DIGITAL REALITY SCIENTIFIC AND PRACTICAL FORUM 2021

ІНФОРМАЦІЙНА БЕЗПЕКА ТА ІНФОРМАЦІЙНІ ТЕХНОЛОГІЇ

ПРАЦІ
III МІЖНАРОДНОЇ НАУКОВО-ПРАКТИЧНОЇ КОНФЕРЕНЦІЇ

13 – 19 вересня 2021 року
Харків - Одеса, Україна

MINISTRY OF EDUCATION AND SCIENCE OF UKRAINE

SIMON KUZNETS KHARKIV NATIONAL UNIVERSITY OF ECONOMICS
ODESSA STATE ENVIRONMENTAL UNIVERSITY
ODESSA NATIONAL UNIVERSITY N.A. MECHNIKOV

INTERNATIONAL SCIENTIFIC AND PRACTICAL CONFERENCE "INFORMATION SECURITY AND INFORMATION TECHNOLOGIES"

13-19 September 2021
Kharkiv – Odesa, Ukraine

Conference Proceedings

Kharkiv – Odesa
Simon Kuznets Kharkiv National University of Economics

2021

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ

ХАРКІВСЬКИЙ НАЦІОНАЛЬНИЙ ЕКОНОМІЧНИЙ УНІВЕРСИТЕТ
ІМЕНІ СЕМЕНА КУЗНЕЦЯ
ОДЕСЬКИЙ ДЕРЖАВНИЙ ЕКОЛОГІЧНИЙ УНІВЕРСИТЕТ
ОДЕСЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ ІМЕНІ І.І. МЕЧНИКОВА

МІЖНАРОДНА НАУКОВО-ПРАКТИЧНА КОНФЕРЕНЦІЯ “ІНФОРМАЦІЙНА БЕЗПЕКА ТА ІНФОРМАЦІЙНІ ТЕХНОЛОГІЇ”

13-19 вересня 2021
Харків – Одеса, Україна

Матеріали конференції

Харків – Одеса
Харківський національний економічний університет імені Семена Кузнеця

2021

UDC 681.518.54

I 45

International Scientific And Practical Conference "Information Security And Information Technologies": Conference Proceedings. Kharkiv – Odesa : Simon Kuznets Kharkiv National University of Economics, 2021. 298 p.

ISBN 978-966-676-818-9

Міжнародна науково-практична конференція "Інформаційна безпека та інформаційні технології": матеріали конференції. Харків – Одеса : Харківський національний економічний університет імені Семена Кузнеця, 2021, 298 с.

Збірка містить праці III Міжнародної науково-практичної конференції з інформаційних систем, технологій захисту інформації, використання сучасних інформаційних технологій в управлінні системами за різними галузями народного господарства.

Матеріали публікуються в авторській редакції.

E d i t o r s :

Gunchenko Y., Dr. of Tech.Sc., prof., ONU

Kazakova N., Dr. of Tech.Sc., prof., OSENU

Kuznichenko S., PhD, associated prof., OSENU

Yevseiev S., Dr. of Tech.Sc., prof., KhNEU

Fraze-Frazenko O., PhD, associated prof., OSENU

Редактори

Гунченко Ю.О., д.т.н., проф., ОНУ імені І.І.Мечникова

Казакова Н.Ф., д.т.н., проф., ОДЕКУ

Кузніченко С.Д., к.г.н., доц., ОДЕКУ

Євсеєв С.П., д.т.н., проф., ХНЕУ ім. С. Кузнеця

Фразе-Фразенко О.О., к.т.н., доц., ОДЕКУ

ISBN 978-966-676-818-9

ЗМІСТ

Development Of A Method For Detecting Deviations In The Nature Of Traffic From The Elements Of The Communication Network

O. Laptiev [1], N. Lukova-Chuiko [2], S. Laptiev [3], T. Laptieva [4], V. Savchenko [2], S Yevseiev[3]

[1,2 3 4] *Taras Shevchenko National University of Kyiv, 24 Bogdana Gavrilishina str., Kyiv, 04116,Ukraine,*
[2]*State University of Telecommunications, 7 Solomenska str., Kyiv, 03110, Ukraine*
[3]*Simon Kuznets Kharkiv National University of Economics, 9-A Nauky ave., Kharkiv, 61166,Ukraine,*

Abstract

The article presents an analysis that showed the lack of scientific and methodological apparatus, universal devices or automated software packages to ensure the prompt implementation of traffic analysis and information transfer to automated systems or relevant specialists.

A new developed method is proposed to ensure the prompt implementation of traffic analysis and information about situations that are suspicious and require further detailed analysis by automated systems or relevant specialists.

The developed method allows to carry out operative (real-time) informing of responsible specialists, or transfer of necessary data to the automated complex, about deviation of character of traffic from network elements (separate telephone numbers, number capacities, trunk groups, etc.) which is fixed in primary data. Deviations, the nature of traffic from the elements of network parameters are measured from the usual traffic of the telephone network relative to these elements.

This method has a methodology that takes into account practical recommendations for constant coefficients, calculations. These coefficients are selected by calculation and empirical. This reduces the response of the system using the developed technique to the deviation of the communication parameters.

Keywords

traffic deviation, coefficient, model, telecommunication networks, primary data, communication.

1. Introduction

According to the latest research by the World Association for the Control of Telecommunication Network Violations (CFCA), in 2017 the losses from violations in the telecommunications industry amounted to 74.4-90 billion. This is approximately 57% more than the figure obtained in CFCA studies three years ago [1]. Violations on telecommunications networks are actions of subscribers, telecommunications operators or third parties that are aimed at obtaining telecommunications services at a lower rate or without payment. CFCA experts count about 200 types of violations on telecommunications networks. The most common violations by subscribers are third-party connection to the subscriber line in order to receive free telematics services «900», the implementation of long-term international calls, the organization of unauthorized negotiation points [2, 3]. It is a violation on the part of third parties to use hardware and software to obtain international traffic from the Internet and complete it on a public telecommunications network under the guise of.

local, which leads to interference in the work of communications, substitution of call information. On the part of operators, the most common is the unauthorized, without relevant agreements, termination of incoming long-distance and international traffic to the public network under the

EMAIL: alaptev64@ukr.net (A. 1); lukova@ukr.net (A. 2); salaptiev@gmail.com (A. 3); savitan@ukr.net (A. 4) tetiana1986@ukr.net (A.5); serhii.yevseiev@hneu.net (A. 6)
ORCID: 0000-0002-4194-402X (A. 1); 0000-0003-3224-4061 (A. 2); 0000-0002-7291-1829 (A. 3); 0000-0002-3014-131X (A. 4);0000-0002-5223-9078 (A. 5); 0000-0003-1647-6444 (A. 6)

guise of local. Abuses lead to loss of revenue, subscriber complaints and disruption of telecommunications networks.

The fight against abuse on telecommunications networks is largely based on the analysis of data on services and data contained in payment systems with subscribers and operators [4, 5-7]. Detection of suspicious actions of subscribers and their analysis is the main principle of modern systems of protection against violations (Fraud Management System, FMS). The key criteria for FMS efficiency are speed of operation, flexibility of debugging algorithms that provide incident detection and analysis, and the availability of standardized interfaces for integration with billing platforms and the Customer Relationship Management System (CRM).

1.1 Literature analysis and problem statement

A significant number of publications are devoted to the task of ensuring the prompt implementation of the analysis of communication traffic.

Thus, in [8] considers the analysis of communication traffic with different technical parameters, which unites only one thing - they can only show and (at best) store panoramas of signals in the communication network. They do not solve the problem of communication traffic analysis at all.

The article [9,10] presents the results of the study of SS7 network security. The Signaling System 7 standard is used to exchange service information between network devices in telecommunications networks. At the time this standard was being developed, only fixed line operators had access to the SS7 network, so security was not a priority. Today, the signaling network is no longer as isolated, so an attacker, who in one way or another gained access to it, has the opportunity to exploit security vulnerabilities in order to listen to voice calls, read SMS, steal money from accounts, bypass billing systems or affect the operation of the mobile network. However, no real protection is offered.

In [11-14] the development of mobile communication over the last decade is considered. It is noted that there has been huge progress in the field of wireless communications and especially in the field of 4G cellular networks. However, it will take several years to fully switch to 4G systems, and work has already begun on 5G technologies and their problems. Network security issues are not addressed.

In [15,16] it is said that the effective work of employees is one of the main conditions for the company's success. Uncontrolled access of employees to the Internet can be a serious obstacle to this. Without proper control, an average of up to a third of working time can be spent visiting non-work-related resources. That is why it is important to set up Internet traffic control and use a traffic counter. Protection and proper control over mobile telephone communication has not been properly considered and described [17].

Thus, the most critical for the operator are: violation of the routing of long-distance and international calls, detection of subscriber numbers on outgoing local traffic, activity of operators on incoming local traffic, similar to the operation of gateways to complete incoming long-distance and international traffic, detection of changes in activity of subscriber numbers, which may be evidence of third-party connection to the subscriber line or actions of the subscriber that potentially lead to complaints, non-payment for services and debt write-off. Automated analysis of data on services must be operational.

From the analysis of modern literature it can be concluded that there are almost no universal devices or automated software to ensure the rapid implementation of traffic analysis and information transmission by automated systems or relevant specialists. Therefore, the topic of developing a method designed to ensure the rapid implementation of traffic analysis and information about situations that are suspicious and require further detailed analysis by automated systems or relevant specialists, the method of informing responsible professionals is relevant and very important.

Thus, the development of a method designed to ensure the prompt implementation of traffic analysis and information about situations that are suspicious and require further detailed analysis by automated systems or relevant specialists, the method of informing responsible professionals is very relevant.

2. The material and methods

The operation of violation detection mechanisms is based on the processing of records of network-registered CDR events (Call Detail Record). The anti-fraud system looks for non-

compliance with certain conditions or non-compliance with a given pattern, the characteristics of the subscriber's behavior. When the detection module finds one of the anomalies, it generates a warning message.

Typical conditional checks for FMS systems include:

1. Non-existent numbering (calling party number «A»)
2. Verification of authorization, temporary blocking of number «A»
3. Correspondence to the set template
4. Checking the «black and white lists»
5. Frequently repeated subscriber numbers «A» or «B»
6. Check the connection duration
7. Verification of suspicious calls from «A» subscribers for inclusion in the list of «B» subscribers who most often receive calls from abroad.
8. Changes in the intensity of signal and information load.

The search for a given template is based on traffic patterns that are created for each telecommunications operator. The difference between the existing signal and information traffic and the template indicates a possible violation. An additional use of templates is to compile a profile of the subscriber (telecommunications operator) of the attacker and search for compliance with such a profile among existing subscribers (telecommunications operators). Profiles can contain such characteristics as:

- activity during the day;
- activity in the evening;
- activity at night;
- volumes of outgoing traffic to mobile phones;
- volumes of outgoing traffic to fixed local numbers (including frequently used numbers);
- volumes of outgoing traffic to fixed numbers in other cities (including frequently used numbers);
- volumes of outgoing traffic to fixed numbers in other countries (including frequently used numbers);
- number range of the operator;
- average number of connections over time;
- average amount of traffic over time;
- average connection duration;
- number of unique numbers;
- characteristic directions.

The most critical for the Customer in terms of reducing revenue loss are: violation of the routing of long-distance and international calls, detection of subscriber numbers on outgoing local traffic, activity of operators on incoming local traffic, similar to the operation of gateways to complete incoming long-distance and international traffic in the activity of subscriber numbers, which may be evidence of third-party connection to the subscriber line or actions of the subscriber that potentially lead to complaints, non-payment for services and debt write-off. Automated analysis of data on services must be operational. Thus, at this stage it is important to develop a method designed to analyze traffic and inform about situations that are suspicious and require further detailed analysis by automated systems or relevant specialists.

The main tasks in developing the method will be:

1. Debugging the elements of the telecommunications network. Automatic or with the participation of the operator
2. Providing automatic analysis, data classification, search for deviations of behavior of elements of a telecommunication network from a usual profile.
3. Creation of an detection algorithm based on the features of violations that create a dynamic over time impact on the network, causing anomalous phenomena.
4. Development of a graphical display of changes in quantitative characteristics over a period of time.
5. Estimation of conformity of parameters of anomalies (non-existent number, big duration of a call, etc.) to the values characteristic of this type.
6. Assessment of anomalies on the degree of probability of violation to determine the priority of response.
7. Development of information on the detection of deviations and events.
8. Development of a user-friendly operator interface.

Block detection scheme, which is based on the characteristics of violations, it is possible to present in Figure 1.

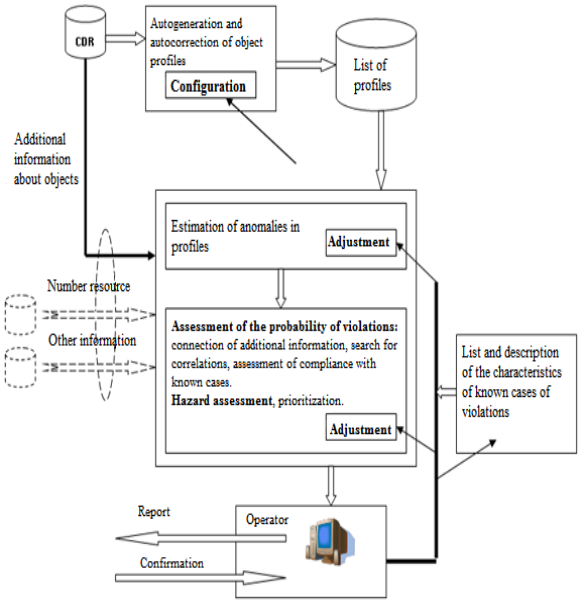


Figure.1: Block diagram of detection of estimates of profile anomalies for detection of violations

To assess the quantitative characteristics of the object and the dynamics of changes over time, it is proposed to use the method of exponential averages with different smoothing coefficients:

$$Q_t = (1-k)Q_{t-\Delta t} + kq_{\Delta t}, \qquad (1)$$

where:

Q is the exponential average value;

q - new dimension;

k is the smoothing coefficient;

Δt - interval between measurements;

The formula uses a constant interval of measurements. The profile correction for each call is complex, because in this case the smoothing factor is a complex exponential function of the measurement interval. However, the features of the parameters allow the use of simpler formulas.

The optimal number of average values and values of smoothing coefficients for each parameter can be obtained experimentally. To begin with, it is assumed to use for each parameter three values with coefficients k = 0.3; 0.05 and 0.005 with a focus on the daily interval of measurements.

For all the parameters and coefficients used below, the values that can be used in the development are

presented, but when obtaining practical results, these values can be changed by the operator. In addition, the use of some profile parameters and anomaly calculations may be impossible or impractical, and others may need to be added.

Traffic will be estimated as the average daily number of seconds of connections:

$$Q_t = (1-k\frac{\Delta t}{86400})Q_{t-\Delta t} + kT, \quad \text{if } \Delta t < 86400 \qquad (2)$$

And

$$Q_t = (1-k)Q_{t-\Delta t} + kT\frac{86400}{\Delta t}, \quad \text{if } \Delta t \geq 86400 \qquad (3)$$

where:

T is the duration of connections in seconds;

Δt - time between the ends (beginnings) of the previous and new call in seconds.

The following types of traffic are provided for analysis:

- local outgoing
- long distance outgoing
- international outgoing
- input

We suggest estimating the intensity of the call flow as the average daily number of connection attempts:

$$Q_t = (1-k\frac{\Delta t}{86400})Q_{t-\Delta t} + kT, \ \Delta t < 86400 \qquad (4)$$

And

$$Q_t = (1-k)Q_{t-\Delta t} + kT\frac{86400}{\Delta t}, \text{if } \Delta t \geq 86400 \qquad (5)$$

where:

T is the duration of connections in seconds;

Δt - time by the ends (beginnings) of the previous and new call in seconds.

It is estimated the intensity of the flow of calls:

- incoming
- outgoing
- effective.

The distribution of traffic by time type is estimated as the average daily number of seconds of connections for working time.

- working hours - 1st-5th day of the week from 8-30 to 17-30;
- non-working hours - 1st-5th day of the week from 0-00 to 8-30 and from 17-30 to 24-00;
- 6th-7th day of the week from 0-00 to 24-00.

The distribution of traffic by time of day will be estimated as the average daily number of seconds of connections during the day.

- daytime from 7-00 to 24-00;
- night time from 0-00 to 7-00.

Signal traffic is estimated as the average number of bytes of signal information per call:

$$Q_t = (1-k)Q_{t-\Delta t} + kB, \quad (6)$$

where:

B is the number of bytes of signal information in the call.

The instability of stable network parameters of the object is estimated by their change from call to call. One characteristic can be used for all parameters.

For each call:

$$Q_t = LQ_{n-1} + \sum h_i, \quad (7)$$

where:

hi - increment levels for parameters whose values differ in previous and subsequent calls;

L is a factor that takes into account outdated information L = 0.9.

Other parameter values (if present in the CDR):

- access (ISDN, non ISDN) h = 10;
- category of the subscriber calling h = 5;
- the presence or absence of signaling interaction when establishing a connection h = 8;
- invalid localization of the calling subscriber (correspondence of the address to the admissible template) h = 200;
- invalid subscriber category that causes h = 100.

It is necessary to provide for the possibility of expanding and changing similar parameters in the future, as well as the use of different characteristics for different groups of parameters.

Additional coefficients:

- is a constant additional factor that allows you to reduce or increase the sensitivity to anomalies in the assessment. Can only be changed by the operator;
- is a temporary additional factor that reduces or increases the sensitivity to anomalies in the assessment. It can be changed only by the operator, but then automatically strive for a normal value.

After each call, a temporary additional factor is determined by:

$$K2_t = (1-k)K2_{t-\Delta t} + kK2_{norm} \quad (8)$$

where:

Δt - time between the ends (beginnings) of the previous and next calls in seconds;

K2norm is the normal value;

k is the smoothing coefficient, k = 0,05.

Normal values for additional coefficients: K1norm = 100, K2norm = 100.

We will evaluate the anomalous behavior of the object by the following method:

The anomaly in the behavior of the object is assessed by the overall rating, as the average of the identified anomaly, taking into account additional coefficients.

$$A_{pr} = \frac{(\sum A) * K1 * K2}{(\sum C) * K1_{norm} * K2_{norm}}. \quad (9)$$

K1 - constant additional coefficient;

K2 - temporary additional coefficient.

When creating an object, the field T starts the time of the beginning of the observation, in the field K2 - a reduced value to stabilize the characteristics, in other fields - the default values.

To determine the anomalies, use the following method:

When determining anomalies, the coefficients and parameters common to all objects are used:

C - weighting factor, taking into account the impact of each anomaly on the overall rating;

m is a parameter that compensates for the high uncertainty in the profiles of low-traffic objects.

Traffic (A1, A2, A3, A4):

$$A(0.3) = C(0.3) * \frac{|Q(0.3) - Q(0.05)}{Q(0.05) + m}, \quad (10)$$

$$A(0.05) = C(0.05) \frac{Q(0.05) - Q(0.005)}{Q(0.05) + m}.$$

To determine the anomalies you need to set the traffic parameters, set the common for all objects coefficients and parameters of table 1 and table 2:

Table 1

Given the weights of anomalies

$C_1(0.3)$	$C_1(0.05)$	$C_2(0.3)$	$C_2(0.05)$
1	3	20	60

Table 2.

The specified parameters for determining anomalies

m_1	m_2	m_3	m_4
200	100	80	200

The connection duration will be calculated as follows:

Outgoing traffic:

$$Q_{tout} = Q_1 + Q_2 + Q_3; m_{tout} = m_1 + m_2 + m_3 \quad (11)$$

Outgoing calls

$$A5(0.3) = C5(0.3) * \left[\left| \frac{(Q_{Tout}(0.3) + m_{Tout}) * (Q5(0.05) + m_5)}{(Q5(0.3) + m_5) * (Q_{Tout}(0.05) + m_{Tout})} - 1 \right| \right] \quad (12)$$

$$A5(0.05) = C5(0.05) * \left[\left| \frac{(Q_{Tout}(0.05) + m_{Tout}) * (Q5(0.005) + m_5)}{(Q5(0.05) + m_5) * (Q_{Tout}(0.005) + m_{Tout})} - 1 \right| \right] \quad (13)$$

Incoming calls

$$A6(0.3) = C6(0.3) * \left[\left| \frac{(Q4(0.3) + m_4) * (Q6(0.05) + m_6)}{(Q6(0.3) + m_6) * (Q4(0.05) + m_4)} - 1 \right| \right] \quad (14)$$

$$A6(0.05) = C6(0.05) * \left[\left| \frac{(Q4(0.05) + m_4) * (Q6(0.005) + m_6)}{(Q6(0.05) + m_6) * (Q_4(0.005) + m_4)} - 1 \right| \right] \quad (15)$$

To determine the duration of the connection, you need to specify the traffic parameters, according to the developed method, the coefficients common to all objects and the parameters are given in table 3:

Table 3

Connection duration settings are set

C_5 (0.3)	C_5 (0.05)	C_6 (0.3)	C_6 (0.05)	m_5 (0.3)	m_6 (0.05)
3	10	3	10	5	5

According to the developed method, we will determine the effectiveness:

Total calls:

$$A7(0.3) = C7(0.3) * \left[\left| \frac{Q7(0.3) + 0.45 * m_{Nall}}{Q_{Nall}(0.3) + m_{Nall}} - \frac{Q7(0.05) + 0.45 * m_{Nall}}{Q_{Nall}(0.05) + m_{Nall}} \right| \right] \quad (16)$$

$$A7(0.05) = C7(0.05) * \left[\left| \frac{Q7(0.05) + 0.45 * m_{Nall}}{Q_{Nall}(0.05) + m_{Nall}} - \frac{Q7(0.005) + 0.45 * m_{Nall}}{Q_{Nall}(0.005) + m_{Nall}} \right| \right] \quad (17)$$

Where C7 (0.3) = 3 and C10 (0.05) = 10

The section by time type will be performed as follows:

Total traffic:

$$A8(0.3) = C8(0.3) * \left[\left| \frac{Q_{Tall}(0.3) - k_1(d,h) * Q8(0.3)}{Q_{Tall}(0.3) + m_{Tall}} - \frac{Q_{Tall}(0.05) - k_2(d) * Q8(0.05)}{Q_{Tall}(0.05) + m_{Tall}} \right| \right] \quad (18)$$

k1(d, h), k2(d) - coefficients that take into account the error of exponential averaging (d - day of the week, h - hour);

The coefficients that take into account the error of exponential averaging are given in table 4 and table 5.

Table 4

Error coefficients of exponential averaging d=1,2,3

h	$k_1(d,h)$	h	$k_1(d,h)$	h	$k_1(d,h)$
0	1.470	0	1.151	0	0.992
1	1.489	1	1.165	1	1.004
2	1.507	2	1.180	2	1.017
3	1.527	3	1.195	3	1.030
4	1.546	4	1.210	4	1.043
5	1.565	5	1.226	5	1.056
6	1.585	6	1.241	6	1.069
7	1.605	7	1.257	7	1.083
8	1.626	8	1.273	8	1.097
9	1.529	9	1.216	9	1.056
10	1.444	10	1.164	10	1.018
11	1.369	11	1.117	11	0.984
12	1.302	12	1.075	12	0.952
13	1.242	13	1.036	13	0.923
14	1.188	14	1.100	14	0.895
15	1.139	15	0967	15	0.870

Table 5

Error coefficients of exponential averaging

d	1	2	3	4
$k_2(d)$	1.031	1.008	0.988	0.970

$$A8(0.05) = C8(0.05) * \left[\left| \frac{Q_{Tall}(0.05) - k_2(d) * Q8(0.05)}{Q_{Tall}(0.05) + m_{Tall}} - \frac{Q_{Tall}(0.005) - Q8(0.005)}{Q_{Tall}(0.005) + m_{Tall}} \right| \right] \quad (19)$$

where C8(0.3)=5 and C8(0.05)=15

The distribution of time of day we calculate by the expression:

$$A9(0.3) = C9(0.3) * \left[\left| \frac{Q_{Tall}(0.3) - k_3(h) * Q9(0.3)}{Q_{Tall}(0.3) + m_{Tall}} - \frac{Q_{Tall}(0.05) - Q9(0.05)}{Q_{Tall}(0.05) + m_{Tall}} \right| \right] \quad (20)$$

$$A9(0.05) = C9(0.05) * \left[\left| \frac{Q_{Tall}(0.05) - Q9(0.05)}{Q_{Tall}(0.05) + m_{Tall}} - \frac{Q_{Tall}(0.05) - Q9(0.005)}{Q_{Tall}(0.005) + m_{Tall}} \right| \right] \quad (21)$$

where:

k3(h) - coefficient that takes into account the error of exponential averaging (h - hour);

Table 6

The error rate of exponential averaging

h	0	1	2	3
$k_3(h)$	0.9709	0.9832	0.9956	1.0082

h	8	9	10	11
$k_3(h)$	1.0347	1.0288	1.0230	1.0173

h	14	15	16	17
$k_3(h)$	1.0012	0.9960	0.9910	0.9861

For the developed technique C9 (0.3) = 8; C9 (0.05) = 24.

We will define signal traffic by expressions:

$$A10(0.3) = C10(0.3) * \left[\left| \frac{Q10(0.3)}{Q_{Nall}(0.3) + m_{Nall}} - \frac{Q10(0.05)}{Q_{Nall}(0.05) + m_{Nall}} \right| \right] \quad (22)$$

$$A10(0.05) = C10(0.05) * \left[\left| \frac{Q10(0.05)}{Q_{Nall}(0.05) + m_{Nall}} - \frac{Q10(0.005)}{Q_{Nall}(0.005) + m_{Nall}} \right| \right] \quad (23)$$

Coefficient C10 (0.3) = 20, coefficient C10 (0.05) = 60

The stability of the network parameter will be determined by the expression

$$A_{11} = W \quad (24)$$

Not all objects can be further processed, but only objects with the highest overall anomaly rating. It is enough to process about 1% of the total.

The assessment of the probability of violation, in contrast to existing methods, will be determined taking into account additional factors. In addition to the high level of anomaly of the object profile, additional factors that increase the possibility of detecting fraud in the assessment are:

- correlation of events of anomalous objects - coincidence of unique addresses in records of calls of objects for the last time (2-3 days);

- compliance of the profile of the object of the known case of violation, the coincidence of specific for this known case information about the call (direction, addressing) recently;

- inconsistency of the object profile with the typical subscriber accounting profile. (It is possible only if there is access to the subscriber accounting database, not necessarily in the early stages of development, but it is necessary to provide for such a possibility in the future).

Determining the probability of violation

$$P = MAX(\frac{A}{A+a} MAX(P_{known}) P_{subbase}) \quad (25)$$

where:

$\frac{A}{A+a}$ - the probability of violation, determined by the anomaly of behavior;

a - anomaly at 50% probability. The value of a can be obtained experimentally.

First you can use: a = 20;

$$A = A_{pr} + \sum A_{cor.pr.} \quad (26)$$

where:

Acor.pr - anomaly of the object, which has a correlation in the calls (when checking it is necessary to exclude coincidence at popular addresses: special services, serial modem pools, etc.), if the correlation is not defined - *Acor.pr=0*;

Psubbase - the probability of fraud, which is estimated by the inconsistency of the object profile to the typical profile in accordance with the subscriber accounting.

Pknown - the probability of a known type of violation (determined for each known type). The method of determining the probability of a known type of violation can also be based on the correspondence of characteristic anomalies in the profile of the observed object and the profile of the violating object at the time of detection, as well as correlations in calls by addresses

or prefixes. More precisely, the method can be determined only after the accumulation of a sufficient number of experimental results.

The assessment of the degree of risk of fraud according to the developed methodology will be calculated as follows.

Assessment of the degree of danger is necessary for cases that require priority intervention. They can be considered as the effect of the probability of violation on loss or unearned income:

$$\Delta Q(0.3) = | Q(0.3) - Q(0.05) | \quad (27)$$

$$\Delta Q(0.05) = | Q(0.05) - Q(0.005) | \quad (28)$$

$$D = P * \begin{pmatrix} \Delta Q1(0.3) + k_2 * \Delta Q2(0.3) + k_3 * \Delta Q3(0.3) + \\ + L * (\Delta Q1(0.05) + k_2 * \Delta Q2(0.05) \\ + k_3 * \Delta Q3(0.05)) \end{pmatrix} \quad (29)$$

where k_2, k_3 – coefficients that take into account the average difference in tariffs;

They will take the values k_2 = 15, k_3 =250, L =3.

Recommendations for the practical application of the developed methodology.

The peculiarity of the operation and the distinction of the developed methodology will be the following:

1. Feature when creating profiles of objects:

- For each group of connecting lines and for each direction of the channel, describes the list of valid addresses of the source party, the list of uncontrolled addresses of the source party, lists of objects that have more than one address in the corresponding list of addresses.

- If a record of object profile information is not found during call processing, it must be generated automatically.

2. Specific profile formation:

If there is a loss in the System of call information for any period, to prevent failures in the formation of information about the profiles of objects, you must check all objects again, using zero values of traffic at the beginning of the period and restore information in profiles at the end.

For ease of use, the user interfaces and methods of working with them must be identical to the System as a whole. But in addition you need to consider the following:

1. The subsystem must contain means of actively informing users about events that need attention, by generating screen messages in the client part of the system, including at the start of the client part, if the event occurred and was not covered before.

2. Provide the ability to graphically display the characteristics of the profile of objects.

3. Provide for the possibility of organizing additional checks, with a slight change in the rules used in the analysis using the rule editor.

Areas of further research.

Further research should be aimed at improving the software for automated software, in order to enable automated recognition and operational implementation of traffic analysis for further detailed analysis of automated systems.

3. Conclusions

The analysis showed the absence of scientific and methodological apparatus, universal devices or automated software packages to ensure the rapid implementation of traffic analysis and information transfer to automated systems or relevant specialists. Therefore, a method has been developed to ensure the prompt implementation of traffic analysis and information about situations that are suspicious and require further detailed analysis by automated systems or relevant specialists.

The developed method allows to carry out operative (real-time) informing of responsible specialists, or transfer of necessary data to the automated complex, about deviation of character of traffic from network elements (separate telephone numbers, number capacities, trunk groups, etc.) which is fixed in primary data. Deviations, the nature of traffic from the elements of network parameters are measured from the usual traffic of the telephone network relative to these elements.

The given technique takes into account practical recommendations concerning constant coefficients, calculations. These coefficients are selected by calculation and empirical. This reduces the response of the System using the developed method to the deviation of the communication parameters by 9% compared to existing methods. This is a perfectly acceptable result.

4. References

[1] Serhii Yevseiev, Roman Korolyov, Andrii Tkachov, Oleksandr Laptiev, Ivan Opirskyy, Olha Soloviova. Modification of the algorithm (OFM) S-box, which provides increasing crypto resistance in the post-quantum period. International Journal of Advanced Trends in Computer Science and Engineering (IJATCSE) Volume 9. No. 5, September-Oktober 2020, pp 8725-8729

[2] Valentyn Sobchuk, Volodymyr Pichkur, Oleg Barabash, Oleksandr Laptiev, Kovalchuk Igor, Amina Zidan. Algorithm of control of functionally stable manufacturing processes of enterprises. 2020 IEEE 2nd International Conference on Advanced Trends in

Information Theory (IEEE ATIT 2020) Conference Proceedings Kyiv, Ukraine, November 25-27. pp.206 –211.

[3] Vitalii Savchenko, Oleksandr Laptiev, Oleksandr Kolos, Rostyslav Lisnevskyi, Viktoriia Ivannikova, Ivan Ablazov. Hidden Transmitter Localization Accuracy Model Based on Multi-Position Range Measurement. 2020 IEEE 2nd International Conference on Advanced Trends in Information Theory (IEEE ATIT 2020) Conference Proceedings Kyiv, Ukraine, November 25-27. pp.246 –251

[4] Serhii Yevseiev, Oleksandr Laptiev, Sergii Lazarenko, Anna Korchenko, Iryna Manzhul. Modeling the protection of personal data from trust and the amount of information on social networks. Number 1 (2021), «EUREKA: Physics and Engineering» pp.24–31 Milov O., Yevseiev S. Milevskyi S. Ivanchenko Y., Nesterov O., Puchkov O., Yarovyi A., Salii A., , Tiurin V., Timochko O. Development the model of the antagonistic agent's behavior under a cyber-conflict. Eastern European Journal of Advanced Technologies. Kharkiv. 2019. 4/9 (100). pp. 6–19

[5] S. Korotin, Y. Kravchenko, O. Starkova, K. Herasymenko, R. Mykolaichuk, "Analytical determination of the parameters of the self-tuning circuit of the traffic control system on the limit of vibrational stability", International Scientific-Practical Conference Problems of Infocommunications Science and Technology, PIC S&T`2019 – Proceedings, pp. 471–476.

[6] Y. Kravchenko, O. Leshchenko, N. Dakhno, O. Trush, O. Makhovych "Evaluating the effectiveness of cloud services", IEEE International Conference on Advanced Trends in Information Theory, ATIT`2019 – Proceedings, pp.120–124.

[7] A.M.Samoilenko, V.G.Samoilenko, V.V.Sobchuk. On periodic solutions of the equation of a nonlinear oscillator with pulse influence Ukrainian Mathematical Journal, 1999 (51), 6 Springer New York – P. 926-933

[8] V. Sobchuk et al .Approximate Homogenized Synthesis for Distributed Optimal Control Problem with Superposition Type Cost Functional. Statistics Opt. Inform. Comput., Vol. 6, June 2018, pp 233–239.

[9] O. Barabash, N. Dakhno, H. Shevchenko, V. Sobchuk. Integro-Differential Models of Decision Support Systems for Controlling Unmanned Aerial Vehicles on the Basis of Modified Gradient Method. IEEE 5th International Conference on Methods and Systems of Navigation and Motion Control (MSNMC) – Ukraine, Kyiv, 16 October 2018. pp. 94 – 97.

[10] S. Toliupa, N. Lukova-Chuiko, O. Oksiuk. Choice of Reasonable Variant of Signal and Code Constructions for Multirays Radio Channels. Second International Scientific-Practical Conference Problems of Infocommunications. Science and Technology. IEEE PIC S&T 2015. pp. 269 – 271.

[11] N.Lukova-Chuiko, I. Ruban, V. Martovytskyi Designing a monitoring model for cluster supercomputers. Eastern-European Journal of Enterprise Technologies.- № 6(2) . 2016. P.32-37.

[12] N. Lukova-Chuiko, I. Ruban, V. Martovytskyi. Approach to Classifying the State of a Network Based on Statistical Parameters for Detecting Anomalies in the Information Structure of a Computing System.Cybernetics and Systems AnalysisV. 54. № 2. pp. 142 – 150. 2018.

[13] N.Lukova-Chuiko, I. Ruban, H. Khudov, O. Makoveichuk, I. Khizhnyak. Method For Determining Elements of Urban Infrastructure Objects Based On The Results From Air Monitoring.Eastern-European Journal of Enterprise Technologies. – № 4/9 (100). – 2019. – P. 52 – 61.

[14] N. Lukova-Chuiko, I Ruban, V. Martovytskyi, A. Kovalenko. Identification in Informative Systems on the Basis of Users' Behaviour. 2019 IEEE 8th International Conference on Advanced Optoelectronics and Lasers (CAOL), Sozopol. Bulgaria. pp. 574-577. 2019.

[15] N. Lukova-Chuiko, V. Saiko, V. Nakonechnyi, T. Narytnyk, M. Brailovskyi. Terahertz Range Interconnecting Line For LEO-System. 2020 IEEE 15th International Conference on Advanced Trends in Radioelectronics, Telecommunications and Computer Engineering (TCSET), Lviv-Slavske, Ukraine, pp. 425-429. 2020.

[16] Oleksandr Laptiev, Vitalii Savchenko, Andrii Pravdyvyi, Ivan Ablazov, Rostyslav Lisnevskyi, Oleksandr Kolos, Viktor Hudyma. Method of Detecting Radio Signals using Means of Covert by Obtaining Information on the basis of Random Signals Model. International Journal of Communication Networks and Information Security (IJCNIS), Vol. 13, No. 1, 2021. pp.48-54.

Analysis of Evil Twin Attack in Wireless Network

Roman Korolkov [1], Serhii Kutsak [2]

[1, 2] *National University "Zaporizhzhia Polytechnic", Department of information security, Zhukovsky St., 64, Zaporizhzhia, 69063, UKRAINE*

Abstract

In this paper, the concept was considered and the practical implementation of one of the security threats to Wi-Fi networks - the Evil Twin attack. It is shown that the implementation of the attack is possible due to the allowed by the 802.11 standard location of several access points with the same service set identifier (SSID) and MAC address in the same area. With the help of several tools that are freely available, it is shown what steps an intruder performs to attack. During the experiment, abnormalities in the behavior of beacon frames at the time of the Evil Twin attack were detected. Based on the results obtained, it can be concluded that the monitoring of beacon frames can be used to develop systems for detecting and preventing intrusions into the WLAN.

Keywords

attack, evil twin, received signal strength, spoofing, rogue access point, wireless network

1. Introduction

With the widespread use of Wi-Fi technology, the challenge is to ensure a high level of security for such networks. Wireless networks use radio broadcasting and are therefore extremely vulnerable to possible attacks and unauthorized access. The disadvantages of the IEEE 802.11 protocols encourage criminals to commit cybercrime. Among all the threats to WLAN security, one of the most serious is the Rogue Access Point (RAP). One of the attacks that uses RAP is the Evil Twin attack, which exploits the same SSID and BSSID (basic SSID) as the nearby legitimate access point (LAP). Evil Twin access point is used for espionage and attacks. After connecting an unsuspecting client to the Evil Twin access point, an attacker can eavesdrop on his messages, receive confidential information, redirect to malicious websites, etc.

Therefore, the investigation of attacks using rogue access points, especially Evil Twin, is an urgent task and is necessary for further improvement of the protection methods against unauthorized interference in wireless networks.

2. Evil Twin Attack

The paper considers a scenario in which an unauthorized access point and a legitimate access point are together in the same area and have the same SSID and BSSID because the attacker installs a Evil Twin rogue access point by cloning the MAC address and SSID of the existing LAP.

The Evil Twin attack can be performed in two ways.

1. The attacker launches the Evil Twin and increases the signal strength of the access point (AP). Thus, whenever a client tries to communicate with the LAP, he will connect to the RAP.
2. An attacker targets clients that are already connected to the LAP. In a situation when Protected Management Frames (PMF) are not used, the attacker forcibly disconnects the client from the LAP, performing a deauthentication attack [1], [2] and waits for the client to reconnect, but by now to RAP, as shown in Fig. 1.

EMAIL: romankor@zntu.edu.ua (A. 1); kuzak@ukr.net (A. 2)
ORCID: 0000-0001-5501-4600 (A. 1); 0000-0001-5238-8957 (A. 2)

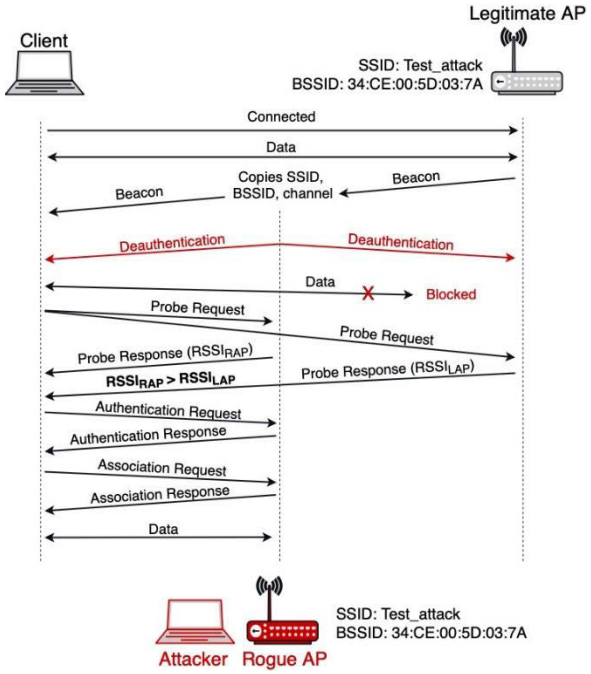


Figure 1: Evil Twin attack scheme

The attack process consists of the following stages.

1. An attacker carries out a reconnaissance attack. At this stage, the attacker puts the network adapter in monitoring mode and scans the air in search of information about AP to be forged (SSID, MAC address, channel).
2. An attacker configures RAP with the same SSID and BSSID as the LAP by performing a spoofing attack.
3. An attacker increases the power level of the network adapter transmitter so that the RAP signal level exceeds the LAP signal level at the point of reception by the client.
4. An attacker launches an Evil Twin access point and sends beacon frames. The procedure for setting up a software-implemented RAP is as follows:

- installation of DHCP-server (the work uses ISC-DHCP-server with open-source code [3]) and configuration of the configuration file /etc/dhcp/dhcpd.conf DHCP-server. The file indicates the network parameters (range of IP addresses, lease time, subnet mask, DNS server) that will be provided to clients;
- activation of RAP Evil Twin with similar SSID, BSSID, channel of the legitimate access point (used the program airbase-ng package Aircrack-ng);
- setting up a computer to work as a router to redirect the victim's traffic to a network card with Internet access. For this purpose, the ifconfig and iptables programs built into the Linux kernel were used.

5. In the event that it is necessary to forcibly disconnect clients from the LAP, the attacker performs a deauthentication attack. After a successful attack, the attacker expects the client to connect to RAP.
6. The client device broadcasts a Probe-request (AP connection request), attempting to reconnect to the same SSID immediately to ensure a seamless connection.
7. Each of the access points that are located in the client's field of vision and satisfies the parameters in the Probe request frame, sends a Probe-response frame containing the synchronizing information. Because the Evil Twin has a higher signal level, the client connects to a rogue access point.
8. Transition to the authentication and association phase to establish a connection and restore Internet access.
9. Data transfer via Evil Twin access point.

Through this process, the attacker can access the data that the victim transmits to the network.

An experiment was performed to confirm the concept of the attack, as a result of which the client was connected to the "Evil Twin". To carry out and implement the “Evil Twin” attack, dual-band Wi-Fi adapters Alfa AWUS036ACH of 802.11ac standard on the Realtek RTL8812AU chipset, Linux operating system, software package for auditing wireless networks Aircrack-ng [4], and Wireshark [5] were used to capture and analyze network traffic.

3. Analysis of results

During the attack, beacon frames had been monitored. It is known that the access point periodically sends beacon frames to indicate its presence in the network. Beacon frames are control frames and are transmitted in unencrypted form, so the attacker easily forges them, posing as LAP [6]. The interval, with which the beacon frames are sent, is determined by the access point, declared to the other nodes in the frame field "beacon interval" and expressed in special Time Units (TU), TU = 1024 μs. In the general case, the typical value of the beacon frame interval is 100TU (102.4 ms).

Monitoring was performed using a network analyzer Wireshark, setting up filtering by MAC-address of the AP and a certain type of frames (in

this case, beacon frames). The observation period was 100ms.

Before the attack, one frame was observed every 100ms, and after the launch of the Evil Twin attack, the number of beacon frames coming from the same BSSID has increased to two. However, it should be noted that sometimes the access point may miss the transmission of the beacon frame if the network is congested or tasks with a higher priority are performed. Simultaneously, the RSSI values of the beacon frames (from the radiotap header) were registered. There were significant fluctuations in RSSI during the attack. Accordingly, it is possible to distinguish two groups of beacon frames with the same SSID and BSSID, which differ significantly in level (in this experiment, one at -49dBm, the other at -28dBm).

4. Conclusion

Practical experiments have shown that Wi-Fi networks have a fundamental security problem - it is allowed by the 802.11 standard to have multiple access points with the same SSID and BSSID in the same area, that is the reason for the violation of the integrity of the network and the possible interception of information as a result of the Evil Twin attack.

The obtained experimental results indicate anomalies of beacon frames during the attack. First, the number of beacon frames from the attacked access point is growing. Second, when there is no attack, the RSSI values from the LAP show small fluctuations. But, during the attack, substantial fluctuations of the RSSI values of the beacon frames for the same MAC address were registered. This is due to either different physical locations of RAP and LAP, or an increase in the power level of the transmitter by an attacker.

Therefore, further research and efforts should be focused on improving existing and developing new methods of RAP detection, in particular Evil Twin, which will improve protection against unauthorized intervention in wireless networks.

5. References

[1] Korolkov R.Y., Kutsak S.V. The features of a deauthentication attack implementation in networks 802.11. Ukrainian Information Security Research Journal, vol. 21, no. 3, pp. 175–181. https://doi.org/10.18372/2410-7840.21.13953

[2] Kristiyanto, Y., Ernastuti Ernastuti (2020). Analysis of Deauthentication Attack on IEEE 802.11 Connectivity Based on IoT Technology Using External Penetration Test. CommIT (Communication and Information Technology) Journal, 14(1), 45–51. https://doi.org/10.21512/commit.v14i1.6337

[3] ISC DHCP SERVER [Online]. – Available: http://www.isc.org/downloads/dhcp/ [Accessed: April 5, 2021].

[4] Aircrack-ng. [Online]. – Available: https://www.aircrack-ng.org/doku.php?id=Main [Accessed: April 5, 2021].

[5] Wireshark. [Online]. – Available: http://www.wireshark.org [Accessed: April 5, 2021].

[6] P. Shrivastava, M. S. Jamal and K. Kataoka EvilScout: Detection and Mitigation of Evil Twin Attack in SDN Enabled WiFi, in IEEE Transactions on Network and Service Management, vol. 17, no. 1, pp. 89-102, March 2020, https://doi.org/10.1109/TNSM.2020.2972774

Using the Sum of Real Type Functions to Encrypt Messages

Viktor V. Avramenko[1], Mykyta O. Bondarenko[2]

[1,2] *Sumy State University, Rymskogo-Korsakova st. 2., Sumy, 40007, Ukraine*

Abstract

This paper presents a symmetric key cryptosystem using the sum of real type functions which allows to increase the cryptographic strength. Both transmitter and receiver choose Key Functions with the same argument, the interval for setting the argument, and the step for changing it. The symbol of the transmitted message is encrypted in an array where each element is the sum of Key Functions with random amplitudes. This sum includes those Key Functions for which the corresponding bit is one. Decryption uses disproportion functions. The system is suitable for encrypting both discrete and continuous messages.

Keywords

Cryptosystems, disproportion functions, function of real variable, key functions, encryption, decryption, text messages

1. Introduction

Widely used cryptosystems are based on the set of integers. They implement symmetric and asymmetric encryption algorithms. In symmetric systems, the same key is used for both encryption and decryption. The most famous symmetric systems are AES [1] and GOST 28147-89 [2, 3]. To hack such a system, an enumeration of possible keys is required. The brute-force complexity is $O(2^k)$, where k is the key length in bits. For symmetric systems, if the communication channel is open, there is a problem of secure key transmission. This problem does not exist for asymmetric open key systems. In these systems, the most widely used algorithms are RSA and El-Gamal [4, 5]. The RSA algorithm is based on the computational complexity of the integer factorization problem. El-Gamal's algorithm is based on the difficulty of computing the discrete logarithm, especially over a group of points of an elliptic curve [6]. For breaking asymmetric cryptosystems, there are cryptanalysis methods which are faster than full search. This circumstance makes it necessary to use longer keys compared to keys in symmetric systems, but it's not promising due to the intensive development of the quantum computers [7], which will significantly affect the cryptographic strength of existing cryptosystems [8]. The ordinal brute force has complexity $O(2^k)$, meanwhile Grover's quantum algorithm [9] reduces it to $O(2^{k/2})$ [9].

Implementing quantum algorithms will also reduce the robustness of asymmetric systems. The RSA system uses the super polynomial computational complexity of the factorization of natural numbers. At the same time, there is a quantum algorithm whose complexity is polynomial $O(n^3)$ [10]. It means the cryptographic strength of asymmetric systems can be reduced as a result of the implementation of Shor's quantum algorithm for computing the discrete logarithm. In [11], Shor's algorithm is given for the group of points of an elliptic curve over the field GF(p) with complexity $O(n^3)$. Implementing quantum algorithms will also reduce the robustness of asymmetric systems. A method for increasing the crypto resistance of the system under these conditions is proposed in [12]. Along with the search for ways to hack cryptosystems, methods for detecting signals of means of secretly obtaining information are also being developed [13].

The above analysis shows that one should look for other ways to create cryptosystems. In particular, to complicate the selection of keys using the simple enumeration method, one should switch from using integers to real ones. It is known [14] the set of real numbers has a higher cardinality compared to the set of natural numbers, so one can expect the cryptographic

EMAIL: vv.avramenko@cs.sumdu.edu.ua (A.1); nikbond97@gmail.com (A. 2)
ORCID: 0000-0002-6317-6711 (A. 1); 0000-0002-8849-7378 (A. 2)

strength of a cryptosystem based on real numbers will be higher. The possibilities of creating cryptosystems using one or more functions of a real variable as keys are considered in [15-18].

So, in [15], characters from the ASCII code table are encrypted by the sum of 10 functions of a real variable, which are keys. Each key-function is preceded by a coefficient, which, depending on the character being encrypted, is equal to zero or one. The amplitudes of these functions are random for each new symbol. The resulting sum of the values of the functions is transmitted over the communication channel. On the receiving side, fragments of key functions are recognized, which are represented in the received encrypted signal. This allows you to decrypt the symbol transmitted at the current time using the disproportion functions [19-22].

In [16, 17], a variant is proposed when symbols for transferring binary codes are encoded with the help of three key functions of a real variable. "1", "0", "space", "new line" are encoded. Any other character is recognized as a new line. For unauthorized access to the intercepted message, you need to select the type and parameters of the key functions.

In [15-17], the disproportion functions over the first-order derivative were used. In this case, it is necessary to apply numerical methods for calculating the current values of the first derivatives. The need for these calculations led to the fact that the ciphertext significantly exceeded the length of the encrypted message.

A completely different encryption principle was proposed in [18]. One function of the real variable is used as the key. The disproportion function of the numerical representation of the encrypted process is calculated with respect to the key function. The obtained values of the disproportion function are an encrypted message and are transmitted over the communication channel. To avoid calculating the derivatives, the integral disproportions of the first order is used [23].

The cryptosystems [15-18] in the process of computer modeling have shown high cryptographic strength when trying to guess the parameters of keys functions, even if their form is known. To further complicate the work of cryptanalysts, the task is to develop a cryptosystem that could combine the advantages of the systems considered in [15-17] and the system [18]. So, it's necessary to develop the algorithms for encryption and decryption of analog and discrete messages, using several functions of a real variable as keys without the necessity to calculate derivatives.

2. Mathematical formulation of the problem

The message that is encrypted is a sequence of T numeric character codes from the ASCII table (or numeric values of the pixel brightness components in the case of a graphic image transmission). Each of them is encrypted using one-dimensional arrays of length N values. These arrays are obtained using one and the same step h of changing the argument of m Key Functions of the real variable. In this case, the value y(j, i) of the matrix y(T, N) has the form:

$$y(j,i) = \sum_{q=1}^{m} k_{qj}\, f_q(i), \qquad (1)$$

where:
j is the number of the character in the transmitted message;
$f_q(i) = f_q(ih)$, (i = 1, 2, … N > m), (q = 1, 2, … m) - an array of values of the q-th Key Function;
k_{qj} - coefficients that are generated during encryption of the j-th element and can be either equal to zero or represent random numbers which are unknown to the recipient.

Key Functions can be either continuous or discrete. These functions should be the same for the transmitting and receiving sides and have the same numbering. Also, the step h of changing the argument of the Key Functions should be the same. An encrypted message in the form of a matrix y(T,N) is transmitted over an open communication channel. The task is to decrypt the message using the matrix received at the receiving end. To solve it, the integral disproportion of the first order is used [23].

3. Disproportion functions

One of the first publications in which disproportion functions were proposed was [19]. In particular, the disproportion with respect to the n-th-order derivative of the function y(x) with respect to x is described by the expression:

$$@d_x^{(n)} y = \frac{y}{x^n} - \frac{1}{n!} \cdot \frac{d^n y}{dx^n}, \qquad (2)$$

Here the @ symbol is chosen to denote the operation of calculating disproportion. The symbol "d" stands for "derivative". The order is

indicated in parentheses. The left part (2) reads "et d n y with respect to x". The order n ≥ 1 is an integer. If for any value of x, the function y(x) has the form $y = kx^n$, then disproportion (2) is equal to zero regardless of the value of the coefficient k.

For the case when n = 1,

$$@d_x^{(1)}y = \frac{y}{x} - \frac{dy}{dx}, \quad (3)$$

For defining the functions parametrically, when, x = φ(t), y = ψ(t), where t is a parameter, disproportion (3) is described by the expression

$$@d_{\varphi(t)}^{(1)}\psi(t) = \frac{\psi(t)}{\varphi(t)} - \frac{d\psi/dt}{d\varphi/dt}, \quad (4)$$

For ψ(t) = kφ(t) disproportion (4) is equal to zero in the entire area of existence x = φ(t), regardless of the value of k. In [19], the case was considered when

$$y(x) = k_1 f_1(x) + k_2 f_2(x) + \cdots + k_m f_m(x), \quad (5)$$

where $f_1(x)$, $f_2(x)$, … $f_m(x)$ are known functions; k_1, k_2, … k_m are coefficients whose values are unknown.

It is shown that the disproportion functions allow calculating the values of the unknown coefficients in (5) from the data obtained for the current value of the argument. This opportunity is used to create cryptosystems [15-17].

In practice, often the first derivative of the function does not exist or is equal to zero on some interval. This excludes the possibility of using disproportions over the first-order derivative (2-4). In this case, it is advisable to use the integral disproportion of the first order [23]. This disproportion of the function y(x) with respect to f(x) has the form:

$$@I_{f(x)}^{(1)}y(x) = \frac{\int_{x-h}^{x} y(x)dx}{\int_{x-h}^{x} f(x)dx} - \frac{y(x)}{f(x)}, \quad (6)$$

where h - is the preset time interval. In the discrete representation of signals, this is a time quantization step.

In this case, y(x) and f(x) are represented by one-dimensional arrays. If the approximate values of the integrals in (6) are calculated using the trapezoid formula, then for the one and the same step h for y(x) and f(x), disproportion (6) takes the following form (7):

$$@I_{f_i}^{(1)}y_i = \frac{y_{i-1} + y_i}{f_{i-1} + f_i} - \frac{y_i}{f_i}, \quad (7)$$

4. Encrypting and decrypting messages

The transmitting and receiving sides must have the same system of m Key Functions of the real variable, their numbering, the interval of changing the argument and step h of its change. The number of elements N of the one-dimensional array corresponding to the encrypted character must also be set. These can be both characters from the ASCII table, and components of pixel brightness when transmitting color graphic images. Each of them is represented by an integer. The required number of Key Functions depends on the maximum value of this number. For example, to encrypt characters from the ASCII table, m = 8 Key Functions are required. They can be either continuous or discrete. If the Key Functions are continuous, it is necessary to calculate N elements of one-dimensional arrays of their values, changing the argument from the initial x_{min} to the final x_{max} value with a step h. When encrypting characters from the ASCII table or the pixel brightness, their numerical representations differ by one. In these cases, the step h of changing the argument must be equal to one.

An m-bit binary code corresponds to each encrypted character. Each bit in this code is associated with a specific number of the Key Function. If the bit is zero, the value of the corresponding Key Function is also zero. If the bit is equal to one, then a random value of the amplitude of the corresponding Key Function is played. The character to be encrypted is represented by the sum (1).

4.1. Encrypting messages

1. The following is a character encryption algorithm:
2. Calculate arrays of N > m values of Key Functions: $f_q(x)$, q = 1, 2… m.
3. Enter the encrypted j-th character and calculate its cipher in the form of values of the one-dimensional array y(j, i), i = 1, 2... N according to (1).
4. Repeat this point for all characters of the message of length T.
5. A sequence of T arrays is an encrypted message transmitted over an open communication channel.

4.2. Decrypting messages

Pre-compute the arrays $f_q(i) = f_q(ih)$, (q = 1, 2, ... m), (i = 1, 2, ... N > m), of Key Functions and to receive T one-dimensional arrays y(j , i), j = 1, 2, ... T, i = 1, 2, ... N over the communication channel. Further, in order to simplify the description of the decryption process, an example is given when only three functions are used in the cryptosystem - the keys: $f_1(x)$, $f_2(x)$, $f_3(x)$. In this case m = 3. Accordingly, the j-th character of the message is encrypted as

$$y(j,i) = k_{1j}f_1(i) + k_{2j}f_2(i) + k_{3j}f_3(i), \quad (8)$$
$$i = 1, 2, \dots N > 3,$$

The process consists of m = 3 levels in accordance with the number of Key Functions.

First level: It is necessary to calculate the array of disproportions (7) y(j,i) with respect to any of the Key Functions , for example, $f_1(i)$:

$$F_{01}(j,i) = @I^{(1)}_{f_1(i)} y(j,i) = \quad (9)$$
$$\frac{y(j,i-1) + y(j,i)}{f_1(i-1) + f_1(i)} - \frac{y(j,i)}{f_1(i)},$$

where i = 2, 3…N.

Also calculate the disproportions (7) of the remaining key functions with respect to $f_1(i)$:

$$F_{r1}(j,i) = @I^{(1)}_{f_1(i)} f_r(j,i) \quad (10)$$
$$= \frac{f_r(j,\ i-1) + f_r(j,i)}{f_1(i-1) + f_1(i)} - \frac{f_r(j,i)}{f_1(i)},$$

where r = 2, 3.

Considering that the disproportion of the function relative to itself is zero, we get:

$$F_{01}(j,i) = k_{2j}F_{21}(j,i) + k_{3j}F_{31}(j,i), \quad (11)$$

Second level: It is necessary to select any disproportion from right-hand of (11), for example $F_{21}(j, i)$. It is used to calculate next disproportions:

$$F_{0121}(j,i) = @I^{(1)}_{F_{21}(j,i)} F_{01}(j,i) \quad (12)$$
$$= \frac{F_{01}(j,\ i-1) + F_{01}(j,i)}{F_{21}(j,\ i-1) + F_{21}(j,i)} - \frac{F_{01}(j,i)}{F_{21}(i)},$$

$$F_{3121}(j,i) = @I^{(1)}_{F_{21}(j,i)} F_{31}(j,i) \quad (13)$$
$$= \frac{F_{31}(j,\ i-1) + F_{31}(j,i)}{F_{21}(j,\ i-1) + F_{21}(j,i)} - \frac{F_{31}(j,i)}{F_{21}(i)},$$

Taking into account that the disproportion of $F_{21}(j, i)$ with respect to $F_{21}(j, i)$ is equal to zero, we get:

$$F_{0121}(j,i) = k_{3j}F_{3121}(j,i), \quad (14)$$

Third level: The disproportion of $F_{0121}(j, i)$ with respect to $F_{3121}(j,i)$ is calculated in the following way

$$F_{01213121}(j,i) = @I^{(1)}_{F_{3121}(j,i)} F_{0121}(j,i) \quad (15)$$
$$= \frac{F_{0121}(j,\ i-1) + F_{0121}(j,i)}{F_{3121}(j,\ i-1) + F_{3121}(j,i)} - \frac{F_{0121}(j,i)}{F_{3121}(i)} = 0,$$

It is equal to zero because, as can be seen from (14), there is a proportional relationship between $F_{0121}(j, i)$ and $F_{3121}(j, i)$. This fact allows calculating from (14) k_{3j} and k_{2j}, k_{1j} for the j-th message symbol.

$$k_{3j} = \frac{F_{0121}(j,i)}{F_{3121}(i)}, \quad (16)$$

$$k_{2j} = \frac{F_{01}(j,i) - k_{3j}\,F_{31}(j,i)}{F_{21}(i)}, \quad (17)$$

$$k_{1j} = \frac{y(j,i) - k_{2j}f_2(i) - k_{3j}f_3(i)}{f_1(i)}, \quad (18)$$

Depending on which of these coefficients are nonzero and which are equal to zero, the j-th message symbol is decrypted. In practice, it must be taken into account that there are calculation errors.

Therefore, it is necessary to compare the disproportion (15) calculated at the last level in modulus not strictly with zero, but with an approximate number ε. For example, it could be $\varepsilon=10^{-4}$. In this case, if $| F_{01213121}(j, i) | <= \varepsilon$, then it should be assumed that it is zero.

The value of ε is determined during testing of the cryptosystem. Theoretically, this disproportion is equal to zero for all i = 2, 3, ... N, but, taking into account the calculation errors, it is recommended to do calculations using formulas (16-18) for i, at which the modulus of disproportion (15) is minimal.

4.3. An example of encrypting and decrypting characters from an ASCII table

Eight Key Functions are used (m =8):

1. $f_1(x) = 1000 \sin((\alpha_1 - \beta_1)x) \cos(w\beta_1 x)$
2. $f_2(x) = 1000 \exp(0.1\alpha_2 x) \sin(w\beta_2 x) \cos((\alpha_2 + \beta_2)x)$
3. $f_3(x) = 1000 \exp(-\alpha_3 x) \sin(w\beta_3 x)$
4. $f_4(x) = 1000 \cos((\alpha_1 x - \beta_1)x) \sin(w\beta_1 x)$

5. $f_5(x) = 1000 \exp(0.1\sin(\alpha_2 x))\ \sin(w \cos(\beta x))\ \cos((\alpha_2+\beta_2)\ x)$

6. $f_6(x) = 1000 \sin(-\cos(\alpha_3 x))\ \cos(w \sin(\beta_3 x))$

7. $f_7(x) = 1000 \sin(wx + \alpha_1)\ \exp(-\beta_1 x^2)$

8. $f_8(x) = 1000 \cos(w\gamma x^2)$

where $\alpha_1 = 1$, $\alpha_2 = 0.12$, $\alpha_3 = 0.5$, $\beta_1 = 0.1$, $\beta_2 = 1.5$, $\beta_3 = 0.7$, $\gamma = 0.5$, $w = 400$ are constants.

A sequence of numbers corresponding to the transmitted characters from the ASCII code table is encrypted. Each character is encoded by a sum of Key Functions

$$y(x) = k_1 f_1(x) + k_2 f_2(x) + k_3 f_3(x) + k_4 f_4(x) + k_5 f_5(x) + k_6 f_6(x) + k_7 f_7(x) + k_8 f_8(x), \quad (19)$$

where:

x = ih – argument;

h = 1 – step of changing the argument.

i – is the ordinal number of the element of the one-dimensional array for each of the Key Functions, as well as the array $y_0, y_1, ..., y_{N-1}$, which is the character cipher;

N – a number of elements of each one-dimensional array. Based on the requirement of N > m, the amount of array elements N = 16.

Table 1 shows the transmitted characters in the upper horizontal line. The corresponding ciphers are given in the form of arrays arranged vertically. The decrypted characters are located horizontally on the bottom line.

It is obvious that the received message matches the transmitted one. It should be noted that the ciphers (arrays) of the adjacent symbols `t` are completely different.

The codes of the other adjacent identical symbols in the message are given in Table 2. The above results indicate that the ciphers of the adjacent identical symbols in the message differ from each other. This circumstance greatly complicates the "hacking" of the cryptosystem. In order to "crack" the message, it is required to select the form of eight Key Functions and the values of their parameters.

Table 1

Encrypted and decrypted characters “Hello”

y	‘H’	‘e’	‘l’	‘l’	‘o’
0	-323.36050	-1096.0141	-872.47149	37.134528	-112.93721
1	257.702939	167.391848	1051.01033	532.400561	427.740614
2	57.298613	175.907791	-408.37541	-216.26334	-116.65218
3	-165.32821	126.358160	-324.75198	-162.19800	-197.22270
4	-186.82906	-394.77504	-929.02530	-439.94548	-449.01146
5	-163.70378	-392.33753	-1059.2853	-385.85981	-170.75848
6	37.446166	299.880685	370.310135	74.675455	44.746439
7	-110.70494	426.787248	-218.90900	-238.68403	-314.75860
8	-2.714026	-59.278796	115.564604	-2.371129	-165.23427
9	9.436954	152.916970	116.697501	-23.361501	281.220083
10	42.465400	-412.02347	-203.82595	84.424717	150.029168
11	-24.295297	615.002251	349.117675	-42.371452	-231.55086
12	101.570285	95.754178	543.764259	227.452661	-122.68102
13	195.422364	132.219196	855.514365	432.359247	754.345004
14	-11.067358	-507.14921	-252.27430	-29.696351	228.457327
15	214.445079	264.682389	659.731238	467.369970	-63.039751

Table 2

Encrypted and decrypted characters ‘A’

y	‘A’	‘A’	‘A’	‘A’	‘A’
0	-597.135343	-762.540347	-609.489179	-1245.052456	-917.400855
1	9.473961	-6.667141	-2.760240	-37.310266	-17.407304
2	274.695430	368.229254	291.933312	625.796927	451.736269
3	15.193014	87.216540	60.428145	237.898008	138.849052
4	-123.497929	-217.377766	-165.579209	-438.953490	-291.370618
5	-58.830278	-107.584825	-81.548078	-221.367775	-145.669069
6	-8.280530	-11.911812	-9.337867	-21.332769	-14.999968
7	199.488556	342.700766	261.876769	683.403833	456.291669
8	-76.316724	-131.227388	-100.265637	-261.818697	-174.769533
9	-60.158608	103.377062	78.993047	-206.183725	137.653657
10	-125.104506	-215.011307	-164.292499	-428.868345	-286.313719
11	214.641127	368.892513	281.874942	735.803375	491.224813
12	-14.047252	24.142272	18.447384	-48.154847	-32.148341
13	6.530344	11.223364	8.575899	22.386440	14.945262
14	-223.052958	-383.349601	-292.921754	-764.640006	-510.476209
15	169.891087	291.983039	223.107534	582.397666	388.810617

Below is an example that illustrates the resistance of the system obtaining keys, even if somehow it was possible to find out the forms of Key Functions. Suppose that the above sequence of characters is encrypted using functions (7), and decrypted using the same kind of functions, but the constant w was guessed incorrectly. Instead of w = 400 was used w = 399.999 during decryption. In this case, the disproportion at the last eighth level in absolute value exceeds the permissible deviation ε from zero. That is, decryption is impossible. Only if w = 399.9999, the message may be decrypted. This result shows that even such a slight deviation of one of the parameters of the Key Functions does not allow decryption of the transmitted character.

5. Requirements for Key Functions

1. The Key Functions must be of real type.
2. They can’t be constant and must not take zero values.
3. When using the key function, there should be no situation where division by a number close to zero occurs, which leads to an unacceptable calculation error. For this purpose, it is recommended to test the cryptosystem for the entire alphabet of characters that will be used in messages.
4. Check that the sum of two or more key functions does not coincide with any other of the key functions.
5. It is recommended to include all parameters in the expression for each key function. In this case, a change in the value of any

parameter leads to a change in all key functions, but not one or several of them only.

6. Before sending an encrypted message, first check what the decrypted message looks like in order to avoid errors that may occur as a result of not taking into account the previous points.

6. Conclusions

A cryptosystem with symmetric keys is proposed. These keys are real variable functions that satisfy the above constraints. They can be either continuous or discrete. The number of functions is equal to the number of binary digits used to encrypt a character, for example, in an ASCII table. Each of the functions corresponds to a certain binary digit. The symbol of the transmitted message is encrypted with a one-dimensional array. The elements of this array represent the sum of Key Functions with random amplitudes. This sum includes those Key Functions, for which the corresponding binary digit is equal to one.

Decryption is performed using disproportion functions. The possibility of encryption and decryption of text information is shown. The given examples show the complexity the guessing Key Functions and the cryptographic strength of the proposed cryptosystem. So, for example, a real-type constant, which equals 400 during encryption, to break the system by brute-force, you need to select with an accuracy of 10^{-4}, but there can be any number of such constants. It is very difficult to find all the constants of the real type at the same time with high precision and thus hack the system, even with well-known formulas of functions - keys.

It should also be noted that the codes of the same adjacent symbols are not repeated, which can be seen from Table 2. This also increases the cryptographic strength of the system.

7. References

[1] National Institute of Standards and Technology, Specification for the ADVANCED ENCRYPTION STANDARD (AES) (2001). doi: 10.6028/NIST.FIPS.197.

[2] GOST 28147-89. Sistemy obrabotki informacii. Zashhita kriptograficheskaya. Algoritm kriptograficheskogo preobrazovaniya [Information processing systems. Cryptographic protection. Cryptographic Transformation Algorithm], 1990.

[3] A. N. Lebedev, Kriptografiya s «otkrytym klyuchom» i vozmozhnosti ee prakticheskogo primeneniya [Cryptography with "public key" and the possibilities of its practical application], Zashhita informacii. Konfident 2 (1992)

[4] R. Rivest, A. Shamir, I. Adleman, A method for obtaining digital signatures and public-key cryptosystems, Communications of the ACM, 1978, 21(2):120-126. doi:10.1145/359340.359342.

[5] I. D. Gorbenko., Y. I. Gorbenko, Prykladna kryptolohiya [Applied Cryptology], Fort, NURE, Kharkiv, 2012, p. 878.

[6] D. R. Hankerson, S. A. Vanstone and A. J. Menezes., Guide to elliptic curve cryptography, Springer, New York, 2003, p. 311.

[7] T. D. Ladd, F. Jelezko, R. Laflamme, Y. Nakamura, C. Monroe, J. L. O'Brien, Quantum Computing, Nature, 464 (2010) 45—53. doi: 10.1038/nature08812.

[8] P. G. Klucharev, Kvantovyj komp'yuter i kriptograficheskaya stojkost' sovremennyx sistem shifrovaniya [Quantum computer and cryptographic strength of modern encryption systems], Herald of the Bauman Moscow State Technical University, Series Natural Sciences 2 (2007).

[9] I.K. Grover, Quantum Mechanics Help in Searching for a Needle in a Haystack, Phys. Rev. Lett. 79, 325 (1997): 326-328. doi: 10.1103/PhysRevLett.79.325.

[10] P. Shor, Polynomial-Time Algorithms for Prime Factorization and Discrete Logarithms on a Quantum Computer, in: Proceedings of the 35th Annual Symposium of Foundations of Computer Science, 1994. doi: 10.1137/S0097539795293172.

[11] J. A. Proos, Shor's discrete logarithm quantum algorithm for elliptic curves, Faculty of Mathematics University of Waterloo, Waterloo, 2003, p. 35.

[12] S. Yevseiev, R. Korolyov, A. Tkachov, O. Laptiev, I. Opirskyy, O. Soloviova. Modification of the algorithm (OFM) S-box, which provides increasing crypto resistance in the post-quantum period, International Journal of Advanced Trends in Computer Science and Engineering, 2020, volume 9, pp. 8725-8729. doi:10.30534/ijatcse/2020/261952020.

[13] O. Barabash, O. Laptiev, V. Tkachev, O. Maystrov, O. Krasikov, I. Polovinkin, The Indirect method of obtaining Estimates of the Parameters of Radio Signals of covert means of obtaining Information, International Journal of Emerging Trends in Engineering Research, 2020, volume 8, pp. 4133 – 4139. doi:10.30534/ijeter/2020/17882020.

[14] A. N. Kolmogorov, S. V. Fomin, Ehlementy teorii funkcij i funkcional'nogo analiza [Elements of function theory and functional analysis], Science, Moscow, 1972.

[15] V. V. Avramenko, M. I. Zabolotny, A Way of Data Coding, 2009. Patent No. 42957, Filled March 16th, 2009, Issued July 27th, 2009.

[16] V. V. Kalashnikov, V. V. Avramenko, N. I. Kalashnikova and Kalashnikov Jr. V.V., A Cryptosystem Based Upon Sums of Key Functions, International Journal of Combinatiorial Optimization Problems and Informatics, 2017, volume 8, pp. 31-38.

[17] N. I. Kalashnikova, V. V. Avramenko, V. Kalashnikov. Sums of Key Functions Generating Cryptosystems, in: ICCS 2019, Chapter 23, Lecture Notes in Computer Science, vol. 11540, Springer, Cham, 2019. doi: 10.1007/978-3-030-22750-0_23.

[18] V. V. Avramenko, V. Demianenko, in: CEUR Workshop Proceedings, 2020, 2608, pp. 661-674. doi: 10.15588/1607-3274-2020-2-8.

[19] V. V. Avramenko, Characteristic properties of disproportionality functions and their application to solving diagnoses problems, Transactions of Sumy State University, SSU, Sumy, 2000, №16, pp. 24-28.

[20] V. V. Kalashnikov, V. V. Avramenko, N. I. Kalashnykova, Derivative disproportion functions for pattern recognition, in: Watada, J., Tan, S.C., Vasant, P., Padmanabhan, E., Jain, L.C. (eds.) Unconventional Modelling, Simulation, and Optimization of Geoscience and Petroleum Engineering, pp. 95–104. Springer, Heidelberg, 2018.

[21] V. V. Kalashnikov, V. V. Avramenko, N. Y. Slipushko, N.I. Kalashnykova, N.I., A. E. Konoplyanchenko, Identification of quasi-stationary dynamic objects with the use of derivative disproportion functions, Procedia Comput. Sci., (2017) 108(C): 2100–2109.

[22] V. V. Avramenko, A. Moskalenko, Operative Recognition of Standard Signals in the Presence of Interference with Unknown Characteristics, in: Proceedings of the Second International Workshop on Computer Modeling and Intelligent Systems (CMIS-2019), Zaporizhzhia, 2019.

[23] A. P. Karpenko, Integral'nye harakteristiki neproporcional'nosti chislovyh funkcij i ih primenenie v diagnostike [Integral characteristics of the disproportionality of numerical functions and their application in diagnostics], Vestnik Sumskogo gos. un-ta. 16(2000): 20-25

Method Of Recognition Sarcasm In English Communication With The Application Of Information Technologies

Trystan S.[1], Matiushchenko O.[2] , Naumenko M. [3]

[1,2]Kharkiv National University of Radio Electronics, Nauky Ave. 14, Kharkiv, 61166, Ukraine
[3]Ivan Kozhedub Kharkiv National Air Force University, Sumska str. 77/79, Kharkiv, 61023, Ukraine

Abstract
The article developed a software application for recognizing sarcasm in English communication. NLP technology is used to implement machine learning. Python programming language. Comparisons with known algorithms and models are made. The advantage in the simplicity of the method implementation and the speed of recognition, which corresponds to live communication, is proved.

Keywords
Artificial intelligence, language recognition, machine learning, sarcasm.

1. Introduction

Human language is extremely complex and contains a significant number of linguistic constructions. Language recognition and translation is a well-developed area of machine learning. However, living human language contains such elements as humor, irony, pun, aphorism, sacredness, which are not always correctly recognized by native speakers, and recognizing them with the help of intelligent information technology becomes quite a difficult task. At the same time, virtual translators must, in a reasonable amount of time (preferably in real time), recognize a person's living language and communicate its content and emotional and logical implication to the user. Today, the universal language of communication is English. Sarcasm is the most complex language construction, because in a sentence with sarcasm one logical construction is confirmed, and the opposite is understood [1]. Thus, recognizing sarcasm in communication is quite a challenge.

2. Analysis of problem-solving methods

At present, there are a sufficient number of electronic translators designed to facilitate the communication process. Living language recognition is based on electronic dictionaries and Data Science (DS) technologies [2]. In DS such direction as Nature - Language Processing (NLP) is allocated. This area studies the problems of computer analysis and synthesis of natural language. For artificial intelligence, analysis means understanding language, and synthesis means generating intelligent text [3]. Solving the problems associated with the analysis and synthesis of language structures will mean creating a more convenient form of interaction between computer and human, as well as ensuring communication through electronic translators.

Examples of using NLP are such services and applications as Siri (assistant for operating systems from Apple: iOS, watchOS, macOS, HomePod and tvOS) [4], Cortana (virtual assistant in Windows) [5], Gmail Spam Filter (analysis service) and selection of mail with spam) [6]. It should be noted that there are currently a sufficient number of applications that implement NLP.

However, simple solutions are needed that will quickly recognize sarcasm in living language in communication. The theoretical basis of the work was works [7], [8], works on applied statistical analysis [9] and applied analysis of text data in Python [10].

EMAIL: serhii.trystan@nure.ua (A. 1); mog28@ukr.net (A. 2); mv.naumenko@ukr.net (A. 3)
ORCID: 0000-0003-1270-5254 (A. 1); 0000-0003-4843-8258 (A. 2); 0000-0002-1216-9263 (A. 3)

3. Main part

3.1. Problem statement and substantiation of tools for its solution

The task to be solved in the article is the automatic recognition of sarcasm in live English communication.

The main tools for solving this problem are:

1. statistical and mathematical methods of big data processing [7], [8], [9], [10];
2. dataset for model learning [11];
3. Python programming language 3.8.1 [12];
4. Jupyter notebook development environment;
5. a set of libraries (sklearn, re, pandas, numpy, nltk (natural language toolkit), matplotlib).

3.2. Dataset choosing and bring it to normal

The date set was chosen on Kaggle.com. The required data set is called “News Headlines Dataset For Sarcasm Detection. High quality dataset for the task of Sarcasm Detection” [11]. This dataset contains news headlines that are collected from two sites: TheOnion and HuffPost. Each record consists of three attributes, and itself:

1. **is_sarcastic** (1, if the entry is sarcastic, and 0 if not sarcastic);
2. **headline** (the title of the page);
3. **article_link** (link to the page from which the title was taken).

In Figure 1 shows the structure of this dataset.

	article_link	headline	is_sarcastic
0	https://www.huffingtonpost.com/entry/versace-b...	former versace store clerk sues over secret 'b...	0
1	https://www.huffingtonpost.com/entry/roseanne-...	the 'roseanne' revival catches up to our thorn...	0
2	https://local.theonion.com/mom-starting-to-fea...	mom starting to fear son's web series closest ...	1
3	https://politics.theonion.com/boehner-just-wan...	boehner just wants wife to listen, not come up...	1
4	https://www.huffingtonpost.com/entry/jk-rowlin...	j.k. rowling wishes snape happy birthday in th...	0
...	...	...	...
26704	https://www.huffingtonpost.com/entry/american-...	american politics in moral free-fall	0
26705	https://www.huffingtonpost.com/entry/americas-...	america's best 20 hikes	0
26706	https://www.huffingtonpost.com/entry/reparatio...	reparations and obama	0
26707	https://www.huffingtonpost.com/entry/israeli-b...	israeli ban targeting boycott supporters raise...	0
26708	https://www.huffingtonpost.com/entry/gourmet-g...	gourmet gifts for the foodie 2014	0

26709 rows × 3 columns

Figure 1: “Sarcasm_Headlines_Dataset” structure

As can be seen from fig. 1, the first steps in creating an information technology for sarcasm recognition - is to bring the column "headline" to normal, which consists of bringing all the letters to lowercase, removing dots and spaces.

In Figure 2 shows the script for bringing the “headline” column to normal.

```
In [7]: ds = pd.read_json('Sarcasm_Headlines_Dataset.json', lines = True)
        headline_re_sub = []
        for i in ds['headline']:
            headline_re_sub.append(re.sub('[^a-zA-Z]', ' ',i))
        ds['headline'] = headline_re_sub
```

Figure 2: Bring the column "headline" to normal

3.3. Stemming words

The next stage of the method is word stemming. In the field of natural language processing, there are cases when two or more words have a common root. Stemming reduces all counter word forms to one, normal vocabulary form.

There are two main steaming algorithms: Porter's algorithm and Lancaster's algorithm [9]. The developed script uses Porter's algorithm because it is less aggressive to word forms. Lancaster's algorithm is quite aggressive, because it strictly "cuts" the word and makes it very

confusing, which is impractical in recognizing such a complex linguistic phenomenon as sarcasm. In Figure 3 shows the use of the Portrait algorithm with respect to the “headline” column.

```
In [29]: headline_re_sub =[]
         for i in ds['headline']:
             headline_re_sub.append(re.sub('[^a-zA-Z]', ' ',i))

         ps = PorterStemmer()

         ds['headline'] = headline_re_sub

         features = ds['headline']
         labels = ds['is_sarcastic']

         features = features.apply(lambda x: x.split())
         features = features.apply(lambda x : ' '.join([ps.stem(word) for word in x]))

         tv = TfidfVectorizer(max_features = 5000)

         features = list(features)
         features = tv.fit_transform(features).toarray()
         features

Out[29]: array([[0., 0., 0., ..., 0., 0., 0.],
                [0., 0., 0., ..., 0., 0., 0.],
                [0., 0., 0., ..., 0., 0., 0.],
                ...,
                [0., 0., 0., ..., 0., 0., 0.],
                [0., 0., 0., ..., 0., 0., 0.],
                [0., 0., 0., ..., 0., 0., 0.]])
```

Figure 3: Using Porter's algorithm for word stemming in a dataset

3.4. Convert text to numbers

The next step of the method is to convert the text into a meaningful representation of numbers, which will be used in machine learning algorithms for prediction. In Figure 4 shows the use of the TfidfVectorizer function, which was taken from the sklearn.feature_extraction.text library.

```
In [28]: headline_re_sub =[]
         for i in ds['headline']:
             headline_re_sub.append(re.sub('[^a-zA-Z]', ' ',i))



         ds['headline'] = headline_re_sub

         features = ds['headline']
         labels = ds['is_sarcastic']

         ps = PorterStemmer()

         features = features.apply(lambda x: x.split())
         features = features.apply(lambda x : ' '.join([ps.stem(word) for word in x]))
         features

Out[28]: 0        former versac store clerk sue over secret blac...
         1        the roseann reviv catch up to our thorni polit...
         2        mom start to fear son s web seri closest thing...
         3        boehner just want wife to listen not come up w...
         4        j k rowl wish snape happi birthday in the most...
                                       ...
         26704                  american polit in moral free fall
         26705                            america s best hike
         26706                                repar and obama
         26707    isra ban target boycott support rais alarm abroad
         26708                          gourmet gift for the foodi
         Name: headline, Length: 26709, dtype: object
```

Figure 4: Using the “TfidfVectorizer” function

After all the steps to bring the data to values that can be used in computer training, we need to determine the model of machine learning.

3.5. Choosing a machine learning model

The logistic regression is chosen as the basic model of machine learning. Logistic regression is a machine learning classification algorithm that is used to predict the probability of a categorical dependent variable. In logistic regression, the dependent variable is a binary variable containing data encoded as 1 (yes, success) or 0 (no, failure). Since our problem is a binary classification problem (1 - sarcasm, 0 - not sarcasm), logistic regression is a relevant model [9]. In Figure 5 presents a graph of logistic regression.

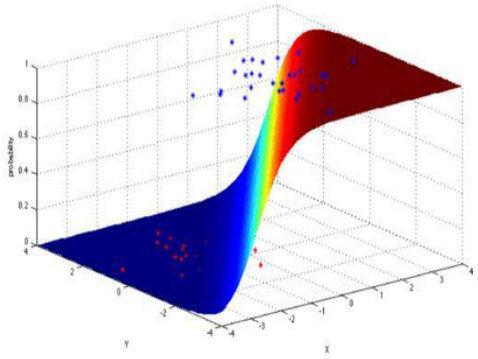


Figure 5: Logistic Regression Plot

3.6. Machine learning

Before training the model, divide the dataset into training and test samples with the following parameters: 30 percent of the entire sample will go to the test data set, and the other 70 to the training (Figure 6).

```
X_train, x_test, Y_train, y_test = train_test_split(features, labels, test_size = .30, random_state = None)
```

Figure 6: Division of the dataset into training and test samples

The accuracy of the model is checked using cross-validation (re-sampling procedure). The decision to choose this method is based on its simplicity and obtaining a less biased or less optimistic assessment of the quality of the model than other methods. In

Figure **7** shows the accuracy of the model that was verified by cross-validation.

```
model = LogisticRegression()
model.fit(X_train, Y_train)
cv = 10
res = cross_val_score(estimator = model, X = X_train, y = Y_train, cv = cv)
print("The average quality of the model, when conducting ",cv," experiments: ",round(np.mean(res),2))
print("Values in the training sample: ", round(model.score(X_train, Y_train),2))
print("Values in the test sample: ", round(model.score(x_test, y_test),2))
```

```
The average quality of the model, when conducting  10  experiments:  0.83
Values in the training sample:  0.88
Values in the test sample:  0.83
```

Figure 7: Model accuracy

Another metric for evaluating the quality of the model is the ROC curve (one of the most popular quality functionalities in binary classification problems) [9]. In Figure 8 shows the ROC - curve obtained in the work.

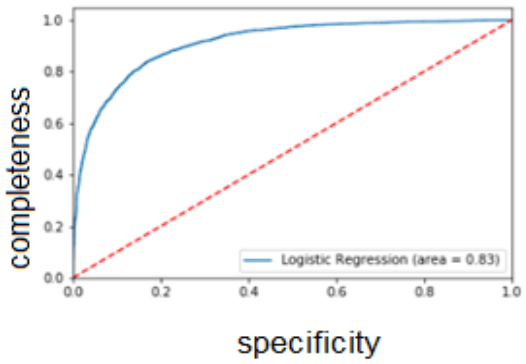


Figure 8: ROC curve

After carrying out stages designing model of machine learning it is necessary to carry out the test.

3.7. Model testing

In Figure 9 shows an example of testing the model on the phrase: *"Oh, have I touched that tiny ego of yours?"*.

Information technology has rightly determined that this sentence is sarcasm.

```
sent = input(str())
sent = re.sub('[^a-zA-Z]', ' ', sent)
text = []
text.append(sent)
data = tv.transform(text).toarray()
pred = model.predict(data)
if(int(pred[0])==1):
    print("Sarcasm")
else:
    print("NOT Sarcasm")
```

```
Oh, have I touched that tiny ego of yours?
Sarcasm
```

Figure 9: Model testing

It is also necessary to compare the results with known algorithms and implementations. This comparison is shown in

Table ***1***.

Table 1
Comparison of the obtained results

Model	KNearest Neighbors	**Logistic Regression**	Naive Bayes	LinearSVC	RandomForest Classifier
Prediction	68.3% (0,8 sec)	**84.04% (0,12 sec)**	75.09% (0,10 sec)	78.08% (0,11 sec)	79.64% (0,11 sec)

Thus, we can conclude about the effectiveness of the developed method and the possibility of its application for the recognition of sarcasm in live communication on English.

4. Conclusions

1. Recognition of linguistic constructions of natural language is a difficult task on the border of such scientific areas as AI, ML, philology.
2. Recognizing sarcasm in living language is one of the most difficult tasks, because a person masks sarcasm.
3. Recognition of sarcasm should be done quickly (commensurate with the pace of communication), so decisions should be simple and effective.
4. The obtained solution has a degree of recognition of 0.83, but in contrast to more powerful solutions, it is quite fast.
5. The article presents the results of the study of ML and NLP in terms of solving the problem of identification and classification of sarcasm.

5. References

[1] "Definition of SARCASM," [Online]. Available: www.merriam-webster.com. Retrieved 2021-06-23. [Accessed 29 June 2021].

[2] "About Data Science / Data Science Association," [Online]. Available: www.datascienceassn.org. [Accessed 3 April 2021].

[3] G. Y., "A primer on neural network models for natural language processing," *Journal of Artificial Intelligence Research,* no. 57, pp. 345-420, 2016.

[4] L. Steven, "An exclusive inside look at how artificial intelligence and machine learning work at Apple Wired. Retrieved .," [Online]. [Accessed 10 June 2017].

[5] APKMirror, "Cortana – Digital assistant," 29 September 2017. [Online].

[6] Giorgio Fumera, Ignazio Pillai, Fabio Roli, "Spam filtering based on the analysis of text information embedded into images," *Journal of Machine Learning Research (special issue on Machine Learning in Computer Security),* no. 7, pp. 2699-2720.

[7] E. Liddy, "Natural Language Processing," *Encyclopedia of Library and Information Science,* 2001.

[8] Практическая статистика для специалистов Data Science, СПБ: БХВ-Петербург, 2018, p. 304.

[9] Бенгфорт Б., Билбро Р., Охеда Т., Прикладной анализ текстовых данных на Python. Машинное обучение и создание приложений обработки естественного языка, Санкт-Петербубг: Питер, 2020, p. 368.

[10] R. Atienza, Advanced Deep Learning with TensorFlow 2 and Keras, 2012, p. 512.

[11] "News Headlines Dataset For Sarcasm Detection," [Online]. Available: https://www.kaggle.com/rmisra/news-headlines-dataset-for-sarcasm-detection. [Accessed 29 June 2021].

[12] J. V. Guttag, Introduction to Computation and Programming Using Python: With Application to Understanding Data, 2017.

Method of Calculation of Information Protection from Clusterization Ratio in Social Networks

Vitalii Savchenko [1], Volodymyr Akhramovych [2], Oleksander Matsko[3] and Ivan Havryliuk [4]

[1,2] *State University of Telecommunications, Solomianska str.7, Kyiv, 03110, Ukraine*
[3,4] *The National Defense University of Ukraine named after Ivan Cherniakhovskyi, Povitroflotsky av. 28, Kyiv, 03049, Ukraine*

Abstract

The article investigates the dynamic models of the information protection system in social networks taking into account the clustering coefficient, and also analyzes the stability of the protection system. In graph theory, the clustering factor is a measure of the degree to which nodes in a graph tend to group together. The available data suggest that in most real networks, and in particular in social networks, nodes tend to form closely related groups with a relatively high density of connections; this probability is greater than the average probability of a random connection between two nodes.

There are two variants of this term: global and local. The global version was created for a general idea of network clustering, while the local one describes the nesting of individual nodes. There is a practical interest in studying the behavior of the system of protection of social networks from the value of the clustering factor. Dynamic systems of information protection in social networks in the mathematical sense of this term are considered. A dynamic system is understood as any object or process for which the concept of state as a set of some quantities at a given moment of time is unambiguously defined and a given law is described that describes the change (evolution) of the initial state over time. This law allows the initial state to predict the future state of a dynamic system. It is called the law of evolution.

The study is based on the nonlinearity of the social network protection system. To solve the system of nonlinear equations used: the method of exceptions, the joint solution of the corresponding homogeneous characteristic equation. Since the differential of the protection function has a positive value in some data domains (the requirement of Lyapunov's theorem for this domain is not fulfilled), an additional study of the stability of the protection system within the operating parameters is required. Phase portraits of the data protection system in MatLab / Multisim are determined, which indicate the stability of the protection system in the operating range of parameters even at the maximum value of influences.

Keywords

dynamic models, information protection system, social networks, clustering coefficient, nonlinearity, exception method, homogeneous characteristic equation, function differential, system stability, phase portrait

1. Introduction

Descriptions of dynamical systems for various problems depending on the law of evolution are also various: with the help of differential equations, discrete mappings, graph theory, Markov chain theory, and so on. The choice of one of the methods of description determines the specific form of the mathematical model of the corresponding dynamic system [3].

The mathematical model of a dynamic system is considered to be given if the parameters (coordinates) of the system are introduced, which unambiguously determine its state, and the law of evolution is specified. Depending on the degree of approximation to the same system, different mathematical models can be matched.

Theoretical study of the dynamic behavior of a real object requires the creation of its mathematical model. In many cases, the

EMAIL: savitan@ukr.net; 12z@ukr.net; macko2006@ukr.net; ivan.havryliuk@gmail.com
Vitalii Savchenko ORCID: 0000-0002-3014-131X

procedure for developing a model is to compile mathematical equations based on physical laws. Usually these laws are formulated in the language of differential equations. As a result, the coordinates of the state of the system and its parameters are interconnected, which allows us to begin to solve differential equations under different initial conditions and parameters.

2. Related works

In the article [1] the definition of the clustering coefficient in the case of (binary and weighted) directional networks is extended and the expected value for random graphs is calculated. In [2], it is noted that the properties of the small world of neighboring connections are higher than in comparative random networks. If a node has one or no neighbors, in such cases the local clustering is traditionally set to zero, and this value affects the global clustering factor. It is proposed to include the coefficient θ for isolated nodes in order to estimate the clustering coefficient, except in cases from the determination of Watts and Strogats. In [3] a method of determining trust and protection of personal data in social networks was developed. In article [4-6] the clustering coefficients for social networks, including power ones, are considered. In [7], a comparison of different generalizations of the clustering coefficient and local efficiency for weighted undirected graphs is made. In the article [8] the analysis of the clustering coefficient on the social network twitter is carried out. In [9], an analysis of the clustering coefficient through triads of connections was performed. In the article [10] the dependence between the clustering coefficient and the average path length in a social network is investigated. In [11,13] the use of clustering methods of social networks for personalization of educational content is investigated. The article [12,15] discusses the behavior of the clustering coefficient for complex networks. In [14], it was concluded that based on the results of the experiment, it can be concluded that among the clustering algorithms there is no universal algorithm that would be significantly ahead of others on all data sets. The leaders of benchmarking are the algorithms Spinglass and Walktrap. From the considered analysis of the works, it can be concluded that currently the protection of users in social networks is considered primarily as a technical problem that does not take into account the structural parameters of the network and its topological features. This emphasizes the relevance of the topic of work regarding the construction of a protection system based on structural parameters, taking into account network clustering.

3. Formulation of the research task

It is necessary to investigate the dynamic system of information protection in the social network (SN) from the clustering factor. Carry out modeling of a nonlinear protection system taking into account the clustering factor in SN. Investigate the stability of the protection system in the SN.

4. Main part

4.1. Nonlinear solution of the protection system in the SN, taking into account the action of a specific parameter - the clustering factor

Analysis of graphical dependences of a linear system [3] indicates the nonlinearity of the system. Therefore, in the system of equations (1) we introduce nonlinear components (2):

$$\begin{cases} \frac{dI}{dt} = Z_p Z + (C_v + C_K) I \\ \frac{dZ}{dt} = -\left(\frac{\sum_{v \in V} C_{v1}}{N^2}\right) - I(C_{d2} + C_{d1}) \end{cases} \quad (1)$$

where: $\sum_{v \in V} C_{v1}$ − the total number of connections in the network, N − the number of vertices in the network.

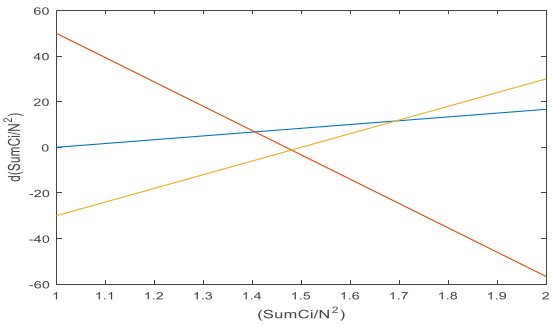


Figure 1: Differential of the clustering coefficient function

$$\begin{cases} \frac{dI}{dt}=Z_p Z+(C_v+C_K)I+L_2(I^2)+L_3(I^3)+... \\ \frac{dZ}{dt}=-(\frac{\sum_{v\in V} C_{v1}}{N^2})-I(C_{d2}+C_{d1})+K_2(Z^2)+K_3(Z^3)+... \end{cases} \quad (2)$$

where: L_2, L_3, etc. K_2, K_3, etc. some linear operators. We consider the nonlinearity of the system to be weak, which allows us to find a solution for each equation of the system (2) by the method of successive approximation, putting:

$$I = I_1 + I_2 + I_3...$$

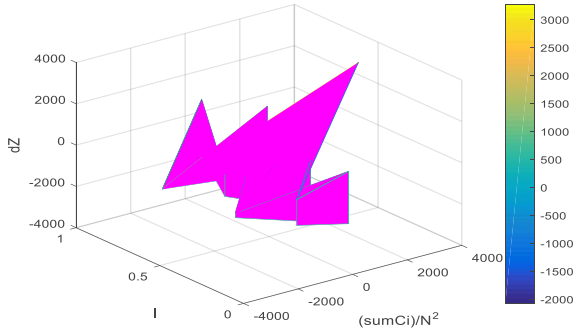


Figure 2: Differential of protection function

Since the differential of the protection function has a positive value in some data domains (the requirement of Lyapunov's theorem for this domain is not fulfilled), an additional study of the stability of the protection system within the operating parameters is required

$$Z = Z_1 + Z_2 + Z_3 + ...$$

Let at

$$dI = 0,\ \frac{dI}{dt} = 0, \text{ and } dZ = 0,\ \frac{dZ}{dt} = 0$$
$$I = I_0 \operatorname{Sin} \omega t, Z = Z_0 \operatorname{Sin} \omega t$$

We obtain a system of equations:

$$\begin{cases} \frac{dI}{dt}=Z_p Z+(C_v+C_K)I-L_2(I_0^2 \operatorname{Sin}^2 \omega t)- \\ -L_3(I_0^3 \operatorname{Sin}^3 \omega t)-... \\ \frac{dZ}{dt}=-(\frac{\sum_{v\in V} C_{v1}}{N^2})-I(C_{d2}+C_{d1})-K_2(Z_0^2 \operatorname{Sin}^2 \omega t)- \\ -K_3(Z_0^3 \operatorname{Sin}^3 \omega t)-... \end{cases} \quad (3)$$

Let's rewrite the system and present it as follows:

$$\begin{cases} \frac{dI}{dt}=\alpha Z+\beta_1 I-\sum_{k=2}^{\infty} L_k I_0^k \sin^k \omega t, \\ \frac{dZ}{dt}=\beta_2 I+\gamma-\sum_{k=2}^{\infty} K_k Z_0^k \sin^k \omega t, \end{cases} \quad (4)$$

where:

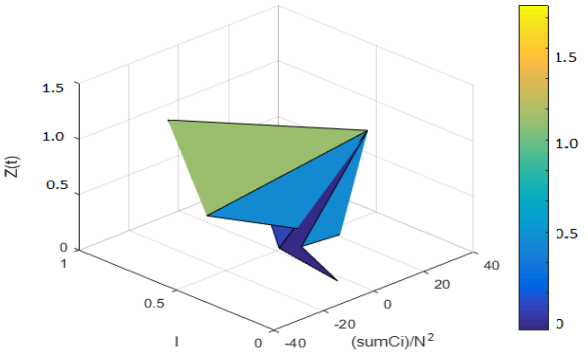
$$\alpha = Z_p, \beta_1 = C_v + C_K, \beta_2 = -\left(C_{d2}+C_{d1}\right), \gamma = -\left(\frac{\sum_{v\in V} C_{v1}}{N^2}\right)$$

Next, use the exception method:

$$\frac{dZ}{dt} = \beta_2 I + \gamma - \sum_{k=2}^{\infty} K_k Z_0^k \sin^k \omega t \Rightarrow$$

$$I = \frac{1}{\beta_2}\left(\frac{dZ}{dt} - \gamma + \sum_{k=2}^{\infty} K_k Z_0^k \sin^k \omega t\right) \Rightarrow$$

$$\frac{dI}{dt} = \frac{1}{\beta_2}\left(\frac{d^2 Z}{dt^2} + \frac{1}{\omega}\sum_{k=2}^{\infty}\left(k K_k Z_0^k \sin^{k-1} \omega t \cos \omega t\right)\right) \quad (5)$$



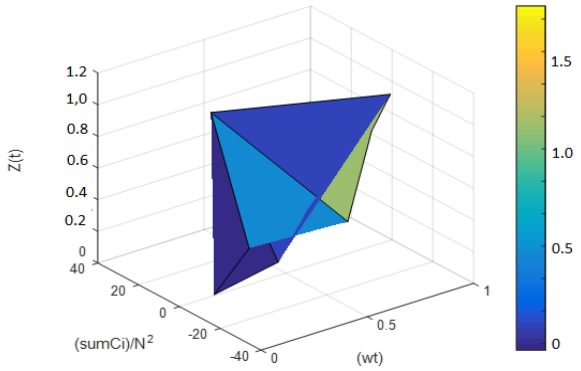


Figure3: Graphs by dependence (4)

Substitute all the found expressions (5) in the first equation of system (4):

$$= \frac{1}{\beta_2}\left(\frac{d^2Z}{dt^2} + \frac{1}{\omega}\sum_{k=2}^{\infty}\left(kK_kZ_0^k \sin^{k-1}\omega t\cos\omega t\right)\right) =$$

$$\alpha Z + \frac{\beta_1}{\beta_2}\left(\frac{dZ}{dt} - \gamma + \sum_{k=2}^{\infty} K_kZ_0^k \sin^k \omega t\right) -$$

$$- \sum_{k=2}^{\infty} L_kI_0^k \sin^k \omega t \qquad (6)$$

or:

$$\frac{d^2Z}{dt^2} - \beta_1\frac{dZ}{dt} - \alpha\beta_2 Z =$$

$$-\frac{1}{\omega}\sum_{k=2}^{\infty}\left(kK_kZ_0^k \sin^{k-1}\omega t\cos\omega t\right) -$$

$$-\beta_1\gamma + \beta_1\sum_{k=2}^{\infty} K_kZ_0^k \sin^k \omega t -$$

$$-\beta_2\sum_{k=2}^{\infty} L_kI_0^k \sin^k \omega t \qquad (7)$$

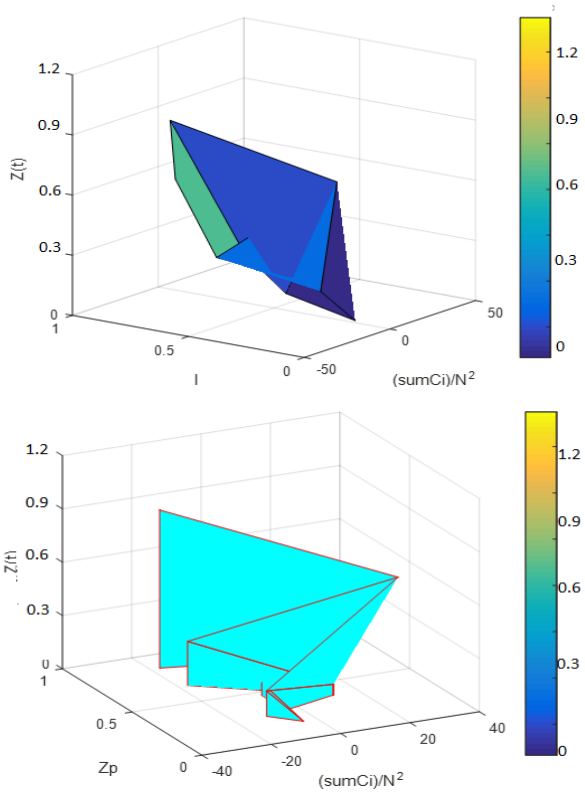


Figure 4: Graphs by dependence (5)

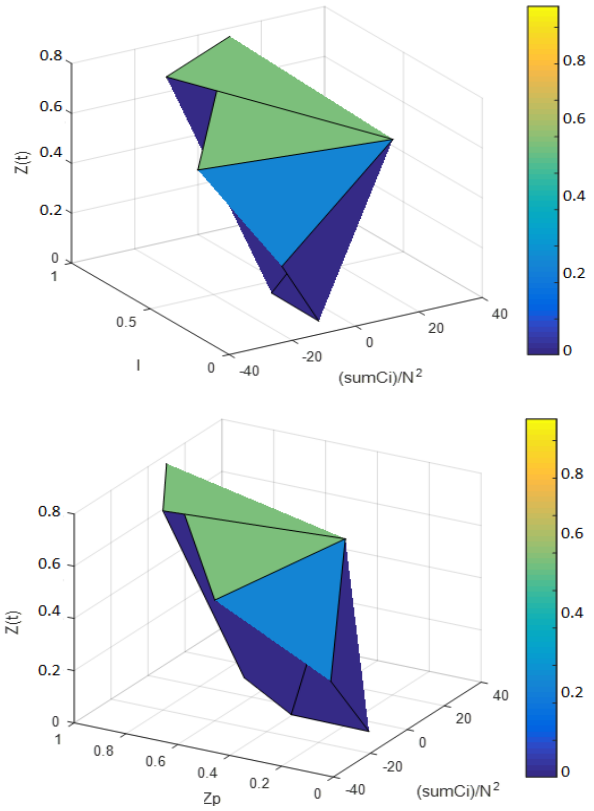


Figure 5: Graphs by dependence (7)

Now we find a common solution of the corresponding homogeneous equation:

$$Z'' - \beta_1 Z' - \alpha\beta_2 Z = 0 \qquad (8)$$

The characteristic equation has the form: $\lambda^2 - \beta_1\lambda - \alpha\beta_2 = 0$. Consider the case of the positive discriminant of this equation:

$$D = \beta_1^2 + 4\alpha\beta_2 > 0 \Rightarrow \lambda_{1,2} = \frac{\beta_1 \pm \sqrt{\beta_1^2 + 4\alpha\beta_2}}{2} \qquad (9)$$

From:

$$Z_{одн}(t) = c_1 e^{\frac{\beta_1 + \sqrt{\beta_1^2 + 4\alpha\beta_2}}{2}t} + c_2 e^{\frac{\beta_1 - \sqrt{\beta_1^2 + 4\alpha\beta_2}}{2}t}$$

joint solution of a homogeneous equation.

To find the general solution of the inhomogeneous equation we use the method of variation of arbitrary constants:

$$Z_{одн}(t) = c_1(t) e^{\frac{\beta_1 + \sqrt{\beta_1^2 + 4\alpha\beta_2}}{2}t} + c_2(t) e^{\frac{\beta_1 - \sqrt{\beta_1^2 + 4\alpha\beta_2}}{2}t}$$

where: $c_1'(t), c_2'(t)$ are from the system:

$$\begin{cases} c_1'(t)e^{\frac{\beta_1+\sqrt{\beta_1^2+4\alpha\beta_2}}{2}t}+c_2'(t)e^{\frac{\beta_1-\sqrt{\beta_1^2+4\alpha\beta_2}}{2}t}=0, \\ c_1'(t)\frac{\beta_1+\sqrt{\beta_1^2+4\alpha\beta_2}}{2}e^{\frac{\beta_1+\sqrt{\beta_1^2+4\alpha\beta_2}}{2}t}+ \\ +c_2'(t)\frac{\beta_1-\sqrt{\beta_1^2+4\alpha\beta_2}}{2}e^{\frac{\beta_1-\sqrt{\beta_1^2+4\alpha\beta_2}}{2}t}=N(t), \end{cases}$$

where:

$$N(t)=-\frac{1}{\omega}\sum_{k=2}^{\infty}\left(kK_kZ_0^k\sin^{k-1}\omega t\cos\omega t\right)- \\ -\beta_1\gamma+\beta_1\sum_{k=2}^{\infty}K_kZ_0^k\sin^k\omega t- \tag{11}$$

From equations (10, 11) we obtain:

$$c_1'(t)e^{\frac{\beta_1+\sqrt{\beta_1^2+4\alpha\beta_2}}{2}t}=-c_2'(t)e^{\frac{\beta_1-\sqrt{\beta_1^2+4\alpha\beta_2}}{2}t}\Rightarrow \\ \Rightarrow c_2'(t)e^{\frac{\beta_1-\sqrt{\beta_1^2+4\alpha\beta_2}}{2}t}\left(-\frac{\beta_1+\sqrt{\beta_1^2+4\alpha\beta_2}}{2}+\frac{\beta_1-\sqrt{\beta_1^2+4\alpha\beta_2}}{2}\right)=N(t) \tag{12}$$

or:

$$c_2'(t)e^{\frac{\beta_1-\sqrt{\beta_1^2+4\alpha\beta_2}}{2}t}\sqrt{\beta_1^2+4\alpha\beta_2}=-N(t) \tag{13}$$

where will we get:

$$c_2(t)=-\frac{1}{\sqrt{\beta_1^2+4\alpha\beta_2}}\int N(t)e^{\frac{-\beta_1+\sqrt{\beta_1^2+4\alpha\beta_2}}{2}t}dt \tag{14}$$

$$c_1(t)=\frac{1}{\sqrt{\beta_1^2+4\alpha\beta_2}}\int N(t)e^{\frac{-\beta_1-\sqrt{\beta_1^2+4\alpha\beta_2}}{2}t}dt \tag{15}$$

Given (13,14,15) we have:

$$Z(t)=\int(N(t)-e^{\frac{-\beta_1-\sqrt{\beta_1^2+4\alpha\beta_2}}{2}t}\frac{e^{\frac{\beta_1+\sqrt{\beta_1^2+4\alpha\beta_2}}{2}t}}{\sqrt{\beta_1^2+4\alpha\beta_2}})dt- \\ -\int(N(t)-e^{\frac{-\beta_1-\sqrt{\beta_1^2+4\alpha\beta_2}}{2}t}\frac{e^{\frac{\beta_1-\sqrt{\beta_1^2+4\alpha\beta_2}}{2}t}}{\sqrt{t\beta_1^2-4\alpha\beta_2}})dt, \tag{16}$$

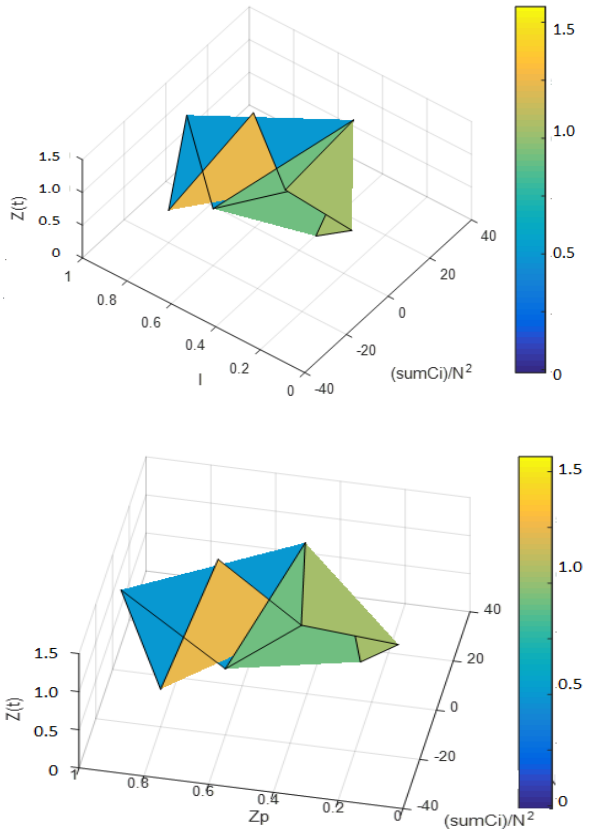


Figure 6: Graphs by dependence (16)

3.2. Define the phase portrait of the data protection system

Initial equation:

$$\frac{d^2Z}{dt^2}-\beta_1\frac{dZ}{dt}-\alpha\beta_2Z=-\frac{1}{\omega}\sum_{k=2}^{\infty}\left(kK_kZ_0^k\sin^{k-1}\omega t\cos\omega t\right)- \\ -\beta_1\gamma+\beta_1\sum_{k=2}^{\infty}K_kZ_0^k\sin^k\omega t-\beta_2\sum_{k=2}^{\infty}L_kI_0^k\sin^k\omega t \tag{17}$$

The solution will be implemented in the program MatLab / Multisim. Let's make the scheme (Fig. 7).

The phase portrait is presented in the form of an ellipse, which indicates the stability of the personal data protection system.

The results of the program are presented in Fig. 8, 9.

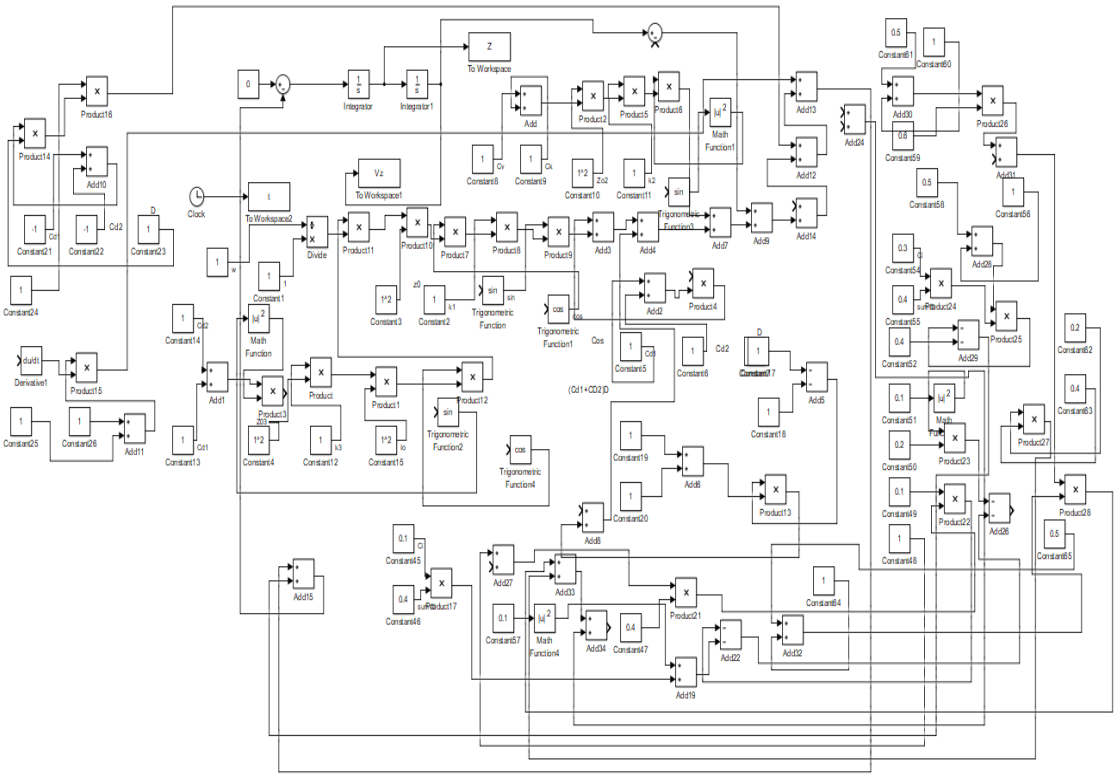


Figure 7: Block diagram of the phase portrait program in the Multisim program, taking into account the attack block

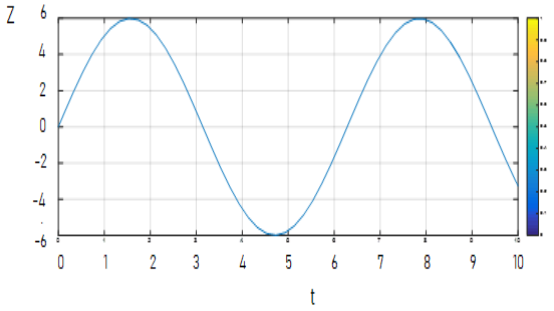


Figure 8: Harmonic oscillations of the protection system on time Z=f(t)

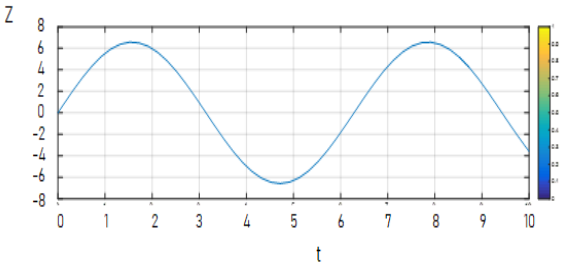


Figure 10: Harmonic oscillations of the protection system on time Z=f(t) taking into account the attacks

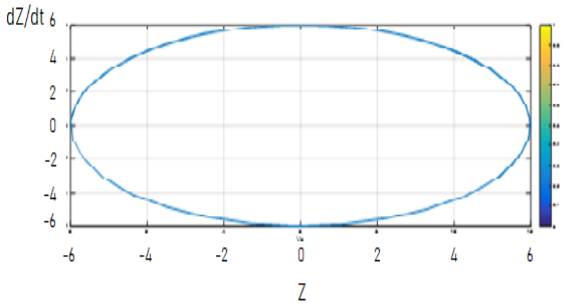


Figure 9: Phase portrait of the protection system on clustering factor

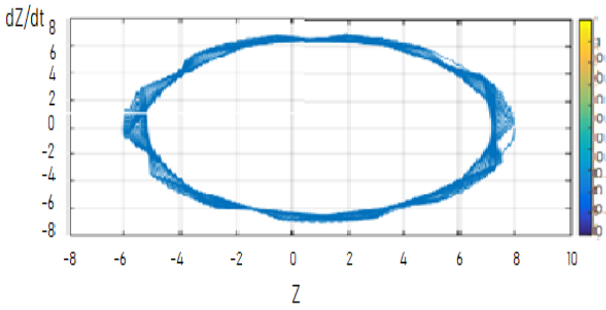


Figure 11: Phase portrait of the protection system on clustering factor taking into account the attacks

5. Analysis of the obtained results

In contrast to previous research by scientists, it has been proven that the SN protection system is stable even from external maximum influences and a specific parameter of the clustering coefficient in the operating range of parameters.

6. Conclusions

For the first time in the article the dynamic model of the information protection system in social networks is investigated taking into account the clustering coefficient, and also the analysis of the stability of the protection system is carried out. A nonlinear equation of information protection is obtained. It is shown that the protection index changes depending on the clustering coefficient. Phase portraits of the protection system are obtained, which indicate the resistance of the system to external influences and the clustering coefficient in SN.

7. References

[1] Giorgio Fagiolo. Clustering in complex directed networks. Phys Rev E Stat Nonlin Soft Matter Phys. . 2007 Aug;76(2 Pt 2):026107. doi: 10.1103/PhysRevE.76.026107. Epub 2007 Aug 16.

[2] Marcus Kaiser (2008). Mean clustering coefficients: the role of isolated nodes and leafs on clustering measures for small-world networks. New Journal of Physics 10 (8): 083042. Bibcode:2008NJPh...10h3042K. arXiv:0802.2512. doi:10.1088/1367-2630/10/8/083042.

[3] O. Laptiev, V. Savchenko, A. Kotenko, V. Akhramovych, V. Samosyuk, G. Shuklin, A. Biehun. Method of Determining Trust and Protection of Personal Data in Social Networks. International Journal of Communication Networks and Information Security (IJCNIS) 2021. №. 1, April 2021. Pp. 15-21.

[4] V. Savchenko, V. Akhramovych, A. Tushych, I. Sribna, I. Vlasov. Analysis of Social Network Parameters and the Likelihood of its Construction. International Journal of Emerging Trends in Engineering Research (IJETER). ISSN: 2347 – 3983, Vol. 8. No. 2, February 2020. pp. 271 – 276.

[5] P. Shchypanskyi, V. Savchenko, V. Akhramovych, T. Muzshanova, S. Lehominova, V. Chegrenets. The Model of Secure Social Networks Activity Based on Graph Theory. International Journal of Innovative Technology and Exploring Engineering (IJITEE). ISSN: 2278–3075, Vol. 9. Issue 4, February 2020, pp. 1803 – 1810.

[6] V. Akhramovych Degree social networks. Colloquium-journal. Warszawa, Polska. 2020. № 5 (57). pp. 27 – 29. http://www.colloquium-journal.org.

[7] Yui Van, Eshvar Humare, Rik Vandenberhe, Patrik Diupon (2017). Comparison of various generalizations of clustering coefficient and local efficiency for weighted undirected graphs. Neural computing. 29 (2): 313–331. doi : 10.1162 / NECO_a_00914 . Retrieved 8 August 2020.

[8] M. Gracheva, Y. Iakobi, V. Stepanenko, Y. Luneva. Analysis of the characteristics of social graphs built according to the data of the social network Twitter. gramar_98.98@mail.ru.

[9] I. Evin. Introduction to the theory of complex networks. Computer research and modeling. 2010 T. 2 № 2 P. 121–141.

[10] I. Zharinov, V. Krylov. Constructing graphs with minimum average path length. Bulletin of Izhevsk State Technical University. №4, 2008. P. 164–169.

[11] H. Mamedova, F. Agaev, L. Zeinalova. Using social media to personalize e-learning. İnformasiya texnologiyaları problemləri, 2019, №1, 27–34.

