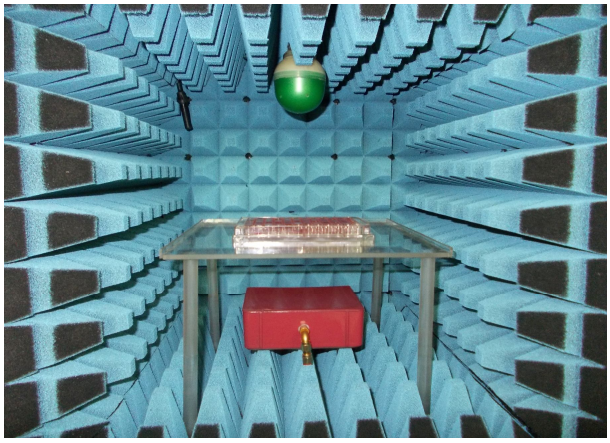


Fig. 7. Small microwave chamber used in biomedical research

Has been used a dedicated software to control the parameters of the icunbator interior. It has been made by means EMF probe (green bulb), which is placed directly above the antenna along the EMF absorbers. Small sizes of the antenna with high gain (3-9dBi) provide higher intensity round about the petri dish with small amount of microwave source.

The paper presents optimized antennas used in systems for bio medical research. Especially exposure for small objects. (eg. Cell incubator showed of fig. 7) The results are satisfactory obtained homogeneous field area (with deviations of less than 1.6 dB) at 10cm above the antenna.

At the same time the system has a high energy efficiency, which can be described as ratio of "energy intensity".

Presented results are step to standard methods and exposure systems used in biomedical research.

REFERENCES

1. Bieńkowski, Paweł, Cała, Paweł, Wyszkowska, Joanna and Zubrzak, Bartłomiej (2015), "Układy Ekspozycyjne PEM W Badaniach Biomedycznych. Przegląd Telekomunikacyjny", *Wiadomości Telekomunikacyjne*, R. 88 No. 4, pp. 510-514.
2. Bieńkowski, Paweł and Zubrzak, Bartłomiej (2011), "Algorytmy Ustalania Zadanych Wartości W Układzie Ze Sprzężeniem Zwrotnym Na Przykładzie Automatycznego Stanowiska Wzorcowego Pola Elektromagnetycznego Z Antenami Tubowymi", *Electrical Review*, R. 87 9a, pp. 160-165/
3. Vallauri, R. Bertin, G. Piovano, B. and Gianola, P. "Electromagnetic Field Zones Around An Antenna For Human Exposure Assessment", *Antennas And Propagation Magazine*, IEEE Vol. 57 (5), pp. 57-63.
4. Cała, Paweł and Słobodzian, Piotr (2013), "Cavity-Backed Slot Antenna For Wireless Sensor Integration", *23th Microwave And Radio Electronics Week* (Marew 2013), IEEE Nr Cfp1385b-Prt, Pardubice, Czechy, pp. 72-75.
5. Cała, Paweł annd Słobodzian, Piotr (2013), „Zastosowanie Elementu Promieniującego Typu Cbsa W Układzie Antenowym Bezprzewodowego Sensora Naziemnego", Przegląd *Telekomunikacyjny I Wiadomości Telekomunikacyjne*, 6/2013, July 2013, pp. 400-403.

Received (надійшла) 14.02.2017
Accepted for publication (прийнята до друку) 30.05.2017

Системи експозиції,
що використовуються для оцінки впливу електромагнітного поля на живі організми

П. Кала, П. Бієнковський

Предметом дослідження є процеси аналізу та оцінки впливу електромагнітного поля на людей. **Мета** - оптимізувати розмір антенних систем експонування, їх електричних параметрів і генералізованого електромагнітного поля (ЕМП) для різних частотних діапазонів. **Завдання**: дослідження дії електромагнітного поля на живі організми. Дане дослідження є однією з важливих галузей біомедичних досліджень. Велика частина цього типу досліджень проводиться з використанням спеціальної системи експозиції з фіксованими та контрольованими умовами експозиції ЕМП. Метою біомедицинських досліджень є визначення впливу електромагнітних полів на живі організми. Для цього розроблені системи експозиції. Основна задача системи антенного експонування полягає в створенні ЕМП з відомими та контрольованими параметрами в конкретній області ЕМП. В залежності від частоти та компоненту використовуваного електромагнітного поля використовуються різні типи систем. Для низьких частот і магнітних полів використовуються соленоїди або котушки Гельмгольца, а для електричних полів – плоскі конденсатори. Для більш високих частот поля використовується система з лінійними антенами. Існують також спеціальні пробники для інвазивного нагрівання тканини. Кожне рішення має свої переваги та обмеження, та для всіх випадків немає універсальних рішень. **Результати**. Для генерації низькочастотного магнітного поля звичайно використовують котушки Гельмгольца із-за їхньої відносно простої конструкції, здатності отримувати високу інтенсивність та хорошу однорідність поля у відносно великій відносній площі до розмірів всієї системи. Область однорідного поля може бути визначена аналітично на основі геометрії або вимірювання системи. В протилежному випадку відбувається пошук системи експозиції вище декількох мГц. Існують частотні та просторові обмеження – припускається, що однорідне поле максимально присутнє. Дуже важливо обрати антену так, щоб очікувана однорідна область могла бути отримана на прийнятній відстані від антени – для підтримки високої інтенсивності ЕМП та зменшення випромінювання антенних сигналів за межами бажаної області. Це може бути досягнуто шляхом обмеження площі викидів, наприклад, шляхом екранізації або використання поглиначів ЕМП. Крім того, автори моделюють нову абляційну антенну для лікування абляції. **Висновки.** Оцінка впливу ЕМП на біологічні об'єкти є міждисциплінарним дослідженням, яке вимагає участі біологічних або медичних спеціалістів, а також спеціаліста з електромагнітних полів та метрології. В роботі розглядається питання правильного вибору та опису, використаного при експерименті систем експонування. Автори представили найбільш часто використовувані емітери ЕМП в низкочастотних та мікрорівневих діапазонах, а також нову модель антен обробки аблації.

Ключові слова: антена, системи експозиції, частота, електромагнітне поле.

Системы экспозиции,
используемые для оценки воздействия электромагнитного поля на живые организмы

П. Кала, П. Биенковский

Предметом исследования являются процессы анализа и оценки воздействия электромагнитного поля на людей. **Цель** - оптимизировать размер антенных систем экспонирования, его электрических параметров и генерируемого электромагнитного поля (ЭМП) для разных частотных диапазонов. **Задачи**: исследования электромагнитного поля на живых организмах. Данные исследования являются одной из важных отраслей биомедицинских исследований. Большая часть этого типа исследований проводится с использованием специальной системы экспозиции с фиксированными и контролируемыми условиями экспозиции ЭМП. Целью биомедицинских исследований является определение влияния электромагнитных полей на живые организмы. Для этой цели разработаны системы экспозиции. Основная задача системы антенн экспонирования заключается в создании ЭМП с известными и контролируемыми параметрами в конкретной области ЭМП. В зависимости от частоты и компонента используемого электромагнитного поля используются различные типы систем. Для низких частот и магнитных полей используются соленоиды или катушки Гельмгольца, а для электрических полей - плоские конденсаторы. Для более высоких частот поле Е используется системы с линейными антеннами. Существуют также специальные зонды для инвазивного нагрева ткани. Каждое решение имеет свои преимущества и ограничения, и обычно для всех случаев нет универсальных решений. **Результаты**. Для генерации низкочастотного магнитного поля обычно используют катушки Гельмгольца из-за его относительно простой конструкции, способности получать высокую интенсивность и хорошую однородность поля в относительно большой относительной площади к размерам всей системы. Область однородного поля может быть определена аналитически на основе геометрии или измерения системы. В противном случае происходит поиск системы экспозиции выше нескольких мГц. Существуют частотные и пространственные ограничения - предполагается, что однородное поле максимально присутствует. Очень важно выбрать антенну так, чтобы ожидаемая однородная область могла быть получена на приемлемом расстоянии от антенны - для поддержания высокой интенсивности ЭМП и уменьшения излучения антенны за пределы желаемой области. Это может быть достигнуто путем ограничения площади выбросов, например, путем экранирования или использования поглотителей ЭМП. Кроме того, авторы моделируют новую абляционную антенну для лечения абляции. **Выводы.** Оценка влияния ЭМП на биологические объекты является междисциплинарным исследованием, которое требует участия биологических или медицинских специалистов, а также специалиста по электромагнитным полям и метрологии. В этой работе рассматривается вопрос правильного выбора и описания, использованного при эксперименте систем экспонирования. Авторы представили наиболее часто используемые эмиттеры ЭМП в низкочастотных и микроволновых диапазонах, а также новую модель антенны обработки абляции.