[12] J. Pavlov, I. Chepliukova. On the asymptotics of the power structure of configuration graphs with constraints on the number of edges. Discrete Math, 2018. T. 30. Issue. 1. P. 77–94.

[13] V. Starodubtsev. Personalization of the virtual educational environment. Pedagogical Education in Russia, 2015, №7, p.24–29.

[14] M. Firsov. Benchmarking graph clustering algorithms for decision-making problems. Basic research. – 2017. – № 12 (part 1) – C. 138-142.

[15] J. Pavlov. On the asymptotics of the cluster coefficient of a configuration graph with an unknown distribution of vertex degrees. Information and its application, 2019, T 13, issue 3, 9–13.

Modification of query processing methods in distributed databases using fractal trees

Olha Svynchuk[1], Andrii Barabash[2], Serhii Laptiev[3] and Tetiana Laptieva[4]

[1,2]*National Technical University of Ukraine «Igor Sikorsky Kyiv Polytechnic Institute», Politehnichna str. 56, 5, Kyiv, 03056, Ukraine*
[3,4]*Taras Shevchenko National University of Kyiv, Volodymyrska str. 64/13, Kyiv, 01601, Ukraine,*

Abstract

Today in database management systems there is an acute problem of searching for data in large data sets. To solve this problem, we propose a modified search tree and its improvement using a fractal index search tree with a multilevel structure. Each level in such a structure is a separate fractal tree. Algorithms for data processing in DBMS RAM by modified methods are described. These methods can be used to search for the same data from different tables. Increased the minimum filling of the node, which reduces the height of the tree. The symmetry of the fractal tree helps to execute the query quickly and, as a result, reduce the number of requests to the disk subsystem. Also, due to the self-similarity property, the most frequently used indexes will be loaded into the DBMS RAM much faster after selection. This will speed up the process of finding the information you need for the request. Loading data indexes into RAM based on statistics on the frequency of use of indices and index size weights will reduce the number of indexes that are loaded into RAM, in contrast to the classic loading where the loading of indexes occurs during their use and after filling the memory, it is deleted. Another big advantage is that indexes that are almost never used will not be loaded into RAM. The proposed approach with fractal trees also has an important scaling property, as fractal trees are divided into a large number of smaller trees, which is especially true in the era of multicore modern computer systems. To study the effectiveness of the use of indexes based on a modified fractal search tree in the database and select the best system for hosting the database server, we measured the speed of information retrieval in tables for the Windows 10 operating system. During the experiments it was shown that the search speed on the modified trees in comparison with the modified fractal search tree is reduced by 12%.

Keywords

database, data search, B + -trees, modified trees, fractal trees, indexes

1. Introduction

In today's world we can see a rapid increase in information, which complicates the process of its storage and management. Therefore, for its organization and quick search using databases (DB), which are organized according to the concept that describes the characteristics of this data. In modern information systems for high-quality work with databases use DBMS database management systems that provide the ability to create, store, update and search for the necessary information. DBMSs also provide a number of useful services: schema to control data semantics, query language to organize access to part of the database, data granulation, data integrity management, compression to reduce database size, indexing to speed up query processing. However, the integration of different databases into the production process at enterprises and other institutions has a number of shortcomings associated with the organization of their management and monitoring of events in databases [1-5].

In modern databases, an important element is the search for data in tables that contain many rows and columns and are not always ordered. Therefore, to implement a quick search, indexes are created that are formed from the values of one

EMAIL: 7011990@ukr.net (A. 1); andrew.barbsh@gmail.com (A. 2); Salaptiev@gmail.com (A. 3) tetiana1986@ukr.net (A.4)
ORCID: 0000-0001-9032-6335 (A. 1); 0000-0001-8433-2827 (A. 2); 0000-0002-7291-1829 (A. 3): 0000-0002-5223-9078 (A. 4)

or more columns and pointers to the corresponding rows. Indexes allow you to avoid sequential or step-by-step browsing of the file in search of the desired data. They are ordered, each element of the index contains the name of the searched object and a pointer-identifier of its location. The more indexes, the better the performance of database queries, but a very large number of indexes does not guarantee high performance [5-10].

Many databases use different trees and their modifications to build such indexes. However, if the tree has an insufficient number of nodes and their fullness, the data search time increases [11-13]. The disadvantages may also be the use of identical indexes for different tables and sending to the RAM of indexes that are rarely used [14-15].

The base trees in index construction and data retrieval are B-trees, namely their type B + trees. These trees easily implement the independence of the program from the structure of the information record, have the ability to sequential access and all key data are contained only in the sheets. The main disadvantages of such trees are the compactness of filling and the number of levels of trees [16-18].

You can also select K-trees, which contain all the characteristics of the B + tree, but have a better strategy of splitting and merging nodes. Also, these trees have more elements at the root of the node and the fullness of the node is ¾. All this saves hard disk space and increases the speed of access to information [19-20].

However, the index structures used in modern databases have some limitations due to the long process of restructuring the index structure in the case of adding or removing new data. Accordingly, this leads to a slow process of searching for information in a database with large data sets.

The aim of the article is to improve the process of processing indexes in databases using fractal trees and speed up query execution.

2. Modified search tree

The existing mechanisms of data modification in the tables have a certain feature - the change of keys in the corresponding nodes of the tree is performed with the subsequent restructuring of the index. This significantly affects the speed of writing information to the database and, accordingly, is an important factor in increasing the number of queries to the database. You also need to store only the most frequently used indexes, then, accordingly, the access time to the data storage location will be reduced. Therefore, the existing methods need to be improved, which will allow to find the necessary information faster [21-22].

In the + tree we will improve as follows:

- increase the minimum filling of the node, which will reduce the height of the tree;
- change the rule of separating the nodes of the tree - splitting the node with its two neighbors into four new nodes;
- change the rule of connecting tree nodes - connecting four nodes into three new nodes;
- in the tree leaf we will store records of links to the same fields in different tables, which will increase the time of receipt of links to data in the tree and speed up the search.

We describe the search for data using indexes. Indexes are loaded into the RAM of the database after receiving the request. Next, a list of data is formed, which contains the necessary information, and the found data is sent to RAM. However, in the classical algorithm for loading indexes in the RAM are indexes that are almost not used, and, accordingly, take place until they are replaced by other indexes. Therefore, it is necessary to improve the procedure for processing indexes in the RAM of the database (Picture 1) by:

- reducing the specific storage in the RAM of indexes that are little used;
- processing little-used indexes by reading them from disk.

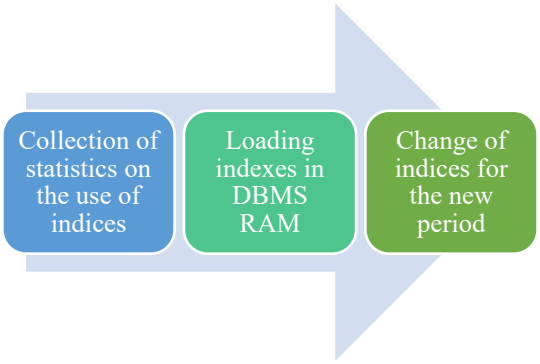


Figure 1: Algorithm for loading indexes in the DBMS RAM by hashing

Here is an algorithm for loading indexes into memory based on the index hashing method:

- DBMS loads indexes into RAM according to the classical algorithm and collects statistics on the number of used indices during Δt;
- after collecting statistics, the DBMS loads into RAM only those data that were used most often during the time period Δt;
- if there is no data in the RAM during the query, the search is performed by reading nodes from the disk index space of the database;
- if the time Δt has expired, then in RAM are loaded those indexes that are used most often and have not been loaded before.

This algorithm is implemented in two stages:

1. statistics are collected on the number of used indices for the corresponding period Δt;
2. the indices that were most often used in the previous time interval Δt are loaded into RAM.

We have a formula for calculating time:

$$\Delta t = \frac{(\sum_{i=1}^{n} k_i W_i)t}{(\sum_{i=1}^{n} W_i)k}, \quad (1)$$

where k_i – the number of used i-th index, k – the number of indexes used, W_i – the weighting factor of the i-th index, t – time of statistics collection.

Loading data indexes into RAM (figure 1) based on statistics on the frequency of use of indices and index size weights leads to a decrease in the number of indexes that are loaded into RAM, in contrast to the classic loading, where the loading of indexes occurs during their use, and after filling the memory, it is deleted. Another big advantage is that indexes that are almost never used will not be loaded into RAM.

3. A modified method of searching for queries using fractal trees

Recently, fractals are increasingly being used in various areas of our lives. Fractals can be used to model and describe various phenomena in the fields of radio engineering and electronics, digital information processing, and computer graphics [23-28].

The concept of «fractal» was proposed by the French-American mathematician Benoit Mandelbrot. In 1977, he published Fractal Geometry of Nature, describing repetitive drawings from everyday life. According to him, many geometric shapes consist of smaller shapes, which when enlarged accurately repeat a large shape. After research, he also found that fractals have chaotic behavior, fractional infinite dimension and can be described mathematically using simple algorithms.

Fractal in a more general sense means an irregular, self-similar structure, set, subsets and elements of which are similar to the set itself. Fractals can be deterministic or stochastic. They can also be classified according to self-similarity. There are three types of self-similarity in fractals: exact self-similarity (looks the same at different magnifications); almost self-similarity (fractal looks approximately (but not exactly) self-similar at different magnifications); statistical self-similarity (fractal has numerical or statistical measures that persist with magnification). Examples of fractals are the Cantor set, the Lyapunov fractal, the Serpinsky triangle, the Serpinsky carpet, the Menger sponge, the Apollonia grid, the dragon curve, and the Koch curve. Also recently, attention is paid to fractal trees: from each branch depart smaller, similar to it, from them - even smaller (figure 2). By a separate branch of mathematical methods can describe the properties of the whole tree.

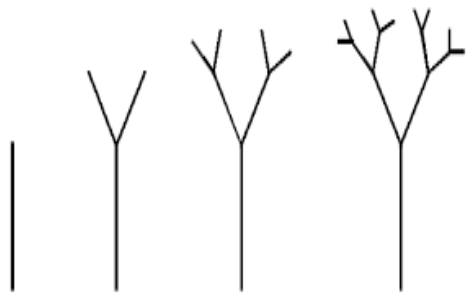


Figure 2: An example of constructing a fractal tree

To construct the structure of the indices will be used Pythagorean fractal tree - a flat fractal, consisting of interconnected right triangles of squares built on the legs and hypotenuse (figure 3).

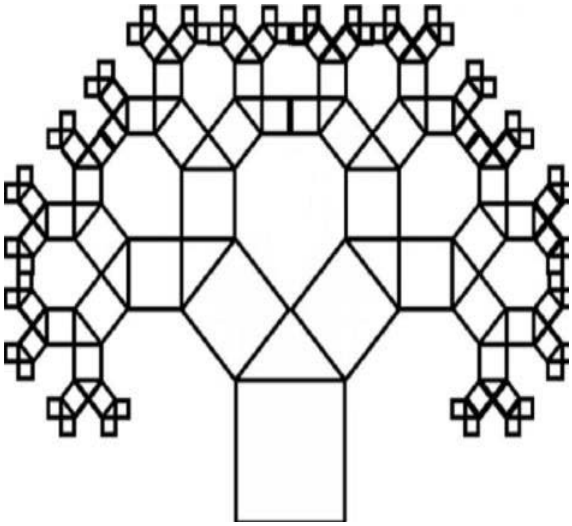


Figure 3: Pythagorean tree

The Pythagorean tree with N levels is a trunk and two Pythagorean trees with N-1 levels depart from it symmetrically, so that the length of their trunks is 2 times less and the angle between them is 90 degrees (figure 4).

The Pythagorean tree is divided into subtree blocks, where each tree is a full-fledged fractal tree. We present this subtree in the form of a new horizontal level, which complements the vertical structure of the original tree. If the new horizontal level is too large, then in order to fit into one block of the disk, it is divided into two blocks and indexed in the third horizontal level.

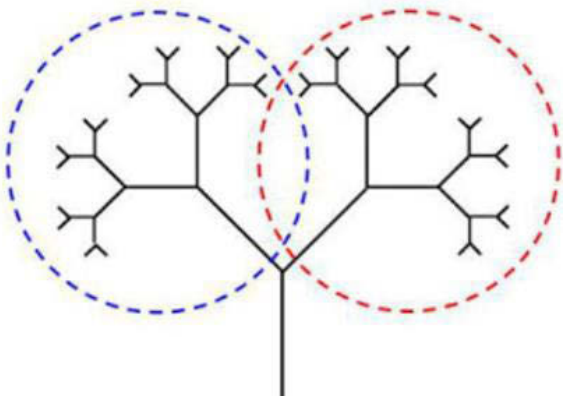


Figure 4: Pythagorean tree for 6 levels

These indexes can be easily used for large databases. The structure of such indexes is presented in the form of arrays with a length equal to powers of number 2. This structure is easily scalable for a large number of keys, and is not sensitive to the content of the entered queries.

The main advantage of using fractal trees is that the resulting structure is symmetrical and internally balanced. Symmetry helps to execute the request quickly and, as a result, there will be much fewer requests to the disk subsystem. Also, due to the self-similarity property, the most frequently used indexes will be loaded into the DBMS RAM much faster after selection. This will speed up the process of finding the information you need for the request.

The index uses a new multi-level approach - additional levels of the tree allow you to search in the data block that contains the information on request. Each request accesses the same number of levels, which provides balanced access to the index and disk subsystem.

Updating, inserting and deleting indexes can be done very efficiently. The update is performed as a sequential deletion of the old key, followed by the insertion of a new key value. Inserting a key into a fractal tree involves adding one new node or adding an edge to an existing node. Inserting requires changes to only one block at level 1. First, look for a block to update - if the block is crowded, it must be divided, and this leads to the creation of a new node in level 2. Separation of blocks is very rare and does not affect performance.

To study the effectiveness of indexes based on a modified fractal search tree in the database and choose the best system for hosting the database server, we measured the speed of information retrieval in tables for Windows 10. Experiments show that the search speed of modified trees compared to modified fractal search tree is reduced by 12% (Picture 5).

The average error of the result for the modified search tree is 0.91%, and for the modified fractal search tree is 0.89%. Therefore, the experiments are performed correctly and provide the results with a given accuracy.

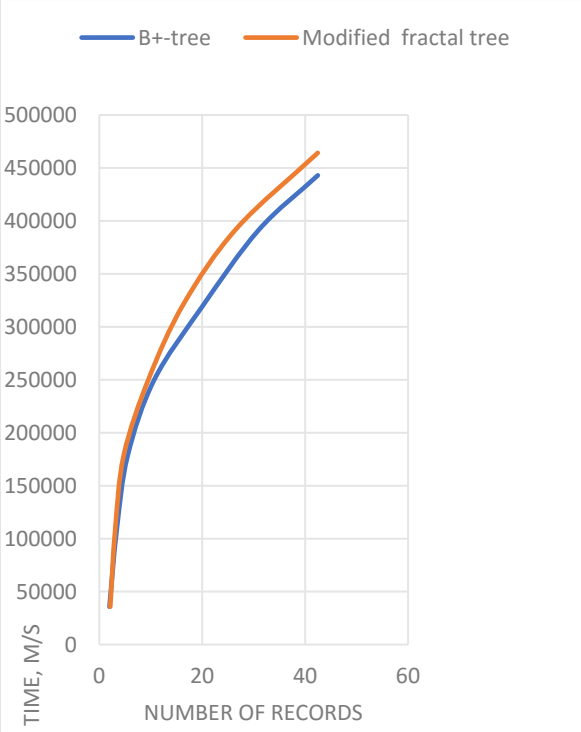


Figure 5: Comparison of query search speed for modified tree and modified fractal tree

4. Conclusions

New methods of index processing in databases for speeding up information processing are offered. The developed modified methods differ from the known methods of processing queries in databases in that they can be used for a large amount of information. Loading data indices into RAM based on statistics on the frequency of use of indices and index size weights leads to a decrease in the number of indexes that are loaded into RAM. A modification of the data processing algorithm in RAM has been performed, which has made it possible to exclude indexes that are rarely used in memory. The resulting structure is balanced and optimized for storage in the disk subsystem, reduces the number of I / O operations to a minimum. The method of constructing indexes based on a modified fractal tree allows to increase the data search speed by 12% compared to the modified method of index search based on a classic B + tree. The proposed approach also has an important property of scaling, as fractal trees are divided into a large number of smaller trees, which is especially true in the era of multicore modern computer systems.

Prospects for further research are seen in the creation of new methods for processing queries in distributed databases based on index hashing using fractal trees.

5. References

[1] V.A. Mashkov, O.V. Barabash, Self-Testing of Multimodule Systems Based on Optimal Check-Connection Structures. Engineering Simulation. Amsterdam: OPA, 13 (1996) 479-492.

[2] V.A. Mashkov, O.V. Barabash, Self-checking and Self-diagnosis of Module Systems on the Principle of Walking Diagnostic Kernel. Engineering Simulation. Amsterdam: OPA, 15 (1998) 43-51.

[3] O. Barabash, G. Shevchenko, N. Dakhno, O. Neshcheret, A. Musienko, Information Technology of Targeting: Optimization of Decision Making Process in a Competitive Environment. International Journal of Intelligent Systems and Applications. Hong Kong: MECS Publisher, 9 (12) (2017) 1-9.

[4] O.V. Barabash, P.V. Open'ko, O.V. Kopiika, H.V. Shevchenko, N.B. Dakhno, Target Programming with Multicriterial Restrictions Application to the Defense Budget Optimization. Advances in Military Technology, 14(2) (2019) 213-229.

[5] V. Sobchuk, O. Barabash, A. Musienko, O. Svynchuk, Adaptive accumulation and diagnostic information systems of enterprises in energy and industry sectors. 1st Conference on Traditional and Renewable Energy Sources: Perspectives and Paradigms for the 21st Century (TRESP 2021), Volume 250, 09 April 2021. doi.org/10.1051/e3sconf/202125008002

[6] H. Zhenbing, V. Mukhin, Ya. Kornaga, O. Herasymenko, Y. Bazaka, The scheduler for the grid system based on the parameters monitoring of the computer components. Eastern European Journal of Enterprise Technologies, 1 (2017) 31-39.

[7] V. Savchenko, O. Ilin, N. Hnidenko, O. Tkachenko, O. Laptiev, S. Lehominova, Detection of Slow DDoS Attacks based on User's Behavior Forecasting. International Journal of Emerging Trends in Engineering Research (IJETER) 8(5) (2020) 2019-2025.

[8] O. Laptiev, O. Stefurak, I. Polovinkin, O. Barabash, V.Savchenko, O. Zelikovska. The method of improving the signal detection quality by accounting for interference. 2020 IEEE 2nd International Conference on

Advanced Trends in Information Theory (IEEE ATIT 2020) Conference Proceedings Kyiv, Ukraine, November 25-27, pp.172-176.

[9] V. Tkachov, V.Tokariev, Y. Dukh, V. Volotka, Method of Data Collection in Wireless Sensor Networks Using Flying Ad Hoc Network. 2018 5th International Scientific-Practical Conference Problems of Infocommunications. Science and Technology, October 9-12, 2018 Kharkiv, Ukraine, pp. 197-201.

[10] K. Smelyakov, S. Smelyakov, A. Chupryna Advances in Spatio-Temporal Segmentation of Visual Data. Chapter 1. Adaptive Edge Detection Models and Algorithms. Series Studies in Computational Intelligence (SCI), volume 876, publisher Springer, Cham, 2020, pp. 1-51.

[11] S. Yevseiev, R. Korolyov, A. Tkachov, O. Laptiev, I. Opirskyy, O. Soloviova, Modification of the algorithm (OFM) S-box, which provides increasing crypto resistance in the post-quantum period. International Journal of Advanced Trends in Computer Science and Engineering (IJATCSE) 9(5) (2020) 8725-8729.

[12] O. Barabash, O. Laptiev, O. Kovtun, O. Leshchenko, K. Dukhnovska, A. Biehun, The Method dynavic TF-IDF. International Journal of Emerging Trends in Engineering Research (IJETER), 8(9) (2020) 5713-5718.

[13] O. Laptiev, V.Savchenko, S. Yevseiev, H. Haidur, S. Gakhov, Spartak Hohoniants, The new method for detecting signals of means of covert obtaining information. 2020 IEEE 2nd International Conference on Advanced Trends in Information Theory (IEEE ATIT 2020) Conference Proceedings Kyiv, Ukraine, November 25-27, pp.176 –181.

[14] V. Sobchuk, V. Pichkur, O. Barabash, O. Laptiev, I.Kovalchuk, A. Zidan, Algorithm of control of functionally stable manufacturing processes of enterprises. 2020 IEEE 2nd International Conference on Advanced Trends in Information Theory (IEEE ATIT 2020) Conference Proceedings Kyiv, Ukraine, November 25-27, pp. 206-211.

[15] V. Savchenko, O. Laptiev, O. Kolos, R. Lisnevskyi, V. Ivannikova, I. Ablazov, Hidden Transmitter Localization Accuracy Model Based on Multi-Position Range Measurement. 2020 IEEE 2nd International Conference on Advanced Trends in Information Theory (IEEE ATIT 2020) Conference Proceedings Kyiv, Ukraine, November 25-27, pp.246-251.

[16] Z. Hu, V. Mukhin, Ya. Kornaga, O. Herasymenko, Y. Mostoviy, The Analytical Model for Distributed Computer System Parameters Control Based on Multi-factoring Estimations. Journal of Network and Systems Management, 27(2) (2019) 351-365.

[17] O. Barabash, O. Laptiev, V. Tkachev, O. Maystrov, O. Krasikov, I. Polovinkin, The Indirect method of obtaining Estimates of the Parameters of Radio Signals of covert means of obtaining Information. International Journal of Emerging Trends in Engineering Research (IJETER), 8(8) (2020) 4133-4139.

[18] S. Yevseiev, R. Korolyov, A. Tkachov, O. Laptiev, I. Opirskyy, O. Soloviova, Modification of the algorithm (OFM) S-box, which provides increasing crypto resistance in the post-quantum period. International Journal of Advanced Trends in Computer Science and Engineering (IJATCSE) 9(5) (2020) 8725-8729.

[19] M. Pratsiovytyi, O. Svynchuk, Spread of values of a Cantor-type fractal continuous nonmonotone function. Journal of Mathematical Sciences, 240(3) (2019) 342-357. doi.org/10.1007/s10958-019-04354-0

[20] O. Laptiev, G. Shuklin, O.Stefurak, O. Svynchuk, O. Urdenko, S. Hohoniants, Method of the increasing the detection system and recognition of digital radiosignals. Wschodnioeuropejskie Czasopismo Naukowe, East European Scientific Journal, 2 (54) (2020) 4-16.

[21] O. Svynchuk, O. Barabash, J. Nikodem, R. Kochan, O. Laptiev, Image compression using fractal functions Fractal and Fractional, 5(2), (2021) 31.

[22] O.V. Barabash, A.P. Musienko, V.V. Sobchuk, N.V. Lukova-Chuiko, O.V. Svynchuk, Distribution of Values of Cantor Type Fractal Functions with Specified Restrictions. Chapter in Book “Contemporary Approaches and Methods in Fundamental Mathematics and Mechanics”. Editors Victor A. Sadovnichiy, Michael Z. Zgurovsky. Publisher Name: Springer, Cham, Switzerland AG 2021, pp. 433-455. doi.org/10.1007/978-3-030-50302-4_21

Detection of Slow DDoS Attacks based on Time Delay Forecasting

Vitalii Savchenko[1], Valeriia Savchenko[2], Oleksandr Laptiev[3], Oleksander Matsko[4], Ivan Havryliuk[5], Kseniia Yerhidzei[6] and Iryna Novikova[7]

[1,2,3] *State University of Telecommunications, Solomianska str.7, Kyiv, 03110, Ukraine*
[4,5,6,7] *The National Defense University of Ukraine named after Ivan Cherniakhovskyi, Povitroflotsky av. 28, Kyiv, 03049, Ukraine*

Abstract

The article deals with the problem of detecting low and slow distributed DDoS attacks. Detecting such DDoS attacks is challenging because slow attacks do not significantly increase traffic. The authors suggest that detecting slow DDoS attacks will be effective based on analyzing and predicting host response latency in the network. The article proposes an original method for detecting such attacks, based on statistics of host interaction and predicting the individual trajectory of the traffic parameter behavior. The host response time delay is taken as a traffic parameter. An algorithm for calculating the individual trajectory of the time delay is proposed. The possibilities of using this method are shown based on the simulation of RUDY attacks on HTTP services. The parameters of the forecast accuracy are investigated depending on the accumulated information on the response delays.

Keywords

Slow and low DDoS attack**s**, slow attack detection, network response prediction, latency, individual trajectory**.**

1. Introduction

Recently, DDoS attacks are rapidly increasing in scale, frequency and technical complexity. For organizations that rely on Internet resources and applications for their activities (for example, for e-commerce enterprises), the consequences of DDoS attacks can be devastating. Inaccessible websites and servers can cast a shadow on a company's reputation and customers turn to competitors' resources [1].

One type of DDOS attack is slow denial of service attacks. Their feature is that denial of service is achieved in a hidden way using a small amount of traffic and does not require bandwidth filling. The attacker opens many endless connections and, when a certain threshold is exceeded, causes a denial of service in the victim's network. It uses transport (TCP) or application (HTTP) protocols. Detection and countermeasures must be built based on the characteristics of the attack.

Countering such attacks should include two main measures: 1) diagnose the attack at the earliest stages; 2) separate malicious traffic from normal traffic. By understanding which user requests are the result of a DDoS attack, you can configure appropriate settings for firewalls, routers, or implement other security measures.

1.1. Problem Statement

Methods for detecting slow DDoS attacks fall into two categories:

1. Signature methods, which are based on the construction of a model of "abnormal behavior" [2]. This model builds signatures of "abnormal" traffic behavior (a huge number of simultaneously arriving SYN + ACK packets, an inadequately long packet lifetime, too long a packet route "length", and so on). The model is most effective against attacks that fill the network bandwidth, or on local networks, where you can make a list of source addresses whose packets are guaranteed to be "normal". But such a model is ineffective

EMAIL: savitan@ukr.net; savchenko.valeriya@gmail.com (A.2); alaptev64@ukr.net (A.3); macko2006@ukr.net (A.4); ivan.havryliuk@gmail.com (A.5); ergidzey@ukr.net (A.6); irina_nov@ukr.net (A.7)
ORCID: 0000-0002-3014-131X

against low-intensity DDoS, when it is difficult to reliably distinguish ordinary user requests from “malicious” ones.

2. Based on anomalies. This method is the opposite of signature. A general model of "normal" behavior is built, then the incoming traffic is compared with it, and if the differences exceed an acceptable threshold, an "alarm" is triggered. Research is conducted in the areas of statistical (parametric and nonparametric) methods, as well as data mining and neural networks. The last two approaches are being actively developed to detect low-intensity attacks. Disadvantages of the model: a large number of errors of the first kind due to the individuality of networks and traffic; long-term calculation of data on "normal" behavior; sensitive to the choice of statistical distributions.

In any case, the problem of early detection of low or slow DDoS attacks remains relevant. The sooner the traffic parameters are found to be inconsistent with their normal values, the faster it will be possible to take measures to neutralize the attack. In this case, it is necessary to add parameter prediction modules to the existing detection systems.

1.2. Related Works Overview

There is a huge number of publications on the detection of slow DDoS attacks.

Reference [3] proposes an architecture that mitigates low and slow DDoS attacks by leveraging the capabilities of a software-defined infrastructure. At the same time, this approach requires a significant amount of computing resources, which will be involved in diagnostics.

The article [4] proposes a methodology for detecting LDDoS attacks based on the characteristics of malicious TCP streams by classifying them by decision trees. The studies are conducted using a combination of two datasets, one generated from a simulated network and the other from a publicly available CIC DoS dataset. Since this approach includes elements of artificial intelligence, a significant amount of statistics is required to train the system.

In [5], the authors tried to measure the impact of different variants of pulsating distributed denial-of-service attacks on the self-similar nature of network traffic and see if changing the H index can be used to distinguish them from a normal network. This approach is quite effective in the case of traffic self-similarity elements. Otherwise, detecting low and slow DoS attacks is very difficult.

Paper [6] proposes Canopy, a novel approach to detecting LSDDoS attacks by using machine learning techniques to extract meaning from observed TCP state transition patterns. At the same time, as in other models based on artificial intelligence, the detection system requires a large sample of training and significant resources for processing the results.

The work [7] compares machine learning methods for recognizing slow DDoS attacks: multilayer perceptron (MLP), backpropagation neural network, K-Nearest Neighbors (K-NN), Support Vector Machine (SVM) and polynomial naive Bayesian (MNB) algorithm. As in the previous cases, the application of the methods requires a large number of patterns for recognition.

In [8-9], a new classification method and model is proposed to protect against slow HTTP attacks in the cloud. The solution detects slow HTTP header attacks (Slowloris), slow HTTP body attacks (RUDY), or slow HTTP read attacks. At the same time, such approaches do not guarantee effective detection of attacks at the early stages of their development.

The papers [10-11] show a system that can detect and mitigate attacks in the network infrastructure. The main identification parameters in both models are the packet transmission rate and the uniform distance between packets, which does not allow to forestall the actions of intruders. Reference [12] discusses sampling data to create different class distributions to counteract the effects of highly imbalanced slow HTTP DoS datasets. At the same time, a significant number of samples (the authors use 1.89 million copies of attacks) in reality is quite difficult to achieve. The study [13] developed a metric-based system for detecting traditional slow attacks, which can be effective with limited resources, based on the study of similarities and the introduction of the Euclidean metric. This approach is only effective enough for a large number of such slow attack patterns, and for a large variety of such an approach is unlikely to be effective.

The most practical for implementation is the method proposed in [14], which determines the quality parameters of TCP connections, typical for slow HTTP attacks. This allows you to estimate the likelihood and time of the web server going into overload mode. However, such attack detection is based on observation statistics and uses predictions. The article [15] proposes an

algorithm for detecting slow DDoS attacks based on traffic patterns depending on the server load state. This does not consider the decision-making process. In [16], various scenarios are considered and a hybrid neural network for detecting DDoS attacks is proposed. However, the method and general technique for detecting low intensity DDoS attacks are not considered. In [17], the authors consider interval forecasting based on a probabilistic neural network with a dynamic update of the smoothing parameter. But the problem of the dynamics of the model remains unresolved.

Thus, most of the works devoted to countering slow DDoS attacks are based on statistical models, do not address the issues of predicting host behavior, and therefore are not effective enough to detect attacks at early stages.

The aim of this work is to form a system for detecting slow DDoS attacks based on predicting traffic elements in the network. To successfully solve the identified problem, it is necessary to build a model and technology for predicting the behavior of traffic parameters taking into account the history of host interaction in the network, as well as to propose a technology for recognizing slow DDoS attacks.

2. Development of a method for detecting slow DDOS attacks based on predicting of traffic parameters

2.1. Determining the traffic parameter for detecting a slow DDoS attack

The most expedient for detecting slow DDoS attacks is the architecture proposed in [18]. Such an IDS should consist of four modules: 1) traffic collection module; 2) module for calculating traffic parameters; 3) forecasting module; 4) module for classifying attacks (Fig. 1).

The system works as follows:

1. For some time, the Traffic Collection Module records the main traffic parameters required for further calculations: IP addresses of the sender and recipient; TCP window size; package arrival time.

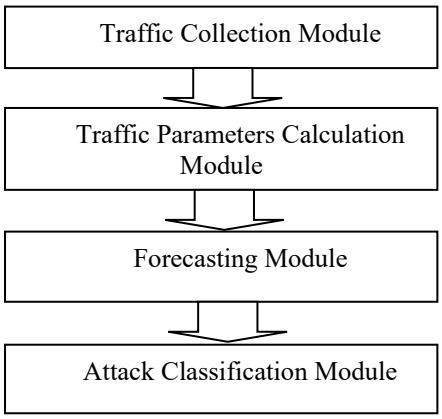


Figure 1: IDS structure

2. In the module for calculating traffic parameters for each IP address, the average delay between transmitted packets is calculated

$$\overline{T} = \frac{1}{k-1}\sum_{i=1}^{k}(t_{i+1} - t_i) \qquad (1)$$

where:

t_i – the i-th package arrival time;

t_{i+1} – the i+1-th package arrival time;

k – the number of packets received during the analyzed period.

The beginning and end of the session are recorded by a built-in timer, after which the duration of open connections is calculated.

3. The decision on the presence of a possible slow HTTP attack is made in the attack classification module based on the comparison of the obtained indicators with the average statistical values.

As it was shown in [18] the decision about the presence of a slow DDoS attack should be made based on the traffic parameters forecast, which can be generated based on the study of statistics in other systems. Thus, it is advisable to add a situation forecast block to the considered action algorithm.

2.2. Predicting the delay time between transmitted packets

The interaction of computer systems in the network forms an individual trajectory of changes in traffic parameters for each pair of interaction. Such trajectories have their own characteristics both in the normal mode of operation and during a slow DDoS attack. In order to start actions on time to neutralize a slow DDoS attack, it is

necessary to predict the time trajectory of traffic parameters, which depends on the actions of the interacting system.

Prediction of an individual traffic trajectory has already been studied in [19], in which traffic parameters were determined at long intervals (week, month). The same approach was used to predict slow DDoS attacks in [18]. At the same time, in both cases, only direct indicators were investigated: in [19] - the amount of information per unit of time, in [18] - the average delay between transmitted packets.

Slow DDoS attacks are characterized by the fact that they are not characterized by significant deviations in traffic indicators and therefore different parameters must be used to detect them.

Along with direct indicators (the amount of information and the average delay time), when using the method of canonical decomposition of a random process, the values of the correlation function are also calculated for each of the measurements, which makes the method more effective for predicting weak disturbances.

To monitor the traffic parameters, as before in [18], it is advisable to use the average time interval of the delay between packets in the session, which can be represented as a vector of parameters $X=(X_1,X_2,...,X_H)$ [20]. Condition fulfillment $X \in S_0$, where S_0 this is the tolerance area of the vector X. Random process $X(t)$ reflects the change in delays between traffic packets over time [21]. Process $X(t)$ statistically defined in the range $t \geq t_1$, where t_1 is the beginning of observations and $t_k \geq t_1$ [22].

The forecasting problem is posed as follows: for the parameter $x_\omega(t) \in S_0$, which is observed in the interval $t_1 \leq t \leq t_k$, determine the release time of a specific implementation $x_\omega(t)$ beyond the limits S_0 based on the definition of a posteriori process $X(t)$ [23].

The probability that a particular trajectory of a parameter ω guaranteed to fall within the acceptable range $s > t_k$, if by then t_k including his condition was described as $x_\omega(t), t_1 \leq t \leq t_k$ [24], will be

$$P^{ps}(s) = P\{X(s) \in S_0 / x_\omega(t)\}, \quad t_1 \leq t \leq t_k, s \geq t_k \qquad (2)$$

To solve the forecasting problem, the process under study must be represented by the formula

$$X(t) = m(t) + \sum_v V_v \phi_v(t), \qquad (3)$$

where $m(t)$ – mean function of the process;

$\phi_v(t)$ – non-random (coordinate) time functions;

V_v – random, uncorrelated coefficients $M[V_v]=0$, $M[V_v, V_\mu]=0$, $v \neq \mu$.

This representation, proposed in [18, 19], allows it to be applied to any traffic parameter that can be represented as a time series. Process $X(t)$ can be written as a random sequence $X(t_i)=X(i), i=\overline{1,I}$ in a discrete series of observations t_i [25]:

$$X(i) = m(i) + \sum_{v=1}^{i} V_v \phi_v(i), i=\overline{1,I}, \qquad (4)$$

where V_v – random coefficient with parameters $M[V_v]=0$, $M[V_v, V_\mu]=0$, $v \neq \mu$; $M[V_v^2]=D_v$; $\phi_v(i)$ – non-random coordinate function, $\phi_v(v)=1$, $\phi_v(i)=0$ while $v > i$.

The formulas for variance and correlation function can be written as

$$D(i) = \sum_{v=1}^{i} D_v \phi_v^2(i), i=\overline{1,I}, \qquad (5)$$

$$D(i,j) = \sum_{v=1}^{inf(i,j)} D_v \phi_v(i) \phi_v(j), \; i,j=\overline{1,I}. \qquad (6)$$

Thus, the representation of random processes of traffic parameters (2) allows solving the problem of detecting a slow DDoS attack based on predicting the delay between transmitted packets.

2.3. Slow DDoS Attack detection algorithm based on delay time prediction

To detect slow DDoS attacks within the framework of approach (1) - (6), the following algorithm for predicting delays between transmitted packets is proposed.

0. **Start**
1. $X(t) \leftarrow X(t), t=\overline{1,T}$ – formation of an array of process observations $X(t)$.
2. $x(\mu) \leftarrow x(\mu), \mu=\overline{1,k}$ – formation of an array of control results.

3. $L \leftarrow Length\left[X(t)\right]$ – determining the number of trajectories observed.
4. $m(t) = Mean\left[X(t)\right]$ – calculating the mean of a random function $X(t)$.
5. $c = Covariance\left[X(t)\right]$ – calculating the covariance matrix for $X(t)$.
6. $d = Variance\left[X(t)\right]$ – calculating an array of variances of a process $X(t)$.
7. $\phi = Table\left[0, \{T\}, \{T\}\right]$ – determining the initial value of the coordinate functions.
8. $\hat{X}(t) = X(t) - m(t), t = \overline{1,T}$ – centering the source data.
9. $V(t) = X_l(t) - m(t), t = \overline{1,T};\ l = \overline{1,L}$ – determination of initial values of random coefficients.
10. $\phi_1 = \frac{c_{1,j}}{d_1}, j = \overline{1,T}$ – definition of the first coordinate function.
11. **For** $i = 1$ to $i = T$
12. $d_i = c_{i,i} - \sum_{j=1}^{i-1} \phi_{i,j}^2 d_j$ – variance override.
13. **For** $j = 1$ to $j = T$
14. $\phi_i = \frac{1}{d_1}\left(c_{i,j} - \sum_{l=1}^{i-1} d_l \phi_{i,l} \phi_{j,l}\right)$ – redefining coordinate functions.
15. **for** *j*
16. **for** *i*
17. **For** $i = 2$ to $i \le T$
18. **For** $k = 1$ to $k < i$
19. $\phi_{i,k} = 0$ – redefining the coordinate functions of a random process.
20. **for** *k*
21. **for** *i*
22. **For** $i = 2$ to $i \le T$
23. **For** $l = 1$ to $l = L$
24. $V_{l,i} = \hat{X}_{l,i} - \sum_{k=1}^{i-1} V_{l,k} \phi_{k,i}$ – determination of random coefficients.
25. **for** *l*
26. **for** *i*
27. $p_s \leftarrow Length\left[x(\mu)\right]$ – size of the array of control results.
28. $M_1 = Table\left[m_i + (x_1 - m_1)\phi_{1,i}, \{i = \overline{1,T}\}\right]$ – determination of the initial predicted trajectory.
29. **For** $h = 2$ to $h = p_s$
30. $M_h = Table\begin{bmatrix} M_{h-1,i} + (x_h - M_{h-1,h})\phi_{h,i}, \\ \{i = \overline{1,T}\} \end{bmatrix}$ – calculation of forecast control points.
31. **for** *h*
32. $X_{forecast} = Table\begin{bmatrix} M_{k,i} + \sum_{j=k+1}^{i} V_{k,j}\phi_{k,j}, \\ \{k = \overline{1,p_s}, i = \overline{1,T}\} \end{bmatrix}$ – calculation of predicted trajectory.
33. **End**

The application of the algorithm makes it possible to construct a forecast of the system response delay time and determine the moment when this parameter goes beyond the critical values. In the event that latency is classified as a slow DDoS attack, security measures must be taken. A slow DDoS attack decision must be made for each sender IP address based on a comparison of predicted latency parameters with critical values to determine when the parameter enters the critical zone. This approach takes into account the statistics of the behavior of the interacting hosts, as well as the behavior of other hosts in similar situations in the event of a slow DDoS attack.

3. Application of the algorithm for detecting slow DDOS attacks based on predicting the response delay time

Slow DDOS attack detection simulations are performed for the RUDY attack. RUDY is a network server attack designed to crash a web server by sending long requests. The attack is carried out using a tool that scans the target website and detects embedded web forms. Once the forms have been detected, RUDY sends valid HTTP POST requests with an abnormally long content-length header field, and then begins entering information, one byte per packet. This type of attack is difficult to detect due to small fluctuations in incoming traffic.

For clarity, only one case of an attack against the background of normal traffic was taken, as shown in Figure 2. The average delay between transmitted packets is considered as the parameter under study.

The prediction algorithm was applied to the process shown in Figure 2, taking as the initial observation values individual points in the time

series that correspond to a partial trajectory (blue line in Figure 2). Considering this line as a control line, the first values of the time series were taken as the initial observation data, corresponding to $t = 1, 30, 60$ *s* of observations.

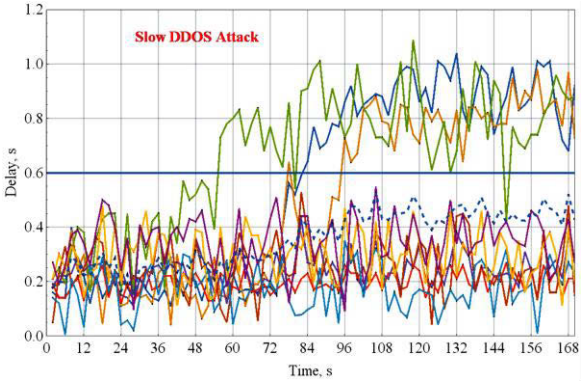
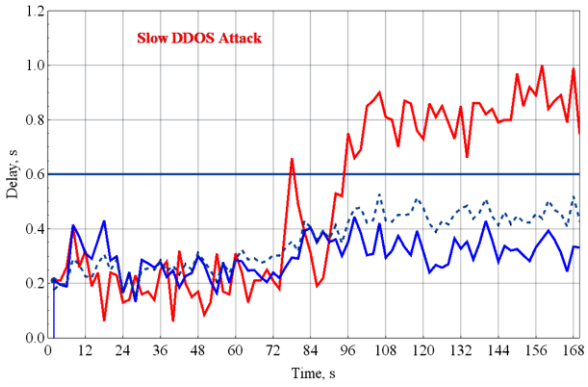


Figure 2: Traffic patterns

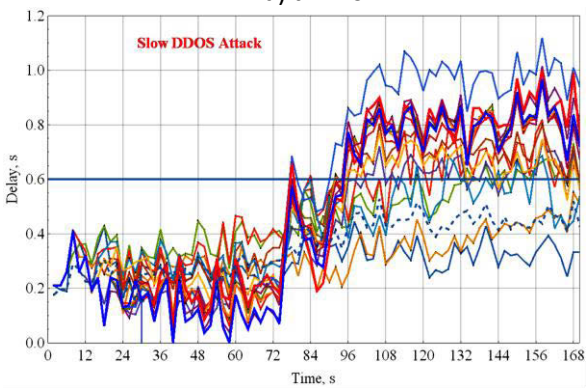
Figure 3a shows the forecast results for $t = 1$ s. Since there are few initial observational data, the process is reproduced as a whole in terms of the average value. In this case, the values of the predicted traffic in the event of an attack will be very different from the real ones (red curve).

Increasing the number of observations to $t = 30$ s (Figure 3b) increases the reliability of further prediction and at $t = 60$ s we can talk about a fairly accurate prediction $P^{ps}(s) \geq 0{,}99$. In Figure 3b and 3c curves of other colors show how forecasting will be carried out when receiving data from other control points $t_\mu, \mu = \overline{1,k}, k < I$, preceding the moment t_k. That is, the probability of error in choosing the correct trajectory depends on the amount of raw data observed. It is logical to assume that in this case the forecast accuracy will be too dependent on the trajectory behavior characteristics that lead to abnormal traffic, as well as on the observed frequency of anomalies. Thus, the method "selects" the required trajectory depending on the entry point and the average trajectory.

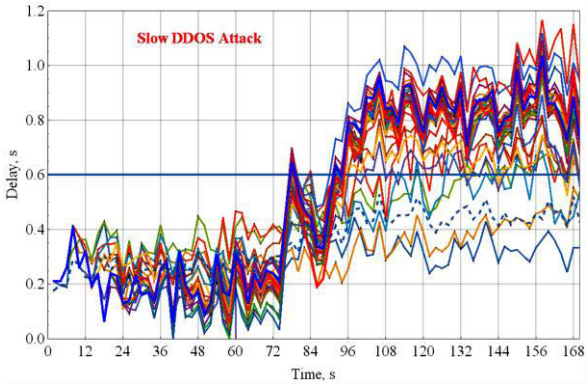
For this example, the important question is how the forecasting accuracy depends on the number of a priori observations. This issue has already been considered in [18], where it was shown that in 60...90 s the deviation of the predicted trajectory from the control one decreases to 5...0%. This confirms the adequacy of the predictive model for identifying slow DDoS attacks based on predicting network latency.



a) $t = 1$ s



b) $t = 30$ s



c) $t = 60$ s

Figure 3. Delay Time forecasting with observation time t = 1, 30, 60 s: — forecast value; — compared value; --- mean value

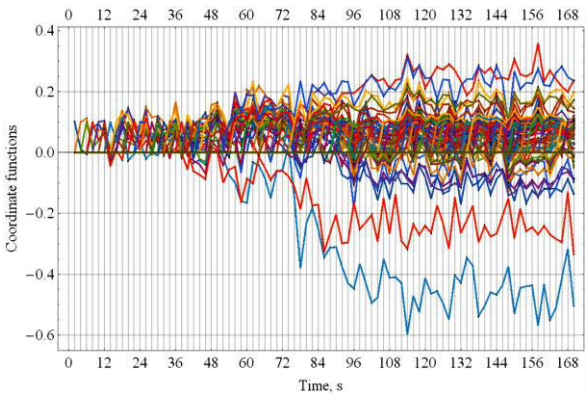


Figure 4: Coordinate functions

Even more interesting is the question of the behavior of the coordinate functions (Fig. 4). These functions are recalculated at each stage of calculating the predicted value and at the final stage are constant for a certain statistical series. They describe the relationship of the current parameter at the time of observation with its statistical data obtained during previous observations. As can be seen from Figure 3 a)–c), the coordinate functions respond to changes in the trajectory over time somewhat more than the average or forecast lines, which can be an additional factor in forecasting.

4. Conclusions

1. Low and slow DDoS attacks are difficult enough to detect due to minor changes in traffic parameters. Existing methods for detecting slow DDoS attacks require significant statistical material for training artificial intelligence systems. More promising, according to the authors, are methods based on predicting traffic parameters, in particular, the packet delay time in the network.

2. Predicting the delay time of packets in the network allows you to solve the problem of detecting slow DDoS attacks based on an algorithm for finding unknown future values for a time series of traffic parameters. The proposed method is a combination of artificial intelligence and statistical analysis and uses a self-learning algorithm provided there are sufficient attack statistics. The developed algorithm of the method makes it possible to accurately determine the random process at control points and to provide a minimum of the mean square of the approximation error in the intervals between these points.

3. Further research in the field of countering slow DDoS attacks can be devoted to the issues of forecasting at intervals that are not covered by statistics or the operation of the method in the absence of some observations or strong data noise.

5. References

[1] Enrico Cambiaso, & Gianluca Papaleo, & Giovanni Chiola, & Maurizio Aiello. (2013). Slow DOS Attacks: Definition and Categorisation. International Journal of Trust Management in Computing and Communications. 1. 300-319. 10.1504/IJTMCC.2013.056440.

[2] David Holmes. Mitigating DDoS Attacks with F5 Technology. [Electronic Resource] URL: https://www.f5.com/pdf/white-papers/mitigating-ddos-attacks-tech-brief.pdf

[3] Vasileios Theodorou, & Mark Shtern, & Roni Sandel, & Marin Litoiu, & Chris Bachalo. (2014). Towards Mitigation of Low and Slow Application DDoS Attacks. Proceedings - 2014 IEEE International Conference on Cloud Engineering, IC2E 2014. 10.1109/IC2E.2014.38

[4] Michael Siracusano, & Stavros Shiaeles, & B.V. Ghita. (2018). Detection of LDDoS Attacks Based on TCP Connection Parameters. Conference: 2018 Global Information Infrastructure and Networking Symposium (GIIS). 1-6. 10.1109/GIIS.2018.8635701

[5] Gagandeep Kaur, Vikas Saxena, J.P. Gupta, Detection of TCP targeted high bandwidth attacks using self-similarity, Journal of King Saud University - Computer and Information Sciences,Volume 32, Issue 1, 2020, Pages 35-49, ISSN 1319-1578, https://doi.org/10.1016/j.jksuci.2017.05.004.

[6] Lucas Cadalzo, Christopher H. Todd, Banjo Obayomi, W. Brad Moore and Anthony C. Wong. Canopy: A Learning-based Approach for Automatic Low-and-Slow DDoS Mitigation. ICISSP 2021 - 7th International Conference on Information Systems Security and Privacy

[7] Vinícius de Miranda Rios, Pedro R.M. Inácio, Damien Magoni, Mário Freire. Detection of reductionof-quality DDoS attacks using Fuzzy Logic and machine learning algorithms. Computer Networks, Elsevier, 2021, 186, pp.107792. ff10.1016/j.comnet.2020.107792ff. ffhal-03182934f

[8] A. Dhanapal and P. Nithyanandam. The Slow Http Distributed Denial of Service Attack Detection in Cloud. Scalable Computing: Practice and Experience. Volume 20, Number 2, pp. 285–298, 2019.

[9] A. Dhanapal_and P. Nithyanandam. The Slow HTTP DDOS Attacks: Detection, Mitigation and Prevention in the Cloud Environment. Scalable Computing: Practice and Experience. Volume 20, Number 4, pp. 669–685, 2019.

[10] T. Lukaseder, S. Ghosh, F. Kargl. Mitigation of Flooding and Slow DDoS Attacks in a Software-Defined Network. 16 August 2018. https://arxiv.org/pdf/1808.05357.pdf

[11] H. Abusaimeh, H. Atta, H. Shihadeh. Survey on Cache-Based Side-Channel Attacks in Cloud Computing. International Journal of

Emerging Trends in Engineering Research. Volume 8, No.4, p.1019-1026, April 2020.

[12] L. Calvert, T. M. Khoshgoftaar Impact of class distribution on the detection of slow HTTP DoS attacks using Big Data. Journal of Big Data. 6, 67, 2019.

[13] B. Cusack, and Z. Tian. Detecting and tracing slow attacks on mobile phone user service. In Valli, C. (Ed.). The Proceedings of 14th Australian Digital Forensics Conference, 5-6 December 2016, Edith Cowan University, Perth, Australia. pp. 4-10, 2016.

[14] Ie. V. Duravkin, A. Carlsson, A. S. Loktionova. Method of Slow-Attack Detection. Information processing systems, issue 8 (124), pp. 102-106, 2014.

[15] I.V. Ruban, D.W. Pribylnov, E.C. Loshakov. A method of detecting a low-speed denial-of-service attack. Science and technology of the Air Force of the Armed Forces of Ukraine, № 4(13). 85-88, 2013.

[16] Ya. V. Tarasov. Investigation of the application of neural networks for the detection of low-intensity DDoS-attacks of the application level. Cybersecurity issues №5(24), 23-29, 2017.

[17] Y. M. Krakovsky, A. N. Luzgin. The cyberattack intensity forecasting to information systems of critical infrastructures. Problems of smart cities and sustainable development of territories. SAFETY2018, Ekaterinburg, October 4-5, 34-42, pp. 180-187, 2018.

[18] Vitalii Savchenko, Oleh Ilin, Nikolay Hnidenko, Olga Tkachenko, Oleksandr Laptiev, Svitlana Lehominova, Detection of Slow DDoS Attacks based on User's Behavior Forecasting. International Journal of Emerging Trends in Engineering Research (IJETER) Volume 8. No. 5, May 2020. Scopus Indexed - ISSN 2347 – 3983. pp.2019 – 2025.

[19] Vitalii Savchenko, O. Matsko, O. Vorobiov, Y. Kizyak, L. Kriuchkova, Y. Tikhonov, A. Kotenko. Network traffic forecasting based on the canonical expansion of a random process. Eastern European Journal of Enterprise Technologies. VOL 3, NO 2 (93). p. 33-41, 2018.

[20] Vitalii Savchenko, Viktor Zaika, Maksym Trembovetskyi, German Shuklin, Liubov Berkman, Kamila Storchak, Ihor Rolin. Composite Radioisotope Coating Parameters and Reflecting Characteristics Calculation Selection Method. International Journal of Advanced Trends in Computer Science and Engineering. Volume 8, No.5, September - October 2019. – P. 2246-2251. https://doi.org/10.30534/ijatcse/2019/60852019

[21] Vitalii Savchenko, Oleh Vorobiov, Oksana Tkalenko, Olha Polonevych, German Shuklin, Maksym Trembovetskyi, Viktor Zaika, Marianna Konopliannykova. Influense of Composit Materials Nonlinear Properties with Radioisotope Inclutions on Reflected Radiations. International Journal of Advanced Trends in Computer Science and Engineering. 2019. No.6. P. 2716-2720.

[22] Vitalii Savchenko, V. Akhramovych, A. Tushych, I. Sribna, I. Vlasov. Analysis of Social Network Parameters and the Likelihood of its Constraction. International Journal of Emerging Trends in Engineering Research. Volume 8, No. 2, p. 271-276, February 2020.

[23] Serhii Yevseiev, Roman Korolyov, Andrii Tkachov, Oleksandr Laptiev, Ivan Opirskyy, Olha Soloviova. Modification of the algorithm (OFM) S-box, which provides increasing crypto resistance in the post-quantum period. International Journal of Advanced Trends in Computer Science and Engineering (IJATCSE) Volume 9. No. 5, September-Oktober 2020, pp. 8725-8729.

[24] Oleg Barabash, Oleksandr Laptiev, Oksana Kovtun, Olga Leshchenko, Kseniia Dukhnovska, Anatoliy Biehun. The Method dynavic TF-IDF. International Journal of Emerging Trends in Engineering Research (IJETER), Volume 8. No. 9, September 2020. pp. 5713-5718.

[25] Oleg Barabash, Oleksandr Laptiev, Volodymyr Tkachev, Oleksii Maystrov, Oleksandr Krasikov, Igor Polovinkin. The Indirect method of obtaining Estimates of the Parameters of Radio Signals of covert means of obtaining Information. International Journal of Emerging Trends in Engineering Research (IJETER), Volume 8. No. 8, August 2020. Indexed- ISSN: 2278 – 3075. pp.4133 – 4139.

Peculiar Properties Of Creating A System Of Support To Make Anti-Crisis Decisions By Experts Of The Situational Center At The Cyber Protection Object

Vadym Tiutiunyk [1], Olha Tiutiunyk [2], Oleh Teslenko [3] and Natalia Brynza [4]

[1] National University of Civil Defence of Ukraine, Chernyshevska Str., 94, Kharkiv, 61023, Ukraine
[2,3,4] Simon Kuznets Kharkiv National University of Economics, Science ave., 9-A, Kharkiv, 61166, Ukraine

Abstract

Considering the uncertainty of the parameters affecting the conditions for the normal functioning of the cyber protection object, it is proposed to create a support system for making anti-crisis decisions by the experts of the situational center, which is an integral part of the information security system of the cyber protection object. The basis of the information security system of a cyber protection object shall be a classical control loop that ensures the collection, processing and analysis of information, as well as modeling the development of information danger at the cyber protection object and the development and implementation of anti-crisis management to prevent the emergence of threats to information circulating during the functioning of the cyber protection object, and also elimination or minimization of their consequences.

In the study, the risk indicator for information circulating during the functioning of a cyber protection object is the summation between the risk indicators of information disclosure and information leakage, as well as the risk indicator for computer information circulating during the functioning of the cyber protection object. The indicator of the risk of information leakage includes indicators of the risk of information leakage through technical channels, information leakage through communication channels, speech information leakage, as well as information leakage, shown information. The risk indicator for computer information includes indicators of the risk of loss and alteration of information, as well as obtaining unauthorized access to information.

In the context of untimely, incomplete and suboptimal information concerning the condition of information security of the cyber protection object, to solve the problem of multi-criteria optimization for the formation of alternatives to anti-crisis decisions by the experts of the situational center, in the study, firstly, the methods of obtaining initial information about the advantages of the on traditional heuristic procedures of expert evaluation, and concerning formal methods of comparator identification. It is shown that regardless of the method of obtaining the initial information and the form of its presentation, the most adequate is the interval assessment of the preferences of the decision maker. Secondly, a model of a multicriteria scalar assessment of the usefulness of feasible alternative solutions has been synthesized. The presented results represent the scientific basis for the development of a support system for making anti-crisis decisions in critical situations by experts of the situational center to ensure the appropriate level of information security of the cyber protection object.

Keywords

cyber protection object, information security system, situational center, anti-crisis decision support system, multi-criteria, uncertainty of initial information

1. Introduction

Cyber protection objects (CPO) in the state are the following: 1) communication systems of all forms of ownership, in which national information resources are processed and/or used in the interests of state authorities, local authorities, law enforcement bodies and military formations formed in accordance with

EMAIL: tutunik_v@ukr.net (A. 1); tutunik.o@ukr.net (A. 2); tov1967@meta.ua (A. 3); natalia.brynza@hneu.net (A. 4)
ORCID: 0000-0001-5394-6367 (A. 1); 0000-0002-3330-8920 (A. 2); 0000-0003-3105-9323 (A. 3); 0000-0002-0229-2874 (A. 4)

the law; 2) objects of critical information infrastructure; 3) communication systems that are used to meet public needs and/or implement legal relations in the areas of electronic government, electronic government services, electronic commerce, electronic document management [1-3].

The creation of an effective information security system of the CPO requires the inclusion of a subsystem of situational centers, rigidly interconnected at the information and performance levels for making appropriate anti-crisis decisions in solving various functional monitoring tasks, preventing the emergence of threats to information circulating during functioning of the CPO, as well as eliminating or minimizing their consequences [4].

One of the topical directions to create a subsystem of situational centers in the information security system of the CPO is the development of a justification methodology, under the uncertainty of initial information for experts of the system of situational centers, optimal anti-crisis solutions to prevent the emergence of threats to information circulating in the process of functioning of the CPO, as well as to eliminate or minimize their consequences.

An obligatory stage in the functioning of the system of situational centers is decision making. At the same time, not only incorrect, but also ineffective decisions lead to losses or irrational use of financial, time, labor, energy and other resources when managing the processes of prevention and elimination of emergency situations. In this regard, the problem of developing a scientifically grounded methodology to make effective decisions is one of the urgent scientific problems.

According to V.M. Hlushkov, the necessary conditions for the effectiveness of decisions are their timeliness, completeness and optimality. The listed requirements are contradictory and their satisfaction is connected with serious difficulties.

Provision the completeness (complexity) of decisions requires the fullest possible consideration of internal and external factors affecting decision-making, a deep analysis of their interrelationships, which leads to increase in the dimension of the decision-making problem, its multicriteria. In turn, this leads to increase in the uncertainty of the initial data, which is due to the incompleteness of knowledge about the relationship of factors and, as a consequence, its inaccurate description, the impossibility or inaccuracy of measuring some factors, random external and internal influences, etc. An additional complication is in the fact that uncertainties are heterogeneous and can be represented as random variables, fuzzy sets or simply interval values.

Thus, an increase in the efficiency of decisions made is connected with the need to solve multicriteria optimization problems in conditions of uncertainty.

The traditional, widespread approach to solving such problems, based on their heuristic simplification, determinization as a means of removing uncertainty, becomes less and less effective as the tasks become more complex and the significance of solutions increases.

In these conditions, it is extremely important to develop formal, normative methods and models for a comprehensive solution to the problem of decision-making in conditions of multi-criteria and uncertainty.

In this direction, principal, fundamental results have been obtained [5–10], however, the only solution to the problem is far from completion and the continuation of research in this direction is undoubtedly relevant both in theoretical and applied aspects for the development of a substantiation methodology, under conditions of uncertainty in the input information for experts of the system of situational centers, optimal anti-crisis solutions to ensure the required level of safety for functioning of the CPO.

2. Peculiar properties of the situation center performance as a component of the support system for anti-crisis decision-making at the cyber protection objects

The situational center while operating in the information security system of the CPO shall, in accordance with the data in Fig. 1, ensure the collection, processing and analysis of information, as well as modeling the development of information threat to the CPO and the development and implementation of anti-crisis management to prevent the emergence of threats to information circulating

during functioning of the CPO, as well as to eliminate or minimize their consequences.

Functioning which is shown in Fig. 1, schemes in the conditions of completeness of the initial information and the presence of one partial criterion for assessing the set of feasible solutions does not present difficulties in substantiating optimal anti-crisis solutions. On the other hand, modern problematic situations are characterized by incompleteness of knowledge (uncertainty) of the initial data and many particular evaluation criteria. Thus, the traditional approach based on the decomposition of the problem into two socalled independent problems – multiobjective optimization in deterministic, that is, without concidering uncertainty, formulation and decision-making under uncertainty for a scalar objective function in modern conditions, does not meet the requirements of practice under accuracy and efficiency.

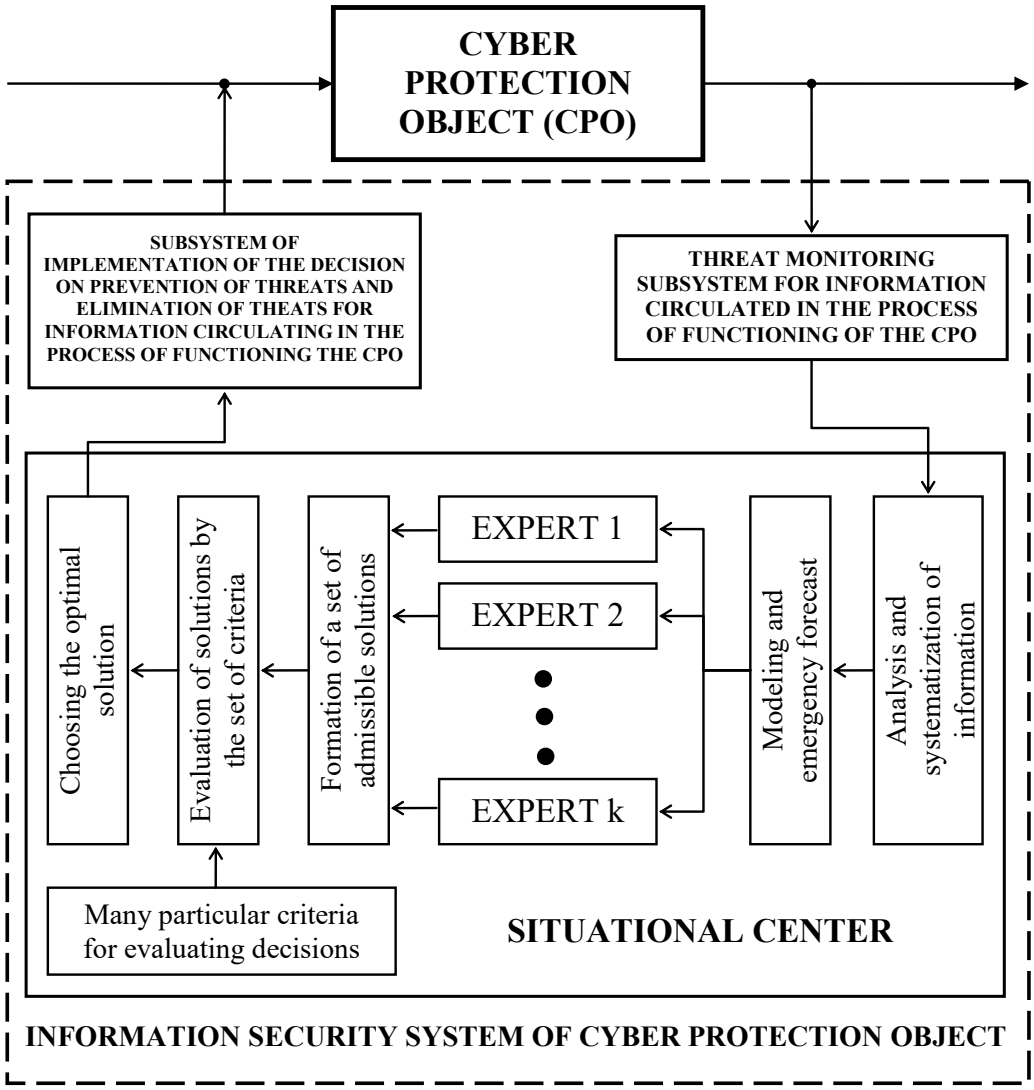


Figure 1: Functional scheme of substantiation of optimal anti-crisis solutions to ensure the appropriate level of security of the cyber protection object, under uncertainty of input information for experts of the situational center

This is due to the fact that the problem of multicriteria optimization is incorrect, because it allows to determine the solution only with precision in the field of compromise solutions, and its regularization to determine a single solution based on generalized multifactor scalar estimation, it is based on poorly structured, subjective expert assessments, the determination of which leads to large errors. On the other hand, methods of decision-making under the uncertainty under scalar estimate and the expected effect, without considering its multicriteria, are also not adequate. Therefore, there is the need to develop a methodology for comprehensive solutions to the

problem of decision-making, considering the multi-criteria and incomplete uncertainty of the original data.

3. Risk assessment of threats to information circulating during the cyber defense object functioning

Based on the basic postulates of the risk-oriented approach, the risk indicator for the information circulating in the process of functioning of the CPO shall be represented as [11]:

$$R_{CPO}^{Inf.} = \sum_{i=1}^{3} R_{CPOi}^{Inf.}, \quad (1)$$

where $R_{CPO1}^{Inf.}$ – is a risk indicator for information circulating during functioning of the CPO, which is characterized by the disclosure of information; $R_{CPO2}^{Inf.}$ – is a risk indicator for the information circulating in the process of functioning of the CPO which is characterized by information leakage; $R_{CPO3}^{Inf.}$ – is a risk indicator for computer information circulating during the functioning.

The components of risk for the information circulating in the process of functioning of the CPO are presented in Fig. 2. The risk components for the information circulating in the process of functioning of the CPO are calculated by the formula:

$$R_{CPOi.j}^{Inf.} = P_{CPOi.j}^{Inf.} \cdot U_{CPOi.j}^{Inf.}, \quad (2)$$

where $P_{CPOi.j}^{Inf.}$ – is assessment of the probability of exceeding the normative indicator for the j-th aspect of the i-th process of danger for the information circulating in the process of functioning of the CPO; $U_{CPOi.j}^{Inf.}$ – is assessment of the damage from exceeding the normative indicator of the impact of the j-th aspect of the i-th process of danger for the information circulating in the process of functioning of the CPO.

At the same influence on the information circulating in the process of functioning of the CPO, several processes of danger, it is necessary to consider a possibility of display of synergetic effect. In this case, the probability of exceeding the norm for two common aspects of the danger to the information circulating in the process of functioning of the CPO shall be calculated as:

$$P_{CPOi.j}^{Inf.} = P_{CPOi.1}^{Inf.} + P_{CPOi.2}^{Inf.} - P_{CPOi.1}^{Inf.} \cdot P_{CPOi.2}^{Inf.}. \quad (3)$$

The assessment of the damage from exceeding the normative indicator is calculated as the amount of damage, the type of threat components for the information circulating in the process of functioning of the CPO. Total expected loss $U_{CPO}^{Inf.}$ is determined by the formula:

$$U_{CPO}^{Inf.} = \sum_{i,j} U_{CPOi.j}^{Inf.}, \quad (4)$$

where $U_{CPO}^{Inf.}$ – is the mathematical expectation of the general economic damage of the CPO from processes of danger for the information circulating in the process of functioning of the CPO; $U_{CPOi.j}^{Inf.}$ – is the mathematical expectation of damage of the CPO concerning the risk of the j-th aspect of the i-th process of danger for the information circulating in the process of functioning of the CPO.

Based on the material presented in the form of expressions (1)–(4) concerning the distribution of the risk-based approach to assessing the vulnerability of the CPO and based on the basic tenets of systems theory and synergetics, the level of the CPO protection in the probabilistic manifestation of various aspects of information threat of economic efficiency of functioning of system of information security of cyber protection object – F_{SISCPO}, shall be written as an equation:

$$Z_{CPO}^{Inf.} = \varphi\left(U_{CPO}^{Inf.}, F_{SISCPO}\right). \quad (5)$$

The expression (5) is presented in the form of a general functionality, the solution to which is possible while conducting the audit by experts of the situation center under security in the probable manifestation of various aspects of the information threat process of a particular cyber protection object.

Figure 2: The main types of threats to the information circulating during the functioning of the cyber protection object [11]

4. Peculiar properties of decision support by experts of the situational center under uncertainty of the input information at emergence of threats to the information circulating in the process of functioning the cyber protection object

In general [12–14], the admissible set of solutions contains subsets of consistent X^S and contradictory (compromise) X^C solutions. A feature of the latter is the impossibility of improving any particular criterion $k_j(x)$, $j=\overline{1,n}$ without deteriorating the quality of at

least one particular criterion. In this case, by definition, an effective solution $x^{\bullet}$ necessarily belongs to the area of compromise. This means that the problem of multiobjective optimization

$$x^{\bullet} = \arg \underset{x \in X}{extr} < k_j(x) >, \forall j = \overline{1,n}, \quad (6)$$

has no solution, i.e. is incorrect according to Adamar, since in the general case it does not provide the definition of the only optimal solution from the set of compromises X^C.

Thus, the problem of multiobjective optimization arises. The main idea of the methods for solving a multicriteria decision-making problem (MDMP) is to develop a certain regularizing procedure that allows choosing a single solution from the area of compromises X^C. There are two possible approaches to the implementation of such a task: heuristic, when the decision-maker (DM) makes a choice based on their experience, and formal, based on some formal rules (compromise schemes).

The main methods of regularizing the problem of multicriteria optimization are the principle of the main criterion, functional-cost analysis and the principle of sequential optimization. Each of the listed optimality principles has its own area of correct application and is used in engineering practice, but the most general and universal approach is based on the formation on a set of particular criteria $K = K_{\phi} \cup K_{з} = \{\kappa_i(x)\}$, $i = \overline{1,n}$ of a generalized scalar estimate (criterion), which is often called a utility function of the form

$$\overline{K}(x) \equiv P(x) = F[\lambda_j, K_j(x)], \; j = \overline{1,m}, \quad (7)$$

where λ_j – is the isomorphism coefficients that bring heterogeneous particular criteria $K_j(x)$ to isomorphic form.

The theoretical basis for the formation of multicriteria scalar estimates is the utility theory, which assumes the existence of a quantitative assessment of the preference of decisions. It means that

$$x_1, x_2 \in X, \; x_1 \succ x_2, \text{ то } P(x_1) > P(x_2), \quad (8)$$

where $P(x_1)$, $P(x_2)$ – are the utility functions.

In the general case, the converse is also true. Thus, utility is a quantitative measure of the "quality" of decisions, therefore

$$x^{\circ} = \arg \max_{x \in X} P(x). \quad (9)$$

In this regard, the problem arises of substantiating the rule (metric), according to which the utility function is formed in the space of particular criteria $k_i(x)$.

It is crucial that there is no objective metric, and the principle of ranking decisions reflects the subjective preferences of a particular decision maker.

Consider the systemological grounds for choosing the metric of the utility function.

The synthesis of any mathematical model, including the synthesis of the utility function, presupposes the need to solve two interrelated problems: structural and parametric identification. The first of them provides for: identification of significant factors that affect the output of the model; structure definition, i.e. the kind of operator that determines the connection between the input and output data of the model.

The solution to the problem of parametric identification is to determine the specific quantitative values of the model parameters.

The problem of structural identification of a model is connected with the heuristic advance and verification of a hypothesis. In the case under consideration, the form of the decision utility function x is determined by particular characteristics (criteria) $k_i(x)$.

The next step in solving the problem is to identify the type of operator F. There are most widely known two forms of the utility function: additive and multiplicative.

Additive utility function. Fishbern made a great contribution to substantiating this hypothesis. He determined the necessary and sufficient conditions for the adequacy of the additive utility function for many cases. In the case of n factors, the condition for the additivity of the utility function according to Fishbern can be formulated as follows: the factors $x_1, x_2, \ldots x_n$ are additively independent if the preference of lotteries on $x_1, x_2, \ldots x_n$ depend only on their marginal probability distributions.

Using this definition, we can formulate the main result of the theory of additive utility:

$$P(x)=\sum_{i=1}^{n}\lambda_i k_i(x). \quad (10)$$

The multiplicative form of the utility function has the following form

$$P(x)=\prod_{i=1}^{n}\lambda_i k_i(x). \quad (11)$$

The analysis showed that the multiplicative form does not allow considering the information about the weight coefficients. The disadvantage of the additive form is that it does not allow considering the nonlinearity and interconnection of particular criteria.

Therefore, in the general case, a more universal structure of the utility function is needed, which would allow considering both the additive form and nonlinear effects.

As such a universal form, the Kolmohorov-Habor polynomial can be used, which in the general case has the form:

$$P(Y)=\lambda_0+\sum_{i=1}^{n}\lambda_i x_i+\sum_{i=1}^{n}\sum_{i\le j}\lambda_{ij}x_i x_j+ \\ +\sum_{i=1}^{n}\sum_{j\le i}\sum_{k\le j}\lambda_{ijk}x_i x_j x_k+\ldots., \quad (12)$$

For the purposes of evaluating utility, it shall be modified by putting $\lambda_0=0$, as a result, it will take the form

$$P(Y)=\sum_{i=1}^{n}\lambda_i k_i+\sum_{i=1}^{n}\sum_{j=1}^{n}\lambda_{ij}k_i k_j+\ldots. \quad (13)$$

Moreover, in most practical situations, it is sufficient to consider only the members of the second order.

The Kolmohorov-Habor polynomial contains the fragments of the additive and multiplicative functions and is linear in parameters. Considering that, by expanding the space of variables by introducing additional variables such as $\sum_{i=1}^{n}\sum_{j=1}^{n}k_i k_j=z_l$, we obtain an additive function of the following form

$$P(x)=\sum_{l=1}^{L}\lambda_l z_l, \quad (14)$$

Based on the above mentioned, we will consider the additive form in more detail, using model (10) for clarity. All particular criteria, by definition, have different dimensions, intervals and measurement scales, i.e. are not comparable to each other.

Consequently, formula (9) is valid only if λ_i considers the importance of particular criteria and, at the same time, are the isomorphism coefficients, i.e. lead heterogeneous $k_i(x)$ to a single dimension and range of change. However, in the general case, it is difficult to determine the values of such isomorphism coefficients. This circumstance can be overcome by presenting the additive utility function in the following form:

$$P(x)=\sum_{i=1}^{n}a_i k_i^{H}(x), \quad (15)$$

where a_i – is the relative dimensionless weight coefficients for which the constraints are satisfied

$$0\le a_i\le 1,\ \sum_{i=1}^{n}a_i=1, \quad (16)$$

and $k_i^{H}(x)$ – normalized, i.e. partial criteria reduced to isomorphic form. The criteria are normalized according to the formula

$$k_i^{H}(x)=\left(\frac{k_i(x)-k_i^{HX}}{k_i^{HЛ}-k_i^{HX}}\right)^{\alpha_{ui}}, \quad (17)$$

where $k_i(x)$ – is the value of a particular criterion; $k_i^{HЛ}$, k_i^{HX} – respectively, the best and worst value of the particular criterion, which he takes on the area of admissible solutions $x\in X$.

Depending on the type of extremum (direction of dominance)

$$k_i^{HЛ}=\begin{cases}\max\limits_{x\in X}k_i(x), & \text{if } k_i(x)\to max\\ \min\limits_{x\in X}k_i(x), & \text{if } k_i(x)\to min\end{cases} \quad (18)$$

$$k_i^{HX}=\begin{cases}\min\limits_{x\in X}k_i(x), & \text{if } k_i(x)\to max\\ \max\limits_{x\in X}k_i(x), & \text{if } k_i(x)\to min\end{cases} \quad (19)$$

The estimation model (15) is constructive only if the weighting coefficients a_i of particular criteria are set by point quantitative values. As it was mentioned above, decision makers are the carriers of this information, which means that some procedures for obtaining it are necessary, i.e. solving the problem of parametric identification of the model. For various reasons, to obtain accurate quantitative information about the values a_i is not always possible, therefore, in the general case, the evaluation of the usefulness of decisions has to be carried out under conditions of a greater or lesser degree of uncertainty about the mutual importance of particular criteria. In general, the general model for determining the utility of a solution $x \in X$ has a form

$$P(x) = G\left[J(a_i), k_i(x)\right], \; i = \overline{1,n}, \quad (20)$$

where $J(a_i)$ – is the information about the values of the coefficients of relative importance.

Extreme situations are ones when:

1) the weight coefficients a_i are specified in the form of exact point quantitative values;

2) information about the preference of particular criteria is completely absent.

Typically, between these extremes, there are many situations with varying degrees of uncertainty in the assignment of weighting factors.

Based on the presented approach, the problem of synthesizing a model for calculating the interval phased value of a scalar multifactorial assessment of the effectiveness (utility) of feasible solutions is solved in this study.

It is assumed that the model for calculating the utility function in the general case is a certain fragment of the Kolmohorov-Habor polynomial, linear in parameters, but nonlinear in variables (partial criteria). This means that in the extended space of variables, the utility function model $P(x)$ can be viewed as an additive function of the form

$$\overline{P}(x) = \sum_{i=1}^{n} \overline{a_i}\,\overline{k_i^H}(x) \quad (21)$$

where $\overline{a_i}$ – is dimensionless weight coefficients that meet the requirements $0 \le a_i \le 1, \sum_{i=1}^{n} a_i = 1;$ $\overline{k_i^H}(x)$ are normalized, that is, reduced to dimensionless form, the same metric and dominance direction, partial criteria; the "-" sign means interval uncertainty.

An analysis of the features of the problem of multicriteria scalar estimates showed that fuzzy sets are a widespread form of representing uncertainties in model (21). Under the accepted assumptions, the parametric identification of the model of the multicriteria optimization problem (21) consists in determining the interval values of the parameters $\overline{a_i}$ and particular criteria $\overline{k_i}(x)$, their fuzzification and calculating the interval phased value of the solution utility function $P(x)$.

Since the problem of multivariate estimation is an intellectual procedure and there are experts who are carriers of the input information, the problem of parametric identification of model parameters (21) is solved directly by the methods of expert assessment or by the method of comparative identification.

The method of comparative identification of the additive model for scalar evaluation of the utility of alternatives is as follows. The input information is the relation of a strict or non-strict order, determined by experts on a set of admissible alternatives

$$x_1 \succ x_2 \sim x_3 \sim x_4 \succ \ldots., \quad (22)$$

where $\succ, \sim$ are the signs of advantage and equivalence correspond. According to the theory of utility for (22), the following relations hold:

$$P(x_1) > P(x_2) = P(x_3) > P(x_4) > \ldots. \quad (23)$$

Based on (23), one can compose a system of equations of the form

$$\begin{aligned} &P(x_2) - P(x_1) \le 0, \\ &P(x_3) - P(x_2) = 0, \\ &P(x_4) - P(x_3) \le 0. \\ &\ldots\ldots\ldots\ldots\ldots\ldots \end{aligned} \quad (24)$$

By substituting the utility function (21) into (24), we obtain a system of a_i irregularities that are linear with respect to the parameters, which determine the area of their possible values. The method of linear programming on the selected area determines the interval values $[a_i^{max}, a_i^{min}]$

of the parameters. In this case, regardless of the method, interval estimates of the parameters are determined $a_i = [a_i^{max}, a_i^{min}]; \forall i = \overline{1,n}$, and the size of the intervals depends on the scatter of the subjective individual labels of experts.

The interval uncertainty of the model variables (particular criteria) is determined by non-factors. Their analysis and accounting allows you to determine the range of possible values of each of them.

The next stage in identifying the model (21) consists in its fuzzification, that is, in the choice of the type and parameters of the membership function of the interval parameters and changes.

The weight coefficients a_i are interval fuzzy numbers, and the value of particular criteria can be specified both numerically, in the form of fuzzy numbers, and qualitatively, in the form of linguistic terms.

5. Conclusions

1. It is shown that the basis of the information security system of a cyber protection object shall be a classical control loop that provides collection, processing and analysis of information, as well as modeling the development of information danger at a cyber protection object and the development and implementation of anti-crisis management to prevent the emergence of threats to information circulating in the process of functioning of the cyber protection object, as well as the elimination or minimization of their consequences.

2. The indicator of risk for information circulating during functioning of the cyber protection object is the sum between the indicators of risk of information disclosure and information leakage, as well as the indicator of risk for computer information circulating during functioning of the cyber protection object.

The indicator of the risk of information leakage includes indicators of the risk of information leakage through technical channels, information leakage through communication channels, speech information leakage, as well as information leakage, shown information.

The risk indicator for computer information includes indicators of the risk of loss and alteration of information, as well as obtaining unauthorized access to information.

3. It is shown that while conducting the audit by the experts of the situational center under security in conditions of probabilistic manifestation of various aspects of the information threat process of a cyber protection object, the procedure for making management decisions is complicated by the fact that the necessary conditions for the effectiveness of decisions are their timeliness, completeness and optimality. Therefore, increasing the efficiency of the decisions made is associated with the need to solve the problem of multi-criteria optimization under the uncertainty, which requires the development of formal, normative methods and models for a comprehensive solution to the problem of decision-making under the multi-criteria and uncertainty in managing the processes of preventing the occurrence of threats to information circulating during functioning of the cyber protection object, as well as elimination or minimization of their consequences.

4. In order to solve the problem of multicriteria optimization under the uncertainty, in the study, firstly, it is formalized the methods for obtaining initial information about the advantages of a decision-maker, based on both traditional heuristic procedures for expert evaluation and formal methods of comparative identification. It is shown that regardless of the method of obtaining the initial information and the form of its presentation, the most adequate is the interval assessment of the preferences of the decision-maker. Secondly, a model of a multicriteria scalar assessment of the usefulness of feasible alternative solutions has been synthesized.

5. The presented results represent the scientific basis for the development of a support system for making anti-crisis decisions in critical situations by experts of the situational center to ensure the appropriate level of information security of the cyber protection object.

6. References

[1] Basic principles of cybersecurity in Ukraine Act dated on October 5, 2017 No 2163-VIII [Electronic resource]. Access mode: https://zakon.rada.gov.ua/laws/show/2163-19

[2] Cybersecurity Strategy of Ukraine approved by the President of Ukraine Order concerning the Regulation of the National Security and Defense Council of Ukraine dated on January 27, 2016 [Electronic resource]. Access mode: https://zakon.rada.gov.ua/laws/show/96/2016

[3] General requirements for cyber protection of critical infrastructure, approved by Cabinet of Ministers of Ukraine Regulation dated on June 19, 2019 No 518

[4] V. Tiutiunyk, V. Kalugin, O. Pysklakova, A. Levterov, Ju. Zakharchenko "Development of Civil Defense Systems and Ecological Safety". IEEE Problems of Infocommunications. Science and Technology (2019): 295–299.

[5] B. Fahimnia, C.S. Tang, H. Davarzani, J. Sarkis. Quantitative models for managing supply chain risks: A review. European Journal of Operational Research, 2015, No.247, pp.1–15.

[6] S. Haugen, J.E. Vinnem. Perspectives on risk and the unforeseen. Reliability Engineering and System Safety, 2015, No.137, pp.1–5.

[7] F. Khan, S. Rathnayaka & S. Ahmed Methods and models in process safety and risk management: Past, present and future. Process Safety and Environmental Protection, 2015, No.98, pp.116–147.

[8] T. Aven. Risk assessment and risk management: Review of recent advances on their foundation. European Journal of Operational Research, 2016, Vol.253, No.1, pp.1–13.

[9] V. Tiutiunyk, I. Ruban, O. Tiutiunyk "Cluster analysis of the regions of Ukraine by the number of the arisen emergencies". IEEE Problems of Infocommunications. Science and Technology (2020).

[10] J. Gehandler, U. Millgård. Principles and Policies for Recycling Decisions and Risk Management. Recycling, 2020, Vol.5, No.21, pp.1–18.

[11] I. Ruban, V. Tiutiunyk, V. Zabolotnyi, O. Tiutiunyk. Dissemination of Risk-Oriented Approach for Assessment the Effectiveness of the Information Security System of Cyber Defense Objects. Ukrainian Scientific Journal of Information Security, 2020, volume 26, No.3, pp.145–155.

[12] Ye.H. Petrov, N.I. Kalita Methods for evaluating the vector of individual preferences. Bionics problems, 2003, No.58, pp. 27–35.

[13] Ye.H. Petrov Methods and means of decision making in socio-economic systems. Kiev, Appliances, 2004.

[14] Ye.H. Petrov, N.A. Brynza, L.V. Kolesnik, O.A. Pysklakova. Methods and models of decision making under the multi-criteria and uncertainty. Kherson, 2014.

The Basic Principles Of The Compact Video Frames Representation Technology, Which Are Presented In A Differential Form In Computer Systems

Oleksandr Tymochko [1], Maksim Pavlenko [2], Volodymyr Larin [3]

[1,2,3] *Ivan Kozhedub Kharkiv National Air Force University, 77/79 Sumska str., Kharkiv, 61023, Ukraine*

Abstract

In order to reveal regularities in sequences of series lengths, it is necessary to justify an informative attribute possessing the following properties:

1) is informative for the lengths of the binary series, taking into account the adaptation to the peculiarities of the formation of arrays of the binary mask of the differential frame.

Here, it is required to provide a potential opportunity for reducing redundancy for arbitrary content of the bit plane;

2) do not require significant computational costs for estimating and detecting regularities that do not exceed order $O(n)$;

3) to ensure that there are sharp structural differences for the binary indicators of the stationary and dynamic components of the differential frame represented.

The compression ratio of the differential-represented frame's binary mask varies from 3 to 21 depending on the correlation coefficient between adjacent frames. The most preferable method for constructing the compact representation technology of the binary masks of frames represented in a differential form is the approach.

It will be developed an approach for reducing redundancy in arrays of a binary mask of a differential frame based on the requirements advanced.

In order to take into account the proposed requirements, it is proposed to use the approach for code representation of the sequence of binary mask series lengths. Which is based on the discovery of regularities in the alphabet's power Ω . The data source alphabet is a set of values that message elements can accept. Then the power Ω of the message source alphabet is the number of different elements in the alphabet. One of the simpliest and at the same time effective codes that take account of restrictions on the alphabet's power are Bodo codes. The Bodo code corresponds to the first two requirements.

Keywords

Binary series, binary mask, differential frame, redundancy, indicator, component, Bodo code, compact representation.

1. Introduction

A simple Bodo element-by-element code provides information about:

- the size of the computer memory;
- the maximum value $r_{\max}$ of the series length in the arrays of the differential frame's binary mask [1,2].

If a lengths sequence of binary series is given, i.e., $\Theta = \{r_1,...,r_{\Phi}\}$ then a simple Bodo code is formed from three stages:

Stage 1. The maximum value of the length of the binary series is sought, for which the formula is used:

$$r_{\max} = \max_{1 \le i \le \Phi}(r_i). \quad (1)$$

Stage 2. The determination of the number of bits $L(r)$, which is required to represent the

EMAIL: timochko.alex@gmail.com (A. 1); bpgpma@ukr.net (A. 2); l_vv83@ukr.net (A. 3)
ORCID: 0000-0002-4154-7876 (A. 1); 0000-0003-3216-1864 (A. 2); 0000-0003-0771-2660 (A. 3)

maximum value of the binary series $r_{\max}$ length, which is given by the relation:

$$L(r) = [\log_2 r_{\max}] + 1. \quad (2)$$

Step 3. The value $L(r)$ is writing at the beginning of the code representation and is the service information, which is indicating the code's description boundaries of the neighboring image elements [3-7]. After that, for every length of the binary series, a bit $L(r)$ is assigned to the code representation [8-10]. The total number of bits $L(r)_\Sigma$, which is required to represent all the lengths of a binary series is given by the expression:

$$L(r)_\Sigma = \Phi \cdot L(r). \quad (3)$$

Bodo's simple block code consists in representing in each code word several elements of the original image fragment. For example, this situation occurs when several elements of the encoded sequence are represented in one computer word (one external memory register).

2. Research of a compact representation of a differential-represented frame's stationary component's binary mask array

The Bodo method is mono-alphabetic. In this case, all elements of the processed sequence belong to the same alphabet. Such sequences are called mono-alphabetic [11-13].

However, the Bodo code does not meet the third requirement. This is due to the fact that the differential-represented frame's binary mask, under conditions of removal by a stationary camera, has a significant heterogeneity of the structural content. Under the heterogeneity of the structural content is understood that the stationary component can occupy a considerable space, cut by small elements of the dynamic component. In this case, the lengths $r(0)$ formed for the zero sequences will prevail over the length relative to the lengths $r(1)$ of the individual element sequences [14-17]. For such situation, the use of a power code in one alphabet will lead to the formation of code redundancy. Indeed, in accordance to the power code of one alphabet for all series lengths, regardless of their origin, code sequences of the same length $L(r)$ are formed. In this case, the total number of bits $L(r)_\Sigma$ per representation of the entire sequence of binary series lengths will be equal to:

$$L(r)_\Sigma = \sum_{i=1}^{\Phi} L(r)_i$$

Here are

$L(r)_i$ - the number of bits per representation of the i-th element of the sequences of the mask's binary series lengths;

Φ - the number of the binary series lengths, which are formed for the binary mask array of the differential frame.

At the same time, due to the heterogeneity of the structural content, the actual number of binary bits necessary to represent the entire sequence of binary series $L(r)'_\Sigma$ lengths will be much less than the value $L(r)_\Sigma$, ie:

$$L(r)'_\Sigma <<< L(r)_\Sigma$$

This leads to the presence of code redundancy:

$$R = L(r)_\Sigma - L(r)'_\Sigma$$

This situation is due to the fact, that for the code representation of the units' series lengths, a significantly smaller number of bits is required in comparison with the code representation of the zeros' series lengths, ie:

$$L(r(1)) <<< L(r(0))$$

Here are

$L(r(1))$ - the number of bits for the code representation of the zeros series lengths;

$L(r(0))$ - the number of bits for the code representation of the units' series lengths.

In order to eliminate the code redundancy, it is proposed to use two alphabets for the sequence Θ of binary series lengths [18]. The first alphabet Ω_0 is defined for the zeros series lengths, respectively the second alphabet Ω_1 is defined for the lengths of the one sseries. This approach allows to take into account the presence of a sharp heterogeneity in the structural content of the binary mask array. Accordingly, the generation of a power code for such sequences will be realized using a two-alphabet scheme [19].

The essence of the scheme is that:

1. The lengths of the zeros and ones series are formed, which are based on the array of the binary mask.

2. The entire sequence of binary series lengths is divided into two sub-sequences.

The first sub-sequence is formed on the basis of the zeros' series lengths:

$$\Theta^{(0)} = \{r(0)_1,...,r(0)_{\Phi_0}\}$$

The second sub-sequence is formed on the basis of the units' series lengths:

$$\Theta^{(1)} = \{r(1)_1,...,r(1)_{\Phi_1}\}$$

Then the total number of bits per representation of the subsequences of the zeros' series lengths will be:

$$L(r(0))_\Sigma = \Phi_0 \log_2 r(0)_{\max}, \quad (4)$$

And the total number of bits per sub-sequence representation of the units' series lengths will be:

$$L(r(1))_\Sigma = \Phi_0 \log_2 r(1)_{\max}. \quad (5)$$

3. For each subsequence, own alphabet is forming, respectively, Ω_1 and Ω_0.

4. The power code is constructed in accordance with the constructed alphabets [20].

The power code is constructed according to the scheme, which is considered above, is called a two-halftone code. In other words, a two-alphabetic power code is a power code generated for two-alphabetic sequences.

Here, the sizes of the binary regions are taken into account as a result of identifying the binary series lengths. It will be shown, that for a two-index power code relative to the binary series lengths of the differential frame's binary mask, the condition holds, i.e. provides a degree of compression:

$$\eta_M = \frac{m_M n_M}{\Phi_0 \log_2 r(0)_{\max} + \Phi_1 \log_2 r(1)_{\max}} = \frac{\sum_{i=1}^{\Phi} r_i}{\log_2 (r(0)_{\max}^{\Phi_0} \cdot r(1)_{\max}^{\Phi_1})}$$

Here are

Φ_0 -the number of the zeros' lengths for the binary mask of the differential-represented frame;

Φ_1 - the number of units' series lengths for the binary mask of the differential-represented frame.

Example. Let's calculate the number of digits $L(r)_\Sigma$ in order to represent the entire sequence of series lengths for the binary mask of the differential-represented frame Q due to a one-rate power code.

First, let's define the maximum value of the binary series length $r_{\max}$ in a sequence of binary series lengths $\Theta = \{r_1 = 19; r_2 = 1; r_3 = 4; r_4 = 5; r_5 = 1; r_6 = 3; r_7 = 3\}$, which is based on expression $r_1 = 19$; $L(r)_1 = 5$ bits; $r_2 = 1$; $L(r)_2 = 1$ bit; $r_3 = 4$; $L(r)_3 = 2$ bits; $r_4 = 5$; $L(r)_4 = 3$ bits; $r_5 = 1$; $L(r)_5 = 1$ bit; $r_6 = 3$; $L(r)_6 = 2$ bits; $r_7 = 3$; $L(r)_7 = 2$ bits.

The maximum binary mask series length of a differential-represented frame $r_{\max} = 19$. Then, on the basis of expression (2), the number of bits required to represent the maximum binary mask series length is equal to $L(r) = 5$ bits.

The number of the binary series lengths is formed for the differential frame's binary mask's array $\Phi = 7$. Then, on the basis of the expression (3) the total number of bits on the representation of the binary series lengths sequence will be equal to a $L(r)_\Sigma = 5 \cdot 7 = 35$ bits.

At the same time, 36 digits are required for the code representation of the original image fragment (the image fragment is classified as highly saturated with details having different dynamic components) [21]. Consequently, by applying a single-alphabetic power code for all sequences of series lengths, the binary mask size of the differential-represented frame will be reduced by 3%.

At the same time, 36 bits are required for the code representation of the original image fragment (the image fragment is classified as highly saturated with details having different dynamic components). Therefore, due to the use of a double-alphabetic power code for the subsequences of the lengths of zeros and ones series. The differential-represented frame's binary mask volume will decrease by 20%. Also, due to the double-alphabetic power code, the volume of the differential-represented frame's binary mask is relative to the single-alphabet code will decrease by 17%.

3. Conclusions

1. As the correlation coefficient between adjacent frames increases, the compression ratio of the differential-represented frame's binary mask increases.

2. The compression ratio of the differential-represented frame's binary mask varies from 3 to 21 depending on the correlation coefficient between adjacent frames.

3. Estimation of the bit representation's information content of the differential-represented frame's binary mask on the basis of accounting for the nonequilibrium of the bases of the lengths of the binary series does not require an increase in the complexity of the software-hardware implementation.

4. Due to the double-alphabetic power code, the differential-represented frame's binary mask is relative to the single-alphabet code will decrease by 17%.

4. References

[1] V. Larin, D. Yerema, Y. Bolotska. The reasoning of necessity enhancing video privacy in conditions of providing the quality of the video information service provided in virtual infocommunication systems. Системи озброєння і військова техніка 2(35). – Х. ХНУПС. 2019, P. 158-162. http://www.hups.mil.gov.ua/periodic-app/article/19290.

[2] Qassim, H., Verma, A., Feinzimer, D. (2018). Compressed residual-VGG16 CNN model for big data places image recognition. 2018 IEEE 8th Annual Computing and Communication Workshop and Conference (CCWC). DOI: https://doi.org/10.1109/ccwc.2018.8301729.

[3] Centaur ® Enhanced High Capacity Data Radio (EnHCDRTM) – ITT Exelis Inc., 2012. [Електронний ресурс].URL: http:// www.exelisinc. com/ solutions/ Enhanced-High-Capacity-Data-Radio/ Documents/Centaur-Enhanced-High-Capacity-Data-Radio-(EnHCDR).pdf.

[4] VNI Forecast Highlights, [Электронный ресурс] / Cisco // Cisco. – 2015. – http://www.cisco.com/c/en/us/solutions/service-provider/visual-networking-index-vni/vni-forecast.html.

[5] Pavlenko. Conceptual Basis of Cascading Differential Masking Technology. / Pavlenko, Tymochko, Kolmykov, Khmelevskiy, Larin.// IEEE 11 th International Conference on Dependable Systems, Services and Technologies. DESSERT: 2020. – p. 290 -294. DOI: 10.1109/DESSERT50317.2020.9125024.

[6] Li, L. (2015). The UAV intelligent inspection of transmission lines. Proceedings of the 2015 International Conference on Advances in Mechanical Engineering and Industrial Informatics. DOI: https://doi.org/10.2991/ameii-15.2015.285.

[7] Gonzales R.C. Digital image processing / R.C. Gonzales, R.E. Woods. – Prentice Inc. Upper Saddle River, New Jersey, 2002. – 779 p. http://web.ipac.caltech.edu/staff/fmasci/home/astro_refs/Digital_Image_Processing_2nd Ed.pdf.

[8] Kharchenko V., Mukhina M. Correlation-extreme visual navigation of unmanned aircraft systems based on speed-up robust features //Aviation. 2014. Vol. 18, Issue 2. P. 80–85. DOI: https://doi.org/10.3846/16487788.2014.926645.

[9] M.Pavlenko, A.Timochko, N.Korolyuk, M.Gusak. Hybrid model of knowledge for situation recognition in airspace. Automatic Control and Computer SciencesVolume 48, Issue 5, 2014, Pages 257-263. https://www.edi.lv/wp-content/uploads/2019/09/Vol.48_Issue-5_2014.pdf.

[10] Wang, S., Zhang, X., Liu, X., Zhang, J., Ma, S., Gao, W. Utility-Driven Adaptive Preprocessing for Screen Content Video Compression. (2017) IEEE Transactions on Multimedia, 19 (3), art. no. 7736114, pp. 660-667. DOI: 10.1109/TMM.2016.2625276.

[11] Tkachov, V. M., Tokariev, V. V., Radchenko, V. O., Lebediev, V. O. (2017). The Problem of Big Data Transmission in the Mobile "Multi-Copter – Sensor Network" System. Control, Navigation and Communication Systems, 2, 154–157. URL: http://openarchive.nure.ua/bitstream/document/4536/1/suntz_2017_2_40.pdf.

[12] Kharchenko N. The Problem Aspect of Control of Bit Speed of the Video Stream in Telecommunication Networks / Andrii Krasnorutskij, Andrii Tristan, N. Kharchenko // International Conference TCSET'2014 ["Modern problems of radio engineering, telecommunications, and

computer science"] (Lviv-Slavske, Ukraine, February 25 – March 1, 2014) / Lviv Polytechnic National University, 2014. – P. 533-534. https://www.researchgate.net/publication/301793981_Developing_PC_Software_Project_Duration_Model_based_on_Johnson_transformation.

[13] Mistry, D., Modi, P., Deokule, K., Patel, A., Patki, H., Abuzaghleh, O. (2016). Network traffic measurement and analysis. 2016 IEEE Long Island Systems, Applications and Technology Conference (LISAT). URL: http://ieeexplore.ieee.org/abstract/document/7494141.

[14] The Problem of Big Data Transmission in the Mobile "Multi-Copter – Sensor Network" System / Tkachov V. M., Tokariev V. V., Radchenko V. O., Lebediev V. O. // Control, Navigation and Communication Systems. 2017. Issue 2. P. 154–157. URL: http://nbuv.gov.ua/UJRN/suntz_2017_2_40.

[15] Network traffic measurement and analysis / Mistry D., Modi P., Deokule K., Patel A., Patki H., Abuzaghleh O. // 2016 IEEE Long Island Systems, Applications and Technology Conference (LISAT). 2016. DOI: 10.1109/lisat.2016.7494141.

[16] Buranova M. A., Kartashevskyi V. H., Samoilov M. S. The comparative analysis of statistical characteristics of the video traffic in networks of the packet transmission of data // Infokommunikacionnye tehnologii. 2013. Vol. 11, Issue 4. P. 33–39. URL: https://readera.ru/read/140191662.

[17] Development of a method for the experimental estimation of multimedia data flow rate in a computer network. Sumtsov, D. Osiievskyi, S. Lebediev, V. Eastern-European Journal of Enterprise Technologies. Volume 2, Issue 2-92, 2018, Pages 56-64. URL: http://journals.uran.ua/eejet/article/view/128045.

[18] Ruban, I., Smelyakov, K., Vitalii, M., Dmitry, P., Bolohova, N. Method of neural network recognition of ground-based air objects (2018) Proceedings of 2018 IEEE 9th International Conference on Dependable Systems, Services and Technologies, DESSERT 2018, pp. 589-592. URL: https://ieeexplore.ieee.org/abstract/document/8409200.

[19] Mashtalir, S., Mikhnova, O., Stolbovyi, M. Sequence Matching for Content-Based Video Retrieval (2018) Proceedings of the 2018 IEEE 2nd International Conference on Data Stream Mining and Processing, DSMP 2018, art. no. 8478597, pp. 549-553. URL:https://ieeexplore.ieee.org/document/8478597.

[20] Piramanayagam, S., Saber, E., Cahill, N.D., Messinger, D. Shot boundary detection and label propagation for spatio-temporal video segmentation (2015). Proceedings of SPIE - The International Society for Optical Engineering, 9405. DOI: 10.1117/12.2076661.

[21] Serhii Yevseiev. Development of an advanced method of video information resource compression in navigation and traffic control systems. EUREKA: Physics and Engineering. No. 5 (2020), Pages 31-42. DOI: 10.21303/2461-4262.2020.001405.

Protection Of Numerical Information Based On Permutations

Oleksiy Borysenko [1], Oleksii Horiachev [2], Viktor Serdyuk [3], Andriy Horyshnyak [4], Oleksandr Kobyakov [5] and Olga Berezhna [6]

[1-6] *Sumy State University, st. Rimsky-Korsakov, 2, Sumy, Ukraine*

Abstract

The article solves the problem of protecting decimal numbers used in systems of information transmission, processing and storage from unauthorized access with simultaneous correction of single errors in them and detection of error bursts. To protect the decimal number, each of its digits is first converted to a binary-decimal digit, and then, using a special table, into a binary-coded permutation. After that, the digits of the decimal number themselves are mixed. The paper gives estimates of the level of secrecy of decimal numbers encoded in this way. Since each digit of a decimal number can contain one of 10 digits, 10 permutations are required to encode them. To obtain them, at least 4 elements 0, 1, 2, 3 are required. They form 24 permutations, of which 14 are redundant. Specially selected 10 binary-coded permutations out of 24 form a binary-coded permutation code with a minimum code distance equal to 4. This allows correction of any single error and detection of double errors on the set of permutations.

Keywords

Information protection, numerical codes, secrecy, permutations, errors, noise immunity

1. Introduction

In practice, binary-decimal codes have become widespread, with the help of which information from various sensors is extracted and transmitted, for example, information about the amount of consumed thermal and electrical energy, water and other similar indications. Usually, each binary-decimal digit taken from the sensor is transmitted over a communication channel, essentially a telecommunication system, which includes a buffer memory with an encoder, a communication line, an information display device, and a receiver with a decoder [1]. The communication line can be both wired and mobile, using radio communication. In the latter case, information can be transmitted directly to moving objects, such as cars.

However, the transmitted information in some cases must be protected from unauthorized access. To do this, the binary-decimal digits of each decimal number are uniformly mixed using the appropriate tables. At the receiving end, these tables allow to restore the original information. They are, in essence, cipher keys. Moreover, the secrecy of the mixed each binary-decimal place can be significantly increased by additional mixing of the bits of binary-decimal numbers.

However, in addition to protecting against unauthorized access, it is often required to further increase the noise immunity of the transmitted binary-decimal numbers.

Binary-decimal coding protects to a certain extent the transmitted or stored decimal digits from interference due to the redundancy of a binary-decimal code containing sixteen four-bit binary-decimal code words. However, the level of protection against interference is still low, although for a number of practical cases it may be acceptable. Therefore, it became necessary to increase it.

It was proposed to solve this problem in [1-4] using binary-decimal error-correcting codes, which are essentially decimal digits encoded with error-resistant combinations. For this purpose in [1] the coding of binary-decimal digits by equilibrium code combinations was introduced, which significantly increased the ability of the telecommunications system to detect errors [1-4].

EMAIL: 5352008@ukr.net (A. 1); alevgor@gmail.com (A. 2); viktman2012@gmail.com (A. 3); a.horishnyak@ias.sumdu.edu.ua (A. 4); kobyakova@ukr.net (A. 5); o.berezhna@ekt.sumdu.edu.ua (A. 6).

To assess the noise immunity of such codes, it was proposed to use formulas for the probabilities of transition of code combinations into classes of correct combinations, allowed erroneous combinations that are not detected and forbidden combinations that can be detected [5]. According to the results of the analysis, it was concluded that the use of equilibrium codes provides the requirements of the reliability class I1 of the international standard IEC 870-5-1-95 in the whole range of failure levels of one bit of information [1].

At the same time, the secrecy of information was increased, since there was no reliable test for unravelling their values, because statistics for decimal digits presented in the form of equilibrium code combinations does not help well, unlike text information, for the decoding of which the statistical probabilities of letters play an essential role.

However, errors in the transmission of decimal digits by equilibrium code combinations are difficult to eliminate, and the implementation of ARQ in mobile communications is sometimes difficult. Therefore, the task arose of developing a telecommunication system that would not only detect errors, but also correct them, using inseparable codes, in order to hide the true value of decimal digits during transmission.

2. Problem statement

The task of this work is to increase the noise immunity of transmitted binary-decimal digits, accompanied by error correction, with sufficient protection against unauthorized access.

For this, it is proposed to enhance the noise immunity of binary-decimal information by using inseparable codes on permutations, since, on the one hand, they allow error detection and correction, and on the other hand, they can hide the true information deeper.

Permutations are widespread in mathematics. Permutations are used in abstract algebra, and they are also used to solve combinatorial optimization problems, for example, the travelling salesman problem [6-8].

In addition to solving mathematical problems, permutations are used in practical problems of protecting information from unauthorized access [9-16]. The area of their possible application is constantly expanding. Along with this, permutations successfully solve the problem of anti-jamming coding, since by their nature they contain redundant information, which makes it relatively easy to find and, which is especially important for small mobile devices, to eliminate errors in messages transmitted with their help [17,18]. In addition, the permutations make it possible to combine solutions to the problems of anti-jamming coding with effective protection of information from unauthorized access.

3. Coding with permutations

Any finite sequence of distinct elements of length n is a permutation. While any symbols can be elements of permutations, most often numbers are used as them. For example, a sequence of four different digits 0123 would be a permutation of length $n = 4$. At the same time, a sequence of 1011 of length $n = 4$ would not be a permutation, since it only consists of two different repeating elements 0 and 1.

The set of n! permutations of length n forms a permutation code. The difference $n \cdot \log_2 n - \log_2 n!$ forms redundant information of this code, which with increasing of n can reach a significant value, determining the high noise immunity of codes on permutations. In addition, permutations do not have repeating elements and, therefore, obtaining their statistics is difficult. It can be obtained, with high effort, only on a large number of permutations, which greatly complicates the deciphering of information hidden in the permutations.

In the tasks of anti-jamming coding and information protection the elements of permutations are represented in binary form. Such their representation will be called binary-coded. The number of binary bits in binary-coded permutations is defined as the whole logarithm of the permutation elements number n:

$$m = \lceil \log_2 n \rceil \quad (1)$$

10 different binary-coded permutations are required to encode binary-decimal information. Therefore, the minimum value of n that can provide the required number of permutations will be 4, since $4 \times 3 \times 2 = 24 > 10$. Of these 24 permutations, 10 permutations are used to encode 10 binary-decimal digits. Each of them encodes one of the digits, for example, permutation 0123 is used to encode 0. The remaining 14 possible permutations are redundant. One of the possible variants of representation of binary-decimal digits by permutations is shown in Table 1. Together, binary-decimal digits in Table 1 form a binary-decimal code (2-10 code).

Table 1
Coding with permutations

№	2-10 code	Permutations
0	0000	0123
1	0001	0132
2	0010	0213
3	0011	0231
4	0100	0312
5	0101	0321
6	0110	1023
7	0111	1032
8	1000	1203
9	1001	1230

3.1. Information secrecy

The number of encoding variants of binary-decimal digits by permutations will be equal to the number of combinations 10 out of 24, each of which can be specified by the corresponding table, like Table 1. Each of these variants, in turn, can be represented by one of 10! permutations encoding 10 digits, each of which can also be represented in the form of a table. Each of these tables can act as a cipher key, consisting of $10!\cdot C^{10}_{24}$ permutations for one decimal place.

In addition, the decimal digits, the number of which is equal to k, can also be shuffled in various ways during their transmission. Accordingly, the total number of permutation variants that can be used to encrypt the decimal permutation code will be equal to $M = k!\cdot 10!\cdot \cdot C^{10}_{24}$. If k, for example, equals 10, then the number of variants of the cipher $M = 10!\cdot 10\cdot \cdot C^{10}_{24} = 2.58\cdot 10^{19}$. This is a fairly large number of brute force options required to break the cipher. It should be borne in mind that the statistics of the numbers in the permutation cipher is poorly expressed, which greatly complicates its disclosure. The dependence of the M value, which characterizes the complexity of the proposed cipher disclosure, from the parameter k is shown in Table 2 and in the graph Figure 1.

Table 2
Number of permutations M

k	M	k	M
1	$7.11\cdot 10^{12}$	5	$8.54\cdot 10^{14}$
2	$1.42\cdot 10^{13}$	6	$5.12\cdot 10^{15}$
3	$4.27\cdot 10^{13}$	7	$3.58\cdot 10^{16}$
4	$1.70\cdot 10^{14}$	8	$2.86\cdot 10^{17}$
9	$2.58\cdot 10^{18}$	15	$9.30\cdot 10^{24}$
10	$2.58\cdot 10^{19}$	16	$1.48\cdot 10^{26}$
11	$2.84\cdot 10^{20}$	17	$2.53\cdot 10^{27}$
12	$3.40\cdot 10^{21}$	18	$4.55\cdot 10^{28}$
13	$4.43\cdot 10^{22}$	19	$8.65\cdot 10^{29}$
14	$6.20\cdot 10^{23}$	20	$1.73\cdot 10^{31}$

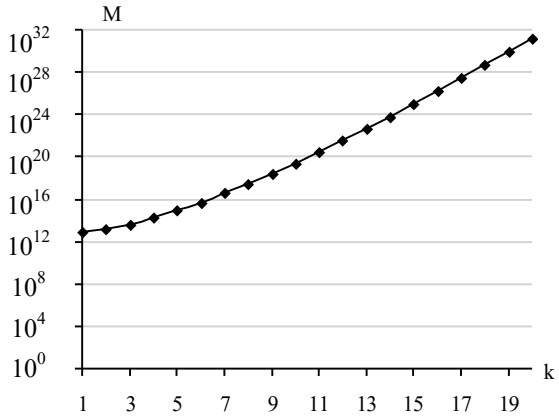


Figure 1: Graph of M versus k

3.2. Evaluation of the noise immunity of the code on permutations

In addition to secrecy, permutations can significantly increase the noise immunity of the binary-decimal code. This is due to the fact that the binary-coded representation of such permutations according to formula (1) will contain four digits of length $m = 2$. Permutations P of length $n = 4$ and their binary-coded representation BCP are presented in Table 3.

Table 3
Binary-coded permutations

P	BCP	P	BCP
0123	00 01 10 11	2013	10 00 01 11
0132	00 01 11 10	2031	10 00 11 01
0213	00 10 01 11	2103	10 01 00 11
0231	00 10 11 01	2130	10 01 11 00
0312	00 11 01 10	2301	10 11 00 01
0321	00 11 10 01	2310	10 11 01 00
1023	01 00 10 11	3012	11 00 01 10
1032	01 00 11 10	3021	11 00 10 01
1203	01 10 00 11	3102	11 01 00 10
1230	01 10 11 00	3120	11 01 10 00
1302	01 11 00 10	3201	11 10 00 01
1320	01 11 10 00	3210	11 10 01 00

Each permutation differs from others by at least two elements, and therefore, the minimum code distance in a binary code on permutations is 2. Such a code distance allows detecting in binary-coded permutations all single errors, as well as all errors of odd multiplicity 1, 3, 5, ...

Increasing the code distance will improve the noise immunity of binary-coded permutations. To achieve this, out of all 24 permutations of length $n = 4$, 10 allowed permutations should be selected, as shown in Table 4, which differ from each other by three elements, and thereby ensure the minimum code distance between their binary representations equal to 4. This allows not only detecting double errors in binary-coded permutations, but also correcting any single error in them.

Table 4

Permutations with minimum code distance 4

P	BCP	P	BCP
0123	00 01 10 11	2013	10 00 01 11
0231	00 10 11 01	2130	10 01 11 00
0312	00 11 01 10	2301	10 11 00 01
1203	01 10 00 11	3021	11 00 10 01
1320	01 11 10 00	3102	11 01 00 10

3.2.1. The fraction of detected errors

The noise immunity of a code on binary-coded permutations can be estimated using a characteristic called the fraction of detected errors D [5, 18]. It shows the probability with which any error translates the permutation into a forbidden combination that can be detected. The D value is defined as the ratio of the number of forbidden combinations Z_f to the total number of combinations $D = Z_f / n^n = 246 / 256 = 0.96$.

4. Error detection

A transmission error can translate a binary-coded permutation into either a forbidden combination that is not a permutation, or into one of the permutations. In the case where an error converts a permutation to a non-permutation combination, it can be easily detected as follows.

First, since all permutations contain the same elements, arranged in a different order, the sum of the binary numbers encoding these elements must remain constant. It forms a checksum, the same for all permutations, equal to

$$S = n \cdot (n - 1) / 2 . \quad (2)$$

It can be used to detect erroneous combinations, the checksum of which does not coincide with the value determined by the formula (2) [17]. For the considered code on permutations, such a checksum is equal to $S = 4 \cdot (4 - 1) / 2 = 6$.

Example 1. On the receiving side, during permutation transmitting, a sequence of elements 1231 was received, which is not a permutation. Counting the sum of these elements gives the result 1 + 2 + 3 + 1 = 7. This number does not coincide with the checksum value obtained above for the code on permutations $S = 6$. This means that the resulting sequence is not a permutation and contains an error.

Second, the appearance of two or more identical elements in a permutation, during its transmission or storage obviously transforms it into a combination that is not a permutation. Then, by comparing the elements of the transmitted combinations on the receiving side, it is possible to establish whether they are permutations or not.

Example 2. On the receiving side, a sequence of elements 1231 was obtained. As a result of comparing the first element of this sequence with all other elements, it is found that it coincides with the fourth element: 1 23 1. Therefore, the resulting sequence is not a permutation and contains an error.

4.1. Double error detection

In the case when a double error occurs during the transmission of a binary-coded permutation, it can translate into one of the 14 forbidden permutations. The fact that the allowed permutation can translate solely into the forbidden permutation is explained by using for the encoding of numerical information only permutations with the minimum code distance 4. Such an error can be detected on the receiving side by comparing the received permutation with all allowed permutations given in Table. 4. If a match of the received permutation with one of the 10 allowed permutations is found, then the decision is made that it is correct; otherwise it is forbidden and contains a double error.

Example 3. Permutation 0123 (00 01 10 11) after the interference translated into permutation 1023 (01 00 10 11). Comparing this permutation with all allowed permutations presented in Table 4, shows no coincidence with any of them and, accordingly, indicates that it is forbidden. Therefore, it contains a double error. Indeed, in

the permutation 0123 0 transformed into to 1, and 1 into 0.

4.2. Error correction

Comparing a binary-coded permutation containing an error in any element with all 10 allowed permutations allows a single error to be corrected. All permutations except one will differ from the erroneous sequence by more than one element. Any permitted permutation that differs from a permutation with an error in one element will be considered its corrected value.

Example 4. On the receiving side, a sequence of elements 1231 was received. By calculating the checksum and comparing the elements with each other, it is found that this sequence is not a permutation, which means that it contains an error. Since the minimum coding distance for permutations of Table 4 is 4, it is possible to correct a single error. To correct it, the erroneous sequence 1231 is compared with all allowed permutations in Table 4. As a result of this comparison, it is found that among the allowed permutations only one permutation 0231 differs from the obtained sequence by one element. This permutation is recorded as the correct value of the received sequence: 1231 → 0231.

However, the use of specially selected permutations for detecting double errors and correcting single errors reduces the level of secrecy of information, since the opponent can start breaking the cipher just from the analysis of these permutations. Therefore, it is necessary to weigh what is more important for the transmission of information, its noise immunity or secrecy, and accordingly choose the method of protecting decimal digits from interference.

4.3. Algorithm for detecting and correcting errors

The error detection and correction algorithm contains the following steps.

Step 1. In the received binary combination of 8 bits, the sum of its permutation elements, each of which consists of 2 binary digits, is calculated. If the calculated value equals 6, then it is considered as one of 24 binary-coded permutations, which may be correct or incorrect.

Step 2. The received permutation is compared with 10 allowed binary-coded permutations representing decimal digits. In the case when there is allowed permutation that coincides with the received permutation, then it is written as correct. If it differs from all the allowed permutations by the value of two or more elements, then it is erroneous and can be corrected by ARQ.

Step 3. If the calculated value doesn't equal 6, then the received binary combination is an erroneous sequence that is not a permutation. In this case, some of its elements have the same value. If the received sequence differs from one of the 10 allowed permutations in only one element, then this one permutation will be the corrected permutation. In other case the error can only be corrected by ARQ.

5. Conclusions

The inseparable code on permutations proposed in the work for encoding digits allows solving the problem of digital information transmission secrecy, and at the same time ensures its noise immunity. Wherein, the secrecy of information can reach acceptable values for many applications due to the special properties of the permutations, which make it possible to hide the statistics of the transmitted decimal digits.

Along with the secrecy the permutations can effectively solve the problem of increasing the noise immunity of the transmitted digits. They allow detection of errors bursts and fix single errors. It is also important that the considered methods of detecting and correcting errors in permutations, used to encode decimal digits, are quite simple to implement.

6. References

[1] O. Borysenko, O. Berezhna, A. Novhorodtsev, V. Serdyuk, M. Yakovlev, "Information transmission and display system with numerical data protection", Information processing systems. Vol. 2 (157), 2019, pp. 103-108. (in Ukrainian)

[2] O. Borysenko, V. Kalashnikov, Chapter 7: "Description and applications of binomial numeral systems complex" in Security and noise immunity of telecommunication systems: new solutions to the codes and signals design problem: Collective monograph. ASC Academic Publishing, Minden, Nevada, 2017, pp. 147-159.

[3] A. Kuznetsov, R. Serhiienko, D. Prokopovych-Tkachenko, B. Akhmetov, "Chapter 3: Representation of cascade codes

in the frequency domain" in Security and noise immunity of telecommunication systems: new solutions to the codes and signals design problem: Collective monograph. ASC Academic Publishing, Minden, Nevada, 2017, pp. 71-101.

[4] A. Kuznetsov, S. Ksvun, Y. Gorbenko, "Chapter 4: The methodology of evaluating the energy gains from coding in channels with grouping errors" in Security and noise immunity of telecommunication systems: new solutions to the codes and signals design problem: Collective monograph. ASC Academic Publishing, Minden, Nevada, USA, 2017, pp. 102-119

[5] N.T. Berezyuk, Information coding (binary codes). Directory. Edited by N.T. Berezyuk, Vishcha shkola, Kharkiv, 1978. (in Russian)

[6] E. Reinhold, J. Nivergelt, N. Deo, Combinatorial algorithms: theory and practice, Mir, Moscow, 1980. (in Russian)

[7] D.Knuth, The Art of Computer Programming, Vol. 1: Fundamental Algorithms, 3rd ed., Addison-Wesley Professional, 1997.

[8] D.Knuth, The Art of Computer Programming, Vol. 4A: Combinatorial Algorithms, Part 1, 1st ed., Addison-Wesley Professional, 2011.

[9] D. Smith, R. Montemanni, "A new table of permutation code", Designs, Codes and Cryptography, Vol. 63, pp. 241–253, 2012.

[10] W. Stallings, Cryptography and Network Security Principles and Practices, fourth ed., Prentice Hall, 2005.

[11] R. Girija, H. Singh, "A new substitution-permutation network cipher using Walsh Hadamard Transform" in Proceedings of International Conference on Computing and Communication Technologies for Smart Nation (IC3TSN), 2017, pp. 168 - 172. DOI: 10.1109/IC3TSN.2017.8284470

[12] A. Aryal, S. Imaizumi, T. Horiuchi, H.i Kiya, "Integrated algorithm for block-permutation-based encryption with reversible data hiding" in Proceedings of Asia-Pacific Signal and Information Processing Association Annual Summit and Conference (APSIPA ASC), 2017, pp. 203 - 208. DOI: 10.1109/APSIPA.2017.8282028

[13] I. Janiszczak, R. Staszewski, "An improved bound for permutation arrays of length 10", [On-line]. Available: http://www.iem.uni-ue.de/preprints/IJRS.pdf [October 16, 2014].

[14] R. Montemanni, J. Barta, D.H. Smith, "Permutation codes: a branch and bound approach" in Proceedings of the International Conference on Pure Mathematics, Applied Mathematics, Computational Methods (PMAMCM), 2014, pp. 86-90.

[15] J. Barta, R. Montemanni, "Hamming Graphs and Permutation Codes" in Proceedings of Fourth International Conference on Mathematics and Computers in Sciences and in Industry (MCSI), 2017, pp. 154 -158. DOI: 10.1109/MCSI.2017.35

[16] J. Barta, R. Montemanni, D.H. Smith, "A branch and bound approach to permutation codes" in Proceedings of the IEEE Second International Conference of Information and Communication Technology (ICOICT), 2014, pp. 187–192. DOI: 10.1109/ICoICT.2014.6914063

[17] O. Borysenko, O. Horiachev, "Interference-free transmission of economic information on the basis of permutations", Actual problems of economics. Kyiv, vol. 3 (141), 2013, pp. 156 - 163. (in Russian)

[18] O. Borysenko, O. Horiachev, S.Matsenko, O.Kobiakov, "Noise-immune codes based on permutations" in Proceedings of 9th International IEEE Conference «Dependable Systems, Services and Technologies DESSERT'2018», 2018, pp. 645 - 648. DOI: 10.1109/DESSERT.2018.8409204

Methodical Approach To The Development Of A Mathematical Model For Calculating The Combat Potentials Of Strike Unmanned Aircraft

Dmytro Ikaiev[1], Yaroslav Yaroshenko[2], Andrii Shalyhin[3], Volodymyr Nerubatskyi[4], Valerii Bondar[5], Volodymyr Herasymenko[6]

[1,2,5,5]*The National Defence University of Ukraine named after Ivan Cherniakhovskiy, 28 Povitroflotskyi avenue, Kyiv, 03049, Ukraine*
[3,4]*Ivan Kozhedub Kharkiv National Air Force University, 77/79 Sumska street, Kharkiv, 61023, Ukraine*

Abstract

The article considers the issue of assessing the combat potential of a strike unmanned aerial vehicle. An analysis of existing methods for assessing the combat potential of manned aircraft and found that they often use methods of expert assessment, which require a significant number of experienced experts and are quite time consuming. The scientific and methodical apparatus for calculations is given: probabilities of unmanned aerial vehicle damage for one departure and for a certain number of departures; mathematical expectation (average number) of combat sorties; mathematical expectation (average value) of the number of single targets hit in one combat flight by an unmanned aerial vehicle; the maximum value of the mathematical expectation (average value) of the relative number of single targets hit in one combat flight by an unmanned aerial vehicle; mathematical expectation of the number of single targets hit by an unmanned aerial vehicle; maximum mathematical value expectations of the number of single targets hit by an unmanned aerial vehicle for the entire period of life; the coefficient of combat potential of the unmanned aerial vehicle; the average combat potential of an unmanned aerial vehicle. The construction of a mathematical model of combat potentials of strike unmanned aerial vehicles based on a block-hierarchical approach is carried out. In this approach, the mathematical model of the modeling object is not represented as a function of many variables, but as a hierarchy of models of much smaller dimension. The basis for building a hierarchy of models is the physical content of the modeling object and the patterns it reflects.

Keywords

group of manned and unmanned aerial vehicles, combat potentials of unmanned aerial vehicles, indicators of combat effectiveness, unmanned aerial vehicle, methods of calculating combat potential.

1. Introduction

In the field of unmanned aerial vehicles, there is a transition from the single use of unmanned aerial vehicles (UAVs) to the group (mass) use in cooperation with manned aircraft. In addition to reconnaissance tasks and individual tasks of combat support of manned aircraft, strike tasks of UAVs are becoming increasingly important [1-6]. This raises the questions of the assessment of the combat potential (CP) of strike UAVs.

The problem is that the methods of estimating of the CP of UAVs, which are similar to the methods of estimating of the CP of manned aircraft, have not found appropriate distribution.

EMAIL: chvtau@gmail.com (A. 1); yar_yaroshenko@ukr.net (A. 2); shalyhin_andrii@ukr.net (A. 3); ner1976@ukr.net (A. 4); valerii.bondar.ua@gmail.com (A. 5); gera410@ukr.net (A. 6);
ORCID: 0000-0003-4161-7579 (A. 1); 0000-0002-8651-4920 (A. 2); 0000-0002-1828-2443 (A. 3); 0000-0003-3090-1865(A. 4); 0000-0001-8843-680X (A. 5); 0000-0003-2014-7408 (A. 6)

The known methods of estimating of the combat potential of the manned aircraft are based mainly on the methods of expert assessments [7, 8, 9, 10]. This is a quite time-consuming process and requires the involvement of a significant number of experts with experience in combat use of aircraft. The application of such methods for a large number of existing and perspective UAVs is problematic and practically impossible to implement. Therefore, there is a need to develop approaches to the assessment of the CP of UAVs, which do not require the use of expert assessment methods.

Analysis of the recent researches and publications

In [7] it was noted that in the late 50s of the last century the military authorities had the need for a simple and clear way to compare different types of weapons to solve combat tasks and correctly calculate the balance of forces of the parties in operations. This was due to the fact that with the increase in the variety of weapons and their increasingly narrow specialization, it became almost impossible to determine the ratio of forces by the ratio of individual types of weapons. It was assumed that different types of weapons could be compared in terms of contribution to the end result of hostilities, and therefore each of them could be assigned a weight efficiency factor. Over time, this factor has been defined as the combat potential (CP) of the sample of armaments. CP of the sample of armaments could be considered as a criterion of the totality of samples of armaments for its contribution to the achievement of the objectives of an operation (hostilities).

Initially, the CP of armaments samples were determined either empirically, based on statistics obtained from past wars (armed conflicts) [7], or by methods of expert evaluation.

In the 80s years of the last century the methods of mathematical modeling of hostilities [8] began to be used to determine the CP. The special studies conducted on mathematical models of combat operations have revealed that there is no constant uniform measure of comparison of different types of weapons. CP of a sample of armaments – is a variable value and it is determined not only by its characteristics, but also by its quantity, structure of armaments of confronting groups, type of operation, quality of management, combat and other types of maintenance and by other operational factors.

The construction of mathematical models of aircraft CP, which take into account a fairly complete list of aircraft characteristics and conditions of their use, proved to be quite a problematic task. An alternative solution of this problem remains the methods of expert assessments.

The purpose of the article is to determine the approach to construction of a mathematical model for calculating the combat potential of a strike UAV without the involvement of expert or other "fuzzy" information.

2. Presentation of the main material

The difficulty of constructing analytical mathematical models for calculating the CP of aircraft functionally related to the characteristics of aircraft, their weapons and parameters of combat conditions, can be attributed to the non-integrability of the vast majority of systems of differential equations [11]. Including differential equations that adequately describe the fighting. Regressive mathematical models, which can be built on the basis of mathematical modeling data (numerical experiments) or expert survey data, have significant shortcomings and limitations [12]. They do not provide a full-fledged replacement for analytical models. In this article, the construction of a mathematical model of CP of UAVs is based on a block-hierarchical (decomposition) approach. In this approach, the mathematical model of the modeling object (CP of UAV) is not represented as a function of many variables, but as a hierarchy of models of much smaller dimensions. The basis for building a hierarchy of models, as will be noted below, is the physical content of the modeling object and the patterns it reflects [13].

The concept of "combat potential of a sample of weapons", judging by its various definitions [14], still remains controversial. Below, for example, there are two different definitions of "the combat potential of a sample of weapons".

Combat potential of a sample of weapons is an integral indicator that characterizes the maximum set of tasks performed by the sample weapons and military equipment (WME) for the intended purpose in the implementation of the limit tactical and technical characteristics (TTC) for the typical operating time in typical design conditions [15, 16].

The combat potential of a sample of weapons is an integral indicator that characterizes the maximum amount of combat tasks that can perform a sample of weapons for its functional

purpose in the given (calculated) conditions of use during its existence [17].

In the definition [17], the most significant difference from the definition [15] is that the key feature is not a vague feature – the characteristic time, but the time of existence of the sample of weapons before its defeat. In particular, if the characteristic time is taken as a time interval that is less than the lifetime of the sample, the combat potential will be determined essentially by the fire performance or firepower of the sample. But the concept of "fire performance" reflects the meaning of a different indicator than "combat potential", because it does not take into account the ability of the weapon to survive in the face of the enemy and continue to function.

As shown in [13], the overall purpose of the operation of weapons at the highest level is divided into two partial tasks – the failure of enemy targets and maintaining the functioning of their own means. This follows from the basic law of armed fight. The indicator that describes the first task can be "fire performance" or "firepower" of the weapon. The indicator that describes the second task – "survivability". The other properties of the weapon are the means to achieve the main properties.

It is the indicator "combat potential of the sample of weapons", which combines the indicators of "firepower" and "survivability" should be used in conceptual research on the formation of basic requirements for UAVs on a complex criterion of "combat potential – cost".

The model of combat operations of reusable UAVs can be thought of as a series of repetitive combat sorties in each of which it hits a number of targets. Each subsequent flight can be performed provided that the previous ones were performed.

Suppose that in the process of performing a combat sortie UAV is exposed to fire from the enemy with an intensity of λ, which leads to its defeat in one sortie with probability P_{UAV1} [18]. Assuming the Poisson nature of fire effects, this probability is determined by:

$$P_{UAV1} = 1 - e^{-\lambda P_1 t_{cf}} \quad (1)$$

where P_1 – conditional probability of the sample damage under one exposure;

t_{cf} – duration of the combat flight

The number of combat sorties that a UAV can perform before its defeat is a random variable. When performing n combat sorties UAV will be struck with a probability of W_n:

$$W_n = 1 - (1 - P_{UAV1})^n \quad (2)$$

Mathematical expectation (the average number) of combat sorties is determined by the ratio of this probability to the probability of defeat in one combat sortie:

$$\bar{n} = \frac{1 - (1 - P_{UAV1})^n}{P_{UAV1}} \quad (3)$$

For multiple UAVs n>>1 i $\bar{n}$ and is reduced to the inverse probability P_{UAV}:

$$\bar{n} = \frac{1}{P_{UAV1}} \quad (4)$$

The mathematical expectation (average value) of the number of single targets hit in one UAV combat flight is determined by the number of successful target attacks during the combat flight. It is limited by the number of means of destruction in combat charge. It is assumed that the ammunition of the aircraft consists of the same type of means of destruction, and launches on one target is carried out by only one means of destruction. This simplification is not fundamental and allows you to reduce the recording of basic expressions in the article. Expression for mathematical expectation (average value) of the relative number of single targets hit in one UAV combat flight:

$$\frac{M\left[N^k_{PT_{ij}}\right]}{N^k_{T_{ij}}} = P_{PT_{ij}} \cdot P_{T_{ij_1}} \cdot m^k_i \quad (5)$$

where $N^k_{PT_{ij}}$ – the number of single potential targets of the j-type, hit in the k-combat flight of the UAV by means of the i-type;

$M\left[N^k_{PT_{ij}}\right]$ – mathematical expectation of the number of single targets of the j-type, struck in the k-combat flight of the UAV by means of the i-type;

$P_{PT_{ij}}$ – the probability of fulfilling the conditions preceding the launch (reset, etc.) of the means of defeat of the i-type on the target of the j-type: detection and recognition of the target by external means, long-range guidance, target detection by own means of UAVs, target attack. Depending on the problem to be solved and the method of using the UAV, the composition of the stages of preparation for the launch of the means of destruction may differ from the above. For example, in

the case of an autonomous method of UAV application, the stages of external targeting may be absent, and target detection and recognition may be carried out by its own means;

$P_{T_{ij1}}$ – the probability of defeat by one means of defeat of the i-type of the j-type target;

m_i^k – the number of means of defeat of the i-type AV used in the k-combat flight;

The maximum value of the mathematical expectation (average value) of the relative number of single targets hit in one combat flight of UAVs is determined by the expression:

$$max \frac{M\left[N_{PT_{ij}}^k\right]}{N_{T_{ij}}^k} = P_{PT_{ij}} \cdot P_{T_{ij1}} \cdot m_{MD_i}^k \qquad (6)$$

where $m_{MD_i}^k$ – the total number of means of defeat of the i-type aircraft, used in the k-combat flight.

For the entire period of the UAV's life, ie during $\bar{n}$ combat sorties, the mathematical expectation of the number of single targets hit by the UAV:

$$M\left[N_{T_{ij}}\right] = \sum_{k=1}^{\bar{n}} M\left[N_{T_{ij}}^k\right] \qquad (7)$$

The maximum value of the mathematical expectation of the number of single targets hit during the entire life of the UAV, ie during $\bar{n}$ combat sorties by definition is the UAV CP as to destruction by i-type means of the j-type targets:

$$CP_{UAV_{ij}} = max \sum_{k=1}^{\bar{n}} M\left[N_{PT_{ij}}^k\right] = N_{T_{ij}} \cdot P_{PT_{ij}} \cdot P_{T_{ij1}} \cdot \bar{m}_{MD_i} \cdot \bar{n} \qquad (8)$$

or

$$CP_{UAV_{ij}} = max \sum_{k=1}^{\bar{n}} M\left[N_{PT_{ij}}^k\right] = \bar{N}_{T_{ij}} \cdot P_{PT_{ij}} \cdot P_{T_{ij1}} \cdot \frac{P_{T1_{ij}}}{P_{UAV1}} \bar{m}_{MD_i} \qquad (9)$$

where $\bar{m}_{MD_i}$ – the average value of the number of means of aircraft destruction (combat kits) of i-type on departures;

$\bar{N}_{T_{ij}}$ – the average number of single potential targets of the j-type, affected by means of the i-type on departures.

If the CP of UAV is already known, which can be taken as a reference, it is more convenient to use the CP coefficient instead of the CP. It is determined by the ratio of the CP of UAV to the reference CP of UAV. It is assumed that UAVs are used in similar conditions. In this case, expression (9) is simplified because the variables $N_{T_{ij}}$ are reduced:

$$K_{CP\,UAV_{ij}} = \frac{P_{PT_{ij}}}{P_{PT_{ij}}^{REF}} \cdot \frac{P_{T1_{ij}}}{P_{T1_{ij}}^{REF}} \cdot \frac{P_{UAV1}}{P_{UAV1}^{REF}} \cdot \frac{\bar{m}_{MD_i}}{P_{MD_i}^{REF}} \qquad (10)$$

The CP coefficient has a clear physical meaning. It is reduced to the product of the ratios of the indicators of effectiveness of the destruction means, the number of means in the ammunition and the inverse ratio of survivability.

Model (10) can be applied during researches at the initial stages of UAV creation (external design) when searching for a design compromise between the combat potential and the cost of UAVs.

To optimize (select) the options of technical and design solutions of UAVs, it is necessary to use the dependences of the generalized indicators $< P_{PT_{ij}}, P_{T1_{ij}}, P_{UAV1}, \bar{m}_{MD_i} >$ of the TTC of UAVs. Such dependences should be considered as components of mathematical models of CP.

$K_{CP\,UAV_{ij}}$ in (10) is an element of the matrix, where the types of means by which the UAV will hit the enemy's targets are indicated in the lines, and the types of targets - in the columns.

The matrix (10) is similar to the matrix of efficiency of application of different models of weapons in different conditions. The use of the data contained in the matrix (10) depends on the objectives of research and the method of decision-making based on them.

For example, in comparing $K_{CP\,UAV_{ij}}$ of different UAVs, several different approaches can be used to select the best option.

The simplest approach is to collapse the matrix (10) into a scalar quantity. Then the average CP of UAV is determined:

$$\bar{K}_{CP\,UAV} = \frac{1}{M \cdot N} \cdot \sum_{i=1}^{N} \sum_{j=1}^{M} \alpha_i \cdot \beta_j \cdot K_{CP\,UAV_{ij}} \qquad (11)$$

where N – the number of types of UAVs destruction;

M – number of types of targets.

α_i – weight factor that determines the relative frequency (probability) of use of weapons

of the i-type, $\sum_{i=1}^{N} \alpha_i = 1$;

β_j – weighting factor that determines the relative part (probability) of the targets of the j-type that will be affected, $\sum_{j=1}^{M} \beta_j = 1$.

Weight multipliers α_i, β_j are determined by the typical composition of enemy targets and weapons of strike UAVs [10].

With a more detailed approach, it is possible to make comparisons when folding the matrix (10) into a vector or without folding. In this case, the problem is reduced to a comparison of a set of criteria [18]. When folded into a vector column, it is assumed that the weapon of the i-type is used for all targets:

$$\overline{K}_{CP\,UAV} = \frac{1}{M} \cdot \sum_{j=1}^{M} \beta_j \cdot K_{CP\,UAV_{ij}} \qquad (12)$$

When folded into a vector-line, it is assumed that the entire weapon is used only for targets of the j-type:

$$K_{CP_{UAV}} = \frac{1}{N} \cdot \sum_{i=1}^{N} \alpha_i \cdot K_{CP\,UAV_{ij}} \qquad (13)$$

Obviously, $K_{CP\,UAV_{ij}}$ reaches its maximum value when using ammunition to hit targets of the same type with maximum efficiency.

3. Conclusions

To select options for technical and design solutions of unmanned aerial vehicles, it is necessary to use the dependences of generalized indicators: the probability of fulfilling the conditions preceding the launch (reset) of a certain type of destruction means for the determined target, ie detection and recognition of targets by external means, long-range guidance, target detection by own means of a UAV, target attack; the probability of defeat by one means of defeat of a certain type of a certain type of a target; the probability of a UAV damage in one flight; the average value of the number of means of destruction of unmanned aerial vehicles (combat kits) of a certain type by departures from the tactical and technical characteristics of the unmanned aerial vehicle. Such dependences should be considered as components of mathematical models of CP.

The considered methodical approach to development of mathematical model of combat potential of strike UAVs allows to build mathematical models for conducting researches of military and economic efficiency of strike unmanned aerial vehicles without involvement of expert or other “fuzzy” information.

4. References

[1] Strelnikov D. Kontseptualnye vzglyady komandovaniya VVS SShA na razvitie bespilotnoy aviatsii, 2017. URL: http://pentagonus.ru/publ/konceptualnye_vzgljady_komandovanija_vvs_ssha_na_razvitie_bespilotnoj_aviacii_2017/16-1-0-2776.

[2] Unmanned Systems Integrated Roadmap FY2013-2038. URL:archive.defense.gov/pubs/dod-usrm-2013.pdf.

[3] United States Air Force Unmanned Aircraft Systems Flight Plan 2009-2047. URL: http://fas.org/irp/program/collect/uas_2009.pdf.

[4] The United States Air Force Remotely Piloted Aircraft Vector: Vision and Enabling Concepts: 2013-2038. URL: http://www.af.mil/Portals/1/documents/news/USAFRPAVectorVisionandEnablingConcepts2013-2038.pdf.

[5] Small Unmanned Aircraft Systems Flight Plan: 2016-2036. URL: http://apps.dtic.mil/dtic/tr/fulltext/u2/1013675.pdf.

[6] Strelnikov D. Sidorov A., Mgimov Yu. Sovmestnoe primenenie pilotiruemoy i bespilotnoy aviatsii SShA v pervoy polovine KhKhI, 2018. URL: http://pentagonus.ru/publ/sovmestnoe_primenenie_pilotiruemoj_i_bespilotnoj_aviacii_ssha_v_pervoj_polovine_xxi_veka_2018/16-1-0-2829

[7] Tsygichko V.I., Stoili F. Metod boevykh potentsialov: istoriya i nastoyashchee, 1997. URL:http://militaryarticle.ru/voennaya-mysl/1997-vm/9650-metod-boevyh-potencialov-istorija-i-nastojashhee8. Tomashev V.N. O sovershenstvovanii metodov otsenki boevykh vozmozhnostey voysk, 2006. URL:http://militaryarticle.ru/nauka-i-voennaya-bezopasnost/2006/11946-o-sovershenstvovanii-metodov-ocenki-boevyh.

[9] Leontєv O.B., Kompanієts O.M., Shmakov V.V. Metodika otsinki boyovogo potentsialu udarnikh aviatsiynikh kompleksiv pri

virishenni nimi vognevikh zadach. Zbirnik naukovikh prats KhNUPS, 2008. – vipusk 2(17). – S.23–27.

[10] Leontєv O.B., Grib D.A., Ukraïnets Є.O., Kompanієts O.M. Viznachennya vagovogo vnesku osnovnikh grup vlastivostey udarnogo aviatsiynogo kompleksu v uzagalneniy pokaznik boyovoï efektivnosti shlyakhom ekspertnogo otsinyuvannya. Zbirnik naukovikh prats KhNUPS. – Kharkiv, 2009. – vipusk 3(21). – S.5–9.

[11] Mukhin R.R. Dinamicheskiy khaos: trudnyy put otkrytiya, 2014. URL: https://cyberleninka.ru/article/n/dinamicheskiy-haos-trudnyy-put-otkrytiya/viewer.

[12] Konovalov Yu.V. Statisticheskoe modelirovanie s ispolzovaniem regressionnogo analiza, 2013. URL: http://cmmp.bmstu.ru/docs/Konovalov.pdf.

[13] Lazebnik C. V., Malyuga V. G., Nerubatskiy V.O. Pidkhid do formuvannya sistemi pokaznikiv efektivnosti ugrupovan viysk, 2012. URL: http://nbuv.gov.ua/UJRN/ZKhUPS_2012_4_4

[14] Protasov A.A. Morozov N.A., Strelkov S.N. Nechetko mnozhestvennyy podkhod k otsenke boevykh potentsialov, sootnosheniya sil i boevykh vozmozhnostey gruppirovok voysk (sil) v operatsiyakh Voennaya Mysl. – Moskva, 2008. – № 9. – S. 48–54.

[15] Bonin A.C., Gorchitsa G.I. O boevykh potentsialakh obraztsov VVT, formirovaniy i sootnosheniyakh sil gruppirovok storon, 2010. URL: http://militaryarticle.ru/voennaya-mysl/2010-vm/10318-o-boevyh-potencialah-obrazcov-vvt-formirovanij-i.

[16] Buravlev A.I. Osnovy metodologicheskogo podkhoda k otsenke boevykh potentsialov obraztsov VVT i voinskikh formirovaniy, 2009. URL: http://www.viek.ru/7/4-12.pdf.

[17] Bobrikov A.A. Otsenka effektivnosty ognevogo porazheniya udarami raket i ognem artillerii. Galeya Print. – Sankt Peterburg, 2006. – s. 421.

[18] Klyushnikov I. M., Nerubatskiy V.O., Shaligin A.A. Pidkhid do formuvannya kriterialnogo aparatu otsinki efektivnosti zmishanikh ugrupovan pilotovanoï ta bezpilotnoï aviatsiï, URL:http://nbuv.gov.ua/UJRN/Nitps_2019_4_

Розробка і тестування програмного забезпечення інформаційно-вимірювальної системи на базі віртуальних комп'ютерних тренажерів як концепція підвищення ефективності навчального процесу

Юрій Скорін[1], Олександр Щербаков[2], Ірина Ушакова[3]

[1,2,3] *Харківський національний економічний університет ім. С. Кузнеця, пр. Науки, 9-А, Харків, 61166, Україна*

Анотація

У статті в якості концепції вдосконалення навчального процесу, підвищення ефективності використання перспективних форм професійного навчання визначено впровадження в навчальний процес імітаційних віртуальних тренажерів, побудованих на базі віртуальних вимірювальних приладів і віртуалізації вимірювальних процесів. Дослідження базується на проведеному аналізі традиційних, методів і засобів вимірювань і пропозиції в якості альтернативного вирішення проблеми, віртуалізації вимірювального процесу. Проводиться оцінка переваг та області застосування віртуальних приладів. Відзначається, що крім застосування власне за призначенням, тобто в якості віртуальних засобів вимірювальної техніки, досить перспективним є використання віртуальних приладів для побудови на їх основі віртуальних тренажерів, які забезпечують підвищення наочності і якості навчання, в першу чергу, на так званих, приладових навчальних дисциплінах, що, в свою чергу, створює передумови для включення їх в уже існуючі або створення на їх основі нових систем дистанційного навчання. Дослідження передбачає: проведення аналізу, осмислення й узагальнення досвіду використання сучасних методів і засобів вимірювань, визначення переваг та недоліків традиційних підходів до вимірювального процесу; обґрунтування вибору віртуалізації вимірювального процесу, як найбільш ефективного засобу вдосконалення приладового парку; проведення аналізу структури і підходів до побудови віртуальних приладів, оцінку області їх застосування; виділення віртуальних приладів в якості базових для побудови на їх основі віртуальних тренажерів, які забезпечують підвищення ефективності і наочності навчального процесу та створюють передумови для створення і вдосконалення систем дистанційного навчання.

Ключові слова

віртуалізація, прилад, ефективність, тренажер, метод, засіб, парк, система, навчання, дослідження, концепція, удосконалення, аналіз, вибір, наочність.

Development and testing of software for an information-measuring system based on virtual computer simulators as a concept for increasing the efficiency of the educational process

Yuri Skorin[1], Alexander Shcherbakov[2], Irina Ushakova[3]

[1,2,3] *Kharkiv National Economic University named after S. Kuznets, Nauki Ave., 9-A, Kharkiv, 61166, Ukraine*

Abstract

In the article, as a concept for improving the educational process, increasing the efficiency of using promising forms of vocational training, the introduction into the educational process of

EMAIL: skorin.yuriy@gmail.com (A. 1); oleksandr.shcherbakov.kafis@gmail.com (A. 2); vara-vina.ira@gmail.com (A. 3)
ORCID: 0000-0002-4613-3154 (A. 1); 0000-0001-8315-0917 (A. 2); 0000-0001-8315-0917 (A. 3)

imitation virtual simulators, built on the basis of virtual measuring instruments and virtualization of measuring processes, is defined. The study is based on the analysis of traditional methods and measuring instruments and a proposal as an alternative solution to the problem, virtualization of the measuring process. An assessment of the advantages and scope of virtual instruments is being carried out. It is noted that in addition to the actual use for its intended purpose, i.e. as virtual measuring instruments, it is quite promising to use virtual instruments for building virtual simulators on their basis, which provide an increase in the visibility and quality of training, primarily in the so-called instrumental educational disciplines, which, in turn, creates the preconditions for their inclusion into existing ones or creation on their basis of new distance learning systems. The study assumes: analysis, comprehension and generalization of the experience of using modern methods and measuring instruments, identification of the advantages and disadvantages of traditional approaches to the measurement process; substantiation of the choice of virtualization of the measuring process as the most effective means of improving the instrument park; analysis of the structure and approach-es to the construction of virtual devices, assessment of the scope of their application; allocation of virtual devices as basic ones for building virtual simulators on their basis, providing an increase in the efficiency and visibility of the educational process and creating prerequisites for the creation and improvement of distance learning systems.

Keywords
virtualization, device, efficiency, simulator, method, means, park, system, training, research, concept, improvement, analysis, choice, visibility.

1. Вступ

Проведений аналіз сучасного стану вимірювальної техніки, а також тенденцій її подальшого розвитку, свідчить про те, що поряд з розробленням і вдосконаленням традиційних засобів вимірювань все більшого значення набуває відносно новий напрямок, а саме розроблення віртуальних вимірювальних приладів.

Цьому сприяє [1]: по-перше, суттєвий прогрес у розвитку засобів саме електронно-обчислювальної техніки, в результаті якого персональні комп'ютери стали звичним і навіть необхідним інструментом інженерів, вчених, викладачів; по-друге, парк вимірювальних приладів дуже часто поповнюється і відновлюється не такими швидкими темпами, як того вимагають сучасні реалії; по-третє, порушення різноманітних інтеграційних зв'язків значно ускладнює процес розроблення, також виробництва сучасних вимірювальних приладів.

Все це викликає необхідність пошуку альтернативних способів вдосконалення парку вимірювальної техніки, наприклад, шляхом розроблення і створення віртуальних вимірювальних приладів. Таким чином, поступальний розвиток обчислювальної техніки, а також комп'ютеризація усіх галузей народного господарства, наводить на думку про використання такого досить потужного технологічного потенціалу, як комп'ютеризація в справі вдосконалення процесу вимірювань у вимірювальних системах. Пошуки такого рішення привели до необхідності створення віртуальних вимірювальних приладів, аналоги яких уже існують і демонструють величезні переваги перед, так званими, традиційними приладами, що дає стимул і можливість до створення на базі віртуалізації процесу вимірювань зразків віртуальних комп'ютерних тренажерів, покликаних забезпечити підвищення наочності і ефективності навчального процесу і створити передумови для значного розширення функціональних можливостей систем дистанційного навчання.

Актуальність розглянутого напрямку полягає в тому, що [3]: по-перше, склад штатних вимірювальних приладів, який є в наявності і потрібен для забезпечення якісного проведення навчального процесу, як правило, є обмеженим, часто вимагає ремонту, відновлення або заміни, тому значення віртуальних комп'ютерних тренажерів в таких випадках важко переоцінити; по-друге, за допомогою віртуальних комп'ютерних тренажерів можна забезпечити набуття практичних навичок роботи з найбільш сучасними вимірювальними приладами, які в зв'язку з обмеженням технічних або економічних можливостей в даний час

ще не використовуються в навчальному процесі; по-третє, віртуальні комп'ютерні тренажери можуть використовуватися студентами під час самостійної підготовки до занять, тому що вони досить прості в експлуатації, не вимагають спеціальних знань в області програмування, не є критичними до апаратному складу і програмного забезпечення персонального комп'ютера, містять підказки та коментарі, які практично керують діями оператора, відпрацьовують його помилки; по-четверте, віртуальні комп'ютерні тренажери, на наш погляд, доцільно створювати, в першу чергу для найбільш сучасних приладів, які ще відсутні в складі лабораторно-технічної бази закладу, також на попередньому етапі підготовки до робіт на штатній техніці, під час самостійної підготовки до занять, при заочній формі навчання тощо, тобто в тих випадках, коли доступ до штатних засобів вимірювальної техніки є обмеженим або недоцільним; по-п'яте, віртуальному комп'ютерному тренажеру можна надати додаткові функції, які не притаманні реальному приладу, наприклад, відображати фізичні процеси, які відбуваються "всередині" приладу під час проведення вимірювального експерименту, а також надавати довідкову інформацію, здійснювати обробку та зберігання результатів вимірювань і діагностики, проводити тестування і контроль рівня знань студентів тощо; по-шосте, віртуальні комп'ютерні тренажери, що розглядаються в статті, мають зовнішній вигляд, який повністю відповідає вигляду реальних приладів, для цього були створені нестандартні ActiveX елементи, що теж є важливим з точки зору ефективності процесу навчання.

Таким чином, можна сформулювати цілі проведених досліджень, а саме, обґрунтування альтернативних способів вдосконалення парку засобів вимірювальної техніки шляхом розробки віртуальних вимірювальних приладів і підвищення ефективності навчального процесу шляхом розробки та впровадження віртуальних комп'ютерних тренажерів на базі розроблених віртуальних приладів.

2. Матеріали і методи

Проведення практично будь-якого наукового дослідження є глибоко індивідуальний, творчий процес, успіх якого часто залежить від раціонального поєднання якісних оцінок з використанням, наприклад, аналітичних методів, з кількісними оцінками, які спираються на конкретні факти і досвід попередніх досліджень. Часто, при проведенні більшості досліджень, зокрема досліджень, пов'язаних з розробкою концепції підвищення ефективності навчального процесу шляхом впровадження віртуалізації і комп'ютерних тренажерів, побудованих на базі віртуальних вимірювальних приладів, в повній мірі можуть використовуватися конкретно-наукові методи, що представляють собою сукупність теоретичних і емпіричних методів. Емпіричні методи, задіяні під час проведення досліджень, забезпечили можливість збору, систематизації і організації емпіричного матеріалу, що представляє собою повну гаму фактів, результатів експериментів і спостережень в області, як дослідження концепції підвищення ефективності навчального процесу взагалі, так і з використанням віртуальних тренажерів на базі віртуальних приладів з широким використанням інформаційних технологій. Логічні, теоретичні методи, засновані на реалізації узагальнення всієї маси даних, отриманих емпіричним шляхом, дозволили оцінити проблему, яка полягає в необхідності вдосконалення навчального процесу, методів і засобів, в рамках даної проблеми, провести аналіз публікацій, сформувати гіпотезу і провести оцінку зібраних емпіричним шляхом фактів, запропонувавши, як напрямки вирішення поставленого завдання, вибір віртуалізації і комп'ютерних тренажерів, як найбільш ефективного засобу підвищення ефективності навчального процесу.

Новизна проведених досліджень полягає в тому, що було проведено комплексне дослідження теоретичних і практичних аспектів підвищення ефективності навчального процесу, в результаті якого на основі порівняльно-порівняльного методу був проведений аналіз ефективності використання традиційних приладів і підходів на базі використання останніх досягнень інформаційних технологій у вигляді віртуалізації вимірювального процесу та внесені конкретні пропозиції щодо комплексного використання традиційних і віртуальних приладів, розглянуто комбінований метод використання віртуальних тренажерів в навчальному процесі, розробити конструкцію та оригінальні ActiveX елементи, що роблять зовнішній вигляд віртуальних тренажерів повністю відповідним зовнішнім виглядам традиційних приладів, що повністю збігається з поглядом

на критерії новизни наукових досліджень, наведених в таких публікаціях, як [8; 9]. Так в публікації [8] під новизною дослідження розуміється "наскільки є сучасними і оригінальними використовувані в дослідженні уявлення і методи", крім того, в публікації [9] автору видається цілком правомірним введення цих критеріїв в оцінювання наукової новизни поряд з фіксацією фактів приросту знань [9].

3. Літературний огляд

Підвищенню ефективності навчального процесу в цілому і проектування систем, що забезпечують досить ефективну професійну підготовку фахівців, а також навчальних середовищ з використанням комп'ютерних тренажерів, завжди приділялося багато уваги, про що свідчить значна кількість публікацій щодо питань вдосконалення навчального процесу [1–5]. Так, різні аспекти та шляхи підвищення ефективності використання перспективних форм інтерфейсів і тренажерів розглядалися в роботах цілого ряду авторів, таких як [11–15]. Питаннями, пов'язаними з ергономічним проектуванням перспективних форм інтерфейсів і комп'ютерних тренажерів, приділяли увагу автори таких робіт, як [10–12]. Практикою побудови тренажерів для широкого кола об'єктів в різний час займалися такі автори, як [6–11]. Дослідженнями феноменів, пов'язаних з віртуальною реальністю і інтерактивністю, займалися [9; 12].

4. Вирішення проблеми

Віртуальні прилади є концепцією, яка створює передумови для організації програмно-керованих систем збору даних і управління широкою номенклатурою різних технічних об'єктів і технологічних процесів, причому система реалізується за допомогою створення програмної моделі якогось гіпотетичного або реально існуючого вимірювального засобу, або іншого об'єкта, при цьому і засоби управління (кнопки, тумблери, рукоятки, перемикачі, лампочки і т. п.), і сама логіка роботи приладу реалізуються програмним шляхом. Зв'язок же програми з зазначеними технічними об'єктами здійснюється через інтерфейсні вузли, які представляють собою драйвери зовнішніх пристроїв, а саме, контролерів промислових інтерфейсів, цифро-аналогових перетворювачів (ЦАП), аналого-цифрових перетворювачів (АЦП) і т. п. [5].

При традиційному проведенні вимірювального експерименту прийнято визначати значення тієї чи іншої фізичної величини за допомогою спеціалізованого вимірювального приладу, що представляє собою конструктивно закінчену систему певного функціонального призначення з заздалегідь фіксованими можливостями з'єднання з іншими пристроями. Відмінною перевагою віртуальних приладів, є, перш за все, універсальність таких приладів і, що не менш важливо, практично необмежений потенціал щодо розширення функціональних можливостей приладів, причому без зміни апаратного складу приладів, а тільки за рахунок вдосконалення програмного забезпечення [1; 3].

Аналіз показує, що багато компаній в своїх приладах фактично реалізують перевернуту концепцію віртуальних інструмент, коли вимірювальний прилад з'єднується з комп'ютером не за допомогою інтерфейсу, а шляхом вбудовування ПК в корпус приладу. Успіхи мікроелектроніки в створенні елементної бази з субмікронними розмірами елементів дозволяють розмістити в одному корпусі і вимірювальний прилад, і комп'ютер. Це дозволяє розширити універсальність застосування вимірювальної апаратури нового покоління, але подібна практика відповідним чином відбивається на ціні і ускладненні процесу управління подібними приладами. У той же час не дуже матеріально забезпечені навчальні заклади цілком можуть вирішувати проблеми оснащення своїх лабораторій за допомогою високопродуктивних та одночасно відносно дешевих плат збору даних, вбудованих в комп'ютер [2].

Більш перспективним, на наш погляд, є підхід, в основу якого покладено принцип об'єднання комп'ютера з блоком управління, основу якого складає плата збору і перетворення даних.

Таким чином, в загальному випадку віртуальний прилад складається з двох наступних основних компонентів, а саме, пристрої управління та обробки інформації, тобто персонального комп'ютера, і плати збору і перетворення даних. Перший компонент, а саме персональний комп'ютер, не вимагає витрат на його виготовлення або придбання, тому що є необхідним атрибутом сучасності, і, вже зараз є обов'язковим інструментом на робочому мі-

сці інженера-метролога. Тому будемо розглядати його, як уже існуючий, компонент віртуального вимірювального приладу. Другий компонент, а саме, блок управління, містить аналогово-цифровий перетворювач (АЦП), цифро-аналоговий перетворювач (ЦАП), для вироблення керуючих аналогових сигналів, перетворювач код-код (ПКК) і плату збору і перетворення даних, яка в загальному випадку містить мультиплексор мікроконтролер, порт RS-485, пристрій, перетворювач напруги і фільтр.

Плата збору і перетворення даних є раціональною альтернативою набору складних пристроїв і комплектуючих реального приладу.

Виробництво плати збору і перетворення даних в кілька разів дешевше, ніж приладу в цілому, що підтверджено проведеним аналізом орієнтовних цін. Обслуговування складних великогабаритних пристроїв, приладів і систем вимагає значних витрат часу, коштів і обслуговуючого персоналу з високою кваліфікацією. Плата збору і перетворення даних, в свою чергу, відрізняється простотою у використанні і обслуговуванні, а також завдяки наявності в програмному забезпеченні системи підказок, робота з віртуальним приладом не вимагає від оператора спеціальних знань в області програмування. Таким чином, можна констатувати, що сучасний віртуальний вимірювальний прилад є технічно об'єднаної сукупністю персонального комп'ютера, в найпростішому випадку, з вбудованою спеціальною платою збору і перетворення даних, або з додатковим блоком, який підключений до персонального комп'ютера за допомогою з'єднувального кабелю, якщо проводяться більш складні і багатофункціональні вимірювання. Плата збору і перетворення даних здійснює ряд функцій, а саме, функцію введення інформації в комп'ютер, комутацію, дискретизацію, квантування і кодування сигналів, які надходять від контрольованих об'єктів. Функцію ж моделювання вимірювальної системи і обробки вхідних сигналів, які є фактично результатами вимірювання цих сигналів, за допомогою заданих алгоритмах, а також функцію відображення результатів обробки вхідних сигналів на екрані монітора, визначає комп'ютер, керований спеціально розробленим програмним забезпеченням.

Відмінною особливістю віртуальних приладів є також і те, що всі органи управління, а також структурні особливості модельованої вимірювально-інформаційної системи відображається на моніторі комп'ютера, а сам процес управління здійснюється в наочній і зручній для користувача формі, за допомогою стандартного маніпулятора або клавіатури. При використанні подібної плати збору і перетворення даних, а також відповідного програмного забезпечення, розробник як би проектує даний конкретний засіб вимірювань, оптимізуючи його для проведення того чи іншого вимірювального експерименту або конкретного метрологічного завдання [3].

Так на базі плати збору і перетворення даних ADC 16-32 був розроблений діючий макет віртуального вимірювального приладу, а саме - віртуального вольтметра постійного струму, і пакет програмного забезпечення для його реалізації. Експериментальні дослідження приладу показали, що при реалізації усереднення результатів вимірювань з метрологічними характеристиками віртуальний вольтметр є аналогом поширеного штатного цифрового вольтметра В7-16А. Крім того, на базі разработанніх віртуальніх приладів був розроблений віртуальний вимірювальний комплекс у вигляді пакету програмного забезпечення під загальною назвою "Віртуальна вимірювальна лабораторія" до складу якої увійшли кілька комп'ютерних тренажерів, таких як "Віртуальний цифровий вольтметр", "Віртуальний цифровий частотомір", а також тренажери аналогових приладів, таких як "Віртуальний електронний осцилограф", "Віртуальний комбінований прилад", "Віртуальний електронний вольтметр".

Перераховані комп'ютерні тренажери можуть використовуватися в навчальному процесі як окремо, так і в складі загального циклу-практикуму. Методика проведення вимірювального експерименту за допомогою того чи іншого віртуального приладу-тренажеру практично не відрізняється від існуючих методик, притаманних відповідним традиційним вимірювальним приладам, тому і не розглядається в рамках даної статті.

Розроблений програмний продукт за принципом побудови є модульною структурою і містить блок управління або програмну оболонку, загальну для всіх віртуальних тренажерів, що входять до складу віртуальної вимірювальної лабораторії і дозволяє користувачеві ознайомитися зі структурою віртуального практикуму, здійснити прямий доступ до основних розділів

довідкової інформації, здійснювати запуск інтерактивних модулів лабораторних робіт, а також зберігати результати роботи, роздруковувати звіт про результати проведених дослідженнях і т. д.

5. Результати

Важливою особливістю розробленого програмного продукту є те, що його робота може бути реалізована в режимі підказки, коли програма фактично керує діями оператора, надає коментарі та підказки, а також блокується при здійсненні оператором дій, здатних викликати критичну помилку. Практично необмеженої представляється можливість розширення функціональних можливостей комп'ютерного тренажера, в першу чергу, не властивих традиційному приладу. Тому в залежності від призначення кожного конкретного віртуального тренажера деякі модулі програмного продукту містять інтерактивні електронні таблиці, тимчасові діаграми, графіки, що відображають фізичні про-процеси, які відбуваються в приладі під час проведення вимірювального експерименту, чим сприяють підвищенню ефективності навчального процесу.

Що стосується сфери застосування віртуальних комп'ютерних тренажерів, то на наш погляд, в першу чергу їх доцільно створювати для моделювання найбільш сучасних приладів, ще відсутніх в складі лабораторно-технічної бази закладу або придбання яких є скрутним з точки зору їх вартості, а також на попередньому етапі підготовки до проведення робіт на штатній техніці або під час самостійної підготовки до занять, при заочній формі навчання тощо, тобто в тих випадках, коли доступ до штатних засобів вимірювальної техніки обмежений або недоцільний.

Розроблений пакет програмного забезпечення є закінченим і самодостатнім програмним продуктом, до складу якого входить інсталяційний модуль, адаптований під більшість платформ програмного забезпечення. Представлений програмний продукт повністю адаптований до використання в мережі інтернет або локальних комп'ютерних мережах. Ще одна важлива особливість програмного продукту полягає в тому, що він є базовим для побудови віртуальних вимірювальних приладів і комп'ютерних тренажерів інших видів і типів.

Але слід зазначити, що впровадження комп'ютерних тренажерів в процес навчання жодним чином не передбачає якусь підміну штатних традиційних приладів їх комп'ютерними моделями, а навпаки тільки доповнює і розширює можливості як викладачів, так і студентів. Питання, яке пов'язане з виробленням концепції, методики спільного використання в навчальному процесі, як штатних традиційних приладів, так і їх комп'ютерних моделей-тренажерів ще вимагає серйозного осмислення і на жаль не є метою даної публікації.

У плані подальшого розвитку пакета програмного забезпечення слід зазначити, що можливості поповнення парку віртуальних приладів є практично необмеженими, тому цікаво було б здійснити побудова, наприклад, віртуальних аналогових приладів, аналізаторів спектру і т. д. Також є практично необмеженою сфера використання розроблених віртуальних приладів, на їх основі можна будувати вимірювальні системи для досліджень не тільки автономних засобів вимірювань, а й вимірювально-інформаційних систем, параметри і зовнішній вигляд яких можна коригувати як на стадії розробки, так і в процесі роботи.

6. Висновки

У статті, по-перше, був проведений аналіз традиційних підходів до вимірювального процесу, проведено обґрунтування вибору віртуалізації вимірювального процесу, як найбільш ефективного засобу вдосконалення приладового парку, по-друге, на базі плати збору і перетворення даних ADC 16-32 було розглянуто діючий макет віртуального вимірювального приладу, а саме, віртуального вольтметра постійного струму, і пакет програмного забезпечення для його реалізації, по-третє, було зроблено виділення віртуальних приладів в якості базових для побудови на їх основі віртуальних тренажерів, які забезпечують підвищення ефективності і наочності навчального процесу та створюють передумови для створення і вдосконалення систем дистанційного навчання; по-третє, вирішена досить важлива прикладна задача, тобто представлені віртуальні комп'ютерні тренажери мають зовнішній вигляд, повністю відповідний вигляд реальних приладів, для цього були створені нестандартні ActiveX елементи, на відміну від інших тренажерів, де зовнішній вигляд приладів і органів

управління не відповідає зовнішньому вигляду реальних штатних приладів, що важливо з точки зору наочності і ефективності процесу навчання.

7. Література References

[1] Скорін Ю. І. Віртуальні прилади у вимірювальній лабораторії / Ю. І. Скорін, В. В. Стаднік, А. М. Клименко // Вісник Національного технічного університету "ХПІ". Збірник наукових праць. Серія: Інформатика та моделювання. – Харків: НТУ "ХПІ". – № 38. – 2012. – С. 84–92.

[2] Скорин Ю. И. Создание виртуальных измерительных приборов средствами технологии Windows Presentation Foundation / Ю. И. Скорин, В. В. Стадник // Материалы 10-й Международной научно-технической конференции "Приборостроение-2017", 1–3 ноября 2017 г., – Минск: БИТУ, 2017. – с. 185–187.

[3] Скорін Ю. І. Віртуальні вимірювальні та діагностичні прилади / Ю. І. Скорін, О. В. Щербаков, Т. І. Магдалиць // Системи обробки інформації. Збірник наукових праць. Вип.4(102), том 1. Інформаційні технології та захист інформації. Х.: ХУПС.- 2012. – С. 65–68.

[4] Скорін Ю. І. Робоча програма навчальної дисципліни «Метрологія і стандартизація» для студентів напряму підготовки «Комп'ютерні науки» всіх форм навчання / Ю. І. Скорін, В.В. Федько, О. В. Щербаков . – Навчальне видання. Харків: Вид. ХНЕУ, 2012. – 48 с.

[5] Скорін Ю. І. Якість програмного забезпечення та тестування : робоча програма для студентів спеціальності 121 "Інженерія програмного забезпечення" першого (бакалаврського) рівня / Ю. І. Скорін. – Харків : ХНЕУ ім. С. Кузнеця, 2019. – 11 с.

[6] Виртуальные измерительные приборы [Электронный ресурс]. – Режим доступа : https://strpo.ru/electricity/viii-virtual-measuring-instruments/.

[7] Принципы построения виртуальных тренажеров [Электронный ресурс]. – Режим доступа : https://www.sunspire.ru/articles/part35/.

[8] Бермус А. Г. Общие основы педагогики: учеб пособие / А. Г. Бермус. – Ростов-на-Дону : Изд-во Ростов, гос. пед. ун-та, 1999. – 114 с.

[9] Солнышков М. Е. Критерии новизны научно-педагогических исследований / М. Е. Солнышков [Электронный ресурс]. – Режим доступа : https://cyberleninka.ru/article/v/kriteriy-novizny-nauchno-pedagogicheskih-issledovaniy.

[10] Белов В. В. Компьютерная реализация решения научно-технических и образовательных задач: учебное пособие / В. В. Белов, И. В. Образцов, В. К. Иванов и др. // Тверь : ТвГТУ, 2015. – 108 с.

[11] Рахманов Ф. Г. Применение имитационных виртуальных тренажеров в процессе профессионального обучения / Ф. Г. Рахманов // Молодой ученый. – 2015. – №9. – С. 1173-1175 [Электронный ресурс]. – Режим доступа : https://moluch.ru/archive/89/17867/.

[12] Дмитриев В. М. СВИП – система виртуальных инструментов и приборов / В. М. Дмитриев, Т. В. Ганджа, В. В. Ганджа и др. – Томск: В-Спектр, 2014. – 216 с.

[13] Зеленко Л. С. Интерактивная интеллектуальная обучающая система, построенная на основе технологии виртуальных миров, как средство активизации учебно-познавательной деятельности учащихся / Л. С. Зеленко, Л. В. Топунов, Д. Д. Загуменнов // Телематика 2010. СПб., 2010. – С. 335–336.

[14] Сергеев С. Ф. Виртуальные тренажеры: проблемы теории и методологии проектирования / С. Ф. Сергеев [Электронный ресурс]. – Режим доступа : https://elibrary.ru/item.asp?id=22513675.

[15] Баринов К. А., Концепция разработки программного обеспечения виртуальных лабораторных / К. А. Баринов, А. Б. Николаев, А. В. Остроух // Международный журнал прикладных и фундаментальных исследований. – 2014. – № 3-2. – С. 68–70.

Special Features Of The Designation Of The Necessary Number Of Inputs (Information Channels) In The Interests Of Realizing The Strategic Narrative Of The State On The Basis Of An Analytical Model Of The Development Of Information

Oleksandr Voitko [1], Volodymyr Cherneha [1], Vladislav Solonnikov [1], Olena Poliakova [1], Roman Korolyov [2]

[1] *National Defense University of Ukraine named after Ivan Cherniakhovskyi, Kyiv, Ukraine*
[2] *Simon Kuznets Kharkiv National University of Economics, Kharkiv, Ukraine*

Abstract

The article considers issues related to the study of processes that characterize the dissemination of information materials, as well as analysis of qualitative characteristics of information to assess the potential coverage of target audiences and the degree of perception of this information by the relevant audience.

The purpose of the article is to develop an analytical model for determining the required number of tools (information channels) to achieve certain goals in the implementation of the strategic narrative of the state, taking into account the requirements that affect the dissemination of information.

The application of the proposed mathematical tools to determine the required number of tools (information channels) in the interests of implementing the strategic narrative of the state on the basis of analytical model of information dissemination, will reasonably form the need and volume of information and psychological impact on target audiences. , and the quality of news channels. This will provide an opportunity to identify the main tasks for the system of strategic communications and to realize the interests of the state in the form of public support for the strategic course of the state to gain full membership of Ukraine in the EU.

Keywords

Target audience, narrative, dissemination of information, strategic communications

1. Introduction

Ukraine's integration into the Euro-Atlantic security space and the acquisition of NATO membership have been identified as the main goal of Ukraine's Military Security Strategy, which was enacted by the Decree of the President of Ukraine in March 2021. To achieve this goal, Ukraine will take a set of appropriate measures. One such measure is countering in cyberspace and imposing one's will in the information space [1].

To organize the implementation of such a task, it is necessary to have an effective and efficient system of strategic communications of the state, which uses a single information space, has reliable channels of communication with the population and an appropriate branched information infrastructure.

2. General Problem Statement

In previous publications, the authors solved the problem of scientific substantiation of accession to the EU, NATO on the basis of analysis of statistical data of public opinion and forecasting scenarios for its development [2, 3].

The obtained forecast data allowed to determine the peculiarities of the implementation

EMAIL: o.voytko@ukr.net (A. 1); chevn1980@gmail.com (A. 2); vladislavsolonnikov@ukr.net (A. 3); elena9669@gmail.com (A. 4); korolevrv01@ukr.net (A. 5);
ORCID: 0000-0002-4610-4476 (A. 1); 0000-0001-6190-3252 (A. 2); 0000-0002-7653-416X (A. 3); 0000-0003-4370-2187 (A. 4); 0000-0002-7948-5914 (A. 5);

of the strategic narrative of the state by the system of strategic communications and to realize the interests of the state in the form of public support for its strategic course to Ukraine's full membership in the EU and NATO. The proposed approach will allow to develop effective and efficient materials of information and psychological impact, which will be implemented by a system of strategic communications when influencing the relevant target audiences. An extremely important task will be to study the processes that characterize the distribution of information materials, as well as the analysis of qualitative characteristics of information to assess the potential coverage of target audiences and the degree of perception of this information by the relevant audience. This article is devoted to the statement of a possible variant of the decision of the resulted problems.

2.1. Analysis of recent research and publications

The armed aggression of the Russian Federation against Ukraine is carried out in various directions of the "hybrid war". Aggressive influences are carried out both simultaneously and consistently, practically on all spheres of life of the state, thus the received results in one sphere are at once used for strengthening of influence in other spheres. To date, a large number of domestic and foreign scientists are engaged in research on "hybrid actions". In the works of Landa D.V., Danyka Y.G., Salnikova O.F., Snitsarenko P.M. and many others, covers materials on the forms and methods used by the aggressor to achieve its imperial goals, and contains a number of theoretical provisions, recommendations on possible ways to counter. Unfortunately, scientific publications on the mathematical justification of the necessary forces and means, in achieving specific goals, are not enough.

A number of software services are available on the Internet, with which it is possible to simulate the process of information dissemination. The authors with the help of one of such services (Melting Asphalt) visualized a model of information dissemination among the target audience [4]. Indicators that influence the dissemination of information among target audiences are proposed, and a visualization of the information dissemination model is developed [5].

The purpose of the article is the development of an analytical model for determining the required number of tools (information channels) to achieve certain goals in the implementation of the strategic narrative of the state, taking into account the requirements that affect the process of dissemination of information.

2.1.1. Research results

Today, along with Ukraine, there are several states and their associations, more powerful than Ukraine, which have interests different from the national interests of Ukraine, and Ukraine is not able to resist their aggressive actions alone. Therefore, joining NATO is one of the government's priorities in order to protect national interests.

Public opinion gained very drastic changes in the direction of European and North Atlantic cooperation with the beginning of the armed aggression of the Russian Federation. Unfortunately, during the war, Ukrainian society did not get the desired result in terms of proper support and national security of Ukraine from the EU and NATO. Starting in 2017, the number of supporters of such integration began to gradually decrease.

Public opinion on EU accession has changed somewhat depending on the political, military and economic processes that have taken place in Ukraine over the past two decades. To achieve the stated goal of the study, it is not enough for us to assess only the current distribution of public opinion on this issue. It is necessary to identify the general trends of its change in the future, to choose those that are directed in the desired direction for us and are characterized by the greatest reliability. This was achieved using scientific forecasting, namely the method of statistical extrapolation. The analysis of the obtained results shows that in order to ensure further positive forecast development of public opinion of the population of Ukraine on EU accession it is necessary in 2022 and 2023 to increase the number of supporters of society in this direction by 2.4 million people, respectively. (6.3%) in 2022 and 0.7 million people. (2.1%) in 2023 [2].

The obtained forecast data provided an opportunity to determine the peculiarities of the implementation of the strategic narrative of the state by the system of strategic communications and to realize the interests of the state in the form

of public support for its strategic course to Ukraine's full membership in the EU and NATO. An extremely important task will be to study the processes that characterize the distribution of information materials, as well as the analysis of qualitative characteristics of information to assess the potential coverage of target audiences and the degree of perception of this information by the relevant audience. In order to calculate the required number of information channels that will be used in the implementation of the strategic narrative of the state, it is necessary to calculate the corresponding need for such means of influence on the relevant target audiences. This article is devoted to the statement of a possible variant of the decision of the resulted problems.

It is known that such problems are solved on the basis of modern scientific methods of social research theory and information theory. However, recently, research methods have been used, which are based on the similarity of the processes of dissemination of information on social networks and the processes of epidemics [6 - 9]. Therefore, the process of disseminating information on social networks and viral disease can be analytically formalized using the same system of differential equations. This system of differential equations is a mathematical model of the process of information dissemination (viral disease) and can be used to optimize the processes of increasing the potential coverage of the target audience, as well as identifying qualitative characteristics of information that affects the perception of the target audience. This makes it possible to predict the reactions of target audiences to a particular information, i.e., provides an opportunity to develop strategies to improve the efficiency of working with the information product, which is provided to the target audience for its wider coverage.

Let's move on to a direct consideration of the analytical model of information dissemination. This model can be represented as the following system of differential equations [10 -12]:

$$\begin{cases} dA/dt = -A(t)\mu + B(t)\xi + C(t)\xi\lambda; \\ dB/dt = -B(t)\mu - B(t)\xi + C(t)\lambda(1-\xi); \\ dC/dt = \big(A(t)+B(t)\big)\mu - C(t)\lambda. \end{cases}$$

where A – the number of active subscribers to the news channel, i.e., those who read the news;

B – the number of inactive subscribers to the channel, i.e. those who have not read the news, but are subscribers;

C – the number of non-subscribers who did not read the news;

λ – the intensity of subscribing to a news agent;

μ – the intensity of unsubscribing from the news agent;

ξ – intensity of reading the news.

With the initial conditions at the time $t = 0$:

$$A(0) = A_0, B(0) = B_0, C(0) = C_0.$$

$$A_0 > 0, B_0 > 0, C_0 > 0.$$

The solution of this system of equations can be presented as follows:

$$A(t) = C_1 g + C_2\, \nu e^{t(-\mu-\lambda)} - C_3\, e^{t(-\mu-\xi)},$$

$$B(t) = -C_1 r - C_2\, u e^{t(-\mu-\lambda)} + C_3\, e^{t(-\mu-\xi)},$$

$$C(t) = C_1 + C_2 e^{t(-\mu-\lambda)},$$

where $C_1 = \frac{A\_0 + B_0 + C_0\, u - C_0\, \nu}{g - r + u - \nu}$,

$$C_2 = \frac{-A_0 - B_0 + C_0 g - C_0\, r}{g - r + u - \nu},$$

$$C_3 = \frac{A_0 r - A_0 u + B_0 g - B_0 \nu + C_0 g u - C_0\, r u}{g - r + u - \nu},$$

where $g = \left[\frac{\lambda\xi}{\mu} - \frac{\xi(-\lambda\xi+\lambda)}{\mu(-\mu-\xi)}\right]$,

$$\nu = \left[-\xi + \frac{\xi(-\lambda\xi+\lambda)}{\lambda(\lambda-\xi)}\right],$$

$$r = \frac{(-\lambda\xi+\lambda)}{-\mu-\xi},$$

$$u = \frac{(-\lambda\xi+\lambda)}{\lambda-\xi}.$$

Data on the quantitative values of the first two parameters can be obtained by monitoring the news agent and the number of his subscribers. Parameter ξ takes into account such properties of the news as the relevance and timing of publication, as well as the activity of interaction of subscribers in the internal networks of the news agent.

Relevance of the news φ we will interpret as the probability of meeting the selected news in all the sources under consideration. That is

$$\varphi = \frac{m}{M},$$

where m – the number of news sources that describe the selected news;

M – total number of sources.

A parameter that characterizes the time of publication of the news δ визначається наступним чином:

$$\delta = \frac{e}{E},$$

where e – the amount of news on a particular topic, which includes controlled news, located in the user's news feed above the control news;

E – the total amount of news on a specific topic in the user's news feed.

The next parameter ω characterizes the probability of users to influence the process of increasing the readability of news. Let's assume that

$$\omega = \frac{S}{(A_0 + B_0)},$$

where S – the number of users who performed one of the actions: like or repost;

$(A_0 + B_0)$ – number of news agent subscribers.

Thus, the probability of reading the news can be given by the following expression:

$$\xi = \varphi\delta\omega.$$

Based on the above, we can conclude that if all the considered parameters of the model are known, then the values of the function can be calculated $A(t)$ at the right time and built a schedule of growth in the number of subscribers for the specified time of the study.

The study separately assessed the impact on the growth of the number of news channel subscribers under the following initial conditions of the study: information and technical capacity of the news channel (its ability to provide news information to a given population of the study region), socio-political characteristics of target audiences. as well as the level of popularity of the selected news channel among the population (skill, professionalism of the authors of the news, the relevance of the news, the time of its publication). For each of these initial conditions of the study, three variants of news channels were selected, for which the values of all necessary parameters of the Table 1 model were calculated.

Table 1

Parameters of the analytical model of information dissemination

№	Parameter	A_0	B_0	C_0	λ	μ	φ	δ	ω	ξ	g	ν	r	u	C_1	C_2	C_3
Version 1	Parameter value	5500	1500000	1300000	0,00135	0,000645	0,90	0,85	0,00399	0,0030	1,714	-1,808	-0,367	-0,812	910081	389925	1003817
	Equation	$A(t) = 1559879 + 707984e^{-0,002t} - 1003817e^{-0,00365t}$															
Version 2	Parameter value	3000	850000	800000	0,00135	0,000645	0,90	0,85	0,00399	0,0030	1,714	-1,808	-0,367	-0,812	536171	263828	534032
	Equation	$A(t) = 918997 + 477001e^{-0,002t} - 534032e^{-0,00365t}$															
Version 3	Parameter value	1850	515000	485000	0,00135	0,000645	0,90	0,85	0,00399	0,0030	1,714	-1,808	-0,367	-0,812	324962	160017	323404
	Equation	$A(t) = 556985 + 289310e^{-0,002t} - 323404e^{-0,00365t}$															

So, in fig. 1 shows the results of information dissemination for three information channels of different capacity, able to bring information news to regions with a population of 2.80, 1.65 and 1.00 million people, respectively. It should be emphasized that in order to identify the impact of the information capacity of the channel on the growth of its active subscribers, other parameters of the analytical model for all three news channels under consideration were chosen to be the same.

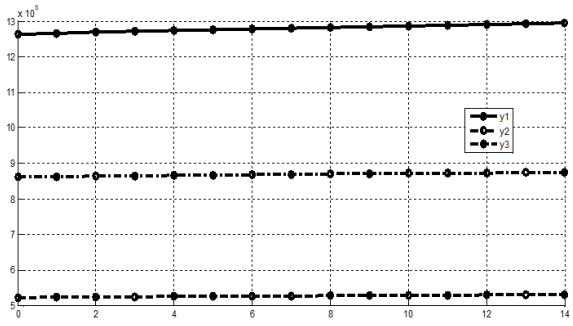


Figure 1: Graphs of growth of the number of subscribers of the news channel according to the information capacity of the channel

The analysis of the obtained results shows that the growth rate of active subscribers of the news

channel depends on the number of researched target audiences. This is absolutely self-evident and logically justified. But the growth of the number of active subscribers significantly depends on the relevance of information news, political, economic, social orientation of the information message, professional skills of its presentation, as well as the level of rating authority of the information channel of its energy capacity and information capacity to disseminate news. It is clear that these characteristics of the information channel always have certain limitations. That is why in order to achieve the success of the information impact, it is necessary to assess in advance the capabilities of each available information channel on the capabilities of its information impact on the growth of the channel's active subscribers from the total population. Based on the results of these calculations, it is possible to determine the required number of information channels of different information capacity, for example, to achieve the planned positive forecast development of public opinion of the population of Ukraine on accession to the EU.

Thus, from the analysis of the results obtained with the help of the considered analytical model of information dissemination, we can conclude that for the studied period of time (two weeks), for the considered variants of the studied population the increase of active subscribers will increase by:

1294500 - 1264000 = 30500 new active subscribers - for option 1;

875400 - 861970 = 13430 new active subscribers - for option 2;

531010 - 522890 = 8120 new active subscribers - for option 3.

That is, with the use of the considered information channels of the corresponding information and technical capacity for the given variants of quantitative groups of the population the growth of the number of active subscribers during the year can increase accordingly by:

30500 * 2 * 12 = 732000 new subscribers;

13430 * 2 * 12 = 322320 new subscribers;

8120 * 2 * 12 = 194880 new subscribers.

According to the forecast [2] to ensure the desired trends in public opinion in Ukraine, we need to increase the number of supporters of European integration during 2022-2023 by at least 3.1 million citizens. That is, based on the capabilities of one information channel, it is possible to estimate the required number of such channels to obtain the desired result of information impact on public opinion, taking into account the population of the studied regions. as well as the popularity of the selected information channel in the area. Thus, to realize the projected increase in supporters of European integration over the next two years through the information impact of channels with information capacity and capacity, corresponding to options 1-3, it is necessary at least:

3100000: 732000 ≈ 5 information channels with the capacity of option 1;

3100000: 322320 ≈ 10 information channels with the capacity of option 2;

3100000: 194880 ≈ 16 information channels with the ability of option 3.

Thinking similarly, you can calculate the required number of information and news channels targeted at specific target audiences or the number of channels of the required level of popularity and quality of information materials. However, it is clear that the qualitative assessment of information materials, their favorableness, and i.e., the impact on public opinion during the year cannot be equally effective. The success and effectiveness of the information channel depends on staffing, training, acquisition, purchase of technical means for the development of materials and many other factors.

3. Conclusions

The main goal for the system of strategic communications of the Ministry of Defense and the Armed Forces of Ukraine is to achieve a strategic narrative. As noted, the positive statistics of public opinion on support for EU accession is somewhat reduced, so such a narrative for this system should be the formation and strengthening of public opinion on supporting the strategic course of the state.

The application of the proposed mathematical tools to determine the required number of tools (information channels) in the interests of implementing the strategic narrative of the state on the basis of analytical model of information dissemination, will reasonably form the need and scope of information and psychological impact on target audiences, and the quality of news channels. This will provide an opportunity to identify the main tasks for the system of strategic communications and realize the interests of the state in the form of public support for the strategic course of the state to gain full membership of Ukraine in the EU.

Further development of this study should be carried out on the basis of modern scientific methods of the theory of social research and the theory of information operations in order to identify time indicators that characterize the distribution of materials of information influences to each target audience. It is especially important to receive such information from the temporarily occupied territories of Donetsk and Luhansk regions, as well as the Autonomous Republic of Crimea, which will allow to reasonably identify target audiences, argue the subject of messages and channels of information and psychological influence. To ensure the optimal total information impact, it is advisable to carry out a scientifically sound distribution of the projected total volume of tasks between the various structural units of the system of strategic communications, taking into account the characteristics of different target audiences. This will provide an opportunity not only to specify the goals and objectives for each structural unit of the strategic communications system, but also to develop effective and efficient materials of information and psychological impact to achieve them. This will allow to argue the subject of messages and choose the channels of distribution of materials of information and psychological influence, taking into account the individual characteristics of target audiences.

Reviewer: Doctor of tech. sciences. Professor Evseev S.P., Head of the Department of Cybersecurity and Information Technology, S. Kuznets Kharkiv National University of Economics.

4. References

[1] Decree of the President of Ukraine №121 / 2021 of March 25, 2021 on the decision of the National Security and Defense Council of Ukraine "On the Strategy of Military Security of Ukraine" URL: https://www.president.gov.ua/documents/12 12021-37661.

[2] [2] Solonnikov V.G. Rationale for the implementation of the strategic narrative of the state. / V.G. Solonnikov, O.V. Voitko, T.P. Pashchenko // Modern information technologies in the field of security and defense. - 2020. - №1 (37). - P. 203-212.

[3] [3] Voitko O.V. Peculiarities of application of the method of fractal analysis of the sustainability of the process of development of public opinion in the implementation of the strategic narrative of the state / O.V. Voitko, V.G. Solonnikov, O.V. Polyakova // Modern information technologies in the field of security and defense. - 2020. - №2 (38). - P. 145-150.

[4] Visualization of the model of information distribution. Internet resource URL: https://hhsbc.csb.app/

[5] [5] Voitko O.V. Indicators of information dissemination among the target audience / O.V. Voitko, S.A. Mikus // Proceedings of the 8th International Scientific and Practical Conference «Challenges in Science of Nowadays» (April 4-5, 2021). Washington, USA: EnDeavours Publisher, 2021. R.1053-1057.

[6] Kermack, W. O.; McKendrick, A. G. (1927). "A Contribution to the Mathematical Theory of Epidemics". Proceedings of the Royal Society A: Mathematical, Physical and Engineering Sciences

[7] Gubanov D.A. Review of online reputation / trust systems. Internet conference on governance issues. Moscow: IPP RAS, 2009. 25p.

[8] Gubanov D.A., Novikov D.A., Chkhartishvili A.G. "Social networks: models of information influence, management and confrontation", 2010 - 228 pages.

[9] Roberts F.S. Discrete mathematical models with applications to social, biological and ecological problems. - Moscow: Science, 1986.

[10] Mikhailov A.P., Petrov A.P., Marevtseva N.A., Tretyakova I.V. - Development of a model for the dissemination of information in society, 2014, Journal "Mathematical Modeling", p.74.

[11] D.V. Lande, V.A. Dodonov, Fractal Properties of Multiagent News Diffusion Model, 2016, 10p.

[12] Bolotin A.V. Development of a news dissemination model in social networks based on the SIR - epidemic model. Moscow: Moscow Institute of Electronics and Mathematics, 2018.

The criterion of the effective use of energy resources while producing plant products of specified quality

Vitaliy Lysenko[1], Valerii Koval[2], Igor Bolbot[3], Taras Lendiel[4], Kateryna Nakonechna[5], Anastasija Bolbot[6]

[1-6]*National University of Life and Environmental Sciences of Ukraine (Kyiv), 12v Heroiv Oborony str. (Building No. 11), Kiev, 03041, Ukraine*

Abstract

A new criterion for efficient use of energy resources, the essence of which is to minimize the difference between the relative indicators of phytoclimatic life support and phyto-development of plants, is proposed for use in automation systems implemented in protected ground facilities. It minimizes energy costs, while ensuring a specified quality of plants and products, and takes into account the phases of plant development.

Keywords

energy efficient control system, energy resources, phytomonitoring, mathematical modeling, greenhouse facilities, product quality monitoring, control strategies.

1. Introduction

At present, specialized studies have not established links between energy consumption and the state of the biological component of the object in protected ground facilities, which are characterized by the spatial distribution of technological parameters and indicators of plant quality. This is not taken into account in the development of principles for the construction and operation of energy-flow automation systems in spatially distributed facilities – greenhouse facilities for the production of products of specified quality.

Rational regulation of the microclimate in the greenhouse provides 90% of the crop [1]. The main components of the microclimate are temperature, light, CO_2 level in the greenhouse and relative humidity. The maximum level of productivity is achieved by reducing plant stress and ensuring an optimal balance of all factors. The condition of the plant and development are evidenced by uniform flowering, fruiting (generativeness) and leaf formation and development of the root system (vegetativeness) [2, 3].

EMAIL: lysenko@nubip.edu.ua (A. 1); v.koval@nubip.edu.ua (A. 2); igor-bolbot@ukr.net (A. 3); taraslendel@gmail.com (A. 4); kln273125@gmail.com (A. 5); anastasiyabolbot78@gmail.com (A. 6);
ORCID: 0000-0002-5659-6806 (A. 1); 0000-0003-0911-2538 (A. 2); 0000-0002-5708-6007 (A. 3); 0000-0002-6356-1230 (A. 4); 0000-0002-1537-7201 (A. 5)

There also arises a need to develop the criterion of the effective use of energy resources, the essence of which is to minimize the difference between the relative indicators of phytoclimatic life support and phyto-development of plants. The use of the above-mentioned criterion in automation systems for the control of energy flows in protected ground facilities for the cultivation of plant products ensures the minimization of energy costs and the predetermined quality of plant products, taking into account the phases of plant development.

2. Problem Statement

The purpose of this paper is to develop a criterion for the efficient use of energy resources by the control system in an industrial greenhouse, which will increase the energy efficiency of plant production, while ensuring its specified quality.

3. Research Methods

The assessment of the quality of tomatoes grown in protected ground facilities, both based

on the traditional differential and integrated methods, does not solve the problem successfully, because there is a need to take into account plant development at different phases.

It is proposed to define phytometric parameters of plant development in a non-contact manner. In the recognition system, the image is processed and entered into the data bank, where it is stored in the control unit, subjected to wavelet analysis, determination and comparison of the coefficients of mathematical decomposition with the database for determination of plant phytometric parameters [3, 20].

Phytometry criterion $\Phi\kappa$ is characterised by a large number of indicators of plant development in different plant phases, which have different measurement scales. We use the following correspondence to bring them to one scale of quality assessment of plant development:

$$\Phi\kappa = f(K_1, K_2, \ldots K_n), \quad (1)$$

where K_1, K_2,…K_n – individual indicators of plant development quality at different phases.

In general, the definition of quality indicators of plant development will be presented as [2, 4]:

$$K = \sum_{j=1}^{T}\left(A_j \cdot \sum_{i=1}^{H_j}(a_i \cdot k_i)\right) = \sum_{j=1}^{T}\left(A_j \cdot G_{jg}\right), \quad (2)$$

where T – number of groups of tomato quality indicators; H – the number of quality indicators in the j group; ai – weighting factor of the i property; k_i – relative i quality indicator; G_{jg} – the level of quality of the j group of indicators ($0 \le Gjg \le 1$); A_j – the weight parameter of the j group of tomato quality indicators.

Based on the use of the principles of qualimetry [5] we obtained complex indicators for assessing the quality of plant development (K_1-K_n) on the atmospheric temperature Θ and solar radiation L. The following regression equations were derived from the studies:

- formation by a plant of quantity of flowers in an inflorescence:

$$K_1(\Theta, L) = -0{,}05417 + 0{,}0375\cdot\Theta - ,55843\cdot L - 0{,}00225\cdot L\cdot\Theta^2 + 0{,}066563\cdot L\cdot\Theta + 0{,}11419\cdot L^2 - -0{,}01188\cdot L^2\cdot\Theta + 0{,}000339\cdot L^2\cdot\Theta^2; \quad (3)$$

- formation by the plant of the number of fruits on the branch:

$$K_2(\Theta, L) = 0{,}24375 - 0{,}03125\cdot\Theta - 0{,}00203\cdot L - 0{,}00013\cdot L\cdot\Theta^2 + 0{,}014219\cdot L\cdot\Theta + +0{,}020176\cdot L^2 - -0{,}00194\cdot L^2\cdot\Theta + 0{,}0000181\cdot L^2\cdot\Theta^2; \quad (4)$$

- the average weight of the fruit:

$$K_3(\Theta, L) = 1{,}79762 - 0{,}08929\cdot\Theta - 1{,}1082\cdot L - -0{,}0012\cdot L\cdot\Theta^2 + 0{,}084598\cdot L\cdot\Theta + 0{,}102193\cdot L^2 - -0{,}00625\cdot L^2\cdot\Theta + 0{,}0000658\cdot L^2\cdot\Theta^2; \quad (5)$$

- the weight gain of the fruit:

$$K_4(\Theta, L) = 0{,}211504 + 0{,}01404\cdot\Theta - 0{,}39973\cdot L - 0{,}00051\cdot L\cdot\Theta^2 + 0{,}023981\cdot L\cdot\Theta + +0{,}027996\cdot L^2 - -0{,}00039\cdot L^2\cdot\Theta + 0{,}0000093\cdot L^2\cdot\Theta^2 \quad (6)$$

Assessment of the quality of plant development by the integral dependence of indicators with the same weighting factor of 0.25 made it possible to obtain the dependence of the phytometry criterion of plant development quality on the influence of average daily atmospheric temperature and light intensity (Fig. 1):

$$\Phi\kappa(\Theta, L) = 0{,}517645 - 0{,}01491\cdot\Theta - 0{,}49627\cdot L - 0{,}00099\cdot L\cdot\Theta^2 + 0{,}045348\cdot L\cdot\Theta + 0{,}063845\cdot L^2 - 0{,}00488\cdot L^2\cdot\Theta + 0{,}000103\cdot L^2\cdot\Theta^2 \quad (7)$$

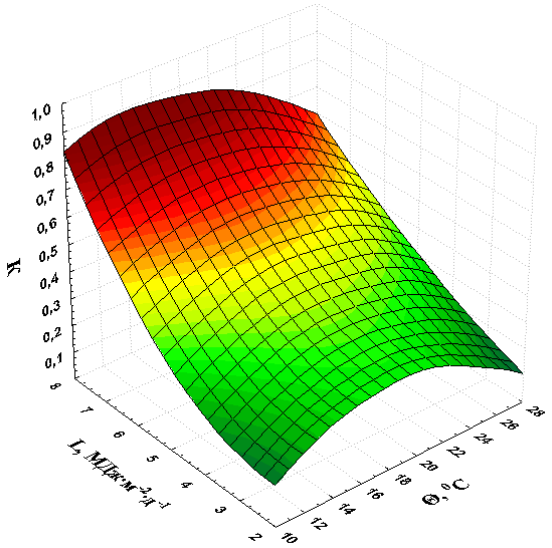


Figure 1: Dependence of phytometric criterion on average daily atmospheric temperature and light intensity

Using phytometry criterion, we determine the level of plant development during its growing season. Maintaining the maximum level of development will allow to form the maximum yield in plants at the initial stage. At the

temperatures of 15 - 24ºC in the greenhouse we may observe the best formation of the plant yield (the number of flowers in the inflorescence, the number of fruits on the branch, the average weight of the fruit, the weight gain of the fruit).

To improve plant development, production conditions must be maintained, during which temperatures measured at different points in the greenhouse will be evaluated and compared. The control of technological parameters of the microclimate during plant growing is based on the measured phytometric parameters of the plant, which allows to assess the development of plants by introducing a phytotemperature criterion to assess the condition of the plant [6, 20].

The phytotemperature criterion $\Phi\kappa$ for estimating the development of a plant and its temperature environment evaluates the part of the heat coming from the heat carrier of the greenhouse heating system for heating the plant and the environment around it [6]. Description of experimental data was performed using a standard technique based on the least square method. Thus, the regression equation was obtained explicitly:

$$\Phi\kappa\,(\Theta_p, \Theta)=-4{,}96+0{,}059\cdot\Theta_p-0{,}243\cdot\Theta+0{,}027\cdot\Theta_p\cdot\Theta+0{,}0031\cdot\Theta_p-0{,}0091\cdot\Theta--0{,}0175\cdot\Theta_p^2-0{,}0175\cdot\Theta^2 \quad (8)$$

To ensure the technological requirements for growing quality plant products in the greenhouse, it is proposed to assess the temperature of plants (Θ_p) and the atmosphere of the greenhouse (Θ) based on the use of phytotemperature criteria for assessing plant development (Fig. 2).

According to the analysis of research materials, it is established that the use of phytotemperature criterion makes it possible to obtain the maximum yield from the plant. As a result, from one bush we get less than 160 grams of weight gain per day, because at the temperatures of 17 - 22ºC the plant receives insufficient energy for better development and the increase is 5.2 - 6 grams, and at temperatures above 25ºC the increase in yield will be less than 6 g per hour.

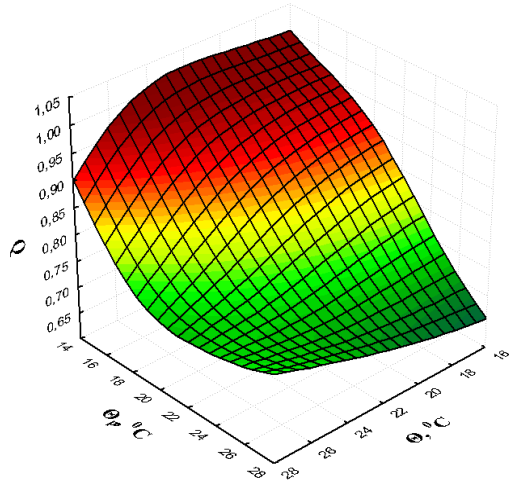


Figure 2: Dependence of phytotemperature criterion on atmospheric and plant temperatures

To determine the indicator of plant life support ($\Phi\kappa$), we use the following algorithm on the entire area of the greenhouse. Let $\tilde{v}_{ij}(\tilde{t}_{jk})$ – the value of the indicator of the life support of the plant, determined on the i row of the j place at the corresponding total intensity of solar radiation $(\tilde{t}_{jk})$, where $i=\overline{1,n}$; $j=\overline{1,n}$; n – number of rows; k – the measurement number in the row $(k=\overline{1,K_j})$; K_j – the number of measured plant life support factors in the j place; $(j=\overline{1,m})$; m – the number of measurements.

We interpolate discrete dependences $\tilde{v}_{ij}(\tilde{t}_{jk})$ by splines:

$$V_{ij}(t)\ \ (i=\overline{1,n};\ j=\overline{1,m}), \quad (9)$$

where $t\in[t_{\min}, t_{\max}];\ \ t_{\min}=\max\limits_{j=1,m} t_{j1};\ \ t_{\max}=\min\limits_{j=1,m} t_{jK_j}$ are respectively the lowest and highest value of the total intensity of solar radiation, for which the life support of the plant was determined during the measurement period.

We choose on the interval of $t\in[t_{\min}, t_{\max}]$ N evenly spaced nodes tk $(k=\overline{1,N})$. Let us calculate the values of splines (9) at these points:

$$v_{ij}(t_k)\ \ (i=\overline{1,n};\ j=\overline{1,m};\ k=\overline{1,N}) \quad (10)$$

These values describe the $\Phi\kappa$ for all rows and places with the same total intensity of solar radiation. The value of the indicator for the entire area of the greenhouse (10) is presented in (Fig. 3).

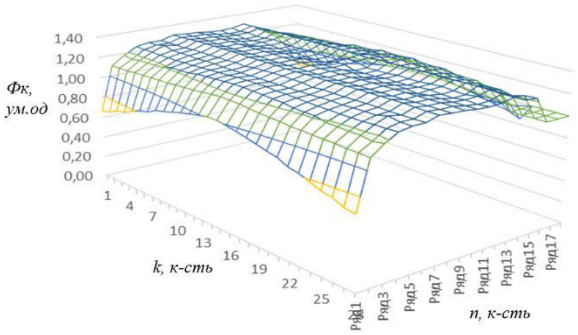


Figure 3: The value of the phytoclimatic indicator of plant life support over the entire area of the greenhouse

Given that φ_i, λ_i – are coordinates of the *i* row, we will determine the coordinates of the center of all rows:

$$\bar{\varphi} = n^{-1}\sum_{i=1}^{n}\varphi_i\ ,\ \bar{\lambda} = n^{-1}\sum_{i=1}^{n}\lambda_i\ . \qquad (11)$$

Taking into account the zones of similarity in the distribution of microclimate parameters, we determine the distances between the rows relative to their central row, describing the spatial density of the rows in which the measurements were made:

$$r_i = \sqrt{(\bar{\varphi}-\varphi_i)^2 + (\bar{\lambda}-\lambda_i)^2}\ \ (i=\overline{1,n})\ . \qquad (12)$$

Values inverse to distances $r_i\ \ (i=\overline{1,n})$, make sense of weighted averaging coefficients $\tilde{w}_i = 1/r_i\ \ (i=\overline{1,n})$.

Let us determine the average value $\tilde{v}_{ij}(\tilde{t}_{jk})$ in the rows:

$$\bar{v}_j(t_k) = \sum_{i=1}^{n} w_j v_{ij}(t_k)\ \ (j=\overline{1,m};\ k=\overline{1,N})\ . \qquad (13)$$

Graphs of the average value of the phytoclimatic indicator of plant life in rows (13) are shown in (Fig. 4).

The average value of the plant life support over the entire area of the greenhouse is determined by the expression:

$$\bar{v}(t_k) = n^{-1}\sum_{i=1}^{n}\bar{v}_i(t_k)\ \ (k=\overline{1,N})\ . \qquad (14)$$

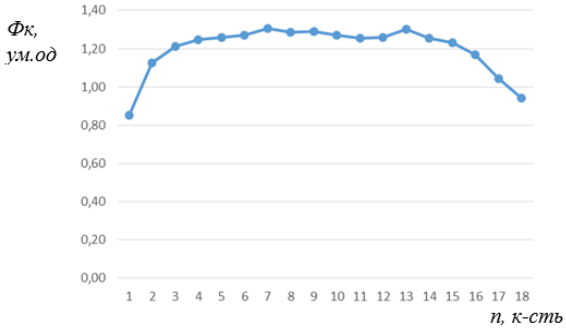


Figure 4: The average value of the phytoclimatic indicator of plant life support in rows

The average value of the plant life support over the entire area ΦK = 1.2 indicates an excessive level of plant life support parameters.

According to the considered algorithm we will determine the value of phytometric criterion (Φ_M), phytotemperature criterion (Φ_m) and their average value – phytodevelopment index (Φ_p) by rows (Fig. 5), which will allow to establish the level of plant development and crop quality [7].

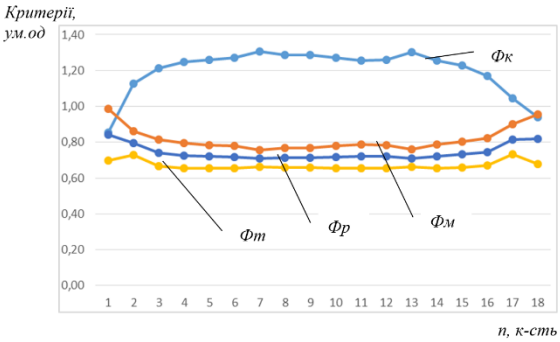


Figure 5: Dependence of change of average value of an indicator of plant life support, phytometric and phytotemperature criteria on all area in rows

It was found that the average value of phytoclimatic index is Фк=1,2, of phytometric criterion is Фм=0,82, of phytotemperature criterion is Фт=0,67 and their average value of phytodevelopment index is Фр=0,74 on the whole area of the greenhouse.

Exceedance in the value of the Фк>1 indicator shows an excessive level of parameters of plant life support established by agrotechnology, respectively, and the overuse of energy carriers for their provision. The value of Фр<1 indicates insufficient levels of plant development and quality of plant products in the greenhouse. Obtaining quality products with minimal consumption of energy resources is possible provided that the criterion of efficient use of

energy resources for the production of plant products of a specified quality is minimized (Fig. 6):

$$R = \Phi_к - \Phi_р \rightarrow min. \quad (18)$$

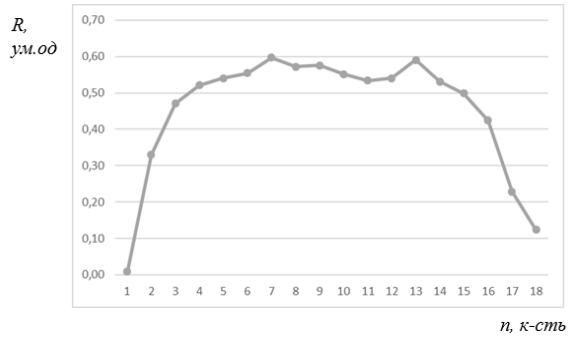


Figure 6: Criterion of efficient use of energy resources during the production of plant products of specified quality

The strategy of effective control is to reduce the standard deviation between the phytoclimatic indicator of plant life support and the value of phyto-development, when its increase indicates inefficient energy consumption by the existing control system of plant production technology of a specified quality.

4. Conclusions

1. The authors offer to introduce the following components into the algorithm of operation of the control system:

- phytometric criterion, which is characterized by a significant number of indicators of plant development in its various phases, namely flowering, fruit formation and harvest; assessment of the quality of plant development will be carried out using the integrated dependence of indicators. The use of phytometry criterion determines the level of plant development during its growing season, and its strict observance allows to form the maximum yield of plants at the initial stage;
- phytotemperature criterion for assessing the state of development of the plant, which creates conditions for obtaining the maximum yield of tomatoes; analysis of changes in plant temperature and atmospheric temperature in a greenhouse equipped with an automatic air temperature control system proves the need to use the proposed criterion.

2. To assess the conditions of plant development in the greenhouse the authors used phytoclimatic indicator of plant life support and assessment of the plant itself – the indicator of phyto-development, which allows to determine the level of plant development and crop quality. Exceedance of phytoclimatic value over 1 has been found to indicate an excessive level of plant life support from established agro-technology, and, respectively, an overexpenditure of energy resources spent on their provision. The value of the indicator of phyto-development less than 1 indicates the insufficiently possible level of plant development and the quality of plant products. It has been established that obtaining quality products with a minimum consumption of energy resources is possible provided that the criterion of efficient use of energy resources is minimized, when the average growth of the greenhouse to 46% indicates inefficient energy consumption of existing control systems.

5. References

[1] Bryzgalov V.A. (Ed.), Sovetkina V.E., Savinova N.I. (1995). Vegetable growing in protected ground. M.: Kolos [in Russian].

[2] Lendiel, T.I. (2016). Energy-efficient control of the electrotechnical complex in the greenhouse considering the state of the biological object. Extended abstract of candidate's thesis. Kyiv: NuBiP [in Ukrainian].

[3] Lysenko V. P., Zhyltsov A. V., Bolbot I. M., Lendiel T. I., Nalyvaiko V. A. Phytomonitoring in the phytometrics of the plants. E3S Web of Conferences 154, 07012 (2020) ICoRES 2019 https://doi.org/10.1051/e3sconf/202015407012

[4] Bolbot, I. M. (2013). Mathematical model of the influence of the thermal regime on the development and productivity of tomatoes in the plant-soil-air system. MOTROL. Lublin. Vol. 15 No. 4, 153–158 [in Russian].

[5] Toybert, P. (1988). Assessment of the accuracy of measurement results (V.N. Khramenkova, Trans.). M.: Energoatomizdat [in Russian].

[6] Lysenko, V.P, Bolbot, I.M, Lendiel, T.I. Phytotemperature criterion for assessing plant development. Enerhetyka i avtomatyka, 3, 122–128 [in Ukrainian].

[7] Bolbot, I. M. (2014). Criterion for ensuring the productivity of plants – the basis for the effective consumption of energy resources by greenhouse complexes. *Proceedings of the international scientific and technical*

conference "Energy supply and energy saving in agriculture" (pp. 157-162) Vol. 2. [in Russian].

[8] Lysenko, V., Bolbot, I., & Lendel, T. (2019). Energy efficient system of electrotechnological complex control in industrial greenhouse. Technical Electrodynamics, 2019(2), pp. 78-81. doi:10.15407/techned2019.02.078. [in Ukrainian].

[9] Martynenko, I.I., Lysenko, V.P., Tishchenko, L.P. et al (2208). Design of electrification and automation systems of agro-industrial complex. Textbook [in Ukrainian].

[10] Ahmed Ouammi, Yasmine Achour, Driss Zejli, Hanane Dagdougui, "Supervisory Model Predictive Control for Optimal Energy Management of Networked Smart Greenhouses Integrated Microgrid", Automation Science and Engineering IEEE Transactions on, vol. 17, no. 1, pp. 117-128, 2020.

[11] O. Vovna, I. Laktionov, S. Sukach, M. Kabanets and E. Cherevko, "Method of adaptive control of effective energy lighting of greenhouses in the visible optical range", Bulgarian Journal of Agricultural Science, vol. 24, pp. 335-340, 2018.

[12] Ouammi, A., Achour, Y., Dagdougui, H., & Zejli, D. (2020). Optimal operation scheduling for a smart greenhouse integrated microgrid. Energy for Sustainable Development, 58, 129-137.

[13] N. Kiktev, H. Rozorinov and M. Masoud, "Information Model of Traction Ability Analysis of Underground Conveyors Drives", 13th International Conference MEMSTECH, 2017.

[14] V. Bodrov, M. Bodrov and V. Kuzin, "Ensuring the parameters of microclimate of hothouses during a warm season", ARPN Journal of Engineering and Applied Sciences, vol. 12, no. 6, pp. 1864-1869, 2017.

[15] Tregub V, Korobiichuk I, Klymenko O, Byrchenko A, Rzeplińska-Rykała K (2020) Neural network control systems for objects of periodic action with non-linear time programs. In: Szewczyk R, Zieliński C, Kaliczyńska M (eds) Automation 2019. Advances in intelligent systems and computing, vol 920. Springer, Cham.

[16] Revathi S, Radhakrishnan TK, Sivakumaran N (2017) Climate control in greenhouse using intelligent control algorithms. Paper presented at the proceedings of the American control conference, pp 887–892. https://doi.org/10.23919/acc.2017.7963065 .

[17] S. A. Shvorov, D. S. Komarchuk, N. A. Pasichnyk, O. A. Opryshko, Y. A. Gunchenko and S. D. Kuznichenko, "UAV Navigation and Management System Based on the Spectral Portrait of Terrain," 2018 IEEE 5th International Conference on Methods and Systems of Navigation and Motion Control (MSNMC), 2018, pp. 68-71, doi: 10.1109/MSNMC.2018.8576304.

[18] S. A. Shvorov, N. A. Pasichnyk, S. D. Kuznichenko, I. V. Tolok, S. V. Lienkov and L. A. Komarova, "Using UAV During Planned Harvesting by Unmanned Combines," 2019 IEEE 5th International Conference Actual Problems of Unmanned Aerial Vehicles Developments (APUAVD), 2019, pp. 252-257, doi: 10.1109/APUAVD47061.2019.8943842.

[19] Yu. Gunchenko, S. Shvorov, N. Rudnichenko and V. Boyko, "Methodical complex of accelerated training for operators of unmanned aerial vehicles", 2016 IEEE 4th International Conference Methods and Systems of Navigation and Motion Control, 2016.

[20] Bolbot I. M. (2020). Automation of greenhouse complex control processes on product quality monitoring. Extended abstract of doctoral thesis. Kyiv: NuBiP [in Ukrainian].

Проблеми Аналізування Та Прогнозування Інформаційно-Психологічних Впливів У Соціальних Мережах

Браіловський М.М. [1], Толюпа С.В. [2]

[1] *Київський національний університет імені Тараса Шевченка, вул. Богдана Гаврилишина, 24, Київ, 04116, Україна*
[2] *Київський національний університет імені Тараса Шевченка, вул. Богдана Гаврилишина, 24, Київ, 04116, Україна*

Анотація

Для захисту від інформаційно- психологічного впливу необхідно застосовувати не тільки оборонні методи, а й превентивні. Серед таких засобів є аналіз та прогнозування подій, інформація про які з зростаючою частотою починає з'являтися та обговорюватися в соціальних мережах. Розглядаються питання впливу на людину і суспільство за допомогою «м'якої сили» та застосування мережевих структур, які можуть ефективно обчислювати, прогнозувати і протидіяти прояву маніпуляцій в цифровому просторі.

Ключові слова

Соціальні мережі, аналіз, прогнозування, управління, інформаційний вплив, м'яка сила.

Mykola Brailovskyi [1] , Serhii Toliupa [2]

[1] *Taras Shevchenko National University of Kyiv, Bohdana Havrylyshyna Street, 24, Kyiv, 04116, Ukraine*
[2] *Taras Shevchenko National University of Kyiv, Bohdana Havrylyshyna Street, 24, Kyiv, 04116, Ukraine*

Abstract

To protect against information and psychological influence, it is necessary to use not only defensive methods, but also preventive ones. Such tools include analysis and forecasting of events, information about which is beginning to appear and discuss on social networks with increasing frequency. The issues of influencing people and society through "soft power" and the use of network structures that can effectively calculate, predict and counteract the manifestation of manipulation in the digital space are considered.

Keywords

Social networks, analysis, forecasting, management, information impact, soft power.

1. Вступ

На сьогодні онлайнові соціальні мережі, мають надзвичайною популярністю, та є одним з основних інструментів інформаційно-психологічного впливу на значну частину населення, і в більшій своїй частині на молодь. Необхідність протидії загрозам інформаційної безпеки, які можуть бути реалізовані через онлайнові соціальні мережі, підтверджена Стратегією національної безпеки і Доктриною інформаційної безпеки України, що вказує на значну актуальність дослідження інформаційних процесів в онлайнових соціальних мережах, які є зваженими неоднорідними мережами.

Глибинні зміни у ставленні більшості країн світу, зокрема й України, до власної інформаційної, а отже, і кібернетичної безпеки спонукають приділяти дедалі більшу увагу розробленню рекомендацій стосовно коротко- та довгострокових пріоритетів трансформації безпекового сектору за напрямками пошуку й збору інформації з відкритих і відносно відкритих джерел, а також добування її із закритих електронних джерел, переймаючись водночас питаннями захисту власного інформаційного ресурсу від стороннього кібервпливу [1]. Розв'язанню зазначених

EMAIL: bk1972@ukr.net (A.1) , tolupa@i.ua (A. 2);
ORCID: 0000-0002-3148-1148 (A.1), 0000-0002-1919-9174(A.2)

проблем у певних аспектах присвячено чимало публікацій зарубіжних і вітчизняних авторів, таких як В. Бурячок, А. Корченко, В. Домарєв, В. Богданович, Дж. Козіол, М. Кузнєцов, Кр. Касперські, К. Митник, І. Симдянов.

2. Основна частина.

З розвитком інформаційних систем та глобальної мережі Internet світове суспільство крім отримання значних можливостей щодо обміну інформацією стало надто уразливим від стороннього кібернетичного впливу, а саме від фактично неприхованих спроб впливу протиборчих сторін на інформаційний і кіберпростори один одного за рахунок використання засобів сучасної обчислювальної та/або спеціальної техніки й відповідного програмного забезпечення (так званих кібервтручань) та інших проявів їх дестабілізуючого негативного впливу на певний об’єкт, що реалізуються за рахунок використання технологічних можливостей інформаційного і кіберпросторів, створюючи при цьому небезпеку як для них самих, так й для свідомості людини у цілому (так званих кіберзагроз) [2].

В епоху глобальної інтенсифікації інформаційних процесів і їх проникнення в усі сфери (соціальну, політичну, економічну) діяльності людини, коли практично кожній людині доводиться виконувати різні завдання, взаємодіючі з численними елементами IT-інфраструктури, залежність кожного індивіда від інформаційних систем і мереж та його уразливість щодо стороннього кібернетичного впливу постійно зростають. Зрештою травмується психіка людини, а це, у свою чергу, може спонукати її до розголошення інформації з обмеженим доступом (ІзОД). Саме тому соціальні інженери в пошуках об’єктів своїх атак беруть до уваги передусім психологічний стан причетних до них осіб [3].

Найважливішими завданнями інформаційно-аналітичної підтримки роботи з онлайновими соціальними мережами є їх моніторинг, аналіз, а також прогнозування та управління.

Перші два завдання служать для розуміння процесів, що відбуваються в соціальних мережах. Моніторинг включає отримання та структурування первинних даних. При цьому проводиться збір текстів повідомлень, зв'язків між користувачами та посилань на зовнішні ресурси. Можливості цих систем багато в чому визначаються багатством використовуваних даних і режимом їх обробки. За можливості аналізу даних системи моніторингу та аналізу соціальних мереж можна поділити на три види:

• системи, які не здійснюють аналіз даних;

• системи, що здійснюють ретроспективний аналіз даних;

• системи, що здійснюють аналіз даних в режимі реального часу [4].

Системи моніторингу, які здійснюють роботу в режимі реального часу, складніше в розробці і експлуатації, ніж комплекси, що використовують ретроспективний збір даних. Тому стає очевидним роль даних, отриманих раніше і на підставі яких вже були зроблені деякі висновки і прогнози, а також створені відповідні бази знань. Аналіз має на увазі кілька етапів обробки первинних даних. В першу чергу, обчислюються базові показники, що відповідають на прості питання кількісного характеру, наприклад, «скільки користувачів в мережі?», «скільки повідомлень написав користувач?», «скільки з них активних?», «скільки з них мають високий рівень авторитету», тощо. Потім проводиться виявлення статистичних та структурних закономірностей в отриманих даних, що дозволяє зрозуміти природу досліджуваної мережі. Наприклад, типи розподілів, до яких відносяться обговорення тих чи інших тем. З точки зору практичного застосування найбільший інтерес представляє виявлення специфічних закономірностей у вузьких предметних обговореннях. Виявлення найбільш популярних тем обговорення і, головне, реакції користувачів на них.

Етап прогнозування використовується для передбачення з певною часткою ймовірності стану соціальної мережі через певний проміжок часу за певних умов.

Вони можуть фокусуватися на аналізі різних об'єктів соціальної мережі [5], таких як:

• мережа «в цілому» (за допомогою агрегованих глобальних показників);

• підмережі і спільноти;

• окремо взяті користувачі;

• інформаційні повідомлення;

• думки (за допомогою показників тональності повідомлення щодо деяких інформаційних об'єктів);

• зовнішні вузли - інформаційні ресурси мережі Інтернет. Варто відзначити, що

інформаційним об'єктом може бути деяка персона, подія, організація і т. п.

На думку авторів, на сьогоднішній день мало приділяється уваги такому процесу як прогнозування подій. Це можливо пов'язано з тим, що завдання аналізу, прогнозування та управління можуть бути різними. По-перше, в залежності від того, хто ставить завдання, хто є кінцевим користувачем системи, хто цікавиться цією темою. Існують різні типи користувачів, яким необхідно проводити аналіз, прогнозування та управління онлайновими соціальними мережами [3]:

• органи державної влади та місцевого самоврядування;

• підприємства державного і приватного сектора економіки (комерційні, науково-дослідні організації, засоби масової інформації (ЗМІ));

• суспільство (політичні партії, окремі фізичні особи).

По-друге, на скільки очікуваний прогноз вигідний користувачеві. Чи не призведе цей прогноз до загального погіршення політичної чи економічної ситуації користувача, а то і взагалі національної безпеки. Бувають випадки, і таких досить багато, коли після проведення аналізу відсутня будь-яка реакція на ситуацію, що склалася, або інформацію про подію. Або не наводяться припущення, прогнози очікуваного розвитку ситуації. Немає тривожного сигналу на негативну інформацію. Виникає питання: «Ми не бачимо загрози або не хочемо її бачити?». Особливо це стосується ситуації з культурними заходами, такими як література, кінематограф, естрада, живопис і т.д.

Як відомо, людина живе в трьох вимірах - в світі реальному, світі інформаційному і світі символічному. Однак саме в сучасному світі нові технології і засоби комунікації надають настільки потужний вплив на свідомість, що реальні дії і події тільки тоді стають значущими, коли вони представлені в ЗМІ, тобто стають функцією віртуальності. Події як би і немає в реальному житті, якщо про неї не написано на сайті чи вона не відображено в соцмережі. Це одна сторона справи. Важливо ще й те, що сучасні технології дозволяють легко і швидко маніпулювати свідомістю великих мас людей, формувати потрібні маніпулятору образи і символи [5].

Кращим прикладом такої ситуації, беручи до уваги масово-публічні соціальні мережі, є як раз - кіно, назване не дарма одним із класиків світового пролетаріату - найважливішим з мистецтв. Воно дозволяє в собі втілити всі можливі прийоми психологічного впливу - відео, звук, ритм, ідеї, настанови і т.п. У кінофільмах досить легко можна словами і діями головного героя вселити глядачеві алгоритм дій і «правильне» сприйняття проблеми. Прикладами можуть бути свого часу популярні фільми, виробництва Росії, - «Брат» та «Брат-2», «72 метри», «Кандагар», що представляють українців другосортною нацією зрадників, ненав'язливо формуючи у глядача необхідний стереотип.

Такі підходи починають управляти користувачем. І тому необхідно розпізнати зовнішній вплив і спрогнозувати до чого це може привести надалі.

Фаза управління полягає в наданні цілеспрямованих впливів на соціальну мережу для переведення інформаційних процесів в бажаний стан. На цьому етапі можливі якісні рекомендації користувачеві, так звана - «м'яка сила».

Поняття «м'яка сила» (МС) було введено в науковий обіг (англ. "Soft power") Джозефом Наєм - американським політологом, професором Гарвардського університету на початку 90-х років минулого століття.

Основний сенс soft power полягає в формуванні привабливої влади або умов існування, тобто в здатності впливати на поведінку людей, опосередковано примушуючи їх робити те, що в іншому випадку вони ніколи не зробили б. Такою влада стає, не лише спираючись на переконання, умовлянні або здатність спонукати людей зробити щось за допомогою аргументів, а й на «активах», які продукують її привабливість. Досягти цього, на думку Ная, можливо, використовуючи «владу інформації та образів», владу смислів. Іншими словами, ядро «м'якої сили» є нематеріальність, а інформативність і рухливість.

М’якосиловий вплив на великі маси людей може бути здійснено в досить короткий період - він, як правило, не перевищує декількох місяців. У цьому випадку найбільш ефективними інструментами soft power якраз і є ЗМІ, традиційні і нові соціальні медіа.

У довгостроковій перспективі м’яка сила в меншій мірі залежить від риторики, але більше пов'язана з практичною діяльністю. В цьому випадку ефективними інструментами «м'якої сили» є: надання послуг з навчання мови,

культури країни, її історії, вищої освіти, а також розвиток наук, в тому числі громадських, основне завдання яких полягає у виробництві смислів - теорій і концепцій, легітимізуючих позицію і погляди держави, яка проводить політику популяризації свого світогляду, традицій укладу життя. Сукупність цих стратегій дозволяє впливати на систему соціокультурних фільтрів або «матрицю переконань» конкретного індивіда, суспільства, по відношенню до якого застосовується даний тип впливу, змушуючи його в кінцевому підсумку змінити свою поведінку на потрібну маніпулятору.

Щоденна життєва практика, переконливо доводить: забезпечення інформаційної і кібернетичної безпеки — процес безперервний, надзвичайно складний і багатогранний, причому успіх у його реалізації зумовлюється соціумом і залежить від кожного його представника, але передусім від неухильно здійснюваної державної політики в цій сфері, цілеспрямованих зусиль усіх гілок влади, наукової громадськості, керівників усіх рівнів [6]. Водночас систематизовані заходи із запобігання численним загрозам не повинні перешкоджати дедалі стрімкішому формуванню національного інформаційного і кібернетичного простору, а також інтеграції України у світове інформаційне суспільство [7]. Саме тому стратегічним завданням державної політики має стати формування комплексної системи інформаційної і кібернетичної безпеки, в основу якої покладено науково обґрунтовані політичні, соціальні й економічні критерії та світовий досвід щодо правових і організаційних аспектів функціонування [8].

3. Висновок

Таким чином стає очевидним необхідність приділяти більше уваги процесам, що відбуваються в соціальних мережах та інформації, яка в них циркулює. Як мовиться у відомій приказці: «Немає диму без вогню», тобто якщо якась інформація з'являється в мережі і починає бурхливо обговорюватися користувачами то це комусь потрібно. При чому це може бути штучно створений ажіотаж. Тому необхідно приділити особливу увагу не тільки її окремими складовими, а й їх сукупності. Необхідне створення критеріїв, алгоритмів і програмного забезпечення для прогнозування, попередження ситуації і своєчасного прийняття правильних рішень. Зрозуміло, що влада, яка прагне зберегти суверенність, повинна мати в своєму розпорядженні набір інструментів, що обмежують (зводять до мінімуму) ефективність маніпулятивного впливу «м'якої сили». Державам необхідно розробити і застосовувати ті мережеві структури, які можуть ефективно виявляти, прогнозувати і протидіяти прояву маніпуляцій в цифровому просторі, працювати в тому ж операційному полі, що і їх потенційні і реальні противники.

4. Література

[1] Mykola Brailovskyi, Volodymyr Khoroshko, Volodymyr Artemov, Oleksandr Lytvynenko Information war in modern conditions. Part 1 // Scientific & practical cyber security journal (SPCSJ) VOL 5. №2. [Electronic journal]. https://journal.scsa.ge/ru/papers/information-war-in-modern-conditions-part-1-3/

[2] Бурячок В.Л., Толюпа С.В., Толубко В.Б., Хорошко В.О. «Інформаційна та кібербезпека: соціотехнічний аспект» // Навчальний посібник. – К.: Наш формат, 2015. – 288с.

[3] Бурячок В.Л., Толюпа С.В., Семко В.В. Інформаційний та кіберпростори. Проблеми безпеки, методи та засоби боротьби. Навчальний посібник. К.: ТОВ “Наш формат”, 2016. – 176с.

[4] Браиловский Н.Н., Хорошко В. А. Методы распознавания кибератак с учетом мониторинга информационной среды. Безпека інформації. Том 27, № 1 (2021) С.6-13

[5] Toliupa. S. V, Nakonechny. V. S, Brailovskyi. N. N. Building Cyber-Security Systems of Information Networks Based on Intellectual Technologies// Scientific & practical cyber security journal (SPCSJ) №1. [Electronic journal]. URL: http://journal.scsa.ge/issues/ 2017/09/432.

[6] В.Л. Бурячок, С.В. Толюпа, А.О. Аносов “Системний аналіз та прийняття рішень в інформаційній безпеці”. - К. : ДУТ, 2015. – с.345.

[7] Бурячок В.Л. Основи формування державної системи кібернетичної безпеки: Монографія. – К.: НАУ, 2013. – 432 с.

[8] Nikolay Brailovskyi, Volodymyr Khoroshko, Volodymyr Artemov, Ivan Opirskyi, Ihor Ivanchenko Information war in Ukraine// Scientific & practical cyber security journal (SPCSJ) VOL 4. №4. [Electronic journal]. https://journal.scsa.ge/ru/papers/information-war-in-ukraine-2/

Methods For Assessing The Risk Of Approaching Ships As An Integral Part Of The Vessel Traffic Control System

V. Strelbitskyi [1], Nataliia Punchenko [2] and Oleksandra Tsyra [3]

[1] *Odessa National Maritime University, Odesa, Ukraine*
[2] *Odesa State Environmental University Odesa, Ukraine*
[3] *Odesa State Environmental University Odesa, Ukraine*

Abstract

The article presents a brief overview of methods for ensuring the navigation safety of vessel traffic, which are divided into three categories: methods of early detection of the collision possibility of ships, methods of maneuvering to avoid a collision and planning trajectory methods of the ship. A detailed theoretical review of methods for assessing the risk of a dangerous approach of ships, associated with ensuring the navigation safety of ship traffic, is carried out in detail. The representation of ship domains is disclosed to assess the risk of a dangerous approach of ships. The work provides links to sources that clarify the presented material.

Keywords

Navigation safety, navigational control methods, risk assessment, ship convergence, "ship domain"

1. Introduction

The science of ensuring safe navigation in the civil and military spheres is in the process of improvement. A global issue in this scientific area is prevention of groundings and collisions of ships. This science examines the aspect of the problem of navigation safety from all sides. Navigation figure 1, since antiquity, as a result, has created problems of navigation safety. Ensuring navigational safety is a task that is a complex multi-level complex.

To solve this problem, the forces are united: manufacturers of maritime navigation aids, international organizations, administrations of states participating in world shipping. The cooperation of these entities forms a system for ensuring safe navigation. Despite such cooperation, a high percentage of ship accidents at sea is an objective reality that cannot be denied and is primarily due to the peculiarities of external and internal factors accompanying navigation, which will always be present regardless of the human factor. The level of state and reliability of navigation in modern conditions, the real accuracy of navigation and the quality of navigation problems is about twice worse than expected. It follows that the complete elimination of the accident rate of ships has no chance. But it is quite possible to influence the number of accidents with the help of various measures and try to achieve its relative maximum reduction for a period that is limited. Such a drop in the accident rate can be achieved up to a certain level, after which the accident rate will inevitably grow again or temporarily stabilize [1]. This conclusion follows from the realities of the present time, which can be characterized:

1. An increase in the volume of water transport
2. The increasing traffic intensity in areas of busy shipping leads to a constant increase in the workload on boat masters

EMAIL: vict141174@gmail.com (A. 1); iioonn24@rambler.ru (A. 2); aleksandra.tsyra@gmail.com (A. 3)
ORCID: 0000-0001-7027-9498 (A. 1); 0000-0003-1382-4490 (A. 2); 0000-0003-3552-2039 (A. 3)

Figure 1: Water transport

Experimental studies show that the largest number of accidents in water transport occur in the areas of responsibility of ports and on the approaches to them. In this regard, the problem of safe movement at sea becomes most acute in limited waters and cramped navigation conditions [2].

2. Aspects of the tasks for ensuring the navigation safety

One of the seven ancient man-made wonders of the world - the Pharos lighthouse, and the miraculous miracle - the Pillars of Hercules were navigational landmarks on the approaches to Alexandria and Gibraltar and helped mariners prevent their ships from aground. And this is one of the proofs that at that time the knowledge, experience and intuition of the navigator was not enough to guarantee the safety of navigation. In modern conditions when the main cause of maritime accidents is breakdown, damage, or equipment failure. The worst regions in terms of maritime accidents, according to the AGCS report, are the waters of southern China, Indonesia, and the Philippines. Every fourth incident occurs in those areas. Even though Asia remains the most unfavorable region due to the busiest routes and the old fleet. Next come the Eastern Mediterranean and the Black Sea and the British Isles. From the analysis of catastrophes, the existing problems of the safety of navigation becomes acute in limited waters and cramped navigation conditions. As a result, special methods of preventing collisions of ships, introduced into complex technical navigation systems, are in great demand [4,5]. The legal framework at this stage, despite the emergence of unmanned navigation, regulates that the management of a ship is the exclusive right of its captain. In his actions, the boat master is only guided by the information provided by various navigation aids, but the final decision on the movement of the vessel is made only by the boat master. And because of this, it has led to the fact that in navigation, extraordinary approaches to traffic management have developed and are used. Because of this, the methods of ensuring the navigation safety of vessel traffic can be divided into three categories: methods of early detection of the collision possibility (collision risk assessment), methods of maneuvering to avoid a collision (collision avoidance), and planning trajectory methods of the safe movement of the vessel. Brief comparative characteristic these methods:

Method 1. On-board radio and computer systems, which are called on-board collision avoidance systems, have been recognized as highly effective means of preventing collisions in shipping. The English name for these complexes is Collision Avoidance System. The on-board collision avoidance system is a proven system based on the use of surveillance radar signals and other navigational aids. It operates independently of ground equipment and provides information on situations that other vessels can create in various navigational conditions. The collision avoidance system provides information to the officer of the watch on the situation in the navigation area through the provision of visual and voice information, ensures the timely detection of threatening vessels, classifies vessels according to their degree of danger, and issues recommendations for the appropriate maneuver. The collision avoidance system monitors vessels in the surrounding water area within a radius of up to 24 miles from own vessel [3]. Such observation makes it possible to determine the trajectory of the relative movement of each oncoming object, to assess the risk of collision of own ship with other objects. With the help of communication facilities, coordination of planned maneuvers can be carried out with other vessels.

Method 2. The problem of divergence of vessels in the water area is a priority in the

management of the vessel. Without disregarding the increasing intensity of traffic on all international water communications, it is possible to ensure a satisfactory level of traffic safety in recent years using innovative means of radio navigation. For this reason, the problem of divergence of ships should be considered only in accordance with the section "Use of automatic radar plotting means".

The main document among the normative ones that determine the reliability of the divergence of ships is the "International rules for preventing collisions of ships at sea" (IRPCSS-72) [6].

These Rules oblige each vessel to carry the appropriate lights and signs, to sound the appropriate sound signals, to use all available means in accordance with the prevailing circumstances and conditions to enable each of them to:

1. To detect in advance the presence of other vessels;
2. To determine the degree of danger in order to identify the existence of a collision hazard;
3. Take into account the mutual obligations when maneuvering the gap;
4. Ensure safe divergence in all visibility conditions.

Method 3. The lack of a quantitative description of the concept of "limited visibility" in the IRPCSS-72 causes a contradiction between R. 19 ("Swimming with limited visibility") and R. 15 ("Situation of intersecting courses in sight of each other") in cases where the visibility range is of the same order of magnitude with D. Having detected in such conditions with the help of the radar an approaching vessel from the right side, a prudent navigator will make way for him, without waiting for this vessel to come within the distance of visual visibility and he will have to act in conditions: the short period of time and minimal space.

In addition, the International Maritime Organization at the United Nations (IMO) in 1978 adopted the Convention on the Training, Certification and Watchkeeping of Seafarers. This Convention defines the minimum requirements for the knowledge and practical skills of boat masters in relation to ship divergence and the use of radar information. IMO has also formulated requirements for programs for radar surveillance, laying and use of automatic radar laying facilities. All this is aimed at increasing the reliability of the divergence of ships.

Method 3. Get answers to the questions: determination of the current coordinates of the vessel in the coordinate system - bearing and distance relative to a given point; determination of the actual trajectory of the vessel's movement, the actual elements of movement, is possible with the help of navigation methods for monitoring the position and movement of the vessel. Evaluation of the trend of the vessel's movement to predict the current coordinates in time, control of the lateral deviation of the vessel from and calculation of the course correction. The listed monitoring tasks are referred to as “Real-time tasks”. The more difficult the navigation conditions are, the shorter the “real time clock” should be. The advantage of each navigation method is determined by the main features of the characteristics: the accuracy of determining the current coordinates of the vessel, the duration of navigation determination and the discreteness of the definitions [7]. Methods of control over the position and movement of the vessel are divided into two groups: "navigational" and "pilotage". With “navigator” control methods based on navigation measurements, the point at which the vessel was located, and depending on the position of this point relative to the line of the given path, solve the remaining navigation problems. The navigational methods include the reckoning of the ship's coordinates, its refinement along one line of position, navigational observations, as well as methods formed by their combinations, including "corrected dead reckoning"

2.1. Security Domains

The area around a ship of a certain radius, shape, and size, not considering geometry, actual dimensions, the current course, into which the oncoming ship should not enter is called the ship's domain. The ship's heading is determined by evaluating the speed vector from radar observations during several turns of the antenna. This definition indicates that the information is not received in real time, but nevertheless this area is called the "navigation safety zone". In methods for assessing the risk of dangerous approach by the foundation, there is a point of the shortest approach of ships (closest point of approach). For navigational safety, the shortest distance is greater than the critical value. The following values are provided: "time of movement to the point of the shortest approach of ships" (time of closest point of approach), "distance to the point of the shortest approach of ships" (distance to closest point of approach).

Research groups that study the issue of ship collision avoidance use a variety of domains: circular, elliptical, and other complex shapes. The domain boundary is interpreted as a function of the ship's heading angle. At this point in time, to use the security domain, each domain is analyzed separately. Based on this, we can conclude that the domain cannot fully solve all the problems of discrepancy due to strictly defined domain boundaries.

The Goodwin domain model is divided into 3 sectors. The dimensions of the free zone from other objects are different. Depends on the situation in a certain period. The radius of the sectors corresponds to the critical values of the closest approach of ships for each scenario Figure 2.