Ключевые слова: антенна, системы экспозиции, частота, электромагнитное поле.

УДК 004.94 **doi: 10.20998/2522-9052.2017.1.15**

С. Г. Семенов[1], Кассем Халифе[2], М. М. Захарченко[3]

[1] Национальный технический университет "ХПИ", Харьков, Украина
[2] Технический институт, Мараке, Ливан
[3] Харьковский национальный университет Воздушных Сил имени И. Кожедуба, Харьков, Украина

УСОВЕРШЕНСТВОВАННЫЙ СПОСОБ МАСШТАБИРОВАНИЯ ГИБКОЙ МЕТОДОЛОГИИ РАЗРАБОТКИ ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ

Предметом изучения статьи является усовершенствованный способ масштабирования гибкой методологии разработки программного обеспечения. **Цель** - снижение потенциальных потерь, обусловленных рисками безопасности разработки и эксплуатации программного обеспечения на большинстве этапов его жизненного цикла. **Задачи**: анализ существующих методологий и подходов разработки программного обеспечения, исследование возможностей масштабирования методологий в рамках отдельных проектов, усовершенствование общей схемы цикла разработки программного обеспечения, разработка структуры управления разработкой программного обеспечения в рамках как отдельно взятого проекта, так и организации-разработчика в целом, разработка практических рекомендаций по повышению безопасности программного обеспечения на различных этапах жизненного цикла. Используемыми **методами** являются**:** системный анализ рисков, причинно-следственный анализ. Получены следующие **результаты.** Проведен анализ существующих гибких методологий разработки программного обеспечения, определены перспективные направления и подходы данной индустрии, выявлены возможности масштабирования гибких методологий. Усовершенствована схема жизненного цикла разработки программного обеспечения, отличительной особенностью которой является введение дополнительных подразделов и ролей, имеющих целью повышение безопасности программного обеспечения. Усовершенствована структура управления разработкой программного обеспечения, отличающаяся от известных учетом рисков безопасности в процессе разработки. Разработаны практические рекомендации использования усовершенствованного способа масштабирования гибкой методологии. **Выводы.** Реализация предложенного усовершенствованного способа масштабирования существующей методологии разработки ПО, отличается от известных включением и использованием в команде разработчиков дополнительных специалистов безопасности. Это может повлечь некоторое замедление выполнения кода и увеличение количества выявленных дефектов (багов) при альфа-тестировании, а, следовательно, увеличение времени жизненного цикла багов. Однако в перспективе эти локальные ухудшения позволяют добиваться лучшего конечного результата (повышения безопасности разработанного ПО) и обеспечивать как быстрый рост функционала, так и приемлемый уровень качества сервиса. А это в свою очередь будет привлекательным мотивом дальнейшего сотрудничества заказчика и фирмы-разработчика.

Ключевые слова: безопасность программного обеспечения, гибкие методологии разработки программного обеспечения, Agile, Scrum.

Введение

Концепция качества программного обеспечения (ПО) возникла как обобщение ряда похожих, но в то же время и имеющих определенные отличия концепций. Эти концепции были предложены рядом крупных специалистов в области менеджмента [1, 4], которых часто называют «учителя качества». Все они оказали огромное влияние на экономики целых стран и способствовали переходу к эпохе «всеобщего качества» (TQM). Их теории, в отличие от социально-экономических доктрин прошлых лет, проверены по критерию эффективности, они имеют комплексный, собирательный характер, анализируя и синтезируя все наиболее ценное в опыте различных компаний и даже стран [4]. Эти концепции демонстрируют возрастающую роль всех участников процесса в достижении успешного развития и конкурентоспособности компаний (изделий), при этом подчеркивают важность мотивации и непрерывного обучения, совершенствования персонала, его адаптации к изменениям конъюнктуры и «вызовам» внешних факторов.

Основываясь на уже известные постулаты менеджмента IT-индустрии, в последнее время разработчики программного обеспечения непрерывно ищут новые пути решения задач оптимизации процесса управления разработкой ПО и усовершенствуют существующие гибкие методологии. Это приводит к появлению усовершенствованных правил и способов разработки, новых подходов коммуникаций и управления и даже появлению новых профессий (например, DevOps). При этом вопросы, связанные с организацией работы, при неизменном качестве ПО, остаются. Кроме того в условиях возникновения новых рисков на всех этапах жизненного цикла программного обеспечения (в частности рисков безопасности ПО) эти вопросы усложняются и, как показали исследования, спектр нерешенных актуальных задач имеет тенденцию расширения.

Анализ проблемы и постановка задачи

Анализ литературы [1–13] а так же результаты проведенных исследований показали, что комплексное использование современных подходов разработки ПО (Agile, DevOps, Lean и др.), которые, благодаря современным средствам автоматизации, получили новый стимул к развитию, в совокупности с технологиями синтеза и адаптации новых участников проектов (в соответствии с требованиями минимизации рисков), могут позволить минимизи-

ровать временные затраты на разработку и обеспечить определенное заказчиком качество ПО.

Можно заметить, что итеративность, обратная связь и гибкость Agile-методов, основанных на взаимодействии команд разработчиков, дают возможность для постоянного и непрерывного выпуска ПО, а синтез и адаптация усовершенствованных подходов [5, 13] в Agile-методы позволяет устранить ряд недостатков, связанных с существующими рисками экономического, социального, правового и других направлений [12].

В то же время, мировые тенденции увеличения киберпреступности и повышенного внимания заказчиков к безопасности эксплуатации ПО, требуют от разработчиков усовершенствования и реализации новых подходов и способов масштабирования методологий разработки ПО. В связи с этим поставленная задача масштабирования гибкой методологии разработки программного обеспечения является актуальной.

Решение проблемы

Как отмечено выше, воспользоваться существующим опытом масштабирования, а так же разработать новые решения необходимо в условиях повышения требований к безопасности программного обеспечения. В таких условиях необходимо видоизменять некоторые положения менеджмента и разработки ПО, а также вносить новые элементы в уже существующую систему и жизненный цикл ПО. Для обеспечения качества ПО предлагается усовершенствованная схема цикла разработки ПО представленная на рис. 1.

Как видно из этой схемы в общий цикл разработки ПО рекомендуется включить следующие подразделы:

1. «Чистота» кода – введение безопасного кодирования;

2. Безопасный DevOps – включение дополнительных субъектов и инструментов безопасности;

3. Моделирование угроз – предполагает введение новой роли специалиста управления кибербезопасностью;

4. Анализ рисков безопасности – анализ приоритетности в отставания.

Кроме этого дополнительные требования безопасности ПО требует введения новой роли «Этичный» хакер.