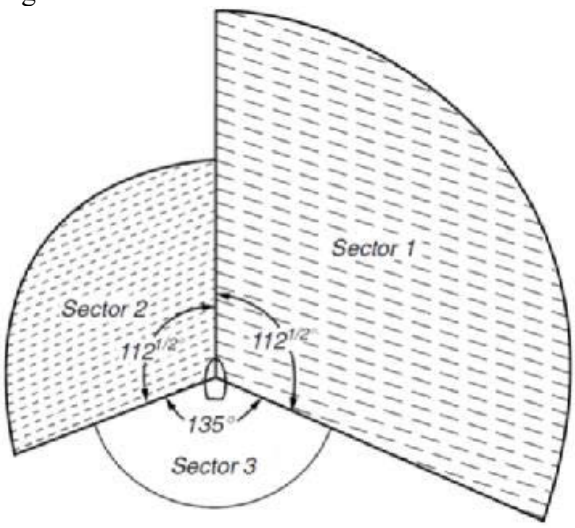


Figure 2: Goodwin domain

Deepening the idea of Goodwin is carried out by the Davis domain, presented in the form of an ellipse with an offset center, divided into sectors. For the navigator, this is an indicator for deciding to perform an evasive maneuver when other objects intrude into the active domain Figure 3.

Caldwell's ship domain is a different configuration depending on the ship's approaching scenario. With oncoming traffic in the domain, the stern part is completely absent. When overtaking, the domain has an ellipsoidal shape.

Tszyu's ship domain is based on neural networks trained by the backpropagation method, which makes it possible to partially consider the influence of the external environment without resorting to complex classical deterministic mathematical models of its description [8].

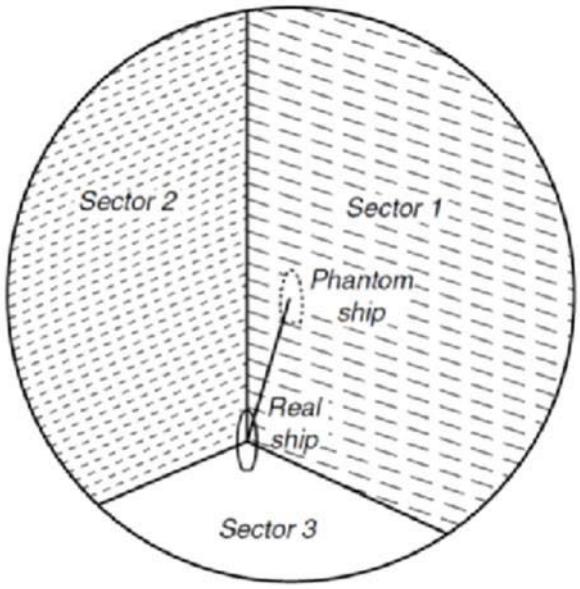


Figure 3: Davis domain

The ship domain proposed by S. V. Smolentsev, A. E. Filyakov considers the navigation features of the navigation area and the hydrometeorological situation. Eliminates the occurrence of false alarms when a vessel enters the safety domain that is moving in the opposite direction in its lane [9]. The position of the security domain boundary is parameterized and depends on the value of one parameter, which is convenient for performing calculations. In addition, the border of the proposed safety zone is smooth, which excludes jumps in solutions for different course angles of entry of targets into this zone [10].

There are groups of our and foreign researchers who are working towards assessing the risk of collision and improving ship domains. An unconventional method for clarifying the situation of approaching ships at sea based on information from an automatic identification system was proposed by Bukaty Vitaly Mikhailovich, Morozova Svetlana Yurievna. Titov A.V., Zaikova S.N., Volynskiy I.A., Khmelnitskaya A.A. in their work the current state and problems of using inland waterways (on the example of the Volga-Caspian Sea shipping canal) and Nitsevich A.A., Melnikov N.V., Khristich D.Yu., Lebedev V.P. in work Collision of ships use the method of M.A. Konoplev, who presents the risk assessment in the form of a fuzzy system.

3. Conclusions

One of the main problems of navigation, namely the navigation safety, remains unresolved,

although the work is carried out by all groups according to the law of a conical spiral.

The article presents a brief overview of methods for ensuring the navigation safety of vessel traffic, which are divided into three categories: methods of early detection of the possibility of collision of ships, methods of maneuvering to avoid a collision and methods of planning the trajectory of the safe movement of the ship. A detailed theoretical review of methods for assessing the risk of a dangerous approach of ships, associated with ensuring the navigation safety of ship traffic, is carried out in detail. To assess the risk of a dangerous approach of ships, the presentation of ship domains of complex figures is given - a dangerous approach of ships.

The work provides links to sources that clarify the presented material.

4. Acknowledgements

We thank the anonymous reviewers for their important and valuable suggestions. We wish to thank V. Kychak, prof., I. Trotsyshyn, prof., O. Punchenko, prof., G. Bortnyk, prof. for their insightful comments on earlier drafts.

We would also like to thank Vinnitsa National Technical University for the application of theoretical and practical research in the R&D "Development of the theory and methodology of digital radio signal processing in real time" (Ministry of Education and Science of Ukraine, Vinnitsa National Technical University);

R&D "Development of methods for designing a fiber-optic transmission system" (Ltd "Budivelnik-3", Vinnitsa National Technical University).

5. References

[1] Punchenko N., Tsyra O., Kazakova N. Conceptualization of the paradigm "integrated technologies as a global trend in the development of shipping safety of an innovative society" /N. Punchenko, O. Tsyra, N., Kazakova. International Journal of 3D Printing Technologies and Digital Industry, pp. 278-284 e-ISSN 2602-3350

[2] Grinyak Viktor Mikhailovich. Development of mathematical models for ensuring the safety of the collective movement of sea vessels: dissertation ... Doctor of Technical Sciences: 05.13.18 / Grinyak Viktor Mikhailovich; [Place of defense: FGBUN Institute of Automation and Control Processes of the Far Eastern Branch of the Russian Academy of Sciences], 2017.- 297 p.

[3] Vagushchenko L.L., Vagushchenko A.L. Support for decisions on disagreement with the courts: Fenix, 2010.- 229 p.

[4] Punchenko N., Korchenko O., Kazakova N., Tsyra O., Warwas K. Cognitive technologies in the profession-al knowledge as a means of the optimizing management decisions XIX International Mul-tidisciplinary Scientific GeoConference SGEM 2019 28 June - 7 July, 2019 Albena, Bulgaria ISSN 1314–2704, doi:10.5593/sgem 2019/2.1 pp. 161-166.

[5] Trotsyshyn, I., Shokotko, G., Strelbitskiy, V. New Technologies and Precision Measuring Transformations Radiosignals and the Perspectives of Use of their use for Systems of Control with safe Literal Appliances (UAVs) (2019) 2018 International Scientific-Practical Conference on Problems of Infocommunications Science and Technology, PIC S and T 2018 – Proceedin, pp. 685-690.

[6] International regulations for preventing collisions at sea, 1972 Moscow 2013 International rules for the prevention of collisions of ships at sea, 1972 (IRPCSS-72). - 5th ed., Rev. - M: Morkniga, 2013.- 156 p., ISBN 978-5-030033-73-0

[7] A. V. Matokhin Application of expert assessments to analysis of risks associated with navigation methods of control of the position and movement of vessels while navigation in confirmed water / Journal: Science of the 21st century: Questions, hypotheses, answers (Taganrog), № 2, 2013, pp. 95-109 ISSN: 2307-5902

[8] Grinyak, V. M. “Review of collision risk assessment methods for vessel traffic systems”. Modern problems of science and education 1-1 (2015) – 171 p.

[9] Fujii, Yahei, and Kenichi Tanaka. “Traffic capacity.” The Journal of navigation 24.4 (1971): pp. 543–552. DOI: 10.1017/S0373463300022384.

[10] Smolentsev S. V. Assessment of the degree of danger of rendezvous based on the dynamic ship security domain / S. V. Smolentsev, A. E. Filyakov // Bulletin of the State University of Marine and River Fleet named after Admiral S. O. Makarov. - 2020. - T. 12. - № 5. - pp. 831–839. DOI: 10.21821 / 2309-5180-2020-12-5-831-839.

Model Of The System For Special Purpose Of Critical Infrastructure Objects

Mikolaj Karpinski [1], Bogdan Tomashevsky[2], Natalia Zahorodna[3], Serhii Yevseiev[4], Stanislaw Rajba [5], Oleksandr Milov[6]

[1,3,5] *University of Bielsko-Biala, Department of Computer Science and Automatics, Willowa Str. 2, Bielsko-Biala, 43-309, Poland*
[2] *Ternopil Ivan Puluj National Technical University, Department of Cyber Security, Ruska str., 56, Ternopil, 46001, Ukraine*
[4,6] *Simon Kuznets Kharkiv National University of Economics, Cybersecurity and Information Systems Department, ave. Science, 9-A, Kharkiv, 61166, Ukraine*

Abstract

The rapid development of computing, mobile and Internet technologies, the digital economy, on the one hand, hybridity and synergy, the development of post-quantum cryptography (the emergence of a full-scale quantum computer), on the other, put forward more stringent requirements for the principles of building special security mechanisms in modern special-purpose systems. Targeted attacks in cyberspace also require a change not only in the principles of building a special communication system for critical infrastructure objects (SCS CIO), the system for communicating commands / control signals to the CIO elements, as well as the creation of fundamentally new approaches to the formation and transmission of commands for their use not only of the SCS equipment, as well as open modern commercial systems based on Internet technologies. This approach allows, in the context of the economic crisis, to ensure the delivery of the signal within a certain time frame in the conditions of modern hybrid cyber threats to the control system through the use of cyberspace infrastructure (synthesis of modern technologies of computer systems and networks, Internet technologies and technologies of mobile communication). The proposed mathematical component of the assessment of the reliability and probability of delivering the corresponding commands / signals allows the proposed model to be used to simulate various interventions into a special-purpose system, both external and internal.

Keywords

modified special purpose system, critical infrastructure, cyberspace, quantum period.

1. Introduction

The modern development of computer technology, the rapid development of cyberspace technologies, the emergence of new hybrid threats and their modification put forward more stringent requirements for special-purpose systems. This is due to the need to bring commands / control signals with a high degree of reliability, safety and efficiency to the elements of the CIO infrastructure in the post-quantum period (the emergence of a full-scale quantum computer). This approach requires not only the formation of programs for the standardization of the information infrastructure of the CIO elements based on international standards and Green Paper approaches, but also the ability to counter modern threats with signs of hybridity and synergy.

1.1. Analysis of recent research and publications

[1-8] determines the need to create a special-purpose system for critical infrastructure

EMAIL: mkarpinski@ath.bielsko.pl (A. 1); bogdan_tomashevsky@tntu.edu.ua (A. 2); zagorodna.n@gmail.com (A. 3); Serhii.Yevseiev@hneu.net (A. 4); srajba@ath.bielsko.pl (A. 5); Oleksandr.Milov@hneu.net (A. 6)
ORCID: 0000-0002-8846-332X (A. 1); 0000-0002-1934-4773 (A. 2); 0000-0003-1647-6444 (A. 4); 0000-0001-9291-8879 (A. 5); 0000-0001-6135-2120 (A. 6);

facilities, which makes it possible to form a control system in the conditions of post-quantum cryptography, the growing demands of cyber terrorists, targeted cyberattacks on communication channels and elements of the CIO. In [7], it is predicted that by 2025, 2.8 billion subscribers will use the 5G network. By the same year, the share of fixed wireless access networks in global traffic will increase to 25%, reaching 160,000,000 connections. According to research [9], today more than 5,000,000,000 consumers interact with data every day − by 2025 this number will be 6,000,000,000, or 75% of the world's population. In 2025, every connected person will have at least one data access every 18 seconds. Many of these interactions are driven by the billions of IoT devices connected around the world, which are expected to generate over 90 ZB (10^{21} bytes) of data in 2025. This indicates the possibility of considering the use of these systems as possible channels of a modified special-purpose system, subject to additional information transformation. However, in [2-5], US experts note the possibility of breaking symmetric and asymmetric cryptosystems that provide security in cyberspace as a combination of Internet technologies, computer systems and networks, as well as LTE (Long-Term Evolution − long-term development) technologies in the context of the emergence full-scale quantum computer (post-quantum period).

1.2. The purpose and objectives of the study

The aim of the research is to develop a model of a promising special-purpose system for critical infrastructure facilities.

To achieve the goal of the reserch, it is necessary to solve the following tasks:

− development of a mathematical model of a promising special-purpose system CIO;

− mathematical assessment of the probability of delivering a message using a special-purpose system CIO;

− mathematical assessment of the reliability of the proof of the message using the special-purpose system CIO.

2. Development of a mathematical model of a promising special-purpose system.

To ensure the safety, reliability and efficiency of the transmission of commands and / or control signals, a national system of confidential communication is used.

The national confidential communication system is a set of special dual-use communication systems (networks) that, using cryptographic and / or technical means, ensure the exchange of confidential information in the interests of state authorities and local governments, create appropriate conditions for their interaction in peacetime and in in the case of the introduction of a special and martial law [1, 6].

A special communication system (network) is a communication system (network) intended for the exchange of information under limited access. A special dual-purpose communication system (network) is a special communication system (network) designed to provide communication in the interests of state authorities and local authorities, using part of its resource to provide services to other consumers. The subjects of the National System of Confidential Communication are state authorities and local self-government bodies, legal entities and individuals who take part in the creation, functioning, development and use of this system. Management of the National System of Confidential Communications, its functioning, development, use and protection of information are provided by a specially authorized central executive body in the field of confidential communications in accordance with the legislation. Centralized systems of information protection and operational and technical management are state-owned and are not subject to privatization. The owners of other components of the National System of Confidential Communications may be subjects of economic activity, regardless of the form of ownership. The main feature of such systems is its hierarchical structure and transmission method based on forward error correction. This approach requires the transmission of additional ("unnecessary" − checking) characters, greatly simplifies the detection-suppression and / or complete blocking of these communication channels for the adversary.

However, the rapid development of computing resources for both Internet and mobile technologies LTE (Long-Term Evolution) allows the use, given the "steganographic" properties of these communication channels. The "steganographic" property is understood as the possibility of hiding from the attacker the fact, place, time and content of information transmitted

by breaking the commands and / or control signals of the OCI into separate blocks (packets). This approach allows the use of open communication channels with a commercial method of delivering information to the recipient − the decisive feedback. In addition, the use of this approach does not require significant economic and human resources. Consider the model of a modified CIO control system on the example of the Armed Forces of Ukraine. In the system that is proposed to be used as a projects of the National Confidential Communication System: special communication systems (networks) as well as systems of open public Internet systems and mobile communication systems based on "G" technologies. In this system, the switching nodes are denoted by: ch_i^{scsGF} (special communication systems of the Ground Forces), $i \in \overline{1,\dots I}$,, ch_j^{scsAF} (special communication systems of the Air Force), $j \in \overline{1,\dots J}$, ch_l^{scsNF} (special communication systems of the Naval Forces), $l \in \overline{1,\dots L}$, special dual-purpose system ch_k^{sdpsD} (special dual-use system), $k \in \overline{1,\dots K}$, open Internet system ch_m^{oIS} $m \in \overline{1,\dots M}$, open mobile communication system ch_q^{omcs} (open mobile communication system) $q \in \overline{1,\dots Q}$. Communication channels are denoted accordingly: l_{ix}^{scsGF}, $x \in \overline{1,\dots X}$, l_{jy}^{scsAF}, $y \in \overline{1,\dots Y}$, l_{lz}^{scsNF}, $z \in \overline{1,\dots Z}$, special dual-purpose system l_{kf}^{sdpsD} ,, $f \in \overline{1,\dots F}$, open Internet system l_{mv}^{oIS} ,, $v \in \overline{1,\dots V}$, open mobile communication system l_{qn}^{omcs} ,, $n \in \overline{1,\dots N}$.

Thus, the overall system of the proposed special purpose control system CIO will be a set of individual components of the intermediate switching nodes and channels, and the total probability of receiving a command and / or signal is determined by the formula:

$$P_{cr}^{Q^{ACCS}} = \left(\sum_{i=1}^{I} p_i^{scsGF} ch_i^{scsGF} \times \sum_{ix=1}^{X} p_{ix}^{scsGF} l_{ix}^{scsGF} \right) \cup$$
$$\cup \left(\sum_{j=1}^{J} p_j^{scsAF} ch_j^{scsAF} \times \sum_{jy=1}^{Y} p_{jy}^{scsAF} l_{jy}^{scsAF} \right) \cup$$
$$\cup \left(\sum_{l=1}^{L} p_l^{scsNF} ch_l^{scsNF} \times \sum_{lz=1}^{L} p_{lz}^{scsNF} l_{lz}^{scsNF} \right) \cup$$
$$\cup \left(\sum_{k=1}^{K} p_k^{sdpsD} ch_k^{sdpsD} \times \sum_{kf=1}^{F} p_{kf}^{sdpsD} l_{kf}^{sdpsD} \right) \cup$$
$$\cup \left(\sum_{m=1}^{M} p_m^{oIS} ch_m^{oIS} \times \sum_{mv=1}^{V} p_{mv}^{oIS} l_{mv}^{oIS} \right) \cup$$
$$\cup \sum_{q=1}^{Q} p_q^{omcs} ch_q^{omcs} \times \sum_{qn=1}^{N} p_{qn}^{omcs} l_{qn}^{omcs}.$$

where:

p_i^{scsGF} − the probability of correct reception / transmission of the i-th switching node ch_i^{scsGF};

p_{ix}^{scsGF} − the probability of correct transmission from the i-th switching node ch_i^{scsGF} through the x-th channel l_{ix}^{scsGF};

p_j^{scsAF} − the probability of correct reception / transmission of the j-th switching node ch_j^{scsAF};

p_{jy}^{scsAF} − the probability of correct transmission from the j-th switching node ch_j^{scsAF} through the y-th channel l_{jy}^{scsAF};

p_l^{scsNF} - the probability of correct reception / transmission of the l-th switching node ch_l^{scsNF};

p_{lz}^{scsNF} - the probability of correct transmission from the l-th switching node ch_l^{scsNF} through the z-th channel l_{lz}^{scsNF};

p_k^{sdpsD} − the probability of correct reception / transmission of the k-th switching node ch_k^{sdpsD};

p_{kf}^{sdpsD} − the probability of correct transmission from the k-th switching node ch_k^{sdpsD} through the f-th channel l_{kf}^{sdpsD};

p_m^{oIS} - the probability of correct reception / transmission of the m-th switching node ch_m^{oIS};

p_{mv}^{oIS} - the probability of correct transmission from the m-th switching node ch_m^{oIS} through the v-th channel l_{mv}^{oIS};

p_q^{omcs} - the probability of correct reception / transmission of the q-th switching node ch_q^{omcs};

p_{qn}^{omcs} - the probability of correct transmission from the q-th switching node ch_q^{omcs} through the n-th channel l_{qn}^{omcs}.

3. Mathematical assessment of the probability of delivering a message using a special-purpose control system for the OQI

Taking into account the possibility of modern cyber threats, the computing capabilities of cyber terrorists in the special-purpose control system of the CIO, it is proposed to transmit commands and / or control signals by separate independent units through all channels, both a special confidential communication system and over open networks. Commands are transmitted in parallel. Each of the networks can be subject to attacks of a different nature, which lead to the failure of the corresponding network. We calculate the probability of delivery of a message that is transmitted (hereinafter, a packet), with the parallel operation of three networks (a special communication system (network) of the aircraft, an open Internet network, an open mobile network), provided that there is a majority body on the receiving side that makes decisions and the correctness of information transmission in the case of identity of at least two packets.

Let the probability of command transmission without distortion and failure for a special system (network) of communication – $P_{cr}^{Q^{SCS}}$, second network – $P_{cr}^{Q^{oIS}}$, third network – $P_{cr}^{Q^{omcs}}$, ie packet transmission without failures and losses, which can be caused by attacks of different classes. If there was no majority body on the host side, the probability of receiving a package on at least one of the networks could be calculated as follows:

$$P_{cr}^{Q^{ACCS}} = P_{cr}^{Q^{oIS}} + P_{cr}^{Q^{oIS}} + P_{cr}^{Q^{omcs}} = \\ = \left(1 - P_{err}^{Q^{SCS}}\right) \times \left(1 - P_{err}^{Q^{oIS}}\right) \times \left(1 - P_{err}^{Q^{omcs}}\right),$$

where

$P_{err}^{Q^{SCS}}$ - the probability of erroneous reception of the command in a special system (network) of communication; $P_{err}^{Q^{oIS}}$ – the probability of erroneous reception of the command on the Internet; $P_{err}^{Q^{omcs}}$ – the probability of erroneous reception of the command in the mobile network.

This expression can be interpreted as the value of the probability that all three networks will not fail simultaneously.

If there is a majority body on the receiving party to the calculation of the probability of receipt and confirmation of the correctness of the received package must be approached in a slightly different way.

Consider all possible states of the three listed networks. All sets of states are summarized in table. 1.

Table 1

Possible states of the three command transmission networks

№ situations	Network status			Probability of implementation
	$P_{err}^{Q^{SCS}}$	$P_{err}^{Q^{oIS}}$	$P_{err}^{Q^{omcs}}$	
1	+	+	+	$P_{cr}^{Q^{ACCS}} = P_{cr}^{Q^{SCS}} \times P_{cr}^{Q^{oIS}} \times P_{cr}^{Q^{omcs}}$
2	+	+	-	$P_{cr}^{Q^{ACCS}} = P_{cr}^{Q^{SCS}} \times P_{cr}^{Q^{oIS}} \times \left(1 - P_{cr}^{Q^{SCS}}\right)$
3	+	-	+	$P_{cr}^{Q^{ACCS}} = P_{cr}^{Q^{SCS}} \times \left(1 - P_{cr}^{Q^{oIS}}\right) \times P_{cr}^{Q^{omcs}}$
4	-	+	+	$P_{cr}^{Q^{ACCS}} = \left(1 - P_{cr}^{Q^{SCS}}\right) \times P_{cr}^{Q^{oIS}} \times P_{cr}^{Q^{omcs}}$
5	+	-	-	$P_{cr}^{Q^{ACCS}} = P_{cr}^{Q^{SCS}} \times \left(1 - P_{cr}^{Q^{oIS}}\right) \times \left(1 - P_{cr}^{Q^{omcs}}\right)$
6	-	+	-	$P_{cr}^{Q^{ACCS}} = \left(1 - P_{cr}^{Q^{SCS}}\right) \times P_{cr}^{Q^{oIS}} \times \left(1 - P_{cr}^{Q^{omcs}}\right)$
7	-	-	+	$P_{cr}^{Q^{ACCS}} = \left(1 - P_{cr}^{Q^{SCS}}\right) \times \left(1 - P_{cr}^{Q^{oIS}}\right) \times P_{cr}^{Q^{omcs}}$
8	-	-	-	$P_{cr}^{Q^{ACCS}} = \left(1 - P_{cr}^{Q^{SCS}}\right) \times \left(1 - P_{cr}^{Q^{oIS}}\right) \times \left(1 - P_{cr}^{Q^{omcs}}\right)$

The "+" sign indicates that the packet was transmitted successfully, and the "-" sign indicates that due to various reasons (attacks, physical damage, technical failures, etc.), the packets were not delivered, or the packet came with distortions. The first four situations correspond to cases where the majority body can confirm that 2 of the 3 packets are identical, and can be interpreted as a correctly transmitted command. In other cases, the majority body cannot confirm the identity of the received packets on at least 2 networks. The probabilities of realization of the corresponding situations are given in the last column of table. 1.

Then the probability of receiving identical packages on at least 2 networks, which allows the majority body to work, will be equal to the sum of the probabilities of the first four situations:

$$P_{cr}^{Q^{ACCS}} = P_{cr}^{Q^{SCS}} \times P_{cr}^{Q^{olS}} \times P_{cr}^{Q^{omcs}} + \\ + P_{cr}^{Q^{SCS}} \times P_{cr}^{Q^{olS}} \times \left(1 - P_{cr}^{Q^{omcs}}\right) + \\ + P_{cr}^{Q^{SCS}} \times P_{cr}^{Q^{omcs}} \times \left(1 - P_{cr}^{Q^{olS}}\right) + \\ + P_{cr}^{Q^{olS}} \times P_{cr}^{Q^{omcs}} \times \left(1 - P_{cr}^{Q^{SCS}}\right)$$

However, when using a special network, it is possible to detect and correct any number of errors based on decoding algorithms. The payment for reliability and efficiency is the additional transmission of redundant (check) characters, which greatly simplifies the execution of a DOS0 attack by a cyber attacker.

4. Mathematical assessment of the control signal reliability using a special-purpose system.

A detailed study of the statistical properties of error sequences in real communication channels [10, 11] showed that errors are dependent and tend to group (package), ie there is a certain relationship between them − correlation. Most of the time the information passes through communication channels without distortion, and at certain points in time there are condensations of errors, so-called packets (packs, groups) of errors, within which the error probability is much higher than the average error probability calculated for a significant transmission time. In such conditions, the protection methods that are optimal for the hypothesis of independent errors are ineffective when used in real communication channels. HF radio channels and wired data transmission channels used for the organization of control and communication in a special system (network) of communication of the Armed Forces, prone to a significant grouping of errors with a slight mean asymmetry. Then, with the group nature of the error distribution, one parameter (error probability) does not fully characterize the channel, additional parameters are needed that reflect the degree of error grouping in different data transmission channels.

To calculate the reliability of command transmission in a special system (network) of communication of the Armed Forces, we use a simplified mathematical model of Bennett-Freulich, which does not impose restrictions on the type of law of distribution of error packet lengths [10, 11]. The advantages of the simplified Bennett – Freulich model include relatively low computational complexity, a small number of parameters, high accuracy compared to the Gilbert model, and the possibility of arbitrary choice of the nature of the distribution of error packet lengths. To set a simplified Bennett – Freulich model, it suffices to set the probability P_n − the probability that from this position will begin a continuous package of errors of any length and distribution, $P(l)$ − the probability of a continuous package of length l. Then $P_n(l)$ − the probability that from this position will start a continuous packet of errors of length l is equal to:

$$P_n(l) = P_n \times P(l).$$

Consider a simplified Bennet-Freulich model with disparate bundles of errors and their possible adjacency. In this case, no more than n characters can occur on a block length

$$\lambda' = \left\lfloor \frac{n}{l} \right\rfloor$$

blocks of length errors l.

Then the probability of correct receiving of commands and / or signals in a special communication system (network) of the Armed Forces is determined by the formula:

$$P_{cr}^{Q^{SCS}} = 1 - (1 - P_{err}^{Q^{SCS}})^n - \sum_{\xi=1}^{\lambda'} C_n^{\xi} \cdot P_{err}^{\xi} \cdot \left(1 - P_{err}^{Q^{SCS}}\right)^{n-\xi} = \\ = 1 - \sum_{\xi=0}^{\lambda'} C_n^{\xi} \cdot P_{err}^{\xi} \cdot \left(1 - P_{err}^{Q^{SCS}}\right)^{n-\xi}.$$

where ξ − number of packet combinations, n − packet length.

To calculate the probability of correct reception of commands on the Internet, we also

use a simplified Bennet-Freulich model. One of the modifications of the Bennett-Freulich model, which provides a polygeometric distribution of the lengths of error packets considered in[10, 11].

In [11] it was shown that the lengths of error packets in most real channels are distributed according to the normal law. Thus, instead of the packet length distribution function F (ln), it is sufficient to specify the mathematical expectation mln and the standard deviation σln. The length of the interval between the beginnings of neighboring error packets Λ is a discrete random variable (DRV). We construct a series of DRV distributions and find the DVV distribution function Λ. The range of distribution of DRV Λ is shown in table. 2.

Table 2

A series of distributions of a discrete random length of the interval between the start of error bursts Λ

Λ	0	1	2	…	i	…
$P\{\Lambda = \lambda\}$	P_b	$P_b\,(1 - P_b)$	$P_b\,(1 - P_b)\,2$	…	$P_b\,(1 - P_b)$ i	…

where P_b is the probability of an error packet.

DRV distribution function Λ

$$F_\Lambda(\lambda) = P\{\Lambda < \lambda\} = \sum_{i=0}^{\lambda-1} P(\lambda) =$$
$$= P_b\left(1 + (1-P_b) + (1-P_b)^2 + ...(1-P_b)^{\lambda-1}\right) =$$
$$= P_b \times \frac{1-(1-P_b)^\lambda}{1-(1-P_b)} = P_n \times \frac{1-(1-P_b)^\lambda}{P_b} = 1-(1-P_b)^\lambda.$$

The error burst length L_n is also a random variable. It is distributed according to the normal distribution law with the parameters m_{ln} and σ_{ln}, and in the general case can take values from 0 to ∞.

Let's introduce into consideration a random variable A equal to the difference between Λ and L_n

$$A = \Lambda - L_n.$$

Random variable A can take values from 0 to ∞. A is the length of the i-th error-free interval (Fig. 1).

The probability of correct transmission of an n-bit data block can be defined as the probability of a random event, random variable A takes on a value greater than or equal to n, that is

$$P_{cor} = \mathrm{P}\{\mathrm{A} \ge \mathrm{n}\} = 1 - \mathrm{P}\{\mathrm{A} < \mathrm{n}\} = 1 - F_A(n),$$

where $F_A(n)$ is the distribution function of the random variable A from the argument n.

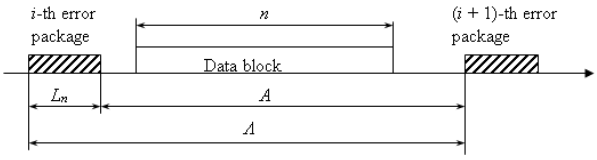


Figure 1: Explanation of the meaning of the random variable A

A random event B, which is that random value A will take a value less than n, can be represented as the sum of incompatible events:

B_0 − a random event, which is that Λ <n and 0≤L_n <1;

B_1 − a random event, which is that Λ <n + 1 and 1≤ L_n <2;

B_2 − a random event, which is that Λ <n + 2 and 2≤ L_n <3;

…

V_i − a random event, which is that Λ <n + i and i≤L_n <i + 1.

The random variables Λ and Ln are independent. Then the probabilities of these events are equal

$$P(B_0) = P\{(\Lambda < n) \bigcap (0 \le L_\text{n} < 1)\} =$$
$$= P\{\Lambda < n\} \times P\{0 \le L_\text{n} < 1\};$$
$$P(B_1) = P\{(\Lambda < n+1) \bigcap (1 \le L_\text{n} < 2)\} =$$
$$= P\{\Lambda < n+1\} \times P\{1 \le L_\text{n} < 2\};$$
$$P(B_2) = P\{(\Lambda < n+2) \bigcap (2 \le L_\text{n} < 3)\} =$$
$$= P\{\Lambda < n+2\} \times P\{2 \le L_\text{n} < 3\};$$
$$\dots$$
$$P(B_i) = P\{(\Lambda < n+i) \bigcap (i \le L_\text{n} < i+1)\} =$$
$$= P\{\Lambda < n+i\} \times P\{i \le L_\text{n} < i+1\};$$
$$\dots$$

Since the events B_0, B_1, B_2,…, B_i,… incompatible, then

$$\mathrm{P}\{\mathrm{A} < \mathrm{n}\} = P(B) = \sum_{i=0}^{\infty} P(B_i) =$$
$$= \sum_{i=0}^{\infty} \left[P\{\Lambda < n+i\} \cdot P\{i \le L_\text{n} < i+1\}\right].$$

The probability P{Λ <n + i} is nothing but the distribution function random variables Λ from the argument n + i

$$\mathrm{P}\{\Lambda < \mathrm{n} + \mathrm{i}\} = F_\Lambda(n+i) = 1 - (1 - P_\text{п})^{n+i}.$$

In order to find the probability that the value of random variables L_n, distributed by the normal law with the parameters m_{Ln} and σ_{Ln}, falls in the interval [i, i + 1), we use the known formula

$$P\{i \le L_{\text{п}} < i+1\} = \Phi\left(\frac{i+1-m_{l_n}}{\sigma_{l_n}}\right) - \Phi\left(\frac{i-m_{l_n}}{\sigma_{l_n}}\right),$$

where $\Phi(x)$ is the Laplace function of the argument x.

Substituting (2), (3) into (1), we obtain the distribution function BB BB

$$\mathrm{F_A(n)} = \mathrm{P}\{\mathrm{A} < n\} =$$

$$= \sum_{i=0}^{\infty}\left\{\left[1-(1-P_n)^{n+i}\right]\cdot\left[\Phi\left(\frac{i+1-m_{l_n}}{\sigma_{l_n}}\right) - \Phi\left(\frac{i-m_{l_n}}{\sigma_{l_n}}\right)\right]\right\}.$$

Then the formula for calculating the probability of correct transmission of a data block of length n bits takes the form

$$P_{cor} = 1 - F_A(n) = 1 -$$

$$-\sum_{i=0}^{\infty}\left\{\left[1-(1-P_{\text{п}})^{n+i}\right]\cdot\left[\Phi\left(\frac{i+1-m_{l_n}}{\sigma_{l_n}}\right) - \Phi\left(\frac{i-m_{l_n}}{\sigma_{l_n}}\right)\right]\right\}.$$

Thus, for an open Internet with crucial feedback and a positive receipt, the probability of receiving the correct commands is determined by the formula:

$$P_{cr}^{Q^{olS}} = 1 - \sum_{i=0}^{\infty}\left\{\left[1-(1-P_n)^{n+i}\right]\cdot\left[\Phi\left(\frac{i+1-m_{l_n}}{\sigma_{l_n}}\right) - \Phi\left(\frac{i-m_{l_n}}{\sigma_{l_n}}\right)\right]\right\}\times$$

$$\times\frac{1-\sum_{i=0}^{\infty}\left\{\left[1-(1-P_n)^{n+i}\right]\cdot\left[\Phi\left(\frac{i+1-m_{l_n}}{\sigma_{l_n}}\right) - \Phi\left(\frac{i-m_{l_n}}{\sigma_{l_n}}\right)\right]\right\}\cdot\left\{1-\frac{1}{2^r}\cdot\left[\frac{1}{2}-\Phi\left(\frac{r+1-m_{l_n}}{\sigma_{l_n}}\right)\right]\right\}^N}{1-\sum_{i=0}^{\infty}\left\{\left[1-(1-P_n)^{n+i}\right]\cdot\left[\Phi\left(\frac{i+1-m_{l_n}}{\sigma_{l_n}}\right) - \Phi\left(\frac{i-m_{l_n}}{\sigma_{l_n}}\right)\right]\right\}\cdot\left\{1-\frac{1}{2^r}\cdot\left[\frac{1}{2}-\Phi\left(\frac{r+1-m_{l_n}}{\sigma_{l_n}}\right)\right]\right\}},$$

where n – length of i-th frame, P_n − probability of burst errors; m_{Ln} − mathematical expectation of packet length in errors; σ_{Ln} -standard deviation of length packet of errors, N is the maximum number of repetitions determined by the formula, which is determined by by the formula:

$$N \ge \left\lceil \frac{\ln\left(1-\frac{P_{nec}\cdot\left(1-P_{I\,ae}\right)}{P_{I\,ct}}\right)}{\ln P_{I\,ae}} \right\rceil,$$

where

P_{nec} − necessary probability delivery packagein;

P_{Iae} − the probability of an error in the package;

P_{Ict} − probability right packet transmission with one attempts;

$\lceil x \rceil$ − the nearest integer greater than or equal to x.

In cellular networks for determination of signal strength and interference at the input of the receiver of the subscriber terminal for prediction of losses when signal propagation is used model Okamura-Cottage. In accordance with this model, the signal power at the input of the receiver $\mathrm{P_{ave}}$ subscriber station, which is at a distance R from the transmitter,is equal to

$$P_{cr}^{Q^{omcs}}(R) = P_{rad}(\Theta)\times L(R),$$

where $P_{rad}(\Theta)$ − which emits the power of the transmitter depending on the direction to the subscriber station; at this is expectedthat the antenna of the subscriber station has a pie chart; $L(R)$ − losses (size, reverse attenuation) signal at distribution in urban areas,, depends from altitude, antennas which transmit and accept, distance between them,, carrier frequencies, empirical coefficient.

Power signal on during receiver back proportional distance to transmitter:

$$P_{cr}^{Q^{omcs}}(R) = \frac{P_{rad}(\Theta)}{B\times R^x},$$

where B − coefficient, calculated empirically and depends from altitude, transmitting and reception antennas -h_{BS}, carrier frequencies; x -indicator degree at R:

$$x = 4.49\text{-}0.655\lg(h_{\mathrm{BS}}).$$

Power interference obstacles,, created six interfering transmitters the first hexagon,, is equal to

$$P_{n1} = 6\frac{P_{rad}(\Theta)}{B\times(R_3)^x}\times\frac{1}{\left(\sqrt{27}\right)^x}$$

Formula power interference obstacles,, created six interfering transmitters another hexagon:

$$P_{n1} = 6\frac{P_{rad}(\Theta)}{B\times(R_3)^x}\times\frac{1}{9^x},$$

the third hexagon:

$$P_{n1} = 6\frac{P_{rad}(\Theta)}{B\times(R_3)^x}\times\frac{1}{(108)^x}$$

At work in cellular network appear interference from transmitters base stationsthat work on matching frequencies (in adjacent channels), and in results on during receiver necessary consider relation signal/ (noise + interference obstacle):

$$h_{\sum} = \frac{P_s}{P_{noise} + P_{obs\sum}}$$

The probability of non-compliance with the requirements for permissible relation signal/obstacle (S/OBS) in point reception P(C) depends from dimensionality cluster. Probability *P(C)* decreases with growth dimensionality cluster. At this simultaneously falls frequency efficiency network. Evaluated different options clusters and absorbs optimal. Results evaluation different options clusters for standard GSM-900 bent in table. 2.

Table 3

Evaluation of clusters for the GSM-900 network

Dimensionality cluster C	Parameters	Sectorality M								
		1			3			6		
3	*P*(C), %	-	-	-	6.2	21.8	29.5	0.4	6.6	14.5
4	*P*(C), %	39	49.6	-	2.3	14.7	23.6	0.3	4.3	11.5
7	*P*(C), %	6.4	25.8	35	0.2	6.4	15.2	0.01	1.7	6.8

Thus, for a mobile network based on LTE technologies, the probability of correct command reception is determined by the formula:

$$P_{cr.}^{Q^{ACCS}} = P_{cr}^{Q^{SCS}} + P_{cr}^{Q^{omcs}} + P_{cr}^{Q^{olS}} = \left(1 - \sum_{\xi=0}^{\lambda'} C_n^{\xi} \cdot P_{noM}^{\xi} \cdot \left(1 - P_{obs}^{Q^{SCS}}\right)^{n-\xi}\right) \times \left(1 - h_{\sum} = \frac{P_s}{P_{noise} + P_{obs\sum}}\right) \times$$

$$\times \left(1 - \sum_{i=0}^{\infty} \left\{ \left[1 - (1 - P_n)^{n+i}\right] \cdot \left[\Phi\left(\frac{i+1-m_{l_n}}{\sigma_{l_n}}\right) - \Phi\left(\frac{i-m_{l_n}}{\sigma_{l_n}}\right) \right] \right\} \times \right.$$

$$\left. \times \frac{1 - \sum_{i=0}^{\infty} \left\{ \left[1 - (1 - P_n)^{n+i}\right] \cdot \left[\Phi\left(\frac{i+1-m_{l_n}}{\sigma_{l_n}}\right) - \Phi\left(\frac{i-m_{l_n}}{\sigma_{l_n}}\right) \right] \right\} \cdot \left\{ 1 - \frac{1}{2^r} \cdot \left[\frac{1}{2} - \Phi\left(\frac{r+1-m_{l_n}}{\sigma_{l_n}}\right) \right] \right\}^N}{1 - \sum_{i=0}^{\infty} \left\{ \left[1 - (1 - P_n)^{n+i}\right] \cdot \left[\Phi\left(\frac{i+1-m_{l_n}}{\sigma_{l_n}}\right) - \Phi\left(\frac{i-m_{l_n}}{\sigma_{l_n}}\right) \right] \right\} \cdot \left\{ 1 - \frac{1}{2^r} \cdot \left[\frac{1}{2} - \Phi\left(\frac{r+1-m_{l_n}}{\sigma_{l_n}}\right) \right] \right\}} \right).$$

5. Conclusions

1. The analysis of the existing special-purpose model in the control systems of critical infrastructure facilities does not allow the transmission of control signals / commands to the elements of the AQI infrastructure with the required level of reliability in the context of modern targeted cyber threats requires new approaches and the use of all possible channels for communicating combat orders.

$$P_{cr}^{Q^{omcs}} = 1 - h_{\sum} = \frac{P_s}{P_{noise} + P_{obs\sum}}.$$

Then the probability of correct reception in the proposed modified special-purpose system is equal to:

2. The proposed model of a promising special-purpose system for managing objects of OKI uses both a system of special communication equipment and open commercial systems of cyberspace. When transmitting, it is proposed that each message is split into separate components, which are transmitted over all channels. In open channels, it is proposed to use digital steganography and / or unprofitable cryptography methods. Interception in each channel of individual components will not allow the enemy to get the original text. The final recipient (an element of the OCI infrastructure), on the basis of majority choice from all channels in all parts of

the message, receives a command / control signal. This approach allows, in the context of the economic crisis, to ensure the fulfillment of the assigned tasks on time,

3. The mathematical component of assessing the reliability and probability of delivering the corresponding commands / signals allows modeling the proposed model taking into account various interventions into the special-purpose system of critical infrastructure objects, both external and internal. A promising area of further research is the formation of mechanisms for breaking into parts and concealment during transmission over open channels.

6. References

[1] Hrishchuk R. V., and Danyk Yu. G. Fundamentals of cyber security: Monograph (ed. Dannik Yu. G.). Zhytomyr: ZhNAEU, 2016.

[2] Lily Chen et. al. Report on Post-Quantum Cryptography. National Institute of Standards and Technology Internal Report 8105. National Institute of Standards and Technology, Gaithersburg, Maryland, April 2016, 15pp. http://nvlpubs.nist.gov/nistpubs/ir/2016/NIST.IR.8105.pdf

[3] Ankur Lohachab, Anu Lohachab, Ajay Jangra. A comprehensive survey of prominent cryptographic aspects for securing communication in post-quantum IoT networks. Internet of Things, Vol. 9, March 2020, 100174. https://doi.org/10.1016/j.iot.2020.100174.

[4] Kyrylo Petrenko, Atefeh Mashatan, Farid Shirazi. Assessing the quantum-resistant cryptographic agility of routing and switching IT network infrastructure in a large-size financial organization. Journal of Information Security and Applications, Volume 46, 2019, Pages 151-163. https://doi.org/10.1016/j.jisa.2019.03.007.

[5] Jeffrey Cichonski, Joshua M. Franklin, Michael Bartock. Guide to LTE Security. NIST Special Publication 800-187. National Institute of Standards and Technology, December 2017. 49pp. https://doi.org/10.6028/NIST.SP.800-187.

[6] G. P. Leonenko, and A. Yu. Yudin, “Problems of ensuring information security of systems of critical information infrastructure of Ukraine”, Information Technology and Security, № 1 (3), s. 44 − 48. 2013.

[7] Ericsson Mobility Report: 5G is growing faster than forecasted. https://softline.ua/ua/news/ericsson-mobility-report-5g-zrostaie-shvydshe-za-prohnozy.html

[8] Experts predict "the onset of smart attachments". https://www.ukrinform.ua/rubric-technology/2444363-eksperti-prognozuut-nastup-smartpristroiv.html

[9] IDC "The Digitization of the World − From Edge to Core". https://www.seagate.com/gb/en/our-story/data-age-2025/

[10] Sklar Bernard. Digital communication. Fundamentals and Applications. Prentice Hall, 2012. 954pp.

[11] Fink L.M. The theory of transmission of discrete messages. Moscow, Publishing house "Soviet Radio", 1970. 728pp.

Detection Of Intrusion Attacks Using Neural Networks

Mikolaj Karpinski[1], Alexander Shmatko [2], Serhii Yevseiev[3], Daniel Jancarczyk[4] and Stanislav Milevskyi[5]

[1,4] *University of Bielsko-Biala, Department of Computer Science and Automatics, Willowa Str. 2, Bielsko-Biala, 43-309, Poland*
[2,3,5] *Simon Kuznets Kharkiv National University of Economics, Cybersecurity and Information Systems Department, ave. Science, 9-A, Kharkiv, 61166, Ukraine*

Abstract
The rapid expansion of computer networks makes security issues among computer systems one of the most important. Intrusion detection systems are using artificial intelligence more and more. This article discusses intrusion detection. Multi-layer perceptron (MLP) is used to detect offline intrusion attacks. The work uses the issues of determining the type of attack. Various neural network structures are considered to detect the optimal neural network by the number of input neurons and the number of hidden layers. It has also been investigated that activation functions and their influence on increasing the ability to generalize a neural network. The results show that the neural network is a 15x31x1 way to classify records with an accuracy of about 99% for known types of attacks, with an accuracy of 97% for normal vectors and 34% for unknown types of attacks.

Keywords
detection of anomalies, expert systems, neural networks, intrusion detection system, network attacks.

1. Introduction

Currently, information technology has penetrated practically all spheres of life of modern society. And an integral part of information technology is the Internet. The reason for such an intensive development of information technology is the growing need for quick and high-quality processing of information, the instantaneous transmission of information to various parts of the world. In this regard, one of the main tasks is to ensure the security of information that is transmitted or processed on the network, protection against network attacks.

At the moment, complex information security systems are becoming increasingly important. As components of such system act as antivirus protection systems, integrity monitoring systems, firewalls, vulnerability analysis, detection and prevention systems, etc. Intrusion Detection and Intrusion Detection Systems, or, as they are called, the means of detecting attacks, is precisely this mechanism of protection of the network, which is assigned the functions of protection against network attacks.

There is a large number of methods for detecting network attacks, but as attacks constantly change special databases with rules or signatures to detect attacks requiring continuous administration, there is a need to add new rules. One of the ways to eliminate this problem is to use the neural network as a mechanism for detecting network attacks. Unlike the signature approach, the neural network performs an analysis of information and provides information about the attacks that it is trained to recognize. In addition, neural networks have the advantage - they are able to adapt to previously unknown attacks and detect them [1-3].

EMAIL: mkarpinski@ath.bielsko.pl (A.1),
asu.spios@gmail.com, (A.2), Serhii.Yevseiev@hneu.net, (A.3),
djancarczyk@ath.bielsko.pl (A.4),
Stanislav.Milevskiy@hneu.net (A.5)
ORCID: 0000-0002-8846-332X (A.1), 0000-0002-2426-900X (A.2), 0000-0003-1647-6444 (A.3), 0000-0003-4370-7965 (A.4), 0000-0001-5087-7036 (A.5)

2. Analysis of existing methods for intrusions detecting

Detecting network attacks is a process of recognizing and responding to suspicious activity directed to the network or computing resources of an organization [3]. From what information analysis methods are used for analysis, the effectiveness of the technology of detecting network attacks strongly depends on. Currently, there are many methods for detecting attacks, let's consider some of them.

Behavioral methods are called methods based on the use of information about the normal behavior of the system and its comparison with the parameters of observable behavior [1]. The presented group of methods is oriented on the construction of a standard, or normal, system or user system. In the course of their work, systems that use this approach compare current activity figures with a profile of normal activity, and the case of significant deviations can be considered as evidence of an attack. These methods are characterized by the presence of false positives, which are explained primarily by the complexity of the exact and complete description of the plurality of legitimate user actions. In addition, for most such systems, it is necessary and necessary to carry out the stage of the previous setting, during which the system "gaining experience" to create a model of normal behavior. The length of this interval for data collection may take several weeks, and sometimes a few months. These disadvantages are often the main reasons for the refusal to use systems based on behavioral methods in favor of systems that use accurate representation of network security breaches. One of the behavioral methods is statistical analysis.

Statistical analysis is the core of methods for detecting anomalies in the network. At the very beginning of this method, profiles are defined for each subject of the analyzed system. Any deviation of the profile used from the reference is considered to be unauthorized activity. [2]

It should be noted that in the statistical systems an important role is played by the correct choice of controlled parameters that characterize the differences in normal and abnormal traffic. It may turn out that due to the wrong choice of the number of observed parameters, the model describing the behavior of entities in the system will be incomplete or excessive. This results in the passage of attacks or false alarms in the system.

The advantages of statistical systems are their adaptation to change the behavior of the user, as well as the ability to detect the modifications of the attack. Among the shortcomings

it is possible to note the high probability of occurrence of false reports of attacks, as well as their pass.

Knowledge-based methods include such methods, which in the context of the given facts, rules of output and comparison, reflect the signs of given attacks, produce actions to detect attacks based on the found mechanism of search [4]. As a search procedure, a pattern matching, a regular expression machine, a logical sequential conclusion, a state transition, etc. can be used. Their name implies that systems based on their application work with a knowledge base, including information about already known attacks. Here the knowledge base is represented by a repository containing expert records supporting the logic of their processing and interpretation (that is, it is characterized by the presence of a subsystem of logical output). If there is no precise knowledge about the modification of the harmful activity, then these methods can not cope with the detection of various variations of this harmful activity. The group of data methods includes signature methods.

In signature methods, system events are presented in the form of strings of characters from a certain alphabet. The essence of these methods is to set the set of attack signatures in the form of regular expressions or patterns based on model matching and verify the match of the observed events with these expressions. Signature is a set of attributes that can distinguish network attacks from other types of network traffic. In the input package, the byte is viewed by byte and compared to the signature (signature) - a characteristic line of the program, indicating the characteristics of malicious traffic. Such a signature may contain a key phrase or a command that is associated with an attack. If a match is found, an alarm is announced [4].

The main advantage of the signature method is that the detection of known samples of abnormal events is carried out as effectively as possible. But at the same time, the use of a signature database of a large volume negatively affects the performance of the detection system. The disadvantage of this method is the impossibility of detecting attacks whose signature has not yet been determined.

Methods of computing intelligence. This category includes neural networks. The neural

network is a set of processing elements - neurons, interconnected by synapses, which convert the set of input values into a set of desired output values [5-6]. Neural networks are used in a wide range of applications: pattern recognition, control theory, cryptography, data compression. Neural networks have the ability to learn from the sample and generalize with noisy and incomplete data. In the learning process, adjustment of the coefficients associated with synaptic weights is performed.

There are several methods for training neural networks. One of the most well-known and most widely used learning algorithms for multilayer neural networks is the direct dissemination of the method of reverse error propagation [7-8]. This algorithm uses a gradient descent with minimization of the mean square error for each iteration of its execution.

One of the important advantages of neural networks is their ability to take into account the characteristics of attacks, identifying elements that are not similar to those studied [9-10].

3. Method

Neural networks are one of the areas of research in the field of artificial intelligence, based on attempts to recreate the human nervous system, namely the ability of the nervous system to learn and correct mistakes that should enable the work of the human brain to be simulated, albeit roughly, [11]. The neural network consists of neurons. The block diagram of the neuron is shown in Figure 1.

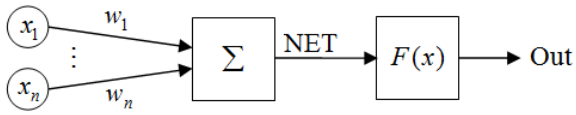


Figure 1: Structural scheme of the neuron

The structure of the neuron from the following blocks represented:

1. Input signals.
2. Weighting factors.
3. Composer and its output NET.
4. The activation function of the neuron F(x).
5. Output signal.

There are many properties in the neural network, but the most important is its ability to learn. The process of training the network reduced to the change in weight coefficients.

$$NET = \sum_n x_n w_n \quad (1)$$

The multilayer neural network includes input, output and hidden layers (Figure 2).

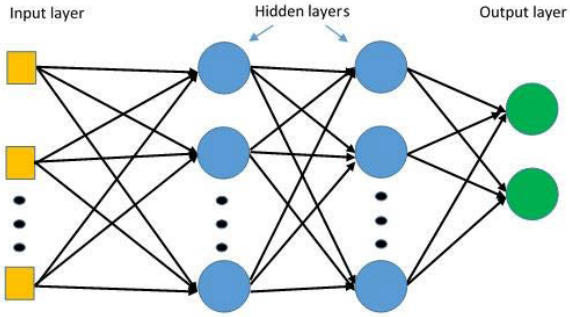


Figure 2: Multilayer Neural Network

Input layer - serves to distribute data over the network and does not do any calculations. Outputs of this layer transmit signals to the inputs of the next layer (hidden or output).

Hidden layers are layers of normal neurons that process data obtained from the previous layer and transmit signals from the input to the output. Their input is the output of the previous layer, and the output is the input of the next layer.

Output layer - usually contains one neuron (maybe more), which gives the result of calculations of the entire neural network. [11].

To conduct research, it was decided to use the NSL-KDD attack database. This database is based on the basis of the KDD-99 on the initiative of the American Association for Advanced Defense Research DARPA. [12]

It covers a wide range of different intrusions. Data is a text file. This file contained both normal vectors and an abnormal activity vector. Abnormal activity is marked by an attack type. All attacks in NSL-KDD are divided into four groups: DoS (Denial of Service Attack), U2R (Users to Root Attack), R2L (Remote to Local Attack) and Probe (Probing Attack). Table 1 lists the types of attacks, their number and the class to which the attack belongs.

Table 1
Information about attacks

Type	Number	Class
back	956	DOS
land	18	DOS
neptune	41214	DOS
pod	201	DOS
smurf	2646	DOS
teardrop	892	DOS

Type	Number	Class
buffer_overflow	130	U2R
loadmodule	72	U2R
perl	34	U2R
rootkit	30	U2R
ftp_write	43	R2L
imap	126	R2L
guess_passwd	1231	R2L
multihop	254	R2L
phf	7	R2L
spy	3	R2L
warezclient	890	R2L
warezmaster	205	R2L
ipsweet	3599	Probe
nmap	1493	Probe
portsweep	2931	Probe
satan	3633	Probe
normal	67343	-

Each record has 42 attributes describing different attributes (table 2).

Table 2

List of attributes for each entry

№	Attribute name
1	duration
2	protocol_type
3	service
4	flag
5	src_bytes
6	dst_bytes
7	land
8	wrong_fragment
9	urgent
10	hot
11	num_failed_logins
12	logged_in
13	num_compromised
14	root_shell
15	su_attempted
16	num_root
17	num_file_creations
18	num_shells
19	num_access_files
20	num_outbound_cmds
21	is_host_login
22	is_guest_login
23	count
24	srv_count
25	serror_rate
26	srv_serror_rate
27	rerror_rate
28	srv_rerror_rate
29	same_srv_rate
30	diff_srv_rate
31	srv_diff_host_rate
32	dst_host_count
33	dst_host_srv_count
34	dst_host_same_srv_rate
35	dst_host_diff_srv_rate
36	dst_host_same_src_port_rate
37	dst_host_srv_diff_host_rate
38	dst_host_serror_rate
39	dst_host_srv_serror_rate
40	dst_host_rerror_rate
41	dst_host_srv_rerror_rate
42	attack_type

The Deductor Academic 5.3 software to construct and test the neural network was used. Deductor is a platform for creating complete analytical solutions. The platform employs advanced methods for extracting, rendering data and analyzing data. Deductor Academic - The free version for educational purposes only intended.

In this paper, the study for attacks like DoS conducted. Therefore, a parser written to extract the necessary vectors. There were 4 files for training and testing of the neural network: KDDTrainDos + .txt, KDDTestDefinedDos + .txt, KDDTestNormalDos + .txt, KDDTestUndefinedDos + .txt. The files contain a set of training data, a set of known attacks and normal vectors that listed in the training set, as well as a set of unknown attacks.

The file for training the neural network contains 7,000 records, the contents of the file given in Table 3.

Table 3

Contents of the training file

Attack name	Number of attacks
back	556
neptune	4000
smurf	1446
teardrop	492
normal	506

A test file with known attack types contains 5000 entries. The table of contents given in Table 4.

Table 4
The contents of the file for testing with known types of attacks

Attack name	Number of attacks
back	400
neptune	3000
smurf	1200
teardrop	400

A normal testing file contains 781 entries. The file with unknown types of attacks are attacks such land and pod, the number of entries is 219. Research of intrusion detection was performed using multilayer perceptron.

4. Experimental results

Before the construction of the neural network training data set excluded parameters have the same meaning throughout the sample. This was done to accelerate results.

The first neural network was built on 28 parameters. It consisted of an input, one hidden and output layers. The input and hidden layer neurons had 28 each, consisting of one output neuron containing conclude attack (1 - attack, 0 - normal traffic). This neural network is presented in Figure 3.

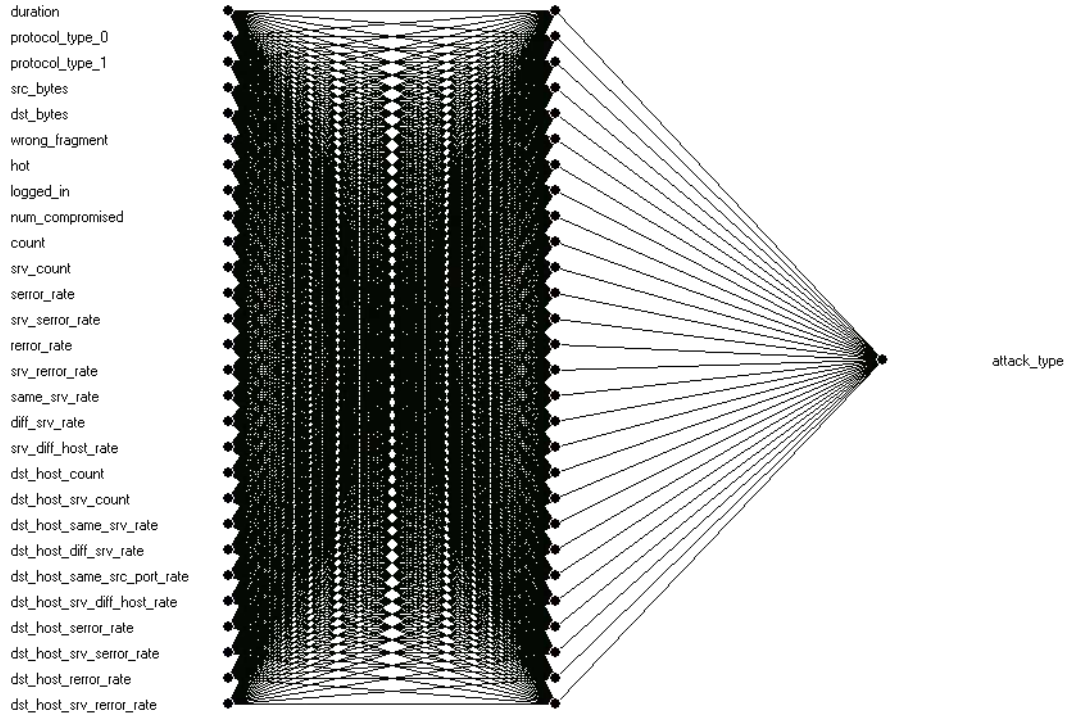


Figure 3: Neural network 28x28x1

After building a neural network was conducted three tests to assess the quality of its work in detecting attacks. The first test was carried out for attacks from known types for neural network (back, neptune, smurf, teardrop). Neural network with almost 100% (99.78%) accurately recognizes known types of attacks. Further testing was conducted for normal traffic. In this case, the results were similar to results for known types of attacks (98.98%). And the last test was performed with unknown types of attacks for the neural network, namely attacks like land and pod.

Unlike previous tests, the result is very different. That is, in this case, we can say that only every 4th attack will be detected. But it should be noted that since these types of attacks were not present in the training set, we can say that this is a good result. And also the knowledge that such methods as statistical analysis and the method of signature analysis, in the absence of information about the attack data in general, would mark them as normal traffic suggests that the use of neural networks to detect intrusions is justified, since they have the ability to adapt to unknown attacks.

Since satisfactory results were obtained, a decision was made to construct neural networks with different parameters to determine the optimal configuration for detecting the maximum number of attacks. Changes were made in the number of input parameters, in the change of activation

function and its steepness, and in the number of hidden layers.

The following neural networks have a common configuration: 15 input neurons, 16 neurons in the hidden layer and 1 output neuron (Figure 4).

All neural networks 15x16x1 have the same look, the difference between them is only in different activation functions and the value of the slope parameter (Table 5).

Table 5
Test Neural Networks

№	Size	Activation function	Slope function
1	15x16x1	Sigmoid	1
2	15x16x1	Sigmoid	1,5
3	15x16x1	Hypertangens	1
4	15x16x1	Arctangens	1

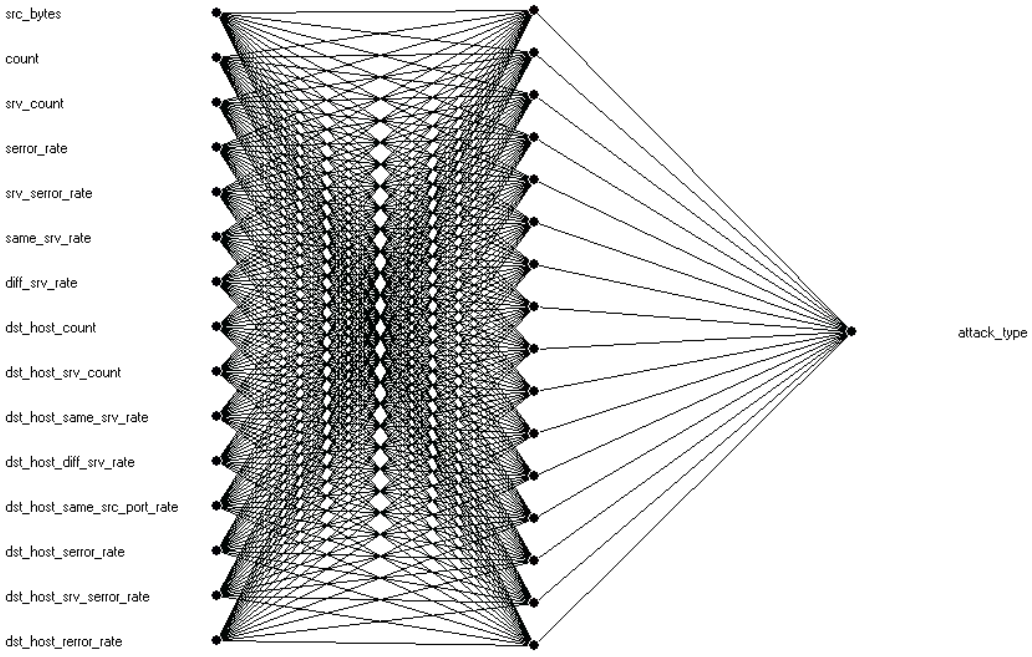


Figure 4: Neural network 15x16x1

For each of the networks built previously described tests were conducted, such as intrusion detection with known types, normal traffic and attacks with unknown types. The results obtained with the use of these neural networks are presented in Table 6.

Table 6
Results of neural network 15x16x1

№	Detection of known attacks,%	Detection of normal vectors,%	Detecting Unknown Attacks,%
1	99,76	97,18	34,25
2	99,88	95,13	33,79
3	100	0	100
4	99,18	60,69	57,08

Based on the results, we can say that the best of all has shown itself the function of activation of the sigmoid. The artagens and the hypertension, however, did not give satisfactory results, although the recognition of attacks with an unknown type has increased significantly, the quality of the definition of normal traffic has suffered greatly. Therefore, in this case, we can conclude that for this task, the function of activating the sigmoid is better suited. Regarding the slope coefficient, we can say that the coefficient 1.5 did not improve the results. Therefore, the following studies were conducted with sigmoid and factor 1, since the best results were obtained for this configuration. Further changes relate only to the number of neurons and the number of hidden layers.

Next, neuronal networks with 21, 26 and 31 neurons were constructed on a hidden layer.

Further tests were carried out. The results are presented in Table 7.

Table 7
Results of neural networks

Size	Detection of known attacks,%	Detection of normal vectors,%	Detecting Unknown Attacks,%
15x21x1	99,68	95,77	33,79
15x26x1	99,78	96,03	33,79
15x31x1	99,7	96,8	34,7

The last two experiments were conducted with a neural network with two hidden layers (Figure 5) and a neural network with a smaller number of input neurons - 10 (Figure 6).

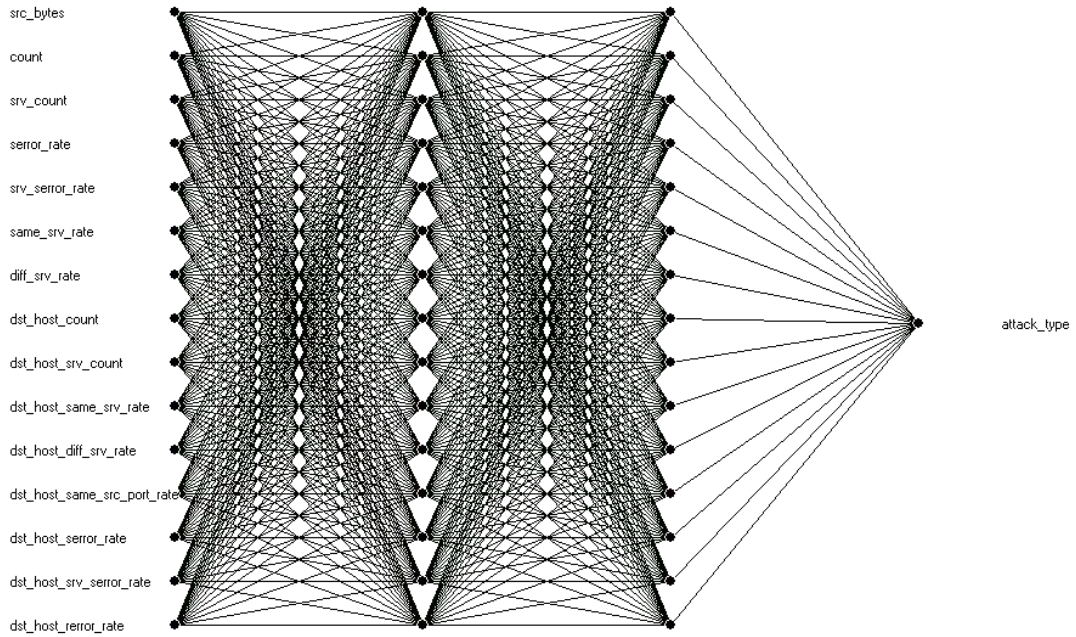


Figure 5: Neural network with two hidden layers

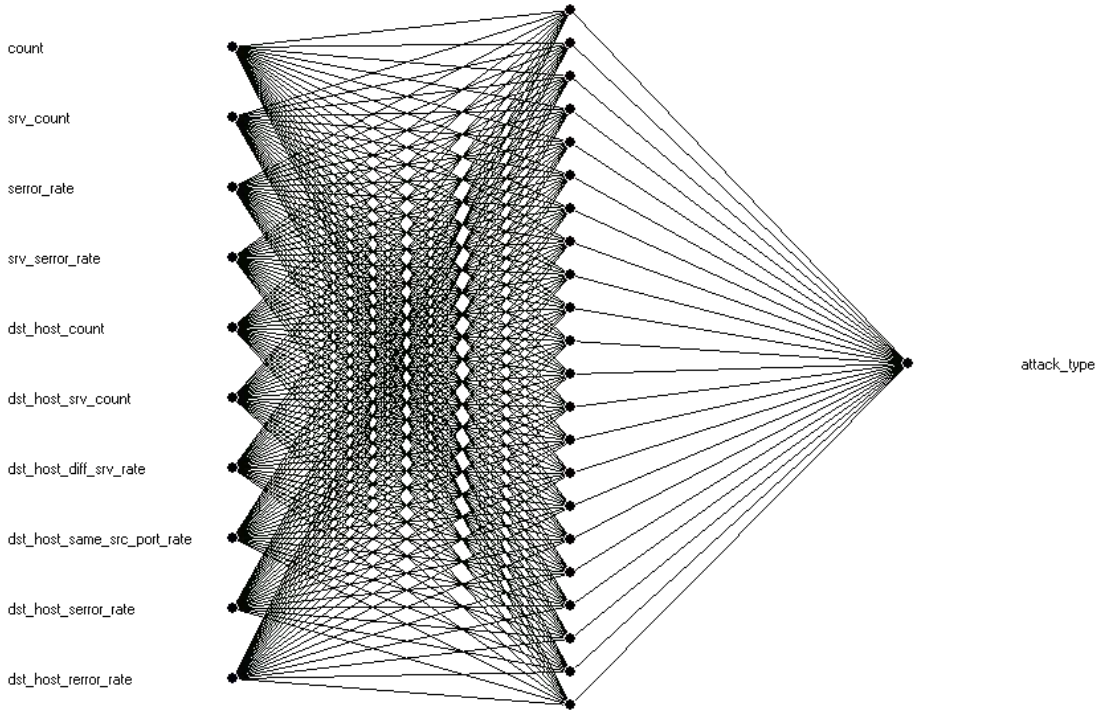


Figure 6: Neural network with 10 input neurons

The results represented in Table 8.

Table 8
Results of neural networks 15x15x15x1 and 10x22x1

Size	Detection of known attacks,%	Detection of normal vectors,%	Detecting Unknown Attacks,%
15x15x15x1	99,8	95,01	34,25
10x22x1	99,96	93,34	31,51

From the results it can be seen that the neural network with 10 input neurons has worse results than neural networks with more input parameters. Thus, a strong reduction in the number of input parameters has a negative effect on the result. As for a neural network with two hidden layers, it has approximately the same results as the neural networks 15x16x1 and 15x31x1. If you summarize the value (to sum up the percentage and find it divided by the number of experimentation findings) for networks with better results, namely for 15x16x1, 15x31x1 and 15x15x15x1, then you can see which neural network has better coped with the task (table 9).

Table 9
Neural network results with the best results

Size	Detection of known attacks,%	Detection of normal vectors,%	Detecting Unknown Attacks,%	Generalized value, %
15x15x15x1	99,8	95,01	34,25	76,35
15x31x1	99,7	96,8	34,7	77,07
15x16x1	99,76	97,18	34,25	77,06

5. Conclusions

Among the considered neural networks, the best with the task of detecting attacks was copied neural network with 31 neurons in the hidden layer.

So, as can be seen in comparison with the first experiment, where the percentage of unknown attacks was 27.4% managed to get an increase to 34%, that is, every third unknown attack would be detected.

Thus, we can conclude that although the percentage is not very large, it is satisfactory, as it is much better than skipping attacks as normal traffic. It can be said that the use of multilayer perceptron for this task is justified.

6. References

[1] Beqiri E. Neural Networks for Intrusion Detection Systems. In: Jahankhani H., Hessami A.G., Hsu F. (eds) Global Security, Safety, and Sustainability. ICGS3 2009. Communications in Computer and Information Science, vol 45. Springer, Berlin, Heidelberg

[2] Reddy E. K. Neural networks for intrusion detection and its applications //Proceedings of the World Congress on Engineering. – 2013. – Т. 2. – №. 5. – С. 3-5.

[3] Mustafaev, AG, A Neural Network System for Detecting Computer Attacks Based on Analysis of Network Traffic, Security Issues. - 2016. - №. 2. - p. 1-7.

[4] Alekseev A.S., TEACHING THE APPLICATION OF NEURAL NETWORKS FOR DISPLACEMENT OF INCORPORTS // Problems of modern pedagogical education. - 2017. - no. 57-6. - p. 44-50.

[5] Subba B., Biswas S., Karmakar S. A neural network based system for intrusion detection and attack classification //2016 Twenty Second National Conference on Communication (NCC). – IEEE, 2016. – С. 1-6.

[6] Park S., Park H. ANN Based Intrusion Detection Model //Workshops of the International Conference on Advanced Information Networking and Applications. – Springer, Cham, 2019. – С. 433-437.

[7] E. Belov, M. Maslennikov, A. Korobeinikov. The use of a neural network to detect network attacks. Scientific and Technical Journal of Information Technologies, Mechanics and Optics. - 2007. - №. 40

[8] Subba B., Biswas S., Karmakar S. Intrusion detection systems using linear discriminant analysis and logistic regression //2015 Annual IEEE India Conference (INDICON). – IEEE, 2015. – С. 1-6.

[9] Fernandes G. et al. A comprehensive survey on network anomaly detection //Telecommunication Systems. – 2019. – Т. 70. – №. 3. – С. 447-489.

[10] Kaja N., Shaout A., Ma D. A two stage intrusion detection intelligent system //The international arab conference on information technology, IEEE-ACIT. – 2017.

[11] NSL-KDD dataset // https://github.com/defcom17/NSL_KDD

Technology of Secure Data Exchange in the IoT System

Hassan Mohamed Muhi-Aldeen[1], Yurii Khlaponin[2], Ibtehal Shakir Mahmoud[3], Volodymyr Vyshniakov[4], Vadym Poltorak[5], Dmytro Khlaponin[6], Muwafaq Shyaa Alwan[7]

[2, 4, 6]*Kyiv National University of Construction and Architecture, Kyiv, Ukraine*
[1,3,7] *Al Iraqia University, Baghdad, Iraq*
[5]*NTUU "Igor Sikorsky Kyiv Polytechnic Institute", Kyiv, Ukraine*

Abstract. The use of public Internet channels for managing objects in the IoT system can lead to the emergence of security threats not only for this IoT system, but also it can provide cybercriminals with resources to carry out attacks on any other objects of the global network. Therefore, you should use secure data exchange technologies that prevent unauthorized entry into the system when building IoT systems. This technology is discussed in detail in this article. The purpose of this work is to improve safety of IoT systems through the use of a perfectly secure data exchange channel.

Keywords :
IoT system, safety of IoT systems, secure data exchange technologies, secure data exchange channel.

1. IoT security challenges

In 2020 the number of connected devices to the IoT exceeded 30 billion, and their annual growth increased from 3 billion in 2017 to 5 billion in 2020 as shown by the published data of researchers [1].

Forecasts up to 2025 assume that this growth will not decrease, but tends to increase. This testifies to the rapidly growing need for managing remote sites and ample opportunities for their implementation using existing tools and technologies. However, the rapid growth of needs and the broad possibilities of implementing IoT in a short time often leads to insufficiently thought out solutions from the point of view of security, which is described in [2-4], where security at the network level is attributed to the most vulnerable area. Attackers are given the opportunity to use them to implement DDoS attacks due to insufficient protection of IoT devices, the number and power of which increases with the number of IoT users. The overwhelming majority of users believe that general security rules for the IoT should be developed at the state or interstate level.

However, it is difficult to develop uniform recommendations or standards due to the difference in security requirements depending on the area of use of the IoT. The variety of areas of use is shown in Table 1.

Table 1.
Gartner's analysis of the number of IoT devices in use globally, billion

Application area	2018	2019	2020
Housing	0.98	1.17	1.37
Building automation	0.23	0.31	0.44
Security systems	0.83	0.95	1.09
Extraction of minerals	0.33	0.4	0.49
Automotive	0.27	0.36	0.47
Medicine	0.21	0.28	0.36
Trade	0.29	0.36	0.44
Transport	0.06	0.07	0.08
Government sector	0.4	0.53	0.7

Gemalto's survey of IoT users found that 90% were unsure about security. Thus, it seems to be relevant the analysis of IoT systems from the point

EMAIL: muhialdeen.hassan@aliraqia.edu.iq (A. 1); y.khlaponin@gmail.com(A. 2); ibtehal.shaker@aliraqia.edu.iq (A. 3); volodymyr.vyshniakov@gmail.com (A. 4); poltorak_vp@online.ua (A. 5); dmytro.khlaponin85@gmail.com (A. 6); dr.muwafaqalwan@aliraqia.edu.iq (A. 7)
ORCID: 0000-0002-9287-0817 (A. 1); 0000-0002-9287-0817 (A. 2); 0000-0001-8333-461X (A. 3); 0000-0003-4668-712X (A. 4); 0000-0001-9231-9411(A. 5); 0000-0002-7797-4319 (A. 6); 0000-0001-7980-2716 (A. 7)

of view of ensuring the secure exchange of data over the Internet channels, as well as the technical solutions in this area, given in the work.

2. Analysis of data exchange options in IoT systems

To connect IoT devices to the Internet, one of two schemes can be used, shown in Fig. 1 and Fig. 2 respectively.

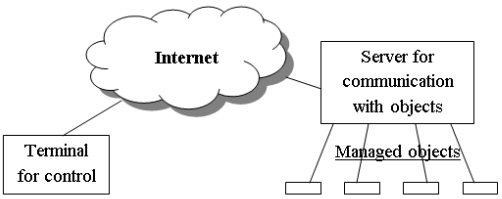


Figure 1: Direct management of objects through the public network

The scheme shown in Fig. 1 is the simplest one and can be successfully used in internal computer networks. But such solution has a number of disadvantages in the conditions of the public Internet:

- Connecting the server directly to the Internet facilitates the intervention of unpredictable external threats into management processes.

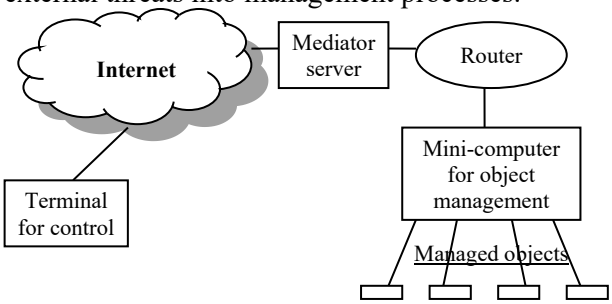


Figure 2: Object management using a mediation server

- Cybercriminals are more likely to install their botnets (malware) on your server to implement DoS and DDoS attacks.
- This server requires a dedicated IP address on the Internet, which is associated with additional material costs.
- To ensure the information security of the server, qualified service is required.

Disadvantages listed above are absent in the circuit shown in Fig. 2, where data flows between the terminal and management objects are filtered by the proxy server. This server can simultaneously serve many users, protecting their data streams from malicious attacks. Internet service providers (ISPs) can install such servers, providing customers with cloud-based access to resources. However, the user can install own separate or corporate broker server in case of high security requirements for information about objects managed. In cases when the broker's server is hit by a threat, the information about the managed objects will be kept intact. An increase in signal latency should be noted as a disadvantage of control through an intermediary server in comparison with the first scheme. But this disadvantage can be considered insignificant, since the performance in control systems cannot be high due to the presence of unpredictable network access latency using Internet channels.

3. Technical solutions to secure the IoT

Object management via the Internet does not require the transfer of large amounts of data and high-speed messaging. This allows you to use the most advanced methods of protecting data from threats of disclosure or spoofing during transmission over channels. The use of such methods makes it possible to exclude the possibility of these threats being realized, which is mathematically provable. It should be noted that no expensive technical solutions are needed for absolute protection. This protection is implemented using simple software methods. It is mathematically proven that the absolute protection of information is provided by the Vernam cipher, which is called one-time pad [5]. The use of this cipher requires the fulfillment of the conditions, the list of which is presented in Table 2.

Table 2.
Conditions for ensuring absolute data protection during transmission

Condition	Condition fulfillment
Generation of random bit sequences (not pseudo-random)	A method for random bits generating is implemented, which allows you to generate random sequences on any computer, as described in [3]
Each random bit sequence can be used for encryption only once	For each communication session, random bit sequences are generated independently of each other
For the exchange of random bit sequences,	The exchange of random bit sequences occurs according to

an absolutely secure communication channel should be used	the Diffie-Hellman algorithm with such parameters for which there is no possibility of data disclosure in modern conditions

The work [7] substantiates the choice of the Diffie-Hellman algorithm parameters. The parameters of the algebraic group for the implementation of the algorithm are selected based on two conditions. In first, it is needed to ensure the impossibility of disclosing data. From the other hand, it is needed that the time of cryptographic transformations does not exceed the allowable value. In order to prevent data disclosure, an algebraic group in the form of a Galois field with characteristic 2 was chosen and a degree, which is a safe prime number from the series 503, 563, 587, 719, was chosen too. Since the solution to the discrete logarithm problem for such fields is unknown today, this protection cannot be hacked in modern conditions. All cryptographic transformations are implemented in the form of several dozen lines in JavaScript and can be copied and placed both in the client and server parts of the software of IoT systems. If the Node.js platform is used to write the server side, then the cryptographic transformations in the server and client sides will be identical. All fragments of the data protection program for a field of (2^503) elements are presented below.

The beginning of filling the array with N random bits looks like this:

```
var N = [504]; // Array of 503 random bits (N [0] is not used)

var T1 = new Date (); // Take the timestamp for transformations

var TN = T1.getTime (); // TN - the number of milliseconds from 01/01/1970

N [1] = TN% 2; // Fill the first bit depending on the parity of TN
```

The rest of the random bits will be formed in the cycle of filling the array MA with powers of the primitive root of the Galois field.

The block for filling an array MA with powers of A looks like this:

```
// Elements of arrays with index 0 are not used

var A = [504]; // Sequence of 503 bits for exponentiation

var B = [504]; // A sequence of 503 bits of the exponent

// Arrays for multiplying the elements of the Galois field GF (2 ^ 503)

var M1 = [504], M2 = [504], R = [504];

// M1 [], M2 [] - factors R [] - the result of multiplication

var MA = new Array (504); // Array MA [] [] of degrees A []

for (var i = 0; i<504; i ++) MA [i] = new Array (504);

for (var i = 1; i<= 503; i ++) MA [1] [i] = A [i];

// The first line of the array was filled with the value A []

for (var I = 2; I <= 503; I ++)

{// Loop filling the array MA [] [] with powers of A []

// In the next 3 lines, we continue filling the array N []

T1 = new Date (); // Take the timestamp for transformations

TN = T1.getTime (); // TN - the number of milliseconds from 01/01/1970

N [I] = TN% 2; // Fill in the next bit depending on the parity of TN

for (var J = 1; J <= 503; J ++) M1 [J] = M2 [J] = MA [I-1] [J];

MULT (); // Function for multiplying the elements of the Galois field GF (2 ^ 503)

for (var j = 1; j <= 503; j ++) MA [I] [j] = R [j];

} // Put degree 2 in MA [2] , put degree 4 in MA [3],

// put degree 8 in MA [4], put degree 16 in MA [5], etc.
```

Our task is to get the same random bit sequences C[] on both sides of the data exchange. This allows to add modulo 2 (XOR operation) bits of the C[] sequence to each bit of data being sent on the transmitting side. With such information coding, absolute protection against disclosure threats in the communication channel is provided. The recipient of the information must add modulo 2 bits of the C[] sequence to the received bits for decryption, which is exactly the same procedure as on the transmitting side.

The transformation process begins by generating a sequence of 503 random bits on each side. This is done simultaneously with filling the array MA[][] with powers of the primitive root of the Galois field. The number 2 is one of primitive roots, which should be entered into the array A[]. In our example, the least significant bits correspond to the lower array indices. Therefore, we get a primitive root like this:

```
for (var i = 1; i<= 503; i ++) A
[i] = 0; A [2] = 1; // Put the
number 2 in A []
```

For raising to a power, a well-known method of simplifying calculations was used, which consists in replacing the operation of raising to a power by a product of powers according to the next expression:

$$A^B = \prod_{i=1}^{503} A^{B_i}, \quad (1)$$

where

$$B = \sum_{i=1}^{503}$$

Since any exponent B can be represented as a sum of values selected from a range of weights 2^0, 2^1, 2^2, 2^3,…, 2^{502}, to calculate AB it is enough to multiply no more than 503 elements from the array MA.

The block for raising A to power B looks like this:

```
for (var i=1; i<=503; i++) A[i]=0;
A[1]=1; // Put a unit in A[]

for (var J=1; J<=503; J++)

if (B[J]==1) // Select the bits
equal to 1 from the binary form of
exponent

{

for (var I=1; I<= 503;
I++){M1[I]=MA[J][I]; M2[I]=A[I];}

MULT(); // Function for
multiplying the elements of the
Galois field GF(2^503)

for (var I=1; I<= 503; I++)
A[I]=R[I];

} // The elements MA[][] was
Multiplied, where B[J]=1.
```

The function of multiplying the elements of the Galois field according to the rule of polynomials looks like this:

```
function MULT()

{ // Multiplication using the
polynomial X^503=X^3+1

var i, j, r, r1, r2, r3;

for (i = 1; i<= 503; i ++) R[i] =
0;

for (i = 1; i<= 503; i ++)

if (M1[i] == 1) // Select units,
because multiplication by 0 gives
0

{

for (j = 1; j <= 503; j ++)

if (M2[j] == 1)

{

r = i + j-1;

if (r> 503)

{

r = r-503;

if (r> = 501)

{

r = r-501;

r1 = 1 + r; r2 = 4 + r; r3 = 501 +
r;

if (R[r3] == 0) R[r3] = 1; else
R[r3] = 0;

}

else {r1 = r; r2 = r + 3;}

if (R[r1] == 0) R[r1] = 1; else
R[r1] = 0;

if (R[r2] == 0) R[r2] = 1; else
R[r2] = 0;

}

else {if (R[r] == 0) R[r] = 1;
else R[r] = 0;}

}

}

} // End of function MULT ()
```

Let's imagine an algorithm for obtaining bit sequences that will be the same on both sides of the data exchange.

Step 1. The client enters a random bit into the first element of the array N, and enters the value of the primitive root of the Galois field into array A.

Step 2. The client executes the block of filling the array MA with powers of A with the simultaneous completion of filling the array with N random bits.

Step 3. The client copies array N to array B and executes the exponentiation block of A.

Step 4. The client sends to the server the result of raising A to the power of B as a sequence of 503 bits

Step 5. The server stores the sequence of bits received from the client in array C and performs actions similar to steps 1-3 of the client.

Step 6. The server sends to the client its result of raising A to power B.

Step 7. The client stores the sequence of 503 bits received from the server in array A.

Step 8. The client executes the block of filling the array MA with powers of A without filling the array with N random bits.

Step 9. The client executes the block for raising A to the power B and enters the result into array C.

Step 10. The server copies array C to array A and performs the steps similar to steps 8 and 9 of the client.

The result of performing the above actions is to obtain the same random sequences of bits in the arrays C of the same name on the client and server sides, which was required for encryption using the one-time pad method.

4. Full-scale model of a secure IoT system

The main element of the IoT system that needs to be protected from false control commands and from intrusion by attackers who can create threats such as DDoS attacks is computer for object management (see Fig. 2). Connecting this computer through the Router without providing a real IP address does not provide the ability to control this computer other than through the console used to install the software or an application program that provides the protection described in the previous section. A well-known minicomputer of the Raspberry Pi 3 type, which has a 40-pin GPIO interface with wide possibilities for connecting objects for monitoring and control, was chosen as hardware. Linux version Ubuntu 20.10 was selected as the operating system, and the Node.js platform version v12.18.2 with the onoff package was used as a programming tool, which allows objects to be controlled via the GPIO interface.

The initial snippet of the CONPIN.js program installed on this computer in the / home / ubuntu / directory looks like this:

```
const HOST = '91 .198.50.144 ';
const PORT = 3000;
const Gpio = require ('onoff').
Gpio;
const fs = require ('fs');
const net = require ('net');
let SYM; // String.fromCharCode
let STREB = '////////';
let i = 0;
let TR = '';
const Gp4 = new Gpio (4, 'out');
// Pin 7 Gpio_4 # 0
const Gp17 = new Gpio (17, 'out');
// Pin 11 Gpio_17 # 1
```

This client program regularly contacts the server (Mediator server) (see Fig. 2) with a period of 20 seconds to transmit information about the state of objects and receive control signals. The duration of the period of 20 seconds is chosen from the condition of proportionality with the time of entering the Internet. The operation of this program must be protected against possible power outages. To automatically start the program after power-up, add the following three lines to the /etc/rc.local file:

```
#! / bin / sh
echo "#################### CONPIN
######################"
/ usr / bin / node / home / ubuntu
/ CONPIN &
```

The SOCKET.js program must be running on the Mediator server (see Fig. 2) located at the ISP (Internet Service Provider) site that provides services in SaaS (Software as a Service) mode. The initial snippet of this program looks like this:

```
// server / SOCKET.js //
const HOST = '91 .198.50.144 ';
const PORT = 3000;
const net = require ('net');
const fs = require ('fs');
net.createServer (function (sock)
{
```

With a single intermediary computer with a single real IP address, the provider can serve multiple IoT client systems. The number of supported systems depends only on the technical data of the computer. The operation of the SOCKET.js program must be protected from failures that can lead to an emergency shutdown. To do this, use the process manager pm2 automatic program restart tool, which must be downloaded using the npm install pm2 –g command. After that, the SOCKET.js program should be launched with the pm2 start SOCKET.js command. In this case, in case of any failures, the program will automatically restart [8].

The main task of the Mediator server is to protect the resources of IoT systems from the penetration of intruders who have as their goal the implementation of DoS and DDoS attacks. This requires unauthorized entry into the Mediator server, which is unlikely, provided the provider follows standard instructions. Usually this situation arises due to the fault of the provider's staff. In any case of failures on this server, the provider always has the ability to switch to a backup server or restore the operation of the same server using copies, which is the norm in the work of providers [9].

The exchange of data between users of the IoT system and their objects is carried out via a web interface through intermediate data files. These files are created anew at each data exchange session. Each individual user on the Mediator server is allocated his own directory, where, in addition to the SOCKET.js program with a unique value for the PORT parameter, the vybir.js program is located, the initial fragment of which looks like this:

```
// vybir.js - HTTP Server Ver. 18 February 2021

var http = require ('http');

var url = require ('url');

var fs = require ('fs');

var static = require ('node-static');

var querystring = require ('querystring');

var file = new static.Server ('.');

http.createServer (function (req, res)

{
```

In the vybir.js program, a separate TCP port number is allocated for each user. The CONPIN.html file with images of object state indicators and control buttons is also located in the user directory. The user can download this file through the link given to him like http://91.198.50.144:8000/CONPIN.html. All communication processes, including the authorization procedure, are protected using the means described in the previous section. The above link is unprotected as it is only intended to demonstrate the control process using eight binary objects as an example. Authorization data is stored in the same directory in an encrypted file.

5. Conclusions

The reasons for the emergence of security problems in IoT systems are described. Potential security threats have been identified, both for the IoT itself and for the use of its resources by intruders in the implementation of attacks on other objects of the Internet.

Variants of data exchange schemes in IoT systems have been analyzed and the choice of the most secure scheme has been substantiated.

The technical solutions that make it possible to secure data exchange in IoT systems by building an ideally secure data exchange channel are considered in detail. These solutions are presented in the form of text programs in the JavaScript language and can be embedded in any user software.

Using the example of the current model of the IoT system, it is shown that it is possible to eliminate problems with emergencies in IoT systems that arise for various reasons, including malfunctions of programs, temporary power outages or attempts to unauthorized entry into the system. A link to a resource on the Internet is provided to demonstrate the process of managing objects.

The technical solutions proposed in this work make it possible to fully secure IoT systems from information threats.

6. References

[1] Orlov S. (2020) Pochemu problem bezopasnosti interneta veshhej okazalos' tak trudno reshit'? https://safe.cnews.ru/articles/2020-05-1_pochemu_problemu_bezopasnosti_interneta

[2] Frustaci, M., Pace, P., Aloi, G., & Fortino, G. (2018). Evaluating critical security issues of the iot world: Present and future challenges. IEEE Internet of Things Journal, 5(4), 2483-2495.
[3] Conti, M., Dehghantanha, A., Franke, K., & Watson, S. (2018). Internet of Things security and forensics: Challenges and opportunities. Future Generation Computer Systems, 78(2), 544-546.
[4] Giray, G., Tekinerdogan, B., & Tüzün, E. (2018). IoT system development methods. In Internet of Things (pp. 141-159). CRC Press/Taylor & Francis.
[5] Shannon C. Communication Theory of Secrecy Systems. Bell System Technical Journal. 1949. 28 (4). Pp. 656–715.
[6] Chupryn V.M. Generuvannja vypadkovyh chisel shtatnymy zasobamy hostiv merezhi Internet./ V.M. Chupryn, V.M.Vyshnjakov, M.P. Prygara // Zahyst informacii'. – 2016. – T. 18, №4. – C. 323-335.
[7] Chupryn V.M., Vyshnjakov V.M., Prygara M.P. Metod protydii' nezakonnomu vplyvu na vyborciv u systemi Internet golosuvannja. Bezpeka informacii'. – 2017. – Tom 23, №1. – C. 7–14.
[8] V.M. Chupryn, V.M.Vyshnjakov, O.O. Komarnyc'kyj, Metod protydii' atakam poserednyka u transparentnij systemi internet golosuvannja, Zahyst informacii', Ukrainian Information Security Research Journal. - K.: NAU, 2018. – T.20. -№3. – C.180-187. http://jrnl.nau.edu.ua/index.php/ZI/article/view/13079
[9] V. Khoroshko, Y. Khokhlacheva, Y. Khlaponin, E. Gavrilko. Parametric monitoring of computing processes in information and computing systems. Workshop Proceedings (http://ceurws.org) Vol-2067 urn:nbn:de:0074-2067-8-0 P. 45 – 53. – ISSN 1613-0073

Critical Points of Information Influence in Social Networks

Oleksandr Milov [1], Serhii Yevseiev [1], Stanislav Milevskyi [1], Krzysztof Kajstura [2] and Ruslana Ziubina [2]

[1] *Simon Kuznets Kharkiv National University of Economics, Nauki ave., 9a, Kharkiv, 61166, Ukraine*
[2] *University of Bielsko-Biala, Willowa str., 2, Bielsko-Biala, 43-309, Poland*

Abstract
Social networks are considered from the point of view of informational influences on network participants (agents). The dynamic processes of forming opinions and the dynamics of information influence on network agents are considered. Models and algorithms for identifying critical points of a social network (influencing agents) are presented, the impact on which allows manipulating the aggregate opinion of network participants that form a social network.

Keywords
social network, agent, informational influence, influence models

1. Introduction

An instrument of active influence on the actions of network users and a means of forming and disseminating opinions is undoubtedly a new type of resource - online social networks. Their role has grown significantly with the advent of Web 2.0 [1]. The target segments for using this tool can vary significantly and range from the formation of consumer demand to the formation of public opinion during elections at various levels (from state to district or city). All this allows to talk about the transformation of social networks into a tool for strategic management of the population [2].

A social network can be represented as a graph, the vertices of which are individuals (agents), and the edges are the various relationships between them. It is known that the opinion of an individual in a social network is largely determined by the opinion of his influential neighbors [3, 4]. Knowing this, it is possible, both outside the network and inside it, in order to achieve our goals, to try to change the opinions of a small set of key users in popular online social networks (such as Facebook, Twitter, LinkedIn), through which opinions will spread throughout the network.

The decisions of most agents can be based on the decisions of other agents they observe. This is especially typical in conditions of a lack of information or the impossibility for various reasons to process it and draw appropriate conclusions. At the same time, the structure of the network, which determines who trusts whom, can contribute to the emergence of large information cascade changes even with insignificant changes in the decisions of an insignificant part of agents [5].

In this paper, the formation and dynamics of opinions in a social network is considered, and an attempt is made to highlight those critical points of the social network (influencing agents), the impact on which allows manipulating the aggregate opinion of the network participants forming the social network, as well as the resulting game-theoretic problems information confrontation.

2. Social network as a medium of information impact

A *social network* at a qualitative level is understood as a social structure consisting of a set of *agents* (subjects - individual or collective, for example, individuals, families, groups,

EMAIL: Oleksandr.Milov@hneu.net (A. 1); Serhii.Yevseiev@hneu.net (A. 2); Stanislav.Milevskiy@hneu.net (A. 3); kkajstura@ath.bielsko.pl (A. 4); rziubina@ath.bielsko.pl (A. 5)
ORCID: 0000-0001-6135-2120 (A. 1); 0000-0003-1647-6444 (A. 2); 0000-0001-5087-7036 (A. 3); 0000-0001-8739-1224 (A. 4); 0000-0002-8654-6981 (A. 5)

organizations) and a set of relations defined on it (a set of *connections* between agents, for example, acquaintance, friendship, cooperation, communication). Formally, a social network is a *graph* $G(N, E)$, in which $N = \{1, 2, ..., n\}$ is a set of vertices (agents) and E is a set of edges reflecting the interaction of agents.

Social networks contribute, firstly, to the organization of *social communications* between people and, secondly, to the realization of their *basic social needs*. There are two intersecting interpretations of the social network - as a social structure and its specific Internet implementation.

When modeling social networks, the mutual influence of their members (*agents*), the dynamics of their *opinions*, etc. there is a need to take into account the factors (effects) that take place in real social networks. In general, in real social networks, the following **effects and properties** can occur, due to both the characteristics and needs of agents (influencing and being influenced), the nature of their interaction, and the properties of the social network itself. Of the many effects and properties of the social network presented in [6], the following are of interest from the point of view of information impact:

1. the presence of agents' own opinions;
2. changing opinions under the influence of other members of the social network;
3. the different significance of the opinions (influence, trust) of some agents for other agents;
4. varying degrees of agents' susceptibility to influence (conformism, stability of opinions);
5. the existence of an indirect influence in the chain of social contacts. Decrease in indirect influence with increasing "distance";
6. the existence of "opinion leaders" (agents with the maximum "influence"), formalization of influence indices;
7. the impact of the structural properties of social networks on the dynamics of opinions;
8. the activity (purposeful behavior) of agents;
9. optimization of information impacts;
10. information management in social networks.

Should be noted the peculiarities of the impact of the structural properties of social networks on the opinions dynamics [7, 8]:

- the more connections an agent has, the more opportunities he has through his environment to influence the entire network, on the one hand, and, on the other, more vulnerability to someone else's influence;
- the effect of clustering (the higher the density of connections between active agents-neighbors, the greater the likelihood of activation of the agent associated with them; see below the related concept of “strong tie”);
- local intermediateness (the greater the intermediate value of the agent, the, on the one hand, the greater its value in the dissemination of opinion / information from one part of the network to another (the role of an information broker), and, on the other hand, the less its influence on the neighbor agent - see the related concept of “weak tie” below);
- the small diameter of the social network causes a short chain of dissemination of opinion in the network.

Influence is the process and result of an individual (subject of influence) changing the behavior of another subject (individual or collective object of influence), his attitudes, intentions, ideas and assessments (as well as actions based on them) in the course of interaction with it. *Influence* - the ability to influence someone's ideas or actions. Distinguish between directed and undirected influence. Directed (purposeful) influence - influence that uses persuasion and suggestion as mechanisms of influence on another subject. In this case, the subject of influence sets itself the task of achieving certain results (for example, choosing certain actions) from the object of influence. Non-directed (non-targeted) influence is an influence in which the individual does not set himself the task of achieving certain results from the object of influence.

In a social network, agents often do not have sufficient information for making decisions or cannot independently process it, so their decisions can be based on the decisions they observe or the perceptions of other agents (social influence). Social influence is realized in two processes: communication (in the course of communication, exchange of experience and information, discussion of certain issues with authoritative neighbors for the agent, he comes to certain ideas, attitudes, opinions) and comparison (in search of social identity and social approval, the agent accepts representations and actions expected from him by other agents in a given situation; the agent asks the question “what would the other agent (the standard for comparison) do if he were in my situation?” and, comparing himself with him, determines his adequacy and plays the corresponding role; can be explained by

comparison and the search for strategic advantage: by comparing himself with other agents occupying the same positions in the social system, the agent can introduce or accept innovations that will make him more attractive as an object of relations). It should be noted that with a communicative approach to influence, agents may arrive at similar ideas, but not necessarily similar behavior. In comparison, the agent usually copies the behavior indirectly. Obviously, the behavior of an agent is determined not only by perceptions, but also by the constraints it faces. Therefore, agents with similar views can behave differently, and vice versa, agents with different views can behave in the same way.

The social network plays a large role in the dissemination of information, ideas and influence among its members. Influence in the social media literature is closely related to the term *diffusion of innovations*.

3. Identification of influential agents in the network

A social network can be viewed as a set of agents - potential voters who "vote" for a particular product, service, or candidate from a particular political party in the elections. In this case, the *value* (utility) of an *agent* in a social network depends not only on himself (for example, directly by the expected choice), but also on his influence on other agents. In other words, the configuration and state of the network is important - the totality of the opinions of potential voters regarding their choice. Therefore, there is a need to identify a small number of agents (*the problem of maximizing influence*) that contribute to the formation of the required opinion throughout the network.

The problem of determining the k most influential agents in a social network arose in the context of the so-called *viral marketing* [9]. To solve the problem, the market is modeled as a social network of agents (Markov network), the value of each of which is determined not only by the immediate expected profit from the sale (*intrinsic value of customer*), but also by the expected profit from sales to other agents that will be affected by this, from sales to agents which they can influence, etc. (*network value of customer*).

To identify the most valuable (authoritative, influential) agents, the task can be formulated as follows. Let us define the optimal informational influences $IA = \{IA_1, \ldots, IA_n\}$ (IA_i can be both a Boolean variable: 1 - the presence of informational influence, 0 - its absence for the i-th agent; and continuous - the level of influence) for a set of n agents with a predicate $X_i = 1$ if agent i made the required choice and $X_i = 0$ otherwise. Suppose that the choice is described by the following set of attributes: $Y = \{Y_1, \ldots, Y_m\}$. Each agent i has a set of neighbors N_i that directly affect X_i, thereby defining a network of agents. In turn, the i-th agent influences its neighbors.

Let the cost c of the implementation of the information influence per one agent be given, the utility rv_1 from the adoption of the required decision, if the corresponding information influence was exerted on it, and the utility rv_0 from the adoption of the required decision, if the information influence was not carried out. For simplicity, let IA be a Boolean vector.

Let $f_i^1(IA)$ will be the set-result of setting IA_i to 1 (all other values are unchanged), similarly defined for $f_i^0(IA)$. Then the expected increase in utility from the information impact for the agent without taking into account its impact on other agents, i.e., the expected utility from the successful implementation of the information impact (*intrinsic value of customer*) is determined by the formula

$$ELP_i\left(X^k, Y, IA\right) = rv_1 P\left(X_i = 1 \mid X^k, Y, f_i^1(IA)\right) - ,$$
$$- rv_0 P\left(X_i = 1 \mid X^k, Y, f_i^0(IA)\right) - c$$

where X^k – the set of agents whose decisions are known (about whom it is known that they made the required decisions), $P\left(X_i \mid X^k, Y, IA\right)$ – conditional probability of making the required decision by the i-th agent.

Then the expected increase in utility from the information campaign for the selected agents will be

$$ELP\left(X^k, Y, IA\right) = \sum_{i=1}^{n} rv_1 P\left(X_i = 1 \mid X^k, Y, IA\right) - ,$$
$$- \sum_{i=1}^{n} rv_0 P\left(X_i = 1 \mid X^k, Y, IA_0\right) - |IA| c$$

where IA_0 – zero vector; $rv_i = rv_1$, if $IA_i = 1$ (else $rv_i = rv_0$); $|IA|$ – number of selected agents.

The overall value of an agent on the network (*total value of customer = network value of customer + intrinsic value of customer*) will be $ELP\left(X^k, Y, f_i^1(IA)\right) - ELP\left(X^k, Y, f_i^0(IA)\right)$, (i.e., the value of IA will change for other agents and may affect their probability of making a decision). Then the agent's *network value*

(*network value of customer*) is the difference between his general and personal value (*network value of customer = total value of customer - - intrinsic value of customer*). As can be seen, the value depends on whether the promotions were held for other agents and whether other agents made the required decision.

Let's return to the problem of determining the k most influential nodes in a social network. Obviously, in order to find them in this case, you need to find an IA that maximizes ELP. In the general case, finding the optimal IA requires an enumeration of all its possible combinations. The following approximating procedures are possible, giving an approximate solution:

1) A single bypass. For the i-th agent there is a special offer

$IA_i = 1$, if $ELP\left(X^k, Y, f_i^1\left(IA_0\right)\right) > 0$;

2) Greedy algorithm. Set $IA = IA_0$. It is necessary to bypass IA_i in the loop, setting the value to one, if

$ELP\left(X^k, Y, f_i^1\left(IA\right)\right) \geq ELP\left(X^k, Y, IA\right)$;

Hill-climbing search. Set $IA = IA_0$, $IA_{i1} = 1$, where $i_1 = \arg\max_i \left(ELP\left(X^k, Y, f_i^1\left(IA\right)\right)\right)$. Repeat as long as the i-th agent exists, setting for which $IA_i = 1$ leads to an increase in ELP.

4. Maximizing influence in the basic models of the diffusion of innovations

In [10], the problem of influence maximization is considered on the example of the following two basic models of the propagation of innovations: *a linear threshold model and a model of independent cascades*, in which there is an initial set of active agents A_0 and at some moment in time a new active agent gets a chance to activate its neighbors with probability p_{vw}, and the latter, if successful, are activated at the next step, and so on until new activations are possible.

The problem of maximizing influence can be formulated as follows. The influence $\sigma(A)$ of the set of agents A is defined as the expected number of active agents upon completion of the process of propagation of information actions initiated by agents from the set A. For both models (linear threshold and independent cascades), an NP-hard problem arises: for a given parameter k, find k-elements set A maximizing $\sigma(A)$. Since the problem of maximizing the influence is similar to the problem of maximizing submodular functions, then for the appropriate application of the algorithm it is only necessary to prove that $\sigma(A)$ is a submodular function. The submodular function f maps a finite set U to non-negative real numbers and satisfies the natural property of "diminishing returns" (the marginal revenue from adding an element to a set S is at least as high as the marginal revenue from adding the same element to any set including S).

Generalized Threshold Model. An agent's decision to activate is determined by a monotonic threshold function $f_v : S \subseteq N_v \to [0,1]$, where N_v is the set of neighbors v and $f_v(\varnothing) = 0$. Each agent initially chooses a threshold θ_v uniformly randomly and becomes active if $f_v(S) \geq 0$.

Generalized cascade model. The probability $p_v(u, S)$ that agent u activates agent v depends on the set S of agents that have already unsuccessfully tried to activate agent v. A restriction is imposed on the model: if neighbors $u_1, ..., u_l$ try to activate v, then the probability that v will become active after l attempts does not depend on the order of activation attempts.

Generalized information impact strategies. Let there be m different ways of informational influence $I_1, \ldots, I_m$, each of which can affect a certain subset of agents of the social network, increasing their probability of activation. That is, the initial set of active agents A_0 is not defined. The amount of investments x_i in each marketing action is selected, which is limited in aggregate by the budget. Marketing strategy - vector $\boldsymbol{x} = \{x_1, ..., x_m\}$. The probability $h_v(x)$ of agent v becoming active is determined by strategy x. The function $h_v(\cdot)$ is non-decreasing and has the property of "*diminishing incomes*", that is

$\forall x \geq y \; \forall a \geq 0 \; h_v\left(x + a\right) - h_v\left(x\right) \leq h_v\left(y + a\right) - h_v\left(y\right)$

The resulting expected number of active agents in this case (taking into account direct marketing and subsequent influence) is equal to

$$EG\left(x\right) = \sum_{A \subseteq V} \sigma\left(A\right) \prod_{u \in A} h_u\left(x\right) \prod_{v \notin A} \left[1 - h_v\left(x\right)\right]$$

In order to approximately maximize this functional, it is assumed that can be estimated $EG(x)$ at each point $\boldsymbol{x}$ and can be found the direction i with an approximately maximum gradient. Let e_i be the unit vector of the i-axis and δ a constant. It is assumed that there exists $\gamma \leq 1$ such that can be found i for which $EG(\boldsymbol{x} + \delta e_i) - EG(\boldsymbol{x}) \geq \gamma(EG(\boldsymbol{x} + \delta e_i) - EG(\boldsymbol{x}))$ for any j. Then, dividing the budget k into parts of size δ, at each step (all of these parts k/δ), we can invest δ funds

from the budget into I_i, which maximizes the gradient $EG(\cdot)$.

Competing information influences. In [11], the problem of influence maximization is considered for the case of two competing influences A and B (there are player A and player B) for the model of independent cascades. Accordingly, an agent in the network represented by the graph *G(N, E)* can be in three states: A (reaction to informational action A), B (reaction to informational action B) and C (no decision has been made yet - no response). An agent can move from state C to any other and nothing more. The initial disjoint active sets of nodes are I_A and I_B, respectively ($I_A \cup I_B = I$). The problem of influence maximization is considered for player A. Formally, it is necessary to maximize $f(I_A | I_B)$ - the expected number of agents that will be affected by A for a given I_B by choosing I_A.

Two models extended in relation to the model of independent cascades are proposed:

1) *A model based on distance (distance-based),* in which the agent receives the corresponding innovation from the "closest" activated agent from *I.*

2) *The wave model.* The innovation is spreading step by step. An agent that is not active at the previous step is activated at the current step by uniformly randomly choosing one of the neighbors located at a distance proportional to the number of the step.

For these conditions, it is promising to calculate the Nash equilibrium and consider the Stackelberg game.

Voting model. In [12], the problem of maximizing influence is considered on the example of a probabilistic *voting model*. In the voting model (belonging to the class of *Interacting Particle Systems models*), at each step, each agent can change his mind, randomly choosing one of the neighbors and accepting his opinion. This model is similar to the threshold model in the sense that the agent is more likely to change his mind to the one supported by the majority of his neighbors. However, in the voting model, in contrast to the threshold model, the agent can become inactive.

The social network is represented by an undirected graph with loops *G(N, E)*. Each node *v* has many neighbors *N(v)* and is randomly initialized (assigned a value of 1 or 0). At each moment in time, each node randomly chooses one of its neighbors (the probability of choosing each neighbor is the same) and accepts his opinion:

$$f_{i+1}(v) = \begin{cases} 1, \text{ with probability } \dfrac{\left|\left\{u \in N(v) : f_t(u) = 1\right\}\right|}{\left|N(v)\right|} \\ 0, \text{ with probability } \dfrac{\left|\left\{u \in N(v) : f_t(u) = 0\right\}\right|}{\left|N(v)\right|} \end{cases}$$

The budget is bounded from above by a constant *B*, the cost of the initial "persuasion" $f_0(v)=1$ of agent *v* is c_v. Thus, the problem of maximizing influence is formulated as follows: f_0: $N \rightarrow 0; 1\}$ maximizing the mathematical expectation $E[\sum_{v \in N} f_t(v)]$ for a given budget constraint $\sum_{\{v | f\,0(v)=1\}} c_v \le B$.

5. Conclusions

The paper considers the dynamic processes of forming opinions in a social network, and also presents models and algorithms for identifying critical points of a social network (influencing agents), the impact on which allows manipulating the aggregate opinion of network participants forming a social network, as well as the resulting game-theoretic problems information confrontation.

6. References

[1] *Watts D., Dodds P.* Influentials, Networks, and Public Opinion Formation // Journal of Consumer Research. — December, 2007. — P. 123—134.

[2] *Granovetter M.* Threshold Models of Collective Behavior // The American Journal of Sociology. — 1978. — Vol. 83, N 6. — P. 1420—1443.

[3] *Kempe D., Kleinberg J., Tardos E.* Maximizing the Spread of Influence through a Social Network / Proc. of the 9-th ACM SIGKDD Intern. Conf. on Knowledge Discovery and Data Mining, Washington, DC, 2003. — P. 137—146.

[4] *Morris S.* Contagion // The Review of Economic Studies. — 2000. — Vol. 67, N 1. — P. 57—78.

[5] *Goldenberg J., Libai B., Muller E.* Talk of the network: A complex systems look at the underlying process of word-of-mouth // Marketing Letters. — 2001. — N 2. — P. 11—34.

[6] D. A. Gubanov, D. A. Novikov, A. G. Chkhartishvili, "Models of influence in

social networks", UBS, 27 (2009), 205–281 (Д. А. Губанов, Д. А. Новиков, А. Г. Чхартишвили, "Модели влияния в социальных сетях", *УБС*, **27** (2009), 205–281).

[7] GRANOVETTER M. *The Strength of Weak Ties* // American Journal of Psychology. – 1973. – №78(6). – P. 1360-1380.

[8] BURT R. S. *Brokerage and Closure*. – Oxford: Oxford University Press, 2005.

[9] DOMINGOS P., RICHARDSON M. *Mining the Network Value of Customers* / Proceedings of the Seventh International Confer- ence on Knowledge Discovery and Data Mining. 2002. P. 57-66.

[10] KEMPE D., KLEINBERG J., TARDOS E. *Maximizing the Spread of Influence through a Social Network* / Proceedings of the 9-th ACM SIGKDD International Conference on Knowledge Discovery and Data Mining. – 2003. – P. 137-146.

[11] CARNES T., NAGARAJAN C., WILD S. M., ZUYLEN A. *Maximizing Influence in a Competitive Social Network: A Follower's Perspective* / Proceedings of the Ninth International Conference on Electronic Commerce. – 2007. – P. 351-360.

[12] EVENDAR E., SHAPIRA A. *A Note on Maximizing the Spread of Influence in Social Networks* / Internet and Network Economics. – 2007. – P. 281-286

Application Of Greedy Algorithms On Classes (ψ, β) – differentiable Periodic Functions In Lebesgue Spaces For Optimization Problems

Iryna Zamrii [1], Viktoriya Shkapa [1], Valentyn Sobchuk [1] and Hanna Vlasyk [1]

[1] *State University of Telecommunications, 7, Solomyanska str., Kyiv, 03110, Ukraine*

Abstract

Many problems in economics, industry, science, as well as the problems of managing complex technical objects lead to the need to solve optimization problems. The problem of constructing algorithms for the approximate solution of optimization problems is of considerable interest. To do this, the properties of the space of variables are investigated and the regularities of the behavior of functions in this space are revealed. The paper describes the application of greedy algorithms to obtain estimates of functions in special classes. Sparse representations of a function are not only a powerful analytical tool, but they are used in many areas, such as image processing, signal processing, numerical computing, directly in optimization problems, as they significantly increase the ability to process large data sets. The key to the search for sparse representations is the concept of m-term approximation of the objective function by the elements of this system of functions. A universal method that allows this is the greedy algorithm, the principle of which is to use the greedy step in search of a new element to be added to this m-term approximation. In this work, using approximations by greedy algorithms (ψ, β)-differentiable functions in Lebesgue spaces, the exact order estimates under conditions $1 < p < q \leq 2, 1 < p \leq 2 \leq q < \infty$ and $2 \leq \mathrm{p} \leq \mathrm{q} < \infty$ were found. The estimates obtained allow us to effectively use mathematical models that describe the routes between atomic nodes of the system, which require the use of (ψ, β)-differentiable functions in the space L_q, in optimization problems.

Keywords

(ψ, β) −derivative, greedy approximation, greedy algorithms, best approximations, optimization problem

1. Introduction

The solution of most real problems in the field of decision-making requires the formalization of the situation when the choice should be made, in the form of an optimization problem of a certain class. The optimal choice of one of several valid alternatives according to a certain criterion corresponds to the assignment of variables to specific values from the range of acceptable values. Often variables can take only one of two values - zero or one. The corresponding problems are called optimization problems with Boolean variables or pseudo-Boolean optimization problems. This issue has been actively studied in recent years in the works of many scientists [1-11]. This approach allows to obtain good results for adaptive algorithms for optimal prefix coding of the alphabet with minimal redundancy, algorithms for finding a minimum weight spanning tree in a graph and finding a minimum weight spanning tree in a connected graph, and so on.

In essence, these are greedy algorithms, which implement the following principles: at each step of the algorithm we abstract from the previous and next steps and think only about the optimal solution at this stage. The approach does not provide for the cancellation of the choice already made (return to previous steps) and does not predict anything for the future; the speed of

EMAIL: irinafraktal@gmail.com (A. 1); vshkapa@ukr.net (A. 2); v.v.sobchuk@gmail.com (A. 3); annawlasik@gmail.com (A. 4)
ORCID: 0000-0001-5681-1871 (A. 1); 0000-0003-3591-7583 (A. 2); 0000-0002-4002-8206 (A. 3); 0000-0002-0680-4128 (A. 4)

program execution is easy to predict, because the complexity of the algorithm is linear. However, it is necessary to understand when this approach can be used and when not. Even if the greedy algorithm gives the optimal solution in certain cases, it is difficult to prove that the approach will work in all other possible cases.

Most known optimization methods involve specifying objective functions and constraints in the form of algebraic expressions, while in many real problems some or all functions are given, algorithmically, which makes it impossible to apply standard algorithms to them; and requires the development of search engine optimization procedures and their evaluation. At the same time, the analysis of many practical problems, to the solution of which greedy algorithms can be applied, allows to reveal in them some features in the form of constructive properties, inherent both in objective functions, and the restriction imposed by the conditions of the problem. It should also be noted that when solving a specific problem, it is useful to have information about the effectiveness of algorithms, which allows you to get the result with the appropriate accuracy.

Often, when solving practical problems, the researcher deals with a specific problem statement. This paper aims to evaluate the solutions of a class of problems described by certain classes of (ψ,β) −differentiable functions. The study of these functions is of particular practical interest, for example, for problems in the description of which models are used, which to describe the routes between the atomic nodes of the system require the use of classes of (ψ,β) − differentiable functions.

Before proceeding to the presentation of the main results, we present necessary notations and we will give definitions of the approximate characteristic which will be investigated.

Let L_q be the space of 2π −periodic functions f summable to a power q, $1 \le q < \infty$ (resp., essentially bounded for $q = \infty$), on the segment $[-\pi,\pi]$. The norm in this space is defined as follows:

$$\| f \|_{L_q} = \| f \|_q =$$
$$= \begin{cases} \left(\frac{1}{2\pi} \int_{-\pi}^{\pi} |f(x)|^q dx \right)^{\frac{1}{q}}, & 1 \le q < \infty, \\ \operatorname{esssup}_{x\in[-\pi,\pi]} |f(x)|, & q = \infty. \end{cases}$$

For a function $f \in L_1$, we consider its Fourier series

$$\sum_{k\in\mathbb{Z}} \hat{f}(k) e^{ikx},$$

where

$$\hat{f}(k) = \frac{1}{2\pi} \int_{-\pi}^{\pi} f(x) e^{-ikx} dx$$

are the Fourier coefficients of the function f. In what follows, we always assume that the function $f \in L_1$ satisfies the condition

$$\int_{-\pi}^{\pi} f(x) dx = 0.$$

Further, let $\psi \neq 0$, be an arbitrary function of natural argument and let β be an arbitrary fixed real number. If a series

$$\sum_{k\in\mathbb{Z}\setminus\{0\}} \frac{\hat{f}(k)}{\psi(|k|)} e^{i(kx+\beta\frac{\pi}{2}\operatorname{sign} k)}$$

is the Fourier series of a summable function, then, following Stepanets [12] we can introduce the (ψ,β)–derivative of the function f and denote it by f_β^ψ. By L_β^ψ we denote the set of functions f satisfying this condition. In what follows we assume that the function f belongs to the class $L_{\beta,p}^\psi$ if $f \in L_{\beta,p}^\psi$ and

$$f_\beta^\psi \in U_p = \{\varphi : \varphi \in L_p, \| \varphi \|_p \le 1\},$$
$$1 \le p \le \infty.$$

If

$$\psi(|k|) = |k|^{-r},\ r > 0,\ k \in \mathbb{Z}\setminus\{0\},$$

then the (ψ,β)–derivative of the function f coincides with its (r,β)–derivative (denoted by f_β^r) in the Weyl–Nagy sense.

We give definition of the greedy approximation under investigation. Let $\{\hat{f}(k(l))\}_{l=1}^{\infty}$ — the Fourier coefficients $\{\hat{f}(k)\}_{k\in\mathbb{Z}}$ of the function $f \in L_1$, that are arranged in non-increasing order of their absolute value, i.e

$$|\hat{f}(k(1))| \ge |\hat{f}(k(2))| \ge \ldots$$

Denote for $f \in L_q$

$$G_m(f,x) = \sum_{l=1}^{m} \hat{f}(k(l)) e^{ik(l)x}$$

and if $F \subset L_q$ is a certain function class, then we set

$$G_m(F)_q := \sup_{f\in F} \| f(\cdot) - G_m(f,\cdot) \|_q. \quad (1)$$

At present, there are many works devoted to the investigation of quantity (1) for important classes of functions. For details and the corresponding references, see, e.g., [13, 14].

By B we denote the set of functions ψ, satisfying the following conditions:

1) ψ — are positive and nonincreasing;
2) there exists a constant $C > 0$ such that

$$\frac{\psi(\tau)}{\psi(2\tau)} \le C, \quad \tau \in \mathbb{N}.$$

Thus, the functions $\frac{1}{\tau^r}, r > 0$; $\frac{\ln^\gamma(\tau+1)}{\tau^r}, \gamma \in \mathbb{R}$, $r > 0, \tau \in \mathbb{N}$, and some other functions belong to the set B.

For the quantities A and B, the notation $A \asymp B$ means that there exist positive constants C_1 and C_2 such that $C_1 A \le B \le C_2 A$. If $B \le C_2 A$ $(B \ge \ge C_1 A)$, than we can write $B \ll A$ $(B \gg A)$. All C_i, $i = 1,2,\ldots$, encountered in our paper may depend only on the parameters appearing in the definitions of the class and metric in which we determine the error of approximation.

2. Main results

The following assertion is true:

Theorem 1. Let $\mathbf{1 < p < q \le 2}$, $\boldsymbol{\psi} \in \boldsymbol{B}$, $\boldsymbol{\beta} \in \mathbb{R}$ and let, in addition, there exist $\boldsymbol{\varepsilon > 0}$ such that the sequence $\boldsymbol{\psi(t)t^{\frac{1}{p}-\frac{1}{q}+\varepsilon}}$, $\boldsymbol{t} \in \mathbb{N}$, does not increase. Then the following order estimate is true:

$$G_m(L^{\psi}_{\beta,p})_q \asymp \psi(m)m^{\frac{1}{p}-\frac{1}{2}}.$$

Proof. The upper bounds follow from the estimate for the approximation of functions from the classes $L^{\psi}_{\beta,p}$ by their Fourier sums [15, p. 215]:

$$\mathcal{E}_m(L^{\psi}_{\beta,p})_2 =$$

$$= \sup_{f \in L^{\psi}_{\beta,p}} \| f(x) - \sum_{k=-m}^{m} \hat{f}(k)e^{ikx} \|_2 \asymp$$

$$\asymp \psi(m)m^{\frac{1}{p}-\frac{1}{2}}.$$

We now determine the lower bounds. We will use the Rudin-Shapiro polinomials $\mathcal{R}_l(x)$:

$$\mathcal{R}_l(x) = \sum_{j=2^{l-1}}^{2^l-1} \varepsilon_j e^{ijx},$$

$$\varepsilon_j = \pm 1, \quad x \in \mathbb{R},$$

satisfying the order estimate (see, e.g., [16, p. 155])

$$\| \mathcal{R}_l \|_\infty \ll 2^{\frac{l}{2}}.$$

We also need the well-known de la Vallee-Poussin kernels

$$V_m(x) = \frac{1}{m} \sum_{l=m}^{2m-1} D_l(x),$$

$x \in \mathbb{R}$, $m \in \mathbb{N}$, where

$$D_l(x) = \sum_{|k| \le l} e^{ikx}$$

is the Dirichlet kernel.

Further, we set for

$$\varepsilon = \pm 1 \ \Lambda_{\pm 1} := \{k : \hat{\mathcal{R}}_l(k) = \pm 1\},$$

and let $\varepsilon = \pm 1$ will be such that

$$|\Lambda_\varepsilon| > |\Lambda_{-\varepsilon}|.$$

Then for given m, we take $l \in \mathbb{N}$ from the relation $2^{l-2} \le m < 2^{l-1}$, take a small positive parameter δ and consider a function

$$f(x) = C_3 \psi(2^l) 2^{l\left(\frac{1}{p}-1\right)} f_1(x), \quad C_3 > 0,$$

where

$$f_1(x) = V_m(x) + \varepsilon\delta\mathcal{R}_m(x),$$

$$0 < \delta \le m^{\frac{1}{2}-\frac{1}{p}}.$$

We now show that, for a certain choice of the constant $C_3 > 0$, the function f belongs to the class $L^{\psi}_{\beta,p}$. To this end, it suffices to verify that

$$\| f^{\psi}_{\beta} \|_p \ll 1.$$

For this purpose, we use the estimate [17]

$$\| t^{\psi}_{\beta} \|_p \ll \psi^{-1}(n) \| t \|_p \qquad (2)$$

(for any polynomial $t \in T_n$, $1 < p < \infty$), and the well-known relation (see, e.g., [18, p. 66])

$$\| V_{2^l} \|_p \asymp 2^{l\left(1-\frac{1}{p}\right)}, \ 1 \le p \le \infty. \qquad (3)$$

Hence, we can write

$$\| f^{\psi}_{\beta} \|_p \ll \psi^{-1}(m) \| f \|_p \le$$

$$\le \psi^{-1}(m)\psi\left(2^l\right)2^{l\left(\frac{1}{p}-1\right)} \cdot$$

$$\cdot \left(\| V_m \|_p + \delta \| \mathcal{R}_m \|_p\right) \le$$

$$\le \psi^{-1}(m)\psi(2^l)2^{l\left(\frac{1}{p}-1\right)} \cdot$$

$$\cdot \left(\| V_m \|_p + \delta \| \mathcal{R}_m \|_\infty\right) \ll$$

$$\ll \psi^{-1}(m)\psi(2^l)2^{l\left(\frac{1}{p}-1\right)} \cdot$$

$$\cdot \left(2^{l\left(1-\frac{1}{p}\right)} + 2^{l\left(\frac{1}{2}-\frac{1}{p}\right)}2^{\frac{l}{2}}\right) \ll 1.$$

This implies that, for a proper choice of the constant $C_3 > 0$, function $f \in L^{\psi}_{\beta,p}$.

By using the estimate (see, e.g., [14], p. 581) for $1 \le q \le 2$ and $1 < p \le 2$

$$\| f_1 - G_m(f_1) \|_q \gg m^{\frac{1}{2}},$$

we obtain

$$\sup_{f \in L^{\psi}_{\beta,p}} \| f - G_m(f) \|_q \gg \psi(2^l)2^{l\left(\frac{1}{p}-1\right)} \cdot$$

$$\| f_1 - G_m(f_1) \|_q \gg$$

$$\gg \psi(m)m^{\frac{1}{p}-1}m^{\frac{1}{2}} = \psi(m)m^{\frac{1}{p}-\frac{1}{2}}.$$

The required lower bound is established, which proves the theorem.

Theorem 2. Let $\mathbf{1 < p \le 2 \le q < \infty}$, $\boldsymbol{\psi} \in \boldsymbol{B}$, $\boldsymbol{\beta} \in \mathbb{R}$ and let, in addition, there exist $\boldsymbol{\varepsilon > 0}$ such

that the sequence $\boldsymbol{\psi(t)t^{\frac{1}{p}+\varepsilon}}$, $\boldsymbol{t\in\mathbb{N}}$, does not increase. Then the following order estimate is true:

$$G_m(L^{\psi}_{\beta,p})_q \asymp \psi(m)m^{\frac{1}{p}-\frac{1}{q}}.$$

Proof. The upper bound follows from the following inequality

$$\| f-G_m(f)\|_q \le \le \left(1+3m^{\left|\frac{1}{2}-\frac{1}{q}\right|}\right)e_m(f)_q,$$

$1\le q\le\infty$, (see [14]), and the estimate

$$e_m(L^{\psi}_{\beta,p})_q = \sup_{f\in L^{\psi}_{\beta,p}}\inf_{\Theta_m}\inf_{T(\Theta_m,\cdot)}\| f(\cdot)-T(\Theta_m,\cdot)\|_q \asymp \asymp \psi(m)m^{\frac{1}{p}-\frac{1}{2}},$$

$$1<p\le 2\le q<\infty,$$

where

$$T(\Theta_m,x)=\sum_{k=1}^{m}c_k e^{in_k x},$$

Θ_m is a set of m integers $n_1,\dots,n_m$ and c_k are arbitrary complex numbers (see [19]).

$$\| f-G_m(f)\|_q \le \le (1+3m^{\frac{1}{2}-\frac{1}{q}})e_m(f)_q \ll \ll m^{\frac{1}{2}-\frac{1}{q}}\psi(m)m^{\frac{1}{p}-\frac{1}{2}}=\psi(m)m^{\frac{1}{p}-\frac{1}{q}}.$$

Therefore

$$G_m(L^{\psi}_{\beta,p})_q \ll \psi(m)m^{\frac{1}{p}-\frac{1}{q}}. \quad (4)$$

We now determine the lower bounds. For given m we take $l\in\mathbb{N}$ from the relation $2^{l-1}\le m<2^l$ and consider a function

$$f_2(x)=C_4\psi(2^l)2^{l\left(\frac{1}{p}-1\right)}V_{2^l}(x),\quad C_4>0.$$

It is easy to see that the function f_2 belongs to $L^{\psi}_{\beta,p}$. Indeed, according to relations (2) and (3), we can write

$$\| (f_2)^{\psi}_{\beta}\|_p \ll \psi^{-1}(m)\| f_2\|_p \ll \ll \psi^{-1}(m)\psi(2^l)2^{l\left(\frac{1}{p}-1\right)}2^{l\left(1-\frac{1}{p}\right)}=1.$$

This implies that, for the proper choice of the constant $C_4>0$, the function f_2 belongs to $L^{\psi}_{\beta,p}$.

Using the inequality of different metrics, we obtain the ratio

$$\| T_n\|_p \ll n^{\frac{1}{q}-\frac{1}{p}}\| T_n\|_q,\quad 1\le q\le p\le\infty,$$

we obtain the ratio

$$\| V_{2^l}-G_m(V_{2^l})\|_q \gg \gg m^{-\frac{1}{q}}\| V_{2^l}-G_m(V_{2^l})\|_{\infty}\gg \gg m^{1-\frac{1}{q}}. \quad (5)$$

Therefore, given (5), we will have

$$\sup_{f_2\in L^{\psi}_{\beta,p}}\| f_2-G_m(f_2)\|_q \gg \gg \psi(2^l)2^{l\left(\frac{1}{p}-1\right)}\| f_2-G_m(f_2)\|_q \gg \gg \psi(m)m^{\frac{1}{p}-1}m^{1-\frac{1}{q}}= =\psi(m)m^{\frac{1}{p}-\frac{1}{q}}.$$

Thus for

$$1<p\le 2\le q<\infty$$

we obtain

$$G_m(L^{\psi}_{\beta,p})_q \asymp \psi(m)m^{\frac{1}{p}-\frac{1}{q}}.$$

The estimate from below, and with it Theorem 2, is proved.

Theorem 3. Let $2\le p\le q<\infty$, $\psi\in B$, $\beta\in\mathbb{R}$ and let, in addition, there exist $\varepsilon>0$ such that the sequence $\psi(t)t^{\frac{1}{2}+\varepsilon}$, $t\in\mathbb{N}$, does not increase. Then the following order estimate is true:

$$G_m(L^{\psi}_{\beta,p})_q \asymp \psi(m)m^{\frac{1}{2}-\frac{1}{q}}.$$

Proof. We first establish the upper bound. Since

$$L^{\psi}_{\beta,p}\subset L^{\psi}_{\beta,2},$$

then

$$G_m(L^{\psi}_{\beta,p})_q \le G_m(L^{\psi}_{\beta,2})_q$$

and therefore, taking into account the ratio (4) for $p=2$, we obtain the upper bounds

$$G_m(L^{\psi}_{\beta,p})_q \ll \psi(m)m^{\frac{1}{2}-\frac{1}{q}}.$$

To set the upper bound for given m we take $l\in\mathbb{N}$ so that the relation is fulfilled $m\asymp 2^l$, we will take small positive parameter δ and consider a function

$$f_3(x)=C_5\psi(2^l)2^{-\frac{l}{2}}f_4(x),$$

where

$$f_4(x):=\mathcal{R}_m(x)+\varepsilon\delta D_m(x),\quad 0<\delta\le m^{\frac{1}{p}-\frac{1}{2}}.$$

We now show that, for a certain choice of the constant $C_5>0$, the function f_3 belongs to the class $L^{\psi}_{\beta,p}$.

For this purpose, it suffices to check that

$$\| (f_3)^{\psi}_{\beta}\|_p \ll 1.$$

To this end, we use (2) and the known relation (see, e.g., [20, p. 155])

$$\| D_{2^l}\|_p \asymp 2^{l\left(1-\frac{1}{p}\right)},\qquad 1<p<\infty.$$

So we will have

$$\| (f_3)^{\psi}_{\beta}\|_p \ll \psi^{-1}(m)\| f_3\|_p \le \le \psi^{-1}(m)\psi(2^l)2^{-\frac{l}{2}}\cdot \cdot\left(\| \mathcal{R}_m\|_p+\delta\| D_m\|_p\right)\le$$

$$\leq \psi^{-1}(m)\psi\left(2^{l}\right)2^{-\frac{l}{2}}\cdot$$
$$\cdot\left(\| \mathcal{R}_m \|_{\infty}+\delta \| D_m \|_{p}\right)\ll$$
$$\ll \psi^{-1}(m)\psi\left(2^{l}\right)2^{-\frac{l}{2}}\cdot$$
$$\cdot\left(2^{\frac{l}{2}}+2^{l\left(\frac{1}{p}-\frac{1}{2}\right)}2^{l\left(1-\frac{1}{p}\right)}\right)\ll 1.$$

This implies that, for a proper choice of the constant $C_5 > 0$, the function f_3 belongs to the class $L_{\beta,p}^{\psi}$.

Further, use the estimate set in [14, p. 582]:

$$\| f_4 - G_m(f_4) \|_q \gg m^{1-\frac{1}{q}}, \quad 2 \leq q \leq \infty.$$

Taking into account this ratio, we will have

$$\sup_{f_3 \in L_{\beta,p}^{\psi}} \| f_3 - G_m(f_3) \|_q \gg$$
$$\gg \psi(2^{l})2^{-\frac{l}{2}} \| f_4 - G_m(f_4) \|_q \gg$$
$$\gg \psi(m)m^{-\frac{1}{2}}m^{1-\frac{1}{q}} = \psi(m)m^{\frac{1}{2}-\frac{1}{q}}.$$

Thus for

$$2 \leq p \leq q < \infty$$

we obtain

$$G_m(L_{\beta,p}^{\psi})_q \asymp \psi(m)m^{\frac{1}{2}-\frac{1}{q}}.$$

The lower bound is established. This completes the proof of the theorem.

Remark. The assertion of Theorems for a special case of the classes $W_{p,\beta}^{r}$ were established by Temlyakov [21].

3. Conclusions

The possibilities of precise methods are very limited, especially when solving large-scale problems. For many classes of discrete optimization problems that occur in practice, no effective (polynomial) exact algorithms have been developed. In addition, the use of regular algorithms is possible only in the presence of a priori information about the properties of the target functional. This leads to the need to develop and study approximate algorithms to obtain the necessary solution. Because if the dimension is close to the hundredth step, then the exact algorithm is no longer able to find a solution in real time. This paper proposes the use of a greedy algorithm, the essence of which is to select the next element at each step in an optimal way, to effectively solve problems of optimization of functions in the presence of constraints. In particular, we obtain the exact order estimates of approximations by greedy algorithms of the classes $L_{\beta,p}^{\psi}$ of periodic functions in the space L_q for some relations between parameters p and q. Using approximation by greedy algorithms (ψ, β) - differentiable functions in Lebesgue spaces, the exact order estimates under conditions $1 < p < q \leq 2$, $1 < p \leq 2 \leq q < \infty$ and $2 \leq \mathrm{p} \leq \mathrm{q} < \infty$ were found. The estimates obtained allow us to effectively use mathematical models that describe the routes between atomic nodes of the system, which require the use of (ψ,β)-differentiable functions in the space L_q, in optimization problems.

4. References

[1] S. Yevseiev, R. Korolyov, A. Tkachov,O. Laptiev, I. Opirskyy, O. Soloviova, Modification of the algorithm (OFM) S-box, which provides increasing crypto resistance in the post-quantum period, International Journal of Advanced Trends in Computer Science and Engineering (IJATCSE) 9 (2020) 8725-8729. doi:10.30534/ijatcse/2020/261952020

[2] O. Barabash, O. Laptiev, O. Kovtun, O. Leshchenko, K. Dukhnovska, A. Biehun, The Method dynavic TF-IDF, International Journal of Emerging Trends in Engineering Research (IJETER) 8 (2020) 5713-5718. doi:10.30534/ijeter/2020/130892020

[3] O. Barabash, O. Laptiev, V. Tkachev, O. Maystrov, O. Krasikov, I. Polovinkin, The Indirect method of obtaining Estimates of the Parameters of Radio Signals of covert means of obtaining Information, International Journal of Emerging Trends in Engineering Research (IJETER) 82020, Indexed- ISSN: 2278 – 3075, 4133 – 4139. doi:10.30534/ijeter/2020/17882020

[4] V. Savchenko, O. Ilin, N. Hnidenko, O.Tkachenko, O. Laptiev, S. Lehominova, Detection of Slow DDoS Attacks based on User's Behavior Forecasting, International Journal of Emerging Trends in Engineering Research (IJETER) 8 (2020) 2019 – 2025. doi:10.30534/ijeter/2020/90852020

[5] O. Laptiev, O. Stefurak, I. Polovinkin, O. Barabash, S. Vitalii, O. Zelikovska, The method of improving the signal detection quality by accounting for interference, 2020 IEEE 2nd International Conference on Advanced Trends in Information Theory (IEEE ATIT 2020) Conference Proceedings Kyiv, Ukraine, 2020, pp. 172 –176.

doi:10.1109/ATIT50783.2020.9349259

[6] O. Laptiev, V. Savchenko, S. Yevseiev, H. Haidur, S. Gakhov, S. Hohoniants, The new method for detecting signals of means of covert obtaining information, 2020 IEEE 2nd International Conference on Advanced Trends in Information Theory (IEEE ATIT 2020) Conference Proceedings Kyiv, Ukraine, 2020, pp. 176 –181. doi:10.1109/ATIT50783.2020.9349322

[7] V. Sobchuk, V. Pichkur, O. Barabash, O. Laptiev, I. Kovalchuk, A. Zidan, Algorithm of control of functionally stable manufacturing processes of enterprises, 2020 IEEE 2nd International Conference on Advanced Trends in Information Theory (IEEE ATIT 2020) Conference Proceedings Kyiv, Ukraine, 2020, pp. 206 –211. doi:10.1109/ATIT50783.2020.9349332

[8] V. Savchenko, O. Laptiev, O. Kolos, R. Lisnevskyi, V. Ivannikova, I. Ablazov, Hidden Transmitter Localization Accuracy Model Based on Multi-Position Range Measurement, 2020 IEEE 2nd International Conference on Advanced Trends in Information Theory (IEEE ATIT 2020) Conference Proceedings Kyiv, Ukraine, 2020, pp. 246 –251. doi:10.1109/ATIT50783.2020.9349304

[9] I. Zamrii, M. Prats'ovytyi, Singularity of the Digit Inversor for the Q_3-Representation of the Fractional Part of a Real Number, Its Fractal and Integral Prorerties, Journal of Mathematical Sciences 215 (2016) 323–340. doi:10.1007/s10958-016-2841-y

[10] O. Barabash, O. Kopiika, I. Zamrii, V. Sobchuk, A. Musienko, Fraktal and Differential Properties of the Inversor of Digits of Q_s-Representation of Real Number, Modern Mathematics and Mechanics. Fundamentals, Problems and Challenges. Springer International Publishing AG (2019) 79 – 95. doi: 10.1007/978-3-319-96755-4_5

[11] H. M. Vlasyk, V. V. Shkapa, I. V. Zamrii, Estimates of the best orthogonal trigonometric approximations and orthoprojective widths of the classes of periodic functions of many variables in a uniform metric, Journal of Mathematical Sciences 246 (2020) 110-119. doi:10.1007/s10958-020-04725-0

[12] A. I. Stepanets', Methods of Approximation Theory. Vols. 1,2, Institute of Mathematics, Ukrainian National Academy of Sciences, Kyiv, 2002.

[13] V. N. Temlyakov, Greedy approximation, Cambridge, Cambridge University Press, 2011. doi: 10.1017/CBO9780511762291

[14] V. N. Temlyakov, Greedy algorithm and m-term trigonometric approximation, Constr. Approx 14 (1998) 569-587.

[15] A. I. Stepanets, Classification and Approximation of Periodic Functions [in Russian], Naukova Dumka, Kiev (1987).

[16] B. S. Kashin, A. A. Sahakyan, Orthogonal series [in Russian], M .: Science, 1984.

[17] A. S. Romanyuk, Inequalities for the L_p - norms of (ψ,β)-derivatives and Kolmogorov widths of the classes of functions of many variables $L^{\psi}_{\beta,p}$, in: Investigations in the Approximation Theory of Functions [in Russian], Proc. of the Institute of Mathematics, Academy of Sciences of Ukr. SSR, Kiev (1987), 92–105.

[18] V. N. Temlyakov, Approximation of functions with bounded mixed derivative, Tr. Mat. Inst. Akad. Nauk SSSR, 178 (1986).

[19] A. S. Fedorenko, On the best m-term trigonometric approximations of classes of $(\varphi;\beta)$-differentiable functions of one variable, Boundary value problems for differential equations: Coll. Science. pr. - Kyiv: Inst. of Mathematics of the National Academy of Sciences of Ukraine, 3 (1998), 250 - 258.

[20] V. N. Temlyakov, Approximation of periodic functions, New York: Nova Sc. Publ. Inc, 1993.

[21] V. N. Temlyakov, Greedy algorithms with regard to multivariate systems with special structure, Constr. Approx. 16 (2000) 399 – 425.

Evaluation of Cryptographic Strength and Energy Intensity of Design of Modified Crypto-Code Structure of McEliece with Modified Elliptic Codes

Serhii Yevseiev [1], Olha Korol [2], Olga Veselska [3], Serhii Pohasii [4],Vladyslav Khvostenko [5]

[1,2,4,5] *Simon Kuznets Kharkiv National University of EconomicsUniversity, Nauky ave., 9-A, Kharkiv, 61166, Ukraine*
[3] *Akademia Techniczno-Humanistyczna, ul. Willowa 2, Bielsku-Białej, 43309, Poland*

Abstract

The computing development in the post-quantum cryptography era puts forward new requirements for cryptographic mechanisms for providing basic security services. The advent of a full-scale quantum computer casts doubt on the cryptographic strength of cryptosystems based on symmetric cryptography and public-key cryptography. One of the promising areas in the opinion of US NIST experts is the use of crypto-code constructions (crypto-code schemes or code-theoretic schemes) by McEliece or Niederreiter. The construction allows one integrated mechanism to provide the basic requirements for cryptosystems - cryptographic stability, speed of cryptoconversion and besides - reliability based on the use of noise-resistant coding. However, their use is difficult due to the large volume of power of the alphabet, and the possibility of hacking based on Sidelnikov's attack. The paper proposes to use non-cyclic noise-resistant codes on elliptic curves in a modified McEliece cryptosystem that are not susceptible to Sidelnikov's attack. The main criteria for constructing a modified crypto code based on the McEliece scheme on elongated elliptic codes are investigated. It is proposed to reduce the energy intensity in the proposed crypto-code design by reducing the power of the Galois field while ensuring the level of cryptographic stability of the modified cryptosystem as a whole with its software implementation. To reduce the field power, it is proposed to use modified elliptic codes, which allows to reduce the field power by 2 times. A comparative assessment of the performance of cryptosystems is carried out. The results of statistical stability studies based on the NIST STS 822 package confirm the cryptographic strength of the proposed cryptosystem on modified elongated elliptic codes. It is proposed to use the method of evaluating the cryptographic strength of various cryptosystems based on the entropy approach.

Keywords

Asymmetric McEliece Crypto-Code System, Crypto-Code Construction on Algebro-geometric Codes, Modified (extended) Elliptic Codes, Confidentiality, Integrity.

1. Introduction

The rapid growth of the volume of data being processed and the development of computing technology has put forward new requirements for reliability and data security. Studies on the influence of quantum computing using quantum superposition and quantum entanglement to transmit and process data have shown that quantum computers that use special algorithms (for example, Shor's algorithm) will be able to factorize numbers in polynomial time [1], [2]. Thus, RSA, ECC, DSA cryptographic systems will be vulnerable to brute force attacks using a full-scale quantum computer. Therefore, the main research and development of cryptographic information security tools (CIST) are currently

EMAIL: serhii.yevseiev@hneu.net (A. 1); olha.korol@hneu.net (A. 2); oveselska@ath.bielsko.pl (A. 3); spogasiy1978@gmail.com (A. 4); vladyslav.khvostenko@gmail.com (A. 5)
ORCID: 0000-0003-1647-6444 (A. 1); 0000-0002-8733-9984 (A. 2); 0000-0002-4914-2187 (A. 3); 0000-0002-4540-3693 (A. 4); 0000-0000-0000-1234 (A. 5)

aimed at finding solutions that confront quantum computing and at the same time must be resistant to attacks using ordinary computers. Such algorithms are related to the section of quantum-resistant cryptography (quantum secure cryptography or quantum-resistant cryptography) [3], [4]. Through the imminent emergence of new schemes, sufficient attention has not been paid to the well-known, asymmetric crypto-code systems (ACCS) based on McEliece's theoretical code schemes (TCS), which are also quantum-stable.

The advent of a full-scale quantum computer casts doubt on the cryptographic strength of cryptosystems based on symmetric cryptography and public-key cryptography. One of the promising areas in the opinion of US NIST experts is the use of crypto-code constructions (crypto-code schemes or code-theoretic schemes) by McEliece or Niederreiter. The construction allows one integrated mechanism to provide the basic requirements for cryptosystems – cryptographic stability, speed of cryptoconversion Pand besides – reliability based on the use of noise-resistant coding.

The analysis showed that for the provision of basic security services, crypto-code constructions are usually used based on the McEliece and Niederreiter schemes. To ensure the level of cryptographic strength in post-quantum cryptography, it is necessary to use the power of the alphabet in a field of 210-213 degrees, which is a significant drawback of their practical application [4]. Even at the current level of computer technology, this is a rather difficult task.

The second drawback is the hacking attack on the McEliece scheme based on linear-fractional transformations and the property of triply transitivity of the automorphism groups of the generalized Reed-Solomon code, proposed in the work of professor Sidelnikov from Moscow State University. The essence of which is to find the elements of the generating matrix and remove the action of masking matrices [4].

The orthogonality of the matrices, which is generative and test, allows us to consider the effectiveness of the attack on the Niederreiter scheme. A promising way to eliminate the identified patterns Sidelnikov proposes to use cascade or algebraic geometry codes – codes built based on the algebra of the theory of noise-resistant coding and geometric parameters of the curve, in particular elliptic curves.

The algebraic-geometric code uses the mathematical apparatus of noise-resistant coding and the parameters of the spatial curve. This allows us to provide resistance to Sidelnikov's attack and proper (n, k, d) parameters of the error-correcting code, which, under equal conditions of length n, provides bigger values of the d and k parameters (allows to transmit more characters in open text and correct more errors)

The paper proposes to use non-cyclic noise-resistant codes on elliptic curves in a modified McEliece cryptosystem that are not susceptible to Sidelnikov's attack. The main criteria for constructing a modified crypto code based on the McEliece scheme on elongated elliptic codes are investigated. It is proposed to reduce the energy intensity in the proposed crypto-code design by reducing the power of the Galois field while ensuring the level of cryptographic stability of the modified cryptosystem as a whole with its software implementation. To reduce the field power, it is proposed to use modified elliptic codes, which allows to reduce the field power by 2 times. A comparative assessment of the performance of cryptosystems is carried out. The results of statistical stability studies based on the NIST STS 822 package confirm the cryptographic strength of the proposed cryptosystem on modified elongated elliptic codes.

2. Analysis of Recent Studies and Publications

The main advantage of symmetric and asymmetric Crypto-Code Systems (CCS) is the high speed of information conversion and the integrated provision of reliability and information concealment (confidentiality) that satisfies the basic security requirements.

For security reasons, the perspective direction is the use of asymmetric cryptosystems based on CCS McEliece integrated (with one mechanism) providing reliability values at the level of 29 – 212 and cryptostability 230 – 235 group operations when constructed over the field GF(210).

Figure 1 shows the classification of crypto-code structures and the provision of basic security services.

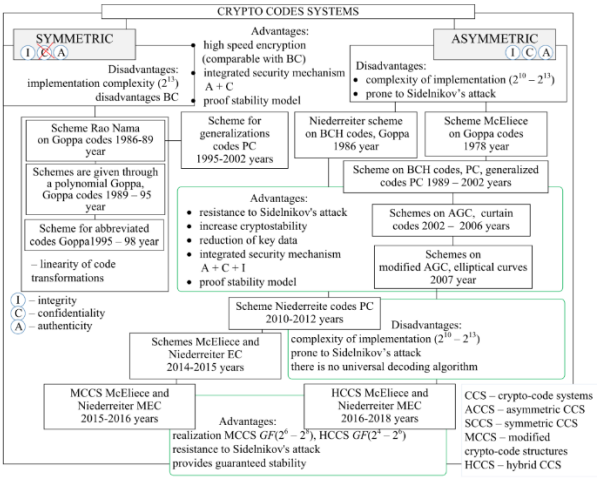


Figure 1: Classification of crypto-code constructions

The main advantage of which is the provision of cryptographic stability, efficiency and reliability in the transmission of information in the post-quantum period.

Table 1 shows the results of comparative studies of the effectiveness of cryptographic information security methods at a fixed level of stability.

Table 1

Results of comparative researches of efficiency of cryptographic methods of information security at the fixed stability level

Methods of cryptographic transformation	Security model	Key length [bits	Speed of cryptographic transitions, [bits/sec	Additional features
Block symmetric ciphers	Practical security	128, 256, 512	$10^6 – 10^9$	None
Stream symmetric ciphers	Practical security	128, 256, 512	$10^7 – 10^{10}$	None
Asymmetric PCAs are similar cryptographic algorithms	Proof Security	3248 (128), 15424 (256)	$10^2 – 10^3$	None
Asymmetric CCS using code structures	Proof Security	$0{,}5 \cdot 10^6$ (128), $2 \cdot 10^6$ (256)	$10^6 – 10^8$	Error monitoring, increasing reliability

In Table 1, there are presented values: average (the complexity of cryptanalysis is the best-known algorithm of at least 2128 operations); high (the complexity of cryptanalysis is the best-known algorithm of at least 2256 operations); super-high (the complexity of cryptanalysis is the best-known algorithm of at least 2512 operations) [4].

Hence, as it follows from the above results of the comparative analysis (Table 1), asymmetric cryptographic algorithms using TCS allow the cryptographic protection of information to be realized on the technology of public keys. And thus they provide the speed of crypto-code transformation of information with the speed of encryption of block-symmetric ciphers (BSC). In addition, the practical use of ACCS information security allows to ensure the security and reliability of data, based on the integration of channel coding and encryption mechanisms in a comprehensive manner.

In [5–8], the authors propose McEliece crypto-code systems based on various codes. In [9–11], an equilibrium coding method based on m-folded Reed-Solomon codes were proposed; however, the disadvantage is the lack of a practical algorithm for decoding the syndrome on the receiving side and the possibility of hacking based on a rearranged decoder. In [13], there is proposed a modification of the Reed-Solomon codes, which exceeds the Guruswami-Sudan decoding radius $1 – \sqrt{R}$ of the Reed-Solomon codes at low speeds R. The idea is to select the Reed-Solomon codes U and V with the corresponding speeds in (U | U + V) and decode them using the soft information decoder Koetter-Vardy.

In [5, 12], the use of alternating Goppa codes in the McEliece cryptosystem and the classical Goppa codes in the Niederreiter cryptosystem are proposed. In [14], the authors confirm the complexity of the practical implementation of the Niederreiter scheme and consider the possibility of using cryptosystems in VPN channels. In [15] article proposes a new class of convolutional codes, which allows an effective algorithm for algebraic decoding, the use of the McEliece cryptosystem in a variant. Unlike the classic McEliece cryptosystems, which use block codes, the authors propose the use of a convolutional encoder as part of the public key.

In [16] the authors propose a new Niederreiter cryptosystem based on quasi-cyclic codes which is quantum-secure. This new cryptosystem has a good transfer rate compared to the one that uses the Hopp binary codes and uses smaller keys.

In the following papers [6, 7, 12], the authors use low-density quasi-cyclic parity codes (QC-LDPC) [8] and on codes with the maximum rank distance [6, 7] to build McEliece and Niederreiter cryptosystems. In [12], the construction of the

McEliece and Niederreiter schemes based on the alternating Goppa codes is considered.

In computer networks with decisive feedback, the authors ensure the use of the McEliece crypto-code design in the G.709 optical transport network (OTN) infrastructure to provide integrated requirements for both reliability and security [17]. In [18], the authors proposed to use the Niederreiter asymmetric crypto-code system on elliptic codes. This approach provides protection against possible attacks described in [19, 20, 21] and the required level of cryptographic strength. But there are remained unresolved questions of practical implementation with the necessary power of the GF(210–213) field to ensure a guaranteed level of cryptographic strength.

Thus, the analysis showed that crypto-code constructions belong to the section of quantum-resistant cryptography and can be used instead of asymmetric cryptosystems soon. In this regard, their improvement is of wide interest among the scientific community.

However, all the codes proposed by the authors are cyclical and prone to Sidelnikov's attacks [19]. The essence of Sidelnikov's attack comes down to finding the elements of the generating matrix and removing the action of masking matrices based on linear fractional transformations and the property of triply transitivity of the automorphism group of the generalized Reed-Solomon code. As a solution, Sidelnikov proposes the use of non-cyclic codes based on cascade or algebraic-geometric codes (codes on elliptic curves). This approach provides not only opposition to Sidelnikov's attack, but also the ability to reduce key data based on the use of the coefficients of the equation of the curve as a secret parameter [4]. Besides, US NIST experts consider the security (cryptographic strength) of cryptosystems in post-quantum cryptography only if they built in the Galois field GF (2^{10}–2^{13}). However, the level of computing capabilities of modern information and communication systems does not allow them to be fully implemented. To reduce energy costs, the authors propose using modified crypto-code constructions on modified (extended codes). **Fig. 2** shows the exchange protocol based on the modified McEliece crypto-code system on modified (shortened) elliptic codes, in **Fig. 3** – on modified (extended) codes.

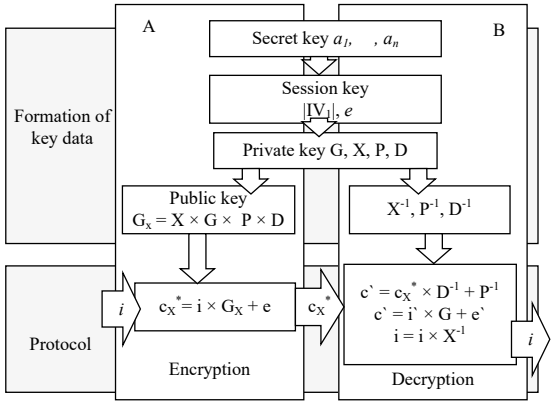


Figure 2: Exchange protocol based on a modified McEliece crypto-code system on modified (shortened) elliptic codes (secret (closed) key – matrices X, P, and D; X – non-degenerate k×k matrix over GF(q); P – permutational n×n matrix over GF(q); D – diagonal n×n matrix over GF(q),\; G^{EC}– generating k×n matrix of elliptic code over GF(q); vector IV_1 (sets of fixed positional sets of clear text {MF})

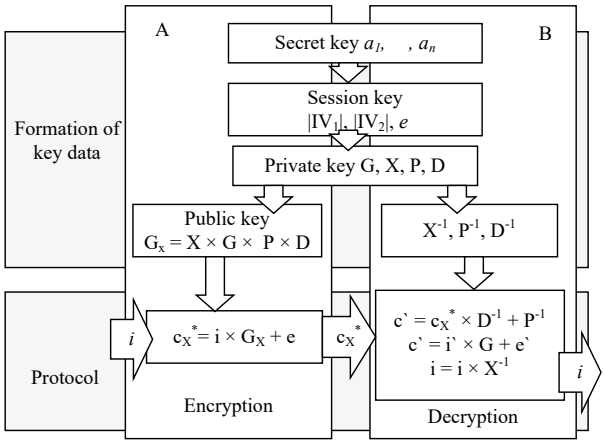


Figure 3: Exchange protocol based on a modified McEliece crypto-code system on modified (extended) elliptic codes (secret (closed) key – matrices X, P, and D; X – non-degenerate k×k matrix over GF(q); P – permutational n×n matrix over GF(q); D – diagonal n×n matrix over GF(q); G^{EC}– generating k×n matrix of elliptic code over GF(q); vector IV_1 (sets of fixed posi-tional sets of clear text {MF}); vector IV_2 (defines the position for adding plaintext characters)

The main code characteristics and parameters of cryptosystems are given in Tables 2 and 3.

Table 2. The main (n, k, d) properties of MEC.

Table 2

The main *(n, k, d)* properties of *MEC*

Property	Shortened MEC	Extended MEC
(n, k, d) code parameters constructed by displaying the view ϕ:X→Pk-1	$n = 2\sqrt{q} + q + 1 - x$, k ≥ α – x, d ≥ n – α, α=3×degF, k + d ≥n	$n = 2\sqrt{q} + q + 1 - x + x_1$, k ≥ α – x + x1, d ≥ n – α, α = 3 × degF
(n, k, d) code parameters constructed by displaying the view ϕ:X→Pr-1	$n = 2\sqrt{q} + q + 1 - x$, k ≥ n – α, d ≥ α, α = 3×degF, k + d ≥ n	$n = 2\sqrt{q} + q + 1 - x + x_1$, k ≥ n – α, d ≥ α, α = 3 × degF

Table 3

Basic parameters of McEliece MACCS on *MEC*

Property	Shortened MEC	Extended MEC
dimension of the secret key	$l_{K+} = x \times \left\lfloor \log_2\left(2\sqrt{q} + q + 1\right) \right\rfloor$	$l_{K+} = (x - x_1) \times \log_2\left(2\sqrt{q} + q + 1\right)$
dimension of information vector	$l_I = (\alpha - x) \times m$	$l_I = (\alpha - x + x_1) \times m$
dimension of the cryptogram	$l_S = \left(2\sqrt{q} + q + 1 - x\right) \times m$	$l_S = \left(2\sqrt{q} + q + 1 - x + x_1\right) \times m$
relative transmission speed	$R = (\alpha - x) / \left(2\sqrt{q} + q + 1 - x\right)$	$R = (\alpha - x + x_1) / \left(2\sqrt{q} + q + 1 - x + x_1\right)$

The proposed McEliece MCCS can reduce the power of the alphabet, which al-lows them to be implemented in practice, while ensuring the required level of crypto-graphic strength due to the introduction of additional initialization vectors: IV_1 – defines shortening characters from a code word (cryptograms), IV_2 – defines elongation characters (plain text) of a codeword (cryptogram), see also **Fig. 3**. Let us con-sider the results of a study of the basic properties of the proposed crypto-code systems.

3. Evaluation of Energy Costs for Program Implementation and the Complexity of the Proposed McEliece MACCS Code Transformation

To estimate time and speed parameters it is common to use the unit of measurement CPB (cycles per byte) – the number of processor cycles, which should be spent to process 1 byte of incoming information.

Table 4.

Research results according to the length of the code sequence in McEliece ACCS on modified elliptic codes in dependency of CPU cycles number.

Code sequence length		McEliece on shortened codes			McEliece on elongated codes			McEliece		
		10	*100*	*1000*	*10*	*100*	*1000*	*10*	*100*	*1000*
The number of function calls realizing elementary operations	Symbol reading	10294397	28750457	76759874	11432131	33460317	82473442	11·018·042	30·800·328	80·859·933
	String comparing	3406921	9246748	25478498	3673756	12119867	29469389	3·663·356	10·199·898	26·364·634
	String concatenation	1705544	5045748	12379422	1947681	6114478	14456729	1·834·983	5·125·564	13·415·329
Sum		15406862	43042953	114·61794	114·61794	51694662	126399560	16516381	46·125·790	120·639896
Duration of executing functions in processor cycles*	295·374	810·478	2001·167	2001·167	300·479	843·705	2·745·148	297·487	831·609	2·183·218
	178·814	531·379	1248·684	1248·684	213·478	561·754	1·739·170	197·821	550·794	1·423·690
	544·990	1328·114	3586·486	3586·486	578·174	1·647·638	4·007·883	544·990	1·522·293	3·984·353
Sum		1006·781	2749·548	7247·488	7247·488	1·092·131	3·053·097	1040298	2·904·696	7·591·261
Executing duration** in msec		0.52	1.37	3.4	3.4	1,55	4,1	0,55	1,53	4

Notes:* duration of 1000 operations in processor cycles: reading a character – 27 cycles, com-paring strings – 54 cycles, string concatenation - 297 cycles.

** for the calculation, a processor with a clock frequency of 2 GHz was used, taking into account the load by the operating system, is taken 5%

Algorithm complexity is calculated from expression [4]:

$$Per = Utl \cdot CPU\_clock / Rate,$$

where Utl – utilization of the CPU core (%) and Rate – algorithm bandwidth (bytes/sec).

In Table 4 there are shown dependency research results of code length sequence of algebrogeometric code in McEliece TCS from the number of processor cycles due to executing elementary operations in the program realization of crypto-code systems.

Table 5

Investigation Results for Evaluating Time and Speed Parameters of Procedures of Forming and Decoding Information

Crypto-code systems	Code sequence length	Algorithm bandwidth, Rate (Byte / sec)	CPU utilization (%)	Algorithm complexity, Per (CBP)
McEliece ACCS	100	46 125 790	56	61,5
	1000	120 639 896	56	62,0
	100	51 694 662	56	61,7

McEliece at shortened MEC	1000	126 399 560	56	62,2
McEliece at shortened MEC	100	46 125 790	56	61.5
	1000	120 639 896	56	62.0

Tab. 5 shows the investigation results for evaluating time and speed parameters of procedures of forming and decoding information in the non-symmetric crypto-code systems based on McEliece ACCS and MCCS.

Analysis of Tables 4 and 5 shows that the use of modified (elongated) elliptic codes allows to save the volume of transmitted data in McEliece a crypto-code sys-tem, but at the same time it provides the required level of cryptographic resistance during the implementation over the smaller field GF(2^6 – 2^8) through the use of en-tropy of initialization vector.

4. Study of the Properties of the McEliece ACCS on the EC and the Modified McEliece on MEC

In order to estimate the parameters of asymmetric code-theoretic schemes using elliptic codes, let us introduce the following notation:

- l_I – length of the information sequence (block) arriving at the input of the crypto-code structure (in bits);
- l_K – the length of the public key (in bits);
- l_{K+} – the length of the private key (in bits);
- l_s – the length of the code (in bits);
- O_K - the complexity of the formation of the code (number of group operations);
- O_{SK} – the difficulty of decoding the cryptogram (the number of group operations);
- O_{K+} – the complexity of solving the analysis problem (the number of group operations).

For the construction of graphs, conditional abbreviations (prefixes) were used:

- u_k – MACCS with truncated MEC;
- u_d – MACCS with elongated MEC.

In calculating the parameters of cryptosystems, the Galois fields were used:

- for McEliece TCS – $GF(2^{10})$;
- for MACCS with truncated / elongated MEC – $GF(2^6)$.

In the next step, we perform a comparative analysis of the parameters of the McEliece asymmetric code-theoretic scheme (MACS) using EC, with the parameters of the modified MACCS McEliece on MEC. To estimate the length of the infor-mation sequence (in bits) arriving at the input of the MACCS with the algebraic (n, k, d)-code over GF(2m) (where m − the power of the extended Galois field), we use the expressions:

- $l_I = k \times m$, for ACCS on the EC;
- $l_I = 1/2k \times m$, for MCCS on truncated MEC;
- $l_I = k \times m$, for MACCS on elongated MEC.

In Tab. 6 and in Figure 4 we show the cryptogram formation complexity from the power of the field, where code rate (R) stands for the relative speed of coding R=k/n, the encoder assigns to each message of *k* digits a longer message of *n* digits called a codeword.

From the provided data it can be seen that the cryptogram formation complexity for the chosen power of the GF 26 on the truncated and elongated codes is much lower (by 5 times and more) than in the original realization of MACCS to the EC. Respectively, the speed of the formation of the cryptogram will significantly increase.

- In order to estimate the length of the cryptogram (in bits), we use the expressions:
- ls = n × m, for ACCS on the EC;
- l_s=(2√q+q+1-1/2k)×m, for MCCS on truncated MEC;
- l_s=(2√q+q+1-1/2k+1/2k)×m, for MCCS on elongated MEC.

Table 4.

Dependence of the complexity of forming a cryptogram in various GF(2^m)

GF(2^m)	R					
	0.5	*0.75*	*0.5(u_d)*	*0.75 (u_d)*	*0.5(u_k)*	*0.75 (u_k)*
3	31	87	242	603	817	968
4	76	340	760	980	2140	6282
5	335	872	2241	6121	8706	11461
6	582	2170	6348	9830	10722	60760
7	1023	6172	17092	61751	83000	210170
8	5237	10673	67016	105265	207422	605005

9	10563	50487	98765	510780	710920	1018079
10	52704	103822	497309	908243	4572881	5561379

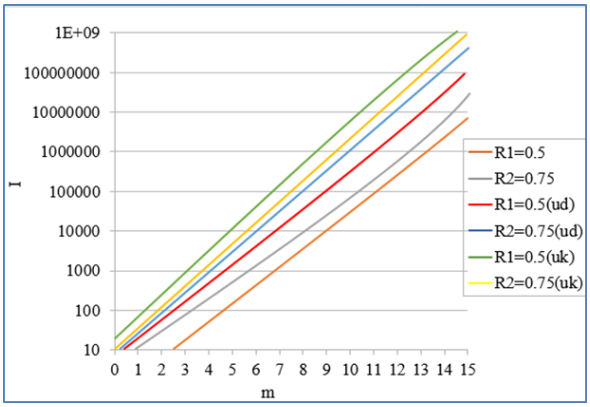


Figure 2: Dependence of the complexity of forming a cryptogram in various GF(2^m)

In Tab. 7 and Figure 5 we show the dependence of the decoding complexity of the cryptogram on the field strength.

Table 5.

Dependence of the Decryption Complexity of the Cryptogram in Various GF(2^m)

GF (2^m)	R					
	0.5	*0.75*	*0.5(u_d)*	*0.75 (u_d)*	*0.5(u_k)*	*0.75(u_k)*
1	43	57	78	81	82	96
2	67	98	456	457	457	556
3	120	640	1024	1168	1280	5127
4	680	2378	7672	8232	11028	23674
5	2092	7512	21073	42082	78634	277830
6	12397	61246	103862	281472	760553	5220573
7	127523	136495	642648	752018	4566721	19768512
8	1203984	1494284	3564898	3957812	12948312	52694229
9	10637991	12768954	54678128	67458242	92516734	102564872
10	175645127	193648924	1e+09	1e+09	1e+09	1e+09

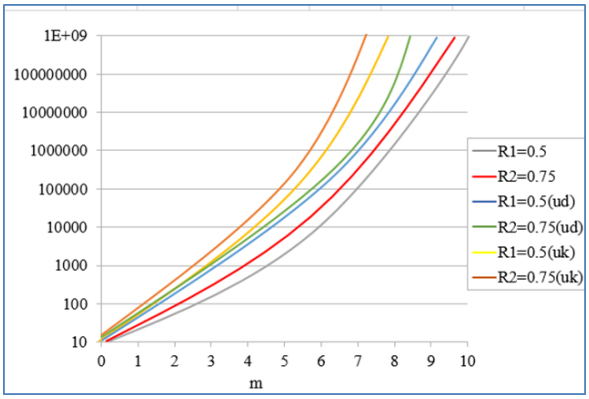


Figure. 3: Dependence of the decryption complexity of the cryptogram in various GF(2^m)

Analysis of calculation results, as in the case of cryptogram formation, shows a significant increase in the decoding rate when using truncated and elongated MEC.

The length of the public key (in bits) is determined by the sum of the elements of the matrix and is given by the expressions:

- $l_K = k \times n \times m$, for ACCS on the EC:;
- $l_s = \frac{1}{2k} \times (2\sqrt{q} + q + 1 - 1/2k) \times m,$ for MCCS on truncated MEC;
- $l_s = \frac{1}{2k} \times (2\sqrt{q} + q + 1 - \frac{1}{2k} + \frac{1}{2k}) \times m,$ for MCCS on elongated MEC.

The length of the private key (in bits) is determined by the sum of the elements of the matrices X, P, D (in bits) and is given by the expressions:

- $l_{K+} = n^2 \times k^2 \times m,$ for ACCS on the EC;
- $l_{Ks} = \frac{1}{2k}[\log_2(2\sqrt{q} + q + 1)],$ for MCCS on truncated MEC;
- $l_{Ks} = (\frac{1}{2k} - \frac{1}{2k})[\log_2(2\sqrt{q} + q + 1)],$ for MCCS on elongated MEC.

In Tab. 8 and Figure 5 there are shown the dependency of the breaking complexity based on the permutation decoding on the field strength.

Table 6.

Dependence of Breaking Complexity in Various GF(2^m)

GF(2^m)	R					
	0.5	***0.75***	***0.5(u_d)***	***0.75(u_d)***	***0.5(u_k)***	***0.75(u_k)***
1	1.056	1.38	2.786	2.835	4.122	4.257
2	2.237	3.017	4.978	5.961	6.233	6.781
3	2.868	4.867	7.568	8.120	8.234	9.764
4	4.843	6.613	9.87	12.1	12.647	13.32
5	6.22	8.03	12.017	14.224	14.742	16.892
6	7.891	12.245	**14.983**	**17.483**	**18.767**	**19.76**
7	8.995	13.13	17.14	20.32	21.102	22.93

8	10.37	15.16	19.55	23.23	24.05	26.11
9	11.74	17.18	21.96	26.15	27.002	29.302
10	13.19	19.23	24.37	29.06	29.95	32.484

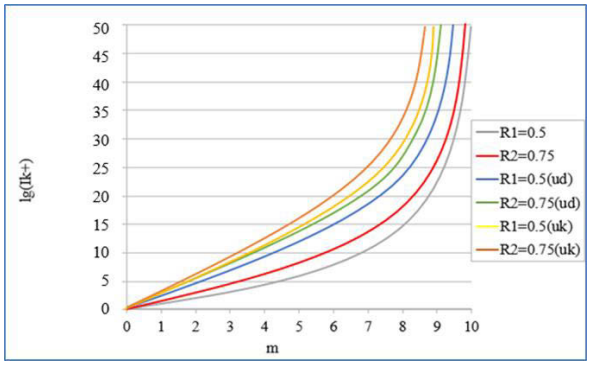


Figure 4: Dependence of breaking complexity in various GF(2^m)

The analysis of Figure 6 shows that reducing the field power to 2^6 has not led to a significant reduction in the complexity of breaking cryptograms by permutation decoding.

The complexity of the cryptogram formation is estimated by the expressions:

- for ACCS on the EC:
  when implementing systematic coding:
  $$O_K = (r+1) \times n,$$
  for non-systematic coding:
  $$O_K = (k+1) \times n;$$
- for MCCS on truncated MEC:

when implementing systematic coding:

$$O_k = (r+1) \times (2\sqrt{q} + q + 1 - 1/2k),$$

for non-systematic coding:

$$O_k = (k+1) \times (2\sqrt{q} + q + 1 - 1/2k);$$

- for MCCS on elongated MEC:
  when implementing systematic coding:

$$O_k = (r+1) \times (2\sqrt{q} + q + 1 - \frac{1}{2k} + \frac{1}{2k}),$$

for non-systematic:

$$O_k = (k+1) \times (2\sqrt{q} + q + 1 - \frac{1}{2k} + \frac{1}{2k}).$$

The complexity of decoding of a pattern is defined by expressions:

- for ACCS on EC:

$$OSK = 2\times n^2+k^2+4t^2 + (t^2 + t - 2)^2/4,$$

- for MCCS on truncated MEC:

$$O_{SK} = 2(2\sqrt{q} + q + 1 - \frac{1}{2k})^2 - \frac{1}{2k^2} + 4t^2 + \frac{(t+t-2)^2}{4}.$$

- for MCCS on elongated MEC:

$$O_{SK} = 2(2\sqrt{q} + q + 1 - \frac{1}{2k} + 1/2k) \quad - k^2 + 4t^2 + \frac{(t+t-2)^2}{4}$$

The complexity of the task of the analysis (decoding) solution is set by expressions:

- for ACCS on EC:

$$O_{K+} = N_{cov} \times n \times r,$$

where

$$N_{cov} \geq \frac{C_n^t}{C_{n-k}^t} = \frac{n(n-1)...(n-t-1)}{(n-k)(n-k-1)...(n-k-t-1)}$$

$$t=[(d-1)/2]$$

The potential strength of the cryptosystem is defined by size $\rho \times t$, and noise stability of system – $(1 - \rho) \times t$.

- For MCCS on truncated codes:

$$O_{MACCS} = N \times (2\sqrt{q} + q + 1 - \frac{1}{2k}) \times r.$$

- For MCCS on elongated codes:

$$O_{MACCS} = N \times (2\sqrt{q} + q + 1 - \frac{1}{2k} + 1/2k) \times r.$$

In Tab. 9 and Figure 7 it is presented dependence of complexity of breaking and complexity of coding for various speeds of the EC (MEC).

Table 7

Summary diagram of breaking complexity and encoding complexity for different speeds of the EC

lg(l_s)	0.5	0.75	0.5(u_d)	0.75(u_d)	0.5(u_k)	0.75(u_k)
1	4.75	12.1	15.6	18.23	19.12	19.82
2	10.52	21.76	32.47	35.67	38.63	39.18
3	18.22	33.17	43.75	51.61	56.88	58.03
4	21.42	51.75	59.43	72.81	78.92	80.52
5	38.77	61.09	68.26	87.32	94.91	104.56
6	54.13	78.37	101.72	112.46	120.83	128.79
7	82.14	83.72	156.75	164.72	182.39	189.74
8	165.84	179.13	223.64	231.57	276.27	287.33
9	358.33	371.09	421.97	428.63	459.81	476.52
10	672.37	684.94	716.41	722.26	783.46	794.28

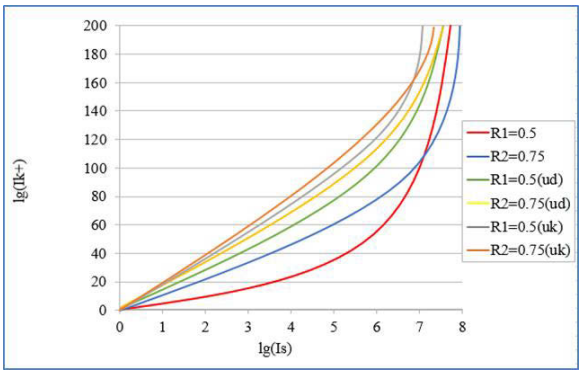


Figure 7: Summary diagram of breaking complexity and encoding complexity for different speeds of the EC (MEC)

Dependences of the volume of open key data for various indicators of firmness are presented in Table 10 and Figure 8.

The results of the research of the capacitor characteristic at program realization from field power are presented in Table 11.

Table 10

Dependencies of the volume of open key data for various indicators of durability

$lg(I_{k+})$	R					
	0.5	*0.75*	*0.5(u_d)*	*0.75(u_d)*	*0.5(u_k)*	*0.75(u_k)*
5	30	87	240	602	968	799
20	2278137	4351076	926137	987234	1034682	1897092
35	12329538	14097276	4253109	5237688	6126273	6832018
50	22541273	77520337	43076332	60122407	8602376	7027160

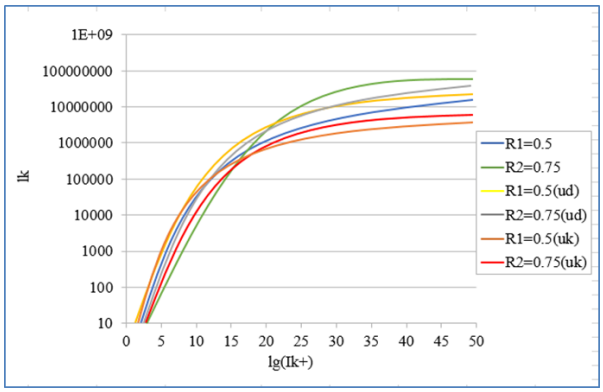


Figure 8: Dependencies of the volume of open key data for various indicators of durability.

The results of the research of the capacitor characteristic at program realization from field power are presented in Table 11.

Table 11

The dependence of the program implementation rate on the power of the field (the number of group operations).

Cryptosystems	2^5	2^6	2^7	2^8	2^9	2^{10}
ACCS McEliece on EC	10018042	18048068	32847145	47489784	63215578	82467897
MACCS McEliece on truncated MEC	10007947	17787431	28595014	44079433	61974253	79554764
MACCS McEliece on elongated MEC	11156138	18561228	33210708	48297112	65171690	84051337

The results of studies of the dependence of the software implementation depend-ing on the field power and the parameters of algebra-geometric codes are also pre-sented, as can be seen from Table 11, the use of modified crypto-code constructions provides a 5-fold reduction in energy costs for the software implementation, that allows for their practical implementation

5. Results of Studies of the Proposed Public-Key Cryptosystems Based on the NIST-STS 822 Package

One of the main components of the evaluation of the stability of cryptographic algorithms is the estimation of its statistical security. It is believed that the algorithm is statistically secure if the sequence it generates by its properties is not inferior to a random sequence - such sequences are called “pseudorandom”. For the experi-mental estimation of how close the crypto-algorithms approximate the generators of the “random” sequences, statistical tests are used. The NIST STS benchmark pack-age for testing random or pseudorandom number generators is one of the approach-es to realizing the task of evaluating the statistical security of cryptographic primi-tives.

The use of this package makes it possible to conclude with a high degree of probability as to how much sequence that is generated by the investigated primitive is statistically secure. A set of NIST STS tests was proposed during the contest for a new national standard for US block coding in 2000 and developed by the staff of the National Institute of Standard and Technologies [22]. This set was used to study the statistical properties of candidates for a new block cipher. To date, the test methodology, which is offered by NIST, is the most common for developers of cryp-tographic means of information protection. The test procedure for an individual binary sequence S is as follows:

1. A null hypothesis H_0 is advanced-the assumption that the given binary sequence S is random.
2. From the S sequence, the test statistics from (S) are calculated.
3. Using the special function and test statistics, a probability value $P=f(c(S))$, $P \in [0,1]$

4. The value of probability P is compared with the level of significance $\alpha \in [0.001,0.01]$. If $P \geq \alpha$, then the H_0 hypothesis is accepted. Otherwise, an alternative hypothesis is adopted.

In accordance with the methodology, the decision to pass statistical testing is taken by the event that fulfills the following rules:

1. The rule #1. All q tests were executed, ($q = \overline{(1,189)}$), and if the value of the coefficient rj is inside the confidence interval [0.96, 1.00];
2. The rule #2. All q tests were executed, ($q = q = \overline{(1,189)}$), and if for all tests by the Pearson χ^2 criterion the condition is met $P(\chi^2)>0.0001$.

For carrying out experimental research about the properties of the developed code cryptosystems the program is developed to realize the offered means of protec-tion of the information.

The following parameters have been selected during the tests:

- length of the test sequence $n = 10^6$ bits;
- number of tested sequences m = 100. Thus, the volume of the test sample was $N = 10^6 x100 = 10^8$ bits;
- significance level $\alpha = 0.01$;
- number of tests $q = 189$.

Authors have obtained the results of statistical testing and statistical portraits of the developed means of information protection. The final values and results of the best world crypto-algorithms are summarized in Table 12.

As it can be seen from the presented data in Table 12 the proposed crypto-code systems on the modified codes are not inferior to the statistical characteristics of the randomness of the code sequence formation to the world standards of providing basic services: confidentiality, integrity and accessibility, while ensuring the required level of reliability of data transmission.

Consequently, the practical application of the developed information protection means allows to obtain good statistical properties of the generated sequences and to effectively ensure the security and reliability of the data being processed and transmitted.

Table 8
Results of experimental testing

Cryptosystems	The number of tests in which the testing passed more than 99% of the sequences	The number of tests in which tests were over 96% of the sequences	The number of tests in which testing was less than 96% of the sequences
CCS McEliece	149 (78,83%)	189 (100%)	0 (0%)
MCCS McEliece on shortened MEC	151 (79,89%)	189 (100%)	0 (0%)
MCCS McEliece on extended MEC	152 (80,42%)	189 (100%)	0 (0%)
Keccak (SHA-3)	134 (71,9%)	187 (98,9)	2 (1,05)
ANSI X9.17(3-DES)	124(66%)	62(33%)	3(1%)
BBS	132(70%)	55(29%)	2(1%)
SHA-1	134(71%)	54(28%)	1(1%)
Generator based on elliptic curves	146 (77,2%)	188 (100 %)	1(1%)

6. Analysis of Cryptographic Algorithms Based on the Entropy Approach

The proposed express analysis makes it possible, without significant computational and energy costs, at the intuitive level, to compare not only the resistance of various crypto-algorithms (cryptosystems), but their software implementation. The algorithm of the entropy method for assessing crypto-resistance is shown in Figure 9.

Table 13 gives the results of the study into the stability and software effectiveness of the implementation of block and stream ciphers of varying complexity. We applied DES, 3DES, GOST 28147-2015, Kalina-256, AES-256 as block ciphers. To imple-ment a stream cipher, we used pseudo-random sequence generators of two different types: based on the rule “60” of cellular automata in its classical form, without mod-ifications, and the cryptographically resistant generator SecureRandom from Java crypto-libraries, which is marketed as suitable for cryptographic applications.

Table 13
Results of testing the resistance of crypto-algorithms using an express-method

No.	Cipher	Entropy of the input message	Entropy of the encrypted message	Difference	Percentage of entropy, added by the cipher
1	Cellular automata, the rule “60”	0.502377575 (5.023775)	0.682017979 (6.820179)	0.179640404 (1.796404)	35.7580505
2	Crypto-resistant generator SecureRandom from Java crypto-libraries	0.502376767 (5.023767)	0.799998282 (7.999982)	0.297621515 (2.976215)	59.2426958
3	DES	0.469276	0.812043	0.342767	73.0416642
4	3DES	0.469276	0.812043	0.342767	73.0416642
5	GOST 28147-89	0.469276	0.811348	0.342072	72.8935637
6	Kalina-256	0.469276	0.954519	0.485243	103.4024753
7	AES-256	0.469276	0.95454	0.485264	103.4069503

In Table 13, we calculated the entropy of the input and the encrypted text, differ-ence, as well as the percentage of entropy added to the entropy of plaintext by the cipher itself. An analysis of Table 1 allows us to assess the contribution of the cipher in the total entropy of the encrypted message. As they all were tested under identical conditions, it is possible to judge their relative performance.

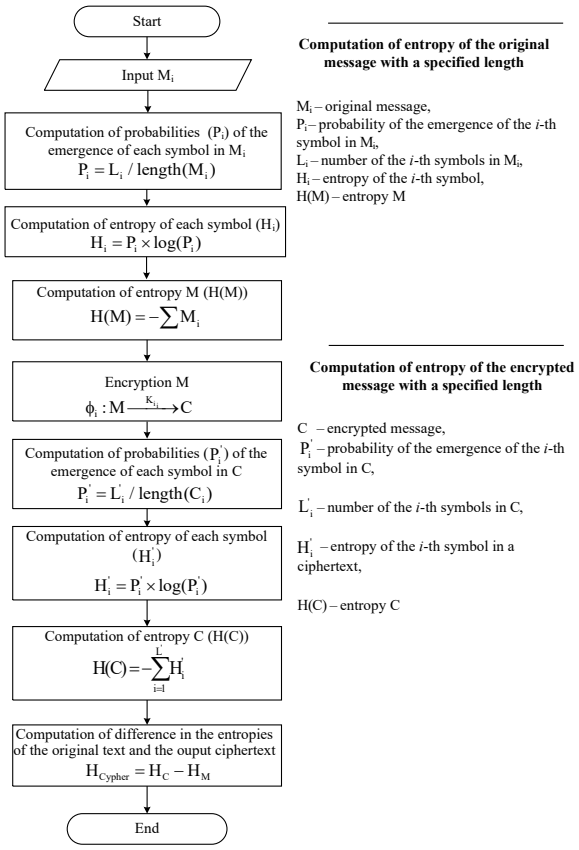


Figure 5. Algorithm for testing the cryptosystem for resistance based on the method for the estimation of randomness.

The AES-like ciphers (SPN-system, substitution-permutation schemes) are worth mentioning. Both such ciphers, Kalina and AES, made the greatest contribution, larger than 103 %, to the entropy of the plaintext. According to the given results, both ciphers have the best diffusing effect. Approximately the same results were demonstrated by the symmetric block cipher (SBC) GOST 28147-2015: 72.89 % against 73.04 % for DES/3DES. This probably confirms conclusions about the max-imally possible degree of dispersion as a characteristic of the architecture.

To compare the results, we conducted experiments using stream ciphers based on two different generators with a pseudorandom key sequence. Encryption was per-formed by the rule of addition for modulo two. In the first case, this is a generator based on cellular automata (the rule “60”). This is not a crypto-resistant generator whose sequence does not pass testing for NIST STS 822, while the second one is positioned as the crypto-resistant generator SecureRandom in the Java crypto-library. In both cases, the obtained values for entropy are much smaller than those for

classic SBC, which does not allow us to argue about quality encryption with their help. Thus, the presented results suggest that a simple entropy method allows rapid assessment of the quality of ciphers used without referring to expert estimations. Such an express technique is available to anyone with a minimal knowledge of the information theory.

Moreover, in this way, one can evaluate different implementations of ciphers that will make it possible to select the best (optimal) software implementation that matches the terms and requirements of the user. For example, in our computer ex-periments, we used two implementations of the DES algorithm. One of them, given in Table 13 at number 3, demonstrated a 73.04 % increase in entropy after encrypting compared to the original text, another algorithm − 64.4 %. It is obvious that for practical purposes it makes sense to choose the first implementation, since it appears that its scattering characteristics are better. Thus, the express-analysis allows assessment of the quality of implementation of classic (and other) crypto-algorithms in order to select an optimal crypto library out of many commercially available libraries.

We shall consider the results obtained in terms of maximum cryptographic infor-mation protection. An indicator of such protection is the entropy of the encrypted binary file, given in Table 14.

Table 14

Estimation of maximal cryptographic protection of information.

No.	Cipher	Entropy of the input message	Entropy of the encrypted message	Probability of cryptographic protection, P_c
1	Cellular automata, the rule "60"	0.469276	0.637079949	0.637079949
2	Crypto-resistant generator SecureRandom from Java crypto-libraries	0.469276	0.747287753	0.747287753
3	DES	0.469276	0.812043	0.812043
4	3DES	0.469276	0.812043	0.812043
5	GOST 28147-89	0.469276	0.811348	0.811348
6	Kalina	0.469276	0.954519	0.954519
7	AES-256	0.469276	0.95454	0.95454
8	Perfect cipher		1.000	1.000

It is known that the maximum possible cryptographic protection is provided by the so-called "perfect cipher" by Shannon, which as a result of encryption produces a random number [23,24]. Such a file will have maximum entropy, which in the bina-ry case is equal to unity. We assume that encryption using a given cipher will ensure maximal cryptographic protection; we assume that it equals unity. One can say that the probability of protection using such a cipher is equal to unity. It is natural that imperfect ciphers do not produce such a probability of cryptographic protection. By using such an approach, one can rank all the examined ciphers for the probability of cryptographic protection. This indicator can be employed for various procedures for the assessment of the security of integrated protection systems of different corporate networks, which testifies to its universality.

In Figure 10 there are shown the results of studies of the average entropy of crypto-grams of different BSS of meaningful plaintext with a length of M = 108 bits, with an interval of N = 5 × 106 bits.

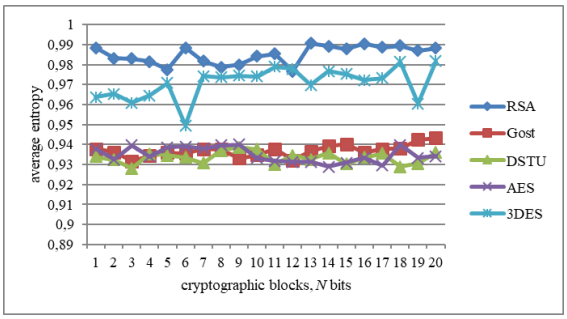


Figure 6. The results of studies of the average entropy of cryptographic blocks

Analysis of Figure 10 practically confirms the possibility of using the express method for the selection of software security mechanisms based on cryptoalgorithms.

7. Conclusions

As a result of the conducted research, it can be concluded that

1. Evaluation by NIST specialists of the computing capabilities of quantum com-puters requires a review of the use of traditional encryption algorithms to provide basic security services based on symmetric and asymmetric cryptography. The growth and synergy of modern threats put forward new requirements for systems for protecting confidential information. At the same time, the use of crypto-code constructions allows us to provide not only the required level of cryptographic stability, but also the reliability of the transmitted information. However, their use in communication devices is associated with significant energy and computation-al costs, which does not allow their practical use. Besides, the proposed Sidelnikov attack does not allow the use of many well-known codes; to counter it, it is pro-posed to use algebraic geometries based on the parameters of elliptic curves.

2. The overall structure of asymmetric crypto-code systems based on the McEliece TCS enabling integrated (with a single device) provision of the required indicators of reliability, efficiency and data security was analyzed. A major shortcoming of ACCS based on the McEliece TCS is a big volume of key data, that constricts their use in different communication system areas (today cryptographic strength on the level of the provable strength model is provided while building ACCS in the Galois field GF(213)). The use of modified (shortened) elliptic (algebraic) codes helps to reduce the volume of key data while maintaining the requirements for cryptographic strength of ACCS. Estimation of the data conversion performance is comparable to the speed of direct and inverse cryptographic conversion of modern BSC, this ensures the cryptographic strength at the level of asymmetric cryptosystems (cryptographic strength is based on the theoretical complexity problem – random code decoding).

3. The use of modified crypto-code constructions in modified (shortened, elongated) elliptic codes allows to reduce the level of the alphabet with the required level of cryptographic strength. For this, additional session keys are used (initial initializa-tion, which specify the symbols of correlation and/or extension), as well as valid codewords on the receiving side. The alphabetical index of the cryptosystem without reducing the cryptographic strength of the system as a whole ensures their practical application and use in the protocols of Internet resources and infor-mation and communication systems in the conditions of post-quantum cryptog-raphy.

8. References

[1] Report on Post-Quantum Cryptography, http://nvlpubs.nist.gov/nistpubs/ir/2016/NISTIR.8105.pdf, last accessed: 2020/02/19.

[2] Security requirements for cryptographic modules, https://csrc.nist.gov/publications/fips/fips140-2/fips1402.pdf, last accessed 2017/12/1.

[3] Grischuk, R.V., Danik, Yu. G.: Basics of Cybersecurity. Zhytomyr: ZhNAEU, p. 636 (2016).

[4] Hryshchuk, R., Yevseiev, S., Shmatko A.: Construction methodology of information secu-rity system of banking information in automated banking systems. Monograph, p. 284, Premier Publishing, Vienna (2018).

[5] Dinh, H., Moore, C., Russell, A.: McEliece and Niederreiter Cryptosystems that Resist Quantum Fourier Sampling Attacks. https://dl.acm.org/citation.cfm?id=2033093, last ac-cessed 2020/03/10.

[6] Baldi, M., Bianchi, M., Chiaraluce, F., Rosenthal, J., Schipani, D., Enhanced public key se-curity for the McEliece cryptosystem. https://arxiv.org/abs/1108.2462, last accessed 2020/03/10.

[7] Zhang, G., Cai, S., Secure error-correcting (SEC) schemes for network coding through McEliece cryptosystem. https://link.springer.com/article/10.1007/s10586-017-1294-5 (2017).

[8] Zhang, G., Cai, S.: Universal secure error-correcting (SEC) schemes for network coding via McEliece cryptosystem based on QC-LDPC codes. https://link.springer.com/article/10.1007/s10586-017-1354-x (2017).

[9] Rossi, M., Hamburg, M., Hutter, M., Marson, M.: A Side-Channel Assisted Cryptanalytic Attack Against QcBits. https://link.springer.com/chapter/10.1007/978-3-319-66787-4_1 (2017).
[10] Dudikevich, V.B., Kuznetsov, O.O., Tomashevsky, B.P.: Crypto-code protection of infor-mation with non-binary equilibrium encoding. The hour zahist of information, No. 2, p. 14–23 (2010).
[11] Dudikevich, V.B., Kuznetsov, O.O., Tomashevsky B.P.: Non-dual equilibrium coding method. Modern information protection. No. 3, p. 57–68 (2010).
[12] Morozov, K., Roy, P.S., Sakurai, K.: On unconditionally binding code-based commitment schemes. https://dl.acm.org/citation.cfm?id=3022327&dl=ACM&coll=DL, last accessed 2019/09/1.
[13] Corbella, I.M., Tillich, J.-P.: Using Reed-Solomon codes in the (U | U + V) construction and an application to cryptography. In: IEEE International Symposium on Information, https://ieeexplore.ieee.org/document/7541435, last accessed 2019/09/1.
[14] Rossi, M., Hamburg, M., Hutter, M., Marson, M.E.: A Side-Channel Assisted Cryptana-lytic Attack Against QcBits. https://link.springer.com/chapter/10.1007/978-3-319-66787-4_1, last accessed 2019/09/1.
[15] Almeida, P., Avelli, D.N.: A new class of convolutional codes and its use in the McEliece Cryptosystem. https://www.researchgate.net/publication/324745076_A_new_class_of_convolutional_codes_and_its_use_in_the_McEliece_Cryptosystem, last accessed 2019/09/1.
[16] Kapshikar, U., Mahalanobis, A.: A Quantum-Secure Niederreiter Cryptosystem using Qua-si-Cyclic Codes. https://www.researchgate.net/publication/327660637_A_Quantum-Secure_Niederreiter_Cryptosystem_using_Quasi-Cyclic_Codes, last accessed 2019/09/1.
[17] Cho, J.Y., Griesser, H., Rafique, D.: A McEliece-Based Key Exchange Protocol for Optical Communication Systems. In: Proceedings of the 2nd Workshop on Communication Securi-ty, WCS 2017, pp. 109-123, https://link.springer.com/chapter/10.1007%2F978-3-319-59265-7_8, last accessed 2019/09/1.
[18] Evseev, S.P., Rzaev, Kh.N., Tsyganenko, A.S.: Analysis of the software implementation of direct and inverse transformation using the method of non-binary equilibrium coding. Bezpeka Informatsii 2016 Volume 22 # 2 – Kiev "Nash Format", pp. 96–203 (2016).
[19] Sidel'nikov, V. M.: Cryptography and coding theory. In conference materials: Moskovskij Universitet i razvitie kriptografii v Rossii, MGU, p. 22 (2002).
[20] Minder, L.: Cryptography based on error correcting codes. Ph.D. thesis, Ecole Polytech-nique Fédérale de Lausanne (2007).
[21] Faure, C., Minder, L.: Cryptanalysis of the McEliece cryptosystem over hyperelliptic codes. In: Eleventh International Workshop on Algebraic and Combinatorial Coding Theory, pp. 99-107, Pamporovo, Bulgaria (2008).
[22] Rukhin, A., Soto., J.: A Statistical Test Suite for Random and Pseudorandom Number Generators for Cryptographic Applications. NIST Special Publication 800-22 (2000).
[23] Hlobaz, A., Podlaski, K., Milczarski, P.: Enhancements of encryption method used in SDEx. Communications in Computer and Information Science Vol. 718, pp. 134-143, Springer International Publishing (2017).
[24] Milczarski, P., Hlobaz, A., Podlaski, K.: Analysis of enhanced SDEx method. Proceedings of the 2017 IEEE 9th International Conference on Intelligent Data Acquisition and Ad-vanced Computing Systems: Technology and Applications, IDAACS (2017).

Determining the Level of Flight Crew Readiness Based on Fuzzy Logic Approaches

Oleksandr Blyskun [1], Volodymyr Herasymenko [1], Oleksii Martyniuk [1], Yurii Kolomiiets [1], Yevhen Honcharenko [1]

[1] *The National Defence University of Ukraine named after Ivan Cherniakhovskyi, Povitroflotsky Avenue, 28, Kyiv, 03049, Ukraine*

Abstract

The application of aviation as the main mobile firepower in achieving the objectives of military operations today is obvious and necessary. In solving a number of important tasks for aviation in practice, it is necessary to be able to assess the effectiveness of the aviation group. The effectiveness of aviation application depends on a number of factors, most of which are unmanageable. Therefore, the authors chose the level of flight crew readiness in the study as the main factor that can be influenced by taking into account the indicators of crew readiness and their subsequent appointment on missions with different levels of complexity.

In the article, the authors analyzed the indicators that affect the readiness of the flight crew, which make up the specifics of a particular task. Qualitative indicators of the level of readiness and their compliance with the complexity of the relevant missions are determined. Quantitative values of qualitative indicators of the level of crew readiness were also obtained.

The article proposes a method of determining the readiness level of the flight crew, taking into account: the total flight hours, the flight hours for 12 months, the flight hours of personal improvement, breaks in flights and the age of a pilot.

The methodology considered in the article could increase the efficiency of fighter aviation application by reducing the time for the commander in the decision-making process and the exclusion of the subjective approach in the decision-making process.

An algorithm for methodology for determining the level of crew readiness has been developed. The algorithm of this technique is implemented by the software package MATLAB: Simulink and Fuzzy Logic Designer.

Keywords

readiness level, fighter aviation, flight crew, mission, fuzzy logic, aviation application

1. Introduction

Taking into account the influence of the flight crew readiness degree on the success of the flight task (combat missions) is carried out by entering the appropriate coefficient C_{prep}. In the works [1, 2, 3, 4] for the flight crew of tactical aviation the level of preparation considers only the level of class qualification. And according to [5] the level of class qualification takes into account only the total flight hours and exercises that have been completed in the relevant training course. That is, in works [1, 2, 3, 4], it is said that the pilot of the first class, or the pilot-sniper when performing combat missions uses all combat capabilities inherent in the combat aircraft without exception. Therefore, the coefficient of flight crew readiness of these class qualification levels is proposed to be equal to one ($C_{prep} = 1$) [6]. For a flight crew with a level of qualification lower than the first class, the values of this coefficient are assigned depending on the passage of the relevant training course and the total flight hours acquired by them ($C_{prep} < 1$). This does not take into account weighty indicators that effect on the readiness level of crews to perform specific combat missions [7]. The readiness level does not have clear boundaries. In conditions when there are no

EMAIL: bliskun1985@gmail.com; gera410@ukr.net; o.r.martyniuk@gmail.com; Ip48212@gmail.com; yevhen_@ukr.net

ORCID: 0000-0002-7751-8313; 0000-0003-2014-7408; 0000-0003-2578-0018; 0000-0002-9767-0750; 0000-0001-7654-6083;

clear boundaries of readiness level, the raised problem can be solved quite successfully with the use of fuzzy logic which is successfully implemented in MATLAB software which authors use for building a fuzzy logic system. Fuzzy set theory is one of the mathematical theories designed to formalize indefinite information for solving analytical problems. Therefore, the purpose of this work is to determine the scientific and methodological apparatus using fuzzy logic approaches to determine the readiness level of the flight crew with taking into account weighty indicators.

2. Algorithm of determining the readiness level of the flight crew

At the stage of decision-making for flights and combat missions, the aviation commander assesses the situation, hears and analyzes the proposals of his deputies, heads of services, commanders of aviation units, commanders of support units, etc. [8]. Commander relies on his own experience and intuition. The decision is made in conditions of some uncertainty.

Obviously, the higher the readiness level of the flight crew to perform the task, the higher probability of its successful completion. In times of shortage, the commander must be able to clearly identify the crew to perform a specific combat mission.

To determine the effectiveness of the fighter aviation application it is necessary to investigate all the factors that affect the readiness level of the flight crew and identify the main ones. But these factors have no clear boundaries. In conditions when there are no clear boundaries, the problem can be solved quite successfully using fuzzy logic. The fuzzy logic theory is one of the most suitable mathematical theories designed to formalize indefinite information for solving these kinds of issues.

To perform calculations by the fuzzy logic apparatus, it is necessary to create an algorithm of determining the readiness level, which will allow assigning flight crews on different types of missions based on the results of determining their readiness level. This algorithm is shown in Figure 1.

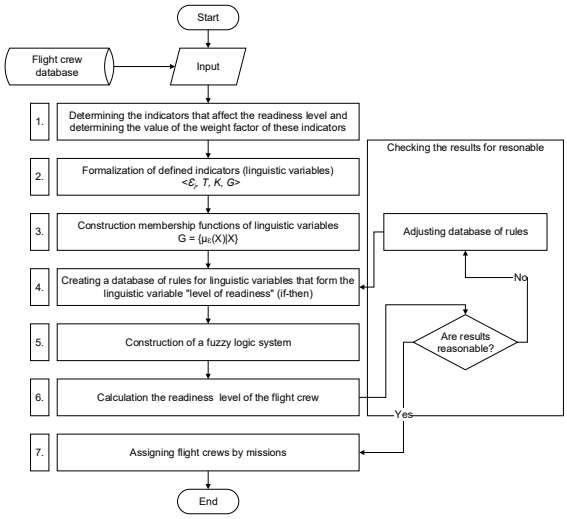


Figure 1: Algorithm of determining the readiness level of the flight crew

2.1. Description of the algorithm steps

Step 1. Selection of indicators to determine the readiness and formation of input data. That is, to decide the flight crew appointment to perform the particular mission will be used to quantify the readiness of the crew. The group of experts determines by voting the five indicators that have the greatest impact on the level of readiness of the flight crew.

Step 2. Formalization of the assessment of input readiness indicators as a tuple is carried out, <Ɛj, T, K, G> where Ɛj – name, T – terms, K – boundaries, G={μƐ(X)|X} – membership functions [7]. Definition of terms for linguistic variables that characterize the level of readiness of the flight crew and the linguistic variable “level of readiness”.

Step 3. Construction of membership functions of linguistic variables. At this step, the limits of the terms selected to determine the level of readiness and for the linguistic variable "level of readiness" are also set. The construction of membership functions is carried out based on regulatory requirements and expert assessments.

Step 4. Determining the relationship between input and output data in the form of linguistic rules "if - then".

Step 5. Building a fuzzy logic system for each subsystem using the graphical toolkit Fuzzy Logic Designer, from the MATLAB software package. In this application there is a choice of either Sugeno or Mamdani system [9]. The functions of membership should be determined through

statistics and consultation with aviation experts. In this research, the authors use the Mamdani fuzzy inference algorithm. This is the most common inference in fuzzy systems. It uses a minimax composition of fuzzy sets. The centroid of area method of Defuzzification was used.

Step 6. The initial readiness level of the flight crew is calculated and its values are checked for reasonable. The operation of each fuzzy logic block is checked so that it gives the expected initial values and, therefore, confirms that the developed method of analysis is acceptable.

After that, need to run several launches with different input values, and compare the results with each other. The aim is to determine whether the results are reasonable for the model to give realistic and consistent results. After confirming this, the result should be checked for acceptable limits set for the type of operation. If necessary, appropriate adjustments are made.

The assessment of the initial level of readiness is being formalized. Also, values are determined, as well as the choice of the required fuzzy inference algorithm.

Step 7. The obtained values of the readiness level are compared with quantitative indicators that correspond to the values of the linguistic variable "level of readiness" and then appoint flight crew on a mission with an applicable level of complexity.

Next, consider an example of calculating the readiness level of flight crews for fighter aviation.

3. Calculation of the readiness level of flight crews for fighter aviation

Since quantitative values of variables are required to formalize t-he decision-making algorithm, use fuzzy logic methods to assess the qualitative indicator of the level of readiness [10], namely, place on the scale of the value of the linguistic variable “the level of readiness”:

1. dangerously low (corresponds to value 1 – the pilot needs additional training)
2. low (corresponds to the value 2 – the pilot is able to perform disruption (violation) of enemy air freight cargo missions)
3. medium (corresponds to a value 3 – the pilot is able to perform missions of defeating enemy airborne troops in the air)
4. sufficient (corresponds to the value 4 – the pilot is able to perform the missions of destroying the air threat means of the enemy over own territory)
5. high (corresponds to value 5 – the pilot is able to perform the missions of destroying the air threat means of the enemy over hostile territory)

Since the readiness level is considered as the probability of implementation of the mission, the quantitative assessment of the readiness level should be in the range from 0 to 1. Divide the selected interval into 10 segments. The degree of belonging of a value is defined as the ratio of the number of responses in which the value of a linguistic variable occurs in a certain interval, to the maximum value of this number at all intervals. Authors conducted a survey of 40 aviation experts on prominent questionnaires. The results of calculations performed on the survey analysis are given in Table 1**Ошибка! Источник ссылки не найден.**.

Table 1

The results of the experts’ survey

value	Interval, unit									
	0-0.1	0.1-0.2	0.2-0.3	0.3-0.4	0.4-0.5	0.5-0.6	0.6-0.7	0.7-0.8	0.8-0.9	0.9-1
1	24	12	4	0	0	0	0	0	0	0
2	0	6	21	11	2	0	0	0	0	0
3	0	0	0	3	7	21	9	0	0	0
4	0	0	0	0	0	0	11	18	11	0
5	0	0	0	0	0	0	0	3	13	24
k_j	24	18	25	14	9	21	20	21	24	24

To process the data, we use a hint matrix, which is a string with elements defined by the equation

$$k_j = \sum_{i=1}^{5} b_{ij}, \qquad j = \overline{1.10} \tag{1}$$

The hint matrix in this case has the form:

$$M = \|24\ 18\ 25\ 14\ 9\ 21\ 20\ 21\ 24\ 24\|$$

Choose the maximum element from the hint matrix:

$$k_{max} = \max_j k_j =$$

$$= max\{24; 18; 25; 14; 9; 21; 20; 21; 24; 24\} = 25$$

and convert the elements of table 1 according to the equation

$$c_{ij} = \frac{b_{ji} k_{max}}{k_j}, i = \overline{1.5}, j = \overline{1.10} \tag{2}$$

The results of the calculations are put in Table 2, on the basis of which the membership functions are built.

Table 2
Processing of survey results

value	Interval, unit									
	0-0.1	0.1-0.2	0.2-0.3	0.3-0.4	0.4-0.5	0.5-0.6	0.6-0.7	0.7-0.8	0.8-0.9	0.9-1
1	25.0	16.7	4.0	0	0	0	0	0	0	0
2	0	8.3	21.0	19.6	5.6	0	0	0	0	0
3	0	0	0	5.4	19.4	25.0	11.3	0	0	0
4	0	0	0	0	0	0	13.8	21.4	11.5	0
5	0	0	0	0	0	0	0	3.6	13.5	25.0

To do this, find the lines of the maximum elements by the equation

$$c_{1max} = \max_j c_{ij}, i = 1.2, \dots, m, j = 1.2, \dots, n \quad (3)$$

and receive next result:

$$c_{1max} = 25.0; c_{2max} = 21.0; c_{3max} = 25.0; c_{4max} = 21.4; c_{5max} = 25.0$$

The value of the membership function is found by the equation

$$\mu = \frac{c_{ij}}{c_{imax}} \quad (4)$$

The results of the calculations are given in Table 3.

Table 3
The value of the membership function

μ_i	Interval, unit									
	0-0.1	0.1-0.2	0.2-0.3	0.3-0.4	0.4-0.5	0.5-0.6	0.6-0.7	0.7-0.8	0.8-0.9	0.9-1
μ_1	1	0.67	0.16	0	0	0	0	0	0	0
μ_2	0	0.40	1	0.94	0.26	0	0	0	0	0
μ_3	0	0	0	0.21	0.78	1	0.45	0	0	0
μ_4	0	0	0	0	0	0	0.64	1	0.53	0
μ_5	0	0	0	0	0	0	0	0.14	0.54	1

Fuzzy logic theory does not oblige to choose the type of membership function absolutely clearly or precisely [11]. It can be clarified in the research process based on the results of solving the problem. The most common are triangular, trapezoidal and bell-shaped membership function, which will be used in the proposed model. Predetermined intervals of fuzzy sets are the basis for constructing the membership function of input linguistic variables.

The membership functions for each value of the linguistic variable "level of readiness" are shown in Figure 2.

Figure 2: The membership functions of the value of the linguistic variable "level of readiness"

From the obtained diagram it is possible to determine quantitative indicators that correspond to the values of the linguistic variable "level of readiness". Display these values in Table 4.

Table 4
Quantitative and Qualitative indicators of the level of readiness in decision-making tasks

Mission	Qualitative assessment	Quantitative assessment
Not allowed	Dangerously low	0.1
Disruption of enemy air freight cargo missions	Low	0.35
Defeating enemy airborne troops in the air	Medium	0.6
Destroying the air threat means of the enemy over own territory	Sufficient	0.8

Destroying the air threat means of the enemy over hostile territory	High	1

That is, to decide on the appointment of the crew to perform the mission, the commander will use the quantitative assessment of the readiness of the crew from Table 4.

4. Indicators that affect the readiness level of the crew to perform the mission

The directive documents regulating the procedure for training and conducting flight training in the state aviation of Ukraine stipulate that the preparation for flight crew flights is the process of bringing the flight crew into readiness for flight tasks [8]. But the readiness of the flight crew is an integral property and complex psychological formation of the military pilot's personality, which manifests itself as a mental state of his readiness for flight activity and provides optimal mental functioning and reliability of knowledge, skills, and abilities to control technical systems of combat aircraft in various flight conditions [12, 13]. Taking into account these definitions, the authors analyzed the indicators that may effect on the readiness level of flight crew.

In research authors found that the readiness level of flight crew to perform combat action that constitute the specifics of each type of mission depends on a large number (more than 30) indicators. However, for the study, experts identified 5 main indicators that have a greater impact on the final result. These include the total flight hours, the flight hours for 12 months, the flight hours of personal improvement, breaks in flights and the age of a pilot.

Using the same method used to determine the readiness level of the flight crew, the authors calculated these indicators.

4.1. The total flight hours

The total flight hours is compared to the experience, the larger it is the easier it is for the pilot to perform any task that he has encountered in his flying activities before. The total flight hours in the study is considered as a pilot's flight hours on all types of aircraft for all years of flight activity, including training in Air Force Academy and flight schools outside the service in the Armed Forces of Ukraine. The flight hours on simulators and the operating time on the ground during engine' star up and taxiing are not taken into account.

To describe the membership function of the linguistic variable “Total flight hours” the terms were named T = {dangerously low; low; medium; sufficient; high} and their limits in flight hours K = [50, 700] were determined. The maximum value of each term was taken as 1.

The membership function for the linguistic variable “The total flight hours” built in Microsoft Excel is shown in Figure 3.

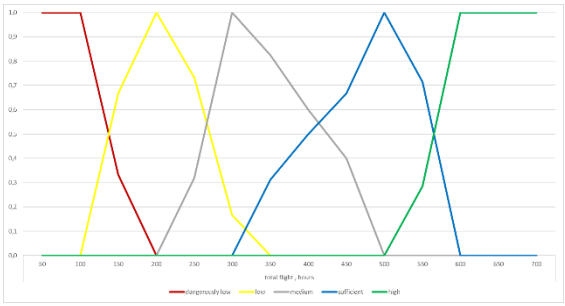


Figure 3: The membership function of the value of the linguistic variable “Total flight hours”

4.2. The flight hours for 12 months

The flight hours for 12 months in the study is considered to be flight hours on all types of aircraft on which the pilot has flown in the last year at the time of data input. The authors and experts also took into account the organizational and methodological recommendations of the Command of the Air Force on the implementation of annual flight hours per year.

To describe the membership function of the linguistic variable “The flight hours for 12 months” the terms were named T = {dangerously low; low; medium; sufficient; high} and their limits in flight hours K = [10, 140] were determined. The maximum value of each term was taken as 1.

The membership function for the linguistic variable “The flight hours for 12 months” built in Microsoft Excel is shown in Figure 4.

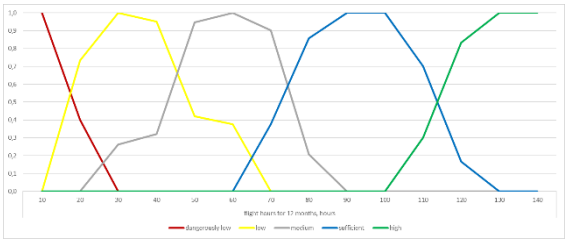


Figure 4: The membership function of the value of the linguistic variable "The flight hours for 12 months"

4.3. The flight hours of personal improvement

The flight hours of personal improvement is the percentage of flights performed by the pilot in the interest of advancing on the appropriate training course. The value of the flight hours of personal improvement is taken into account for the last year at the time of data input in percentage in relation to the flight hours for 12 months only on the main type of aircraft (combat aircraft).

To describe the membership function of the linguistic variable "The flight hours of personal improvement" the terms were named T = {dangerously low; low; medium; sufficient; high} and their limits in percentage K = [10, 100] were determined. The maximum value of each term was taken as 1.

The membership function for the linguistic variable "The flight hours of personal improvement" built in Microsoft Excel is shown in Figure 5.

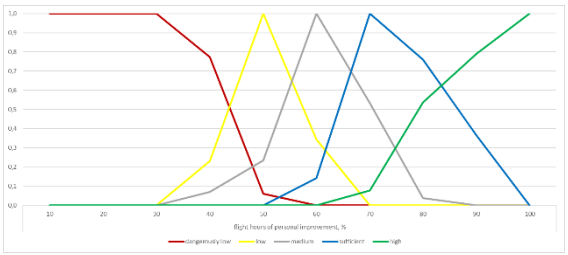


Figure 5: The membership function of the value of the linguistic variable "The flight hours of personal improvement"

4.4. Breaks in flights

In considering the linguistic variable "Breaks in flight", the author and experts, in addition to the empirical approach, took into account the requirements of the Fighter Training Course and the Rules of State Aviation. These documents set requirements for breaks in flights by type of training and meteorological conditions.

To describe the membership function of the linguistic variable "Breaks in flight" the terms were named T = {dangerously high; high; medium; acceptable; slight} and their limits in days K = [3, 42] were determined. The maximum value of each term was taken as 1.

The membership function for the linguistic variable "Breaks in flight" built in Microsoft Excel is shown in Figure 6.

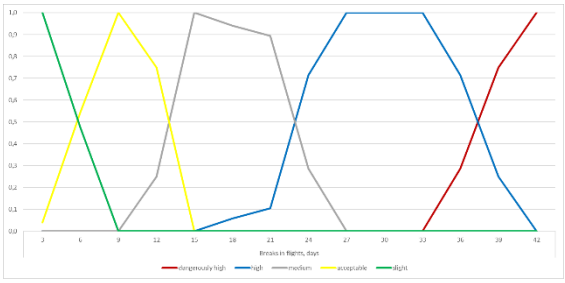


Figure 6: The membership function of the value of the linguistic variable "Breaks in flight"

4.5. Pilot's age

To perform tasks, the specifics of which are the speed of reaction and the body's ability to resist g-force during combat maneuvering, an important indicator that affects the progress of the task of the flight crew is its age. The value of the linguistic variable "Pilot's age" is understood by authors and experts as the length of the period from birth to the time of data input.

To describe the membership function of the linguistic variable "Pilot's age" the terms were named T = {unsuitable; admissible; suitable; optimal; regular} and their limits in years K = [20, 70] were determined. The maximum value of each term was taken as 1.

The membership function for the linguistic variable "Pilot's age" built in Microsoft Excel is shown in Figure 7.

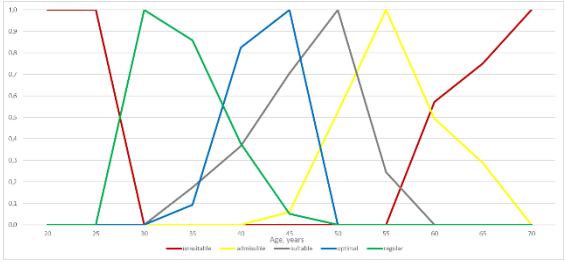


Figure 7: The membership function of the value of the linguistic variable "The flight hours of personal improvement"

5. Simulink model for calculating the level of readiness and appointment flight crews by missions

Based on the analysis of indicators that affect the level of crew readiness, the obtained quantitative indicators of the value of the linguistic variable "level of readiness" and processing of expert data, a hierarchical structure of the flight readiness level tree and their distribution by tasks in Simulink and shown in Figure 8.

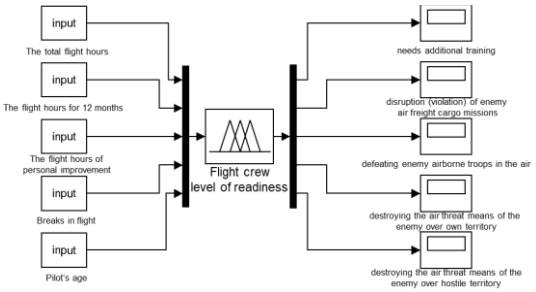


Figure 8: Simulink model of the flight crew level of readiness and appointment flight crews by missions

6. Construction fuzzy rules

Fuzzy control simulation is performed using the Fuzzy Inference System (FIS). For each FIS unit Model of calculation of the level of readiness and distribution of crews by tasks (Figure 8.) it is necessary to define a system of fuzzy rules.

Fuzzy rules "if-then" are the core of a fuzzy logic system because they combine all the other components and determine the output of the system. When assessing the level of readiness, input data are often assigned as indicators and results as readiness. Then fuzzy rules "if – then" are established for the ratio of readiness and set of indicators with a certain level of linguistic tolerance [14]. For example, the following is a fuzzy rule "if – then", consisting of two inputs and one output:

IF indicator 1 is low, AND indicator 2 is high, THEN readiness is average

The rules are built systematically, looking at all possible combinations of fuzzy sets of each input from the smallest to the largest. The consequences are adjusted so that the smallest sum of fuzzy sets is equal to the minimum, and the largest sum is equal to the maximum value of readiness. Subtotals are interpolated between these two values. The number of rules is the product of the number of fuzzy sets of each input. For example, for FIS "flight crew level of readiness" the number of logic inputs - 5, the number of terms of the output function - 5, the number of rules is $5^5 = 125$.

7. Crew readiness assessment results

The calculation of clear readiness values is carried out in the Simulink environment. The calculation model is presented in Figure 8. The input data are data of the total flight hours, the flight hours for 12 months, the flight hours of personal improvement, breaks in flights and the age of a pilot. At the output we get a numerical value of the readiness level from 0 to 1. An example of the obtained values is shown in Figure 9.

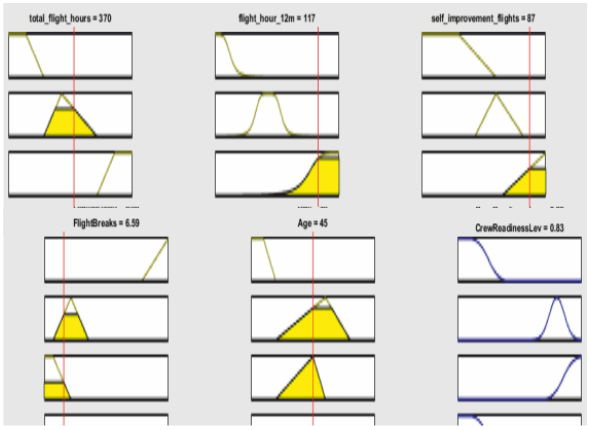


Figure 9: The calculation of clear readiness values in the Simulink environment

After receiving the numerical values of the crew readiness level, the obtained values are compared with the quantitative indicators of the "flight crew level of readiness". Depending on the complexity of the task, this figure varies. In case of discrepancy between the level of complexity of the task and the level of readiness of the crew, appropriate changes are made to the input data, the crew or task is replaced. If the level of

readiness and complexity of the task corresponds, the crew is assigning to a mission.

8. Conclusions

Thus, the authors analyzed the indicators that affect the readiness of the flight crews, which constitute the specifics of each particular task. Qualitative indicators of the level of readiness and their compliance with the complexity of the relevant missions are determined. Quantitative values of qualitative indicators of the readiness level of flight crew were also obtained.

The algorithm of determining the readiness level of the flight crew has been developed. The algorithm is implemented by the software package MATLAB: Simulink and Fuzzy Logic Designer.

The proposed methodology will allow to quantify the readiness level of the flight crew, to take timely measures to organize effective training of crews for possible tasks. By reducing the time in decision-making process in assigning flight crews on missions, taking into account the level of readiness of crews, and exclusion of a subjective approach in solving this task, the methodology could increase the efficiency of fighter aviation.

9. References

[1] A.S. Bonin, Osnovnye polozheniya metodicheskih podhodov k ocenke boevyh potencialov i boevyh vozmozhnostej aviacionnyh formirovanij, 1nd. ed., Voennaya mysl', Voen. Izd, Moscow, 2008, pp. 43-47.

[2] N.M. Skomorohov (Ed.), Bor'ba za gospodstvo v vozduhe, Voenizdat, Moscow, 1990.

[3] B.I. Semon, Suchasnyi metod boiovykh potentsialiv v prykladnykh zadachakh planuvannia rozvytku ta zastosuvannia taktychnoi aviatsii, NAOU, Kyiv, 2009.

[4] V.N. Shubin, Modelirovanie boevyh dejstvij aviacionnyh chastej i soedinenij pri unichtozhenii vozdushnogo protivnika, Monino, VVA im. YU.A. Gagarina, 1989.

[5] Doc № 79/26524, Instrukciya pro klasifikaciyu aviacijnogo personalu derzhavnoi aviacii Ukrainy, Ofic. vid., MOU, Kyiv, 2015.

[6] S.S. Drozdov, Metodychnyi pidhid do kil'kisnogo ociniuvannia vplyvu rivnia pidgotovlenosti ekipazhiv na bojovu mogutnist' bojovogo skladu taktichnoi aviacii, Nauka i tekhnika Povitrianih Syl Zbrojnyh Syl Ukrainy 3 (24) (2016), 49–53.

[7] Y. Goncharenko, O. Blyskun, O. Martyniuk et al., Flight safety fuzzy risk assessment for combat aviation system, in: Proceedings of the 2nd. IEEE International Conference on Advanced Trent in Information Theory, Kyiv, 2020, pp. 132–137.

[8] Doc 82/26527, Pravyla vykonannya pol'otiv v derzhavnij aviacii Ukrainy, Ofic. vid., MOU, Kyiv, 2015.

[9] V.I. Gostev (Ed.), Nechetkie regulyatory v sistemah avtomaticheskogo upravleniya, Radioamator, Kyiv, 2008.

[10] A.N. Borisov, Prinyatie reshenij na osnove nechetkih modelej: primery ispol'zovaniya, Zinatne, Riga, 1990.

[11] V. Harchenko, T. Shmel`ova, Yu. Sikirda, Pryjnyattya rishen v sociotexnichnyh systemah: monograph, NAU, Kiyv, 2016, ISBN 978-966-932-010-0.

[12] O.M. Kernic'kij, Metodyka formuvannya psihologichnoi gotovnosti kursantiv-l'otchikiv do l'otnoi diyal'nosti, Ph.D. thesis, Kharkiv University of Air Force, Kharkiv, 2005.

[13] Doc, Metodychni rekomendacii z psyhologichnoi pidgotovky l'otnogo skladu pid chas organizacii zahodiv kolektyvnoi pidgotovky osobovogo skladu Povitryanih Syl Zbrojnyh Syl Ukrainy, Ofic. vid., PS ZSU, Vinnytsia, 2015.

[14] A. Leonenkov, Fuzzy modeling in Matlab and Fuzzy Tech, St. PTB, BHV, 2003, ISBN 5-94157-087-2.

Methods of quality assurance of software development based on a systems approach

Iryna Ushakova[1], Yuri Skorin[1], Alexander Shcherbakov[1]

[1] *Simon Kuznets Kharkiv National University of Economics, Nauky Ave., 9-A, Kharkiv, 61166, Ukraine*

Abstract

The aim of the work is to analyze the problems and develop recommendations for quality assurance of software and testing during its creation in IT companies based on a systems approach. The object of research is the processes of testing, quality control and quality assurance. The subject of the study is the functions of quality assurance (QA) and testing (QC) within the system of development and the characteristics and models of quality assessment and software dependability. The research processes used a systematic approach, comparative analysis of quality assessment methods and approaches to the organization of testing, quality control and quality assurance of software products. The essence and main differences of the concepts "testing", "quality control" and "quality assurance" were determined. To assess the quality of the software, various aspects of quality in accordance with international standards, the relationship between them and a multi-level model of software quality were considered. To ensure the quality of the software product, it was proposed to use methods of integrated quality assessment, which allow to obtain the final integrated value of software quality as a whole, expressed in certain quantitative indicators, or its individual characteristics, and considered the most common methods based on costs and hierarchical models. A systematic approach to software quality assurance involves the creation of a QA team, which is an independent subsystem within the software development system while maintaining links with team members. To assess the differences between quality control and quality assurance, an analysis of responsibilities, work planning and documentation of relevant groups in IT companies was conducted, which made it possible to compare the functions performed and working conditions. Thus, the QC function confirms that a specific result meets standards and specifications, and QA is a broader function that covers planning and control throughout the development lifecycle. Testing is an integral part of quality control. In order for an IT company to provide management processes, QA and QC teams must work together. The scientific novelty of the work is to develop a methodological basis for assessing the quality of software, developing recommendations for improving the processes of quality assurance and testing in software development in an IT company.

Keywords

Software, testing, quality control, quality assurance, dependability, security, quality model, metrics, quality indicators, system approach

1. Introduction

The fourth industrial revolution, of course, poses great challenges for "traditional" software development. This is due to the unpredictable behavior of software systems, lack of centralized control, cybersecurity, scalability, fault tolerance, reliability, development, definition of interfaces and communication channels and their management. However, most of these problems can also be seen as opportunities for further development of software development and testing processes [21, 24].

EMAIL: varavina.ira@gmail.com (Irina Ushakova); skorin.yuriy@gmail.com (Yuri Skorin); oleksandr.shcherbakov.kafis@gmail.com (Alexander Shcherbakov)
ORCID: 0000-0001-8315-0917 (Irina Ushakova); 0000-0002-4613-3154 (Yuri Skorin); 0000-0001-8315-0917 (Alexander Shcherbakov)

Quality assurance or software quality assurance is an integral part of the development process and is used in the IT industry by quality assurance professionals as well as testers. Quality assurance is associated with the concept of dependability. Dependability is, first, a guarantee of increased cybersecurity, reliability and protection against failures. In cases where the failure of a software system that belongs to the class of "high confidence" or "high integrity system" can lead to extremely negative consequences, the overall warranty of the system, which includes hardware, software and man, is the main and priority quality requirement in relation to the main functionality of the system.

Both quality assurance and software testing are designed to guarantee the quality of the software application that meets customer requirements. However, these two concepts have a fundamental difference. Testing is performed after the application has been created or for static testing after the software requirements have been defined and recorded in the relevant document [11]. Quality assurance involves activities that ensure the quality of the application during its creation at all stages, from the definition of requirements to the transfer of the finished application to the customer [17].

To understand the differences between these components of the software development process, it is necessary to give a clear definition of these concepts, to relate between their characteristics, to determine methods for assessing the quality of software.

Successful solution of software quality assurance problems is possible only with a systematic approach to software development processes, active involvement of quality assurance specialists and testers, so the work will identify differences between the responsibilities of these specialists, differences in planning tests and documentation, as well as developed recommendations for improving software development processes in terms of quality assurance.

The main purpose of the article is to analyze the problems and develop recommendations for quality assurance of software and testing during its creation in IT companies based on the principles of a systems approach.

2. Review of literature sources

To clarify the differences between the concepts of testing and software quality assurance, consider the related concepts of "testing", "quality control" and "quality assurance", which are widely covered both in the domestic literature and in foreign sources. [6-9, 11, 17].

Software testing according to ISO / IEC TR 19759: 2005 is a process of research, software testing, which aims to verify the correspondence between the actual behavior of the program and its expected behavior on the final set of tests selected by a particular.

Quality Control (QC) according to ISO 9000 is a part of quality management focused on compliance with the requirements for assessing the number of defects, bugs (if any) in the application. Quality control role is a set of processes (actions) aimed at assessing the developed application (draft document, development system, etc.) and compliance with customer requirements. Execution of these processes guarantees check of quality of the delivered application and defines, how well it is designed and executed. The purpose of quality control is to find defects and ensure their correction. Thus, testing is an integral part of quality control (fig. 1).

Quality Assurance (QA) is defined in ISO 9000 as a part of quality management that focuses on ensuring that defect elimination requirements are met. The purpose of quality assurance is to ensure that the application will meet customer requirements. Quality assurance consists of processes aimed at ensuring the quality of application development at each stage of the life cycle. These actions usually precede application development and continue while the process is under development. Quality assurance is responsible for the development and implementation of processes and standards to improve the development life cycle, and to ensure that these processes are performed [1, 2]. The main purpose of quality assurance is to prevent defects at all stages of software development and its continuous improvement. While quality assurance is an activity aimed at ensuring the development of quality software, quality control is an activity that captures and evaluates the quality of an already created application. So testing is a subsystem of quality control, and quality control is a subsystem of quality assurance system.

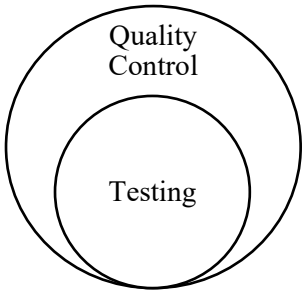


Figure 1: The relationship between the concepts of "testing" and "quality control"

The relationship between quality assurance, quality control and testing shows in fig. 2. Quality assurance activities include setting standards and processes, quality control, and selecting appropriate tools.

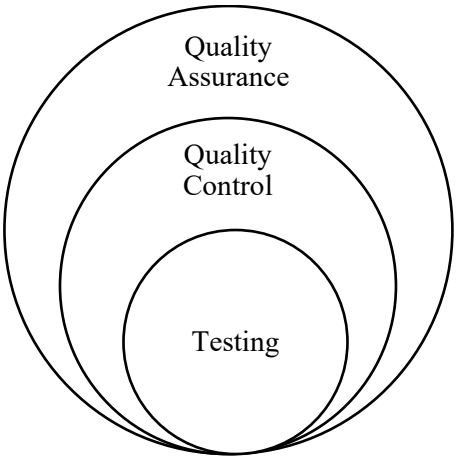


Figure 2: The relationship between QA, QC and Testing

The quality of software is defined in ISO 9126 as the whole set of its characteristics related to the ability to meet the stated or implied needs of all stakeholders.

There are the following aspects of software quality [6]:

1. The quality of technological processes of software development, which affects the creation of quality software;
2. The internal quality of the software associated with its characteristics, without taking into account the behavior of the software application;
3. External quality that characterizes the software in terms of its behavior;
4. The quality of the software when used in different contexts, that is the quality of the software application, which is manifested in its use by users in different specific scenarios.

Metrics have been created for all these aspects of quality that allow them to be evaluated

In fig. 3 shows the relationship of different aspects of software quality.

In addition, the standard describes a multi-level software quality model that can be used to describe both internal and external software quality (fig. 4). At the top level of the model there are 6 main characteristics of software quality, each of which has its own attributes:

functionality: ability to interact, functional suitability, compliance with standards and rules, security, accuracy;

reliability: completeness, ability to recover, compliance with standards, resistance to failure;

usability: intelligibility, ease of learning, ease of operation, attractiveness, compliance with standards;

productivity: time efficiency, resource efficiency, compliance with standards;

ease of maintenance: analysis, ease of making changes, stability, ease of verification, compliance with standards;

transfer: adaptability, ease of installation, ability to coexist, ease of replacement, compliance with standards.

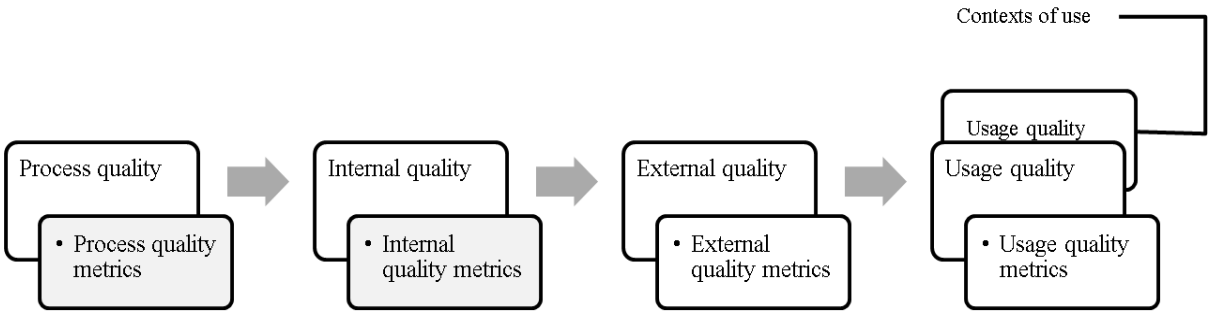


Figure 3: Communication of different aspects of software quality according to ISO 9126

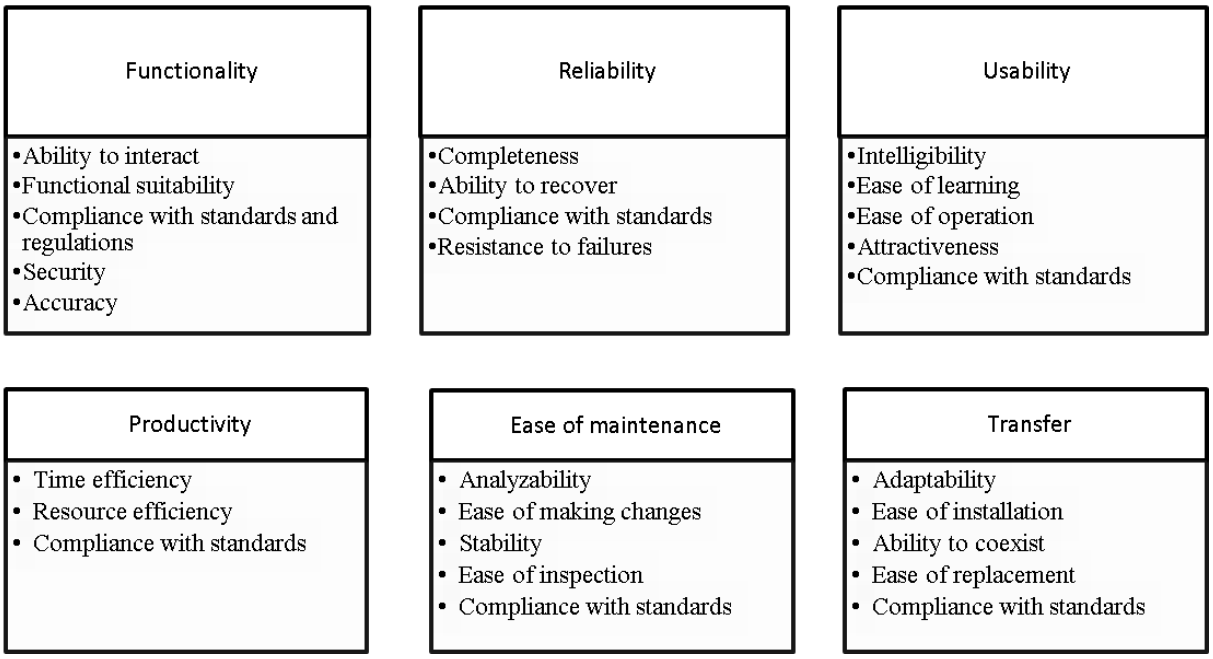


Figure 4: Multi-level software quality model according to ISO 9126

A set of metrics is defined for each attribute that allow it to be evaluated. Metrics must have the following properties:

1) reliability; which is associated with an accidental error; the metric is free from random error, if random changes do not affect the results of the metric;

2) recurrence; the re-use of metrics for the same application and by the same evaluators when using the same evaluation specification (including the environment), the same type of users and environment, should lead to the same results with appropriate tolerances; appropriate tolerances should take into account such components as fatigue and the result of accumulated knowledge;

3) uniformity; the application of metrics for the same application by different assessment professionals using the same assessment specification (including the environment), the same type of users and environment, should lead to the same results with appropriate tolerances;

4) possibility of application; the metric must clearly indicate the conditions (for example, the presence of certain attributes) that limit its use;

5) showiness; it is the ability of a metric to identify parts or elements of a program that need to be improved, based on a comparison of measured and expected results;

6) correctness; the metric must have the following properties:

objectivity; the results of the metric and its input should be based on facts and not be subject to the feelings or opinions of experts in assessment or testing (excluding metrics of satisfaction or attractiveness, which measure the feelings and opinions of the user);

impartiality; the measurement should not be aimed at obtaining any specific result;

adequacy of accuracy; accuracy is determined when designing metrics and especially when choosing descriptions of facts that are used as a basis for metrics; the metric developer must describe the accuracy and sensitivity of the metric;

7) significance; the measurement must give significant results concerning the behavior of the program or the quality characteristics.

Metrics must also be cost-effective. This means that more expensive metrics should provide better evaluation results [1, 2].

The developer of the metric must prove its validity. The metric must meet at least one of the following criteria for the validity of the metric:

1) correlation; the change in the values of quality parameters (promptly determined by measuring the basic metrics), due to a change in the values of the metric, should be determined by a linear relationship;

2) tracing; if the metric M is directly related to the value of the quality characteristic Q, then the change in value $Q(T_1)$, available at the time T_1, to the value of $Q(T_2)$, obtained at time T_2, must be accompanied by a change in the value of the metric from $M(T_1)$ to $M(T_{12})$ in the same direction (for example, if Q increases, then M also increases);

3) consistency; if the values of quality characteristics (promptly obtained by measuring the main metrics) $Q_1, Q_2, \ldots, Q_n$, associated with applications or processes 1,2 ..., n, are determined by the ratio $Q_1 > Q_2 > \ldots > Q_n$, associated with applications or processes 1,2 ..., n, are determined by the ratio $M_1 > M_2 > \ldots > M_n$;

4) predictability; if the metric is used at time T_1 to predict the value (promptly obtained by measuring the main metrics) of the quality characteristics Q at time T_2, the prediction error must fall within the allowable range of prediction errors:

$$(Q_p\ (T_2) - Q_f\ (T_2))\ /\ Q_f\ (T_2), \qquad (1)$$

where $Q_p\ (T_2)$ – the forecast value of the quality characteristics at the time T_2,

$Q_f\ (T_2)$ – the actual value of the quality characteristic at the time $T_{2;}$;

5) selectivity; the metric must be able to distinguish between high and low quality software.

Improving the quality of software development and testing allows you to create a software application that meets customer requirements [10, 12-15]. Attention should be paid to the thorough improvement of all software development processes, both directly related to the development of perfect software code and all processes that affect its quality: definition and management of requirements, creation of test scenarios and testing as early as possible (starting with requirements testing), organization of teamwork, division of responsibilities between participants in the process, etc.