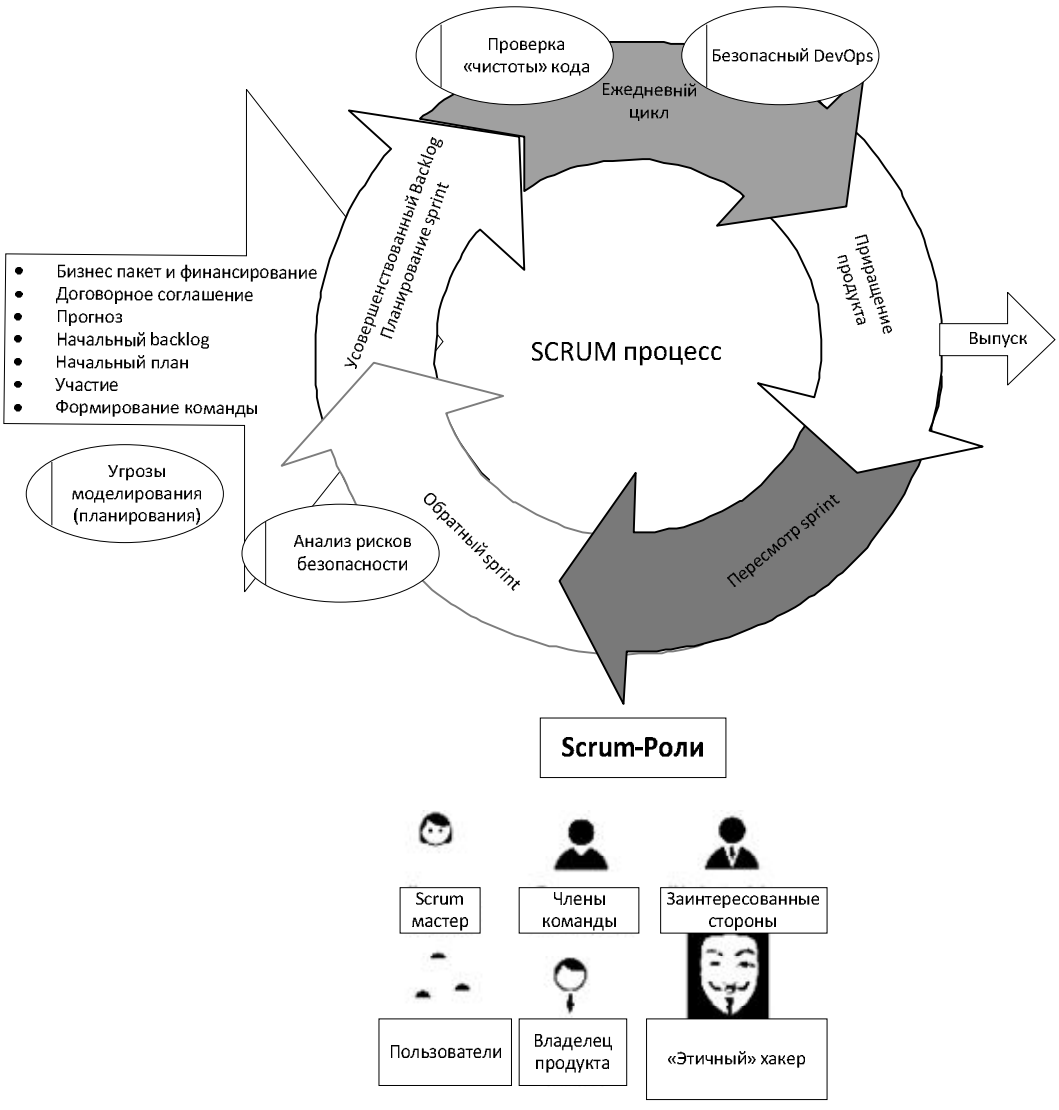


Рис. 1. Усовершенствованная схема цикла разработки ПО

Следует заметить, что внедрение в команду на разных этапах разработки программного обеспечения специалиста кибербезопасности, безопасного программирования и особенно тестирования безопасности («этичного хакинга») [2б 13], является одним из требований современного рынка разработки программного обеспечения. Принципы такого внедрения на данном этапе развития индустрии разработки программного обеспечения должны лежать в рамках «горизонтального» (межкомандного) управления. Данный подход полностью соответствует принципам бережливой разработки (Lean), которая в свою очередь, обеспечивает минимизацию издержек при выпуске новых версий программного обеспечения.

С учетом указанных основных принципов усовершенствованную обобщенную структуру управления разработкой программного обеспечения можно представить в виде схемы, показанной на рис. 2.

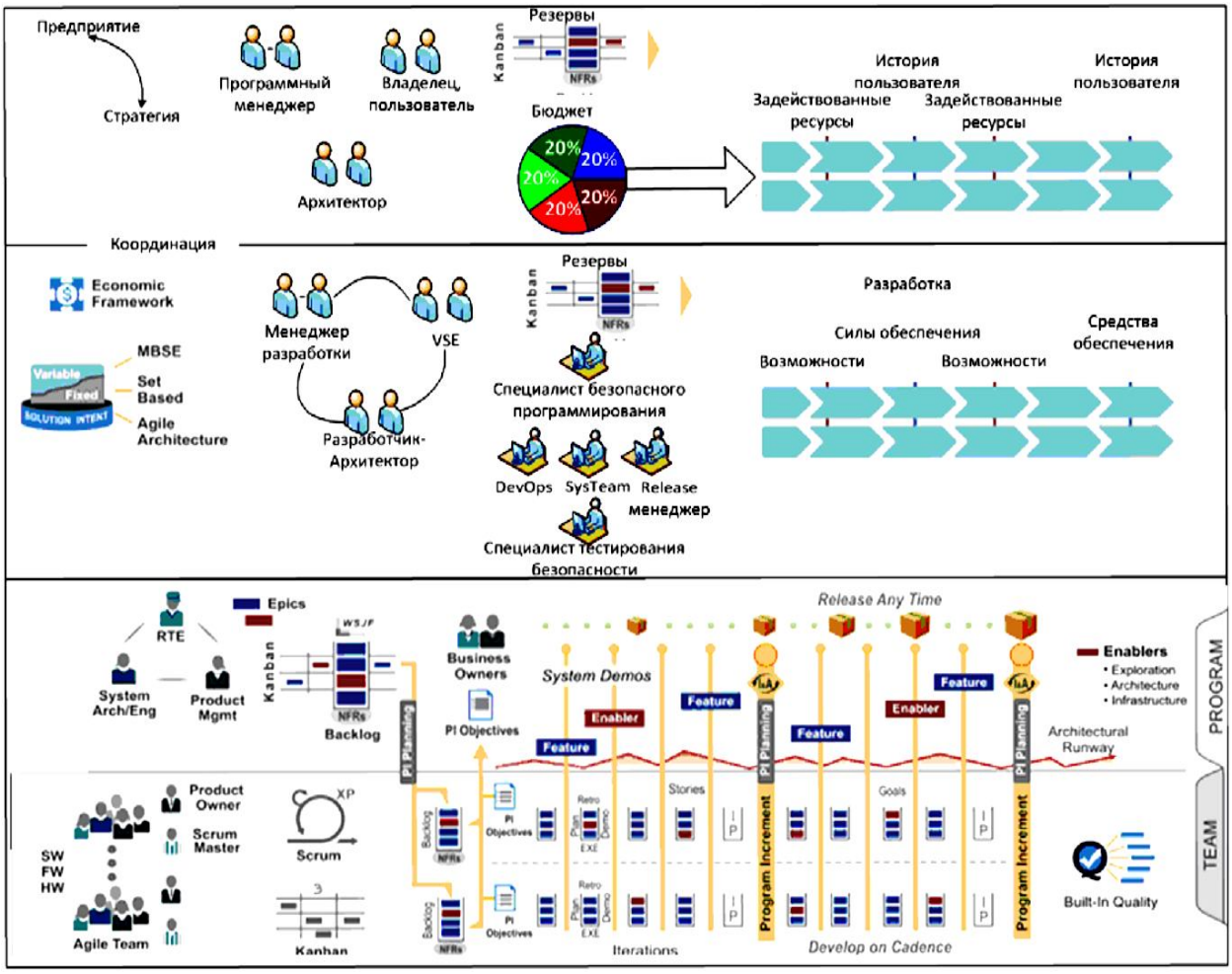


Рис. 2. Усовершенствованная обобщенная структура управления разработкой ПО

Следует заметить, что предложенная схема имеет своей целью оптимизацию и поддержку крупномасштабных разработок, т.е., работа большой команды идет не только по спринтам (двухнедельным циклам), как в Scrum, а с дополнительной итерацией планирования (program increment) длительностью десять недель.

В качестве примера рассмотрим случай, когда от бизнеса (заказчика) поступает запрос на новый функционал.

Бизнес-аналитик его рассматривает и преобразует в задания для разработчиков, которые создают или изменяют код и помещают его в хранилище.

В этот момент возможно подключение специалиста безопасного программирования, который на принципах «смоки» тестирования может оценить уровень безопасности кода.

В среде непрерывной интеграции (CI tools) код автоматически компилируется и сохраняется в нужной версии в репозитории.

Автоматически строится тестовая среда с необходимой конфигурацией для запуска последней версии кода. Автоматически осуществляется регрессионное тестирование и тестирование безопасности.

В случае успеха ресурсы тестовой среды высвобождаются и автоматически создается среда для интеграционного тестирования, а в системе ITSM формируется задание на внесение изменения в промышленную среду. Автоматически выполняется интеграционное тестирование. В случае

успеха и после согласования изменения в системе ITSM код автоматически разворачивается в промышленной среде.

Таким образом, от постановки требований до перевода новой версии в промышленную эксплуатацию проходят часы, а не месяцы, как в традиционных информационных технологиях. Иллюстрация интервалов времени на этапах разработки, а также объемов выполнения указанных функций безопасности представлена на временной диаграмме фаз и этапов разработки программного обеспечения (рис. 3).

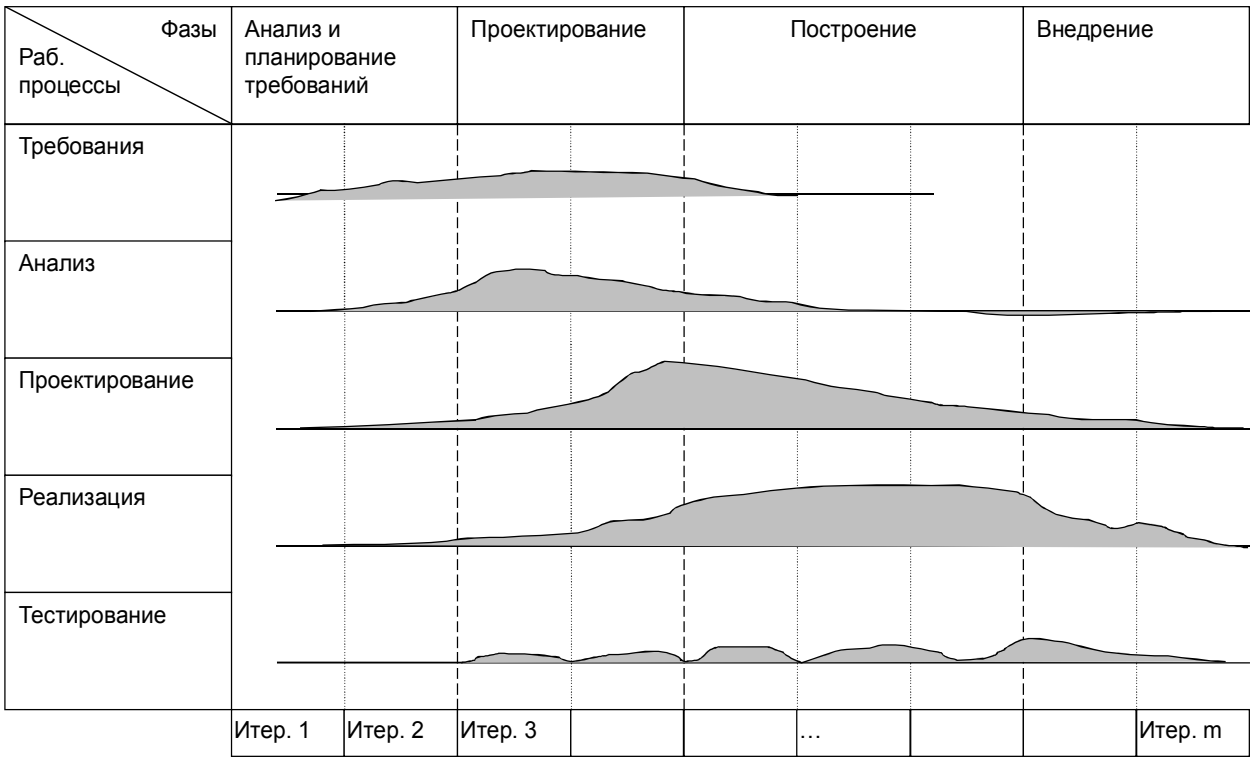


Рис. 3. Временная диаграмма фаз и этапов разработки ПО

Опишем более подробно функции безопасности на каждом этапе.

На этапе анализа и планирования требований идея превращается в концепцию готового продукта. При этом создаются:

- бизнес-план разработки;
- упрощенная модель вариантов использования;
- пробный вариант архитектуры.

На этом же этапе выявляются и оцениваются риски, расставляются приоритеты и выполняется грубая оценка проекта.

Специалистам по безопасному программированию и тестированию безопасности очень важно на этом этапе предоставить достоверную информацию о существующих рисках безопасности и представить общую концепцию (архитектуру) информационной защиты проекта.

На этапе проектирования выполняется детальное описание вариантов использования, формируется архитектура в виде представлений всех моделей и разрабатывается план действий и оценка ресурсов.

В этом случае, как и на первом этапе, очень важно избежать возможных ошибок безопасности и «лазеек» в архитектуре программного обеспечения и рисков их недооценки.

На этапе построения производится уточнение базового уровня архитектуры и реализуются все варианты использования. На этом этапе специалисты безопасного программирования консультативным путем и путем «смоки» тестирования должны обеспечить качество кода программного обеспечения, а специалисты тестирования должны выполнить полный набор тест-кейсов, имеющих отношение к безопасности и информационной защите.

На этапе внедрения осуществляется бета-тестирование, выполняются тренинги сотрудников заказчиков, а также устраняются выявленные дефекты.

Действия рассматриваемых специалистов на этом этапе аналогичны их действиям на предыдущем этапе, с той разницей, что специалисты безопасного программирования должны осуществлять контроль устранения уже выявленных ошибок безопасности программного обеспечения.

Выводы

В целом следует заметить, что реализация предложенного усовершенствованного способа масштабирования существующей методологии разработки программного обеспечения, отличается от известных включением и использованием в команде разработчиков дополнительных специали-

стов безопасности. Это может повлечь некоторое замедление выполнения кода и увеличение количества выявленных дефектов (багов) при альфа-тестировании, а, следовательно, увеличение времени жизненного цикла багов.

Однако в перспективе эти локальные ухудшения позволяют добиваться лучшего конечного результата (повышения безопасности разработанного программного обеспечения) и обеспечивать как быстрый рост функционала, так и приемлемый уровень качества сервиса.

А это в свою очередь будет привлекательным мотивом дальнейшего сотрудничества заказчика и фирмы-разработчика.

Количество дополнительных сил, которые необходимы в том или ином проекте следует оценивать исходя из его сложности (масштаба) а так же уровня требований безопасности заказчика.