Recently, considerable attention in the field of software quality assurance is paid to warranty. Dependability of software includes such characteristics as fault tolerance, safety of use (safety in the context of acceptable risk to human health, business, property, etc.), information security or security - protection of information from unauthorized transactions, including access

to reading, as well as guaranteeing the availability of information to authorized users, in the amount of their rights), as well as convenience and ease of use (usability) [27]. Reliability is also a criterion that can be defined in terms of warranty.

Special attention is paid to creating a perfect code despite the current trends in the field of information technology and in particular testing, [3-5, 16].

Analysis of modern strategies, approaches and methods of testing, identification of their advantages and disadvantages paid attention in [22, 25].

Ways to solve the problem of improving the quality of software development and testing can be the introduction of appropriate methods in IT companies to assess the quality of software, which will contribute to its warranty.

3. A systematic approach to improving quality assurance and testing processes in software development

The need for software quality assurance increases with the size of the organization and the level of its quality policy. Quality assurance is a complex multifaceted process. Therefore, the system approach provides its required level in full. This approach considers quality assurance as a separate subsystem, which is part of the development system, has certain connections with it, as well as certain independence as a system. The IT Company creates a QA group (quality assurance group). It is important that the QA function remains independent of project management and operations. But the links between the QA team and the project team are very important and should provide them with strong support.

Some organizations have a QA feature built into the project management office. Such a model also meets the criteria of independence. However, with such an organization, you need to make sure that the QA group consists of qualified quality assurance analysts.

Given the differences between the concepts of software testing, quality control and quality assurance, there are also differences between the responsibilities of the QA group and testers.

The responsibilities of testers include:

testing planning,

writing test scripts and test cases, checking tests,

performing tests,

analysis of test results,

creation and analysis of reporting on test results for different levels of tests.

As part of their quality control role, testers may make demands on:

checking samples of project documents,

activities for managing software configurations, design, code, etc.

At the same time, the QA group performs the functions:

formation of organizational policy on quality, standards and development processes;

providing assistance with quality assurance training and project quality assurance plans;

checking compliance between project processes and quality plans;

conducting regular inspections of design applications and processes;

regular presentation of the results of quality assessment analysis to management;

resolving a situation with a deviation from guidelines or standards.

As part of its quality assurance role, the QA group monitors:

independent reviews;

availability of project change management procedures;

availability of project configuration management procedures;

availability of retrospective planning and implementation of development life cycle processes;

quality assurance based on the development of the life cycle system;

carrying out continuous improvement in the process of quality control and implementation of recommendations based on previous experience.

Performing the duties of the QA group does not mean their development by the team, but only ensuring their implementation.

When planning tests, testers prepare test strategies and plans based on basic test documents, such as software application requirements and design solutions. These test planning documents are the basis for the implementation of processes at various planned test levels. For each level of testing, tests, sets of input data and expected results, detailed test schedules, environmental requirements, documents for defect management, test management and reporting are compiled. In contrast, software application quality assurance

documentation or quality plans include a broader set of actions throughout all stages of development. This affects the project management methodology.

A typical draft quality plan includes customer expectations, acceptance criteria, planned quality control and process audits, configuration management plans, and change management procedures. Quality plans are based on the organization's own policies, standards, or guidelines that form the basis of quality assurance. The project quality assurance plan is monitored continuously and the planned quality indicators are updated on its basis during the project creation. There are different intersections between risk management and quality, and therefore the risk register can make a significant contribution to the preparation of quality plans.

Recommendations for improving quality assurance processes:

independence. To be successful the QA group must be dependent on the project team. This provides the QA group with the opportunity to conduct an objective evaluation of projects. Testers and QA specialists can be in the same group in small organizations. However, there is a possibility of creating a conflict of interest in monitoring the testing activities. The solution depends on the policy of the organization in the field of quality and is as follows. A separate group can be created for reporting;

relationships within the project team. Quality assurance analysts may be overly process-oriented and may insist on processes or documentation that are of little relevance to the project. This can worsen relationships with project managers. It will be much easier for the QA group to work with project teams if they work on the principle of taking into account the project objectives. In addition, the assistance and assistance of project teams forms the basis for maintaining good relations. This is an important aspect of successful testing;

involvement of the necessary specialists. Qualitative HR policy plays a leading role in the successful operation of the QA Group. People with experience in LC development who have knowledge of ISO standards and CMMI principles for software development have the necessary competencies for the QA team;

requirements list. Standard checklists are a useful mechanism for auditing projects, especially if they are designed in accordance with the LC phases. To ensure fruitful cooperation with project managers, it is important to ensure the participation of stakeholders in the project. This makes it possible to get feedback from them in response to suggestions for changes to the lists;

communication and reporting. Regular reporting is very important to management, developing the right templates and metrics to provide management with the information it needs to ensure that these reports are given the proper attention. This is best achieved by meeting with relevant senior management representatives, providing them with reports and receiving feedback and comments from them. In addition, the QA team must continually obtain approval for changes to quality control processes and standards and ensure effective communication with stakeholders;

constant improvement. Taking into account previous experience provides the QA team with a basis for evaluating processes and recommendations for quality assurance, including continuous improvement. The QA team must be flexible, maintain good relationships with stakeholders when making improvements in management reporting. Continuous improvement may also require amendments to the methodology of development of software systems, so QA group recommended to keep development methodology IT company.

4. Introduction of methods of integrated quality assessment of software applications

Methods of integrated quality assessment have the advantage that they allow to obtain the final integrated value of the quality of the software as a whole or its individual characteristics, expressed in certain quantitative indicators. Cost-based and hierarchical model-based methods of integral software quality assessment are the most common.

The method of integrated software quality assessment, which is based on costs, belongs to the group of calculation methods. According to this method, a quantitative criterion of software quality T is formulated, focused on its life cycle. (LC).

The costs of software development, operation and maintenance include:

R – one-time software development costs;

V – one-time software implementation costs;

E – recurring costs S for software operation for the period of operation time t_e during the life cycle T:

$$E = (\mathrm{T} / t_e) * S; \quad (2)$$

C – repeated at random intervals maintenance costs, which are on average $n-th$ part of the costs R and $m-th$ part of the costs V and are carried out during the life cycle T on average over time t_c:

$$\mathrm{C} = (n * R + m * V) * \mathrm{T} / t_c; \quad (3)$$

B – accidental losses due to unreliability or lateness of the result:

$$\mathrm{B} = S_\mathrm{e} * \mathrm{T} / t_\mathrm{e}, \quad (4)$$

where S_e – the average amount of losses incurred by a single operation of the software during its LC.

Thus, the total cost Z in the software life cycle of the software will be determined as follows:

$$Z = R + V + (S_\mathrm{e} + S) * \frac{\mathrm{T}}{t_\mathrm{e}} + \\ +(n * R + m * V) * \mathrm{T} / t_\mathrm{c}, \quad (5)$$

As a quality criterion, it is proposed to use the minimization of total costs for software development, operation and maintenance. The criterion for software quality is to minimize the total cost Z:

$$Z \rightarrow min. \quad (6)$$

The main disadvantage of this method is that the actual cost values included in the formula can be determined after the development of the software application, and therefore it cannot be used as a tool in the development process to achieve a given level of quality.

The choice of the nomenclature of quality indicators according to the method of quality assessment based on a hierarchical model for a particular software application is based on its purpose and requirements for the scope depending on the affiliation of the software to a subclass determined by the software classifier:

operating systems and means of their expansion;

database management software;

tool-technological means of programming;

software applications for interface and communication management;

software applications for the organization of the computational process (planning, control);

service programs;

software applications for computer maintenance;

research applications;

design applications;

applications for control of technical devices and technological processes;

applications for solving economic problems;

other software applications.

Evaluation of software quality is the choice of nomenclature of indicators, their evaluation and comparison with the basic values. A four-level hierarchical quality model is the basis of this evaluation method. It includes:

level 1 - quality characteristics;

level 2 - quality attributes;

level 3 - metrics;

level 4 - evaluation indicators (software attributes).

For each of the selected quality characteristics, a four-level hierarchical model is developed, which reflects the relationship of characteristics, attributes, metrics and indicators. The type of this model depends on the phase of the LC.

Tables are used for practical application of the model. These tables are created for each characteristic. So to assess the characteristics of information security, you can use the indicators that are in table 1.

Table 1

Indicators of assessment of the characteristic of information security

Indicator	Evaluation method	Evaluation form
Proportion of incidents by type, P_t	Registration, calculated	$P_t = \frac{KS_t}{\sum_t KI_t}$, (7) KI_t – the number of $t-th$ incidents

Proportion of deadlines incidents, P_s	Registration, calculated	$P_s = \frac{KI_s}{KI}$, (8) KI_S – the number of incidents closed in time KI – the total number of incidents
Probability of trouble-free operation, P	Registration, calculated	$P = 1 - q/n$, (9) n – number of tests, q – number of registered failures

Quality assessment is a deterministic process that consists of certain stages. Its implementation involves the main stages:

determining the purpose of evaluation,
development of quality model,
creating a model of metrics,
search for basic metrics,
determination of derived metrics,
formalization of metrics,
determination of metric limit values,
determination of actual values of metrics,
definition of integrated software quality assessment,
software quality analysis.

The first stage involves determining the purpose of evaluation:

evaluate the quality of the finished software application, for example in accordance with the quality standard;

evaluate the quality of the software application during its development.

A certain model of integrated assessment is chosen depending on the goal and then consistently performs certain steps.

To determine, for example, the proportion of incidents of a certain type, it is necessary to record all incidents for a certain period. Then the percentage of a certain incident is determined (table 2). To assess the quality of software for this indicator, the values are compared with the allowable value. These data are used for analysis (fig. 4) and subsequent integrated evaluation of application quality.

Table 2

Proportion of incidents "Injection of malicious code", 01-06/2021

Month	01	02	03	04	05	06
Proportion of incidents,%	20	22	18	16	20	14

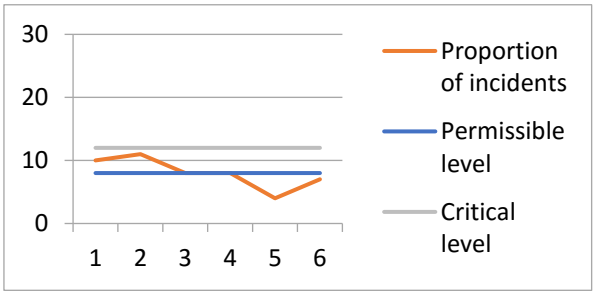


Figure 4: Proportion of incidents "Injection of malicious code"

To ensure quality in the process of software application development, both methods should be used:

to perform quality assessment during development to quickly ensure compliance of processes with certain standards and compliance of the software application with customer requirements,

to estimate the total cost of development, operation and maintenance of the finished software application with.

5. Conclusions

The paper compares the concepts of "testing", "quality control" and "quality assurance", which showed that testing is part of quality control, and quality control coincides with quality assurance in the field of quality control. Dependability, which includes fault-tolerance, safety, information security or security, as well as usability, should be provided primarily for software systems of high reliability, high availability within the quality guarantee.

Software quality assessment should take into account international standards in this field, which define various aspects of quality, such as process quality, internal quality, external quality and quality of use. To assess quality, it is recommended to use a multi-level model that includes the following characteristics:

functionality,
reliability,

usability,
productivity,
convenience of support,
transfer.

From the point of view of the systems approach, quality assurance can be defined as a separate subsystem, which is a component of the development system, has certain connections with it, as well as a certain independence as a system. To assess the differences between quality assurance and quality control processes, an analysis of the responsibilities of the relevant groups of specialists, their work planning and documentation was carry out, which made it possible to compare the functions performed and working conditions. Thus, QC functions are aimed at confirming that specific results meet standards and specifications, and QA is a broader function. It covers planning and control throughout the development lifecycle. Testing is an integral part of quality control. In order for an IT company to have effective quality management processes, the QA and QC group must work together.

A successful QA group can add significant value to an organization, namely:

improving the quality and warranty of software applications;
consistency in the delivery of software applications;
improving the organization of processes;
reduction of total delivery costs;
use applications for application support documentation.

At the same time, it should be borne in mind that QA specialists require additional costs:

firstly, in the staffing schedule for software quality analysts,
secondly, due to the complexity of processes.

At the beginning of implementation it may adversely affect the team.

Software quality assurance requires the introduction of integrated quality assessment methods and individual quality indicators. Integrated evaluation processes include:

defining the purpose of evaluation,
developing a quality model,
creating a model of metrics,
searching for basic metrics, defining derived metrics,
formalizing metrics,
defining metric limits,
determining actual metric values,
defining integrated software quality assessment,
software quality analysis.

To ensure quality, it is necessary to carry out its operational integrated assessment at all stages of LC and integrated assessment of costs for development, operation and maintenance of the finished software application.

6. References

[1] Dzh. Folk, Kaner, E. Nhuen, Testyrovanye prohrammnoho obespechenyia. Fundamentalnыe kontseptsyy menedzhmenta byznes–prylozhenyi, per. s anhl., Yzdatelstvo «Dya-Soft», Kyev, 2001.

[2] K. A. Kulakov, V. M. Dymytrov, Osnovы testyrovanyia prohrammnoho obespechenyia, Yzdatelstvo PetrHU, Petrozavodsk, 2018.

[3] Dzh. Makhrehor D. Saiks, Testyrovanye obъektno-oryentyrovannoho prohrammnoho obespechenyia, Dyasoft, Kyev, 2002.

[4] S. Makkonnell, Sovershennыi kod. Master-klass, Yzdatelsko-torhovыi dom «Russkaia redaktsyia», Moskva, Sankt-Peterburh, Pyter, 2005.

[5] M. A. Plaksyn, Testyrovanye y otladka prohramm dlia professyonalov budushchykh y nastoiashchykh, 2-e yzd. (эl.), BYNOM. Laboratoryia znanyi, Moskva, 2013.

[6] Prohramna inzheneriia. Yakist produktu. Chastyna 1. Model yakosti (ISO/IEC 9126-1:2001, IDT): DSTU ISO/IEC 9126-1:2013, Chynnyi vid 2014-07-01, MINEKONOMROZVYTKU Ukrainy , Kyiv, 2014.

[7] Prohramna inzheneriia. Yakist produktu. Chastyna 2. Zovnishni metryky (ISO/IEC TR 9126-2:2003, IDT): DSTU ISO/IEC TR 9126-2:2008,Chynnyi vid 2010-07-01, Derzhspozhyvstandart Ukrainy, Kyiv, 2011.

[8] Prohramna inzheneriia. Yakist produktu. Chastyna 3. Vnutrishni metryky (ISO/IEC TR 9126-3:2003, IDT): DSTU ISO/IEC TR 9126-3:2012,Chynnyi vid 2013-05-01, MINEKONOMROZVYTKU Ukrainy, Kyiv, 2013.

[9] Prohramna inzheneriia. Yakist produktu. Chastyna 4. Metryky yakosti pid chas vykorystannia (ISO/IEC TR 9126-4:2004, IDT): DSTU ISO/IEC TR 9126-4:2012, Chynnyi vid 2013-05-01, MINEKONOMROZVYTKU Ukrainy, Kyiv, 2013.

[10] S. V. Synytsыn, N. Yu. Naliutyn, Veryfykatsyia prohrammnoho obespechenyia, Yntuyt NOU, Moskva, 2016.
[11] Testuvannia prohramnoho zabezpechennia URL: https://uk. wikipedia.org/ wiki/%D0%A2%D0%B5%D1%81%D1%82%D1%83%D0%B2%D0%B0%D0%BD%D0%BD%D1%8F_%D0%BF%D1%80%D0%BE%D0%B3%D1%80%D0%B0%D0%BC%D0%BD%D0%BE%D0%B3%D0%BE_%D0%B7%D0%B0%D0%B1%D0%B5%D0%B7%D0%BF%D0%B5%D1%87%D0%B5%D0%BD%D0%BD%D1%8F.
[12] I. O. Ushakova, Metodyka upravlinnia vymohamy v hnuchkykh metodolohiiakh, Zbirnyk naukovykh prats KhNUPS, Vyp. 2(56) (2018): 93 – 98.
[13] I. O. Ushakova, Proektuvannia informatsiinykh system: praktykum, KhNEU im. S. Kuznetsia, Kharkiv, 2015.
[14] I. O. Ushakova Roli i kliuchovi yakosti IT-spetsialista, v: Tezysы VII Mezhdunarodnoi nauchno-praktycheskoi konferentsyy “Problemы y perspektyvы razvytyia, 2015, s. 23.
[15] I. O. Ushakova, Systemnыi podkhod k upravlenyiu trebovanyiamy pry proektyrovanyy ynformatsyonnыkh system, v: Ynformatsyonnыe systemы v upravlenyy, obrazovanyy, promыshlennosty : monohrafyia. Vyd. TOV «Shchedra sadyba plius», Kharkiv :, 2014, ss. 86-91.
[16] M. Fauler, Refaktorynh. Uluchshenye sushchestvuiushcheho koda, per. s anhl., Symvol-Plius, Sankt-Peterburh, 2003.
[17] Iakist prohramnoho zabezpechennia. URL: https://uk.wikipedia.org/wiki/%D0%AF%D0%BA%D1%96%D1%81%D1%82%D1%8C_%D0%BF%D1%80%D0%BE%D0%B3%D1%80%D0%B0%D0%BC%D0%BD%D0%BE%D0%B3%D0%BE_%D0%B7%D0%B0%D0%B1%D0%B5%D0%B7%D0%BF%D0%B5%D1%87%D0%B5%D0%BD%D0%BD%D1%8F.
[18] H. Foidl, M. Feldere. Integrating software quality models into risk-based testing, Software Quality Journal, V 26 (2018): 809 – 847.
[19] H. V. Gamido, M. V. Gamido, Comparative review of the features of automated software testing tools, International Journal of Electrical and Computer Engineering, Vol. 9, No. 5, (2019): 4473~4478
[20] P. M. Jacob, P. A. Mani, Framework for evaluating performance of software testing tools, Journal of Scientific and Technology Research, V. 9, Iss. 2 (2020): 2175–2180.
[21] R. S. Kenett, R. S. Swarz, A. Zonnenshain, Zonnenshain. Systems Engineering in the Fourth Industrial Revolution: Big Data, Novel Technologies, and Modern Systems Engineering, Wiley, New York, NY, 2020.
[22] R. Pietrantuono, On the testing resource allocation problem: Research trends and perspectives, Journal of Systems and Software, V. 161 (2020): 42 p.
[23] A. A. Sawant, P. H. Bari, P. M. Chawan, Software Testing Techniques and Strategies, International Journal of Engineering Research and Applications, Vol. 2, Iss. 3 (2012): 980-986.
[24] Software Testing, Verification and Reliability: Special Issue 10th IEEE International Conference on Software Testing, Verification, and Validation (ICST 2017), Software Testing, Verification and Validation, Vol. 30, Iss. 7–8. (2020). URL: https://onlinelibrary.wiley. com/toc/10991689/2020/30/7-8:
[25] V. Garousi, A. Rainer, P. Lauvås jr, A. Software-testing education: A systematic literature mapping, Journal of Systems and Software, V. 165 (2020). URL: https://www.researchgate.net/ publication/339814384_Software-testing_ education_A_systematic_literature_ mapping.
[26] Try QA. URL: http://tryqa.com/
[27] N. G. Bardis, N. Doukas, V. Kharchenko, Vl. Sklyar, S. Yaremchuk, Dependable IoT for Human and Industry: Modeling, Architecting, Implementation, in: Approaches and Techniques to Improve IoT Dependability, River Publishers, 2019, pp. 307-328.

Cyber Defense Is A Modern Component Of Ukraine's Security

Oleksandr Lavrut [1], Tetiana Lavrut [2], Vladyslav Kolesnyk [3], Halyna Kolesnyk [4], Serhii Bohutskyi [5] and Leonid Polishchuk [6]

[1,2,3,5,6] *Hetman Petro Sahaidachnyi National Army Academy, 32 Heroes of Maidan street, Lviv, 79026, Ukraine*
[4] *Lviv Polytechnic National University, 12 Bandera street, Lviv, 79013, Ukraine*

Abstract

The report is devoted to the topical issues of cybersecurity in modern society. It is shown that with the beginning of the war in eastern Ukraine, both the population and infrastructure of Ukraine are significantly affected by cyber attacks. The examples of ways to solve cybersecurity issues in the civil society as well as in the security apparatus of Ukraine that have already been implemented are given. The authors also consider the prospects for the development of this area.

Keywords

cyber security, cyber defense, cyber threat, cyberspace, cyber attack

1. Introduction

In the era of globalization, information technology and telecommunication systems occupy all spheres of human life and the state activity. The volumes of information are growing, technical means are changing, and, accordingly, the risks of information security in information and telecommunication systems are growing both in the civil society and in the security apparatus [7, 9]. Security depends on the use of available opportunities and the proper reaction to emerging threats in cyberspace. Essential infrastructure, national defense and the daily lives of citizens depend on computer and interconnected information technologies. All spheres of life have become more dependent on secure cyberspace; new vulnerabilities are identified and the number of new threats grows.

Cyberspace, along with land, air, sea, and space, is recognized as a new operational space, and cyberspace is an integral part of the hybrid war. Leading countries of the world such as the United States, Great Britain, China and others pay the most attention to operations in cyberspace.

Therefore, the issue of security in cyberspace has always been urgent in the world. Today, the consequences and effectiveness of cyber weapons can be equated to weapons of mass destruction.

2. Measures to ensure cyber protection in the state

Since the beginning of the confrontation with Russia, cyberspace has become another platform for military action. The experience shows that the population and infrastructure of any state are really affected by cyber attacks Today, everyone is a subject of cyberspace. The laptop, tablet, mobile phone are potentially vulnerable gadgets. The simplest threat that anyone in the world can face is sending links and phishing emails with incomprehensible suggestions. Such emails can download malicious software, block your phone or computer, break into your system, extort money, use your personal information, and more. That is why cyber defense reform has begun in Ukraine [6].

The National Cyber Security System of Ukraine is a set of subjects of cyber security and interconnected measures of political, scientific and technical, informational, educational nature, organizational, legal, operational and investigative, intelligence, counterintelligence, defense, engineering and technical measures, as

EMAIL: alexandrlavrut@gmail.com (A. 1); lavrut_t_v@i.ua (A. 2); vector-ua@ukr.net (A. 3); galyna.o.kolesnyk@gmail.com (A. 4); sergij-b@ukr.net (A. 5); vl.kolesnyk@ukr.net (A. 6)
ORCID: 0000-0002-4909-6723 (A. 1); 0000-0002-1552-9930 (A. 2); 0000-0001-5257-3124 (A. 3); 0000-0003-1912-1649 (A. 4); 0000-0001-7454-8894 (A. 5); 0000-0002-4379-3990 (A. 6)

well as measures of cryptographic and technical protection of national information resources, cyber protection of critical information infrastructure [4].

Our state has to to react quickly to new threats and search for effective cyber defense measures. The issue of cyber defense in the country can be solved only through a comprehensive approach. Some decisive steps have already been taken in this direction at the state level. Thus, during the All-Ukrainian Forum "Ukraine 30. Country Security" the Cyber Security Center was opened. The center is a structural subdivision of the State Service for Special Communications. The institution will be oriented as a service structure that will provide cybersecurity services, ranging from individuals to public authorities. One of the heads of the State Service for Special Communications and Information Protection of Ukraine, Deputy Head of the State Special Communications Service Oleksandr Potiy presented the Organizational and Technical Model of cyber defense during his speech at the scientific-practical conference "Information and Telecommunication Systems and Technologies and Cyber Security: New Challenges, New Tasks" [2, 8]. He explained that if we consider cybersecurity as a targeted activity to ensure the security of cyberspace, it is necessary to determine the structure of such activities, the subjects of cybersecurity, the goals of cybersecurity and the appropriate infrastructure that will support these activities [2, 8]. Organizational and technical model of cyber defense will consist of three vertically and horizontally integrated infrastructures (Fig.1)

The first level is the organizational and managing infrastructure of cyber defense. The components of this infrastructure are the subjects of the national cybersecurity system, which are defined by the relevant legislation at present. Cybersecurity entities are grouped into the public, academic, private, public and regional sectors.

The second level is the technological level or technological infrastructure of cyber defense, which consists of a set of forces and means of cyber defense. These are the relevant technology units of cybersecurity subjects in various sectors. At this level, the appropriate interaction of technological units is provided, i.e information exchange, monitoring, ensuring the sustainable security of cyberspace. The technological infrastructure has three horizons - national, sectoral (regional) and object.

The third level is the basic cybersecurity infrastructure, which provides the fundamental capabilities of cybersecurity. The basic infrastructure consists of two layers: a protected information infrastructure and a knowledgeable society (communities and citizens).

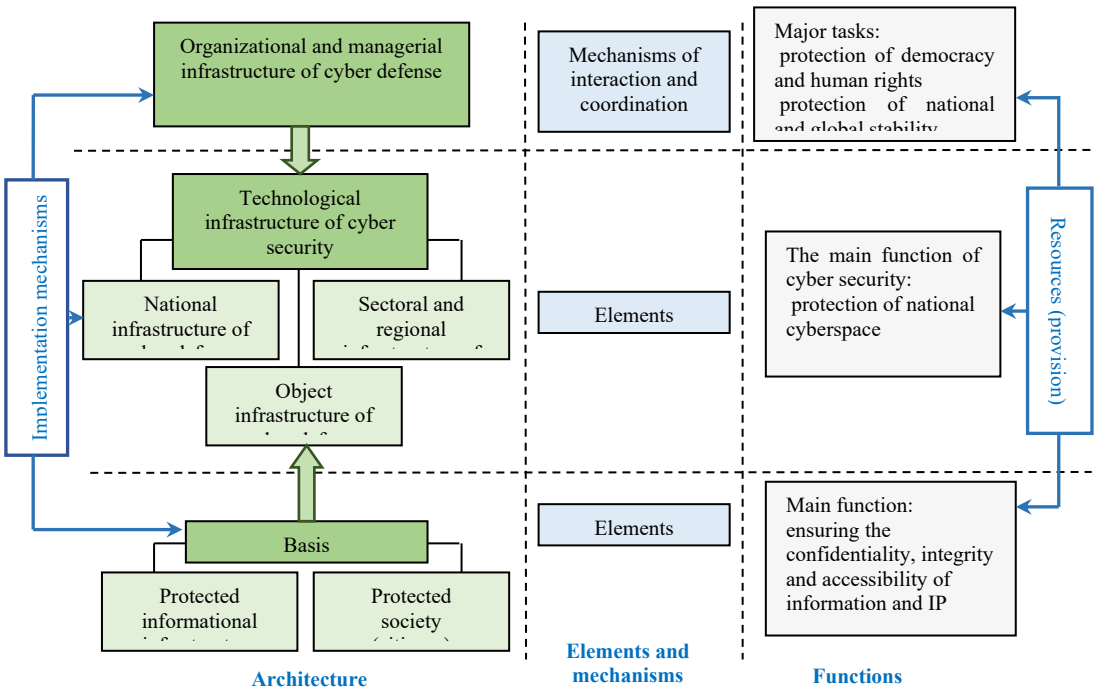


Figure 1: Organizational and managerial infrastructure of cyber defense

Let us consider baseline cybersecurity threats. They can be classified as follows:

1) **Threats from authorized users.** This includes intentional or unintentional (as a result of negligence) actions of employees working with the information system. Such actions may result in theft, destruction or alteration of data on servers or workstations without any third-party interference with the information infrastructure.

2) **External targeted external attacks.** This group includes actions that involve unauthorized intrusion into a computer network from the outside, as well as DDOS attacks. The purpose of such attacks is often to destroy or steal confidential information, change the algorithms of networks and equipment, delete server data, interfere with management systems. DDOS attacks aim to cause congestion on communication channels, servers or nodes of networks, which leads to loss of functionality or a sharp decrease in the performance of these systems.

3) **Computer viruses.** This group is the most dangerous for the information infrastructure, as it is the most common. The source of virus penetration can be e-mail, the Internet, external media, etc. The virus can result in both the theft of information (usually access passwords) and its destruction.

4) ***SPAM*** is a message (mass mailing) coming from unauthorized sources. Today, spam has become so widespread that it can be definitely attributed to sources of information security threats. A lot of spam comes to users' email addresses being the main method of remote virus transmission and can be a source of infection for workstations or simply overload mail servers or routers.

5) **Force majeure** may be refered to a separate group. These include damage to equipment due to wear, misuse or external factors. Such circumstances can also lead to data loss, and they must also be taken into account in the process of designing an information security system.

Today, there are many ways to deal with information security threats. For each threat, its own methods and processes are selected, which control certain "nodes" of the information system and prevent any failures in their work. However, the maximum effect can be achieved only by applying all these methods in combination. That is, the design, construction, implementation and maintenance of information security is a complex task that requires the analysis of potential threats, the choice of methods to combat them and establish interaction between these methods.

Basic means and methods of information protection:

1) **Authentication system.** This is the main method of information protection in almost any field. It comes down to the fact that to gain access to a particular information area, management console or communication channel, the user must provide the system with their authentication data (usually a name and password). The system then compares this data with predefined security policies, and afterwards gives or denies the user access to the requested information. Thus, each user in the information structure has its own personal ID and level of access, which allows him to perform any action only within this level.

2) **Encryption system.** This system is designed so that an attacker who managed to intercept certain data (e-mail, portable storage device ...) could not access with this data without having a specific key. There are many methods of data encryption, but they are all divided into 2 types. They can be distinguished into private key encryption and public key encryption. The former involves the presence of 1 key for encrypting and decrypting data, while the letter involves the presence of 2 different keys and is the most stable method.

3) **Firewall.** The use of a firewall aims to separate the local network from the global Internet. The firewall has its own security policies and access restrictions, so the interaction between the local network and the global one becomes possible only within these policies.

4) **Virtual Private Networks (VPNs).** This technology allows data to be transmitted over global public networks, such as the Internet, through encrypted VPN tunnels. Thus, although the information is transmitted over the global network, it cannot be accessed from it without authorization.

5) **Email filtering.** This system allows setting certain filters on the content of incoming and outgoing correspondence. This protects the internal network from the intrusion of unwanted data, in particular viruses, as well as eliminating the leakage of certain types of information from the internal network.

6) **Control of nodes efficiency.** Control focuses on constant monitoring of serviceability and quality of servers, workstations and network equipment. It helps anticipate and prevent equipment failures that could result in information loss.

7) **Antivirus protection.** It is focused on preventing threats from computer viruses. Closely related to email filtering and firewalls.

8) **Using vulnerability detection systems.** It helps to identify weaknesses in the information security system by modeling the actions of an attacker and testing the system during such actions.

9) **Creating a back-up copy.** The backup system allows backing up certain data.

Information security is one of the main conditions for the normal operation and development of the information system of any enterprise, as well as helps to minimize the possibility of information leakage.

And separately consider the "human" factor, which is the most risky component of this system (Fig. 1). It is human ignorance, negligence and mistakes that lead to such violations as:

- insufficient users awareness of the basics of information protection and misunderstanding of the need for their careful observance;
- the use of uncertificated or uncertified technical means of processing classified data, because this equipment, at best, may simply be just crude, and at worst - it may contain inserts at the physical or software levels;
- poor control over the observance of information protection rules by full-time or part-time information security and cyber security services and engineering units that do not properly monitor the serviceability of equipment or lines;
- staff turnover, because they have information with limited access or official data.

All these factors do much more harm than a whole group of attackers [5].

And so it becomes clear that the mechanisms of implementation of the model (Fig. 1) and its resource provision are the most important components that cover all levels of architecture. Development and improvement of the regulatory framework through the adoption of relevant legislation, regulations, standards, orders at all levels will further allow to implement this model.

3. Measures to build the transport platform of the national telecommunication network

Within the framework of creation of the protected infrastructure of the state and performance of tasks concerning creation and maintenance of functioning of the National telecommunication network actions on construction of a transport platform of the National telecommunication network, system of operational and technical management and automation of activation of services are carried out. In order to create a transport platform of the National Telecommunication Network (hereinafter TP NTM), the following steps have been performed today.

The construction of the first and second stages of the optical segment of the NTM transport platform has been completed. In this area of work, in particular, a system of operational and technical management and automation of activation of NTM TP services has been developed. As part of the construction of the third stage, the development of project documentation of the "Project" stage was provided, which received a positive expert opinion; After obtaining a construction permit, the deployment of telecommunication nodes will be launched at the technological sites of state bodies, which will enable even more state bodies to receive NTM services.

In order to increase the reliability of NTM operation at the interregional level and create opportunities for providing NTM services in the field to stationary, mobile, including mobile facilities, design work on the object "Construction of the satellite segment of the transport platform of the National Telecommunication Network" was provided. In order to create a radio segment of the NTM transport platform, the operation of two research areas is ensured, the results of which are included in the technical requirements for the creation of this segment. To ensure the functioning of the state management system in emergency situations and during special periods, the State Service for Special Communications and Information Protection of Ukraine has started design work on the object "Construction of the mobilization segment of the transport platform of the National Telecommunication Network".

Based on the result of the design, the best option will be taken to create a mobilization segment of the transport platform of the National Telecommunication Networks, which will ensure reliable operation of the state management system, as well as obtaining the necessary modern unified communications services directly at secure control points.

Today, in order to develop a technological platform for the deployment of the national cyber resilience system, measures are being taken to develop an organizational and technical model of cyber security as a set of systems, complexes and measures designed to ensure cyber security of critical infrastructure and cyber security of state electronic information resources and its telecommunications platform - National Telecommunication Network.

The implementation of the organizational and technical model of cyber security as a component of the national cyber security system is carried out by the State Center for Cyber Defense, which ensures the creation and operation of the main components of the system of secure access to the Internet, antivirus protection of national information resources, vulnerability detection and response to cyber incidents and cyber attacks, systems of interaction of teams responding to computer emergencies, as well as in cooperation with other actors of cyber security develops scenarios for responding to cyber threats, measures to combat such threats, programs and methods of cyber training.

In the context of organizational and technical measures attended to prevent, detect and respond to cyber incidents and cyber attacks and eliminate their consequences, a key element of the organizational model is the Cyber Threat Response Center (CRC).

Also, the State Center for Cyber Defense (Cyber center UA30) has already been established in Ukraine - an institution that directly deals with the protection of state information resources. It provides services not only to government agencies but also to citizens and

businesses. In May 2021, with the participation of the President of Ukraine, its official opening took place. The main task of the center is to ensure that the vast majority of state registers are under its protection until 2024.

Cyber center UA30 is part of the State Service for Special Communications and Information Protection of Ukraine. This is the newest state center for responding to cyber incidents, gaining skills and knowledge in the field of cyber security. It also includes an updated training ground with a unique technology for testing real scenarios of cyber attacks in the learning environment. There are only about 20 such platforms in the world, six of which are in the United States [1].

The UA30 cybercenter will have four priorities:

1. Protection of state registers. At this stage, any threats related to database intrusion will be monitored and eliminated. The main goal is to have 100% of the infrastructure sensors that prevent hacker attacks in 3 years. In addition, the creation of a unified Platform for the deployment and maintenance of state registers has already begun. This will allow to create and maintain multi-level registers according to uniform principles and standards that will comply with current legislation.
2. Protection of citizens, private information and business. Citizens of Ukraine will have available tools and adequate knowledge for their own protection. Businesses will be able to protect their information and processes by improving national standards and practices. Private information of citizens will be reliably protected because the Cyber Center provides appropriate response services to cyber threats.
3. Development of cyber hygiene culture. The center will be an educational hub, where everyone will receive knowledge to protect themselves on the Internet. Cyber hygiene is one of the foundations of digital literacy. Currently, 53% of the country's population has a low level of digital skills. This indicator must be changed immediately.
4. Formation of a personnel reserve of cyber security. Today, there is a shortage of cyber security professionals around the world. It is important to change this situation. Therefore, the creation of a network of cyber security training centers is a priority.

The State Center for Cyber Defense is taking measures to counter cyber attacks. Also, owners of information systems, heads of departments responsible for information security of state bodies of Ukraine are constantly provided with recommendations on combating cyber attacks, as well as work conducted to prevent contamination of the infrastructure with malicious software.

In order to ensure effective exchange of information on cyber incidents, analysis of trends, identification of the main sources of cyber incidents, effective counteraction to cyber threats and exchange of risk data, the national Malware Information Sharing Platform "Ukrainian Advantage" (MISP-UA) has been launched [3]. The use of the system allows cyber specialists of the Security Service of Ukraine to anticipate ways of attacks, potential threats and neutralization tools for further response. In terms of its functional content, the platform allows to strengthen the state of cyber security of various sectors of public administration and the economy of Ukraine. With its help a public-private interaction takes place for joint protection of information and cyberspace of the state as a whole.

Ukraine is currently in the process of joining NATO's Joint Center for Advanced Technology in Cyber Defense, which provides anti-cyber attacks and cyber protection of information systems [10].

4. Conclusions

Ukraine is now at the forefront of the fight against cyber challenges. Digitalization and cyber security always go the same way. Therefore, the field of cyber security should not just be on a par with the digitalization of the country, but one step ahead. However, it is not worth relying only on the fact that all cyber security issues will be resolved by the state. Every person, every citizen should know how to secure and protect themselves, their confidential data, bank accounts, etc.

Thus, the issue of cyber security is certainly relevant. Its solution should be comprehensive both at the level of ordinary users and at the state level in the framework of creating a modern legal framework, appropriate software and technical solutions. Increasing investment in cyber security will help prevent attacks on large public and private companies and counter intentions to destabilize society.

5. References

[1] The UA30 Cybercenter has been opened in Ukraine, which will protect the state from cyber attacks. URL: https://www.kmu.gov.ua/news/v-ukrayini-vidkrili-kibercentr-ua30-yakij-zahishchatime-derzhavu-vid-kiberatak

[2] Organizational and technical model of cyber defense was presented in Ukraine. URL: https://softline.org.ua/news/v-ukraini-prezentovano-orhanizatsiino-tekhnichnu-model-kiberzakhystu.html

[3] To counter cyber threats, the SSU launches an updated version of the MISP-UA platform. URL: https:// ssu.gov.ua/novyny/7800

[4] LAW OF UKRAINE "On Basic Principles of Cyber Security of Ukraine". URL: https://zakon.rada.gov.ua/laws/show/2163-19

[5] Cybersecurity as an important component of the entire state protection system. URL: https://www.mil.gov.ua/ukbs/kiberbezpeka-yak-vazhliva-skladova-vsiei-sistemi-zahistu-derzhavi.html

[6] Cyber Defense of Ukraine: state, problems and current measures to ensure it. URL: http://opk.com.ua/кібероборона-україни-стан-проблеми-т/

[7] Lavrut O.O. New technologies and means of communication in the Armed Forces of Ukraine: the way of transformation and prospects of development / O.O. Lavrut, T.V. Lavrut, O.K. Klymovych, Ю.М. Zdorenko. Science and technology of the Air Force of the Armed Forces of Ukraine. 2019. Vol. 1 (34). P. 91–101. DOI: 10.30748/nips.2019.34.13.

[8] Oleksandr Potiy, Andriy Semenchenko, Dmytro Dubov, Oleksandr Bakalynsky, Danylo Myalkovsky. Conceptual principles of implementation of organizational and technical model of cyber defense of Ukraine. URL: DOI: https://doi.org/10.18372/2410-7840.23.15434.

[9] Puzyrenko O.H., Ivko S.O., Lavrut O.O. Analysis of the process of information security risk management in ensuring the survivability of information and telecommunications systems. Information processing systems. 2014. Vol. 8 (124). P. 128-134.

[10] The process of including Ukraine in the NATO Cyber Defense Center has begun. URL: https://www.pravda.com.ua/news/2021/06/7/7296338/

Audit Of Mathematical Models For Software Specification Of The Workplace Decision Support System At The Logistics Management Point

Roman Litvinchuk [1], Andrii Levchenko [2]

[1] *Military Academy (Odesa), Fontanskaya Road 10, Odesa, 65009*
[2] *Odesa Mechnikov National University, Dvorianska, 2, Odesa, 65026, Ukraine*

Abstract

The article analyzes the process of functioning of the system of technical support of combat operations in order to determine it`s capabilities and areas for improvement through for solving problems in modern local wars with the restriction of the use of heavy armored vehicles through application of the models of states and transitions.

In addition, the possibility of creating a mathematical basis for the management of maintenance and restoration of lightly armored vehicles for software implementation of the workplace of a logistics officer on evacuation management and lightly armored vehicles recovery, which will not only explore real support systems, but also solve complex problems of technical support of combat operations in real time - on the battlefield.

Keywords

technical support, armament and military equipment, lightly armored vehicles, intensity, probability, graph, Kolmogorov's equation

1. Introduction

Formulation of the problem.

Analysis of the models of the main states of the technical support system, which were used before beginning of hostilities in the anti-terrorist operation area, shows that the task of managing the evacuation and recovery of arming and military machinery (AMM) during hostilities is more difficult in terms of preconditions and initial data for planning than known it`s solutions. [1-4].

Based on the combat experience of servicemen of the Ukrainian Armed Forces and other military formations that directly participated in repelling the Russian armed aggression, it is well known that Ukraine clearly complies with the requirements of the Minsk agreements and does not use heavy armored vehicles such as tanks and artillery on the line of contact.. Therefore, the main armored vehicles are light armored vehicles such as (BMP, armored personnel carrier, BBM).

It is known that many factors that affect the management of evacuation and recovery of arming and AMM hostilities are accompanied by uncertainties of random, natural and antagonistic nature.

An appropriate way out of this situation is to reduce the dimensionality of the analysis problem by comparing it in order to rank the types of technical support tasks according to some general indicator. As such an indicator can be used the probability stay of the evacuation management system and the restoration of AMM in each state of solving the tasks of combat operations. The choice of the solution of the problem is possible by averaging the optimal partial solutions over time on the highest level of probability. It is the correspondence of the probability models to the realities that requires further research. [5].

The purpose of the article.

Currently, Light Armored Vehicles (LAV) of all-military units are the most common type of military equipment in the armed forces. Also, such equipment is most often affected and fails, and therefore requires constant correction of planned activities of managing the evacuation and recovery of AMM in real time.

EMAIL: Litvinsanr@gmail.com (A. 1);
katyaandreylev@gmail.com (A. 2).
ORCID: 0000-0002-5681-691 (A. 1);
0000-0003-4423-8267 (A. 2)

Systematic shelling of the positions of the Ukrainian Armed Forces in the area of anti-terrorist operation (ATO) leads to the decommissioning of those samples of armaments and military equipment that are located directly at the bases on the line of the collision of the parties. In the context of integration of logistics management as a mechanism for providing and managing evacuation and recovery and subsequent repair of lost samples of armaments and military equipment, it turned out that mathematical models of logistics management and operation, as well as software based on them do not meet the requirements of real-time decision support.

The purpose of the article is to provide a mathematical justification for the management of evacuation and recovery of LAV for software implementation of the workplace logistic officer for evacuation management and recovery of LAV at the logistics management point, which will not only explore real support systems, but also solve complex problems of technical support of combat operations in real time, including in the battlefield.

2. Analysis of the model of the main states of the technical system of combat operations (Conceptual Modeling)

To study the process of technical support, various types of technical support models are currently used. If the models adequately reflect all the states of the system, it is better to use model of states and transitions [5].

The adequacy of the model for processes without aftereffect is explained by the fact that it most accurately reflects the system, in the case when any of its current state does not depend on the state in which the system was before. It is the identity of the model to the real processes that explains the choice of the state model for the software specification of the decision support system of the logistics officer's workplace for evacuation management and light armored vehicles recovery at the logistics management point. This is the system of technical support of warfare. A variant of the graph of states and transitions of this system to different states is presented in **Figure 1**

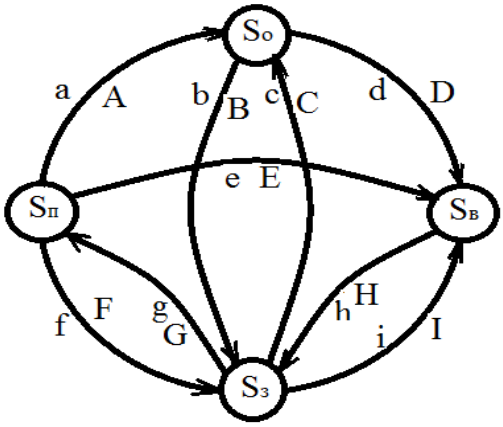


Figure 1. Graph of transitions of the technical system of combat operations in the states: $S_п$ – preparation of LAV for use; $S_з$ – combat use of LAV; $S_в$ – restoration of LAV after its damage; $S_о$ – maintenance of LAV before or after combat actions.

The list of transition intensities and the corresponding probabilities of these transitions is as follows:

a, A – intensity and probability of transitions of the technical support system from the state of preparation of LAV for its maintenance;

b, B – intensity and probability of transitions from the state of LAV maintenance to the state of its combat use;

c, C – intensity and probability of transitions from the state of combat use of the LAV to the state of its maintenance;

d, D – intensity and probability of transitions from the state of maintenance of LAV to the state of recovery of LAV after damage;

e, E – intensity and probability of transitions from the state of preparation of LAV to the state of recovery of LAV after damage;

f, F - intensity and probability of transitions from the state of preparation of LAV to the state of its employment;

g, G – intensity and probability of transitions from the state of combat use of LAV to the state of preparation of LAV for the purpose of their employment;

h, H – intensity and probability of transitions from the state of recovery of LAV after damage to the state of its combat use;

i, I – intensity and probability of transitions from the state of combat use of LAV to the state of recovery of LAV after its damage.

It is also easy to imagine a situation where it is necessary to perform maintenance of LAV after its preparation for use, or after its combat

application, as well as a situation when combat use of LAV has shown the need for new training for deployment, for example, taking into account unsatisfactory combat results due to insufficiently careful preliminary preparation.

In the process of functioning of the system of technical support of combat operations in time, it is in any state with probabilities:

$P_1(t)$ - probability that the system is in a state of preparation of weapons and ammunition for their use;

$P_2(t)$ - the probability that the system is in a state of use of weapons for their intended purpose;

$P_3(t)$ - the probability that the system is in a state of recovery after damage;

$P_4(t)$ - the probability that the system is in a state of maintenance.

Find the probability $P_1(t)$. We provide t small increase Δt and find the probability that at the moment $t+\Delta t$ the system will be in a state S_n. This event can happen in two ways:

- at the moment t the system was already in condition S_n, but by the time Δt did not come out of this state, either

- at the moment t the system was in the state $S_в$, by the time Δt moved from it to the state S_n

The probability of the first variant is shown as the product of the probability $P_1(t)$ that at the moment t the system was in the state S_n, on the conditional probability that, being in a state S_n, system by the time Δt will not pass from it into a state $S_з$.

This conditional probability (up to infinitesimal higher orders of magnitude) is equal to: $1-\lambda_{12}\Delta t$

Similarly, the probability of the second option is equal to the probability of that at the moment t system was at the state $S_в$, which is multiplied by the conditional probability of transition over time Δt into the state S_n: $P_з(t)\lambda_{31}\Delta t$.

Applying the rule of adding probabilities, we obtain:

$$P_1(t+\Delta t)=P_1(t)(1-\lambda_{12}\Delta t)+P_3(t)\lambda_{31}\Delta t \quad (1)$$

Open the brackets on the right side, move $P_1(t)$ to the left and divide both parts of the equation by Δt; we will get:

$$\frac{P_1(t+\Delta t)-P_1(t)}{\Delta t}=\lambda_{12}P_1(t)+\lambda_{31}P_3(t) \quad (2)$$

Now direct Δt to zero and go to the limit:

$$\lim_{\Delta t\to 0}\frac{P_1(t+\Delta t)-P_1(t)}{\Delta t}=\lambda_{12}P_1(t)+\lambda_{31}P_3(t) \quad (3)$$

The left part is nothing but a derivative of the function $P_1(t)$:

$$\frac{\partial P_1(t)}{\partial t}=-\lambda_{12}P_1(t)+\lambda_{31}P_3(t) \quad (4)$$

Thus, the differential equation obtained by the function $P_1(t)$. Similar differential equations can be derived for other probabilities of states $P_2(t)$, $P_3(t)$, $P_4(t)$, which provides initial data for the search of computational methods for solving problems that replace theoretical models in the form of differential equations.

Consider the second state $S_з$. Find the probability that at the moment $t+\Delta t$ the system will be in a state $S_з$. This event can occur in two ways:

- at the moment t the system was already in condition $S_з$, by the time Δt did not come out of this state;

or

- at the moment t system was in condition S_n; by the time Δt moved from it to the state $S_з$;

or

- at the moment t system was in condition S_o, by the time Δt moved from it to the state $S_з$.

The probability of the first option is calculated as follows: $P_2(t)$ multiplied by the conditional probability that the system over time Δt will not pass either $S_в$, nor in S_o. Since the events that are the transition over time Δt into $S_в$ and from $S_з$ into S_o, are incompatible, the probability that one of these transitions will occur is equal to the sum of their probabilities, to wit $\lambda_{23}\Delta t+\lambda_{24}\Delta t$ (up to infinitesimal higher orders). The probability that none of these transitions will occur is equal $1-(\lambda_{23}\Delta t+\lambda_{24}\Delta t)$. Hence the probability of the first option: $P_2(t)(\lambda_{23}\Delta t+\lambda_{24}\Delta t)$.

Adding here the probabilities of the second and third options, we obtain:

$$P_2(t+\Delta t)=P_2(t)(1-\lambda_{23}\Delta t+\lambda_{24}\Delta t)+ \\ +P_1(t)\lambda_{12}\Delta t+P_4(t)\lambda_{42}\Delta t \quad (5)$$

Moving $P_2(t)$ to the left side, dividing by Δt and crossing to the limit, we obtain a differential equation for $P_2(t)$:

$$\frac{\partial P_2(t)}{\partial t} = -\lambda_{23}P_2(t) - \lambda_{24}P_2(t) + \\ +\lambda_{12}P_1(t) + \lambda_{42}P_4(t) \quad (6)$$

Reasoning similarly for states $S_в$ and S_o, we obtain as a result a system of differential equations composed by type **(5)**, **(6)**. Rejecting them for the sake of convenience argument t in functions P_1, P_2, P_3, P_4 rewrite the system in the form:

$$\begin{aligned} \frac{\partial P_1}{\partial t} &= -\lambda_{12}P_1 + \lambda_{31}P_3, \\ \frac{\partial P_2}{\partial t} &= -\lambda_{23}P_2 - \lambda_{24}P_2 + \lambda_{12}P_1 - \lambda_{42}P_4, \\ \frac{\partial P_3}{\partial t} &= -\lambda_{31}P_3 - \lambda_{34}P_3 + \lambda_{23}P_2, \\ \frac{\partial P_4}{\partial t} &= -\lambda_{42}P_4 + \lambda_{24}P_2 + \lambda_{34}P_3. \end{aligned} \quad (7)$$

These equations for the probabilities of states are Kolmogorov's equations.

The integration of this system of equations will give the desired probabilities of states as a function of time. The initial conditions are taken depending on what was the initial state of the system. For example, if at the initial time (at $t=0$) the system was in a state S_n, then the initial conditions must be accepted: $t=0$, $P_1=1$, $P_2=P_3=P_4=0$, which gives an understanding of the universality of the model under study, in terms of its further use as an element of the software specification of the workplace logistic officer for evacuation management and recovery of light armored vehicles decision support system at the logistics management point.

Note that all four equations for P_1,P_2,P_3,P_4 one could not write because $P_2+P_2+P_3+P_4=1$ for all t, and any of the probabilities P_1,P_2,P_3,P_4 can be expressed through the other three. For example, $P_4=1-P_1,P_2,P_3$.

Then a special equation for P_4 not necessary to write. In the future, this fact will reduce the requirements for productivity and speed of the hardware components of the decision support system.

Let's pay attention to the structure of equations **(7)**. They are all built on a general rule that can be formulated as follows. In the left part of each equation there is a derivative of the probability of the state, and the right part contains as many terms as there are gaps connected with the given state.. If the gap leaves the state, the corresponding member has a sign "minus", and if the gap enters the state - the sign "plus". Each term is equal to the product of the intensity of the transition corresponding to a given gap and the probability of the state from which the arc emerges.

If the matrix of transition intensities or the state graph is known, the state probability vector can be determined $P_9(t)=\left(P_1(t),...,P_n(t)\right)$, through the matrix equation $P(t)=P(t)\bullet\Delta$.

From a practical point of view, to ensure the combat effectiveness of the unit is important to reduce the intensity and probability (*g, G*) its transition to the state (S_n) preparation of LAV for the purpose of their application, and also increase in intensity and probability (*f, F*) transition of the system to the state ($S_з$) use of LAV for its intended purpose. This requires keeping the LAV at a high level of its readiness factor, accelerated and sufficient level of preparation of the LAV for the start of combat actions.

It is necessary to significantly reduce the intensity and probability (*i, I*) transition of the technical support system to the state ($S_в$) recovery of LAV after damages, reduce the intensity and probability (*e, E*) transition of the system from the state (S_n) preparation of LAV for the purpose of their application in a condition ($S_в$) recovery from damage, ie before the start of the use of LAV for its intended purpose.

It is necessary to increase the intensity and probability (*h, H*) transition of the system from the state ($S_в$) recovery of LAV after damage to the condition ($S_з$) application for intended use.

The greatest attention is paid to the study of the condition ($S_з$) use of LAV by purpose and condition ($S_в$) recovery of LBT after damages is not accidental. This is due to the fact that these states of the technical system of combat operations are the most important in terms of the importance of the functions of the technical support system, and the structure of unconditional relations in this system.

It is safe to say in advance that, given the uncertainties of a random nature, namely, equally intense and equally probable transitions of the technical system of combat operations from any state to any other state, the total probability ($P_{зв}=P_з+P_в$) stay of this system in a condition ($S_з$) use of LAV on purpose and in condition ($S_в$) recovery of LAV after damage is always the highest in comparison with other general probability, equal to the sum of the probability of the system in the state of preparation of LAV for

their application and the probability of the system in a state of maintenance, that is, with the total probability $P_{on} = P_o + P_n$.

Indeed, it is easy to see this in some arbitrary but concrete example.

2.1. Verification and specification of the obtained models for their further implementation in the software of decision support systems (Modeling verification & validation)

The first test example.

The initial prerequisites for modeling are equally intense and equally likely transitions of the system of technical support of hostilities from any state to any state, namely (check. **Figure 1**): $a = b = c = d = e = f = g = i = h = 1/2$ hours; $A = B = C = D = E = F = G = I = H = 1/9$; $t = (6...48)$ hours.

Identify the general probabilities that need to be quantified, namely: $P_{зв}(t) = P_з(t) + P_в(t)$; $P_{on}(t) = P_o(t) + P_n(t)$,

where $P_n(t)$ - the probability that the system is in a state of preparation of weapons and ammunition for their use;

$P_з(t)$ - the probability that the system is in a state of use of weapons for their intended purpose;

$P_в(t)$ - the probability that the system is in a state of recovery after damage;

$P_o(t)$ - the probability that the system is in a state of maintenance of weapons.

The solution is carried out on machines for data packaging, provided that for the representation of numerical values that the decimal system of systematization of calculations are in the range from 0 to 1, respectively in the binary calculation system the number of characters for the mantissa is 8 bits with the corresponding mantissa.

According to the formulas **(1-7)** we will get:

$P_n(t = 6...48) = 0,13...0,09$;

$P_o(t = 6...48) = 0,17...0,18$;

$P_n + P_o = 0,30...0,27$.

$P_з(t = 6...48) = 0,59...0,26$;

$P_в(t = 6...48) = 0,11...0,47$;

$P_з + P_в = 0,70...0,73$.

Graphs of general probabilities in the form of time functions during the process of technical support of hostilities, obtained according to the initial data **example 1** and emphasize the validity of the statement which was made earlier.

Thus, in the system of technical support of combat actions there is a pattern, namely: under conditions of equally probable transitions of the system from state to state, it is in a state of application or recovery more often (approximately three times) than in a state of maintenance or training.

It is clear that this result is not a new discovery. The problem is solved by a known method for the new initial conditions and the new content of the problem of evacuation and recovery of armaments and military equipment. It only confirms the peculiarity of the structure and the essence of the functioning of a complex system of technical support of combat actions. This is what is needed carefully and always consider.

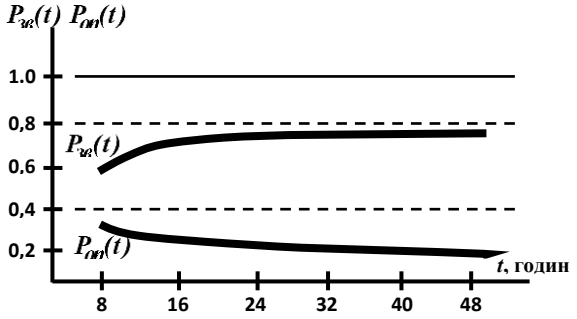


Figure 2. General probabilities of the technical support system being in combat during states: application or recovery, $P_{зв}(t)$ LAV; maintenance or preparing, $P_{on}(t)$ LAV for combat actions.

Next, it is necessary to investigate (for conditions similar to the data according to **Example 1**) the dependence of the time of technical support of combat operations of each of the probabilities, namely: $P_n(t)$ - the probability of the system being in a state of preparation of LAV for the purpose of their application; $P_з(t)$ - the probability that the system is in a state of use of LAV for its intended purpose; $P_в(t)$ - the probability that the system is in a state of recovery LAV after its damage; $P_o(t)$ - the probability that the system is in a state of maintenance LAV.

The second test example.

Output data. We have equally intense and equally probable transitions of the system of technical support of combat actions from any state

to any of its states, namely (check. Помилка! Джерело посилання не знайдено.): $a = b = c = d = e = f = g = i = h = 1/2$ *hours*; $A = B = C = D = E = F = G = I = H = 1/9$; $t = (6...48)$ *hours*.

Identify and plot graph of probabilities: $P_n(t)$, $P_з(t)$, $P_в(t)$, $P_o(t)$, $t = (6...48)$ *hours.*

Regarding the representation of numerical values in the binary calculation system, the assumption introduced in the first test example.

The results obtained from the simulation results of determining and comparing the probabilities of the technical support system in each of the main states are typical for combat operations. These results characterize the full group of phenomena, under conditions of commensurate intensities and commensurate probabilities of transitions of this system to different states. They show the following.

First, with the start of combat actions, the technical support system is: in a state of preparation of weapons and ammunition for the fight with a probability **13%**; in the state of use of weapons for their intended purpose - with probability **60%**; in a state of restoration of armament after damage - with probability **10%**; in a state of service - with probability **17%**.

Secondly, after two days of combat actions, the technical support system is in a state of preparation of weapons and ammunition - with a probability **9%**; in the state of use of weapons for their intended purpose - with probability **26%**; in a state of restoration of armament after damage - with probability **47%**; in the state of service of armaments - with probability **17%**.

This shows that the data obtained (under conditions of equally intense and equally probable transitions of the system to different states) using the model, in the presence of random and antagonistic uncertainties, do not contradict the known experimental results of real events of typical support, according to local fight. Third, the weakest point of a typical unit's technical support system is its ability to recover weapons and military equipment (AMM) damaged during combat.

This situation necessitates further research on the technical system of combat operations, in order to identify measures to increase opportunities for the restoration of AAM damaged during combat.

The solution of the problem of evacuation and recovery using the model of states and transitions confirms the adequacy of the model with real measures of evacuation and recovery of armaments and military equipment.

Therefore, it seems appropriate measures aimed at increasing the survivability of AAM. According to the classical definition, the survivability of AAM is its ability to maintain its functions during the action of the enemy's means of destruction and the ability to quickly recover from damage and return to service.

It is clear that to increase the survivability of weapons part is necessary and sufficient: first, to organize and implement a set of measures to reduce its radio and optical visibility by air and ground reconnaissance by the enemy and before and during its intended use; secondly, to organize and carry out measures and means for artillery and technical reconnaissance: thirdly, to organize and carry out the use of a set of repair forces, the use of replacement units, blocks, devices and materials, to organize the evacuation and rapid recovery of damaged AAM.

According to the graph of states and transitions of the technical system of combat operations, the above measures and means should clearly: first, reduce the intensity and probability of transition of the system from the state of use of LAV for its intended purpose to recovery after damage; secondly, these measures and means will increase the intensity and probability of the transition of the system from the state of recovery of LAV after damage to the state of use for its intended purpose..

We will further determine the direction of change in the operation of the technical system of combat operations for some specific conditions that differ (from the conditions of **Example 2**) by reducing the intensity and probability of transition of the system from the intended use to the recovery state after damage, for example, in two times, in addition, differ in the increase in the intensity and probability of the transition of the system from the state of recovery of LAV after damage to the state of use for its intended purpose also in two times.

The system of technical support of combat operations is: in the state of preparation of the LAV for combat with a probability of (13… 14)%; in the state of application of LAV for the purpose - with a probability of (62… 47)%; in a state of recovery after damage - with probability; in the state of service - with a probability of (18… 29)%. The implementation of measures aimed at increasing the survivability of LAV, compared with measures, showed that the probability of recovery of LAV after damage and its return to

service increases more than four times; the probability of the maintenance system in the state of use for its intended purpose (as of two days) is doubled, the probability of being in the state of maintenance is also increased by one and a half times.

3. Conclusions

1. The weakest point of the standard system of technical support of combat operations of the unit is its ability to restore weapons damaged during combat. The solution of the problem of evacuation and recovery using the model of states and transitions confirms the adequacy of the model with real measures of evacuation and recovery of weapons. This situation necessitates further research on the technical system of combat operations, in order to identify measures to increase the ability to restore weapons damaged during combat.

2. Analysis of the functioning of the technical system of combat operations in order to determine its capabilities and areas for improvement in conditions of random and antagonistic uncertainties - all this necessitates the search for and application of effective models and appropriate quantitative analysis and synthesis for adequate scientific management of technical problems.

3. The use of models of states and transitions allows by building an adequate model and appropriate simple calculations, even in conditions of random and antagonistic uncertainties to obtain sufficiently reliable quantitative estimates of the capabilities of the technical system of combat operations, and to determine appropriate directions and ways to improve it and increase important parameters. its functioning.

3. Under the conditions of creating a software product and implementing a dialog-information model of the operation of the technical system of combat operations using a personal computer, it is possible not only to explore real support systems, but also to solve complex problems of technical support of combat operations in real time and in including on the battlefield.

4. References

[1] Military-political, strategic, operational and tactical content of local wars and armed conflicts. HAOУ, 2001. 222 p.

[2] Varvanets Y.B. Analysis of the use and development trends of rolling stock maintenance and repair of military equipment. Proceedings of the International Scientific and Technical Conference: Prospects for the development of weapons of the Land Forces.- Lviv, 17-18 May 2018 20 p.

[3] Technical support of troops (forces) in operations and combat. Textbook: HAOУ, 2001. – 616 p.

[4] Technical support of service and combat operations (application) Internal troops of the Ministry of Internal Affairs of Ukraine. Tutorial. R. O. Kaidalov, G. M. Marenki, B. O. Temnikov, B. I. Kuzhelovich. – X.: Academy of Internal troops of the Ministry of Internal Affairs of Ukraine, 2013. – 111 p.

[5] Demianchuck B.O. Basics of automotive support. Process modeling / Demianchuck B.O, Werpivskyi S.M., Melenchuck B.M. Textbook with a stamp Ministry of Defense of Ukraine. – Odesa: Military Academy. – 2015. – 391 p.

[6] 2. Application of units and military units of technical support. Part.1: Technical support units; Tutorial.- K:НУОУ named after Ivan Chernyakhovsky, 2017.-136p .

[7] Anolovich B.Y. Reliability of machines in tasks and examples B.Y. Anolovich, O.S. Grinchenko, B.L. Litvinenko. – X.: Eye, 2001. – 320 p.

[8] Methodological guide for comparative assessment of the quality of military engineering equipment - Moscow.: Publisher. Ministry of Defence, 1991. – 50 p.

[9] Technical support management documents. Part 1. Tutorial. – Kyiv.: Kyiv Institute of Land Forces, 1996. – 121 p.

[10] 3. Sedov S.G., Bubliy B.A., Revutskyi A.A. Analysis and forecasts of the development of protection of lightly armored combat vehicles from small arms. Proceedings of the University. National Defense University of Ukraine. 2019. №1, p. 129–137.

Use of The Normalized Gap of Maximum Singular Value of The Image Block to Evaluate The Capacity of The Steganographic Channel

Ivan Bobok[1], Alla Kobozieva[1] and Nataliya Kushnirenko[1]

[1]*Odessa Polytechnic State University, Shevchenko av., 1, Odesa, 65044, Ukraine*

Abstract

The Least Significant Bit (LSB) method is one of the most widespread and demanded steganographic methods nowadays. Detection and decoding the hidden information, embedded in a container using the LSB, is a challenging task, in particular, in conditions of low capacity of the hidden communication channel. The existing steganalysis algorithms developed to detect the LSB, as a rule, solve the main problem of steganalysis - the detection of a hidden communication channel. However, the problem of the additional information recovery remains unfulfilled. The important step in solving this problem is the evaluation of the hidden (steganographic) channel capacity. In the current work, a digital image is used as container. All the results obtained can also be applied to digital video, which is considered as a sequence of frames. The aim of the work is to get estimates for the value of the capacity of the hidden communication channel, formed by the LSB method. To achieve the aim of the work the following studies carried out: performed additional in-depth investigation of properties of the normalized gap of the maximum singular value of non-intersecting image blocks, obtained by standard splitting; studied properties of a discrete function y(QF), that determines the number of image blocks in which the normalized gap of maximum singular value increases when the image is re-saved to lossy format with quality factor QF. As a result of the research, the estimates of the value of the capacity of the hidden communication channel, created using the LSB method and based on a container in a lossy format, were obtained.

Keywords

Steganalysis method, digital image, the capacity of the hidden communication channel, the LSB method, the normalized gap of singular value

1. Introduction

Steganography today is one of the most powerful and widely used areas of information security. One of the main questions here is who holds such a powerful means of protection, since the use of steganography, unfortunately, can lead to the setting up of hidden communication with anti-state, illegal, inhuman goals [1,2]. In such cases, early detection of hidden communication is critical. The main "weapon" for here is steganalysis [3]. Powerful efforts of scientists around the world today are aimed at solving the main task of steganalysis - to identify the presence of hidden (additional) information in information content [4]. However, in the condition of the information confrontation, that takes place in the modern world [2], these actions are not sufficient. Only the decoding of hidden information, its recovery will allow achieving the goal of steganalysis to the fullest. The extracting of hidden information and its decoding are the most complicated tasks. It can be facilitated by determining/evaluating the capacity of the organized steganographic channel [3,5], which is what this work is aimed at.

Today, one of the most widespread and demanded steganographic methods is the least significant bit modification method - *LSB* [3]. However, modern steganalysis methods, as a rule, do not evaluate the capacity of the hidden communication channel [6,7,8].

In [9], a steganalysis method was proposed, which aimed at detecting a hidden communication channel with low capacity.

EMAIL: onu_metal@ukr.net (A. 1); alla_kobozeva@ukr.net (A. 2); infsec2011@gmail.com (A. 3)
ORCID: 0000-0003-4548-0709 (A. 1); 0000-0001-7888-0499 (A. 2); 0000-0003-3722-0229 (A. 3)

The method was based on properties of the normalized gap of the maximum singular value of image matrix block. In particular, it took into account the number of image blocks, obtained by standard matrix splitting, in which the normalized gap of the maximum singular value increased due to re-saving of image to a lossy format with different quality factors QF. This number was reflected by the discrete function $y(QF)$ that was built for the image under examination. Let us introduce the appropriate notation.

Let F be the matrix of the digital image, which is split in a standard way into non-intersecting $l \times l$-blocks with singular values [10] $\sigma_1 \geq \sigma_2 \geq \ldots \geq \sigma_l \geq 0$, which form vector of singular values $\sigma = (\sigma_1, \sigma_2, \ldots, \sigma_l)^T$; the normalized vector of singular values $\bar{\sigma} = (\bar{\sigma}_1, \bar{\sigma}_2, \ldots, \bar{\sigma}_l)^T$ is determined by

$$\bar{\sigma} = \sigma / \|\sigma\|,$$

where $\|\sigma\|$ is a norm of vector σ. Then the normalized gap of the singular value $\sigma_i, i = \overline{1,l}$ is determined as follows [9]:

$$svdgap_n(i) = \min_{i \neq j} |\bar{\sigma}_j - \bar{\sigma}_i|,$$

whence it follows that the normalized gap of the maximum singular value is

$$svdgap_n(1) = \bar{\sigma}_1 - \bar{\sigma}_2$$

and

$$0 < svdgap_n(1) \leq 1$$

The efficiency of algorithmic implementation of the method proposed in [9] exceeds the modern analogues in terms of the detection of the hidden communication channel in conditions of a low capacity. It means, that the mathematical basis of the method provides sensitivity to small disturbances of the container in the process of steganographic transformation, and therefore can be considered promising for evaluating the steganographic channel capacity. To ensure the possibility of determining/evaluating the capacity of the hidden channel, additional studies of the properties of the function $y(QF)$ are required.

The aim of the work is to obtain estimates for the value of the capacity of the hidden communication channel, formed using the LSB method, by identifying the corresponding additional properties of $y(QF)$.

2. Main Body

Let the image were initially saved in a lossy format; F_1 is the matrix of the image, which is subject to examination. Formally, it is saved in a lossless format. If F_1 is a steganographic message, then we will assume that it is obtained on the basis of a Jpeg container with a matrix F. Let us apply to F_1 the steganographic transformation with the low capacity of the hidden communication channel (for example, 1%), which formally represented as [11]:

$$F_{1,1} = F_1 + \Delta F, \quad (1)$$

where ΔF is the matrix representation of the additional information, $F_{1,1}$ is the matrix of the image-steganographic message. Let us define functions $y(QF)$ for F_1 and $F_{1,1}$ re-saving them with losses with all possible values of the quality factor QF. For a particular QF, as a rule, the value $y(QF)$ for $F_{1,1}$ will be greater than that for F_1. Geometrically it means that the $y(QF)$ graph for $F_{1,1}$ will be higher along the ordinate than the $y(QF)$ graph for F_1 whether the message or the container matches the matrix F_1. However, the difference between the values of the function $y(QF)$ (between the corresponding graphs) will be different depending on whether the matrix F_1 corresponds to the original image or steganographic message.

Let F_1 be the matrix of the container, then the steganographic message (1) for it will be the first and only one. If F_1 corresponds to the steganographic message, then for it (1) is a repeated steganographic transformation. Let us show that the primary transformation (1) with the help of the matrix ΔF will "lift" the $y(QF)$ graph higher along the ordinate compared to the graph constructed for F_1, than repeated transformation using the same matrix ΔF.

The steganographic transformation of the Jpeg container almost always leads to an increase in the smallest singular values and decrease in the normalized gap of the maximum singular value in the blocks involved in the steganographic transformation, thereby increasing the likelihood of the growth of the

normalized gap of the maximum singular value when the image is re-saved into a lossy format. If the additional information is embedded in the image-steganographic message, then the normalized gap of the maximum singular value in blocks, involved in the primary steganographic transformation, is less than in the corresponding blocks of the original container. After the additional information is embedded in the steganographic message, the smallest singular values of the corresponding blocks involved in repeated steganographic transformation, which are no longer comparable to zero in those blocks that were involved in the primary transformation, can both decrease and increase. This fact can lead to both an increase and decrease in the normalized gap of the maximum singular value. Re-embedding the additional information in the steganographic message will generally increase the resulting capacity of the hidden communication channel, additionally disturbing the singular values, but the relative change in the smallest singular values of the container blocks be greater than in the smallest singular values of steganographic message with the same disturbance. Thus, the number of blocks in which the normalized gap of the maximum singular value will increase at re-saving with losses of the steganographic message, obtained as a result of consecutive double steganographic transformation will be greater, than when re-saving the primary steganographic message. However, the degree of this increase will be less than the degree of increase using the same (which is characterized by matrix ΔF), but the primary steganographic message on an empty container. Moreover, the degree of increase will be smaller the more the capacity of the hidden communication channel of the primary steganographic transformation. Indeed, the more the capacity of the hidden communication channel of the primary steganographic message, the more the number of container blocks, in which the normalized gap of the maximum singular value will decrease as a result of the steganographic transformation, the less the normalized gap of the maximum singular value in the blocks F_1 involved in the steganographic transformation, the "higher" will be the graph of the function $y\left(QF\right)$, obtained when re-saving F_1 with losses. When re-embedding additional information into a steganographic message formed with a relatively significant primary capacity of the hidden channel, there will be a significant number of blocks, where, after repeated steganographic transformation, the normalized gap of the maximum singular value will increase, rather than decrease, in comparison with the normalized gap of the maximum singular value in the block of the input steganographic message. This will lead to the fact that when re-saving a steganographic message obtained as a result of a double steganographic transformation, although the graph of the function $y\left(QF\right)$ will be higher than the graph of a similar function for the input steganographic message (obtained as a result of a single steganographic transformation), this difference will be the smaller, the larger was the capacity of the hidden channel of primary steganographic transformation. It was confirmed in practice by the results of a computational experiment, in which the following sets of digital images were involved:

- M_{Tif} – 500 images in lossless format (Tiff) (150 images from 4cam_auth base [12], 275 images from img_Nikon_D70s base [13], 75 images taken by non-professional camera);
- $M_{Jpeg,70}$, $M_{Jpeg,75}$, $M_{Jpeg,80}$ – each contained 500 images, obtained by re-saving of images from the set M_{Tif} to the Jpeg format with *QF*=70, 75, 80 respectively (the most frequently used quality factors in practice).

At the first stage, additional information was embedded into the original image (with or without loss) with the capacity of the hidden communication channel of 1, 5, 10%. The original image-container and the obtained steganographic messages were re-saved into lossy format (Jpeg) with all quality factors $QF \in \{1,2,...100\}$. As a result, discrete functions $y_0(QF)$ (for the container), $y_1(QF)$, $y_5(QF)$, $y_{10}(QF)$, $QF \in \{1,2,...100\}$ for the steganographic message were determined, respectively. A value characterizing the change in the function $y_0(QF)$ was considered as a quantitative characteristic of the image change as a result of the primary steganographic transformation:

$$T_{0,i} = \left(\sum_{1}^{100} \left| y_0(QF) - y_i(QF) \right|^2 \right)^{\frac{1}{2}}, i \in \{1,5,10\}. \quad (2)$$

At the second stage, additional information was re-embedded with the channel capacity of 1% into the steganographic messages generated at the first stage (the matrix of additional information ΔF was randomly generated, the same matrix was used for steganographic messages with the channel capacity of 1, 5, 10%, formed on the basis of one container). Steganographic messages obtained after the repeated steganographic transformation were re-saved with losses (Jpeg format) with $QF \in \{1,2,...100\}$. As a result, discrete functions $y_{1,1}(QF)$, $y_{5,1}(QF)$, $y_{10,1}(QF)$, $QF \in \{1,2,...100\}$ were obtained for steganographic messages with the channel capacity of the primary steganographic transformation of 1, 5, 10%, respectively. By analogy with (2), the following value was considered as a quantitative characteristic of the change in the image-steganographic message after repeated transformation:

$$T_{i,1} = \left(\sum_{1}^{100} \left| y_i(QF) - y_{i,1}(QF) \right|^2 \right)^{\frac{1}{2}}, i \in \{1,5,10\}. \quad (3)$$

The experimental results for the original images in the lossy format for the case of the Jpeg format with the quality factor *QF*=75 are shown in Fig. 1 and in Table 1, where can be observed the general tendency of qualitative changes in the values of estimates (2), (3) with increasing the capacity of the hidden channel of the primary steganographic transformation: decreasing the mode of the histogram of values $T_{i,1}$ with a simultaneous increase in the value in the mode; decreasing the length of the interval of possible values $T_{i,1}$ by decreasing the maximum value. $T_{i,1}$. The quality results obtained are typical for lossy images, regardless of the specifics of the format (Jpeg) and the quality factor used (*QF*=75). Using a different lossy format (for example, Jpeg2000) or a different quality factor will only change the quantitative indicators of the histograms.

Analysis of the numerical values of (2), (3) using the obtained histograms (Fig. 1) allows us to make conclusions, that the following points are important for evaluation the value of the capacity of the hidden channel:

- If for image, which is under examination the value $T_{i,1} \geq 125$, then the steganographic transformation were not applied to it;
- If $61 < T_{i,1}$, then for analyzed image the capacity of the hidden channel is <5%, here the image can be a "clean" container;
- If $26 < T_{i,1}$, then for analyzed image the capacity of the hidden channel is <10%.

The results obtained at this stage of the research are not final, the quantitative estimates obtained for the capacity of the hidden channel are one-sided (upper estimates), such that they depend on the value of the capacity of the hidden channel of the primary stegano-transformation of the image in the Jpeg format (*QF*=75). By expanding the computational experiment, by increasing the variety of values of the capacity of the hidden channel for the primary stegano-transformation (for example, from 1 to K% with a step h%), the results obtained can be made more precise, what will be done in the development of the direct method for evaluating the capacity of the hidden communication channel. Using a different lossy format (for example, Jpeg2000) or a different quality factor *QF* will change the quantitative indicators of histograms, therefore, the development of a method requires quantitative characteristics for all possible (most used) values of the quality factor. Taking into account their possible variety, the preliminary step of determining *QF* for a container in a lossy format is required before using the method for estimating the capacity of the hidden communication channel. It can be done using, for example, the method proposed in [14].

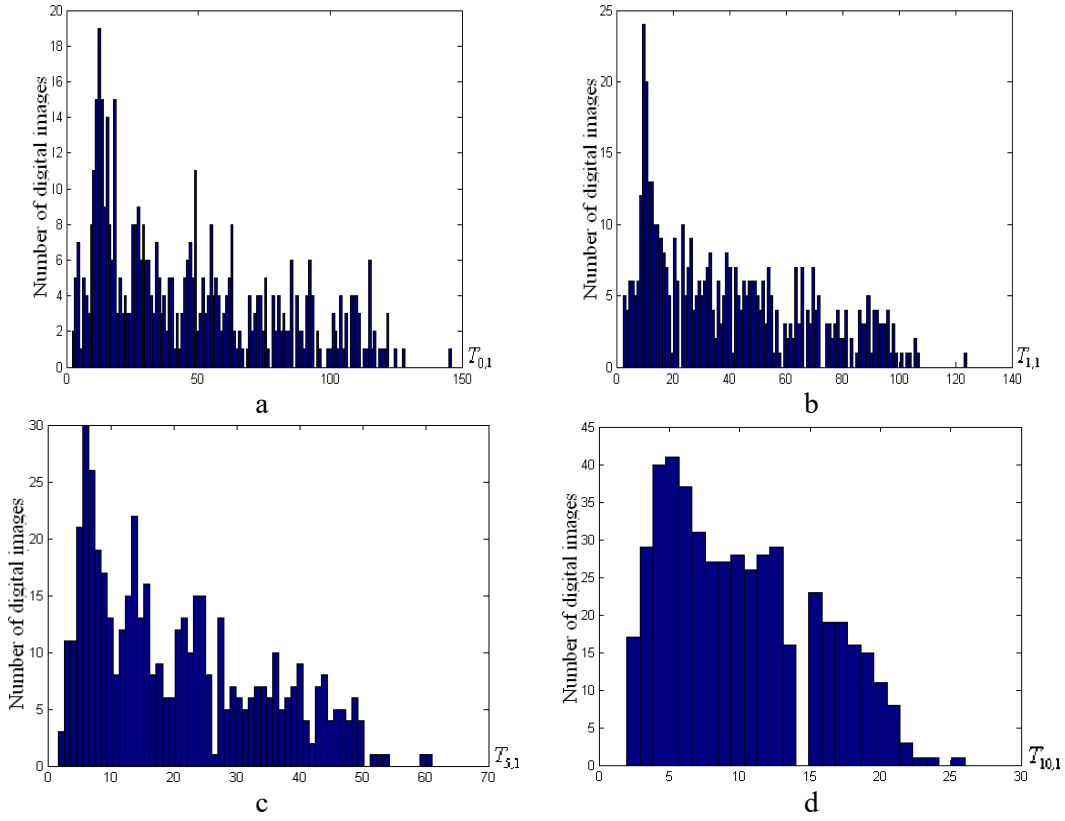


Figure 1: Histograms of values $T_{i,1}$, $i \in \{0,1,5,10\}$, for the original image-container, saved in Jpeg with QF=75: a – $T_{0,1}$ (the mode equals 13, the value in mode is 19); b – $T_{1,1}$ (the mode is 10, the value in mode is 24); c – $T_{5,1}$ (the mode is 6, the value in mode is 30); d – $T_{10,1}$ (the mode is 5, the value in mode is 41)

Table 1

Maximum and minimum values for the experiment $T_{i,1}$, $i \in \{0,1,5,10\}$ for image-containers, initially saved in Jpeg with *QF*=75

$T_{0,1}$		$T_{1,1}$		$T_{5,1}$		$T_{10,1}$	
Max	Min	Max	Min	Max	Min	Max	Min
146	2.1	124	2.4	61	1.7	26	2

3. Conclusions

The paper studied the properties of the normalized gap of the maximum singular value of the image matrix blocks, a discrete function $y(QF)$, that corresponds to the image in the conditions of its re-saving with losses with different quality factors and represents the number of blocks in which the normalized gap of the maximum singular value increases as a result of re-saving.

It is found that:

1. The number of image-steganographic message blocks, for which normalized gap of the maximum singular value increases when re-saving with losses, is greater, than in mage-container regardless of the container format (with/without losses);
2. The primary steganographic transformation of a digital image using a matrix ΔF changes («lifts» along the ordinate) the graph of the function $y\left(QF\right)$ higher, than a repeated steganographic transformation using the same matrix ΔF;
3. The higher the capacity of the hidden communication channel of the primary steganographic transformation, the smaller the difference between corresponding

functions $y(QF)$ for steganographic messages, obtained by single and double steganographic transformations, while the same matrix ΔF is used to re-embed additional information regardless of the capacity of the hidden communication channel of the primary steganographic message.

As a result of the studies, one-sided estimates (from above) of the capacity of the hidden communication channel were obtained in the conditions of the image-container in the Jpeg format (QF=75). The conducted studies and the obtained results indicate that the chosen direction is promising for evaluating the capacity of the hidden communication channel of the primary steganographic transformation of a digital image and is currently being continued by the authors.

4. References

[1] W. Mazurczyk, S. Wendzel, S. Zander, A. Houmansadr, K. Szczypiorski (Eds.), Information Hiding in Communication Networks: Fundamentals, Mechanisms, Applications, and Countermeasures, Wiley, Hoboken, 2016. doi:10.1002/9781119081715

[2] L.G. Pirtskhalava, V.A. Khoroshko, Yu.E. Khokhlachova, M.E. Shelest, Information Confrontation in Modern Conditions, Comprint, Kyiv, 2019.

[3] A.V. Agranovsky, A.V. Balakin, V.G. Gribunin. Steganography, Digital Watermarking, and Steganalysis, Vyzovskaya kniga, Moscow, 2009.

[4] K. Karampidis, E. Kavallieratou, G. Papadourakis, A review of image steganalysis techniques for digital forensics, Journal of Information Security and Applications 40(2018). doi:10.1016/j.jisa.2018.04.005.

[5] V.S. Ponomarenko (Ed.), A method for estimating the value of the hidden bandwidth of a steganographic communication channel. Information systems in management, education, industry. Kharkiv, 2014.

[6] S.S. Chaeikar, A. Ahmadi, Ensemble SW image steganalysis: A low dimension method for LSBR detection, Signal Processing: Image Communication 70(2019). doi:10.1016/j.image.2018.10.004.

[7] S.S. Chaeikar, M. Zamani, A.A. Manaf, A.M. Zeki, PSW statistical LSB image steganalysis, Multimedia Tools and Applications volume 77 (2018). doi:10.1007/s11042-016-4273-6.

[8] S.T. Veena, S. Arivazhagan, Universal secret payload location identification in spatial LSB stegoimages, Annals of Telecommunications 74(2019). doi:10.1007/s12243-018-0676-x.

[9] I.I. Bobok, A.A. Kobozeva, Steganalysis method efficient for the hidden communication channel with low capacity, Radiotekhnika 198 (2019). doi:10.30837/rt.2019.3.198.02

[10] J.W. Demmel, Applied Numerical Linear Algebra, SIAM, 1997.

[11] A.A. Kobozeva, V.A. Khoroshko, Analysis of Information Security, DUT, Kyiv, 2009.

[12] Y. Hsu, S. Chang, Detecting image splicing using geometry invariants and camera characteristics consistency, 2006 IEEE International Conference on Multimedia and Expo, Toronto, 2006. doi:10.1109/ICME.2006.262447

[13] T. Gloe, R. Böhme, The “Dresden Image Database” for benchmarking digital image forensics, 2010 ACM Symposium on Applied Computing (SAC ’10), New York, 2010. P. 1585–1591.

[14] A.A. Kobozeva, I.I. Bobok, L.E. Batiene, Steganoanalytical Method Based on the Analysis of Singular Values of Digital Image Matrix Blocks, *Problemele Energeticii Regionale* 3 (2018). URL: http://journal.ie.asm.md/ru/contents/electronni-jurnal-338-2018

Ентропійні Трансформації Універсуму Та Об’єкта Теорії Захисту Інформації

Кононович І.В. [1]
[1]*Національна академія харчових технологій, вул. Дворянська, 1/3,Одеса, 65023, Україна*

Анотація
Ентропія, маючи високий рівень загальності, впливає на формування моделей та теорії захисту інформації. Сьогодні на роль єдиної основоположної теорії ентропії, енергії, інформації претендує нова ентропія (ПАНтропія) А.М. Панченкова досліджень. Метод дослідження передбачає порівняння аксіоматичних визначень об’єкта теорії захисту інформації В.П. Іванова (унівесуму) та нової концептуальної моделі і теорії. Нова теорія при певних допущеннях включає ентропію та негентропію у себе як часткові випадки. У фазовому просторі ВСС треба оперувати двоїстими локальними координатами: узагальненою координатою; узагальненим імпульсом. Час теж має двоїстий характер. Цю термінологію потрібно буде інтерпретувати до дійсності.
Ключові слова
Ентропія, негентропія, ентропія Панченкова, ПАНтропия, захист інформації, аксіоми, структурна ентропія, двоїстість.

Entropic Transformations Of The Universe And The Object Of Information Security Theory

Kononovich I.[1]
[1]*Ntional Academy of Food Technologies, Dvoryanskaya str. 1/3, Odesa, 65023, Ukraine*

Abstract
Entropy, having a high level of generality, influences the formation of models and theories of information security. At the same time, the notions of entropy are undergoing revolutionary changes. Today, the role of a single fundamental theory of entropy, energy, information claims a new entropy (PANtropy) A.M. Panchenkova research. There is a need to clarify the role of entropy representations on the objects of information and cyber security systems theory. The research method involves comparing the axiomatic definitions of the object of information security theory VP Ivanov (universe) and a new conceptual model and theory. The new theory almost in no way contradicts the existing theories of thermodynamic entropy, Shannon's information entropy, and negentropy. It includes them under certain assumptions as partial cases. Duality is not enough to move from the Ivanov universe to the virtual continuous (VSS). In the phase space of the BCC it is necessary to operate with double local coordinates: generalized coordinate; generalized momentum. In the BCC conceptual model, the world consists of: the Entropy World and the Physical World. The entropy world includes entropy fields, flows, structures, in particular fields and flows of inertia. Time also has a dual character. There is astronomical time and entropy time. There are two types of BCC: inertial solid medium; dissipative continuous medium. Their descriptions cover movement and events. This terminology will need to be interpreted for the validity of security theory in further.
Keywords
Entropy, negentropy, information protection, axioms, structural entropy, duality.

EMAIL: irinakononovich2020@gmail.com
ORCID: 0000-0001-7146-3692 (A. 1);

1. Вступ

Ентропія, маючи високий рівень загальності, впливає на формування моделей природознавства і, конкретно, на теорію захисту інформації. У той же час, зазнають революційних змін уявлення про ентропію. Велике значення мали застосування: термодинамічної ентропії в термодинаміці як функції, що характеризує міру незворотного розсіювання енергії; ентропії в статистичній фізиці, як характеристики ймовірності певного макроскопічного стану системи, в математичній статистиці, як міри невизначеності розподілу ймовірностей; у теорії інформації інформаційна ентропія (ентропія Шеннона) як міра хаотичності або невизначеності очікуваного повідомлення тощо. Завдяки Шедінгеру та Бріллюену, за допомогою негентропії отримали пояснення процеси впорядкованості внутрішньої структури, збільшення складності, зменшення невизначеності. Пригожин розробив теорію самоорганізації систем далеких від рівноваги. Однак це не вирішило всіх проблем. В кінці 20 століття критика ентропії посилилась [1].

Сьогодні на роль єдиної основоположної теорії ентропії, енергії, інформації претендує нова ентропія Панченкова А.М. [2, 3]. Цю ентропію ми далі будемо коротко називати ПАНтропією в честь її розробника.

Метою даного дослідження є виявлення ролі та розробка методології ентропійних уявлень в теорії інформаційної та кібернетичної безпеки систем з використанням ПАНтропії.

2. Аксіоматичні основи теорії захисту інформації

В.П. Іванов розробив аксіоматичну теорію захисту інформації. Його система аксіом Теорії захисту інформації дозволяє формувати та обґрунтовувати постулати та твердження відносно систем захисту інформації. Перші три аксіоми, які лежать у основах цієї теорії, мають такі формулювання [4].

Аксіома Іванова 1. «Всі наслідки і висновки теорії захисту інформації можуть бути отримані з розгляду взаємодії об'єктів-носіїв фундаментальних понять:

– інформація, яка підлягає захисту;

– середовище (простір, поле) існування інформації, утворена як з об'єктів-носіїв властивостей захисту інформації, так і властивостей, які надають дестабілізуючий вплив на неї;

– час, як годинник;

– інерційна система».

Логічним обґрунтуванням такого вибору фундаментальних понять є те, що вони утворюють цілісну систему, в якій інформація, що підлягає захисту, існує в матеріальних формах (поля, електричні сигнали, візуальні образи, ...), а середовище (простір, поле) існування інформації та час є обов'язковими атрибутами матерії. Об'єкти-носії фундаментальних понять теорії захисту інформації існують в одній інерційній системі. Сучасне природознавство визначає наступні основні форми руху: рух переміщення; рух зміни стану.

Аксіома Іванова 2. «Теорія захисту інформації формує висновки з розгляду специфічної форми руху – зміни станів системи (зокрема захищеності системи), утвореної взаємодією об'єктів-носіїв фундаментальних понять. Процеси представляються у вигляді певного «ланцюга» змін у часі станів системи».

Аксіома Іванова 3. «Інформація, що підлягає захисту, вважається захищеною, якщо вона захищена в кожній точці простору, що знаходиться на траєкторії її проходження, і в кожен момент часу, коли вона зберігає цінність».

Аксіома Іванова 4. Методологічною підставою теорії захисту інформації є теорія систем, яка характеризується «своїми» принципами, властивостями, постулатами, зокрема, ентропією.

До основних недоліків понять класичної ентропії С.Хайтун [див. 1] відносить наступне.

Стосовно реальних систем трактовка ентропії як міри безпорядку помилкова і спричиняє великий негативний вплив на сучасну картину світу. Існуючі для ентропії «кількісні вирази не дозволяють безпосередньо визначати (вимірювати) її значення для реальних систем.

Є закон зростання ентропії. В фізиці закон зростання ентропії «формулюється як еволюційний закон неперервної дезорганізації або руйнування початкової заданої структури [5; с. 39]. Зі всього сказаного робиться висновок – виробництво ентропії позитивне у системах, у яких хаос виникає із порядку; так і в системах у яких порядок народжується із хаосу.

Еволюція спостережуваного світу – неорганічного, органічного та соціального – йде у протилежну сторону від спрощення, в сторону ускладнення. Ряд вчених доводять, що зростання ентропії може супроводжуватись ростом складності навіть в ізольованих системах. Ускладнення пояснюються впливом гравітації, зменшенням складності на нижніх рівнях організації систем, зростанням числа можливих макростанів тощо. Інша частина

вчених намагається переосмислити базові поняття подібно А.Н. Панченкову.

До аксіоми Іванова [4] можна включити поняття універсуму, негентропії та еквівалентності енергії, ентропії, інформації.

Універсум створюється з ієрархічно та інтерактивно взаємопов'язаних різноманітних систем. «Універсум складається із нескінченного числа об'єктів у стані неперервного розвитку в умовах величезного різноманіття. Сюди відносяться, крім матеріальних часток та енергії, також різного роду поля, духовне життя, свідомість, емоції, явища культури, енергетичні колапси у космосі та зникнення речовини, простору і часу». Система розглядається як цілісна сукупність елементів та відносин між елементами. По А. Рапопорту абстрактна система є певною частиною універсуму, яку можна описати так, що певній кількості змінних надаються конкретні величини.

А.М. Панченков розробив добре визначену аксіоматичну теорію для «описання Всесвіту та оточуючої нас Дійсності. Об'єктом концептуальної моделі та теорії виступає віртуальне суцільне середовище (ВСС), мірою досконалості якого являється» ПАНтропія [2].

3. Порівняльний аналіз об'єктів теорії захисту інформації та теорії нової ентропії Панченкова

«Віртуальним суцільним середовищем (ВСС) називається абстрактний об'єкт, який визначається аксіомами, що наведені в правій колонці табл. 1. Для порівняння аксіоми теорії В.П.Іванова наведені у середній колонці. Аксіоматичний об'єкт теорії Іванова описується вербально. Об'єкт концептуальної моделі та теорії Панченкова описується строго математично. Це не заважає аналізу.

Таблиця1

Порівняння аксіоматичних основ теорій В.П. Іванова та А.М. Панченкова

№ п/п	**Аксіома Іванова 1.** «Всі наслідки і висновки теорії захисту інформації можуть бути отримані з розгляду взаємодії об'єктів-носіїв фундаментальних понять:	Об'єкт концептуальної моделі та теорії А.М. **Панченкова – віртуальне суцільне середовище (ВСС)**, мірою досконалості якого являється» ПАНтропія. ВСС називається абстрактний об'єкт, який визначається аксіомами [3, с. 38]:
A	– інформація, яка підлягає захисту;	1 ВСС знаходиться в обмеженій області простору $R^n \oplus R_n$, яка називається фазовим простором. R^n та R_n, n – мірний евклідовий простір та спряжений евклідовий простір, відповідно.
B	– середовище (простір, поле) існування інформації, утворена як з об'єктів-носіїв властивостей захисту інформації, так і властивостей, які надають дестабілізуючий вплив;	2 У фазовому просторі ВСС характеризується двоїстими локальними координатами: **p** – узагальненою координатою; **q** – узагальненим імпульсом. При цьому $\mathbf{q} \in \Omega_q$, де Ω_q – конфігураційний простір; $\mathbf{p} \in \Omega_p$, де Ω_p – простір імпульсу; $\Omega_q \subset R^n$; $\Omega_p \subset R_n$; $\Omega = \Omega_q \times \Omega_p$, де Ω – фазовий простір.
C	– час, як годинник;	3 Функціонування ВСС відбувається параметричному просторі $J \subset R$, де J – часовий інтервал, елементом якого являється параметр t – час, що поділяється на астрономічний час та ентропійний час.
D	– інерційна система	4 ВСС володіє щільністю $\rho = \rho(\mathbf{q}, \mathbf{p}, t)$.
E		5 Маса ВСС – є величиною, яка зберігається.
F	– визначені ентропія, негентропія	6 У фазовому просторі визначена ПАНтропія ВСС.
G	– ентропія у незворотних процесах лише збільшується	7 Екстремальним принципом ВСС являється принцип максимуму ентропії.
H	–	8 Фундаментальною симетрією є двійковість»

Таким чином, формальне визначення абстрактного об'єкта – ВСС має вигляд кортежу S = {**q**, **p**, t, ρ | $\mathbf{q} \in \Omega_q$; $\mathbf{p} \in \Omega_p$; $\Omega = \Omega_q \times \Omega_p$; $\Omega_q \subset R^n$; $\Omega_p \subset R_n$; $\Omega \subset R^n \oplus R_n$; m; H_f }, де H_f – ПАНтропія.

Нова теорія майже ні в чому не заперечує існуючі теорії термодинамічної ентропії, інформаційної ентропії Шеннона та негентропії. Вона при певних допущеннях включає їх у себе як часткові випадки.

Загальна ПАНтропія має позитивний смисл, але більш широкий, ніж негентропія. ПАНтропія – це міра досконалості ВСС та його структур. З іншого боку ПАНтропія – це міра впорядкованості ВСС. Важливу роль представляє двоїсте представлення

$$H_f = H_q + H_p, \qquad (1)$$

де H_f – ПАНтропія, H_q – структурна ентропія, H_p – ентропія імпульсу. Крім того, в дисипативному віртуальному середовищі існує пасивна компонента ентропії, що входить до складу структурної ентропії – заморожена ентропія. Остання при деяких припущеннях є ентропією Больцмана, тобто термодинамічною ентропією.

Для переходу від універсуму Іванова до ОСС не вистачає двоїстості. У фазовому просторі ВСС треба оперувати двоїстими локальними координатами: **p** – узагальненою координатою; **q** – узагальненим імпульсом. Це дасть можливість забезпечити захист як інформаційних процесів, так і ресурсів, засобів обробки інформації.

Універсум Іванова одномірний. Він є сукупністю взаємопов'язаних систем чи об'єктів, нехай і дуже різноманітних.

ВСС принципово принаймні двох-мірний. Розрізняються конфігурації та рух, які характеризуються складовими ПАНтропії, відповідно: структурна ентропія та ентропія імпульсу. У концептуальній моделі ВСС світ складається з: Ентропійного світу та Фізичного світу. Ентропійний світ включає в себе ентропійні поля, потоки, структури, зокрема поля та потоки інерції…». Час теж має двоїстий характер. Є астрономічний час та ентропійний час.

Першоосновою, за словами А.М. Панченкова, нової концептуальної моделі природознавства є Принцип максимуму ентропії. Всі процеси у Всесвіті та оточуючої нас Дійсності підпорядковуються єдиному принципу – принципу максимуму ентропії. Глобальна симетрія визначається *теоремою*: у ВСС, яке задовольняє принципу максимуму ентропії Панченкова, існує глобальна симетрія – загальна ПАНтропія зберігає постійне значення $H_f = const$.

4. Висновки

Щоб застосувати нову концептуальну модель ПАНтропії для застосування в теорії та методології захисту інформації необхідно дати детальну інтерпретацію складових архітектури нової ентропії Панченкова. Маємо наступну архітектуру. «Існує два типи ВСС: інерційне суцільне середовище; дисипативне суцільне середовище. Їх описуванні охоплюють рух та події. Універсуму суцільних середовищ відповідає універсум різноманіть, який складається з: Гільбертово поля; екстремального пригранічного шару. Подія, що характеризується локальною калібровочною інваріантністю, відбувається у зоні руйнування Гільбертово поля, В зоні руйнування Гільбертово поля» реалізується і екстремальний пригранічний шар. Ця термінологія буде інтерпретована в ході подальшого дослідження.

Семантичний смисл ПАНтропії на її складових надзвичайно широкий.

5. Література References

[1] S.D. Khaytun, Traktovka entropii kak mery besporyadka i yeye vozdeystviye na sovremennuyu nauchnuyu kartinu mira. Voprosy filosofii. №2. 2013. S. 62–74. Url: http://vphil.ru/index2.php?option=com_content&task=view&id=709&pop=1&page=0.

[2] A.N. Panchenkov, Entropiya. Nizhniy Novgorod: Izdatel'stvo obshchestva «Intelservis». 1999. 592 s.

[3] А.Н. Панченков. Энтропия-2: Хаотическая механика. Нижний Новгород: Издательство общества «Интелсервис». 2002. 592 с.

[4] V. P. Ivanov, Ob osnovaniyakh teorii zashchity informatsii kak vnutrenne sovershennoy i vneshne opravdannoy nauchnoy teorii / Spetsial'naya tekhnika. № 3–4, 2008.

Information Technology For Identification Of Electric Stimulating Effects Parameters

Volodymyr Fedorchenko[1], Igor Prasol[2] and Olha Yeroshenko[3]

[1,2,3] *Kharkiv National University of Radio Electronics, Nauky Ave. 14, Kharkiv, 61166, Ukraine*

Abstract

A wide range of modern therapeutic devices based on various physical principles, widely used in medicine, cosmetology, sports. Among them, electric massage devices occupy a worthy place, alternative to classic manual massage. Therapeutic electromassage procedures are popular, convenient and beneficial for the recovery of the body. They are widely used in the treatment of chronic diseases of the circulatory system, musculoskeletal system, internal organs, etc. The restoration of damaged muscles is especially effective, при условии, что параметры стимулирующих воздействий выбраны правильно. Therefore, in this work, it is proposed to use an information method for studying the neuromuscular system based on electromyography.

The parameters of the stimulating effect do not always optimally correspond to a specific patient or a selected area of the body, which leads to insufficient effectiveness of therapeutic procedures, prolongation of rehabilitation. Elimination of shortcomings is possible due to the adjustment of the parameters of electrical stimuli depending on the data of myographic studies of a particular patient.

Based on the data obtained by EMG, specific parameters of stimulating effects (electrical impulses) are selected, such as amplitude, frequency, duty cycle, etc., which makes it possible to implement a technical device for carrying out rehabilitation procedures. Therefore, an electromassage apparatus is proposed, built on the basis of a modern microcontroller, which allows, on the basis of EMG data, to change stimulating impulses of exposure in a fairly wide range, thereby realizing an individual approach to each patient and increasing the efficiency of therapeutic procedures.

Keywords

Biomedical parameters, electromyostimulator, total electromyography, electromyogram, neuromuscular system, musculoskeletal system, time-frequency analysis

1. Introduction

In the modern world, the number of factors negatively affecting human health is becoming more and more. The human body ceases to have time to heal itself. All this requires a search for new combinations of recovery methods., when medical devices are used in conjunction with drug methods, implementing various types of electrotherapy.

The effectiveness of the use of electrotherapy devices is largely based on the use of methods and means of diagnostic support, which would give objective information about the patient's condition, contributing to the successful solution of the problem localization of zones of influence for electrostimulation, correct setting and achievement of treatment goals.

In order to improve the quality and speed of treatment, system development required, in which automation will be provided, allowingprovide the most effective treatment result.

The ultimate goal of creating an automated electrotherapy system is to develop modeling methodsand research of control systems and devices percutaneous electroneurostimulation, characterized by adaptation to changes in biological objects.

EMAIL: volodymyr.fedorchenko@nure.ua (A. 1); igor.prasol@nure.ua (A. 2); olha.yeroshenko@nure.ua (A. 3)
ORCID: 0000-0001-7359-1460 (A. 1); 0000-0003-2537-7376 (A. 2); 0000-0001-6221-7158 (A. 3)

The novelty is the development of a methodology for analyzing the functions of electrostimulating devices, which makes it possible to minimize negative effects during the stimulation procedure.

2. Electrostimulation

Electrical stimulation in this approach causes minimal changes in the treated area of the skinand nearby tissues, which allows to increase the efficiency of the treatment process.

Skeletal muscle electrical stimulation, which are the basis of the musculoskeletal system, gives a positive healing, preventive and training effects.

During electrical stimulation of the neuromuscular system, a rational choice of modes is importantand a combination of tonic and kinetic contractions, which significantly affect the increase in mass, development of strength, increased excitability and muscle performance [1, 2].

Electrical stimulation is successfully combined with traditional drug therapy. To enhance metabolic and trophic processes, muscle tissue stimulation is performed using targeted stimulation and contraction of a specific muscle group.

An important property of neuromuscular structures when irritated by electric currents, the dependence of excitability on the rate of change in the amplitude of the stimulating signal [1].

Depending on the signal amplitude and the excitation threshold of the neuromuscular structure, the following electrostimulation modes are distinguished: subthreshold, threshold and suprathreshold (fig. 1) [3-5].

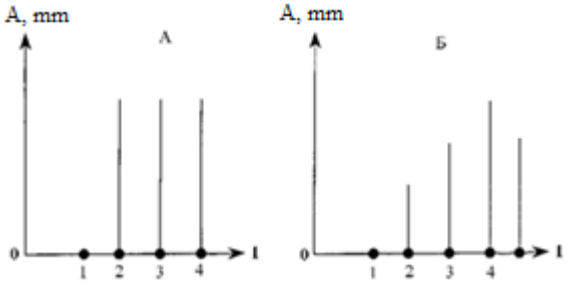


Figure 1: Dependence of the signal amplitude and the excitation threshold of the neuromuscular structure (а) - muscle fiber, б) – muscle, 1) subthreshold stimulus, 2) threshold stimulus, 3) submaximal suprathreshold stimulus, 4) maximum suprathreshold stimulus)

The dependence of the amplitude of muscle contraction on the strength of the stimulus occurs according to the law of power relations:

- Each excitatory tissue has its own functional reserve.
- Each excitatory tissue has its own functional boundary.

3. Electromyographic signal processing method

For a qualitative and quantitative assessment of the state of the human neuromuscular system using electromyogram (EMG) the information method of time-frequency analysis based on spectrograms can be used (fig. 2, fig. 3) [6-12].

To conduct a quantitative analysis of EMG signals, it is necessary to calculate the following parameters of the time-frequency representation of the total EMG: lower and upper cutoff frequency, median frequency, effective spectrum width and a number of others [13-41]. These processing parameters make it possible to fully assess the frequency content of the EMG signal.

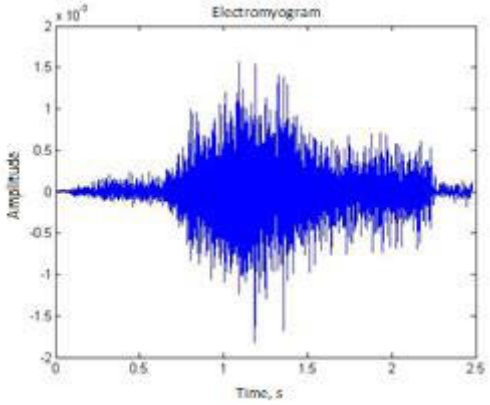


Figure 2: Electromyogram of the muscle *m. bicepsbrachii*

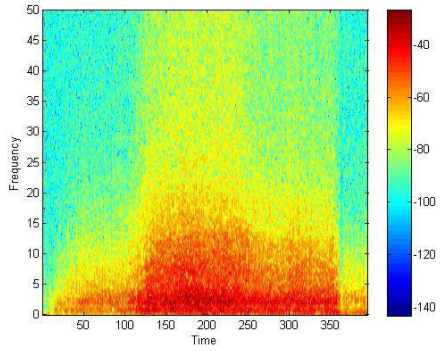


Figure 3: Corresponding spectrogram of the muscle *m. bicepsbrachii*

Let us represent the parameters of the EMG signal in the form of a certain finite set

$$A_m = \{a_i\}(i = \overline{1,m}), \quad (1)$$

where A - the designation of this set; m – cardinality multitudes; ai – elements of the set.

The elements of the set can be amplitudes, frequencies of the spectrum components, phase shifts, etc.

Let us represent the parameters of stimulating influences also in the form of a finite set

$$B_n = \{b_i\}(i = \overline{1,n}), \quad (2)$$

where B - the designation of this set; n – cardinality multitudes; bi – elements of the set.

The elements of the set can be the amplitude and frequency of stimuli, the type of modulation, modulation parameters, time intervals, etc.

Thus, the task is to determine such a transformation ω, which provides an unambiguous display of the elements of the number A to the corresponding elements B

$$A_m \overset{\omega}{\rightarrow} B_n, \quad (3)$$

EMG signal processing allows for ongoing monitoring the effectiveness of therapeutic effects due to the optimal selection parameters of stimulating effects.

4. Conclusions

Thus, carrying out qualitative and quantitative analyzes the structure of an EMG signal that is unsteady in natureand the dynamics of its parameters in the process of muscle contraction is performed based on the spectrogram, realizing graphical visualization of the amplitude, frequency and time components of the biomedical signal in real time. Consequently, specific parameters of stimulating effects can be selected based on the data of the EMG signal, which makes it possible to implement an effective technical device for carrying out individual therapeutic procedures.

5. References

[1] O. A. Yeroshenko, I. V. Prasol, V. V. Semenets, About building a system of muscle electrical stimulation for cadets, The use of information technology in the training and operation of law enforcement: materials International. scientific-practical conf. Mar 14-15 2018 Kharkiv: NANGU (2018) 120–122.

[2] O. M. Datsok, I. V. Prasol, O. A. Yeroshenko, Construction of a biotechnical system of muscular electrical stimulation, Bulletin of NTU "KhPI". Series: Informatics and modeling. Kharkiv: NTU "KhPI", № 13 (1338). (2019) 165–175. doi: 10.20998/2411-0558.2019.13.15

[3] P. P. Pestrikov, T. V. Pestrikova, Measuring system for recording signals from surface electromyography of forearm muscles, Electronic scientific publication "Scientific notes of PNU". Volume 10. No. 2. (2019) 173–180.

[4] O. Yeroshenko, I. Prasol, O. Datsok, Simulation of an electromyographic signal converter for adaptive electrical stimulation tasks, The current state of research and technology in industry. № 1 (15). (2021) 113–119. doi: 10.30837/ITSSI.2021.15.113

[5] S. S. Nikitin, Electromyographic stages of the denervation-reinnervation process in neuromuscular diseases: the need for revision, Neuromuscular diseases. Moscow. №2. (2015) 16–24.

[6] C. J. De Luca, The use of surface electromyography in biomechanics, Journal of Applied Biomechanics. № 13 (2). (1997).

[7] S. H. Roy, G. De Luca, S. Cheng, A. Johansson, L. D. Gilmore, C. J. De Luca, Electro-Mechanical stability of surface EMG sensors, Medical and biological engineering and computing. № 45. (2007).

[8] M. Voelker Implantable EMG measuring system, AMA Conferences. (2015).

[9] O. Yeroshenko, I. Prasol, O. Trubitsyn, and L. Rebezyuk, Organization of a Wireless System for Individual Biomedical Data Collection, International Journal of Innovative Technology and Exploring Engineering, vol. 9, no. 4, (2020) 2418–2421. doi: 10.35940/ijitee.D1870.029420

[10] A. N. Osipov, S. K. Dick, K. G. Senkovsky, Complex biotechnical feedback in electrostimulation systems, Moscow: Medical technology, № 6. (2007) 27– 29.
[11] K. Jermey, Atlas of Musculoskeletal Anatomy, AST Publishing House. (2008) 382 p.
[12] S. H. Roy, G. Luca De, S. Cheng, A. Johansson, L. D. Gilmore, C. J. Luca De, Electro-Mechanical stability of surface EMG sensors, Medical and biological engineering and computing. Vol. 45. (2007).
[13] M. M. Mezhennaya, Time-frequency analysis of the total electromyogram in the qualitative and quantitative assessment of the functional state of the human neuromuscular system. Biomedical radio electronics. № 2. (2012) 3-11.
[14] S. G. Nikolaev, Workshop on clinical electromyography, Ivanovo. (2001) 264 p.
[15] B. M. Gekht, Theoretical and clinical electromyography. (1990) 229 p.
[16] A. V. Sidorenko, V. I. Khodulev, A. P. Selitskiy, Nonlinear analysis of electromyograms, Biomedical technologies and electronics. №11. (200) 53–59.
[17] M. M. Mezhennaya, Choice of parameters of time-frequency processing of electromyograms of the neuromuscular apparatus, RT-2010: materials of the 6th Int. youth scientific-tech. conf. Sevastopol: SevNTU. (2010) 464 p.
[18] I. Perova, Ye. Bodyanskiy, Adaptive Human Machine Interaction Approach for Feature Selection-Extraction Task in Medical Data Mining, International Journal of Computing, no. 17(2). (2018) 113-119.
[19] M. Akay, Time-frequency representations of signals, Detection and estimation methods for biomedical signals. San Diego: Academic Press. (1996) 111–152.
[20] M. Hosokawa, Time-Frequency Analysis of Electronystagmogram Signals in Patients with Congenital Nystagmus, Japanese Ophthalmological Society. Vol. 48. (2004) 262–267
[21] J. Kaipio, Simulation and Estimation of Nonstationary EEG, Natural and Environmental Sciences. Vol. 40. (1996) 110.
[22] Z. Y Lin, D. Z Chen, Time-frequency representation of the electrogastrogram – application of the exponential distributions, IEEE Trans Biomed Eng. Vol. 41. (1994) 267–275.
[23] Rohtash Dhiman et al. Detecting the useful electromyogram signals–extracting, conditioning and classification, IJCSE. – Aug.–Sep. 2011. V. 2. № 4. (2011) 634–637.
[24] A. S. Borgul, A. A. Margun, K. A. Zimenko, A. S Kremlev., A. Y. Krasnov Intuitive Control for Robotic Rehabilitation Devices by Human-Machine Interface with EMG and EEG Signals, 17th international conference on Methods and Models in Automation and Robotics (MMAR 2012). Proceedings. Międzyzdroje: IEEE Xplore digital library. (2012) 308–311.
[25] A. A. Vorobyev, A. V. Petrukhin, O. A. Zasypkina, P. S. Krivonozhkina, A. M. Pozdnyakov, Exoskeleton as a new means in habilitation and rehabilitation of invalids (review), Sovremennye tehnologii v medicine (2015) 185–197. doi: 10.17691/stm2015.7.2.22.
[26] H. Kawamoto, Y. Sankai, Power assist method based on phase sequence and muscle force condition for HAL, Adv Robotic (2005) 717–734. doi: 10.1163/1568553054455103.
[27] D. P. Ferris, G. S. Sawicki, M. A. Daley, A physiologist's perspective on robotic exoskeletons for human locomotion, Int J HR (2007) 507–528. doi: 10.1142/s0219843607001138
[28] K. E. Gordon, M. Wu, J. H. Kahn, B. D. Schmit, Feedback and feedforward locomotor adaptations to ankle-foot load in people with incomplete spinal cord injury, J Neurophysiol (2010) 1325–1338. Doi: 10.1152/jn.00604.2009.
[29] C. K. Battye, A. Nightengale, J. Whillis The use of myoelectric current in the operation of prostheses, J Bone Joint Surg Br 37-B(3). (1995) 506–510.
[30] F. R. Finley, R. W. Wirta, Myocoder studies of multiple myopotential response, Arch Phys Med Rehabil 48(11). (1967) 598–601.
[31] B. Peerdeman, D. Boere, H. Witteveen, R. Huis in `tVeld, H. Hermens, i S. Stramigiol, H. Rietman, P. Veltink, S. Misra, Myoelectric forearm prostheses: state of the art from a user-centered perspective, J Rehabil Res Dev 48(6). (2011) 719. doi: 10.1682/jrrd.2010.08.0161.
[32] M. Aminoff Electromyography in clinical practice, Addison-Wesley (1978).
[33] J. M. Wakeling Spectral properties of the surface EMG can characterize motor unit

recruitment strategies, J Appl Physiol; 105(5). (2008) 1676–1677.

[34] C. Fleischer, A. Wege, K. Kondak, G. Hommel, Application of EMG signals for controlling exoskeleton robots, Biomed Tech 51(5–6). (2006) 314–319. doc: 10.1515/BMT.2006.063.

[35] D. Farina, L. Mesin, S. Marina, R. A. Merletti, Surface EMG generation model with multilayer cylindrical description of the volume conductor, IEEE Trans Biomed Eng 51(3). (2004) 415–426. doi: 10.1109/TBME.2003.820998.

[36] H. J. Hermens, B. Freriks, C. Disselhorst-Klug, G. Rau, Development of recommendations for SEMG sensors and sensor placement procedures, J Electromyogr Kinesiol 10(5). (2000) 361–374. doi: 10.1016/S1050-6411(00)00027-4.

[37] F. Sylos-Labini, V La Scaleia, A. d'Avella, I. Pisotta, F. Tamburella, G. Scivoletto, M. Molinari, S. Wang, L. Wang, E. van Asseldonk, H. van der Kooij, T. Hoellinger, G. Cheron, F. Thorsteinsson, M. Ilzkovitz, J. Gancet, R. Hauffe, F. Zanov, F. Lacquaniti, Y. P. Ivanenko, EMG patterns during assisted walking in the exoskeleton, Front Hum Neurosci 8. (2014) 423. doi: 10.3389/fnhum.2014.00423.

[38] R. Merletti, M. Aventaggiato, A. Botter, A. Holobar, H. Marateb, T. Vieira, Advances in surface EMG: recent progress in detection and processing techniques, Crit Rev Biomed Eng 38(4). (2011) 305–345. doi: 10.1615/CritRevBiomedEng.v38.i4.10.

[39] D. Farina, C. Cescon, Concentric-ring electrode system for noninvasive detection of single motor unit activity, IEEE Trans Biomed Eng 48(11). (2001) 1326–1334. doi: 10.1109/10.959328.

[40] J. L. Nielsen, S. Holmgaard, N. Jiang, K. Englehart, D. Farina, P. Parker, Enhanced EMG signal processing for simultaneous and proportional myoelectric control, Conf Proc IEEE Eng Med Biol Soc (2009) 4335–4338. doi: 10.1109/IEMBS.2009.5332745.

[41] D. P. Ferris, C. L. Lewis, Robotic lower limb exoskeletons using proportional myoelectric control, Conf Proc IEEE Eng Med Biol Soc (2009) 2119–2124. doi: 10.1109/IEMBS.2009.5333984.

Підвищення Кібербезпеки Комп'ютерних Мереж

Хорошко В.О. [1], Зибін С.В. [2], Хохлачова Ю.Е. [3] Аясрах А. [4], Аль-Далваш А. [5]

[1,2,3,4,5] *Національний авіаційний університет, пр-т Любомира Гузара 1, Київ, 03058, Україна*

Анотація

Розвиток комп'ютерних систем та інформаційних технологій неможливий без комплексного вирішення завдання підвищення ефективності передачі інформації спільно з вирішенням завдання захисту переданої інформації. Відомі методи і засоби захисту інформації вимагають додаткових матеріальних ресурсів у вигляді програмного, програмно-апаратного забезпечення або витрат апаратури. У роботі розглядається можливість підвищення кібербезпеки в діючих комп'ютерних мережах шляхом багатокритеріальної маршрутизації, яка враховує критерії живучості та кіберзахисту від несанкціонованого доступу і процесу її передачі від джерела до користувача. Ставиться також завдання підвищення кібербезпеки без додаткових засобів і витрат.

Ключові слова

кібербезпека, комп'ютерні мережі, підвищення кібербезпеки.

Enhancing the cybersecurity of computer networks

Khoroshko V. [1], Zybin S. [2], Khokhlachova Y. [3], Ayasrah A. [4], Al-Dalvash A. [5]

[1,2,3,4,5] *National aviation university, 1, Liubomyra Huzara ave., Kyiv, 03058, Ukraine*

Abstract

The development of computer systems and information technologies is impossible without a comprehensive solution to the problem of increasing the efficiency of information transmission together with the solution of the problem of protecting the transmitted information. Known methods and means of protecting information require additional material resources in the form of software, software and hardware, or hardware costs.

The paper considers the possibility of increasing cybersecurity in operating computer networks by means of multi-criteria routing, which takes into account the criteria of survivability and cyber protection from unauthorized access and the process of its transfer from the source to the user. The goal is also to improve cybersecurity without additional funds and costs.

Keywords

cybersecurity, computer networks, cybersecurity enhancement.

1. Вступ і аналіз публікацій

Аналіз досліджень і публікацій [2] дозволяє зробити висновок, що якість управління кібербезпекою залежить від співвідношення вартості ресурсів захисту до втрат від порушення кібербезпеки. У поняття ресурсів включається програмне і апаратне забезпечення засобів захисту інформації. Отже, цей напрям управління кібербезпекою пов'язаний з додатковими програмними та апаратними витратами на засоби захисту.