СПИСОК ЛИТЕРАТУРЫ

1. Barry W. Boehm, Richard Turner. Balancing Agility and Discipline - A Guide for the Perplexed. New York : Addison-Wesley, 2004. 266 p.
2. Демарко Т., Листер Т. Человеческий фактор: успешные проекты и команды. Санкт-Петербург : Символ–Плюс, 2005. 256 p.
3. Ruby S., Thomas D., Hansson D.H. Agile Web Development with Rails 4. Pragmatic Programmers, LLC., 2013. 439 p. ISBN: 978-1-93778-556-7.
4. Гуру менеджмента качества и их концепции [Электронный ресурс]. [Э. Деминг, Дж. Джуран, Ф. Кросби, К. Исикава, А. Фейгенбаум, Т. Тагути]. Режим доступа: http://www.management.com.ua/qm/qm009.html (last accessed April 10, 2017).
5. Hasan Yasar. Security Practitioner Perspective on DevOps for Building Secure Solutions. [Электронный ресурс]. 2016. Режим доступа: http://www.sei.cmu.edu/webinars/view_webinar.cfm?webinarid=474101&gaWebinar=Security PractitionerPerspectiveonDevOpsforBuildingSecureSolutions (last accessed April 10, 2017).
6. Highsmith J. Agile Software Development Ecosystems. Boston : AddisonWesley, 2006. 448 p.
7. Кузумано Майкл, Поппендик Мэри. Бережливая разработка программ [Электронный ресурс]. Открытые системы : СУБД. 2012. № 08/ Режим доступа: https://www.osp.ru/os/2012/08/13019237/ (last accessed April 10, 2017).
8. Makhmetov G. Ye. Kogda «agile» (ne) k mestu [Электронный ресурс]. Режим доступа: https://makhmetov.ru/ articles/agile.html (last accessed April 01, 2017).
9. Sherman Mark. Building Secure Software for Mission Critical Systems. [Электронный ресурс]. Режим доступа: http://resources.sei.cmu.edu/asset_files/Presentation/2017_017_001_495865.pdf (last accessed April 10, 2017).
10. Sherman Mark, Schiela Robert. From Secure Coding to Secure Software [Электронный ресурс]. Режим доступа: http://www.sei.cmu.edu/webinars/view_webinar.cfm?webinarid=483646 (last accessed April 10, 2017).
11. Putu Adi? Guna Permana Scrum Method Implementation in a Software Development Project Management/ (IJACSA) International Journal of Advanced Computer Science and Applications. 2015. Vol. 6, № 9. P. 199-205.
12. Швачич Г. Г., Семенов С. Г., Главчев М. И., Халифе Кассем. Модель расчета временных границ проектов разработки программного обеспечения. Системи управління, навігації та зв'язку. Полтава : ПНТУ, 2017. Випуск 1 (41) . С. 43-49.
13. Klieber William, Snavely William Automated Code Repair Based on Inferred Specifications [Электронный ресурс]. Режим доступа: http://resources.sei.cmu.edu/asset_files/ConferencePaper/2016_021_001_483599.pdf (last accessed April 10, 2017).

REFERENCES

1. Barry, W. Boehm and Richard, Turner (2004), *Balancing Agility and Discipline* - A Guide for the Perplexed, Addison-Wesley, New York, 266 p.
2. Demarko, T. and Lister, T. (2005), Chelovecheskiy faktor: uspeshnyye proyekty i komandy, Simvol-Plyus, Sankt-Peterburg, 256 p.
3. Ruby, S., Thomas, D. and Hansson, D.H. (2013), Agile Web Development with Rails 4, Pragmatic Programmers, LLC, 439 p., ISBN: 978-1-93778-556-7.
4. Deming, E., Dzhuran, Dzh., Krosbi, F., Isikava, K., Feygenbaum, A. and Taguti, T.(2001), Guru menedzhmenta kachestva i ikh kontseptsii, available at : http://www.management.com.ua/qm/qm009.html (last accessed February 1, 2017).
5. Hasan, Yasar (2016), Security Practitioner Perspective on DevOps for Building Secure Solutions, available at : http://www.sei.cmu.edu/webinars/view_webinar.cfm?webinarid=474101&gaWebinar=SecurityPractitionerPerspectiveon DevOpsforBuildingSecureSolutions (last accessed February 1, 2017).
6. Highsmith, J. (2006), Agile Software Development Ecosystems, Boston : AddisonWesley, 448 p.
7. Kuzumano, Maykland and Poppendik Meri (2012), “Berezhlivaya razrabotka program”, *Otkrytyye sistemy. SUBD*, No. 08, available at : https://www.osp.ru/os/2012/08/13019237/ (February 1, 2017).
8. Makhmetov, G.Ye. (2017), Kogda «agile» (ne) k mestu, available at : https://makhmetov.ru/articles/agile.html (last accessed February 1, 2017).
9. Sherman, Mark (2017), Building Secure Software for Mission Critical Systems, available at : http://resources.sei.cmu. edu/asset_files/Presentation/2017_017_001_495865.pdf (last accessed February 1, 2017).

10. Sherman, Mark and Schiela, Robert (2016), From Secure Coding to Secure Software, available at : http://www.sei. cmu.edu/webinars/view_webinar.cfm?webinarid=483646 (last accessed February 1, 2017).
11. Putu, Adi and Guna, Permana (2015), "Scrum Method Implementation in a Software Development Project Management", *International Journal of Advanced Computer Science and Applications*, Vol. 6, No. 9, pp. 199–205.
12. Shvachich, G.G., Semenov, S.G. Glavchev, M.I. and Kassem, Khalife (2017), "Model' rascheta vremennykh granits proyektov razrabotki programmnogo obespecheniya", *Sistemi upravlínnya navígatsíí ta zv'yazku*, PNTU, Poltava, No. 1 (41), pp. 43-49.
13. Klieber, Williamand and Snavely, William (2016), Automated Code Repair Based on Inferred Specifications, available at : http://resources.sei.cmu.edu/asset_files/ConferencePaper/2016_021_001_483599.pdf (last accessed February 1, 2017).

Надійшла (received) 02.03.2017
Прийнята до друку (accepted for publication) 06.06.2017

Удосконалений спосіб
масштабування гнучкої методології розробки програмного забезпечення

С. Г. Семенов, Кассем Халіфе, М. М. Захарченко

Предметом вивчення статті є удосконалений спосіб масштабування гнучкою методології розробки програмного забезпечення. **Мета** - зниження потенційних втрат, зумовлених ризиками безпеки розробки та експлуатації програмного забезпечення на більшості етапів його життєвого циклу. Завдання: аналіз існуючих методологій і підходів розробки програмного забезпечення, дослідження можливостей масштабування методологій в рамках окремих проектів, удосконалення загальної схеми циклу розробки програмного забезпечення, розробка структури управління розробкою програмного забезпечення в рамках як окремо взятого проекту так і організації-розробника в цілому, розробка практичних рекомендацій щодо підвищення безпеки програмного забезпечення на різних етапах життєвого циклу. Використовуваними **методами** є: системний аналіз ризиків, причинно-наслідковий аналіз. Отримані наступні **результати.** Проведено аналіз існуючих гнучких методологій розробки програмного забезпечення, визначені перспективні напрямки і підходи даної індустрії, виявлені можливості масштабування гнучких методологій. Удосконалено схему життєвого циклу розробки програмного забезпечення, відмінною рисою якої є введення додаткових підрозділів і ролей, що мають на меті підвищення безпеки програмного забезпечення. Удосконалено структуру управління розробкою програмного забезпечення, що відрізняється від відомих урахуванням ризиків безпеки в процесі розробки. Розроблено практичні рекомендації використання вдосконаленого способу масштабування гнучкою методології. **Висновки.** Реалізація запропонованого вдосконаленого способу масштабування існуючої методології розробки ПО, відрізняється від відомих включенням і використанням в команді розробників додаткових фахівців безпеки. Це може спричинити деяке уповільнення виконання коду і збільшення кількості виявлених дефектів (багів) при альфа-тестування, а, отже, збільшення часу життєвого циклу багів. Однак в перспективі ці локальні погіршення дозволяють добиватися кращого кінцевого результату (підвищення безпеки розробленого ПО) і забезпечувати як швидке зростання функціоналу, так і прийнятний рівень якості сервісу. А це в свою чергу буде привабливим мотивом подальшої співпраці замовника і фірми-розробника.

Ключові слова: безпека програмного забезпечення, гнучкі методології розробки програмного забезпечення, Agile, Scrum.

Advanced method
of scaling the flexible methodology of software development

S. Semenov, Kassem Khalifeh, M. Zakharchenko

The **subject** of the article is an improved way to scale flexible methodology of software development. The goal is to reduce the potential losses caused by the security risks of software development and operation at most stages of its life cycle. **Objectives:** analysis of existing methodologies and approaches to software development, exploring the possibilities for scaling methodologies within individual projects, improving the overall design of the software development cycle, developing a software development management framework for both the individual project and the development organization as a whole, developing practical Recommendations to improve the security of software at various stages of the life cycle. The **methods** that are used: system analysis of risks, cause-and-effect analysis. The following **results** are obtained. The analysis of existing flexible software development methodologies has been carried out, prospective directions and approaches of this industry have been determined, and the opportunities for scaling flexible methodologies have been identified. The scheme of the life cycle of software development is improved, the distinctive feature of which is the introduction of additional subsections and roles aimed at increasing the security of software. The structure of software development management is improved, which differs from the known ones taking into account the security risks in the development process. Practical recommendations for using an improved method of scaling a flexible methodology have been developed. **Conclusions.** The implementation of the proposed improved method of scaling the existing software development methodology differs from those known by the inclusion and use of additional security specialists in the development team. This may entail some slowdown in code execution and an increase in the number of detected defects (bugs) during alpha testing, and, therefore, an increase in the life time of bugs. However, in the future, these local impairments can achieve a better end result (improving the safety of the developed software) and provide both rapid growth of functionality and an acceptable level of service quality. And this, in turn, will be an attractive motive for further cooperation between the customer and the developer.

Keywords: software security, flexible software development methodologies, Agile, Scrum.

НАШІ АВТОРИ (AUTHORS)

БАЙРАМОВ Азад Агахар Огли (***Bayramov Azad Agalar oğlu***) — Військова академія Збройних Сил Азербайджанської республіки, Баку, Азербайджан, доктор фізико-математичних наук, професор, професор кафедри

БІЄНКОВСЬКИЙ Павел (***Pawel Bienkowski***) — Вроцлавський технологічний університет, Вроцлав, Польща, доктор наук (технічні), професор, професор науково-дослідного інституту телеінформатики та зв'язку; e-mail: pawel. bienkowski @pwr.edu.pl

ГАВРИЛЕНКО Світлана Юріївна (***Svitlana Gavryilenko***) — Національний технічний університет «ХПІ», Харків, Україна, кандидат технічних наук, доцент, професор кафедри обчислювальної техніки та програмування, e-mail: gavrilenko08@gmail.com; ORCID: 0000-0006-4561-8368

ГАШИМОВ Ельшан Гіяс огли (***Hashimov Elshan Giyas oğlu***) — Військова академія Збройних Сил Азербайджанської республіки, Баку, Азербайджан, кандидат технічних наук, доцент, начальник відділу науки та аспірантури

ГЕЙКО Геннадій Вікторович (***Gennadij Gejko***) — Національний технічний університет "ХПІ", Харків, Україна, старший викладач кафедри обчислювальної техніки та програмування, e-mail: gennady1752@gmail.com; ORCID: 0000-0001-6958-8306

ГОРЮШКІНА Алла Ернестівна (***Alla Goriushkina***) — Національний технічний університет "ХПІ", Харків, Україна, кандидат технічних наук, старший викладач кафедри обчислювальної техніки та програмування, e-mail: aegoriushkina@gmail.com; ORCID: 0000-0002-2134-9485

ДУБРОВСЬКИЙ Марк Сергійович (***Mark Dubrovskyi***) — Харківський національний університет Повітряних Сил імені Івана Кожедуба, Харків, Україна, магістрант, e-mail: m.dubrovskyi@gmail.com

ЄВДОКІМЕНКО Наталія Михайлівна (***Natalia Evdokimenko***) — Український державний хіміко-технологічний університет, Дніпро, Україна, доктор хімічних наук, професор, професор кафедри хімії та технології переробки еластомерів, e-mail: Tanya@ibv.dp.ua

ЖИВОТОВСЬКИЙ Руслан Миколайович (***Ruslan Zhyvotovskyi***) — Центральний науково-дослідний інститут озброєння та військової техніки Збройних Сил України, Київ, Україна; кандидат технічних наук, начальник НДВ – заступник начальника НДУ; e-mail: ruslan_zvivotov@ukr.net; ORCID: 0000-0002-2717-0603

ЗАХАРЧЕНКО Максим Михайлович (***Maksym Zakharchenko***) — Харківський національний університет Повітряних Сил імені Івана Кожедуба, Харків, Україна, магістрант e-mail: m.zaharchenko@gmail.com

КАЛА Павел (***Pawel Cala***) — Вроцлавський технологічний університет, Вроцлав, Польща, аспірант науково-дослідного інституту телеінформатики та зв'язку; e-mail: pawel.cala@pwr.edu.pl

КАССЕМ Халіфе (***Kassem Khalifeh***) — Технічний інститут, Мааракe, Ліван, викладач, (teacher of technical institute, Maarakeh, Lebanon), e-mail: en_kh_kassem@hotmail.com

КОВТУН Анатолій Васильович (***Kovtun Anatolii***) — Національна академія Національної гвардії України, Харків, Україна, кандидат технічних наук, доцент, професор кафедри експлуатації та ремонту автомобілів та бойових машин

КОРОЛЬОВ Роман Володимирович (***Roman Korolev***) — Харківський національний університет Повітряних Сил імені Івана Кожедуба, Харків, Україна, кандидат технічних наук, доцент кафедри бойового застосування та експлуатації АСУ, e-mail: korolevrv01@ukr.net

КОСЕНКО Віктор Васильович (***Viktor Kosenko***) — ДП "Харківський науково-дослідний інститут технології машинобудування", Харків, Україна, кандидат технічних наук, доцент, директор інституту, e-mail: kosv.v@ukr.ua; ORCID: 0000-0002-4905-8508

КУДХАІР Абед Тамер (***Khudhair Abed Thamer***) — Al-Maaref University College, Republic of Iraq, Head of the Chair of Computer Science, e-mail: maaref_database@yahoo.com

КУЧУК Ніна Георгіївна (***Nina Kuchuk***) — Харківський національний університет імені В.Н. Каразіна, Харків, Україна, кандидат педагогічних наук, доцент кафедри теоретичної та прикладної системотехніки, e-mail: nina_kuchuk@ukr.net, ORCID: 0000-0002-0784-1465

ЛІПЧАНСЬКИЙ Максим Валентинович (***Maksym Lipchanskyi***) — Національний технічний університет "ХПІ", Харків, Україна, кандидат технічних наук, доцент, доцент кафедри обчислювальної техніки та програмування, e-mail: maxl@meta.ua; ORCID: 0000-0003-2837-0444

МАЛЄЄВА
***Ольга* Володимирівна**
(*Olga Malyeyeva*)
Національний аерокосмічний університет імені М.Є. Жуковського «ХАІ», Харків, Україна, доктор технічних наук, професор, професор кафедри інформаційних обчислювальних систем, e-mail: omaleyeva@ukr.net, ORCID: 0000-0002-9336-4182

МІЩЕНКО
Максим Олександрович
(*Maksim Mischenko*)
Національний аерокосмічний університет імені М.Є. Жуковського "ХАІ", Харків, Україна, студент факультету авіаційних двигунів, e-mail: gladiator1994max@gmail.com

НОСКОВ
Валентин Іванович
(*Valentin Noskov*)
Національний технічний університет «ХПІ», Харків, Україна, доктор технічних наук, професор, професор кафедри обчислювальної техніки та програмування, e-mail: val1942@mail.ru; ORCID: 0000-0002-7879-0706

ОЛЕЩЕНКО
Володимир Віталійович
(*Vladimir Oleshchenko*)
Національний аерокосмічний університет імені М.Є. Жуковського "ХАІ", Харків, Україна, магістрант кафедри комп'ютерних систем та мереж, e-mail: vladimiroleshenko@gmail.com