EMAIL: professor_va@ukr.net (A.1); zysv@ukr.net (A.2); hohlachova@gmail.com (A.3); ahmadaesr@gmail.com (A.4); abduiiah.dalosh@gmail.com (A.5)

ORCID: 0000-0001-6213-7086 (A.1); 0000-0002-2670-2823 (A.2); 0000-0002-1883-8704 (A.3); 0000-0003-4392-1806 (A.4); 0000-0002-1003-9182 (A.5)

Існує інший напрямок підвищення кібербезпеки, який пов'язаний із забезпеченням необхідної якості і рівня обслуговування в комп'ютерних мережах [3]. Протоколи маршрутизації в комп'ютерних мережах враховують в цьому випадку кілька критеріїв якості [4]. Напрямки та шляхи передачі інформації в цьому випадку визначаються на основі комп'ютерної метрики, між двома вузлами комп'ютерної мережі:

$$M = \left(K_1\beta + \frac{K_2}{256-z} + K_3 r\right)\frac{K_5}{p+K_4}, \qquad (1)$$

де β – пропускна здатність мережі; r – час затримки передачі даних; p – надійність передачі даних; z – відносне завантаження; K_1, K_2, K_3, K_4, K_5 – вагові коефіцієнти.

Недостача композитної метрики (1) пов'язана з відсутністю теоретичного обґрунтування вибору її структури і параметрів. З іншого боку, композитна метрика (1) не враховує критерії якості рівня захисту переданої інформації від несанкціонованого доступу.

2. Постановка завдання

У зв'язку з цим виникає завдання багатокритеріальної маршрутизації, яка враховує критерії якості передачі інформації спільно з критеріями якості кібербезпеки від несанкціонованого доступу.

Метою статті є рішення задачі багатокритеріальної маршрутизації для підвищення кібербезпеки користувачів комп'ютерних мереж.

3. Основна частина

Поставлену задачу будемо вирішувати методом математичного моделювання комп'ютерної мережі на графі, вершини якого моделюють вузли-джерела і вузли-приймачі інформації, а гілки графа відповідають каналам передачі інформації. Введемо систему частинних критеріїв якості, яка, з одного боку, характеризує якість передачі інформації від вузла-джерела до вузла-приймача, а з іншого боку, характеризує рівень кіберзахисту переданої інформації від несанкціонованого доступу. Припустимо, що швидкість передачі даних оцінюється частинним критерієм якості H_1^*; час затримки передачі даних задається частинним критерієм якості H_2^*; надійність передачі даних враховується частинним критерієм якості H_3^* ; втрати інформації або її модифікації оцінюється частинним критерієм H_4^* тощо. У цій системі частинних критеріїв якості H_1^* та H_2^* оцінюють технічні характеристики каналу передавання інформації. Частинний критерій якості H_3^* оцінює надійність передачі інформації в умовах дії внутрішніх і зовнішніх перешкод і збурень. Рівень кіберзахисту каналу передачі даних характеризується ризиком H_4^* втрати інформації або її модифікації в процесі передачі даних. У системі частинних критеріїв, яка розглядається, частинні критерії H_1^*, H_2^*, H_4^* необхідно мінімізувати, а частинний критерій якості H_3^* слід максимізувати. Приведемо всі частинні критерії якості до випадку мінімізації. З цією метою максимізований частинний критерій якості H_3^* замінимо на мінімізований частинний критерій якості $H_3 = H_{3m} - H_3^*$, де H_{3m} – максимально можливе значення надійності, яке задається технічними характеристиками каналу передачі даних.

У загальному випадку вважається, що якість обслуговування і рівень кібербезпеки користувача оцінюється n мінімальними критеріями якості $H_1, H_2, H_3, \dots, H_n$. На підставі технічних характеристик каналів передачі інформації, вимога до якості обслуговування і рівню кібербезопаностью задається гранично допустимими значеннями частинних критеріїв якості $H_{1m}, H_{2m}, H_{3m}, \dots, H_{nm}$. Потім переходимо до системи відносних частинних критеріїв якості H_1/H_{1m} , H_2/H_{2m} , H_3/H_{3m} , … , H_n/H_{nm} , діапазон і зміни яких задаються обмеженнями:

$$0 \le \frac{H_i}{H_{im}} \le 1, i = 1, n. \qquad (2)$$

Відомо, що задача багатокритеріальної оптимізації є некоректною, оскільки частинні критерії якості конфліктують між собою [3]. Покращення одного частинного критерію якості погіршує один або кілька інших частинних критеріїв. Регуляризацію некоректної задачі багатокритеріальної оптимізації зазвичай виконують лінійною згорткою частинних критеріїв якості з ваговими коефіцієнтами:

$$H = \sum_{i=1}^{n} \alpha_i \frac{H_i}{H_{im}}, \qquad (3)$$

де $\sum_{i=1}^{n} \alpha_i = 1$, α_i – вагові коефіцієнти.

Результатом застосування прямолінійного методу згортки частинних критеріїв якості (3) так само як метод композитної матриці (1)

стикається з проблемою вибору вагових коефіцієнтів. Відомий метод вирішення задачі багатокритеріальної оптимізації, який не вимагає рішення проблеми вибору вагових коефіцієнтів. Відповідно до цього методу, регуляризація некоректної задачі багатокритеріальної оптимізації здійснюється скалярною згорткою за нелінійною схемою компромісів [4]:

$$J = \sum_{i=1}^{n} \frac{1}{1 - \frac{H_i}{H_{im}}} \qquad (4)$$

де H_i – i-й частинний критерій якості; H_{im} – гранично допустиме значення частинного критерію якості H_i.

Передбачається, на відміну від композитної матриці (1) і лінійної згортки (3), присвоювати гілкам графа не пропорційно скалярною величиною J, яка визначається за нелінійною схемою компромісу (4).

Математична модель комп'ютерної мережі у вигляді графа, всі гілки якого розраховуються за виразом (4) дозволяє реалізувати многокритериальную оптимізацію маршрутів передачі інформації від вузла-джерела до вузла-приймача шляхом мінімізації критерію якості:

$$\min_{J} L = \sum_{j=1}^{r} \times \sum_{i=1}^{n} \frac{1}{1 - \frac{H_{ij}}{H_{ijm}}}, \qquad (5)$$

де H_{ij} – i-й частинний критерій якості j-ої гілки графу; H_{ijm} – гранично допустиме значення i-го частинного критерію якості у j-й гілці графу; n- кількість гілок графу за маршрутом від вузла-джерела до вузла-приймача.

З урахуванням виразу (4) вираз (5) можна привести до виду:

$$\min_{J} L = \sum_{j=1}^{r} J_{j,}$$

відомої задачі про найкоротший шлях, яка може бути вирішена алгоритмом Дейкстри [5] або паралельними засобами маршрутизації [3].

$$J_j = \sum_{i=1}^{n} \frac{1}{1 - \frac{H_{ij}}{Hijm}}, \qquad (6)$$

де J_j – вага j-ї гілки графа математичної моделі комп'ютерної мережі.

4. Висновки

Завдання мінімізації критерію якості (6) відома як задача про найкоротший шлях між вузлом-джерелом і вузлом-приймачем. Отже, застосування для розрахунку ваг графа математичної моделі комп'ютерної мережі згортки з нелінійної схемою компромісів (4) зводить задачу багатокритеріальної маршрутизації до відомої задачі про найкоротший шлях, яка може бути вирішена алгоритмом Дейкстри [5] або паралельними засобами маршрутизації [3].

5. Литература References

[1] Tomashevsky V.M. Model of systems / V.M. Tomashevsky – K: View. group BHV, 2007.

[2] Tymoshenko A.O. Methods for the analysis and design of systems to obtain information / A.O. Tymoshenko – K: Politechnika, 2007.

[3] Zgurovsky M.Z. Technological foresight / M. V. Zgurovsky, N. D. Pankratova – K: Polytechnic, 2005.

[4] Koval V.N. Applied systems for the analysis of multidimensional processes / V.N. Koval – K: Naukova Dumka, 2002.

[5] Ivakhnenko A.G. Modeling of complex systems based on experimental data / A.G. Ivakhnenko, Yu.P. Yurachkovsky - M: Radio and communication, 2000.

[6] Khoroshko V.O. Bagatocriterial assessment of the efficiency of projects for the safety of cybersecurity / V.O. Khoroshko, M.Є. Shelest, Yu.M. Weaver // Technical sciences and technologies, No. 1 (19), 2020, pp. 121-131.

Identifying the Transition of Interactions in Virtual Communities of Social Networking Services to Chaotic Dynamics

Kateryna Molodetska[1], Serhiy Veretiuk[2] and Volodymyr Pilinsky[3]

[1,2] *Polissia National University, 7, Blvd. Stary, Zhytomyr, 10008, Ukraine*
[3] *National Technical University of Ukraine "Igor Sikorsky Kyiv Polytechnic Institute", 37, Prosp. Peremohy, Kyiv, 03056, Ukraine*

Abstract

The diversification of communication channels influenced by the development of information and communication technologies has made social networking services particularly popular among users. They provide actors with many tools not only for effective communication and networking in virtual communities but also for self-organization and coordination of interactions in real life. As a result of the diffusion of boundaries in the information space, social networking services have become an object of threats to the information security of the state. The experience of information operations against information security of the state has shown that because of targeted information impact on virtual communities of actors can occur chaotization of processes of their interaction. The result of such impact is a transition of such processes from online to real life in the form of mass civil protests. With the constant growth in the number of threats and the emergence of new methods of destructive information impact, the problem of their early detection and effective counteraction becomes particularly important. It is known that the transition of virtual community to deterministic chaos is characterized by increasing levels of entropy in the system. In this article, we use the kernel density estimation of the entropy distribution of the actors' interaction parameters in the social networking services to determine its dynamics to identify growth periods, preceding the system's transition to chaotic dynamics. Determination of the nature of entropy function's variation from time will make it possible to determine the moments of application of controlling influence on information space of the social networking services and actors, which will ensure reduction of the system's degrees of freedom with its subsequent transition to a given state of information security. In this state the structure of virtual communities' changes because of the self-organization of actors, providing information exchange in communities, which is resistant to destructive impact. Application of the proposed approach will improve the effectiveness of countering threats to state information security in the social networking services.

Keywords

Social networking services, chaotic dynamics, kernel density estimation, entropy, Rössler attractor

1. Introduction

The growing influence of social networking services on social communication processes has turned them into a leading channel of communication [1-5]. Under these conditions, social networking services have become not only a leading source of information due to a high degree of trust in the content of the services but also an instrument of covert influence on social and political processes in the state [6-8]. Threats to information security of the state in social networking services of a communicative nature are connected to the realization of the needs of individuals, society and the state for the creation, consumption, dissemination, and development of national strategic content. Threats in social networking services may be aimed at influencing the mental and emotional state of actors, influencing their freedom of choice, calling for

EMAIL: kateryna.molodetska@polissiauniver.edu.ua (A. 1); sergey.veretiuk@gmail.com (A. 2); pww@ukr.net (A. 3)
ORCID: 0000-0001-9864-2463 (A. 1); 0000-0002-7915-9991 (A. 2); 0000-0002-2569-9503 (A. 3)

separatism, the overthrow of constitutional order, violation of territorial integrity, discrediting state authorities, supporting, accompanying, or activating criminal or terrorist activity, etc. [9, 10]. In the conditions of globalization of the national information space, absence of state borders in virtual information environment, constantly growing number of threats to information security of the state, the problem of modelling actors' interaction in virtual social networking services communities becomes especially topical. Research into processes of interaction between actors in the information space of the social networking services, considering the influence of threats, will make it possible to systematically counteract destructive information influence, which remains uncontrollable [11, 12].

Analysis of recent research and publications [13-15] has shown that one of the promising approaches to modelling social networking services as a class of complex dynamic systems is dynamic chaos theory. It allows considering key properties of social networking services – high sensitivity to initial conditions, as well as openness, nonlinearity, non-equilibrium and dissipativity of interaction in virtual communities. When interaction in social networking services turns to chaotic dynamics under the influence of information operations, not only the prediction of such interaction of actors becomes impossible, but also the system's behavior itself changes uncontrollably.

Such behavioral features can occur not only in the virtual space of the social networking services but can also be reflected in the actions of citizens in real life. Therefore, within the framework of solving the problem of modelling actors' interaction in virtual communities of services, not only the synthesis of control actions but also the point in time at which such a measure is implemented, is of particular importance. This approach will make it possible to suppress chaotic dynamics of interaction and form prerequisites for effective counteraction to threats to state information security in the social networking services [11, 15, 16].

The purpose of the article is to determine a point in time for effective implementation of the control action, followed by the transition of virtual communities of actors in the social networking services from chaotic interaction with a given state, in which the levelling of destructive information influence the actors is ensured.

To achieve the goal, the following tasks are required:

1) Formalize the interaction of actors in virtual communities of social networking services under the influence of threats using irregular attractors.

2) Estimate system entropy using kernel density estimation of actor interaction parameters in social networking services.

3) Identify existing precursors of chaotic dynamics of actors' interaction in the social networking services and give practical recommendations for their early identification.

2. Modelling actors' interaction in social networking services based on irregular attractors

In the case of transition of social networking services actors' interaction to deterministic chaos, it is characterized by the high sensitivity of virtual communities to changes in system parameters and the action of disturbances, in particular destructive information influences. Even if the interaction of actors in the social networking services is formalized by deterministic models, in a state of deterministic chaos, their communication turns into random and unpredictable processes (Figure 1).

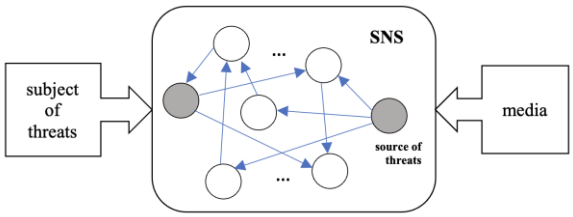


Figure 1: Social networking services as a target of threats

To describe the interaction of actors in the social networking services when the system transitions to chaotic dynamics, it is advisable to use irregular attractors. Even though social networking services is a dissipative system, which can be either open or non-equilibrium, using the irregular attractors is appropriate.

The features of irregular attractors are the complex geometric structure of the set of states of the system they describe. Such attractors are characterized by a simultaneous combination of both stability and instability. Therefore, irregular attractors provide a high degree of adequacy in describing the interaction of actors in the social networking services, which are taking place under the conditions of information confrontation. Such

attractors include Lorenz attractors, Rössler attractors, and others [17, 18].

2.1. Rössler chaotic system

In general terms, the actors' interaction in the social networking services using the Rössler irregular attractor is formalized as a system of differential equations [19]

$$\begin{cases} \frac{dI(t)}{dt} = \gamma R(t) + \theta Z(t); \\ \frac{dR(t)}{dt} = \xi I(t) + \mu R(t); \\ \frac{dZ(t)}{dt} = a + I(t)Z(t) - bZ(t), \end{cases} \quad (1)$$

where $I(t)$ is the destructive information influence, which is carried out by the opposing group in the social networking services information space; $R(t)$ is the function which characterizes the actors' ability to critically perceive the content and determines the level of information resistance to destructive information influence; $Z(t)$ is the function that determines the actor's level of readiness for active actions in real life, which is induced by destructive information influence $I(t)$, $Z(t) > 0$; γ is a parameter that determines the level of destructive information influence on actors aimed at overcoming their information resilience and is related in inverse relation to θ, $\gamma < 0$; θ is a parameter of actor's readiness level to move to active actions in real life; ξ is an information influence that is performed using strategic communication channels and is aimed at building information resilience in actors, $\xi > 0$; μ is a parameter that determines the actors' prior experience in identifying threats in the social networking services; a is an integrative parameter that determines the actors' ability to switch to active actions as a result of destructive information influence and is formed as a result of individual characteristics; b is a parameter that determines the actors' ability to switch to chaotic dynamics under the influence of destructive information influence.

To simulate the interaction of actors in the SIS based on the synthesized model (1) were used the tools of *Google Collaboratory* environment and programming language *Python*. The bifurcation diagram of the system of differential equations (1) at values of parameters $\gamma = 1$, $\xi = 1$, $\theta = 1$, $\mu = 0.2$, $a = 0.2$, $b = \{1; 10\}$ is constructed, which is presented in Figure 2.

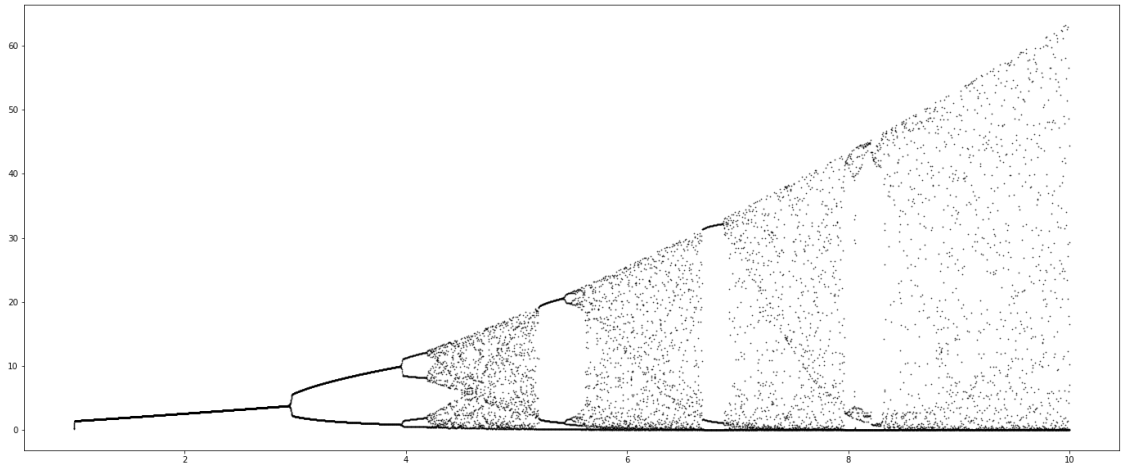


Figure 2: Bifurcation diagram of the Rössler attractor

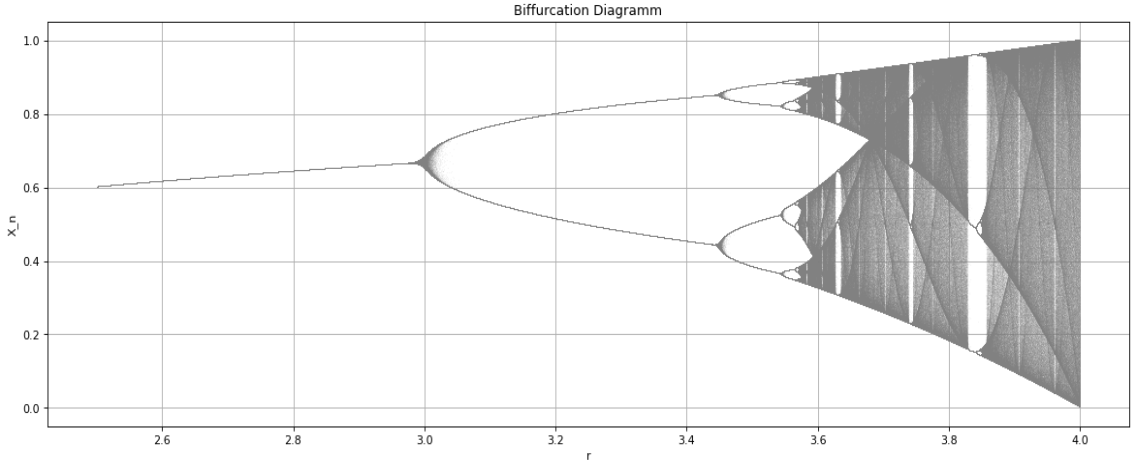
Rössler bifurcation diagram is similar in nature and behavior to the logistic transformation bifurcation diagram (Figure 2 a, b) [20, 21]

$$x_{n+1} = rx_n(1 - x_n). \quad (2)$$

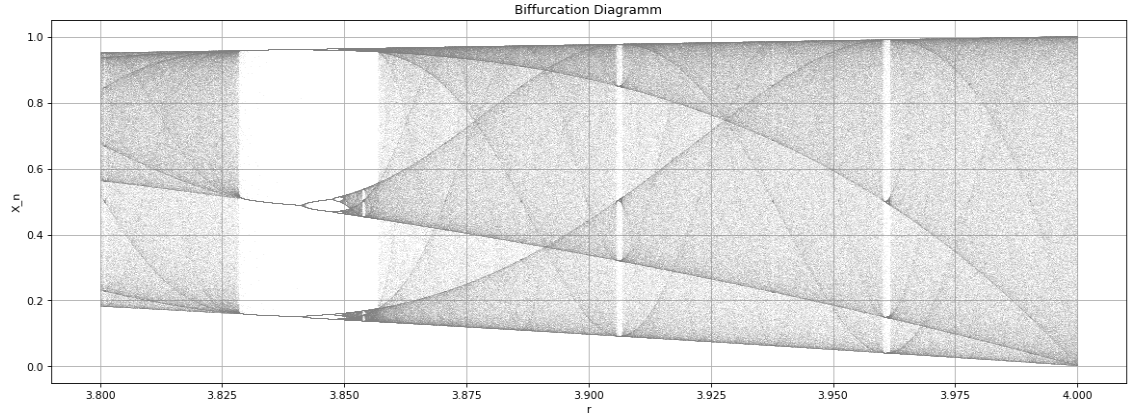
2.2. Determination of the chaotization metric of the system based on entropy

To simplify the calculations, we further analyze the behaviour of Rössler system in the Z-plane based on the analysis of the bifurcation diagram of the logistic transformation.

It is known from analysis of sources [22, 23] that a marker of chaotic dynamics appearance in a system is a senior Lyapunov exponent. Despite the developed mathematical apparatus associated with the study of dynamical systems and their behaviour based on Lyapunov exponents, this approach has an analytical character. In practice, it leads to post-analysis based on a statistical retrospective analysis of the system parameters.



(a) the control parameter $r \in (2.5; 4)$;



(b) the control parameter $r \in (3.8; 4)$;

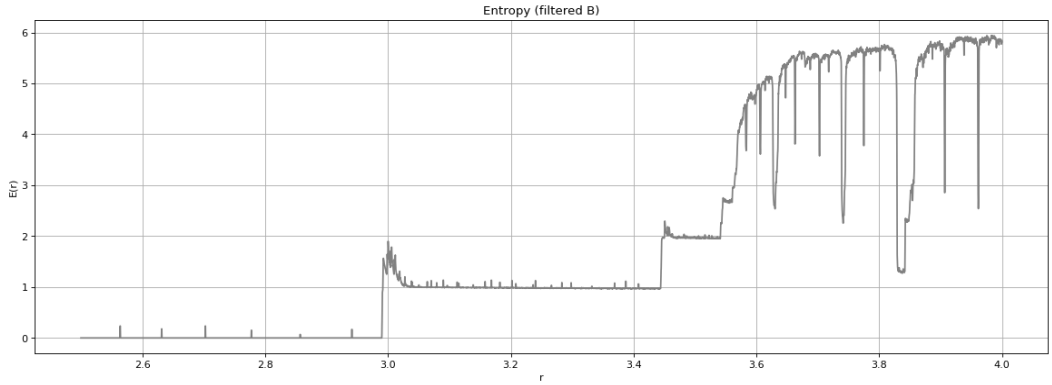
Figure 3: Bifurcation diagram of the logistic transformation

It is well known that the bifurcation diagram in its physical sense describes possible states of the system depending on the control parameter r [24-26]. Each "slice" of the bifurcation diagram $\{X_i(r)\}$ describes a set of system states $x_{ij} \in X_i(r), j \in (1; inf)$ is the number of system states in the j-th "slice" of the bifurcation diagram. We will determine the entropy of the system based on a preliminary analysis of the probability density of states S_{ij}, for this purpose we use the mathematical apparatus *KDE* (*Kernel Density Estimation*) [27]. Therefore, we transform the sequence of "slices" into the sequence of estimates of kernels of normalized probability density distribution – $p_i(x)$.

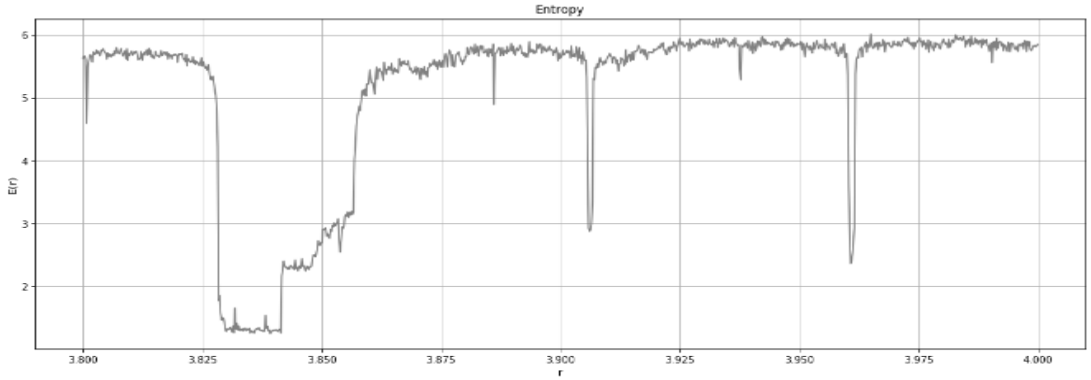
To determine the entropy of the system at known values of the probability density distribution, we use the expression for Shannon's entropy [28]

$$E_i = -\int p_i(x) log_2\big(p_i(x)\big) dx. \qquad (3)$$

Thus, for each set of states $X_i(r)$ the entropy E_i is obtained. The variation of the entropy value is shown in Figure 4.



(a) the control parameter $r \in (2.5; 4)$;



(b) the control parameter $r \in (3.8; 4)$;

Figure 4: Shannon's entropy for the logistic mapping at different values of the parameter r

3. Modelling results

The analysis of the bifurcation diagram and entropy suggests the following:

1. Local maximums of entropy are observed at bifurcation points, which is interpreted by a temporal increase in uncertainty. It can be related to an abrupt change in the behaviour of social networking services' actors because of destructive information influence on virtual communities [29, 30]. Actors need some transition period to form their viewpoint on the events in the information space to further interact with other actors and virtual communities.

2. The life cycle of the virtual community of actors in social networking services is followed by changes in indicators of their interaction from stationary (characterized by a decrease in entropy value) to chaotic dynamics (entropy growth). The result of passing the bifurcation point by the system is structural changes in virtual communities – the number of participants, creation of new associations, interaction through likes, reposts and distribution of given content.

3. The transition of actor interactions in the social networking services to chaotic dynamics is accompanied by a rapid increase in the value of entropy

$$\frac{dE}{dt} \gg M.$$

4. In the field of chaotic dynamics of actors' interaction in the social networking services, the entropy of the system tends to the maximum, as the probability density distribution approaches uniformity. If the number of states of the virtual community of actors is N, then under the conditions of transition to chaotic dynamics $N \to \infty$. In this case, the probability of being the virtual community in one of these states is defined as uniform distribution

$$p = \frac{1}{N}$$

Then the entropy is defined as

$$E = -\sum_{i=1}^{N} p_i \log_2 p_i = -\sum_{i=1}^{N} \frac{1}{N} \log_2 \frac{1}{N}.$$

From where

$$E(N \to \infty) = \lim_{N\to\infty} \left(-\sum_{i=1}^{N} \frac{1}{N} \log_2 \frac{1}{N} \right) =$$

$$= \lim_{N\to\infty} \left(-N \frac{1}{N} \log_2 N \right) = \lim_{N\to\infty} \log_2 N.$$

4. Practical guidelines

Considering the results of the modelling of actor interactions in virtual communities, the following practical recommendations for identifying precursors of chaotic dynamics are given:

1. Applying Rössler chaotic system for modelling actors' interaction in social networking services under the destructive information influence and conduct of information confrontation allows describing the transition of citizens' potential to active actions in real life. Therefore, it is reasonable to apply the proposed approach to modelling interactions in virtual communities when developing and improving the subsystem of information space monitoring within the framework of the state information security system in the social networking services.

2. The simulation of virtual communities in the social networking services based on the chaotic Rössler system is appropriate for monitoring the interaction of groups of actors created and/or managed by an opposing force. Actors of such

virtual communities are potentially used to participate in mass protests and unrest in real life. Therefore, timely identification of signs of their transition to chaotic dynamics based on entropy indicator (3) will allow responding in advance to changes in the situation in the social networking services information space.

5. Conclusions

Simulation of actors' interaction in the social networking services based on irregular attractors investigates the processes of transition of communication in the information space of services into chaotic dynamics, in which associations of actors become unmanageable. The application of irregular attractors helps considering the effect of destructive information influence on actors in the social networking services in the conditions of information confrontation. To achieve this, interaction in the information space of services is modelled using the Rössler irregular attractor, which enables the formalization of interaction not only online but also the transition of actors to acts of defiance in real life. For early detection of signs of transition to chaotic dynamics, we propose to use the kernel density estimation of the entropy distribution of interaction parameters of actors in the social networking services to determine its dynamics to identify periods of growth. Thus, the analysis of entropy value dynamics changes indicates a transition of virtual community to chaotic dynamics and promptly applies methods of its suppression.

6. References

[1] Liu Y., Ni X., and Niu G. “The influence of active social networking services use and social capital on flourishing in Chinese adolescents.” Children And Youth Services Review 119 (2020): 105689. doi: 10.1016/j.childyouth.2020.105689

[2] Laghari A., and Laghari M. “Quality of experience assessment of calling services in social network.” ICT Express 7(2) (2021): 158-161. doi: 10.1016/j.icte.2021.04.011

[3] Yevseiev S., Laptiev. O, Lazarenko S., Korchenko A., and Manzhul I. “Modeling the Protection of Personal Data from Trust and the Amount of Information on Social Networks” EUREKA: Physics and Engineering 1 (2021): 24-31, doi.10.21303/2461-4262.2021.001615

[4] S. Veretiuk, V. Pilinsky and I. Tkachuk, "Cognitive radio systems clustering," 2018 14th International Conference on Advanced Trends in Radioelecrtronics, Telecommunications and Computer Engineering (TCSET) (2018): 1091-1095, doi: 10.1109/TCSET.2018.8336384.

[5] B. Desmarchelier, F. Djellal, F.Gallouj, "Mapping social innovation networks: Knowledge intensive social services as systems builders." Technological Forecasting And Social Change 157 (2020): 120068. doi: 10.1016/j.techfore.2020.120068.

[6] Korobiichuk I., Snitsarenko P., Katsalap V., and Hryshchuk R. “Determination and Evaluation of Negative Informational and Psychological Influence on the Military Personnel Based on the Quantitative Measure.” Proceedings of the 1st International Workshop on Control, Optimisation and Analytical Processing of Social Networks 2392 (2019): 66-78.

[7] Molodetska K., Tymonin Yu., and Hryshchuk R. “Modelling Of Conflict Interaction of Virtual Communities in Social Networking Services on an Example of Anti-Vaccination Movement.” Proc. of the International Workshop on Conflict Management in Global Information Networks 2588 (2020): 250–264.

[8] K. Molodetska, Y. Tymonin, O. Markovets, and A. Melnychyn. “Phenomenological model of information operation in social networking services.” Indonesian Journal Of Electrical Engineering And Computer Science 19(2) (2020): 1078. doi: 10.11591/ijeecs.v19.i2.pp1078-1087

[9] Blokh, I., et al. “Psychological Warfare Analysis Using Network Science Approach.” Procedia Computer Science 80 (2016): 1856-1864. doi:10.1016/j.procs.2016.05.479

[10] Straub, J. "Mutual assured destruction in information, influence and cyber warfare: Comparing, contrasting and combining relevant scenarios." Technology In Society 59 (2019): 101177. doi: 10.1016/j.techsoc.2019.101177.

[11] Molodetska K., Solonnikov V., Voitko O., Humeniuk I., Matsko O., and Samchyshyn O. “Counteraction to information influence in social networking services by means of fuzzy logic system.” International Journal Of

Electrical And Computer Engineering 11(3) (2021): 2490. doi: 10.11591/ijece.v11i3.pp2490-2499

[12] K. Molodetska, "Counteraction to Strategic Manipulations on Actors' Decision Making in Social Networking Services," 2020 IEEE 2nd International Conference on Advanced Trends in Information Theory (ATIT) (2020) 266-269, doi: 10.1109/ATIT50783.2020.9349347.

[13] M. Castells, and G. Cardoso, eds., The Network Society: From Knowledge to Policy. Washington, DC: Johns Hopkins Center for Transatlantic Relations, 2005.

[14] C. Barrett, S. Eubank, and M. Marathe. Modeling and Simulation of Large Biological, Information and Socio-Technical Systems: An Interaction Based Approach. In: Goldin D., Smolka S.A., Wegner P. (eds) Interactive Computation. Springer, Berlin, Heidelberg (2006) doi:10.1007/3-540-34874-3_14

[15] X. Yuan, and H. Hwarng. "Managing a service system with social interactions: Stability and chaos." Computers & Industrial Engineering 63(4) (2012): 1178-1188. doi: 10.1016/j.cie.2012.06.022

[16] A. A. Kolesnikov. Sinergeticheskoe metody upravlenija slozhnymi sistemami: teorija sistemnogo sinteza. Editorial URSS, Moskow (2005) (in Russian).

[17] D. Maris, and D. Goussis. "The "hidden" dynamics of the Rössler attractor." Physica D: Nonlinear Phenomena 295-296 (2015): 66-90. doi: 10.1016/j.physd.2014.12.010

[18] J. Contreras-Reyes. "Chaotic systems with asymmetric heavy-tailed noise: Application to 3D attractors." Chaos, Solitons & Fractals 145 (2021): 110820. doi: 10.1016/j.chaos.2021.110820

[19] S. Li, and Ge, Z. (2009) "A novel study of parity and attractor in the time reversed Lorentz system." Physics Letters A 373(44): 4053-4059.

[20] R. Barrio, F. Blesa, and S. Serrano. "Qualitative analysis of the Rössler equations: Bifurcations of limit cycles and chaotic attractors." Physica D: Nonlinear Phenomena 238(13) (2009): 1087-1100. doi: 10.1016/j.physd.2009.03.010.

[21] R. Alstrom, S. Moreau, P. Marzocca, and E. Bollt. "Nonlinear characterization of a Rossler system under periodic closed-loop control via time-frequency and bispectral analysis." Mechanical Systems And Signal Processing 99 (2018): 567-585. doi: 10.1016/j.ymssp.2017.06.001

[22] A. Lyapunov. Collected Works. Moscow-L., Publishing house of the Academy of Sciences of the USSR, 1956 (in Russian).

[23] D. M. Vavriv, and V. B. Ryabov. "Current Lyapunov exponents and conditions of chaos." J. Comput. Math. and Math. Phys. 32 (9) (1992): 1409-1421 (in Russian).

[24] K. Hung, Y. Suen, and S. Wang. "Structures and evolution of bifurcation diagrams for a one-dimensional diffusive generalized logistic problem with constant yield harvesting." Journal Of Differential Equations 269(4) (2020): 3456-3488. doi: 10.1016/j.jde.2020.03.001

[25] W. Abou-Jaoudé, and P. Monteiro. "On logical bifurcation diagrams." Journal Of Theoretical Biology 466 (2019): 39-63. doi: 10.1016/j.jtbi.2019.01.008

[26] X. Chen, and H. Chen. "Complete bifurcation diagram and global phase portraits of Liénard differential equations of degree four." Journal Of Mathematical Analysis And Applications 485(2) (2020): 123802. doi: 10.1016/j.jmaa.2019.123802

[27] Ph. K. Janert. Section 13.2.2 Kernel density estimates. In: Gnuplot in action: understanding data with graphs. Connecticut, USA: Manning Publications, 2009.

[28] P. Cincotta, C. Giordano, R. Alves Silva, and C. Beaugé. "The Shannon entropy: An efficient indicator of dynamical stability." Physica D: Nonlinear Phenomena 417 (2021): 132816. doi: 10.1016/j.physd.2020.132816

[29] K. Molodetska, and Y. Tymonin. "System-dynamic models of destructive informational influence in social networking services." International Journal of 3D Printing Technologies and Digital Industry 3(2) (2019): 137–146.

[30] S. M. Veretyuk, and V. V. Pilinsky. "A model of the impact of innovation on a technical system. A New Approach to the Analysis of the Physical Meaning of the Gartner Curve." Electrotechnical and Computer Systems 26 (102) (2017): 121-130 (in Ukrainian).

Cyber Terrorism As An Object Of Modeling

Oleksandr Milov [1], Yevgen Melenti [2], Stanislav Milevskyi [3], Serhii Pohasii [4] and Serhii Yevseiev [5]

[1,3,4,5] *Simon Kuznets Kharkiv National University of Economics, Nauki ave., 9a, Kharkiv, 61166, Ukraine*
[2] *Juridical Personnel Training Institute for the Security Service of Ukraine Yaroslav Mudryi National Law University, Myronosytska str., 71, Kharkiv, 61002, Ukraine*

Abstract
The article examines issues related to the characteristics of cyber terrorism, as well as related concepts of terrorism and cyberspace. The definitions of these concepts are given. The types of cyber threats directly related to cyber terrorism are identified. The differences and similarities of the mentioned cyber threats are described. A structure that reflects the main features of cyber terrorism, which should be included in the model of cyber terrorism is presented.

Keywords
Cyber terrorism, cyber threats, hacktivism, cyber espionage, cyber war

1. Introduction

Advances in computer technology, coupled with the widespread availability of inexpensive, effective development tools and the availability of free knowledge on the Internet, have allowed cyber terrorists to improve their methods and conduct attacks remotely, damaging their intended targets. This opens up new opportunities for individuals and groups willing to engage in illegal activities to advance their shared goals, beliefs and agendas, invisible and often undetected through cyberspace, thereby creating new varieties of criminal threats. Generation of cyber terrorism; use of cyberspace to carry out activities classified as "terrorist". Cyber terrorists can launch attacks through cyberspace and the virtual world, uniting the physical world and cyberspace [1]. Connectivity has become a central element of government institutions, critical infrastructures (telecommunications networks, finance, transportation and emergency services), culture and education. [2] Many critical private, public, national and military infrastructures can be vulnerable to cyberattacks as they continue to rely on legacy traditional security solutions rather than comprehensive and sophisticated cyber defense [3]. Cybercrime, cyberterrorism, and cyberwarfare are all common topics in the cybersecurity field. Physical terrorism and cyber terrorism have some common elements and a common goal, namely terrorism. However, cyber terrorism remains a vague concept, and there is a lot of controversy around its precise definition, goals, risk factors, characteristics and preventive strategies [4]. Cybercrime and cyberterrorism are often used interchangeably, or the term "cybercrime" can be used to refer to cyberterrorism, thereby blurring the distinction between the two, especially for the general public. Cyberattacks are still considered one of the highest priority risks for national security around the world [5, 6].

2. Characteristics of terrorism and cyberterrorism

Despite the inherent advantages of information technology, dependence on information technology has made countries and societies far more vulnerable to cyberattacks such as computer intrusions, program encryption, undetected internal threats in network firewalls, or cyber terrorists. The decentralized nature of the Internet,

EMAIL: Oleksandr.Milov@hneu.net (A. 1);
melenty@ukr.net (A. 2); Stanislav.Milevskiy@hneu.net (A. 3);
spogasiy1978@gmail.com (A. 4);
Serhii.Yevseiev@hneu.net (A. 5)
ORCID: 0000-0001-6135-2120 (A. 1); 0000-0003-2955-2469 (A. 2); 0000-0001-5087-7036 (A. 3); 0000-0002-4540-3693 (A. 4); 0000-0003-1647-6444 (A. 5)

on the one hand, ensures the relative anonymity of users, and on the other, makes it insecure and ill-suited for tracking intruders or preventing their abuse by the internal openness of cyberspace [7].

Most researchers agree that a precise definition of cyber terrorism is needed, both for theoretical research and for the implementation of practical applications. At the same time, it is emphasized that this concept is multidisciplinary in nature, and should reflect the legal, economic, technological aspects of the problem. The definition should indicate the main characteristics or principles of the concept, as well as the range of real or potential scenarios to which the term cyber terrorism can be applied [8]. Defining cyber terrorism is even more difficult due to its abstract nature associated with understanding how certain incidents occur in cyberspace. Without a clear definition of the basic concepts, researchers cannot analyze the same sentences, therefore conceptualization is a necessary initial stage of research.

Since cyber terrorism is a combination of the terms "cyberspace" and "terrorism", it is important to clearly define these terms.

"Cyber" in cyber terrorism refers to cyberspace. It is a prefix that is commonly added to a number of subgroups dealing with issues in the cybersecurity discourse, including, but not limited to, cybercrime, cyberwar, cyber espionage, and of course cyber terrorism. Cyberspace, unlike terrorism, is an accepted term. It refers to the virtual world, including the Internet and other computer communications infrastructure, which consists entirely of computers, algorithms, computer networks and data. According to [9], a cyberattack is "a deliberate computer-to-computer attack that disrupts, disables, destroys, or takes over a computer system, or damages or steals the information it contains". While cyberattacks themselves take place in cyberspace, they can have repercussions in the physical world.

Unlike cyberspace, terrorism is a term for which there is no agreed definition. However, there are a number of similar aspects that are broadly agreed upon. [10] contains a definition and criteria for what constitutes terrorism:

«...the deliberate creation and exploitation of fear through violence or threat of violence in the pursuit of political change. All terrorist acts involve violence or the threat of violence. Terrorism is specifically designed to have far-reaching psychological effects beyond the immediate victim(s) or objects of the terrorist attack. It is meant to instill fear within, and thereby intimidate, a wider "target audience" that might include a rival ethnic or religious group, an entire country, a national government or political party, or public opinion in general. Terrorism is designed to create power where there is none or to consolidate power where there is very little. Through the publicity generated by their violence, terrorists seek to obtain the leverage, influence, and power they otherwise lack to effect political change on either a local or an international scale.»

In this way, terrorism is separated from other types of crime and irregular warfare (see Table 1). For a response, having a criterion to distinguish terrorists from other threats is of particular importance in cyberspace, where attribution can be particularly difficult.

Table 1

Characteristics of Terrorism

Number	**Characteristics**
1	Ineluctably political in aims and motives
2	Violent - or, equally important, threatens violence
3	Designed to have far-reaching psychological repercussions beyond the immediate victim or target
4	Conducted either by an organization with an identifiable chain of command or conspiratorial cell structure (whose members wear no uniform or identifying insignia) or by individuals or a small collection of individuals directly influenced, motivated, or inspired by the ideological aims or example of some existent terrorist movement and/or its leaders;
5	Perpetrated by a subnational group or non-state entity.

Source: [10].

Based on the definition of terrorism, a set of criteria for cyber terrorism can be formed (see Table 2).

Table 2
Characteristics of Cyberterrorism

Number	Characteristic
1	Executed via cyberspace
2	Ineluctably political or ideological in aims and motives
3	Violent or threatens violence
4	Designed to have far-reaching psychological repercussions beyond the immediate victim or target
5	Conducted either by an organization with an identifiable chain of command or conspiratorial cell structure (whose members wear no uniform or identifying insignia) or by individuals or a small collection of individuals directly influenced, motivated, or inspired by the ideological aims or example of some existent terrorist movement and/or its leaders
6	Perpetrated by a subnational group or non-state entity

Source: [10].

The term "cyber terrorism" was introduced in the 1980s. There is still no agreement in the international community as to what kind of cyber activity is cyber terrorism [11]. In [12-15] the following definition of cyber terrorism is given:

«*Cyberterrorism is the convergence of cyberspace and terrorism. It refers to unlawful attacks and threats of attacks against computers, networks and the information stored therein when done to intimidate or coerce a government or its people in furtherance of political or social objectives. Further, to qualify as cyberterrorism, an attack should result in violence against persons or property, or at least cause enough harm to generate fear. Attacks that lead to death or bodily injury, explosions, or severe economic loss would be examples. Serious attacks against critical infrastructures could be acts of cyberterrorism, depending on their impact. Attacks that disrupt nonessential services or that are mainly a costly nuisance would not.*»

Other definitions of cyber terrorism are rather derivatives of this basic one. For example [16]:

«Cyberterrorism is the convergence of terrorism and cyberspace. ... unlawful attacks and threats of attack against computers, networks, and the information… done to intimidate or coerce a government or its people in furtherance of political or social objectives...to qualify a cyberterrorism, an attack should result in violence against persons or property, or at least cause enough harm to generate fear».

3. Cyberterrorism and other Cyberspace Threats

The authors of the book [17] propose to consider all actions carried out by a terrorist cell or an individual via the Internet as cyber terrorism. The UN Office on Drugs and Crime has classified six ways the Internet is used for terrorist activities: propaganda (recruitment, radicalization and incitement); financing; preparation; planning (through secret communication and information from open sources); execution; and cyberattacks. Depending on the criminals involved and their motivation, cyber attacks can be classified into the types of cyber threats presented and defined in Table 3.

Table 3
Cyberspace Threats

N	Cyber Threats	Definition
1	Hacktivism	the emergence of popular political action, of the self-activity of groups of people, in cyberspace. It is a combination of grassroots political protest with computer hacking. Hacktivists operate within the fabric of cyberspace, struggling over what is technologically possible in virtual lives, and reaches out of cyberspace utilising virtual powers to mould offline life. Social movements and popular protest are integral parts of twenty-first-century societies. Hacktivism is activism gone electronic [18].

N	Cyber Threats	Definition
2	Cyberwarfare	actions by a nation-state to penetrate another nation's computers or networks for the purposes of causing damage or disruption [19]
3	Cybercrime	use of computers or other electronic devices via information systems to facilitate illegal behaviours [20]
4	Cyber-espionage	cyber espionage involves obtaining secret or classified information without permission from individuals, companies or governments for economic, political or military advantage using illicit means through the Internet, networks and/or computers, and can involve cracking or malicious software such as Trojan horses and spyware [21]
5	Chaotic Actors, Vigilantes	agents that have operated in cyberspace, such as criminals, hacktivists, industrial spies, nation states, terrorists, and insiders, there are also new challenging threats, such as chaotic actors, vigilantes, and regulators [22]

As shown in Table 4, there are a number of overlaps between cyberattacks that create a cyber threat, demonstrating confusion from the media and other actors who mislabel cyberattacks. For example, the distinction between hacktivism and other forms of cyber activity is especially important because acts of hacktivism have been flagged as cyber terrorism in a number of publications. While there is a definite difference between cyber terrorism and hacktivism, the purpose of the latter is not to maim, kill or intimidate; although the means to achieve the desired results may be similar. Consequently, "hacktivism does highlight the threat of cyber terrorism, the potential for people without moral constraints to use methods similar to those developed by hackers to wreak havoc."

Table 4
Other Cyber Threats v. Cyberterrorism

Cyberterrorism Criteria	Hacktivism	Cyberwarfare	Cybercrime	Cyberespionage	Chaotic Actors	Vigilantes	Cyberterrorism
Executed via cyberspace							
Ineluctably political or ideological in aims and motives	✓	✓	**X**	-	-	✓	✓
Violent or threatens violence	**X**	-	**X**	**X**	-	-	✓
Designed to have far- reaching psychological repercussions beyond the immediate victim or target	**X**	-	**X**	**X**	-	**X**	✓
Conducted either by an organization with an identifiable chain of command or conspiratorial cell structure (whose members wear no uniform or identifying insignia) or by individuals or a small collection of individuals directly influenced, motivated, or inspired by the ideological aims or example of some existent terrorist movement and/or its leaders	-	**X**	-	-	**X**	--	✓
Perpetrated by a subnational group or non-state entity.	✓	**X**	-	-	✓	✓	✓

Likewise, although cyber terrorism and cyber warfare are different, they have similarities; to attack computers, networks and information stored in them and cause damage in pursuit of political or ideological goals. In the case of cyber terrorism, its very nature must be violent and must be designed to be terrifying. While cyber war can lead to violence and have psychological consequences that go beyond the immediate victim or purpose, it can be argued that such effects are accidental and not necessary, as in the case of cyber terrorism. Consequently, cyber attacks by nation states cannot be considered acts of cyber terrorism. These distinctions between different cyber threats are important as they enable smarter countermeasures.

The structure reflecting the main objects and processes of cyber terrorism to be modeled is shown in Fig. 1. It consists of three main sections: Operating Forces, Techniques и Objectives.

Five forces are considered: characteristics, purpose / focus, types, capabilities and social factors. Each workforce, in turn, has a number of related subclauses. Operational forces provide the context in which cyber terrorism operates. Various high-level techniques are presented. These high-level techniques are supported by a variety of information gathering and computer and network security techniques. The objectives are similar to the motivation for standard terrorist activities, although there are some differences to show more pronounced intent.

4. Framework of Cyberterrorism

<table>
<tr><td rowspan="2">Operating Forces</td><td>Characteristics
Cheap
Anonymous
Varied
Enormous
Remote
Direct
Effect
Automated
Replicated
Fast</td><td rowspan="2">Target/Focus
Transportation
Utilities
Financial sector
Telecomms
Emergency Services
Government
Manufacturing</td><td>Types of Terrorism
Religious
New Age
Ethnonationalist Separatist
Revolutional
Far Right Extremist</td></tr>
<tr><td>Capabilities
Education
Training
Skill
Expertise
Financial support
Resources
Intelligence
Insider knowledge</td><td>Social Factors
Culture
Beliefs
Political Views
Upbringing
Personality Traits</td></tr>
<tr><td>Techniques</td><td>Practices
Deface web sites
Distribute disinformation
Spread propaganda DOS using worms and viruses
Disrupt crucial systems
Corrupt essential data
Steal credit card info for funds</td><td>Attack Levels
Simply Unstructured
Advanced Structured
Complex Co-ordinated</td><td>Modes of Operation
Perception
Management & Propoganda
Disruptive Attacks Destructive Attacks</td></tr>
</table>

Objectives	Malicious Goals	Support Functions
	Protest Disrupt Kill/Maim	Recruitment
	Terrify Intimidate	Training
	Meet demands	Intelligence
	Sensitive Info	Reconnaissance
	Affect crucial services	Planning
	Publicity Solicit money	Logistics
		Finance
		Propaganda
		Social Services

Figure 1: Framework of Cyberterrorism (Source: [23])

The framework's contribution is to organize the area of cyber terrorism and provide its context for analytical review and in-depth modeling. The operational forces describe the various benefits of using cyberterrorism, the intended systems to be attacked, and the terrorist's mindset. The "Techniques" section discusses the classification of attack tactics. The "Objectives" section discusses the immediate objectives of the attacker and also distinguishes between cyberterror activities and helper functions that can be used by computers and networks (which are often confused with cyberterrorism). This discussion helps to clarify important details regarding the functional thinking of cyber terrorists, as well as clarify which aspects of cybercrime and hacking will be used.

5. Conclusion

Cybercrime, regardless of how it is defined or classified, can have devastating consequences for computerized networks. Until a universally effective solution to this universal problem is found, the strength of a cybersecurity governance regime will depend on an information security management system that emphasizes a comprehensive cyber risk assessment that takes into account all possible threats to an organization's business, including internal and external threats. Modeling the technologies and processes for conducting cyberattacks, and not least the behavior of attackers, should lead to the construction of effective systems for ensuring the cybersecurity of critical infrastructures. The classification of cyber threats given in the article, the definition of cyber terrorism and its characteristics should focus the attention of the model developer on the processes and entities that should be reflected in the models of cyber terrorism in the first place.

6. References

[1] D. A. Simanjuntak, H. P. Ipung and C. lim, "Text Classification Techniques Used to Facilitate Cyber Terrorism Investigation," in Proceeding of Second International Conference on Advances in Computing, Control, and Tele-communication Technologies (ACT 2010), Jakarta, 2010

[2] Lord Jopling UK NATO General Rapporteur, "171 CDS 11 E rev. 1 final InformationS And National Security General Report," NATO Par l iamentary Assembly International Secretariat, Brussles, 2011

[3] M. A. A. &. C. E. Dogrul, "Developing an International Cooperation on Cyber Defense and Deterrence against Cyber Terrorism.," Tallinn, 2011

[4] DCSINT, "Handbook No. 1.02, Critical Infrastructure Threats and Terrorism," US Army Training and Doctrine Command, Fort Leavenworth, Kansas, 2006

[5] World Economic Forum, "Global Risks 2015 10th Edition," World Economic Forum , Geneva, 2015

[6] NATO, "173 DSCFC 09 E bis - NATO and Cyber Defence," NATO, Brussles, Belgium, 2009

[7] Lord Jopling UK NATO General Rapporteur, "171 CDS 11 E rev. 1 final Information And National Security General Report," NATO Parlamentary Assembly International Secretariat, Brussles, 2011

[8] L. Jarvis and S. Macdonald, "What Is Cyberterrorism? Findings From a Survey of Researchers," Terrorism and Political Violence, vol. 27, no. 4, pp. 657-678, (2015)

[9] Michael Kenney, “Cyber-Terrorism in a Post-Stuxnet World,” *Orbis* 59, no. 1 (2015): 112

[10] Bruce Hoffman, *Inside Terrorism: Revised and Expanded Edition* (New York: Columbia University Press, 2017), 40-41
[11] NATO, "171 CDS 11 E rev. 1 final - Information and National Security," 09 11 2011. [Online]. Available: http://www.nato-pa.int/default.asp?SHORTCUT=2589.
[12] D. Denning, "- Cyberterrorism‖, Testimony before the Special Oversight Panel of Terrorism Committee on Armed Services, US House of Representatives," 23 05 2000. [Online]. Available: https://pdfs.semanticscholar.org/7fdd/ae586b6d2167919 abba17eb90e5219b7835b.pdf
[13] Dorothy Denning, 2001. "Is Cyber Terror Next?" New York: U.S. Social Science Research Council, at http://www.ssrc.org/sept11/essays/denning.htm.
[14] Dorothy Denning, 2000b. "Cyberterrorism," *Global Dialogue* (Autumn), at http://www.cs.georgetown.edu/~denning/infosec/cyberterror-GD.doc.
[15] Dorothy Denning, 1999. "Activism, Hacktivism, and Cyberterrorism: The Internet as a Tool for Influencing Foreign Policy," Washington D.C.: Nautilus, at http://www.nautilus.org/info-policy/workshop/papers/denning.html.
[16] Gordon, S. & Ford, R. (2002) Cyberterrorism? *Computers & Security,* **21**(7): 636-647.
[17] UNoDC, "The Use Of The Internet For Terrorist Purposes," United Nations Office On Drugs And Crime, Vienna, 2012
[18] Paul Taylor and Tim Jordan, *Hacktivism and Cyberwars: Rebels with a Cause?* (New York: Routledge, 2004), 1, papers3://publication/uuid/50380B27-672A-4D1A-89C0-6FC517868773.
[19] Richard A. Clarke and Robert Knake, *Cyber War: The Next Threat to National Security and What To Do About It, Terrorism and Political Violence,* vol. 23 (New York: HarperCollins Publishers, 2012), 6.
[20] Samuel C. McQuade, *Understanding and Managing Cybercrime* (Boston: Pearson Education, 2006), 2.
[21] Khan, "States Rather than Criminals Pose a Greater Threat to Global Cyber Security: A Critical Analysis," 93.
[22] Tyson Macaulay, *RIoT Control: Understanding and Managing Risks and the Internet of Things* (Cambridge: Morgan Kaufmann, 2016), 228.
[23] Salih Tutun, Mohammad T. Khasawneh, Jun Zhuang. New framework that uses patterns and relations to understand terrorist behaviors // Expert Systems With Applications 78 (2017) 358–375.

Methodology For Environmental Monitoring With Use Of Methods Of Mathematical Modeling

Nadiia Bielikova [1], Daniil Shmatkov [2]

[1] *Research Centre for Industrial Problems of Development of the National Academy of Sciences of Ukraine, Inzhenerny lane, 1, A, Kharkiv, 61166, Ukraine,*
[2] *Scientific and Research Institute of Providing Legal Framework for the Innovative Development of the National Academy of Legal Sciences of Ukraine, Chernyshevskaya st., 80, Kharkiv, 61002, Ukraine,*

Abstract

The article is aimed at developing methodological support for environmental monitoring using modeling methods, which will optimize the number of studied indicators and facilitate the processing, interpretation and visualization of the results. Developed methodology envisages the following stages: formation of the initial set of partial indicators; factor analysis of partial indicators and reduction of those with a factor load of less than 60%; structuring a set of partial indicators (selection of components and calculation of integrated indicators); application of matrix analysis for grouping of monitoring objects.

Keywords

Environmental monitoring, sustainable development, modeling, factor analysis, integral indicator, partial indicators.

1. Introduction

Sustainable development involves the harmonization of development and functioning of environmental, economic, and social areas. The interaction between these areas is embodied in the formation of the outline of direct and indirect relation between the supervision and dynamics of their development and the results achieved. The problem of sustainable development is complex, as part of its solution it is advisable to monitor the economy, social area, and the state of the environment using methods that would take into account the complexity and difficult predictability of this process.

ICT play a significant role in the transformation of sustainable development approaches. Issues of organization and digitalization of monitoring the functioning of certain areas of sustainable development, of large amounts of information (variety baselines), of the complexity of their processing and interpretation of results, and of the formulation of conclusions require knowledge-intensive approaches.

This article is aimed at developing methodological support for environmental monitoring using modeling methods, which optimize the number of studied indicators and facilitate the processing, interpretation and visualization of the results.

2. Methodology

Ensuring environmental monitoring within the developed methodology envisages the following stages: formation of the initial set of partial indicators; factor analysis of partial indicators and reduction of those with a factor load of less than 60%; structuring a set of partial indicators (selection of components and calculation of integrated indicators); application of matrix analysis for grouping of monitoring objects.

As the initial set of monitoring indicators is large, in conditions of insufficient time it is advisable to use methods of data reduction [1]. One of such methods is the factor analysis which is widely applied in ecological science in various directions [2–5].

EMAIL: nadezdabelikova@gmail.com (A. 1);
d.shmatkov@gmail.com (A. 2).
ORCID: 0000-0002-5082-2905 (A. 1);
0000-0003-2952-4070 (A. 2).

Within the framework of the proposed approach, the first stage determines the number of factors that should be identified within the reduction of monitoring indicators. The initial set of partial indicators takes part in the analysis.

The essence of the analysis is that during the sequential selection of factors, they include less and less variability of monitoring indicators. Therefore, the decision on when to stop the procedure for the selection of factors depends largely on the analysis purposes, but one of the recommendations to streamline the process of selecting the number of factors is to consider the scree plot.

Next, it is proposed to structure the initial set of indicators for monitoring, which remained after the factor analysis. Structuring is done by identifying the components that will be followed by a generalized assessment of the environment. All selected components correspond to the main components of the living environment for monitoring of which the initial set was formed and which includes the following indicators:

I_A – integral indicator of the atmosphere assessment;

I_W – integral indicator of the water resources assessment;

I_S – integral indicator of the soil assessment;

I_{Ws} – integral indicator of the wastes assessment;

I_F – integral indicator of the forest resources assessment;

I_{NR} – integral indicator of the nature reserves and hunting grounds assessment.

To calculate the integrated components of the above indicators, it is proposed to use the entropy method [6], the stages of which (adapted to the objectives of the environmental monitoring) are the formation of a set of partial indicators and their assessment, standardization of partial indicators taking into account their impact on the environment, and calculation of the value of entropy of the environment features and integral indicators for estimation of its components.

This approach allows us to take into account that the greater the entropy of any partial indicator that characterizes a certain feature of any component of the environment, the more disordered the ecological system would be as a whole. If the entropy of the trait, expressed as a partial exponent, is insignificant, then its weight in the total set of traits is also insignificant [6]:

$$R(S_i) = \sum_{j=1}^{n} H_j b_{ij}, \quad i = \overline{1,m}, \tag{1}$$

where $R(S_i)$ – integral value of the object;
H_j – the entropy of j-th feature;
b_{ij} – quantitative assessment of j-th feature of i object;
m – number of objects;
n – number of features.

Matrix analysis is used in this work to visualize the results of monitoring which facilitates their interpretation and the possibility of obtaining homogeneous groups of objects of the study by positioning them in different quadrants of matrices. Having a group of objects in the study we can isolate their common characteristics. To do this, we offer three matrices or positioning planes:

- Atmosphere – Water resources ($I_A - I_W$).
- Soil – Wastes ($I_S - I_{Ws}$).
- Forest resources – Nature reserves and hunting grounds ($I_F - I_{NR}$).

Accordingly, the axes of these matrices are integrated indicators for assessing the six selected components of the environment.

To determine the boundaries of the quadrants of the matrices, the range of values of the integrated indicators for environment components estimation can be divided into three parts by the golden ratio. The golden ratio is such a proportional division of a segment into unequal parts in which the whole segment belongs to the larger part as much as the largest part belongs to the smaller one; or in other words, the smaller segment refers to the larger as the larger segment refers to all [7]:

$$\frac{YB}{AB} = \frac{AB}{YA} = \alpha, \tag{2}$$

where *YB, AB, YA* – parts of a segment or numerical series.

Depending on the defined conditions and features of research objects development, as well as properties and role which they carry out in a system, nine functions of distribution of the investigated sample are allocated: chaos, development of elements, development of properties, development of relations, balance of functions of development and preservation, preservation of relations, preservation of properties, preservation of elements, and collapse [7]. Environmental monitoring objects can be considered as systems with connections and elements. Since the development of this system is unbalanced, in certain periods of time it even

contains signs of chaos, the most suitable function to describe these processes can be defined as "development of elements" with the appropriate percentage distribution of parts of the range of values: [0,0; 0,328) – low, (0,329; 0,735) – medium level, (0,736; 1,0) – high level].

3. Results

At the first stage we formed an initial set of partial indicators for assessing the ecological sphere of sustainable development of the country – its environment.

The environment has the following main components that affect health and quality of life: air, water, soil, wastes, forests, nature reserves and hunting, etc. These components are reflected both in international indices that assess various aspects of habitat quality and in statistics to assess the development of regional environments. Based on this, it is proposed to monitor the environment using the following partial indicators (Table 1).

Table 1
Partial indicators for environmental monitoring

Symbol	Partial indicators
n.1	Emissions of carbon dioxide into the air from stationary sources of pollution, thousand tons
n.2	Emissions of pollutants into the air from stationary sources of pollution, thousand tons
n.3	Emissions of pollutants into the air from stationary sources of pollution per square kilometer, tons
n.4	Emissions of pollutants into the air from stationary sources of pollution per person kilometer, kg
n.5	Emissions of suspended solids into the atmosphere from stationary sources of pollution, thousand tons
n.6	Emissions of sulfur dioxide into the air from stationary sources of pollution, thousand tons
n.7	Emissions of nitrogen dioxide into the atmosphere from stationary sources of pollution, thousand tons
n.8	Emissions of carbon monoxide into the air from stationary sources of pollution, thousand tons
n.9	Emissions of non-methane volatile organic compounds into the atmosphere from stationary sources of pollution, thousand tons
n.10	Emissions of ammonia into the atmosphere from stationary sources of pollution, thousand tons
n.11	Emissions of methane into the air from stationary sources of pollution, thousand tons
n.12	Drawing of water from natural water objects, million m^3
n.13	Drawing of water from natural water objects per person, m^3
n.14	Water loss during transportation, million m^3
n.15	Use of fresh water, including fresh and sea water, million m^3
n.16	Use of fresh water, including fresh and sea water, used for the needs of the national economy and population, million m^3
n.17	Water saving drawing through the circulating and recycling water supply, million m^3
n.18	General drainage, million m^3
n.19	Discharge of return waters into surface water objects, million m^3
n.20	Discharge of contaminated return water into surface water objects, million m^3
n.21	Discharge of contaminated return water without purification into the surface water objects, million m^3
n.22	Discharge of insufficiently treated contaminated return water into surface water objects, million m^3
n.23	Discharge of normatively clean without treatment return water into surface water objects, million m^3
n.24	Wastewater treatment facilities, million m^3
n.25	Application of mineral fertilizers per hectare of acreage, kg
n.26	Application of organic fertilizers per hectare of acreage, tons
n.27	The area of crops fertilized with mineral fertilizers, thousand hectares

Symbol	Partial indicators
n.28	The area of crops fertilized with organic fertilizers, thousand hectares
n.29	Areas where pesticides were used, thousand hectares
n.30	Waste generation, thousand tons
n.31	Waste generation of I–III classes of danger, thousand tons
n.32	Waste generation per square kilometer, tons
n.33	Waste generation per capita, kg
n.34	Waste disposal, thousand tons
n.35	Utilization of wastes of I–III classes of danger, thousand tons
n.36	Waste incineration, thousand tons
n.37	Waste disposal in dedicated places and facilities, thousand tons
n.38	Removal of waste of I-III classes of danger in specially designated places and facilities, thousand tons
n.39	Waste disposal in fly-tipping, thousand tons
n.40	Total amount of waste accumulated during operation in waste disposal sites, thousand tons
n.41	Total amount of waste accumulated during operation in waste disposal sites per square kilometer, thousand tons
n.42	Total amount of waste accumulated during operation in waste disposal sites per person, thousand tons
n.43	Area of forest destruction, hectares
n.44	Number of forest fires, units
n.45	The area of forest lands covered by fires, hectare
n.46	Area of burned and damaged forest, m^3
n.47	Area of reforestation, hectares
n.48	Area of afforestation, hectares
n.49	Area of transfer of forest areas of natural regeneration into land covered with forest vegetation, hectares
n.50	Area of transfer of forest areas into land covered with forest vegetation, hectares
n.51	Number of illegal felling, units
n.52	Damage caused to forestry, millions of Ukrainian hryvnia
n.53	The area of hunting lands provided for use, thousand hectares
n.54	Land area of nature reserves, biosphere reserves and national nature parks, hectares
n.55	Number of wild animals (ungulates) by objects on the territory of which the lands are located, thousand heads
n.56	Number of wild animals (fur animals) by objects on the territory of which lands are located, thousand heads
n.57	Number of wild animals (game birds) by objects on the territory of which the lands are located, thousand heads

The composition of environmental monitoring objects may vary and depends on the objectives. In particular, it can be conducted at the global and national levels: for countries, regions, cities or other territories and settlements.

In this article, the objects of monitoring are defined as regions (administrative-territorial units) of Ukraine which have different characteristics of the environment due to different levels of industrial development, climate, geographical location, state of natural resources, and other factors.

Data collection of partial indicators for environmental monitoring in statistical sources allowed us to establish that the objects of monitoring have significant differences in the values of partial indicators n.1 – n.57. For example, the discrepancy between the maximum (233,7 thousand tons in the Donetsk region) and the minimum (0,2 thousand tons in the Transcarpathian region) values of sulfur dioxide emissions into the air was 1168,5 times (Table 2).

Table 2

Values of partial indicators for environmental monitoring, 2017 (fragment) [8]

The monitoring object	Values		
	n.5	n.6	n.7
Vinnytsia region	17,0	71,9	10,6
Volyn region	1,4	0,4	0,5
Dnipropetrovsk region	86,5	66,8	31,2
Donetsk region	76,2	233,7	44,8
Zhytomyr region	2,7	1,0	1,6
Transcarpathian region	0,4	0,2	0,7
Zaporizhya region	13,1	79	31,9
Ivano-Frankivsk region	37,3	129,6	14,5

The monitoring object	Values		
	n.5	n.6	n.7
Kyiv region	12,4	14,3	4,8
Kirovograd region	4,0	0,9	1,4
Luhansk region	10,4	33,3	8,1
Lviv region	8,4	39,8	6,8
Mykolayiv region	3,6	0,7	2,6
Odessa region	3,6	1,9	2,4
Poltava region	6,3	7,4	10
Rivne region	2,6	0,6	2,8
Sumy region	3,5	3,1	3,2
Ternopil region	1,5	0,3	1
Kharkiv region	6,5	11,3	7,8
Kherson region	1,2	0,7	0,3
Khmelnytsky region	2,8	2,5	5,3
Cherkasy region	8,8	5,0	10
Chernivtsi region	0,9	0,4	0,3
Chernihiv region	3,9	6,4	3,6

Consideration of the scree plot (Fig. 2) allows a researcher to determine the place where the decline in the eigenvalues of the factors from left to right is slowed down as much as possible. In this graph, this place corresponds to the number of factors equal to six. But the maximum variability of the initial indicators is explained by the first and second factors (Table 3).

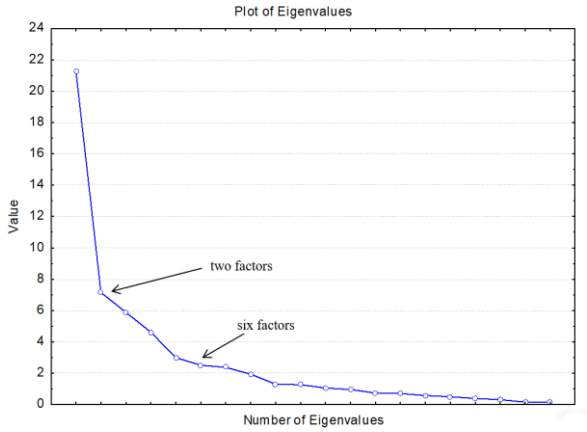


Figure 1: Graph of eigenvalues of environmental monitoring factors (scree plot)

Table 3

Eigenvalues of factors obtained by the principal components' method

Factor	Eigenvalue	% Total – variance	Cumulative – Eigenvalue	Cumulative – %
1	21,2	37,28	21,2	37,3
2	7,2	12,6	28,4	49,8
3	5,9	10,3	34,3	60,1
4	4,6	8,1	38,9	68,3
5	3,0	5,3	41,9	73,5
6	2,5	4,4	44,4	77,9

As can be seen from table 3, the first and second factors explain 49,83%, i.e. half of the variance of the initial indicators of environmental monitoring, and all six factors – 77,92% of the total variance. Therefore, in the process of factor analysis, it is possible to identify either two main factors (factor 1 and factor 2) and to reduce those indicators of environmental monitoring that are not included in their composition or to identify six factors and to reduce those indicators of environmental monitoring that are not included in their composition.

Leaving for analysis factors 1 and 2 and reducing the indicators of environmental monitoring which have a factor load of more than 60% and explain 49,83% of the total variance, the following results were obtained:

- Composition of factor 1 "Dangerous": n.1, n.2, n.3, n.4, n.5, n.6, n.7, n.8, n.11, n.18, n.19, n.20, n.21, n.22, n.24, n.33, n.34, n.35, n.37, n.40, n.41, n.42.
- Composition of factor 1 "Permissible": n.12, n.13, n.15, n.16, n.25, n.44, n.45, n.46, n.47, n.49, n.51, n.55, n.56.

Thus, factor 1 includes monitoring indicators that characterize the negative phenomena of the environment: emissions of hazardous substances into the atmosphere, different types of waste generation, etc. Given the composition of the indicators that fall into factor 1, it can be called "Dangerous" because it has a negative impact on the environment.

Factor 2 includes monitoring indicators that characterize less dangerous phenomena: water intake and its use for various purposes, application of mineral fertilizers to soil, etc. Given the composition of the indicators of factor 2, it can be conditionally called "Permissible" because it has a permissible and, in some cases, positive impact on the environment.

According to the criterion of factor load less than 60%, the following indicators were reduced: n.9., N.10, n.14, n.17, n.23, n.26, n.27, n.28, n.29, n.31, n.32, n.36, n.38, n.39, n.43, n.48, n.50, n.52, n.53, n.54, n.57.

The six selected factors include indicators that characterize areas of environmental monitoring such as air and water pollution by various types of hazardous substances (factor 1 and factor 3); wastes management (factor 3); use of natural resources for different purposes (factor 2); restoration of forest resources (factor 4); soil management (factor 5); loss of forest stands (factor 6).

Factors 1–3 were the largest in terms of the number of included indicators, and only one indicator was included in factor 6, which corresponds to the general rule of factor analysis – reduction of the number of indicators included in each subsequent selected factor due to reduced variability of indicators.

The analysis allowed us to conclude that the minimum number of factors that can be identified is two factors, and the maximum is six factors. And in addition, the logic of this study allowed us to recommend the second option of factor analysis according to which there are six factors influencing the environment which explain the maximum indicators variability.

Thus, as a result of the reduction, the initial set of environmental monitoring indicators was reduced from 57 to 45.

After calculating the entropy of integrated indicators that characterize the state of the selected components of the environment (Fig. 1), we carried out the positioning of monitoring objects in three matrices, for example, the matrix "Soil–Wastes" is presented in Fig. 2.

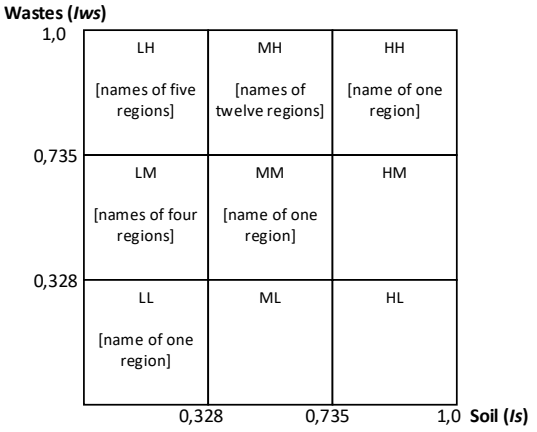


Figure 2: Positioning of monitoring objects in the matrix "Soil–Wastes"

Characteristics of matrix quadrants are the following:

HH – high assessment of soil – high level of wastes management;

HM – high assessment of soil – medium level of wastes management;

HL – high assessment of soil – low level of wastes management;

MH – medium assessment of soil – high level of wastes management;

MM – medium assessment of soil – medium level of wastes management;

ML – medium assessment of soil – low level of wastes management;

LH – low assessment of soils – high level of wastes management;

LM – low assessment of soil – medium level of wastes management;

LL – low assessment of soil – low level of wastes management.

Coordinates of positioning points in the matrix are the following: Ukraine (0,371; 0,735); Vinnytsia region (0,134; 0,773); Volyn region (0,623; 0,775); Dnipropetrovsk region (0,144; 0,234); Donetsk region (0,384; 0,710); Zhytomyr region (0,462; 0,777); Transcarpathian region (0,707; 0,776); Zaporizhzhya region (0,109; 0,761); Ivano-Frankivsk region (0,671; 0,769); Kyiv region (0,574; 0,772); Kirovograd region (0,072; 0,639); Luhansk region (0,392; 0,769); Lviv region (0,571; 0,764); Mykolayiv region (0,241; 0,762); Odessa region (0,072; 0,775); Poltava region (0,321; 0,686); Rivne region (0,710; 0,775); Sumy region (0,215; 0,738); Ternopil (0,469; 0,776); Kharkiv (0,070; 0,740); Kherson region (0,352; 0,761); Khmelnytsky region (0,354; 0,774); Cherkasy region (0,362; 0,776); Chernivtsi region (0,658; 0,777); Chernihiv region (0,230; 0,775).

The quadrants that are on the line of development of monitoring objects from the worst to the best condition are Dnipropetrovsk, Donetsk, and Rivne regions.

4. Conclusions

The given methodology for environmental monitoring with use of methods of mathematical modeling allows a researcher to draw conclusions with regard to a habitat condition as a whole in the country, to define the most dangerous state of ecology according to its administrative units, and to analyze results of an environment condition assessment according to its components.

The proposed methodology support provides the implementation of the complex approach to the establishment of monitoring of an ecological

component of sustainable development and to strengthen its scientific substantiation. Its advantage is the ease and high implementation opportunities through ICT tools to reduce the time of monitoring and systematic analysis for clear conclusions and recommendations for more effective implementation of the concept of sustainable development.

5. References

[1] D. Shmatkov, N. Bielikova, N. Antonenko, O. Shelkovyj, Developing an environmental monitoring program based on the principles of didactic reduction, European Journal of Geography, volume 10, number 1, 2019, 99–116.

[2] A. Deraemaeker, K. Worden, A comparison of linear approaches to filter out environmental effects in structural health monitoring, Mechanical systems and signal processing, volume 105, 2018, 1–15. https://doi.org/10.1016/j.ymssp.2017.11.045

[3] M. S. Guerreiro, I. M. Abreu, Á. Monteiro, T. Jesus, A. Fonseca, Considerations on the monitoring of water quality in urban streams: a case study in Portugal, Environmental monitoring and assessment, volume 192, 2020, 1–11. https://doi.org/10.1007/s10661-020-8245-y

[4] A. H. Hirzel, J. Hausser, D. Chessel, N. Perrin, Ecological-niche factor analysis: how to compute habitat-suitability maps without absence data?, Ecology, volume 83, number 7, 2002, 2027–2036.

[5] O. Ovaskainen, G. Tikhonov, A. Norberg, F. Guillaume Blanchet, L. Duan, D. Dunson, T. Roslin, N. Abrego, How to make more out of community data? A conceptual framework and its implementation as models and software, Ecology letters, volume 20, issue 5, 2017, 561–576. https://doi.org/10.1111/ele.12757

[6] V. Y. Vasylev, V. V. Krasylnykov, S. Y. Plaksyi, T. N. Tiahunova, Statistical analysis of multidimensional objects of arbitrary nature, Moscow, YKAR, 2004.

[7] N. N. Moiseev, E. P. Ivanilov, E. M. Stolyarova, Optimization methods, Moscow, The science, 1978.

[8] O. M. Prokopenko (Ed.) Statistical data Environment of Ukraine for 2017, Kyiv, State Statistics Service of Ukraine, 2018.

Spectral Model of the Encryption Key for a Symmetric Cryptosystem Based on Differential Transformations

Olha Hryshchuk [1]

[1] *Korolyov Zhytomyr Military Institute, 22 Mira Avenue, Zhytomyr, 10004, Ukraine*

Abstract

In the transition and post-quantum periods, the problem of cybersecurity is significantly aggravated. The potential compromise of the best symmetric (AES-256) and asymmetric (RSA-240) cryptosystems when an attacker uses quantum computers puts forward a number of security requirements for such systems. Today, a number of approaches are used to solve the problem of increasing cryptographic strength. Classic, which boils down to solving the problem of distributing encryption keys and new, the essence of which is to create promising cryptosystems based on new mathematical principles. The latter approach is based on cognitive cryptography, dynamic chaos theory, constructive, quantum and post-quantum cryptography, DNA algorithms, proxy models of cryptosystems, attribute-based cryptosystems, batch and non-commutative cryptography. The greatest interest from the point of view of security today is integrated cryptography. Thus, in previous works on this topic, it was proposed to create a symmetric cryptosystem based on differential transformations. The principle of functioning of this cryptosystem does not differ from the principles of functioning of classical symmetric cryptosystems. The only difference is that a symmetric cryptosystem based on differential transformations is based on the Fredholm integral equation of the first kind, the encryption key for which is its core. Special requirements for choosing an encryption key for a symmetric cryptosystem based on differential transformations are the requirements regarding its continuity, innate and symmetric. Following these requirements, the article offers a spectral model of the encryption key for the corresponding cryptosystem, which is built on the basis of differential transformations of Academician of the National Academy of Sciences of Ukraine G. E. Pukhov. It is shown that the spectral model of the encryption key for a symmetric cryptosystem on differential transformations is the sum of discret differential spectra for different values of the integer argument. Representation of the encryption key in the form of a spectral model makes it possible to implement encryption and decryption procedures by a symmetric cryptosystem using differential transformations in real time in the future.

Keywords

Encryption key, spectral model, symmetric cryptosystem, differential transformations, cybersecurity, image, T-spectrum, discrete, numeric argument, Fredholm integral equation of the first kind.

1. Introduction

Cybersecurity has now become a cornerstone on the agenda for many countries around the world. The computerization of all spheres of state and civil society activities, as well as the mass access of citizens to information technologies, threatens their use for illegal and terrorist purposes. It is possible that the fact of carrying out a cyberattack by one state against another can be regarded as the beginning of aggression from cyberspace. That is why in the world and Ukraine, scientist's eyes are increasingly focused on cybersecurity issues.

Based on the assessment of the current state of Science and technology, it becomes obvious that in the next 10 years there will be a breakthrough in the use of quantum computers for solving cybersecurity problems [1]. The most pessimistic predictions show that quantum cryptanalysis based on Grover's algorithm will halve the stability of all symmetric cryptographic mechanisms [2–4]. Plans to create a 100-qubit quantum computer by 2024 significantly exacerbate this problem [5, 6].

EMAIL: Ol.Hry@i.ua
ORCID: 0000-0001-6957-4748

2. The Latest Studies and Printed Works Analysis

Analysis of recent studies and publications [1, 8–11] and others has shown that a number of new approaches to ensuring the cryptographic stability of symmetric cryptosystems are currently known. In the transition and post-quantum period, the approaches described in [1, 8–13] will also be relevant.

At the same time, there are other alternatives to the established classical approaches. In particular, general approaches to creating a new class of cryptosystems are described in [14, 15], but specific cryptographic mechanisms for their implementation are not given.

In [16], the idea of creating symmetric cryptosystems based on the Fredholm integral equation of the first kind was developed, and in [17] the requirements for choosing an encryption key were formalized. However, the key generation mechanism and its spectral model are not given.

3. Purpose

The purpose of this article is to develop a mechanism for generating an encryption key for a symmetric cryptosystem based on differential transformations and obtain its spectral model.

4. Concept presentation

Based on [18], the encryption key $K(x,s)$ is the core of the Fredholm integral equation of the first kind [16, 17]

$$\int_a^b K(x,s)\, z(s)\, ds = u(x), a \le x, s \le b,$$

where $z(s)$ – plaintext;

$u(x)$ – cipher.

There are many special features for choosing an encryption key for the Fredholm cryptosystem, which can be applied to the function of the initial wiggle [19]

$$K(x,s) = \sum_{l=1}^{m} g_l(x) q_l(s). \qquad (1)$$

To obtain an analytical spectral model of the encryption key (1), we will use differential transformations of Academician of the National Academy of Sciences of Ukraine G. E. Pukhov [20–23], the use of which for solving cybersecurity problems was first described in the monograph [24].

According to [20–23], differential transformations are transformations of the form

$$X(k) = \underline{x}(k) = \frac{H^k}{k!}\left[\frac{d^k x(t)}{dt^k}\right]_{t=0} \doteq \doteq x(t) = \sum_{k=0}^{k=\infty}\left(\frac{t}{H}\right)^k X(k), \qquad (2)$$

where $x(t)$ – the original, which is a continuous, differentiable infinite number of times and bounded together with all its derivatives, function of a real argument t;

$X(k)$ and $\underline{x}(k)$ equivalent notation of the differential image of the original representing a discrete (lattice) function of an integer argument $k =: 0, 1, 2, \ldots$;

H – a scale steel that has the dimension of an argument t and is often chosen equal to the segment $0 \le t \le H$ on which the function is considered $x(t)$;

$\doteq$ – a symbol of correspondence between the original $x(t)$ and its differential image $X(k) = \underline{x}(k)$.

To the left of the symbol $\doteq$ is a direct transformation that allows you to find the image $X(k)$ behind the original $x(t)$, and to the right is a reverse transformation that allows you to get the original behind the image in the form of a power series, which is nothing more than an otherwise written Taylor series centered at a point $t = 0$.

Differential images $X(k)$ are called differential T-spectrum, and the values of the T-function $X(k)$ for specific argument k values are called samples.

Using the direct transformation (2) and the general property of the product of functions in the image domain for differential transformations [20–23] for expression (1), we obtain

$$K(x,s) \div K(x,k) \Rightarrow$$
$$\Rightarrow \sum_{l=1}^{m} g_l(x) q_l(s) \div \sum_{l=1}^{m} g_l(x) Q_l(k), \quad (3)$$

where $g_l(x)$ – constant;

$Q_l(k)$ – original image $q_l(s)$, $Q_l(k) = \frac{H_l{}^k}{k!}\left[\frac{d^k q(s)}{ds^k}\right]_{s=0}$.

Let the function $q_l(s)$ belong to a class of power functions, i.e. $q_l(s) = s_l{}^n$.

Then, according to [20–23], its image from the general form $Q_l(k) = \frac{H_l{}^k}{k!}\left[\frac{d^k q(s)}{ds^k}\right]_{s=0}$ will be reduced to an expression

$$Q_l(k) = H_l{}^n \mathfrak{b}(k-n) = \begin{cases} H_l{}^n, k = n, \\ 0, \quad k \neq n. \end{cases}$$

Taking this into account, the right-hand side of expression (3) will have the form

$$K(x,k) = \sum_{l=1}^{m} g_l(x) H_l{}^n \mathfrak{b}(k-n), \quad (4)$$

where $\mathfrak{b}(k-n)$ – displaced "teda", $\mathfrak{b}(k-n) = \begin{cases} 1, k = n, \\ 0, k \neq n. \end{cases}$

We find in general the differential spectra for model (4), substituting sequentially the values of the integer argument $k =: 0, 1, 2, 3$. If, for example $n = 2$, we have:

for $k =: 0$

$$K(x,0) = \sum_{l=1}^{m} g_l(x) H_l{}^2 \mathfrak{b}(0-2) = 0; \quad (5)$$

for $k =: 1$

$$K(x,1) = \sum_{l=1}^{m} g_l(x) H_l{}^2 \mathfrak{b}(1-2) = 0; \quad (6)$$

for $k =: 2$

$$K(x,2) = \sum_{l=1}^{m} g_l(x) H_l{}^2 \mathfrak{b}(2-2) = \sum_{l=1}^{m} g_l(x) H_l{}^2; \quad (7)$$

for $k \geq 3$

$$K(x,k \geq 3) = \sum_{l=1}^{m} g_l(x) H_l{}^2 \mathfrak{b}(3-2) = 0. \quad (8)$$

Thus, the spectral model of the encryption key $K(x,k)$ for a symmetric cryptosystem on differential transformations in general form in the image domain under the accepted conditions is the sum of the discretits found (5)–(8), i.e.

$$K(x,k) = \sum_{l=1}^{m} g_l(x) H_l{}^2. \quad (9)$$

We give examples of constructing a spectral model of the encryption key for a symmetric cryptosystem based on differential transformations based on the initial data given in [25]. So according to [25] the encryption key $K(x,s) = xs$. Then expression (4) is simplified and takes the form

$$K(x,k) = xH\mathfrak{b}(k-1). \quad (10)$$

Changing the value of the integer argument $k =: 0, 1, 2, \ldots$ by analogy with expressions (5)–(8), we obtain the differential spectrum discretits for the desired spectral model.

For $k =: 0$

$$K(x,0) = 0; \quad (11)$$

for $k =: 1$

$$K(x,1) = xH; \quad (12)$$

for $k \geq 2$

$$K(x,k \geq 2) = 0. \quad (13)$$

So, for the example given in [25], taking into account the discrete found (11)–(13), the desired spectral model of the encryption key (4) is determined by the expression

$$K(x,k) = xH\ ,\ m = l\ .$$

We present a graph of the functions of the encryption key (fig. 1 a) and its T-spectrum (fig. 1 b) for the found model (10).

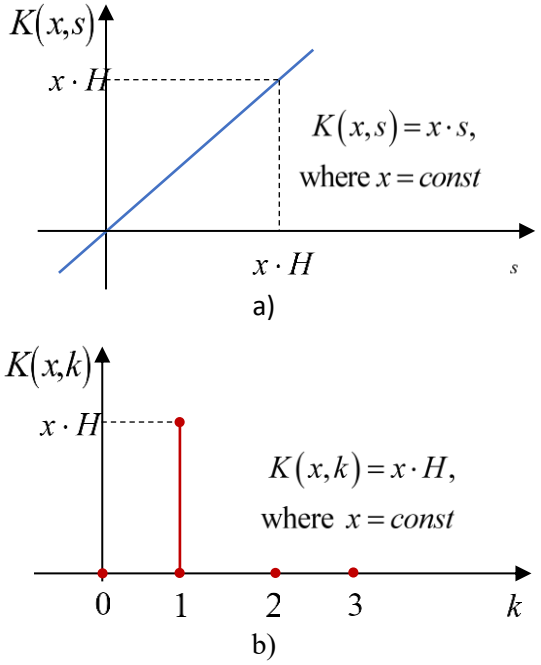


Figure 1: Encryption key function-original (a) and its differential T-spectrum (b) – image

5. Conclusions

In this paper, a mathematical model of the encryption key for a symmetric cryptosystem based on differential transformations is proposed for the first time. The resulting spectral model in the image domain is the sum of discretits for specific argument k values. The model meets the requirements put forward in [19], and its convergence with the results of known studies [25] confirms its adequacy.

The direction of further research will be the formation of a set of possible keys for a symmetric cryptosystem based on differential transformations and obtaining their Spectral models. The main purpose of the resulting model is its use in a symmetric cryptosystem on differential transformations during encryption and decryption in voice message transmission systems (VoIP-traffic).

6. Acknowledgements

I would like to express my gratitude to the staff of the research department of the scientific center of the Korolyov Zhytomyr Military Institute for their support and valuable comments, taking into account which helped to improve the quality of the presentation of the work.

7. References

[1] R. Hryshchuk, Yu. Danik. Osnovy kibernetychnoi bezpeky, (in Ukrainian). Zhytomyr National Agroecological University, Zhytomyr, Ukraine (2016).

[2] I. Hrabar, R. Hryshchuk, K. Molodetska. Bezpekova synerhetyka: kibernetychnyi ta informatsiinyi aspekty, (in Ukrainian). Zhytomyr National Agroecological University, (2019).

[3] B. G. Markaida, X. Larrucea, M. G. Romay Quantum and post-quantum cryptography and cybersecurity: A systematic mapping: Investigación en Ciberseguridad Actas de las VI Jornadas Nacionales (JNIC2021 LIVE) Online 9-10 de junio de 2021 Universidad de Castilla-La Mancha, 2021, pp. 237–244.

[4] K. Kan, M. Une. Recent Trends on Research and Development of Quantum Computers and Standardization of Post-Quantum Cryptography. IMES Discussion Paper Series 21-E-05, Institute for Monetary and Economic Studies, Bank of Japan, No. 2021-E-5, 2021, pp. 1–41.

[5] K. Babber, J. P. Singh. Quantum cryptography and security analysis, Journal of Discrete Mathematical Sciences and Cryptography, 2021, DOI: 10.1080/09720529.2019.1692452.

[6] J.-F. Biasse, B. Pring. A framework for reducing the overhead of the quantum oracle for use with Grover's algorithm with applications to cryptanalysis of SIKE, J. Math. Cryptol. 2021, pp. 143–156, DOI.ORG/10.1515/jmc-2020-0080.

[7] J. Preskill. Quantum computing: Current status and future prospects. Bulletin of the American Physical Society 65 (2020).

[8] Russia sets up lab to create quantum computer [Electronic resource] // huaxia. – 2020. – Resource access mode: http://www.xinhuanet.com/english/2020-11/25/c_139542572.htm.

[9] S. Mitra, B. Jana, S. Bhattacharya, P. Pal, J. Poray. Quantum cryptography: Overview, security issues and future challenges," 2017 4th International Conference on Opto-Electronics and Applied Optics (Optronix), 2017, pp. 1–7, DOI: 10.1109/OPTRONIX.2017.8350006.

[10] A. Ejaz, I. A. Shoukat, U. Iqbal, A. Rauf, A. Kanwal 2021. A secure key dependent dynamic substitution method for symmetric cryptosystems. PeerJ Comput. Sci. 7:e587 DOI 10.7717/peerj-cs.587.

[11] L. Julakidze, Z. Kochladze, T. Kaishauri. New Symmetric Tweakable Block Cipher Bulletin of the Georgian National Academy of Sciences, vol. 15, no. 1, 2021, pp. 13–19.

[12] B. M. Alshammari, R. Guesmi, T. Guesmi, H. Alsaif, A. Alzamil. Implementing a Symmetric Lightweight Cryptosystem in Highly Constrained IoT Devices by Using a Chaotic S-Box. Symmetry 2021, 13, 129. https://doi.org/10.3390/sym13010129.

[13] E. Hernandez-Diaz, H. Perez-Meana, V. Silva-Garcia. Encryption of RGB Images by Means of a Novel Cryptosystem Using Elliptic Curves and Chaos IEEE Latin America Transactions, Vol. 18, NO. 8, August 2020, pp. 1407–14015.

[14] I. Gorbenko, V. Ponomar. Investigation of the possibility of using and the advantages of post-quantum algorithms depending on the conditions of use // Eastern-European Journal of Advanced Technologies. 2017.Vol. 2.No. 9 (86). S. 21–32.

[15] Symmetric block cipher "Kalina" - a new national encryption standard of Ukraine / I. D. Gorbenko et al. // Radio engineering: All-Ukrainian interdepartmental scientific and technical collection - 2015. - Issue. 181. - S. 5 - 22.

[16] G. Bronshpak, I. Gromiko, S. Docenko and E. Perchik, "Kriptografiya novogo pokoleniya Integralnie uravneniya kak alternativa algebraicheskoi metodologiyi", [New generation cryptography: Integral equations as an alternative to algebraic methodology], Prikladnaya elektronika, № 3, pp. 337-349, 2014. DOI: 10.13140/RG.2.1.1973.2645. (In Ukrainian).

[17] I. Gromiko, «Obschaya paradigma zaschiti informacii_ problemi zaschiti informacii v aspektah matematicheskogo modelirovaniya: monografiya», [The general paradigm of information security: problems of information security in aspects of mathematical modeling: a monograph], Harkiv: HNU imeni V.N. Karazina, 2014, p. 216. (In Ukrainian).

[18] R. V. Hryshchuk, O. M. Hryshchuk. A Generalized Model of Fredholm's Cryptosystem. Cybersecurity: education, science, technique, 2019, Vol. 4 (4), pp. 14–23. DOI: 10.28925/2663-4023.2019.4.1423. (In Ukrainian).

[19] O. M. Hryshchuk. Features of the encryption key selection for the Fredholm cryptosystem. Computer Engineering and Cybersecurity: Achievement and Innovation: Materials II All-Ukrainian. nauk.-practical. conf. zdobuvachiv vishoï educate th young pupils, metro Kropyvnytskyi, 25-27 leaf. 2020 p. / Ministry of Education and Science of Ukraine, the State of Science established the “Institute of Modernization for Science of Science”, Central Ukrainian National Technical University; - Kropyvnytskyi: TsNTU, 2020. P. 109-110 p.

[20] G. E. Pukhov, Computational structure for solving differential equations by Taylor transformations, Cybern. Syst. Anal. 14 (1978) 383.

[21] G. E. Pukhov, Expansion formulas for differential transforms, Cybern. Syst. Anal. 17 (1981) 460.

[22] G. E. Pukhov, Differential transforms and circuit theory, Int. J. Circ. Theor. App. 10 (1982) 265. [4] G. E. Pukhov, Differential transforms of functions and equations, in Russian, Naukova Dumka, Kiev, 1980.

[23] G. E. Pukhov, Differential transformations and mathematical modeling of physical processes, in Russian, Naukova Dumka, Kiev, 1986.

[24] R.V. Hryshchuk Theoretical foundations of modeling the processes of attacking information by methods of theories of differential igors and differential revision: monograph / R.V. Grishchuk. - Zhitomir: Ruta, 2010 . - 280 p.

[25] A. M. Wazwaz. The Regularization Method for Fredholm Integral Equations of the First Kind. Comput. Math. Appl. 2011, 61, 2981–2986.

Example of Differential Transformations Application in Cybersecurity

Ruslan Hryshchuk [1]

[1] *Korolyov Zhytomyr Military Institute, 22 Mira Avenue, Zhytomyr, 10004, Ukraine*

Abstract

Cybersecurity as a relatively new science covers quite a large number of areas, most of which are still in their infancy. The basis of cybersecurity, like any exact science, is mathematics. But the non-stationary and at the same time nonlinear nature of phenomena and processes occurring in cyberspace places special requirements on the mathematical tools used in cybersecurity. On the one hand, it should be adapted as much as possible for solving specialized problems, on the other hand, such mathematical tools should describe the phenomena and processes that are being studied quite fully and adequately. Today, in the field of cybersecurity, mathematical tools based on set theories, graphs, logic, probabilities, etc. are widely used. A special place in this field today is given to data mining, simulation, situational and cognitive modeling, parametric and structural synthesis of information security systems. The article develops the idea of applying in the field of cybersecurity the well-known mathematical apparatus of differential transformations of Academician of the National Academy of Sciences of Ukraine G. Pukhov, which has already found wide application in other branches of science and technology-electronics, electrical engineering, mechanics, chemical technologies, space research, etc. For this purpose, examples of the use of differential transformations for constructing models of cyberattack patterns for attack detection systems, mathematical models for assessing the level of security of information and telecommunications systems from zero-day cyberattacks by security analysis systems, and for building new cryptographic systems are given. The prospects for applying differential transformations to study the processes of interaction in social networks, as an example of sociotechnical cybernetic systems, are shown.

Keywords

Cybersecurity, differential transformations, original, image, model, cyberattack pattern, security level, system of differential equations, graph model, differential game.

1. Introduction

Differential transformations of Academician of the National Academy of Sciences of Ukraine G. E. Pukhov [1] have now become an effective tool for studying nonlinear and non-stationary processes in many branches of Science and technology. One of the first applied applications of differential transformations was their use for solving electrical engineering problems [1]. Over time, differential transformations began to be used to solve problems in radio engineering [2], mechanics [3], heat engineering [4], optimal control [5], computer engineering [6], and Space Research [7]. Such a wide range of applications of differential transformations is due to their significant advantages over the known LaPlace, Fourier, Mellin, and Taylor-Cauchy integral transformations. The main advantage of differential transformations over the integral transformations mentioned above is the possibility of their application for the correct solution of nonlinear problems described by a fairly wide class of systems of Integral and differential equations [1].

In the field of cybersecurity, as is known [8], most of the phenomena and processes that occur in information security systems are non-stationary. Many of them can be described and are already described by systems of linear and nonlinear inhomogeneous differential equations. For example, today models of various malicious software samples such as SIS, SIR, SAIR, PSIDR, described by systems of differential equations, are widely known [8]. Some processes, such as the encryption process for a new type of symmetric cryptosystems, are described by Integral Equations [9].

EMAIL: Dr.Hry@i.ua
ORCID: 0000-0001-9985-8477

Therefore, given the prospects of differential transformations as a modern mathematical tool, it is considered appropriate to expand the scope of its application in the interests of Applied Solutions to cybersecurity problems.

2. The Latest Studies and Printed Works Analysis

For the first time, the use of differential transformations for solving cybersecurity problems was proposed in [10]. Their main purpose was to solve linear and nonlinear inhomogeneous systems of differential equations that describe the processes of attacking information in information security systems. During 2009-2010, the theoretical foundations of modeling the processes of attack on information and its protection based on differential transformations were developed. The result of the research was the publication of the corresponding monograph [11]. Over time, differential transformations found a place in the creation of symmetric cryptosystems [12] and began to be used to construct patterns of potentially dangerous cyber attacks [13]. There is still no unified vision of the role and place of differential transformation in the field of cybersecurity.

3. Purpose

The purpose of the article is to systematize the well-known areas of application of differential transformations of Academician of the National Academy of Sciences of Ukraine G. E. Pukhov in the field of cybersecurity and determine further promising ways of their implementation in this industry.

4. Concept presentation

The essence and content of differential transformations are described in the works of their author, for example in [1] and others. let's consider an example of their application for differential game modeling of cyberattack processes [10, 14].

Example. Let the change in cybersecurity States in a computer network be described by a graph model (fig. 1).

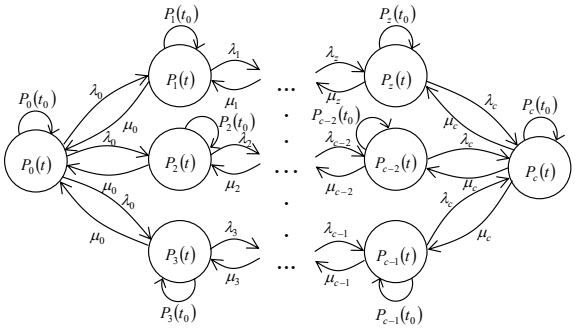


Figure 1: Cybersecurity state change graph model

In fig. 1 the following designations are accepted:

$\{P_z(t)\}$ – probabilities of a computer network being in one of the cybersecurity states $z = \overline{0,c}$ at some point in time t;

$\{P_z(t_0)\}$ – zero initial conditions when a computer network is in one of the cybersecurity states $z = \overline{0,c}$ at a time t_0;

$\{\lambda_z\}$ – intensity of recovery streams of infected hosts on the computer network, $z = \overline{0,c}$;

$\{\mu_z\}$ – intensity of streams infection of hosts in the computer network with malware, $z = \overline{0,c}$.

Circles on fig. 1 indicates the cybersecurity States in which the computer network may be located. Above the transition Arrows are the corresponding flow intensities that put the network in the corresponding states.

According to the above example (see fig. 1) it is necessary to build a differential game model of the cyberattack process on a computer network and assess its level of security under the accepted conditions.

Solving the example. Let's make a system of Kolmogorov-Chapman differential equations. The number of equations in a given system is determined by the number of states in which a computer network can be located (see fig. 1). The following general rule should be followed when compiling the system:

on the left side of each equation of the system is the derivative of the probability of a certain (z -th) state;

on the right - the sum of the products of the probabilities of all states from which the arrows enter this state, on the intensity of the corresponding information flows, minus the total intensity of all flows that bring the system out of this state, multiplied by the probability of this (z -th) state.

Based on the above rule we have

$$\begin{cases} \dfrac{dP_0(t)}{dt} = -3\lambda_0 P_0(t) + \mu_0\left(P_1(t) + \right. \\ \qquad \left. + P_2(t) + P_3(t)\right); \\ \dfrac{dP_2(t)}{dt} = -(\mu_0 + \lambda_1)P_1(t) + \\ \qquad \ldots + \lambda_0 P_0(t); \\ \qquad \vdots \\ \dfrac{dP_c(t)}{dt} = -3\mu_c P_0(t) + \lambda_c\left(P_z(t) + \right. \\ \qquad \left. + P_{c-2}(t) + P_{c-1}(t)\right). \end{cases} \quad (1)$$

Let us impose additional (initial) conditions on System (1) that will provide it with a single solution

$$P_0(t_0) = 1,\ P_2(t_0) = \ldots = P_c(t_0) = 0, \quad (2)$$

we will also define the rationing conditions

$$P_0(t_0) + P_2(t_0) + \ \ldots\ + P_c(t_0) = 1. \quad (3)$$

In the differential game setting [11], the intensity of flows $\{\lambda_z\}$ and $\{\mu_z\}$ are called strategies of players of cyber attack and cyber defense, respectively, and are limited in their boundaries

$$0 \le \lambda_z \le \lambda_{z\max}, \quad (4)$$

$$0 \le \mu_z \le \mu_{z\max}, \quad (5)$$

where $\lambda_{z\max}$ and $\mu_{z\max}$ – are the maximum flow intensities in the z-th state, respectively.

Using the method of differential transformations [1], we obtain a spectral model of cybersecurity states

$$\begin{cases} P_0(k+1) = \dfrac{T}{k+1}\left[-3\lambda_0 P_0(k) + \right. \\ \left. + \mu_0\left(P_1(k) + P_2(k) + P_3(k)\right)\right]; \\ P_1(k+1) = \dfrac{T}{k+1}\left[-(\mu_0 + \lambda_1)P_1(k) + \right. \\ \left. + \ldots + \lambda_0 P_0(k)\right]; \\ \qquad \vdots \\ P_c(k+1) = \dfrac{T}{k+1}\left[-3\mu_c P_0(k) + \right. \\ \left. + \lambda_c\left(P_z(k) + P_{c-2}(k) + P_{c-1}(k)\right)\right]. \end{cases} \quad (6)$$

When receiving the system (6), the condition is assumed that the constant H duration T of infection of the computer network with malware.

Assigning sequentially integer values to the argument $k =: 0, 1, \ldots$ according to the spectral Model (6), we find the discrete of differential spectra for the desired model $P_0(k+1)$, i.e.

$$P_0(0) = \left[P_0(t_0)\right] = 1\ ,\ P_0(1) = \ldots. \quad (7)$$

Let's find the best strategies for allocating players resources λ_z^{opt} i μ_z^{opt}, game price I^* (level of protection of the computer network from the malware) and, in fact, the model $P_0(t)$ itself, which is the trajectory of the game.

To do this, we will present the board I with a general integral model

$$I = \frac{1}{T}\int_{t_0}^{T} P_0(t)\,dt. \quad (8)$$

When players choose a minimax strategy

$$\min_{\lambda(t)\in E_\lambda}\ \max_{\mu(t)\in E_\mu} = I\left(t, P_0(t), \lambda(t), \mu(t)\right)$$

using a direct differential transformation [1], the fee (8) is defined in terms of differential spectrum discretion $P_0(k)$ (7) as

$$I = \sum_{k=0}^{k=\infty} \frac{P_0(k)}{k+1}. \quad (9)$$

To find optimal strategies λ_0^{opt} and μ_0^{opt} allocate available resources (4) and (5), we examine functionality I (9) for an extremum (expression (9) takes the form of a functional when the values of the corresponding discretes (7) are substituted for it).

The necessary conditions for the existence of the extremum of the functional $I(\lambda_0, \mu_0)$ (9) allow us to determine the optimal strategies of players:

$$\begin{cases} \dfrac{\partial I(\lambda_0, \mu_0)}{\partial \lambda_0} = 0; \\ \dfrac{\partial I(\lambda_0, \mu_0)}{\partial \mu_0} = 0. \end{cases} \rightarrow \begin{cases} \lambda_0^{opt}; \\ \mu_0^{opt}. \end{cases} \quad (10)$$

Sufficient conditions for the existence of the extremum of functional $I(\lambda_0, \mu_0)$ (9) allow us to determine the sign of the found extremums, i.e.

$$\begin{cases} \dfrac{\partial^2 I(\lambda_0, \mu_0)}{\partial \lambda_0^2} > 0; \\ \dfrac{\partial^2 I(\lambda_0, \mu_0)}{\partial \mu_0^2} < 0. \end{cases} \rightarrow \begin{cases} \lambda_{0\min}^{opt}; \\ \mu_{0\max}^{opt}. \end{cases} \quad (11)$$

Fulfilling the condition of existence saddle point Δ:

$$\Delta > 0, \quad (12)$$

where

$$\Delta = \left(\frac{\partial^2 I_1(\lambda_0, \mu_0)}{\partial \lambda_0 \, \partial \mu_0} \right)^2 - \left(\frac{\partial^2 I_1(\lambda_0, \mu_0)}{\partial {\lambda_0}^2} \right) \left(\frac{\partial^2 I_1(\lambda_0, \mu_0)}{\partial {\mu_0}^2} \right)$$

indicates that it is inappropriate for players to deviate from their optimal strategies (10), since any deviation from the optimal strategy by one of the players will inevitably lead to losses in the fee, provided that the optimal strategy is chosen by the other player, that is

$$I\left(t, P_0^{opt}(t), \lambda_0, \mu_{0\max}^{opt}\right) \geq$$
$$\geq \min_{\lambda \in E_\lambda} I\left(t, P_0(t), \lambda_0, \mu_{0\max}^{opt}\right),$$
$$I\left(t, P_0^{opt}(t), \lambda_{0\min}^{opt}, \mu_0\right) \leq$$
$$\leq \max_{\mu \in E_\mu} I\left(t, P_0(t), \lambda_{0\min}^{opt}, \mu_0\right).$$

So, if there is a saddle point Δ (12), then when players choose the optimal strategies (10), the price of the game – the level of protection of the computer network from the malware I^* is determined from the board (9).

When moving to the time domain using the inverse transformation [1], the trajectory of a differential game-a differential game model of the cyberattack process on a computer network $P_0^{opt}(t)$, provided that players choose optimal strategies (10), will have the form

$$P_0^{opt}(t) = \sum_{k=0}^{k=\infty} \left(\frac{t}{H} \right)^k P_0^{opt}(k). \quad (13)$$

In all other cases –

$$P_0(t) = \sum_{k=0}^{k=\infty} \left(\frac{t}{H} \right)^k P_0(k). \quad (14)$$

Thus, the given example shows the potential possibilities of using differential transformations in modeling cyberattack processes on computer systems and networks in the case of describing malicious software samples by systems of differential equations.

5. Conclusions

The article provides an overview of one of the examples of using differential transformations to solve cybersecurity problems. After analyzing other well-known examples of the use of differential transformations [15] in conclusion, we note that they can also be used to solve problems in cryptology.

6. Acknowledgements

Thanks to professors Vladimir Baranov, Vladimir Khoroshko and Alexander Korchenko

introduction to differential transformations and cybersecurity.

7. References

[1] G. E. Pukhov. Taylor Transforms and Their Application in Electrical Engineering and Electronics [in Russian], Nauk. Dumka, Kyiv (1978).

[2] I. N. Efimov, E. D. Golovin and O. V. Stoukatch, "Exactitude of the electronic devices analysis by the differential transformations method," 2003 Siberian Russian Workshop on Electron Devices and Materials. Proceedings. 4th Annual (IEEE Cat. No.03EX664), 2003, pp. 150-151, doi: 10.1109/SREDM.2003.1224211.

[3] R. Hołubowski. Application of differential transformation finite element method in aperiodic vibration of non-prismatic beam. Procedia engineering 199 (2017): 360-365.

[4] M. Sharma, K. Singh, A. Kumar. MHD flow and heat transfer through non-Darcy porous medium bounded between two parallel plates with viscous and joule dissipation Spec. Top Rev. Porous Media Int. J., 5 (2014), pp. 1-11

[5] I. Hwang, J. Jinhua, D. Du. Differential transformation and its application to nonlinear optimal control. 2009.

[6] A. I. Stasiuk, R. V. Hryshchuk, L .L. Goncharova. A mathematical cybersecurity model of a computer network for the control of power supply of traction substations. Cybern. Syst. 53(3), 476–484 (2017).

[7] M.Yu. Rakushev, "Method for Prediction Of Space Vehicle Motion Based on the Multidimensional Differential-Teylor Transformations" in Journal of Automation and Information Sciences, Begell House Inc, vol. 51, no. 4, pp. 1-11, 2019.

[8] R. V. Hryshchuk. Osnovy kibernetychnoi bezpeky [Text]: monohrafiya / R. V. Hryshchuk, Yu. H. Danyk; Yu. H. Dannyk (Ed.). – Zhytomyr: ZhNAEU, 2016. – 636 p.

[9] G. Bronshpak, I. Gromiko, S. Docenko and E. Perchik, "Kriptografiya novogo pokoleniya Integralnie uravneniya kak alternativa algebraicheskoi metodologiyi", [New generation cryptography: Integral equations as an alternative to algebraic methodology], Prikladnaya elektronika, № 3, pp. 337-349, 2014. DOI: 10.13140/RG.2.1.1973.2645. (In Ukrainian).

[10] R.V. Hryshchuk Differential-game the spectral model of the process of attacking information has been rounded up / R.V. Grishchuk // Bulletin of ZhDTU. - Zhitomir: ZhDTU, 2009. - No. 48 (I). - S. 152–159.

[11] R. V. Hryshchuk. Teoretychni osnovy modeliuvannia protsesiv napadu na informatsyiu metodamy teoryi dyferentsialnykh ihor ta dyferentsialnykh peretvoren [Text]: monohrafiya / R. V. Hryshchuk. – Zhytomyr: Ruta, 2010. – 280 p.

[12] R. V. Hryshchuk, O. M. Hryshchuk. A Generalized Model of Fredholm's Cryptosystem. Cybersecurity: education, science, technique, 2019, Vol. 4 (4), pp. 14–23. DOI: 10.28925/2663-4023.2019.4.1423. (In Ukrainian).

[13] V.V. Okhrimchuk. The differential-game model is used to the template of a potentially unsafe cyber attack // Cyberbezpeka: education science and technology. Kiev: Kiev. University of B. Grinchenka, 2020. № 4 (8). S. 113-123.

[14] R. V. Hryshchuk. Method of differential-game P-model of processes in attack on information / R. V. Grishchuk // Information security. - Lugansk: SNU im. V. Dahl, 2009. - No. 2 (2). - S. 128-132.

[15] O. M. Hryshchuk. Features of the encryption key selection for the Fredholm cryptosystem. Computer Engineering and Cybersecurity: Achievement and Innovation: Materials II All-Ukrainian. nauk.-practical. conf. zdobuvachiv vishoï educate th young pupils, metro Kropyvnytskyi, 25-27 leaf. 2020 p. / Ministry of Education and Science of Ukraine, Derzh. sciences. established "Institute of Modernization for the Minister of Education", Tsentralnoukr. nat. tech. un-t; - Kropyvnytskyi: TsNTU, 2020. P. 109-110 p.

Possibilities Of Using Watermarks To Protect Software Code

Vadym Poddubnyi[1], Roman Gvozdev[2], Oleksandr Sievierinov[3], Oleksandr Fediushyn[4]

[1,2,3,4] *Kharkiv National University of Radio Electronics, 14 Nauky Ave, Kharkiv, 61166, Ukraine.*

Abstract

This paper considers methods for software code protection from modifying and illegal distribution. Including methods based on digital watermarks, and zero digital signs. One of the promising methods of program code protection is the KeySplitWatermark method. The paper considers it and the possibility of modernization.

Keywords

Watermarks, software, zero watermarks, KeySplitWatermark.

1. Introduction

The problem of software protection from attackers appeared with the advent of the first commercial program. Despite the modernization of software development, delivery, and integrity facilities, the annual cost of distributing unlicensed software is approximately $46.3 billion. Although in recent years the percentage of unlicensed software in the world has decreased from 39% to 37%, the problem of protecting software code and programs in general will remain relevant. This problem is especially important for the post-Soviet space, so in Ukraine the percentage of unlicensed software is 82%, in Russia 62% and in Belarus 82%, which is similar to the indicators of developing countries in Africa (Nigeria 80%, Kenya 74%, Zambia 80%) [1].

It should be noted that not only unlicensed distribution can cause damage, attackers can embed malicious elements in the program, use separate modules of the program, etc. (Figure 1).

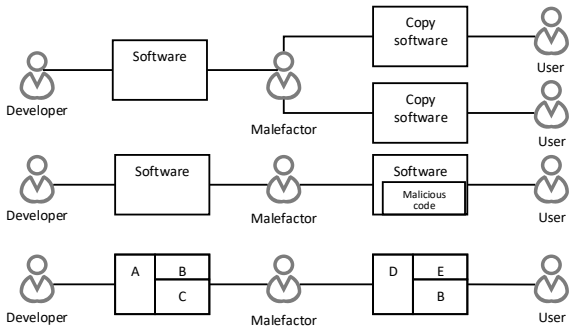


Figure 1. Possible software attacks

2. Methods of program code protection

To reduce the loss from unlicensed distribution and embedding malicious elements in the program code, software developers are forced to use a variety of protections.

Some of the most common methods of software removal are:

1. Adding program code to prevent intrusions;
2. Obfuscation of the program code;
3. Digital watermarks [2].

Obfuscation - is the process of code reorganization, primarily aimed at complicating the disassembly of software code by an attacker. It involves modifying a program, or adding code to a program to increase its complexity.

The main methods of obfuscation:

- Formatting transformations that change only the appearance of the program. This group includes conversions that delete comments, indents in program text, or rename IDs.

EMAIL: vadym.poddubnyi@nure.ua (A. 1); roman.hvozdov@nure.ua (A. 2); oleksandr.sievierinov@nure.ua (A. 3), oleksandr.fediushyn@nure.ua (A. 4)

- Transform data structures that change the data structures that the program works with. This group includes, for example, transformations that change the hierarchy of class inheritance in a program, or transformations that combine scalar variables of the same type into an array.
- Convert a program's control flow to change the structure of its control flow graph, such as sweeping loops, selecting code snippets into procedures, and more.
- Preventive transformations that target certain decompilation methods or use bugs in certain decompilation tools.

The downside of obusfuscation is the complexity of the development process and modernization of software, and the software after obusfuscation may be more complex and slower [3].

To ensure the integrity of the software, developers add to the programs special modules that to check software integrity. Such code blocks check the hash values of the program and its components, encrypt and decrypt the program code, or monitor the status of the program (respond to incorrect data or commands, etc.).

To protect the program from hacking, you need to make sure that it "works as intended" even if attacker tries to interrupt, control or change the execution of the program code.

It should be noted that this is different from obfuscation, where the goal is to make it more difficult for an attacker to understand and read the program.

The disadvantages of this method are the increase in the number of resources for the operation of the program, as it requires additional resources of the protection module. Such modules may also conflict with other software. Also, such modules can interfere with the operation of parts of the program or other programs.

In practice, the line between protection against unauthorized access and obfuscation is blurred: a program that is more difficult to understand because it has been confusing will also be more difficult to modify and attack.

Digital watermarks are special secret messages that are embedded in the program code or program data, they serve to confirm the authorship and preserve the integrity of the data.

Since its inception, digital watermarks have been commonly used for multimedia data embedded in various signal characteristics (frequency, brightness, color, etc.). However, over time, digital watermarks began to be used to protect software.

3. Watermark type

According to the methods of embedding in the program code, digital watermarks are divided into static and dynamic. Static watermarks are embedded in program code or data as opposed to dynamic ones, which store the watermark during program execution. [4]

According to their characteristics, digital watermarks are divided into:

- Fragile. Digital watermarks that are impossible to detect, with the slightest modification. Used to control integrity;
- Semi-fragile. Digital watermarks that can withstand some changes in the carrier digital watermark. Is used to detect an attack;
- Reliable. Watermarks are resistant to all types of attacks. Used for authentication and authentication.

There are various types of embedding digital watermark in the program, the most common of which are:

1. Replacement of the code;
2. Replacement of code logic;
3. QP algorithm;
4. QPS algorithm;
5. Digital watermark on the basis of graphs.

The downside of digital signs is that the digital watermark increases the size of the program. Static watermarks cannot fully protect data and require additional protection methods [4].

Watermarks and protection against unauthorized access are also related. In fact, if perfect protection against unauthorized access were available, it would be easy to add watermarks, watermarks should be combined with any trivial algorithm to protect against unauthorized access, and an attacker would not be able to find or destroy the tag. Precisely because there is no perfect protection against unauthorized access, you need to worry about masking watermarks.

It is assumed that an attacker who can find a watermark will also be able to change the program to destroy the sign [5]. A graphical representation of the digital watermark is shown in Figure 2.

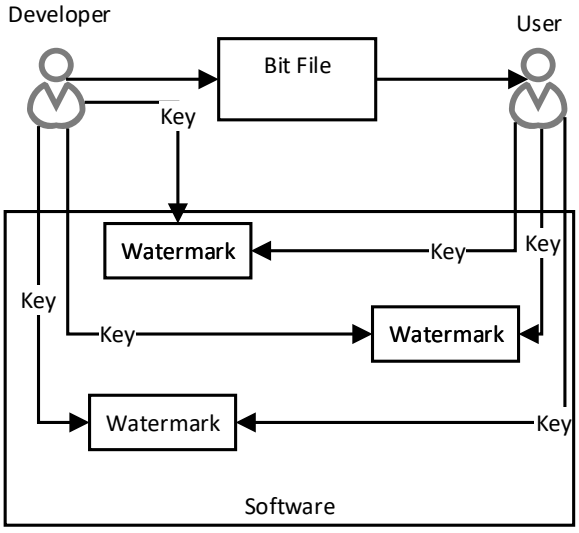


Figure 2. Graphic representation of a digital watermark

4. Zero digital watermark

One of the methods of solving the problems of digital watermarks is "zero watermarks".

A traditional digital watermark hides information about the owner or creator of an object or objects group of objects somewhere inside that object. This hidden information can later be used for many purposes: maintaining integrity, detecting intentional or accidental interference, protecting data copyright, etc.