ПЕРСІЯНОВА
Олена Юріївна
(*Elena Persiyanova*)
ДП "Південний державний проектно-конструкторський та науково-дослідний інститут авіаційної промисловості", Харків, Україна, інженер, e-mail: persikqw@gmail.com; ORCID: 0000-0003-3578-4653

ПЕТРУК
Сергій Миколайович
(*Sergii Petruk*)
Центральний науково-дослідний інститут озброєння та військової техніки Збройних Сил України, Київ, Україна; старший науковий співробітник; e-mail: petruk_serg_@ukr.net; ORCID: 0000-0002-0709-0032

ПЄВНЄВ
Володимир Якович
(*Vladimir Pevnev*)
Національний аерокосмічний університет імені М.Є. Жуковського "ХАІ", Харків, Україна, кандидат технічних наук, доцент, доцент кафедри комп'ютерних систем та мереж, e-mail: v.pevnev@csn.khai.edu

ПІСОЦЬКА
Людмила Анатоліївна
(*Lyudmila Pisotska*)
ДЗ «Дніпропетровська медична академія МОЗ України», Дніпро, Україна, доктор медичних наук, професор, професор кафедри внутрішньої медицини 3

ПОПОВА
Ольга Ігорівна
(*Olga Popova*)
Національний аерокосмічний університет імені М.Є. Жуковського "ХАІ", Харків, Україна, здобувач кафедри інженерії менеджменту, e-mail: Batbkivna@ukr.net

РОГОВИЙ
Антон Іванович
(*Anton Rogovyi*)
Національний технічний університет "ХПІ", Харків, Україна, кандидат технічних наук, доцент, доцент кафедри стратегічного управління, e-mail: npk.asystems@gmail.com; ORCID: 0000-0002-8178-4585

РОМАНЕНКО
Ігор Олександрович
(*Igor Romanenko*)
Центральний науково-дослідний інститут озброєння та військової техніки Збройних Сил України, Київ, Україна; доктор технічних наук, професор, провідний науковий співробітник; e-mail: igor_romanenk@ukr.net; ORCID: 0000-0001-5339-7900

САВИЦЬКИЙ
Віталій Вікторович
(*Vitalii Savitskyi*)
Харківський національний університет Повітряних Сил імені Івана Кожедуба, Харків, Україна, магістрант, e-mail: savitck@ukr.net

САЄНКО
Дмитро Миколайович
(*Dmitriy Saenko*)
Національний технічний університет «ХПІ», Харків, Україна, студент кафедри обчислювальної техніки та програмування, e-mail: dsdeveloper404@gmail.com

СЕМЕНОВ
Сергій Геннадійович
(*Serhii Semenov*)
Національний технічний університет «ХПІ», Харків, Україна, доктор технічних наук, старший науковий співробітник, завідувач кафедри обчислювальної техніки та програмування, e-mail: s_semenov@ukr.net; ORCID: 0000-0002-4905-850

СЕМЕНОВА
Анна Сергіївна
(*Anna Semenova*)
Національний технічний університет «ХПІ», Харків, Україна, студентка кафедри обчислювальної техніки та програмування, e-mail: 7enova98@gmail.com

СОБЧАК
Андрій Павлович
(*Andrii Sobchak*)
Національний аерокосмічний університет імені М.Є. Жуковського "ХАІ", Харків, Україна, кандидат технічних наук, доцент, доцент кафедри інженерії менеджменту, e-mail: Sobchak@ukr.net

ТАБУНЕНКО
Володимир Олександрович
(*Volodimir Tabunenko*)
Національна академія Національної гвардії України, Харків, Україна, кандидат технічних наук, доцент, професор кафедри експлуатації та ремонту автомобілів та бойових машин

ШИШАЦЬКИЙ
Андрій Володимирович
(*Andrii Shyshatskyi*)
Центральний науково-дослідний інститут озброєння та військової техніки Збройних Сил України, Київ, Україна; кандидат технічних наук, науковий співробітник; e-mail: ierikon12@gmail.com; ORCID: 0000-0001-6731-6390

ШОСТАК
Ігор Володимирович
(*Igor Shostak*)
Національний аерокосмічний університет імені М.Є. Жуковського "ХАІ", Харків, Україна, доктор технічних наук, професор, професор кафедри інженерії програмного забезпечення, e-mail: iv.shostak@ukr.net

Подання матеріалів статей до журналу

Обсяг рукопису – не менше 4 повних аркушів українською, англійською або російською мовами.

Формат аркушу А4 (21 × 29,7 см), параметри сторінки (відступи від краю):

– зліва – 2,25 см;

– зправа – 2,25 см;

– зверху – 2 см;

– знизу – 2,5 см.

Основний шрифт статті – Times New Roman, 10 кегль, міжрядковий інтервал (множник) – 1,0.

Для публікації необхідно представити статтю в електронній формі, яка оформлена згідно наведених нижче вимог та її роздрукований екземпляр, підписаний усіма авторами статті.

Структура тексту статті:

– постановка проблеми у загальному вигляді та її зв'язок із важливими науковими чи практичними завданнями;

– аналіз останніх досліджень і публікацій, на які спирається автор;

– формулювання мети статті (постановка завдання);

– виклад основного матеріалу дослідження з повним обґрунтуванням отриманих наукових результатів; висновки з даного дослідження і перспективи подальшого розвитку даного напрямку.

Анотації до статті виконуються українською, англійською та російською мовами та повинні розкривати:

– предмет, тему та мету роботи;

– метод (методи) або методологію проведення досліджень;

– результати досліджень;

– висновки та область застосування результатів досліджень.

Список літератури повинен включати не менш 8 джерел, які видані за останні 10 років. При цьому не менш 50% джерел повинно відноситися до іноземної періодики. Якщо основною мовою статі є українська або російська, то оформлюється два списки літератури: перший (список літератури на мові оригіналу джерела) – відповідно до ДСТУ 8302:2015 «Бібліографічне посилання: загальні положення та правила складання»; другий – на англійській мові та латиниці (транслітерації) – «References».

При подані статті автор повинен гарантувати дійсність наведених джерел та у разі необхідності надати їх у редакційну колегію. Якщо джерело інформації має ідентифікатор цифрового об’єкту DOI, то він обов’язково наводиться наприкінці опису, наприклад doi: 10.20998/2522-9052.2017.1.09.

У відомостях про авторів українською мовою наводяться:

– прізвище, ім’я та по батькові;

– науковий ступінь, вчене звання, посада;

– назва установи, де працює автор, її місце розташування (місто, країна);

– обліковий запис автора ORCID;

– адреса електронної пошти.

Рукопис супроводжується:

– рецензією доктора наук (професора);

– витягом з протоколу засідання кафедри (відділу).

Незалежне експертне рецензування проводиться з метою критичної оцінки рукописів, що подаються до публікації, спеціалістами, які не входять до складу редакційної колегії. Редакційна колегія направляє наукові статті, що публікуються, на зовнішнє анонімне рецензування незалежними експертами.

Схема оформлення статей (обов’язкові елементи)

УДК (кегль – 9 пт).

Перелік авторів статті (кегль – 11 пт).

Перелік установ, де працюють автори (назва без скорочень, місто, країна, кегль – 11 пт).

Назва статті (кегль – 12 пт).

Анотація мовою основного тексту статті (кегль – 9 пт).

Ключові слова мовою основного тексту статті (кегль – 9 пт).

Основний текст статті (кегль – 10 пт).

Список літератури (для статей українською або російською мовами, кегль – 9 пт)

References (кегль – 9 пт).

Вимоги до елементів статті

Набір формул здійснюється в редакторах формул **MS Equation** або **MathType**. Забороняється використовувати для набору формул графічні об'єкти, таблиці та редактор Формула (formula) Word 2007-2016.

В меню "Розмір → Визначити" ввести такі розміри: звичайний – 10 пт; великий індекс – 8 пт; малий индекс – 7 пт; великий символ – 14 пт; малий символ – 10 пт.

В меню "Стиль → Визначити" ввести стиль формул – "прямий", тобто поля "Формат символів" – пусті.

Рисунки обов'язково супроводжуються центрованими підрисунковими підписами (кегль – 9), ширина не більше 16,5 см, всі позначення виконуються кеглем не меншим ніж 8 пт.

У таблицях табличний заголовок (9 кегль) – обов'язковий.

Вимоги до оформлення References

References потрібно приводити окремим блоком, повторюючи послідовність попередньо наведеного списку літератури (при наявності), при цьому джерела англійською мовою дублюються. Джерела при цьому оформлюються за такими основними правилами (гарвардський стиль (Harvard style) оформлення BSI:

– запис завжди починається з прізвища автора, потім, через кому, ініціали (між ініціалами пропуски не ставляться), за якими в дужках вказується дата видання; два автори відокремлюються «and» без коми; кілька авторів розділяються комами, але останнє прізвище повинно бути відокремлено «and» без коми;

– витяги з публікацій, тобто назви статей журналів, глав в книгах наводять у "лапках";

– назва журналу або книги завжди виділяється курсивом;

– ім'я видавця вказується перед місцем видання;

– коми використовують для поділу елементів запису

– для джерел українською або російською мовою, що наводяться у References, назви статей журналів, глав в книгах наводять латиницею (транслітерацією) у "лапках" та перекладом на англійську мову у квадратних дужках. Онлайн-конвертер з української мови для транслітерації: http://translit.kh.ua/?passport.

Приклади оформлення цитування із різних типів неангломовних джерел (кирилиця)

1.1. Книга (ДСТУ 8302:2015).

1. Демарко Т., Листер Т. Человеческий фактор. Санкт-Петербург : Символ–Плюс, 2005. 256 р.

1.2. Книга (Harvard style оформлення BSI).

1. Demarko, T. and ister, T. (2005), *Chelovecheskiy faktor* [Human factor], Simvol-Plyus, Sankt-Peterburg, 256 p.

2.1. Стаття із періодичного видання (ДСТУ 8302:2015).

2. Швачич Г. Г., Семенов С. Г., Главчев М. И., Халифе Кассем. Модель расчета временных границ проектов. Системи управління, навігації та зв'язку. Полтава : ПНТУ, 2017. Вип. 1 (41). С. 43-49.

2.2. Стаття із періодичного видання (Harvard style оформлення BSI).

2. Shvachich, G.G., Semenov, S.G. Glavchev, M.I. and Kassem, Khalife (2017), "Model rascheta vremennykh granits proyektov [Model calculation of time boundaries of projects]",/ *Sistemi upravlínnya navígatsii ta zvyazku*, PNTU, Poltava, No. 1 (41), pp. 43-49.

3.1. Дисертація (ДСТУ 8302:2015).

3. Белозеров И.В. Религиозная политика: дис. … канд. ист. наук: 07.00.02; защищена 22.01.02; утв. 15.07.02 / Белозеров Иван Валентинович. – К., 2002. – 215 с.

3.2. Дисертація (Harvard style оформлення BSI).

3. Belozerov, (2002), "*Relyhyoznaia polytyka*: dissertation" [The religious policy: dissertation], Kiev, 215 p

4.1. Джерела електронного ресурсу віддаленого доступу (ДСТУ 8302:2015).

4. Кузумано Майкл, Поппендик Мэри. Бережливая разработка программ [Электронный ресурс]. Открытые системы : СУБД. 2012. № 08. Режим доступа: https://www.osp.ru/os/2012/08/13019237/ (останнє звернення 10.04.2017).

4.2. Джерела електронного ресурсу віддаленого доступу (Harvard style оформлення BSI).

4. Kuzumano, Maykland and Poppendik, Meri (2012), "Berezhlivaya razrabotka program [Wasteful development of programs]". *Otkrytyye sistemy*. SUBD, № 08, available at: https://www.osp.ru/os/2012/08/13019237/ (last accessed April 10, 2017).

Submission of articles for journal

The manuscript volume should be at least 4 full pages in Ukrainian, Russian or English.

Page size: A4 (21 × 29.7 cm). Page setup (margins):

– left – 2.25 cm;

– right – 2.25 cm;

– top – 2 cm;

– bottom – 2.5 cm.

Body text – use Times New Roman font; face – Roman; font size – 10 pt, Line spacing is set by multiplier of 1.

It is necessary to present the article in electronic form, which is finalized according to the requirements and with printed copy, signed by all authors.

Structure of the manuscript: the article should include the following elements:

– general problem statement and its relation to up-to-date scientific and practical tasks;

– analysis of recent research and publications in the relevant field;

– statement of the article tasks;

– the main part wich explaining the research conducted and obtained scientific results;

– conclusions of the conducted research and prospects to be developed in the future works.

Abstract of manuscript should be written in Ukrainian, English and Russian, and explain:

– subject, theme and objective of the research;

– method (methods) or methodology of research;

– results of research;

– application possibilities of research results.

The reference list should include not less than 8 sources that have been published for the past 10 years. Herewith, not less than 50 percent of sources should be from foreign journals. Self-citation of the authors in the list of references should not exceed 30 percent. If the basic language of the article is Ukrainian or Russian, then two reference lists should be completed: the first one (reference list in original language) – according to the ДСТУ 8302:2015 “Bibliographic references: general statements and compilation rules”;the second one should be in English and in Latin characters (transliteration) – “References” (Annex B). If the reference has digital object identifier DOI, then it should be given at the end of the description, for example doi: 10. 20998/2522-9052.2017.1.09.

Information about the authors must contain:

– full name;

– scientific degree, academic title,

– position, affiliation;

– ORCID ID;

– e-mail.

The authors should:

– ensure that results of research contained in the article constitute independent and original work;

– present the original article, that has not been submitted to other journals and that has not been previously published in other publications;

– provide reliable results of the conducted research;

– recognize the contribution of all persons who influenced the research or helped to define the nature of the scientific work presented in the article;

– in case of using the work fragments by other's or borrowing other author`s materials, the authors are required to provide complete bibliographic references with the obligatory indication of the author and primary source; submitted materials will not be returned to the author.

Independent expert reviewing is carried out for evaluation of articles by specialists that are not the members of the editorial board. An editorial board sends most of the scientific articles for external reviewing by independent peer reviewers.

Conflicts of interests. All the members of independent reviewing and publishing processes must reveal the information about any kinds of relations that can be considered as potential resource of conflicts of interests. This demand is also related to authors and reviewers. Editor-in-chief and editorial board members decide to publish the information revealed by authors, which is related to the potential conflicts only after agreement with the authors.

АЛФАВІТНИЙ ПОКАЖЧИК

Наукове видання

Сучасні інформаційні системи

Advanced Information Systems

Науковий журнал

Том 1, № 1

Відповідальний за випуск *С. Г. Семенов*
Технічний редактор *А. Е. Горюшкіна*
Коректор *Д. С. Гребенюк*
Комп`ютерна верстка *Н. Г. Кучук*

Свідоцтво про державну реєстрацію КВ № 22522-12422Р від 13.01.2017 р.

Формат 60×84/8. Ум.-друк. арк. 11,25. Тираж 120 прим. Зам. 707-17

Адреса редакції: Національний технічний університет "Харківський політехнічний інститут"
Кафедра ОТП, вул. Кирпичова, 2, 61002, м. Харків, Україна, тел.. 707-61-65

Віддруковано з готових оригінал-макетів у друкарні ФОП Петров В.В.
Єдиний державний реєстр юридичних осіб та фізичних осіб-підприємців.
Запис № 24800000000106167 від 08.01.2009.
61144, м. Харків, вул. Гв. Широнінців, 79в, к. 137, тел. **(057) 778-60-34**
e-mail: **bookfabrik@mail.ua**