Zero watermarks, unlike "normal" digital watermarks, are not embedded in program code. Program, data, or code structure is used to generate a null character.

Also, one of the advantages of zero digital characters is that they are resistant to compression of the embedded object.

Graphical representation of the zero digital sign is shown in Fig. 3.

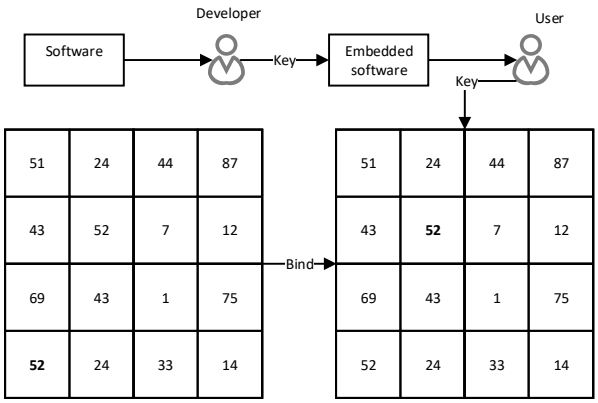


Figure 3. Graphical representation of the zero digital watermark

Zero digital watermarks are widely used in medicine [6] [7] to protect patient data, but zero digital signs can also be used to protect software.

One example of zero digital watermark algorithms for program code protection is the algorithm considered by KeySplitWatermark [8]. There are also algorithms for fragile digital watermarks to protect the database from modifications [9].

These algorithms use statistical data and asymmetric encryption using a certification authority to generate digital watermarks. The characteristics of this type of digital watermarks indicate the prospects for their use to protect software code from unauthorized changes or from unlicensed distribution.

5. KeySplitWatermark Algorithm

KeySplitWatermark algorithm is presented by a group of developers from different universities around the world such as China, Pakistan, India and others. KeySplitWatermark is a new approach based on a blind zero watermark to protect software source code from cyberattacks.

KeySplitWatermark first analyzes the program code to determine the keywords, and then divides the code into sections based on the selected keyword. The algorithm generates a unique key using keywords and the program code itself. If you have any copyright concerns in the future, you can use this key to verify ownership. The implementation algorithm does not make any changes to the program code to create watermarks, and the extraction algorithms do not require the use of watermarks as input, which makes it blind (zero digital sign).

The watermark algorithm consists of two components; embedding and removing watermarks. Watermark embedding is performed by the original owner of the software, and removal is later performed by a trusted third party.

In this algorithm, the program code is first pre-processed to identify the ten most common characters and the five most common keywords. It is then divided into sections based on the user-selected keyword KeySplitWatermark, in which the implementation algorithm accepts the following input:

- Source code: The source code of the software to which the watermarks should be applied.

• Cipher: a numeric value that will be used in the key generation process.

• Watermark: ASCII character group.

The implementation algorithm generates the owner key as the output. This key is written to the certificate authority and then used to remove the watermark (if necessary). The extraction algorithm accepts the following input data:

• Attacked code file: A program code file that has been modified or used illegally as a copyright infringement.

• Owner key: It is obtained from the certification authority to identify the original owner

The certificate authority is a requirement of this algorithm that registers content to the copyright owner. When an attack is suspected, this trusted third party removes the watermarks and provides the original code of the recovery software if a counterfeit is detected. The fake code is replaced by the original code, which makes the actions of the attacker invalid.

The graphical representation of the algorithm is shown in Figure 2.

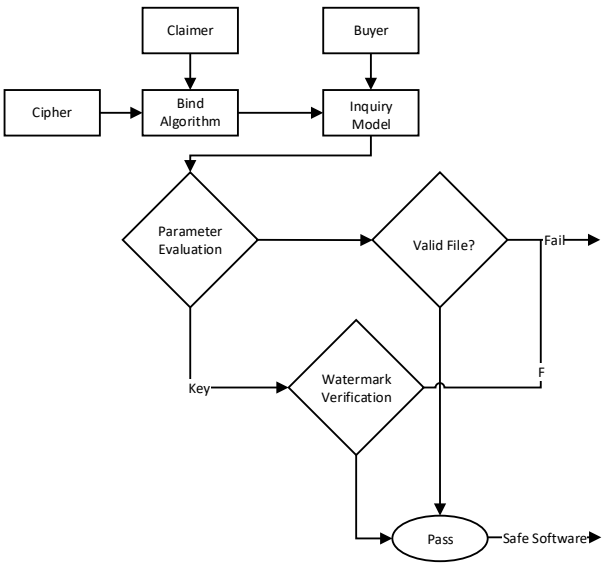


Figure 4. Graphical representation of the KeySplitWatermark algorithm

It is impossible to destroy a watermark without a significant change in the code, and if any changes occur in the code, the source code is restored. The results of research conducted by the authors prove that KeySplitWatermark is reliable, secure and efficient with minimal computational requirements.

The results of research conducted by the authors prove that KeySplitWatermark is reliable, secure and efficient with minimal computational requirements (Table 1)[8].

To evaluate the reliability of KeySplitWatermark, developers of the algorithm used ASProtect, Upx and Aspack to attack the program with watermarks and check the correctness of the removed watermark. The results of the experiment are shown in Table 2.

The watermark can be properly removed after encryption, shelling, and watermark compression attacks. The initial semantics of the program are preserved, although various attacks are carried out.

The algorithm is promising, has potential and requires detailed analysis and study [8]. Since the algorithm is new, the following vectors of research and modernization are offered as improvements:

1. Use Unicode instead of ASCII to generate keywords;
2. Parse program code with keyword pairs to increase the number of code split combinations;
3. National algorithms for certificate authority.

Switching to Unicode is suggested to potentially increase the languages to use and increase the length of the keywords generated.

The use of keyword pairs should expand the variability of the choice and potentially increase the stability of the algorithm. It is also proposed to increase the number of keywords for the same purpose.

The use of national algorithms (such as DSTU 7624 [10], DSTU 4145[11], DSTU 7564[12]) can improve the stability of the algorithm.

A promising task is to create a certification center for the use of the KeySplitWatermark algorithm and its testing.

Table 1

Comparative Results for Increase in the size of the Watermarked Code and in Execution Time for Crptoencryption With 31KB File

Watermark length (bit)	Increase in program (KB)	Increase in program KeySplitWatermark	Execution time(ms)	Execution time KeySplitWatermark
128	18	0	23	18

Watermark length (bit)	Increase in program (KB)	Increase in program KeySplitWatermark	Execution time(ms)	Execution time KeySplitWatermark
256	34	0	40	32
512	67	0	45	39
1024	130	0	123	105

Table 2
Attacks and results

Tool	Attack Mode	Extraction	Extraction KeySplit Watermark
ASProtect	Encrypts program	100%	100%
UPX	Conducts code compression	100%	100%
Aspack	Used to shell the program	100%	100%

6. Conclusions

This paper provides a brief overview of methods for protecting software code from modification and distribution. One such method is digital watermarks. This method has many disadvantages, but they have been eliminated with the advent of a new type of digital watermarks - zero digital watermarks.

One of the promising methods of zero digital sign is KeySplitWatermark. To improve the characteristics, its modernization and further research are proposed. It is also proposed to study and use it together with national algorithms (DSTU 7624, DSTU 4145, DSTU 7564) and certification authority.

7. References

[1] Business Software alliance, Software Management: security imperative, business opportunity, 2018.

[2] Christian S. Collberg, Clark Thomborson Watermarking, Temper-Proofing, and Obfuscation – Tools for Software Protection, 2000.

[3] Чернов А. В., Анализ запутывающих преобразований программ, 2003, URL: http://citforum.ru/security/articles/analysis/.

[4] James Hamilton, Sebastian Danicic Department of Computing, Goldsmiths, University of London United Kingdom, A Survey of Static Software Watermarking, URL: https://www.researchgate.net /publication/224229798_A_survey_of_static _software_watermarking.

[5] C. Collberg, J. Nagra Surreptitious Software - Obfuscation, Watermarking, and Tamperproofing for Software Protection

[6] Aleš Roček, corresponding author Michal Javorník, Karel Slavíček, and Otto Dostál, Zero Watermarking: Critical Analysis of Its Role in Current Medical Imaging, URL: https://www.ncbi.nlm.nih.gov/pmc/articles/ PMC7886926/.

[7] Zulfiqar Ali, Muhammad Imran, Mansour Alsulaiman, Tanveer Zia, Muhammad Shoaib, A Zero-Watermarking Algorithm for Privacy Protection in Biomedical Signals.

[8] Celestine Iwendi, Zunera Jalil, KeySplitWatermark: Zero Watermarking Algorithm for Software Protection Against Cyber-Attacks, 2020, URL: https://ieeexplore.ieee.org/document/906821 7/references#references.

[9] Aihab Khan, Syed Afaq Husain, A Fragile Zero Watermarking Scheme to Detect and Characterize Malicious Modifications in Database Relations, 2013, URL:https://hindawi.com/journals/tswj/201 3/796726/.

[10] National standard of Ukraine, Information technologies. Cryptographic information protection. Symmetric block transformation algorithm DSTU 7624: 2014.

[11] National standard of Ukraine, Cryptographic information protection, Based digital signature on elliptical curves. formation and verification DSTU 4144-2002.

[12] National standard of Ukraine, Cryptographic information protection. Hashing function DSTU 7564: 2014.

Simulation model of Blockchain System in the Higher Education

Shmatko Olexandr [1], Serhii Yevseiev [2] Vladyslav Khvostenko[3]

[1] *National Technical University "Kharkiv Polytechnic Institute" st. Kirpichova, 2, Kharkiv, 61000, Ukraine*
[2,3] *Simon Kuznets Kharkiv National University of Economics, ave. Nauki, 9-A, Kharkiv, 61166 Ukraine*

Abstract
This article presents a mathematical model of a distributed ledger for higher education. The main components of this network are considered, as well as their formal presentation. The model of peer-to-peer network is visualized, the research of the parameters of the centralized and decentralized data processing network is carried out. Based on the data obtained, simulation models were built and investigated. The results of the simulation simulations were analyzed and the most optimal parameters were selected.

Keywords
distributed ledger, blockchain, mathematical modeling, simulation, probability theory, theory of random processes.

1. Introduction

At present in the world there is a revolutionary transition from informatization of the main spheres of human activity to their digitalization.

If informatization involves, in essence, the modernization of certain human activities through the use of information and communication technologies, the digital transformation (or digitization) in its turn involves their qualitative transformation, departure from the usual types and forms of activity to the new ones, based on digital models and technologies [1,2].

The development of the digital environment requires the support and development of both existing conditions for the emergence of promising end-to-end digital platforms and technologies, as well as the creation of conditions for the emergence of new platforms and technologies.

The main end-to-end digital technologies are:
– big data;
– neurotechnology and artificial intelligence;
– distributed registry systems (blockchain);
– quantum technologies;
– new production technologies;
– industrial internet;
– components of robotics and sensors;
– wireless communication technologies;
– virtual and augmented reality technologies.

Continuing the cycle of work on the digital transformation of education [2–4], the paper conducts research on the use of blockchain technology (blockchain) for the tokenization of educational assets and promising areas of its implementation in education.

2. Literature review

In [6] possible scenarios for using blockchain technology in the field of education are considered. Methods and technologies of tokenization of assets, related to the educational process, are investigated. It is concluded, that the blockchain technology is decentralized and transparent with a high degree of reliability, which ensures the equality of all users of the chain's services. The transparency of the technology guarantees the participants in the process against abuse and forgery of documents. The study of the features of smart contracts made it possible to form the advantages of smart contracts in the field of education

In [7], provides a critical analysis of application of the blockchain technology

EMAIL: oleksandr.shmatko@khpi.edu.ua (A. 1);
serhii.yevseiev@hneu.net (A. 2);
vladyslav.khvostenko@gmail.com (A. 3)
ORCID: 0000-0002-2426-900X (A. 1); 0000-0003-1647-6444 (A. 2); 0000-0000-0000-1234 (A. 3)

considering with its applicability opportunities and restrictions in education; it also aims to identify the consequences of its influence upon the development of education.

The article [8] provides an overview of the use of blockchain for academic transcripts. The aim is to find, among the proposed models, overlapping aspects that solve common problems and can lead to a universally accepted de facto standard. In addition, since academic institutions will serve as oracles for specific blockchain applications, a robustness study is underway to see if the proposed applications effectively solve the oracle problem.

The paper [9] is a Systematic Bibliometric Review of the Literature on Blockchain Applications Research in Higher Education. The review includes 37 articles that provide up-to-date knowledge on the current implications of using blockchain technology to improve higher education processes. The LRSB findings show that blockchain is being used to create new interventions to improve the prevailing ways of sharing, delivering and protecting student knowledge data and personal records.

The relevance of this work is due to the increasing popularity of distributed registry systems, in connection with which it is necessary to assess the quantitative parameters of this network and determine the most optimal parameters.

The general network model is a peer-to-peer network in which each participant has m client applications, an application server S, an N node (a server for communicating with other network nodes)

3. Simulation model

Simulation is a method of research in which the studied system is replaced by a model, with sufficient accuracy describes the real system from which experiments are conducted in order to obtain information about this system.

In favor of using the methods of simulation in this situation is the impossibility of experimenting on a real object, because then we would have to develop two full-fledged systems. Also models will allow to demonstrate work of two architectures in time and to calculate indicators for decision-making in favor of one of them.

The main parameter of the study will be the average transaction processing time of the system.

To simulate the model you need to know the following parameters:

1 Average processing time of one application;

2 Number of customers sending applications;

3 Number of servers processing these requests.

Many transactions related to smart contracts circulate on the Ethereum platform. To calculate the average processing time of one application, you need to include several assumptions and simplifications:

1) The generation time of a new block is subject to the exponential law (the covariance coefficient for this law is a constant equal to one) [14].

2) The Ethereum blockchain platform does not have the maximum possible block size and limit on the number and size of transactions, but there is a limit on the maximum amount of gas (gas, transaction fees) used in the block. This value can be reduced or increased in the next block by 20 percent [9].

When developing a mathematical model, it is assumed that the maximum number of transactions in the block will be 77. This number is taken from the average number of transactions in the block of the real network Ethereum [10], obtained as of November 2017

3) The emergence of new transactions (in other words, applications) is subject to the simplest law of distribution, namely Poisson's. In the developed mathematical model it is considered that the flow of incoming applications is the simplest, because it corresponds to the properties of stationary, ordinary and no aftereffects in the considered conditions.

Each transaction is processed sequentially and has a strict order of writing to the decentralized blockchain; this ensures the ordinary flow of applications.

A centralized system can also be considered in the context of queuing theory, because the server is a single-phase queuing system.

AnyLogic software environment is used to build a simulation model and conduct experiments. Simulation models of two systems were built using AnyLogic tools.

Input parameters of the model:

1 Number of customers sending requests

2 Number of miners in the blockchain network

3 Number of requests per 10 minutes from one client

4 Number of requests from one client

Figures 1 and 2 show simulation models of decentralized and centralized networks.

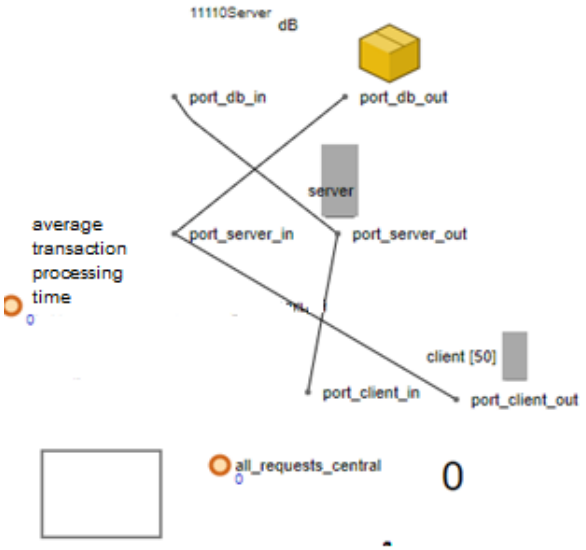


Figure 1: Simulation model of centralized network.

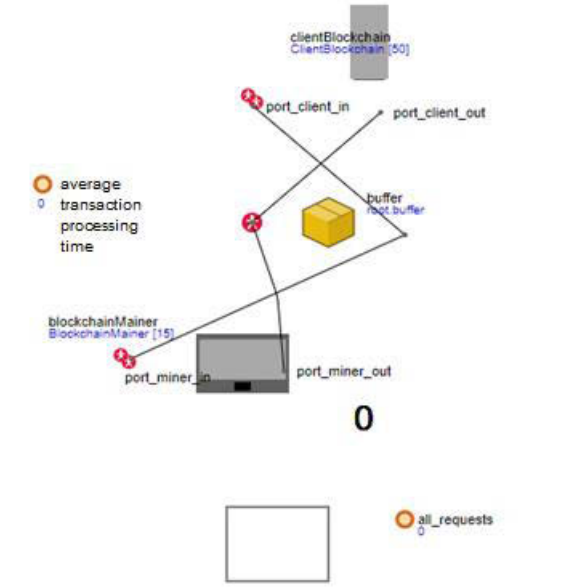


Figure 2: Simulation model of decentralized network.

The algorithm of centralized work is as follows:

1. Requests with a given intensity come from customers
2. Requests are queued on the application server, where they are processed and sent to the database server
3. After processing on the database server, the transactions again fall on the application server, where the result is sent back to the client
4. The client receives a response from the application server regarding the processing of its payment transaction

In the decentralized model, transaction processing has a different form:

1. Customers send transactions with a given intensity
2. Transactions fall into the buffer, where they are collected in blocks
3. When the block is filled with transactions, the miner begins the Mining block process
4. When the first of the miners completes the process, the block is closed and placed in the chain chain, and the transactions in this block are considered processed, so the responses are sent back to customers.

4. Results of modeling

Consider the Hinchin-Polachek formula for calculating the average waiting time of the application:

$$\omega = \frac{\lambda \times b^2 \times (1 + v^2)}{2 \times (1 - \lambda \times b)}$$

where λ - the intensity of the flow of applications,

b is the average processing time of one application,

v is the coefficient of variation of the law of distribution of the average processing time of one application.

If the denominator of the formula is greater than or equal to one, the average waiting time for the execution of one application goes to infinity. Indeed, if the intensity is too high, the application will never be processed at an infinite interval. The calculated values corresponding to the blockchain system considered in the work. The average processing time of one application.

$$b = \frac{the\ average\ mining\ time\ of\ the\ block}{the\ number\ of\ transactions\ in\ the\ block}$$

The average mining time of the block and the average number of transactions in the block were obtained from the average indicators of the actually working Ethereum network in November 2017 [9, 10].

$$b = \frac{15}{77} \approx 0.195\ sec$$

The coefficient of variation for the exponential law, which determines the processing time of one application, is equal to one. Thus, we obtain the formula of the average waiting time for

processing one application, which depends on the intensity of the input stream:

$$\omega = \frac{\lambda \times 0.038}{1 - \lambda \times 0.195}$$

For the centralized model:

b = average time of application processing on the application server + average time of application processing by the database server = 200ms + 103ms. = 0.303 sec.

Then the formula for the average waiting time for processing one application, which depends on the intensity of the input stream for the centralized network model:

$$\omega = \frac{\lambda \times 0.091}{1 - \lambda \times 0.303}$$

It is proposed to conduct several experiments, with different indicators of the intensity of the flow of requests and the number of customers.

Parameters of first experiment.

Number of clients: 5

Miner's number: 10

Number of transactions from the client per minute: 0.2

Number of requests: 10

First of all, you should calculate the intensity of the flow of applications per second:

$\lambda = 0.2 / 60 = 0.003$ sec

The next step is to calculate the average waiting time for processing one application for a centralized system:

$\omega = (\lambda \cdot 0.091) / (1-\lambda \cdot 0.303) = 0.00027$ sec.

And for centralized respectively:

$\omega = (\lambda \cdot 0.038) / (1-\lambda \cdot 0.195) = 0.00011$ sec.

The experiment will run for 10 minutes. The centralized system processed requests in 3190,767 seconds, and the decentralized system in 66,880 seconds. A total of 50 requests were processed, as evidenced by the green colors of both rectangles.

Conduct experiment 2 with another data set:

Number of clients: 20

Miner's number: 15

Number of transactions from the client per minute: 1

Number of requests: 20

Let's calculate the values for modeling:

$\lambda = 0.2 / 600 = 0.016$ sec.

$\omega = (\lambda \cdot 0.091) / (1-\lambda \cdot 0.303) = 0.0014$ sec.

And for centralized respectively:

$\omega = (\lambda \cdot 0.038) / (1-\lambda \cdot 0.195) = 0.00060$ sec.

The experiment will run for 10 minutes. In the decentralized system, this experiment ends at 79.833 seconds of simulation, and the centralized system completed its work in 6673.53 seconds, processing only 124 applications.

Based on this, we can conclude that the processing of transactions in the decentralized network model is almost 47 times faster than in the centralized. At the same time, the centralized system has less fault tolerance than the decentralized one, as experiment 2 showed. In addition, the centralized system is vulnerable to DDoS attacks, while in the decentralized model, one of the nodes would have to take at least 51% of the load, which is completely unrealistic. That is why the confidentiality of data in a decentralized system is an order of magnitude higher than in a centralized one.

In order to clearly demonstrate the importance of the data, it was decided to conduct 23 experiments on different data sets and to track how each of the systems will behave as the number of queries increases. A constant number of clients was selected for the experiments - 5 pieces and the range of requests from 5 to 205. This means that each client will send 1,3,5,7 ... 41 requests. The results of these experiments are presented in Figure 3.

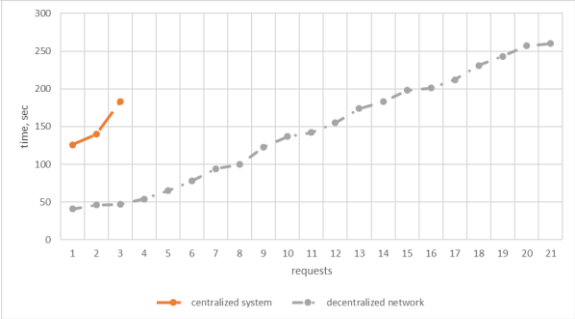


Figure 3: Graph of fault tolerance of systems

As can be seen from the figure, after 25 requests, the centralized system does not process the total number of requests coming into the system. This means that the load of 5 requests from each of the 5 customers per minute for her was the maximum. The decentralized system processed all incoming requests.

The graph clearly shows that the curve of the centralized system breaks at the coordinate (183,132; 25). And the curve of the decentralized system is growing

5. Conclusions

The experiment showed that the performance of the network depends on the intensity of the appearance of applications, while for the correct operation of the blockchain technology of the presented type, it is possible to vary the values of the intensity of nodes and the values

buffer size.

The authors did not consider internal connections between network elements when building the models, which could affect the results. Also, the simulation model does not provide the possibility of obtaining a point estimate of the investigated parameter, but allows one to obtain interval estimates, the accuracy of which depends on the methods and scope of observations, the initial state, and the pseudo-random number generator.

It should be noted that modeling the performance of blockchain technology using the AnyLogic system can be convenient for analysis when changing various parameters. However, for more accurate results, it is necessary to carry out

additional research in the field of blockchain modeling on the AnyLogic emulator.

The analysis of the models showed the applicability of separate simulation systems for assessing the impact of blockchain technology on data transmission and processing networks.

In this paper, an overview of solutions based on blockchain technologies in the field of higher education was carried out and presented, as well as simulation models with an emphasis on queuing systems were presented. The results of comparison of decentralized and centralized systems are presented.

In the future, it is planned to expand the system indicators to obtain more accurate results using the AnyLogic system and propose a methodology for calculating the network infrastructure, taking into account the characteristics of the traffic and the received data.

6. References

[1] . Nakamoto, S., Bitcoin, A. (2008). Bitcoin: A peer-to-peer electronic cash system. Available at: https://bitcoin.org/bitcoin.pdf

[2] Tulchinsky, G. (2017). Digital Transformation of Education: Challenges for Higher School. Russian Journal of Philosophical Sciences, 6, 121–136.

[3] Antonova, D. A., Ospennikova, E. V., Spirin, E. V. (2018). TSifrovaya transformatsiya sistemy obrazovaniya. Proektirovanie resursov dlya sovremennoy tsifrovoy uchebnoy sredy kak odno iz ee osnovnykh napravleniy. Vestnik Permskogo gosudarstvennogo gumanitarno-pedagogicheskogo universiteta. Seriya: Informatsionnye kompyuternye tekhnologii v obrazovanii, 14. Available at: https://cyberleninka.ru/article/n/tsifrovaya-transformatsiya-sistemy-obrazovaniya-proektirovanie-resursov-dlya-sovremennoy-tsifrovoyuchebnoy-sredy-kak-odno-iz-ee

[4] Kozlova, N. Sh. (2019). Tsifrovye tekhnologii v obrazovanii. Vestnik Maykopskogo gosudarstvennogo tekhnologicheskogo universiteta, 1. Available at: https://cyberleninka.ru/article/n/tsifrovye-tehnologii-v-obrazovanii

[5] Svon, M. (2019). Blokcheyn. Skhema novoy ekonomiki. Moscow: Litres, 311..

[6] Shmatko, O., Borova, T., Yevseiev, S., & Milov, O. (2021). Tokenization of Educational Assets Based on Blockchain Technologies. ScienceRise: Pedagogical Education,(3 (42), 4–10. doi: 10.15587/2519-4984.2021. 232321.

[7] Fedorova, Elena P., and Ella I. Skobleva. "Application of Blockchain Technology in Higher Education." European Journal of Contemporary Education 9.3 (2020): 552-571.

[8] Caldarelli, Giulio, and Joshua Ellul. "Trusted Academic Transcripts on the Blockchain: A Systematic Literature Review." Applied Sciences 11.4 (2021): 1842.

[9] Kiffer, Lucianna, Dave Levin, and Alan Mislove. "Stick a fork in it: Analyzing the Ethereum network partition." Proceedings of the 16th ACM Workshop on Hot Topics in Networks. 2017.

[10] Gencer, Adem Efe, et al. "Decentralization in bitcoin and ethereum networks." International Conference on Financial Cryptography and Data Security. Springer, Berlin, Heidelberg, 2018.

Оптимальне Керування Рівнем Вибухонебезпечності Потенційно Вибухонебезпечного Об’єкту

Волков Віктор[1], Макоєд Наталя[2]

[1]*Одеський національний університет ім. І.І. Мечникова, вул. Дворянська, 2, Одеса, 65082, Україна*
[2] *Одеська національна академія харчових технологій, вул. Канатна, 112, Одеса, 65039, Україна*

Анотація

Розглянуто питання про оптимальне керування рівнем вибухонебезпечності потенційно вибухонебезпечного об'єкту. Задачу поставлено математично в загальному вигляді і розв’язано для одного окремого випадку (в цьому випадку рівень вибухонебезпечності об'єкта повністю визначається співвідношенням розмірів об'єкта і довжини переддетонаційної ділянки). Розв’язок базується на отриманій раніше аналітичній оцінці довжини переддетонаційної ділянки. Розв’язок реалізовано в програмному продукті. Розроблена програма застосовується для оптимального керування вибухобезпечністю окремих силосів. Ця програма може стати важливою складовою програмного забезпечення автоматизованої системи керування елеватором або іншим зерновим підприємством, що є потенційно вибухонебезпечним об'єктом.

Ключові слова

Оптимальне керування, вибух, вибухонебезпечність, потенційно вибухонебезпечний об'єкт, довжина переддетонаційної ділянки

Optimal Control of the Degree of Explosion Hazard of a Potentially Explosive Object

Volkov Victor[1], Makoyed Natalia[2]

[1]*Odessa I.I.Mechnikov National University, Dvoryanskaya str.,2, Odessa, 65082, Ukraine*
[2]*Odessa National Academy of Food Technologies, Kanatnaya str., 112, Odessa, 65039, Ukraine*

Abstract

The problem of optimal control of the degree of explosiveness of a potentially explosive object is considered. The problem is set mathematically in general form and solved for one particular case (in this case, the level of explosiveness of the object is completely determined by the ratio of the size of the object and the length of the pre-detonation area). The solution is based on the previously obtained analytical estimate of the length of the pre-detonation section. The solution is implemented in the software product. The developed program is used for optimal control of explosion safety of individual silos. This program can become an important component of the software of an automated control system of an elevator or other grain enterprise that is a potentially explosive object.

Keywords

Optimal control, explosion, explosion hazard, potentially explosive object, detonation induction distance

EMAIL: viktor@te.net.ua (A.1); natamakoyed@gmail.com (A.2)
ORCID:0000-0002-3990-8126(A.1); 0000-0002-4591-555X(A.2)

1. Вступ

Довільний потенційно вибухонебезпечний об'єкт (ПВНО) може розглядатися з позицій системного аналізу як складна система, архітектура якої складається з деяких компонентів (підсистем) і з ієрархічних відносин цих компонентів [1]. В кінцевому підсумку, ПВНО складається з окремих елементарних потенційно вибухонебезпечних об'єктів (ЕПВНО) [1]. При математичному моделюванні виробничого ПВНО, як ЕПВНО, що моделює деякий реальний об'єкт у складі ПВНО, розглядається плоский канал або кругла циліндрична труба. Наприклад, якщо в якості ПВОО розглядається силосний корпус елеватора, то ЕПВНО є окремий силос, що моделюється плоским каналом в разі прямокутного перетину або круглої циліндричної трубою в разі круглого перетину. Нижче з позицій забезпечення вибухобезпеки розглядаються тільки ЕПВНО. Коректна оцінка вибухонебезпечності кожного окремого ЕПВНО надає можливості керування загальним рівнем вибухонебезпечності ЕПВНО.

Метою даного дослідження є постановка і рішення (в досить загальному вигляді) завдання мінімізації рівня вибухонебезпечності ЕПВНО, тобто в переведенні ЕПВНО з даного фізичного стану в найбільш вибухобезпечний стан з усіх припустимих з точки зору технологічного регламенту станів.

2. Розв’язання задачі оптимального керування

Задачу оптимального керування розв’язано для конкретного ЕПВНО, в якості якого обрано окремо взятий силос (в реальності такий силос може бути як окремо розташованим, так і входити до складу силосного корпусу).

Проблема вибухобезпеки силосів представляється актуальною, тому що за статистикою саме на силоси і бункери припадає майже половина від загальної кількості вибухів на підприємствах із зберігання та переробки зерна, тобто саме силоси представляють собою найбільш вибухонебезпечні ЕПВНО в таких ПВНО, якими є зернові та комбікормові виробництва і зернові сховища. При завантаженні і гравітаційному розвантаження силосів в них утворюється пилоповітряна суміш (ППС), здатна займатися і горіти. На стінках бункерів і силосів може осідати і накопичуватись в значній кількості пил, що при зовнішніх збуреннях швидко переходить у зважений стан, також створюючи вибухонебезпечну ППС. Вибух в силосі призводить до тяжких наслідків, так як при цьому руйнуються бічні стінки і перекриття, а також деформується і розривається випускний конус силосу під дією тиску вибуху.

При розв’язанні задачі оптимального керування окремо взятим силосом як вибухонебезпечним об’єктом розглядаються силоси як залізобетонні (монолітні і збірні), так і металеві, але обов'язково з круглої або прямокутної (зокрема - квадратної) формою поперечного перерізу.

Для оптимального керування рівнем вибухонебезпечності окремо взятого силосу в середовищі програмування Visual Basic розроблено програму «Оптимальне керування вибухонебезпекою окремих силосів» («SilosOtdelniyOpt»), яку включено до складу програмного комплексу «Оцінка вибухонебезпечності окремих силосів» («SilosOtdelniy»), розробленого раніше [2, 3]. Інтерфейс програми надає користувачеві можливість вибрати один із стандартних залізобетонних силосів або ж самостійно задати форму і розміри силосу (залізобетонного або металевого). Подальші розрахунки вимагають завдання виду ППС, концентрації пилу, вологості, температури і дисперсності (середнього розміру пилових частинок). Всі ці величини можуть вимірюватися за допомогою стандартних метрологічних приладів в режимі експлуатації зерносховища або зернопереробного підприємства (а сама програма в цьому випадку є складовою частиною програмного забезпечення відповідної автоматизованої системи керування). В результаті розрахунків користувач (як правило, їм є оператор-технолог) отримує інформацію:

- про рівень вибухонебезпечності силосу, про довжину переддетонаційної ділянки і про час можливого переходу повільного горіння (пожежі) у вибух;

- про найбільш вибухонебезпечному стані силосу з усіх його можливих (в рамках технологічного процесу) станів.

Ця інформація є необхідною для прийняття обґрунтованого рішення щодо забезпечення вибухобезпеки та/або вибухозахисту силосу.

Розв’язання задачі про оптимальне керування рівнем вибухонебезпечності окремо взятого силосу створює передумови для розв’язання задачі про оптимальне керування вибухонебезпекою силосного корпусу в цілому, а в перспективі - про оптимальне керування вибухонебезпекою всього елеватора або іншого зернового підприємства.

Інший напрямок подальших досліджень пов'язано з розглядом таких ситуацій, коли нечітка оцінка відносної вибухонебезпечності ЕПВНО не зводиться до розрахунку довжини переддетонаційної ділянки (як у випадку із нечіткою оцінкою вибухонебезпечності силосу). В цьому випадку суттєво ускладнюється вид цільової функції.

3. Висновки

1. Розглянуто питання про оптимальне керування потенційно вибухонебезпечним об'єктом. Показано, що критерії оптимальності можуть бути різними. Поставлено задачу про оптимальне керування рівнем вибухонебезпечності потенційно вибухонебезпечного об'єкту.
2. Поставлену задачу розв’язано в загальному вигляді для найпростішого випадку, коли оцінка рівня відносної вибухонебезпечності елементарного потенційно вибухонебезпечного об'єкту зводиться до розрахунку довжини переддетонаційної ділянки. Розв’язок задачі реалізовано у вигляді програмного продукту.
3. На комп’ютері реалізовано програму оптимального керування рівнем відносної вибухонебезпечності окремо взятого силосу. Дана програма може стати частиною програмного забезпечення забезпечуючої підсистеми автоматизованої системи керування підприємства із зберігання та переробки зерна.

4. Література References

[1] A. Kovalenko, V. Volkov, Information Model for Potentially Detonative Object, in: CEUR Workshop Proceedings, volume 2683, pp. 50-52, 2019.

[2] V. Volkov, Y. Kryvchenko, Transition of combustion to explosion and decision support systems for explosion protection, in: Lecture Notes in Computational Intelligence and Decision Making, Advances in Intelligent Systems and Computing, volume 1246, Springer, Cham. 2021, pp. 437-447. doi: 10.1007/978-3-030-54215-3.

[3] V. Volkov, Decision support systems on hazards of industrial explosions, in: Seventh International Symposium on Hazards, Prevention and Mitigation of Industrial Explosions: Thirteenth International Colloquium on Dust Explosions and Eighth Colloquium on Gas, Vapor, Liquid, and Hybrid Explosions, St. Petersburg, Russia, 7–11 July 2008, volume 3, pp. 343–347, 2008.

Hardware Errors of the Device for Measuring the Average Value of Voltage of İnfrared Frequencies

Aynur Jamal Jabiyeva[1]

[1]*Azerbaijan State Oil and Industry University, Azadlig str.20, Baku, AZE 1010, Azerbaijan*

Abstract

Electronic A method for accurately measuring the average value of an alternating voltage in the infrared frequency range, based on the use of a high-speed electronic digital DC voltmeter and a controlled rectifier-type converter with an averaging link

Keywords

quasi-stationary mode, hardware errors, silicon diode, linear differential equation

1. Introduction

The methodological errors of the device were analyzed (Fig.1). In this case, the following assumptions were made: -the averaging element I is an ideal RC circuit without parasitic capacitances and leaks; -the electronic digital DC voltmeter has an infinitely large input resistance, zero errors and instantaneous speed; -the control unit for the key and electronic digital voltmeter generates an ideal square-wave key control signal and a start pulse for the voltmeter at the moments of transition of the instantaneous value of the measured sinusoidal signal through the zero level; -the key K has an infinitely large resistance in the open state, infinitely small resistance in the conducting state, and the construction of sources of emf. and there is no current in the key.

Let us consider the hardware errors of the device caused by the violation of these conditions. The main relationship that determines the error of the device is found when considering the process of changing the voltage across the capacitor of the equivalent circuit in Fig. 3, given in [1]

$$\delta = \frac{U_{vv}-U_{average}}{U_{averagt}} = \frac{an^{|}}{2(a^{|}+n^{|})} clt\frac{a}{2} - 1, \quad (1)$$

where $U_{VV} = kclt\frac{a}{2}-$ steady-state voltage value at the output capacitor at the moment of measurement;

$U_{average} = \frac{2U_m}{n}$ -average value of measured voltage:

$$k = \frac{anU_m}{a^{|}+n^{|}};\ a = \frac{T}{2RC} - \frac{n}{\omega\tau};$$

$T = -\frac{2n}{\omega}$ - period of the measured voltage;

$RC = \tau$-is the time constant of the averaging element.

2.Basic information

Changes in the resistance R and capacitance C of the capacitor of the averaging element AND affect the measurement result, since this changes the parameter α, on which the error depends1) If the values of R and C are chosen in such a way that a small value of the error is always ensured δ,then even relatively large (2-3%) changes in R and C, which can actually arise as a result of aging or changes in the temperature of these elements, practically do not affect the measurement result.

In general, the partial relative error δ,due to a change in the value α, (due to the change in R and C), can be found from the expression

$$\delta_\alpha = \frac{1}{U_{voltage\ value}} \cdot \frac{\partial U_{vv}}{\partial \alpha} \cdot \Delta\alpha. \quad (2)$$

Taking into account that

$$U_{vv} = kclh\frac{\alpha}{2} - \frac{\alpha n U_m}{\alpha^{|}+n^{|}} clh\frac{\alpha}{2}, \quad (3)$$

EMAIL: Aynur.Jabiyeva@outlook.com(A. 1);
ORCID: *(0000-0002-0336-8586)

the partial derivative is

$$\frac{\partial U_{VV}}{\partial \alpha} = k\left[clh\frac{\alpha}{2}\left(\frac{1}{\alpha} - \frac{clh\frac{\alpha}{2}}{2}\right) + \frac{1}{2}\right]. \qquad (4)$$

The relative error after transformations has the form

$$\delta_\alpha = \left(1 - \frac{\alpha}{sh\alpha}\right)\frac{\Delta\alpha}{\alpha}. \qquad (5)$$

With real values $\alpha = (0{,}05 - 0{,}3)$ and $\frac{\Delta\alpha}{\alpha}$ (0,02-0,03) this error does not exceed 0.075%.

2. The final value of the input resistance of the digital voltmeter and the leakage resistance of the averaging element capacitor can also be sources of error. It is advisable to take into account the influence of these resistances according to the scheme in Fig. 1, where they are combined into one equivalent resistance Re, connected in parallel with the capacitor C.

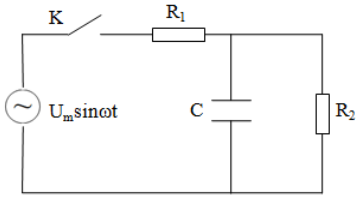


Figure 1: Methodical errors of the device

The output signal - the voltage across the capacitor C - is determined from the difference equation compiled from the differential equations of the circuit in Fig. 1 for cases when the key K is closed and open.

It is convenient to solve this problem by the method of discrete Laplace transform [1].

In quasi-steady-state mode, the voltage across the capacitor U_{vvR} at the moment of opening the key is determined by the expression

$$U_{vvR} = \frac{k_R\left[1+e^{-\alpha_1(1+R_1/R_2}\right]}{1-e^{-\alpha_1(1+2R_1/R_2}}, \qquad (6)$$

where

$$k_R = \frac{U_m \pi \alpha_1}{\pi^2 + \alpha_1^2(1 + R_1/R_2)^2};$$

$$\alpha_1 = \frac{T}{2R_1C}. \qquad (7)$$

Partial relative error $\delta_н$, due to the presence of R2, is expressed as

$$\delta_R = \frac{U_{vvR} - U_{vv}}{U_{уст}} \approx \frac{U_{vvR} - U_{average}}{U_{average}}. \qquad (8)$$

Taking into account (6) and the value $U_{average} = \frac{2U_m}{\pi}$ the expression for the relative error $\delta_н$ will take the form

$$\delta_R = -1 + \frac{\pi^2}{2}\frac{1+e^{-\alpha_1(1+R_1/R_2}}{1-e^{-\alpha_1(1+2R_1/R_2}}\frac{\alpha_1}{\pi^2+\alpha_1^2(1+R_1/R_2)^2}. \qquad (9)$$

If we expand the exponential functions of the numerator and denominator in a series, perform the appropriate algebraic transformations and discard the higher-order terms, starting from the third (since they are small compared to the terms of the first two orders), then (9) is transformed to the form

$$\delta_R \approx -1 + \frac{1}{1+2\frac{R_1}{R_2}} \cdot \cdot\left\{1 + \frac{R_1}{2R_2}\alpha_1 + \alpha_1^2\left[\left(1+\frac{R_1}{R_2}\right)^2 \cdot 0{,}149 + \frac{1}{12}\left(1+\frac{R_1}{R_2}\right)^2 - \left(\frac{1}{4} + \frac{3}{4}\frac{R_1}{R_2}\right) + \frac{1}{2}\left(\frac{R_1}{R_2}\right)^2\right]\right\} \qquad (10)$$

2.1. Problem statement and purpose of work

The dependence of $\delta_н$ on α_1 for different values of the parameter R_1 / R_2 is presented by a family of curves in Fig. 2. From these curves it can be seen that to ensure the partial relative error $\delta_н$ no more than 0.25% at α_1 less than 0.1, it is necessary that the ratio R_1 / R_2 ≤0.01.

To meet this requirement in the package of the device, the dependence of the resistance R2 on the frequency was experimentally determined (this resistance is nonlinear and frequency-dependent due to the specifics of the operation of the adopted ECV).

According to the obtained values of R2, such values of R1 and C were selected, at which sufficiently small errors are combined with a sufficiently short measurement time [1].

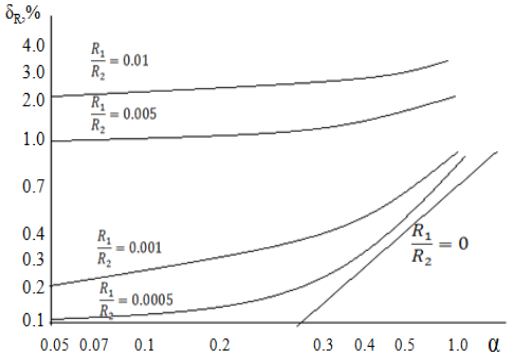


Figure 2: Dependence of $\delta_н$ on α_1 for different values of the parameter R_1 / R_2

3. The influence of the key control unit and an electronic digital voltmeter on the device error can be divided into: the influence of the switching angle (or phase) of the control voltage; the influence of the cutoff angle θ of the control voltage and the influence of the pulse fronts that control the key.

a) The influence of the switching angle ψ is determined from consideration of the circuit in [1] at the input voltage $e = U_m \sin(\omega t + \psi)$ and for different values of the angle ψ. Mathematically, the problem is reduced to solving the difference equation following from the linear differential equation for the voltage u (t) on the capacitor of the circuit in [1] with a closed switch K

$$\tau \frac{du(t)}{dt} + u(t) = U_m \sin(\omega t + \psi). \quad (11)$$

If we take into account the closure and opening of the circuit with the key K at the moments of time 0 and T / 2, then (11) turns into a difference equation of the form

$$U[n+1] - U[n]e^{-\alpha} = Bsin(\varphi - \psi)(1 - e^{-\alpha}) \quad (12)$$

where

$$\alpha = \frac{T}{2\tau}; \quad B = \frac{U_m}{\sqrt{1+\omega^2\tau^2}}; \quad \varphi = arctg\omega\tau.$$

Solution (12) at the intervals of an open switch in a quasi-stationary mode (it is at these intervals that the voltage across the capacitor is measured with an electronic voltmeter) has the form

$$U_{vv\psi} = k_\psi cth\frac{\alpha}{2}, \quad (13)$$

where $k_\psi = Bsin(\varphi - \psi)$.

Partial relative error δ_ψ of the output voltage

$$\delta_\psi = \frac{U_{vv\psi} - U_{vv}}{U_{vv}} = -2sin^2\frac{\psi}{2} - \frac{\alpha}{\pi}sin\psi. \quad (14)$$

As a result of determining the error δ_ψ according to this formula, are shown in Fig. 3 for two values α= 0.1 and 0.25.

b) The influence of the cutoff angle is determined according to the same initial equation as the influence of the switching angle ψ, with the difference that instead of the times of the key operation 0 and T / 2, it is necessary to calculate the circuit when the key is triggered at the moment $\left(\frac{\pi}{2\omega} - \frac{\theta}{\omega}\right)$ and $\left(\frac{\pi}{2\omega} + \frac{\theta}{\omega}\right)$

This somewhat complicates the compilation and solution of the difference equation, without fundamentally changing anything.

The steady-state value of the voltage across the output capacitor in the measurement interval has the form

$$U_{vv\theta} = \frac{U_m}{\sqrt{1+\omega^2\tau^2}}\left(cos\varphi\ cos\ \theta + sin\varphi\ sin\theta\ cth\frac{2\alpha\theta}{2\pi}\right). \quad (15)$$

The relative error δ_θ is equal to

$$\delta_\theta = \frac{\pi\alpha}{\pi^2+\alpha^2}\left[\frac{\alpha}{2}cos\theta + \frac{\pi}{2}\left(sin\theta cth\frac{\alpha\theta}{\pi} - cth\frac{\alpha}{2}\right)\right]. \quad (16)$$

The results of calculating this error for several parameter values are shown in Fig. 3.

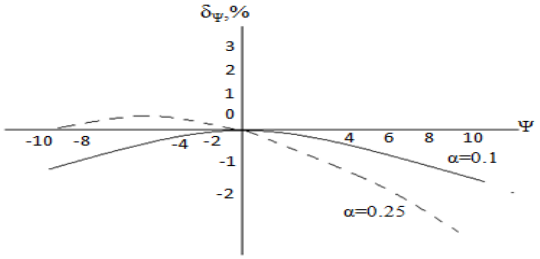


Figure 3: Results of calculating the uncertainty for several values

From the curves in Fig. 3 it can be seen that the moments of supply of the key control impulses have a significant effect on the conversion error. Physically, such a sharp influence on the error is quite natural, since the difference of these moments from the moments corresponding to the change in the sign of the measured voltage (the moments of the transition of the measured voltage through the zero level) directly changes not only the voltage across the capacitor when the switch is open, but also affects the process of changing the instantaneous capacitor voltage values when the switch is closed.

c) The influence of the pulses generated by the key control unit on the device error is also due to the finite value of the duration of the edges of these pulses (the influence of the amplitude of these pulses can be made small by choosing the correct key circuit, for example, with a six-diode key circuit).

Non-identical current-voltage characteristics of the key diodes, as well as non-identical shape of the front and rear the fronts of the control pulse, causes the appearance of switching bursts in the signal at the output of the switch. These bursts do not lend themselves to rigorous mathematical analysis, but are easily detected by an electronic oscilloscope. Due to the fact that switching bursts are frequency-independent, their effect is stronger at high frequencies of the measured voltage.

An experimental study of the device prototype showed that balancing the diode switch (by selecting silicon diodes and introducing a balancing resistance) and using powerful lamps in the output cathode follower of the control unit can easily achieve a short duration (<12 meters per second) and amplitude (<1 / 4Um) of these bursts. These measures, taken in the tested prototype of the device, ensured a negligible influence of the shape of the control pulses at all frequencies below 200 Hz.

1. To consider the influence of the key operation on the error, it is convenient to divide the key operation cycle into three stages: the key conducts, the key does not conduct, and the beak is "thrown over". The third state causes the just considered commutation bursts, and in the first two states an error may arise due to the finite (and not infinitely small or large) switch resistance, as well as due to the appearance of parasitic emf. or current at the output of the key. In the considered device, the final resistance of the conducting switch, practically when using silicon diodes, can always be neglected in comparison with the resistance R1 of the integrating link, since the first resistance is of the order of several ohms, and the second - several hundred or thousands of kilo-ohms. The influence of the final resistance of the open key Rk can be considered in a manner similar to the pleasant one when considering the influence of the resistance R2. In this case, the steady-state value of the voltage at the output capacitor in the measurement interval has the form

$$U_{vvk} = k_1 \frac{1+e^{-\alpha_1}}{1-e^{-\alpha_0}} - k_2 \cdot e^{-\alpha_1} \frac{1+e^{-\alpha_2}}{1-e^{-\alpha_0}}, \quad (17)$$

where $k_{1,2} = \frac{\pm U_m}{\sqrt{1+\omega^2\tau_{1,2}^2}}$;

$$\alpha_{1,2} = \frac{T}{2\tau_{1,2}}; \alpha_0 = \alpha_1 + \alpha_2; \alpha_2 = \alpha_1 \frac{R_1}{R_K},$$

and the conversion error is expressed by the formula

$$\delta_k = \frac{U_{vv} - U_{vv}}{U_{yct}} = -1 + \frac{1-e^{-\alpha_1}}{1-e^{-\alpha_0}} - \frac{k_2}{k_1} e^{-\alpha_1} \frac{(1-e^{-\alpha_1})(1+e^{-\alpha_2})}{(1-e^{-\alpha_0})(1+e^{-\alpha_1})}. \quad (18)$$

Expression (18) with a sufficient degree of accuracy for real values of the parameters α and R_1 / R_K is approximated by the expression

$$\delta_k \cong \frac{R_1}{R_K}. \quad (19)$$

It is clear from (19) that this error when using selected silicon diodes can be small, so that the resistance of the open switch does not affect the overall error of the device.

3 Conclusions

From the above, the following conclusions can be drawn. Equivalent emf a closed switch can have a significant impact, since it is directly added to the measured voltage. The task of balancing the key circuit is to get rid of this emf. Theoretically, this issue does not lend itself to accurate analysis due to the instability and nonlinearity of the current-voltage characteristics of the diodes, but an experimental study of this effect is not difficult. Experiments have shown that daily changes in the equivalent emf the key does not exceed 0.5 mV, and an increase in temperature by 40 ° C (from the value of 200 ° C) causes an emf. not exceeding 5mV. Considering that these switches are intended for use in a device in which the highest value of the measured voltage at the switch output is 10V, then it is clear that such small changes in the equivalent emf. closed key are perfectly valid.

In the open state, a possible source of instrument error is the equivalent output current of a non-conductive switch. However, it can also be brought to a negligible value (in the breadboard, the value of this equivalent current was less than 10-12A). The use of unmatched silicon diodes or diodes of other types limits the upper limit of the value of the resistance R1 of the integrating element.

The carried out consideration of various sources of the device hardware errors (the errors of the electronic digital voltmeter were not considered, since their influence is clear, and they are usually very small) showed that it is easy to fulfill the conditions under which the partial components of the total device error will be small enough and even with a simple arithmetic summation, the total error will not exceed 0.5%.

4. References

[1] Green G.L. Measuring equipment, 1963, №8.

[2] Burgemeister E.A.//Phys. Med.Biol.-2001, - V.26. – N2. – P.269..

[3] Planskoy B.// Phys. Med.Biol.-2000, - N3. – P.519.

[4] Vermeulen L.V., Harris A.J. //J. Appl. Phys.-1998, - V.49. – N2. – P.913.

[5] Pikner G/ Silicon diodes as a detektors relative dosimetry of photon, electron and proton radiation fields.//Thesis, Uppsala, 2003.

Paradigm of Safe Intelligent Ecological Monitoring of Environmental Parameters

Yuriy Bobalo[1], Valeriy Dudykevych[1], Galyna Mykytyn[1], Taras Stosyk[1]

[1]*Lviv Polytechnic National University, Stepana Bandery St, 12, Lviv, 79013, Ukraine*

Abstract

In the context of the development of the 7-year European Union scientific research initiative "Horizon Europe", the paradigm of ecological monitoring of the environment "intellectualization – information security" is proposed. The multilevel paradigm of safe ecological monitoring "intelligent cyber-physical systems (CPS) – integration of CPS levels – information processes of selection, processing, management – threats to information security (IS) – hardware and software security technologies" is a universal in structure and specialized in functionality for the natural environment "water – air – soil – forest". The universal paradigm is revealed by the improved complex model of research monitoring of ecological parameters of water "program – intelligent technology (IT) and IS – methodology". The informational security model of the three-layers structure of the Internet of Things based on the concept "object – threat – protection" provides secure interaction between sensors and devices for ecological monitoring of environmental parameters with computer systems. The created paradigm is the basis for the development of approaches to safe intellectualization of ecological monitoring of environmental components using intelligent systems and technologies to ensure basic safety profiles.

Keywords

Intellectualization, information security, ecological monitoring, intelligent cyber-physical system, paradigm, water, complex model of monitoring, Internet of Things, informational security model.

1. Introduction

Problem formulation. In the conditions of technological development of civilization, the complex of global problems of planetary scale is evolving. One of them is the safety of human life under the influence of natural and man-made threats. Public safety, in particular, is determined by the vector of information and technical condition of critical infrastructure, the disruption of which can lead to impacts on natural ecosystems and losses. The quintessence of solving this problem is the structure "intellectualization – information security – ecological monitoring" within the basic principles: Ukrainian strategy Industry 4.0, Concept of information security of Ukraine, European Union scientific research initiative "Horizon Europe" (2021 – 2027) [1, 2, 3]. The safety of environmental components – water, air, soil, forests – is ensured by the implementation of models of safe ecological monitoring based on intelligent CPS.

Analysis of recent achievements and publications. The strategy of the state ecological policy of Ukraine is aimed at the implementation of: comprehensive ecological monitoring of the condition of the environment and improvement of the system of information support of the management decision-making process [4].

In this regard, the relevant segment is the use of intelligent ecological monitoring systems of environmental components and the implementation of information security technologies, which comprehensively form the tools of environmental security, which is a component of national security of Ukraine and the vector of sustainable development of Ukraine.

EMAIL: rector@lpnu.ua; vdudykev@gmail.com; cosmos-zirka@ukr.net; taras.r.stosyk@lpnu.ua
ORCID: 0000-0001-9185-7074; 0000-0001-8827-9920; 0000-0003-4275-8285; 0000-0001-7896-9792

Intelligent informational measuring systems are effectively used for ecological monitoring [5], as well as geo-information and aerospace technologies, which carry out: registration of ecological parameters of environmental components, rapid analysis, processing, preservation, identification, intelligent decision support [6].

The principles of construction of wireless sensor networks (WSN) for ecological environmental monitoring are developed. In paper [7] WSNs, based on the method of coordinate routing, which takes into account the interaction of sensor nodes and intellectualization of decision-making processes at OSI levels and management functions, were developed.

Progressive are the scientific and technical developments of the National Academy of Sciences of Ukraine in the field of creating sensors for ecological research, intelligent systems for monitoring of environmental parameters [8].

The development of tools for intellectual ecological monitoring at the international level continues. The paper [9] presents trends in the use of IT for monitoring air, water, radiation pollution, including sensors, IoT, machine learning methods.

IoT based smart water quality monitoring system is presented in [10] structurally: sensor for measuring water parameters (temperature, pH, turbidity), Zigbee WSN for data transferring, central processing unit, main data storage module, displaying information for users. Also in this paper known sensors for the environmental water monitoring system were analysed and the permissible limits of drinking water parameters according to the recommendations of the WHO and the Environmental Protection Agency (WHO/USEPA) were highlighted.

The publication [11] considers the structure of smart ecological monitoring of water, air, soil based on IoT platform according to the IEEE 1451 standard and data flow modeling.

Intelligent technologies of ecological monitoring of the environment must be dependable – to meet the requirements of functional and information security by the standard SOU-N NSAU 0060:2010.

The goal of the work. The aim of the work is to create a paradigm of ecological monitoring "intellectualization - information security", which is the basis of safe research monitoring of water quality "program – IT – IS – assessment methodology" and information model of security of the three-layer architecture of IoT.

2. Paradigm of ecological monitoring: "intellectualization – information security"

The multilevel paradigm of ecological monitoring of the environment "intellectualization – information security" created on the basis of the concept "object – threat – protection" is the development of methodological principles of monitoring components – water, air, soil, forests. (Fig. 1).

The first level – functionality of the structure "component of the environment – operating technologies" / "objects ($O_{1\text{-}N(R,S,T)}$) – cyber-physical systems ($CPS_{1\text{-}N(R,S,T)}$)" according to the components – water (W), air (A), soil (S), forests (F). The second level – integration of the levels of the CPS "Internet of Things ($IoT_{1\text{-}N(R,S,T)}$) – wireless technologies ($WT_{1\text{-}N(R,S,T)}$) – computer systems ($CS_{1\text{-}N(R,S,T)}$)". The third level – processes of "information selection ($S_{1\text{-}N(R,S,T)}$)/ monitoring – transmission/reception ($T_{1\text{-}N(R,S,T)}/R_{1\text{-}N(R,S,T)}$) – information processing ($P_{1\text{-}N(R,S,T)}$) / management ($M_{1\text{-}N(R,S,T)}$)". The fourth level – IS threats at the structural and functional levels of the CPS $a_{1\text{-}N} – b_{1\text{-}N} – c_{1\text{-}N}$ (water monitoring); $d_{1\text{-}R} – e_{1\text{-}R} – f_{1\text{-}R}$ (air monitoring); $g_{1\text{-}S} – h_{1\text{-}S} – i_{1\text{-}S}$ (soil monitoring); $k_{1\text{-}T} – l_{1\text{-}T} – m_{1\text{-}T}$ (forest monitoring). Fifth level – hardware and software security technologies in the profiles "confidentiality – integrity – accessibility" $A_{1\text{-}N} – B_{1\text{-}N} – C_{1\text{-}N}$ (W); $D_{1\text{-}R} – E_{1\text{-}R} – F_{1\text{-}R}$ (A); $G_{1\text{-}S} – H_{1\text{-}S} – I_{1\text{-}S}$ (S); $K_{1\text{-}T} – L_{1\text{-}T} – M_{1\text{-}T}$ (F) according to DSTU ISO/IEC 15408.

Secure data collection by intelligent sensors or sensors that interact with objects as components of the environment and the exchange of information in intelligent ecological monitoring technology are carried out by the Internet of Things (CPS physical space) and wireless technologies (CPS communication environment).

The computer system (CPS cyberspace) provides data storage, analysis, processing, identification, forecasting and, on this basis, management of the state of the environment.

The paradigm of safe intellectualization of ecological monitoring of environmental components is the basis for building comprehensive security systems for intelligent systems based on the concept of "object – threat – protection".

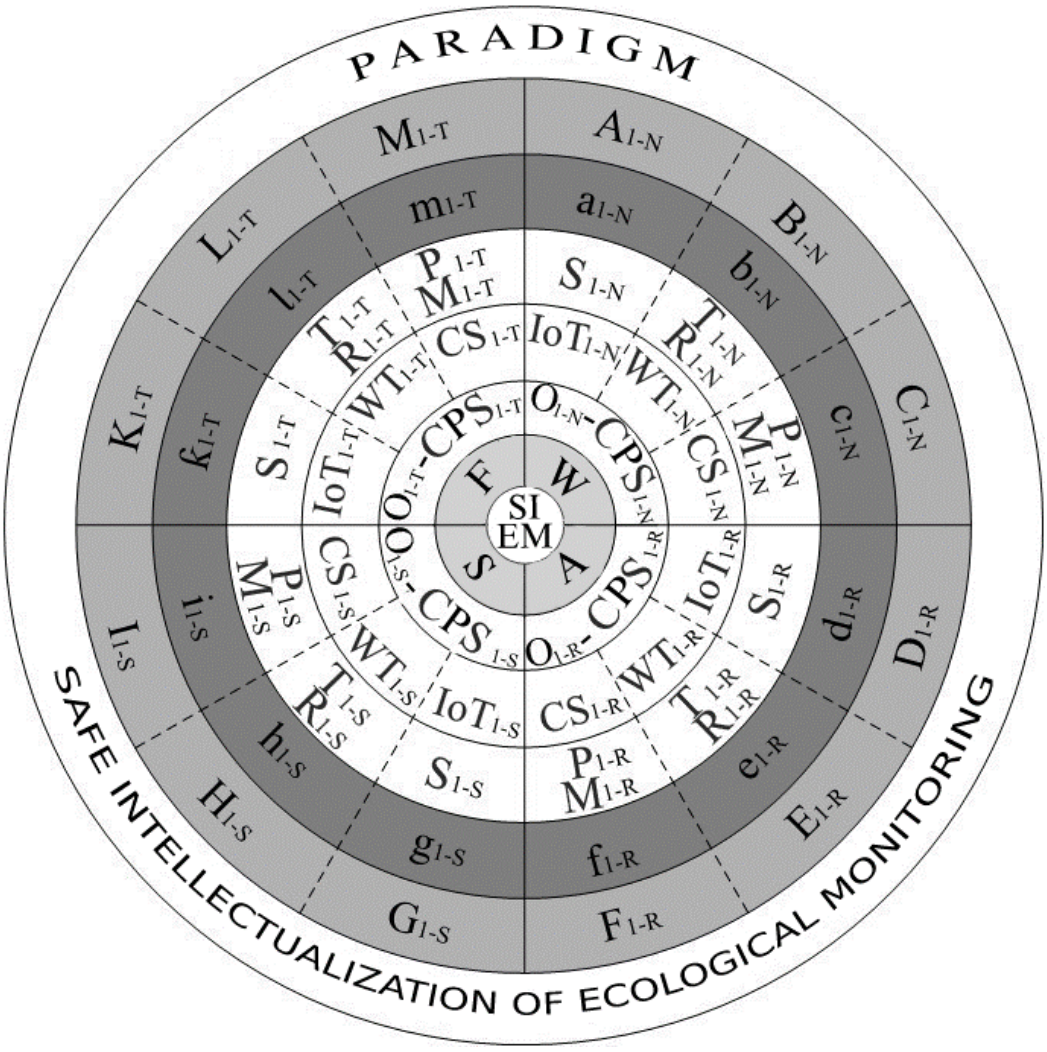


Figure 1: Paradigm of safe intellectualization of ecological monitoring

2.1. Research ecological monitoring of water: complex model "program – IT – IS – methodology"

According to DSTU 3041-95, water monitoring is an observation of the state of natural water and its evaluation. In order to ensure water quality and apply the model of environmental management system, Ukraine has implemented standards DSTU 7525: 2014 and DSTU 14004: 2016, which respectively establish requirements and methods of drinking water quality control and a systematic approach to ecological management in sustainable development and environmental management. The methodological approach to assessing the current state of water quality provides appropriate methods and tools for ecological monitoring: determination of water parameters (registration / measurement), assessment of ecological characteristics of water, forecasting and management decisions on the state of the water. Standardized technologies are used to monitor the set of water parameters, in particular the standard DSTU ISO 15923-1: 2018 describes the use of discrete analysis systems to determine individual environmental parameters. Water quality control with the use of IT ecological monitoring, secure cyber-physical systems, is important and relevant. In order to assess the set of drinking water parameters, research monitoring has been developed at the level of a comprehensive model "program – IT – IS – methodology". In terms of intelligent technologies and information security, a comprehensive model of research monitoring includes: 1) MEMS sensors (microelectromechanical systems), integrated into intelligent informational measuring systems, which are designed for remote sampling of water and its environmental parameters and wireless transmission (DSTU-P CEN/CLC/ETSI/TR

50572:2020) and, on this basis, the creation of databases, information processing and decision-making; 2) security technologies of intelligent systems under the influence of threats to confidentiality, integrity, accessibility, in particular at the IoT level, which provides algorithmic and software interaction between sensors and devices with computer systems (Fig. 2) [12, 13, 14].

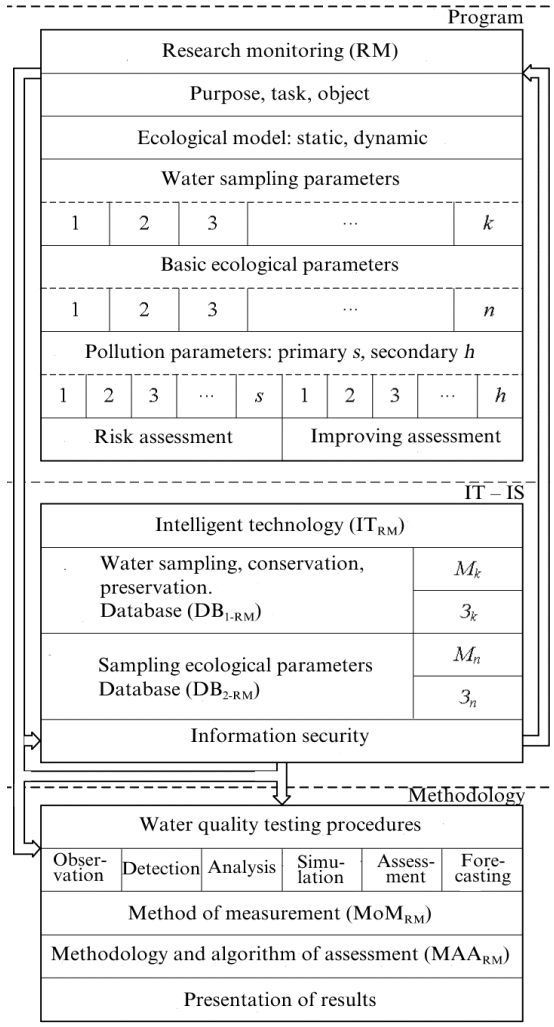


Figure 2: Research monitoring of drinking water parameters

The approach to the assessment of physicochemical and biological properties of drinking water under man-caused influence is determined by the system of regulations:

Standards: DSanPiN 2.2.4-171-10, GOST 27384-2002, DSTU 4808:2007, DSTU 3831-98, DSTU 10260:2007, GOST 8.556-91, GOST R 52180-2003, GOST R 52181-2003, DSTU GOST 18294-2009, DSTU ISO 9377-2:2015.

Experimental conditions:

1. taking into account the system of factors influencing drinking water;
2. water sampling, transportation, canning, storage.

Methodology – method, means, technique:

1. measurement of water parameters, processing, presentation of results;
2. methods and tools for selection of physicochemical and biological parameters of water:
   - methods – selective, multicomponent (atomic emission, X-ray, spectral analysis, chromatography), etc.;
   - tools: conductometers, pH-meters, ionometers, ORP-meters, photoelectric colorimeter, gas chromatographs, automated natural water quality control systems (DSTU 3831-98), laser measuring systems, intelligent informational measuring systems, intelligent geoinformational systems.
3. the result of measuring N-standard:
   - maximum allowable concentration of harmful substances in water (MAC_H);
   - maximum allowable concentration (MAC);
   - maximum allowable emissions (MAE);
   - maximum allowable discharges (MAD);
   - measurement error Δ, range Δ_U, Δ_L; P;
   - for physicochemical: P = 0,95; for biological: P = 0,9;
   - accuracy: $S_L + \Delta_U < MAC$, S_L – device sensitivity threshold.
4. technologies for restoring the properties of water: filters, activators, magnetohydrodynamic systems, biotechnology, etc.

2.2. Informational model of security of three-layer architecture of the Internet of Things

The Internet of Things is one of the intelligent technologies for ecological monitoring of the natural environment. The Internet of Things consists of a large number of different devices, networks and technologies that are sometimes difficult to combine. Accordingly, today there is no single common IoT architecture. However, of all the proposed IoT architectures, the most widely recognized and widespread is the three-layer structure [15, 16]. Based on it, an informational model of Internet of Things security in intelligent ecological monitoring systems was

built, according to standard ETSI TS 103 645 from European Telecommunications Standards Institute (Fig. 3).

The perception layer is the physical level of the IoT architecture. In the context of intelligent CPS-based ecological monitoring, the perception layer consists of sensors and external devices that collect information about the state of environmental components for further transmission. This level is the most vulnerable to attacks due to the possibility of gaining direct physical access to devices operating outside the controlled area. The main threats are node capture and fake node injection. To protect against those attacks security measures, such as asymmetric cryptography (does not allow to obtain a key from the captured node), physical protection and authentication of devices, are provided.

The network layer is responsible for transmitting and processing environmental information collected by sensors at the perception layer. The main threats at this level are DDoS attacks and eavesdropping, including man-in-the-middle. Security measures include multi-factor authentication, wireless encryption, traffic analysis using an intrusion detection system and the organization of a separate network.

The application layer is responsible for processing information received from the network layer, controlling devices and interacting with users. The key issue of information security at this layer is the vulnerability of the software and the implementation of malicious code. Countermeasures include the use of trusted software components, an application-level firewall, and an access control list (ACL).

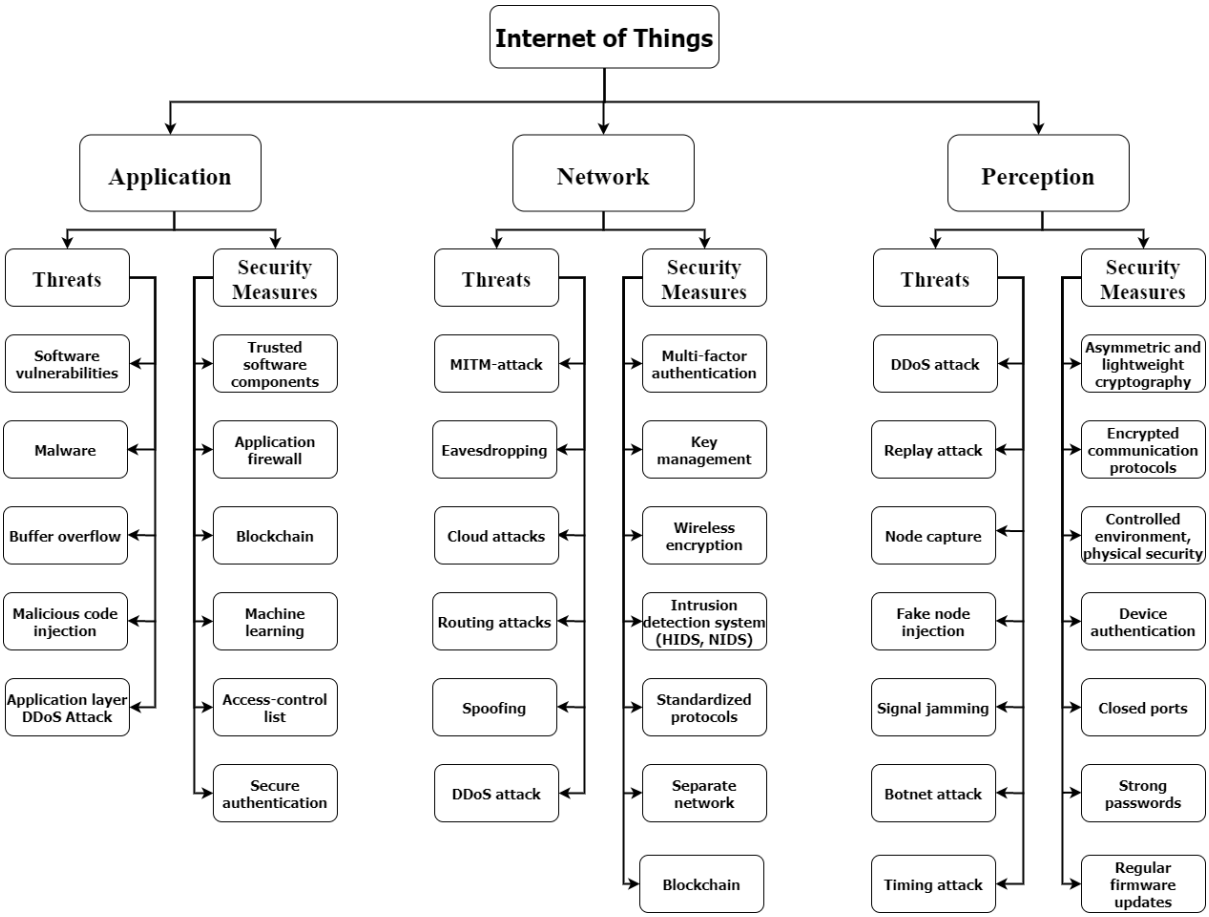


Figure 3: Informational model of security of three-layer architecture of the Internet of Things

3. Conclusions

The paper presents a single methodology for safe ecological monitoring of environmental components: 1) universal paradigm "intellectualization – information security"; 2) a comprehensive model of research monitoring of drinking water quality; 3) informational model of Internet of Things security, which allows the development of approaches and models for monitoring air, soil, forest on the basis of

intelligent systems and the construction of integrated security systems by profiles – confidentiality, integrity, accessibility.

4. References

[1] Yurchak Oleksandr. Ukrayins'ka stratehiya Industriyi 4.0 – 7 napryamiv rozvytku [Elektronnyy resurs]. – Rezhym dostupu: https://industry4-0-ukraine.com.ua/2019/01/02/ukrainska-strategiya-industrii-4-0-7-napriankiv-rozvutku/.

[2] Proekt Kontseptsiyi informatsiynoyi bezpeky Ukrayiny. – [Elektronnyy resurs]. – Rezhym dostupu: http://mip.gov.ua/done_img/d/30-project_08_06_15.pdf.

[3] Horizon Europe. The next eu research & innovation investment programme (2021–2027). URL: https://ec.europa.eu/info/sites/default/files/research_and_innovation/strategy_on_research_and_innovation/presentations/horizon_europe_en_investing_to_shape_our_future.pdf.

[4] Pro osnovni zasady (ctratehiyu) derzhavnoyi ekolohichnoyi polityky Ukrayiny na period do 2030 roku. – Zatverdzheno Zakonom Ukrayiny vid 28 lyutoho 2019 roku # 2697 – VIII. – [Elektronnyy resurs]. – Rezhym dostupu: https://zakon.rada.gov.ua/laws/show/2697-19#Text.

[5] Kropyvnytskyi V., Pavlyshyn M., Chumak V. Vysokomobil'na laboratoriya ekolohichnoho monitorynhu – [Elektronnyy resurs]. – Rezhym dostupu: https://ns-plus.com.ua/2017/06/13/vysokomobilna-laboratoriya-ekologichnogo-monitoryngu/.

[6] Trysniuk V.M., Okhariev V.O., Trysniu T.V, Smetanin K.V., Holovan Yu.M. Stvorennya systemy mobil'noho ekolohichnoho monitorynhu // Ekolohichna bezpeka ta zbalansovane resursokoryt·stuvannya. – №2 (18). – 2018. – S. 118 – 125.

[7] Lysenko O.I. Rozrobka pryntsypiv pobudovy bezprovodovykh sensornykh merezh iz samoorhanizatsiyeyu dlya monitorynhu parametriv navkolyshn'oho seredovyshcha. – [Elektronnyy resurs]. – Rezhym dostupu: https://report.kpi.ua/uk/0115U000269.

[8] Perspektyvni naukovo-tekhnichni rozrobky NAN Ukrayiny. – Ekolohiya ta okhorona dovkillya. – [Elektronnyy resurs]. – Rezhym dostupu: https://www.nas.gov.ua/RDOutput/UA/book2017/Pages/sd.aspx?SRDID=02.

[9] Silvia Liberata Ullo, G. R. Sinha. Advances in Smart Environment Monitoring Systems Using IoT and Sensors // Sensors 2020, 20(11), 3113. doi:10.3390/s20113113.

[10] Farmanullah Jan, Nasro Min-Allah, Dilek Düştegör. IoT Based Smart Water Quality Monitoring: Recent Techniques, Trends and Challenges for Domestic Applications // Water 2021, 13(13), 1729. doi: 10.3390/w13131729.

[11] Tércio Filho, Luiz Fernando, Marcos Rabelo, Sérgio Silva, Carlos Santos, Maria Ribeiro ,Ian A. Grout, Waldir Moreira, Antonio Oliveira-Jr. A Standard-Based Internet of Things Platform and Data Flow Modeling for Smart Environmental Monitoring// Sensors 2021, 21(12), 4228. doi: 10.3390/s21124228.

[12] Stvorennya mikroelektronnykh datchykiv novoho pokolinnya dlya intelektual'nykh system / Ya. I. Lepikh, Yu. O. Hordiienko, S. V. Dziadevych [et al.]. – Odesa: Astroprint, 2010. – 256 s.

[13] Intelektual'ni vymiryuval'ni systemy na osnovi mikroelektronnykh datchykiv novoho pokolinnya / Ya. I. Lepikh, Yu. O. Hordiienko, S. V. Dziadevych [et al.]. – Odesa: Astroprint, 2011. – 351 s.

[14] Vashpanov Yu. O. Suchasni sensory avtomatychnykh system: navch. posib. / Yu. O. Vashpanov – Odesa: VMV, 2014. – 240 s.

[15] Miao Wu, Ting-Jie Lu, Fei-Yang Ling, Jing Sun and Hui-Ying Du, "Research on the architecture of Internet of Things," 2010 3rd International Conference on Advanced Computer Theory and Engineering(ICACTE), 2010, pp. V5-484-V5-487, doi: 10.1109/ICACTE.2010.5579493.

[16] Quandeng Gou, Lianshan Yan, Yihe Liu. Construction and Strategies in IoT Security System. Green Computing and Communications (GreenCom), 2013 IEEE and Internet of Things (iThings/CPSCom), IEEE International Conference on and IEEE Cyber, Physical and Social Computing, 2013, pp. 1129-1132.

Legal Aspects of Blockchain Technology Regulation in the Financial Sphere

Kateryna Tokarieva [1], Nataliya Vnukova[2], Volodymyr Aleksiyev[3]

[1] *Scientific and Research Institute of Providing Legal Framework for the Innovative Development of the National Academy of Legal Sciences of Ukraine, Chernyshevskaya st., 80, Kharkiv, 61002, Ukraine,*
[2,3] *Simon Kuznets Kharkiv National University of Economics, Nauky Avenue, 9A, Kharkiv, 61166, Ukraine*

Abstract
The article is devoted to the investigation of legal aspects of distributed registry technology (blockchain). It is proposed to create a legal environment that facilitates the introduction of distributed registry systems in the financial sector by defining systems as a set of devices that are independent of each other and carry out the formation of digital records of registration, storage and accounting of digital data.

Keywords
legal regulation, blockchain, technologies, cryptocurrency.

1. Introduction

The rapid development of technology has led to the emergence and development of new legal relations in all spheres of public life. In particular, the emergence of blockchain technology (or distributed registry system) and its use in many areas of activity have formed a new type of socio-economic relations, which currently require appropriate legal regulation.

Indicate that the governments of many countries in the world pay attention to the priority of implementing the above technology in existing information exchange systems, tax integration, payment systems and more. This conclusion is based on studies conducted by Deloitte [1]. Depending on this, we can state the need to form a new regulatory environment through which a favorable legal regime for the functioning of modern technologies, including in the financial sector.

Areas of formation of a new regulatory environment are:

(1) removal of legal restrictions that hinder the development of the digital economy;

(2) definition of basic legal concepts,

(3) ensuring equal opportunities in the identification and authentication of individuals and legal entities, which will increase the efficiency of management of economic processes by legal measures.

In order to form such a regulatory environment, it is necessary to adopt a number of new regulations aimed at regulating relations in the financial sector, as well as to amend existing legislation.

2. Problem setting

In view of the above, there is now a need not only to cover the legal aspects of the use of blockchain technology in the financial sector, but also to provide proposals for regulatory regulation of such relations. In addition, it should be noted that in 2020, attacks on blockchain platforms took first place, which indicates the active interest not only of society but also of cybercrime. This approach makes additional demands on the settlement of legal aspects in the use of distributed networks, smart contracts based on blockchain technologies. Therefore, the urgent task of research is the synergy of issues related to the legal aspects of regulation of blockchain technology in the financial sector with technical solutions to ensure the security of blockchain technology.

3. Methodology

To solve the research problem, it is proposed to use the method of system analysis, which provides identification of approaches to financial and legal regulation of the implementation of distributed registry systems, taking into account the scientific concepts of domestic and foreign scientists. With the help of the formal-legal method, the problem related to the formulation of the concept of "distributed registry system", "digital currency" and the identification of the subjective composition of the participants in these systems. The theory of protection and the laws of synergy propose the definition of transaction security requirements in financial systems based on blockchain technology.

The comparative legal method allows us to trace the changing roles of states in the regulation of relations using blockchain technology and analyze such transformations.

4. Results

Obviously, the advantages of integrating blockchain technology into various areas of public administration include:

reduction in economic costs, time and complexity in intergovernmental and public-private information exchange, which enhances the administrative function of governments;

reduction of bureaucracy, discretion and corruption due to the use of distributed registers and programmed smart contracts;

increasing the level of automation, transparency, auditability and accountability of information in state registers in the interests of citizens;

increasing the confidence of citizens and companies in government programs and the introduction of documentation, due to the use of algorithms that are no longer under the sole control of the government [2, 64]. With this in mind, it can be stated that with the help of blockchain technology, trusting, direct and to some extent decentralized relations between citizens and government entities are formed.

But it is necessary to take into account the technical "mistakes" of modern exchanges / platforms based on the use of blockchain and cryptocurrencies, which are formed by a hierarchical structure (as well as banking systems), and only then use distributed networks and blockchain technology to form smart contracts and mining. This approach allows in 2020 to break the hierarchical superstructure and use threats to automated banking systems (ABS) of banking sector organizations (BSO) with signs of synergy and hybridity. Figure 1 shows a block diagram of a synergistic threat model that takes into account threats to the components of security (cybersecurity (CB), information security (IS) and IT-security) [10,11].

In the current national legislation of Ukraine there is no definition of the category "distributed registry system", however, it is basic in this context, as the use of this technology is the introduction of new tools and institutions. In addition, we believe that the very definition of distributed registry technology will allow to correctly determine the legal regime of cryptocurrency / digital and virtual assets and relations in the field of their application.

Based on the analysis of the essence of distributed registry technology, we consider the most successful approach, in which the latter is considered not as a payment system, but directly as a set of devices that are independent of each other and generate digital records of registration, storage and accounting of digital data.

Indicias of the distributed register system are: decentralization, non-mandatory existence of a central body, the absence of intermediaries in the process of such a system, equality of participants and their agreement.

It is widely believed that the use of a distributed registry system in the financial sector is primarily associated with cryptocurrencies (digital or virtual assets). However, these categories are not identical in content.

We are of the opinion that their research and ratio should be conducted taking into account the technological and economic nature. The study of the technological nature of virtual assets and cryptocurrency is appropriate given that their creation is possible only on the basis of appropriate technologies. Clarification of the economic and legal nature will determine the economic essence of cryptocurrencies as one of the modern financial instruments and regulate its functioning within the modern legal field.

Thus, within the analysis of the economic component of the economic and legal nature of the virtual asset of the distributed register, it is necessary to consider the virtual asset of the distributed register from the standpoint of its compliance with the tool by which systems and accounting tokens [8, p. 8].

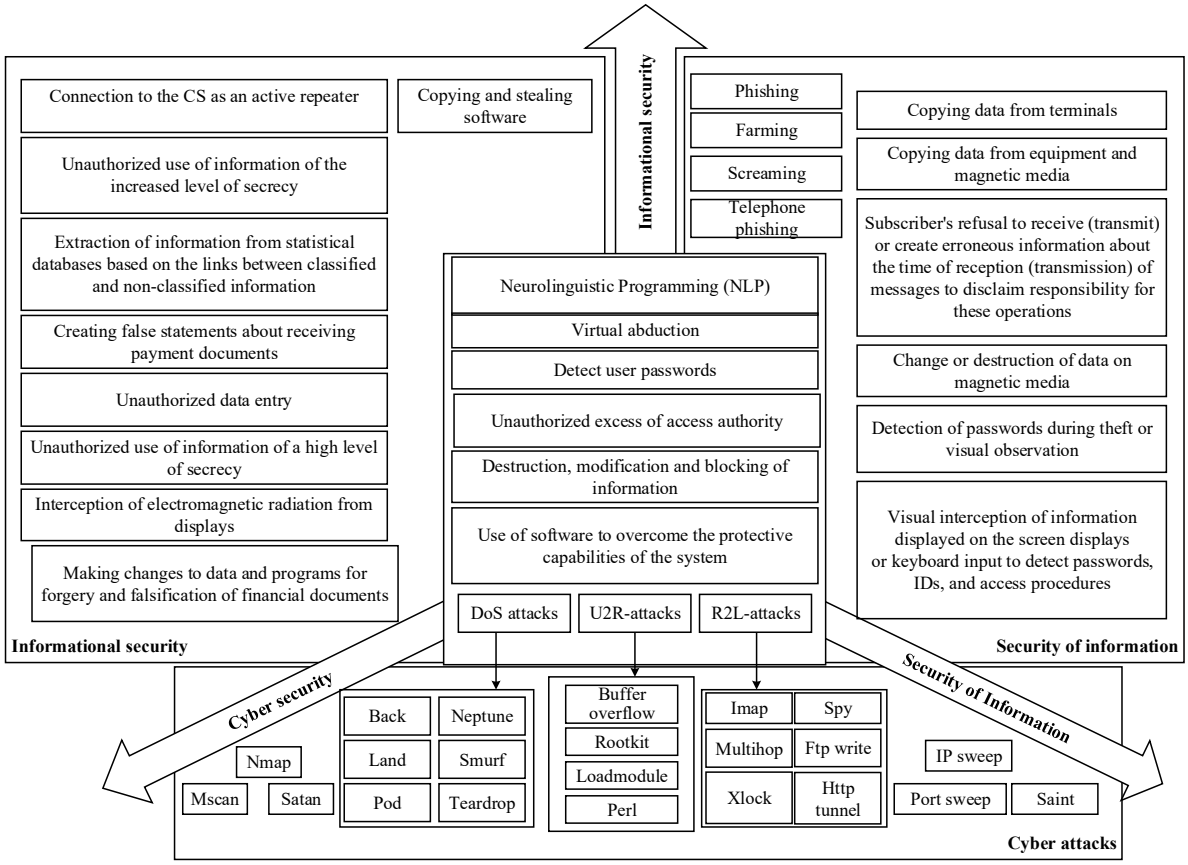


Figure 1 - Synergetic model of security threats

At the same time, regarding the legal nature of the studied phenomena in the world, several basic concepts are identified to determine the legal nature of a virtual asset, in particular, it is about considering the latter (and regulation at the legislative level, respectively) as: 1) means of payment; 2) currency; 3) goods; 4) tangible assets; 5) securities. We also emphasize that some countries around the world are open to the introduction of such a phenomenon, and some – per contra. As can be seen, this is due to many factors, including the form of the state, the form of government, the state regime.

In Japan, at the legislative level, cryptocurrency is considered as a means of payment and is fixed as a value used to fulfill obligations to purchase or borrow goods or services for the benefit of others transmitted by an electronic data processing system, provided that its value is limited to a value recorded on an electronic device or in any electronic form, and does not include Japanese or foreign currencies or assets denominated in such currencies. [3].

Another approach is chosen in China. In particular, the government has taken a number of steps to curb the use of cryptocurrency. First, statements have been published on local exchanges to stop trading cryptocurrencies and to prevent their extraction. Second, access to online platforms and mobile applications that offer cryptocurrency exchange services is blocked. Third, financial institutions and third-party payment transfer operators are prohibited from accepting, using or selling such currency. At the same time, the People's Bank of China tested its own cryptocurrency, striving to become the first major Central Bank, issued digital money under full control over digital transactions [4].

Thus, at a certain stage, China joined the states that are interested in the introduction of cryptocurrency, but with certain features - maintaining a centralized approach to their regulation, which, in our opinion, contradicts the essence of the use of blockchain technology.

Ukraine has not yet formed a unanimous approach to determining the legal regime of cryptocurrency (virtual / digital assets). It is noteworthy that several bills on the legal regulation of cryptocurrency (virtual / digital assets) have been registered, in particular, the following draft Laws of Ukraine: a) "On tokenized assets and cryptocurrencies" № 4328 of 05.11.2020 [5];) "On virtual assets" № 3637

dated 11.06.2020 (adopted in the first reading, finalized within the second reading). [6]

The latest bill is no longer about cryptocurrency, but about a virtual asset, which is defined as a special type of property that is valuable in electronic form, exists in the circulation of virtual assets, and may be in civil circulation. Virtual assets can be secured and unsecured [6, Art. 1]. Thus in h. 1 Art. 4 of the said bill states that virtual assets are property, the peculiarities of the circulation of which are determined by the Civil Code of Ukraine and this Law.

In our opinion, such a position is considered quite constructive given not only the essence of this category, but also the fact that in the national legal field in modern conditions it is the most relevant option of legal regulation. When defining virtual assets as property in the context of taxation, it is advisable to talk about the establishment of a legal mechanism of income tax / income tax on transactions with such property [7, p. 175; 9]. In this context, issues related to the taxation of virtual assets need to be comprehensively studied.

The legal status of participants in distributed registry systems requires a separate legal study. We emphasize that the range of such participants and, accordingly, their legal status will vary depending on what kind of relationship in the financial sphere. We emphasize that the studied technology is peer-to-peer, which provides an opportunity to include in the circle of participants (users) of the distributed registry systems not only legal entities but also individuals. Such a system is based on equal rights of participants (unlike "classic" banking, currency relations, etc., in which there is always an authorized entity), which significantly changes the content of such relations.

It should be emphasized that along with a positive assessment of the use of new technologies in almost all spheres of public life, and financial, in particular, it should be noted the presence of certain risks that occur. In our opinion, first of all, the risks of untested business models, the high potential for abuse of rights by the relevant participants in such relations, fraud, the lack of an effective mechanism for protecting information (data) provided by entities to the relevant registers. To ensure the safety of participants in relations that are formed and developed with the help of blockchain technology, high-quality technical support and an effective legal mechanism for regulating such relations are needed. The primary task of creating a system of legislation in the field of innovative technologies in the financial sector is the formation of an effective legal mechanism for leveling possible financial risks and consumer protection.

In addition, it is necessary to take into account the risks associated with existing and threats of the post-quantum period (which will occur with the advent of a full-scale quantum computer, with its ability to break modern symmetric and asymmetric security algorithms used not only in ABS, but and in distributed networks and systems based on blockchain technology, this approach will ensure that critical target threats on cryptocurrency exchanges / platforms are taken into account in legislation and regulations.

5. Conclusions

It is proposed to create a legal environment that facilitates the introduction of distributed registry systems in the financial sector by defining systems as a set of devices that are independent of each other and carry out the formation of digital records of registration, storage and accounting of digital data. In addition, it is proposed to take into account the impact of current targeted threats with signs of synergy and hybridity on the infrastructure elements of networks / systems based on blockchain technology.

6. References

[1] Blockchain in Public Sector Transforming government services through exponential technologies. Deloitte, FICCI. January 2018. URL: https://www2.deloitte.com/content/dam/Deloitte/in/Documents/public-sector/in-ps-blockchain-noexp.pdf

[2] A. Kud, M. Kucheriavenko, Y. Smychok, Digital assets and their legal regulation in the light of the development of blockchain technology, Right, Kharkiv, 2019. 216 p.

[3] Clifford Chance. The fintech market in Asia pacific – an overview. URL: https://financialmarketstoolkit.cliffordchance.com/content/micro-facm/en/financial-markets-resources/resources-by-type/guides/the-fintechmarket-in-asia-pacific--june2017/_jcr_content/parsys/download/file

.res/The%20fintech%20market%20in%20Asia%20pacific_LR.pdf
[4] Glazer, Phil. State of Global Cryptocurrency Regulation. January 2018. URL: https://hackernoon.com/state-of-globalcryptocurrency-regulation-january-2018-6e03dea0f036
[5] Draft Law of Ukraine "On tokenized assets and cryptocurrencies" No. 4328, 2020. URL: http://search.ligazakon.ua/l_doc2.nsf/link1/JI03596A.html.
[6] Draft Law of Ukraine "On Virtual Assets" No. 3637, 2020. URL: http://w1.c1.rada.gov.ua/pls/zweb2/webproc4_1?pf3511=69110.
[7] K. O. Tokarieva, Some issues of legal regulation of cryptocurrency, in: Actual problems of business activity in the conditions of development of economy, 2021, 171–177.
[8] A. Kud. Comprehensive classification of virtual assets, 2021. URL: https://virtualasset.science/kompleksna-klasifikacziya-virtualnikh-aktiviv.pdf?fbclid=IwAR3wm4R3PKIFWTbDKLdBTN6Qg5MolzuS_JXwvjfO1PW4NcwXxqUl76S76bo.
[9] O. O. Dmytryk, M. P. Kucheriavenko, O. O. Holovashevych, Cryptocurrency: development, features, classification, Financial and credit activities: problems of theory and practice, volume 3, number 30, 2019, 361–370. URL: http://fkd.org.ua/article/view/179737.
[10] Hryshchuk R., Construction methodology of information security system of banking information in automated banking systems : monograph / R. Hryshchuk, S. Yevseiev, A.Shmatko // Vienna.: Premier Publishing s. r. o., 2018. 284 p.
[11] Edited by Serhii Yevseiev, Volodymir Ponomarenko, Oleksandr Laptiev, Oleksandr Milov. Synergy of building cybersecurity systems: monograph / S. Yevseiev, V. Ponomarenko, O. Laptiev, O. Milov and others. – Kharkiv: PC TECHNOLOGY CENTER, 2021. – 188 p.
[12] Pukala R., Hlibko S., Vnukova N., Davidenko D., Usage of E-Technologies to Enhance Infocommunication in Financing Innovation // *International Scientific-Practical Conference Problems of Infocommunications. Science and Technology, PIC S&T'2019*, October 8-11, 2019 Kyiv, Ukraine.

Improving the Stability of Cryptographic Algorithms on Algebraic Lattices

Olha Petrenko [1], Oleksii Petrenko [2]

[1] Kharkiv National University of Radio Electronics, Nauky Ave. 14, Kharkiv, 61166, Ukraine
[2] Ivan Kozhedub Kharkiv National Air Force University, Sumska Str. 77/79, Kharkiv, 61023, Ukraine

Abstract
The paper considers a way to increase the stability of the NTRU Encrypt algorithm by replacing the uniform distribution with a normal one when generating encryption keys to increase the stability of transformations. The use of fast Fourier sampling to reduce the number of operations when performing encryption is justified.

Keywords
Algebraic lattices, NTRU Encrypt algorithm, fast Fourier transform, normal distribution.

1. Introduction

With the constant process of improving quantum computers, which leads to increase in the number of qubits, the classic encryption algorithms can be rapidly hacked. [1] Given this, there is a necessity of developing and further improving of the algorithms, which are able to counteract cryptanalysis in the post-quantum period. The question of defining and substantiating the size of their parameters and conditions of application for solving various applied problems remains relevant. With the practical application of the algorithms, there are problems associated with end-to-end encryption, such as encrypting messages between the UAV and the ground workstation. In solving the tasks, it is necessary to use fast algorithms that can work effectively in the post-quantum period. Finding new solutions to protect information in the post-quantum period and improving existing algorithms by increasing their cryptographic stability is a task that is relevant today.

Algorithms that use transformations on algebraic lattices, the stability of which is based on solving NP-complexity problems, have become an alternative to classical algorithms in fields and rings.

NP-complexity problems include the following tasks: finding the shortest lattice vector (SVP - Shortest Vector Problem) or finding the (approximately) shortest independent vectors (SIVP – Shortest Independent Vectors Problem) [2]. The essence of these problems is to find in a given basis of the algebraic lattice of a nonzero vector that close to a certain normal.

The aim of this article is developing tools of increasing the stability of the algorithm on algebraic lattices, the NTRU algorithm exactly, without effect on its performance

2. Algebraic lattices and fast Fourier transform.

Algebraic lattices have become a convenient tool for cryptographic transformations in modern conditions. An algebraic lattice of dimension m means a set of all possible combinations of linearly independent vectors from a space of dimension n with integer coefficients. [3].

The basis of a lattice $b_1, b_{2,\dots,} b_n$ is a set of linearly independent vectors that generates the specified lattice. Coordinates of basis vectors are $b_i = \{x_{11}, x_{12}, \dots x_{1m}\}\, i = \overline{1,n}$.

The lattice can be associated with a matrix which rows are the coordinates of the basis vectors that form it. It is well known that any lattice can be defined by several bases and build a matrix of transition from one basis to another. This property allows to implement stable

EMAIL: olha.petrenko@nure.ua (A. 1); alexwgs78@gmail.com (A. 2)
ORCID: orcid.org/0000-0002-7862-5399 (A. 1); orcid.org/0000-0001-9903-7388 (A. 2)

algorithms on algebraic lattices by constructing a basis that consisting of the shortest vectors. Using polynomials of degree n, it is possible to specify a basic vector of dimension n, the coordinates of which are equal to the coefficients of the polynomial. These properties allow to apply the fast Fourier transform to represent the basis vectors and build cryptographic transformations with their help. According to [4], the fast Fourier transform can be applied when developing an algorithm on algebraic lattices in a ring of a class of surpluses modulo some number q. In addition, the fast Fourier transform can be represented in matrix form, which allows in the field of surpluses modulo q to move from the values of the polynomial from the original roots from one to its coefficients according to formula 1.

$$\begin{pmatrix} y_0 \\ y_1 \\ \vdots \\ y_{n-1} \end{pmatrix} = \begin{pmatrix} 1 & 1 & \cdots & 1 \\ 1 & w_n & \cdots & w_n^{n-1} \\ \vdots & \vdots & \vdots & \vdots \\ 1 & w_n^{n-1} & \cdots & w_n^{(n-1)(n-1)} \end{pmatrix} \begin{pmatrix} a_0 \\ a_1 \\ \vdots \\ a_{n-1} \end{pmatrix}, \quad (1)$$

where y_j is the value of the polynomial from the degrees of the original root of unity, w_n^i is the value of the original root of unity degree i, a_i are polynomial coefficients that determine the coordinates of the basis vectors.

For any prime number q in the field of surpluses modulo q there is a root g of degree $(q-1)$of unity, which satisfies the following formula:

$$q - 1 = m2^k, \quad (2)$$

where g^m is the root of degree of unity. Formula 2 allows the application of fast Fourier transform algorithms for polynomials of degree . It can be shown that for any natural number k such a prime number q exists. This follows from Dirichlet's theorem on prime numbers [5]. To apply Dirichlet's theorem for cryptographic transformations on lattices, the number q and the degree of the polynomial on which the transformations are performed must correspond to the formula 2. Using the inverse Fourier transform, it is possible to determine the coordinates of the basis vectors with the formula:

$$a_j = \frac{1}{n}\sum_{j=0}^{n-1} y_j w_n^{-jk} \quad (3)$$

where n is the number of basis vectors, k is the degree of the original element, ϖ is the value of the original root of unity, y_j is the value of the polynomial from the degrees of the original root of unity.

This mathematical apparatus allows with performing transformations on algebraic lattices to reduce the number of operations due to the properties of the original roots of unity, such as $w_n^0 = w_n^n = 1$. In addition, $w_n^j \cdot w_n^k = w_n^{j+k} = w_n^{(j+k)modn}$. So, it is enough to use the condition $w_n^{n-1} = w_n^{-1}$ to find the inverse element then.

With the help of fast Fourier transform it is possible to solve a problem which consists in search from a numerical matrix of the big size of extraction of the small size block with the specified properties.

Under the block means the submatrix of the initial matrix. The idea of this algorithm, based on the fast Fourier transform, is to find some pattern $p_0, p_1, \ldots \ldots p_{m-1}$ in a range $t_0, t_1, \ldots, t_{n-1}$, where p_i, t_j are some numbers. It is well known that the subrange enters from the i-th position, if $p_j = t_{i+j}, j = 0,1,2, \ldots, m-1$. Entry of the subrange of the i-th position is equivalent to the fulfillment of the condition:

$$B_i = \sum_{j=0}^{m-1} \left(p_j - t_{i+j}\right)^2 = 0. \quad (4)$$

Calculating the array B_i allows to determine all entries of subranges into the range. This property is used to construct one-sided functions with a trapdoors, which are used in cryptographic transformations on algebraic lattices [6].

The algorithm for calculating B_i according to [6] is to perform the following steps:

1. Polynomial calculations are performed $C(x) = T(x)P(x)$, where $T(x) = t_{n-1}x^{n-1} + \cdots + t_1 x + t_0$, $P(x) = p_0 x^{m-1} + \cdots + p_{m-1}$ the coefficient of the specified polynomial at x^{m-1+i} is equal to $c_{m-1+i} = p_0 t_i + p_1 t_{i+1} + \cdots + p_{m-1} t_{m-1} = \sum_{j=0}^{m-1} p_j t_{j+i}$.

2. Calculations of $S = \sum_{j=0}^{m-1} p_j^2$ are performed and this addend is present in every B_i;

3. Calculations $H = \sum_{j=0}^{m-1} t_j^2$ are performed;

4. Calculations of the recurrent formula: $B_0 = S - 2c_{m-1} + H$, $B_1 = S - 2c_m + \sum_{j=0}^{m-1} t_{j+1}^2 = B_0 - 2c_{m-1} - 2c_m - t_1^2 + t_m^2$, $B_i = B_{i-1} + 2(c_{m-2+i} + c_{m-1+i}) - t_{i-1}^2 - t_{m-1+i}^2$ are performed.

This algorithm allows to determine vectors with certain properties, such as to find the shortest lattice vector.

3. NTRU algorithm

NTRU Encrypt algorithm [7] today is one of the most researched and widespread algorithms. The asymmetric cryptosystem which built on its basis is based on transformations on algebraic lattices. NTRU is a probabilistic stable system, i.e. a random element is used to encrypt messages. Under this condition, each message has a lot of ciphertext. The stability of the cryptosystem NTRU Encrypt [7] was determined experimentally and is based on the fact of the difficulty of finding the shortest vector of the algebraic lattice [2]. The advantage of this system is the fact that encryption and decryption of the message and key generation process is quick and easy for implementing. NTRU Algebraic Lattice Algorithm is an attractive algorithm for encrypting data in the communication channel between the UAV and the ground workstation. The advantage of the algorithm on the one hand is the ability to perform asymmetric encryption, and on the other to provide fast software implementation. The complexity of the algorithm can be reduced by applying a fast Fourier transform [4] from $O(n^2)$ to $O(nlogn)$. The NTRU Encrypt algorithm depends on parameters that are integers and can be represented in polynomial form. In order for the parameters not to contribute to the occurrence of random errors during decryption, it is necessary to include control bits in each message block.

The following parameters are used to build a mathematical model of the algorithm:

- N – the dimension of the ring of polynomials which used in encrypting messages;
- p – a natural number involved in encrypting and decrypting of the message;
- q – a natural number that participates in encrypting, decrypting of the message and determining the public key;
- k – the key security on which resistance to attacks depends;
- d_i (i=1,2) – distributions of polynomial coefficients used in the formation of the public and secret keys.

When generating keys, consider a ring of truncated polynomials $R = Z[x]/(x^N - 1)$. Each element of the ring can be represented in polynomial form $f = \sum_{s=0}^{N-1} f_s x^s$ or in vector form $(f_1, f_2, \dots, f_{N-1})$. All coefficients of a polynomial are integers. To reduce the complexity of calculating the operation of multiplication of polynomials in a ring of truncated polynomials is possible by applying the operation of "convolution" according to the following rule: let it be necessary to multiply 2 polynomials $f = \sum_{s=0}^{N-1} f_s x^s$ and $g = \sum_{s=0}^{N-1} g_s x^s$ in a ring of truncated polynomials $R = Z[x]/(x^N - 1)$. The result of multiplication $h = f \otimes g$ is a polynomial of the form: $h = \sum_{s=0}^{N-1} h_s x^s$, which coefficients are calculated by the formula:

$$h_s = \sum_{i=0}^{s} f_i g_{s-i} + \sum_{i=s+1}^{N-1} f_i g_{N+s-i}.$$

This formula allows to reduce the computational complexity of multiplying polynomials in $R = Z[x]/(x^N - 1)$ due to the lack of a summation of $mod(x^N - 1)$ terms which degree are greater than N.

The parameters p and q do not have to be prime numbers, but they must satisfy the conditions: *НСД (p, q) = 1* and parameter p should be much smaller than q. Using the values of the parameters p and q, two polynomials f and g are randomly selected. A polynomial f belongs to a ring of truncated polynomials $R = Z[x]/(x^N - 1)$ with the distribution of coefficients with the parameter d_1. This means that the polynomial f contains d_1 coefficients equal to 1, d_1 -1 coefficients equal to -1 and all other coefficients equal to 0. This distribution of coefficients is due to the presence of an inverse polynomial to the polynomial f. A polynomial g belongs to a ring of truncated polynomials $R = Z[x]/(x^N - 1)$ with the distribution of coefficients with the parameter d_2. This means that the polynomial g contains d_2 coefficients equal to 1, d_2 -1 coefficients equal to -1 and all other coefficients equal to 0. Using polynomial f coefficients, polynomials $f_p \equiv f(mod\ p)$ and $f_q \equiv f(mod\ q)$ are constructed.

The obtained polynomials have inverse polynomials in the ring of truncated polynomials $R_p = Z_p[x]/(x^N - 1)$ and $R_q = Z_q[x]/(x^N - 1)$. As for polynomials obtained by reducing a polynomial modulo p and q, they do not have inverse polynomials in the ring of truncated polynomials $R_p = Z_p[x]/(x^N - 1)$ and $R_q = Z_q[x]/(x^N - 1)$.

The public key is calculated according to the rule: $h \equiv p f_q^{-1} \otimes g(mod\ q)$. It should be noted that the polynomial h and the numbers p and q are open parameters, and the polynomial f and f_q^{-1} are secret. To encrypt messages a polynomial r, that has a distribution of coefficients d_3 in the ring of truncated polynomials $R = Z[x]/(x^N - 1)$, and a public key h are randomly selected. This means that the polynomial h contains d_3

coefficients equal to 1, d_3 -1 coefficients equal to -1 and all other coefficients equal to 0.

The message m is encrypted as follows: $c \equiv r \otimes h + m(mod\ q)$.

The message is decrypted in two stages.

First, calculate the polynomial p with integer coefficients from the interval $\left(\frac{-q}{2}, \frac{q}{2}\right)$ by the formula: $a \equiv f \otimes c(mod\ q)$. Then calculate $f_q^{-1} \otimes a$.

The specified encryption algorithm has a disadvantage, which is associated with the appearance of parameters that contribute to errors. Therefore, it is necessary to include control bits for each message block. The cause of such errors is incorrect message centering. It is possible to get rid of it by calculating a polynomial $a \equiv f \otimes c(mod\ q)$ with integer coefficients in the interval $\left(\frac{-q}{2} + x, \frac{q}{2} + x\right)$ for a small value of negative or positive x. If this algorithm does not work, then the encryption procedure is repeatable.

From the decryption procedure, it can be concluded that the NTRU cryptosystem is probabilistic, so the plaintext is not always restored correctly from the encrypted text. The correct choice of polynomials f, g, r allows to reduce the probability of such an error to .

4. Means to increase the stability of the NTRU algorithm and its speed

Given the advantages and disadvantages of the NTRU Encrypt algorithm and the existing specific attacks [8-10],]it is possible to increase the stability of the algorithm by applying not uniform but normal distribution law when encrypting a message, namely when choosing polynomial r coefficients.

To determine the coefficients of the polynomial r, it is proposed to use a random number generator and the density of the normal distribution with predetermined mathematical expectations and standard deviation. The standard deviation in this algorithm is the value of safety level control and is a decisive factor. This is due to the fact that the stability of algorithms on algebraic lattices is based on the solution of the SPV problem (the problem of finding a short lattice vector) [11]. The specified value of the parameter should be chosen under the requirements of the stability of transformations, namely the standard deviation should be equal to the shortest vector of the algebraic lattice. As for the mathematical expectation, it can be zero. This point is due to the fact that for successful cryptanalysis it is necessary to find the lattice points within the probable radius $s\sqrt{N}$, where N is the degree of the polynomial, the modulus of which is transformed, s is the Euclidean norm of the shortest lattice vector. The higher the rate of the vector, the greater the freedom of action of the cryptanalyst to carry out attacks. In view of this, it is proposed to choose the standard deviation equal to the Euclidean norm of the shortest lattice vector. It is possible to obtain the shortest lattice vector among the basis vectors with using the algorithm proposed in the paper [8]. This algorithm allows to obtain a basis using the Gram-Schmidt orthogonalization process [12] with predetermined restrictions on the lengths of vectors.

Next, using the obtained value of the standard deviation and a mathematical expectation equal to zero a random sequence is formed according to the following algorithm:

1. a sequence (c_n) of random numbers is generated;
2. divide the field of real numbers into intervals according to the following condition: $I_1 = (-\infty, -3\sigma)$, $I_2 = (-3\sigma, 0)$ $I_3 = (0, 3\sigma)$ $I_4 = (3\sigma, +\infty)$;
3. check in what interval the generated number got c_i. If $c_i \in I_1, c_i \in I_4$, then i - member of the sequence is equal to 0. If $c_i \in I_2$, Then i - member of the sequence is equal to -1. If $c_i \in I_3$, then i - member of the sequence is equal to 1. This sequence is the coefficient of the polynomial r, which is used for encryption.

The sequence proposed by this rule allows to increase the resistance of the algorithm on the algebraic lattices of NTRU Encrypt to the attack described in [12,13].

To find the shortest lattice vector, we use a one-way function with a trapdoor, which allows us to find the shortest lattice vector from an array based on the fast Fourier transform. Next, the Euclidean norm of this vector is calculated, which allows to set the density function of the normal distribution and on the basis of the calculations to obtain a polynomial r.

It is possible to increase the speed of algorithms, as mentioned above, by applying a fast Fourier transform. $R = Z[x]/(x^N - 1)$.

According to formula 2 to determine the modulus q it is necessary to find such a simple value of q that corresponds to the condition $q - 1 = m \cdot 2^7$. It is proposed to apply to

cryptographic transformations that provide a high level of stability the value of $q = 3 \cdot 2^7 + 1 = 769$. This parameter gives possibility to apply the fast Fourier transform algorithm for polynomials of degree N. In a accordance with Dirichlet's theorem on a prime number for a prime number 769 in the field of the class of surpluses there is a root g of degree 768 of unity. Then $\omega = g^3$ is a root g of degree of unity. This fact gives possibility to apply formula 3 and reduce the complexity of the calculation.

5. Conclusion

Based on the analysis of the NTRU Encrypt algorithm, the paper proposes the application of the normal distribution law to determine the coefficients of the polynomial by which encryption is performed. The application of its parameters, namely mathematical expectation and heart-square deviation, is determined and substantiated. The choice of the original root for the representation of the base vectors of the algebraic lattice using fast Fourier transform is substantiated. It allows to reduce the encryption complexity for a high level of stability of transformations based on the NTRU Encrypt algorithm.

6.References

[1] Горбенко, Ю. І. Аналіз шляхів розвитку криптографії після появи квантових комп'ютерів / Комп'ютерні системи та мережі: Вісник національного університету «Львівська політехніка» 806 (2014): 40–49.

[2] Subhash Khot. Hardness of approximating the Shortest Vector Problem in lattices.Journalof the AC M, 52(5) (2005) 789–808.

[3] Шокуров А.В., Кузюрин Н.Н., Фомин С.А. Курс лекций «Решетки, алгоритмы и современная криптография» [Электронный ресурс] - 2008. -127 стр. - Режим доступу: http://discopal.ispras.ru/ru.lectures-lattice-basedcryptography.htm.

[4] J. M. Pollard, "The Fast Fourier Transform in a Finite Field," Mathematics of Computation, vol. 25, 1971, pp. 365–374.

[5] Ю. В. Линник, А. О. Гельфанд. Элементарные методы в аналитической теории чисел. — Физматгиз, 1962.

[6] D. Micciancio and C. Peikert. Trapdoors for lattices: Simpler, tighter, faster, smaller. In EUROCRYPT, 2012, pp. 700–718.

[7] Hoffstein J., Lieman D., Pipjer J., Silverman J. NTRU: A public key cryptosystem. Conference International Algorithmic Number Theory Symposium Springer, Berlin, Heidelberg, 1998, pp. 267-288.

[8] A. K. Lenstra, H. W. Lenstra, Jr., and L. Lov´asz. Factoring polynomials with rational coefficients. Math. Ann., 261(4), 1982, pp. 515–534.

[9] J. Hoffstein, J.H. Silverman, Protecting NTRU Against Chosen Ciphertext and Reaction Attacks, NTRU Technical Report #016, June 2000, www.ntru.com

[10] E. Jaulmes, A. Joux, A chosen-ciphertext attack against NTRU, in Proceedings of CRYPTO, Lecture Notes in Comp ter Science, Springer-Verlag, 2000.

[11]. C. Peikert. Public-key cryptosystems from the worst-case shortest vector problem. In STOC, 2009, pp. 333–342.

[12] Howgrave-Graha N., Silverman J., Whyte W. Meet-in-the-middle attack on an NTRU private key // NTRU Cryptosystems Technical Report #004. Version 2.

[13.] Xuexin Zheng, An Wang, Wei Wei First-order collision attack on protected NTRU cryptosystem, Affiliations Microprocessors & Microsystems Volume 37, 2013, pp. 601–609.

A Mobile Augmented Reality Application For Museum Exhibitions

Anastasiya Molchanova [1], Svitlana Kuznichenko [2], Iryna Buchynska [3]

[1, 2, 3] *Odessa State Environmental University, 15 Lvivska Str, Odesa, 65016, Ukraine*

Abstract

The article discusses software and architectural solutions for creating a mobile application «FindARt», which allows to recognize art objects using augmented reality technology. To implement AR technologies, the Vuforia Engine platform and the Vuforia Cloud Recognition recognition tool were used. It allows saving images and metadata in a Cloud database, and then recognizing them in the application. The mobile application «Find ARt» allows users to independently conduct individual excursions in museums in Odessa and contributes to expanding the creative horizons in matters of fine arts.

Keywords

Mobile guide application, augmented reality, mobile augmented reality, Vuforia Engine.

1. Introduction

Activities that allow us to learn something new with minimal personal contact using electronic devices are becoming increasingly popular in the world that has changed a lot in the last year.

During the quarantine, many museums operate in a safe mode, improve their web-sites and create self-educational portals about art. More and more of them organize virtual tours and online tours.

Modern travel companies are actively using key digital technologies of Industry 4.0, for example, augmented reality (AR) technology [1]. In recent studies, augmented reality has been recognized as one of the most famous digital technologies that have enormous potential in tourism to make excursions more interactive, convenient and fun [2, 3, 4].

AR apps can enhance the experience of museum visitors by overlaying digital information available through smartphone displays in a real-world environment. Three-dimensional virtual objects are integrated into a three-dimensional real environment in real time [5] to provide visitors with useful information, navigation, guides and translations, thereby creating conditions for the development of smart tourism [6].

Despite the fact that there are a large number of publications devoted to the creation of various AR mobile applications [7, 8, 9] the choice of architecture and design solutions for each of them directly related to the task. Thus, architecture choice and development of a mobile application for the recognition of art objects using augmented reality technologies will be very relevant.

The offered mobile application «Find Art» will allow users to take personal tours in the museums, recognize pictures on different objects and expand their creative horizons to become more erudite.

2. The main research material

Augmented reality (AR) is an environment that complements the physical world with digital data in real time using appropriate devices and software.

The specificity of augmented reality technology is that it programmatically visually connects two initially independent spaces: the world of real objects and the virtual world reproduced on a computer. The new virtual environment is created by superimposing programmed virtual objects on top of the video signal from the camera and becomes interactive by using special markers. AR can also be defined as a system that performs three main functions: a combination of real and virtual worlds, real-time

EMAIL: molchanowa1@gmail.com (A. 1); skuznichenko@gmail.com (A. 2); buchiskayira@gmail.com (A. 3)
ORCID: 0000-0001-7982-1298 (A. 1); 0000-0001-7982-1298 (A. 2); 0000-0002-0393-2781 (A. 3)

interaction, and accurate 3D recording of virtual and real objects. Overlaid sensory information can be constructive (i.e., an additive to the natural environment) or destructive (i.e., to mask the natural environment). The basis of augmented reality technology is an optical tracking system. The camera recognizes markers in the real world, "transfers" them to the virtual environment, imposes one layer of reality on another and thus creates a world of augmented reality [10].

The hardware of the augmented reality device consists of processors, displays, various sensors and input devices. Modern mobile devices, such as smartphones or tablets, have all these elements, as well as a camera and MEMS (accelerometer, GPS, digital compass), which make them suitable for use as a platform for AR. This in turn contributes to the spread of augmented reality and the growing popularity of technology among users.

2.1. Basic principles of augmented reality technology

The general scheme of creating augmented reality in all cases is as follows: the camera of the augmented reality device captures the image of a real object; the device software identifies the received image, selects or calculates the appropriate visual complement, combines the real image with its addition and outputs the final image to the visualization device [11]. The scheme is graphically presented in Fig. 1.

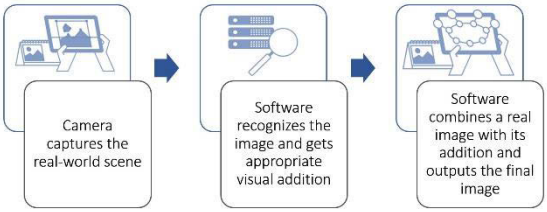


Figure 1: General scheme of creating augmented reality

A smartphone, tablet or smart glasses with a video camera and appropriate software are used to work with AR. If the camera lens is aimed at an object, the software recognizes it either by a pre-set marker or after analyzing the shape of the object. After recognizing the object, the software can connect to a three-dimensional digital duplicate of the object, which is located on the server or in the cloud. Then the AR device downloads the required information and overlays it on the object image. As a result, the screen (or glasses) displays partly physical, partly digital reality. In this case, different observers, looking at one object can see different augmented reality, according to the functions performed. The repairman can see the operating time or operating temperature of the unit he is servicing. The AR can help the operator control the subject with a touch screen, voice or gestures. As the observer moves, the size and orientation of the AR display are automatically adjusted, unnecessary information disappears, and new information appears.

A digital model of an object is usually created at the stage of object development with the help of CAD or by digitization. This digital duplicate collects information about the state of the object, which is obtained from itself, information systems or external sources. With its help, augmented reality software scales and accurately places the actual data on the object image or around it.

2.2. Features of using Vuforia Engine platform

The Vuforia Engine platform, one of the most popular SDKs for developing augmented reality applications, was used to recognize objects and work with augmented reality elements..

Vuforia is a comprehensive, scalable enterprise augmented reality platform and augmented reality software developer toolkit for mobile devices developed by Qualcomm. Vuforia uses computer vision technology, as well as tracking flat images and simple three-dimensional real objects (such as cubic) in real time, recognizes text and cylindrical markers. Vuforia supports various types of targets, including unmarked Image Targets, 3D Multi-Targets, and markers that highlight objects in the scene for recognition. Additional features allow users to avoid the effect of masking (occlusion) of objects using «Virtual Buttons», provide a selection of objects and the ability to programmatically create and modify them.

With PTC developer tools, Vuforia platform can be used to create integrated applications, real-time applications, or develop graphical user interfaces. Vuforia provides application programming interfaces (APIs) in C ++, Java, Objective-C ++ and .NET through extensions for the Unity game engine. Thus, the SDK supports

both development for iOS, Android, and UWP, and also allows to develop AR-applications in Unity, which are easy to transfer to different platforms. The Vuforia Cloud Recognition service was used in the development of the Find ARt mobile application. It is part of the Vuforia platform, which allows to store images and metadata in a cloud databasea and then to recognize downloaded images and receive information about them in the application [12].

The diagram in fig. 2 provides an overview of the application development process using the Vuforia platform. It consists of Vuforia Engine, a target management system hosted on the developer portal (Target Manager), and a cloud or local database [13].

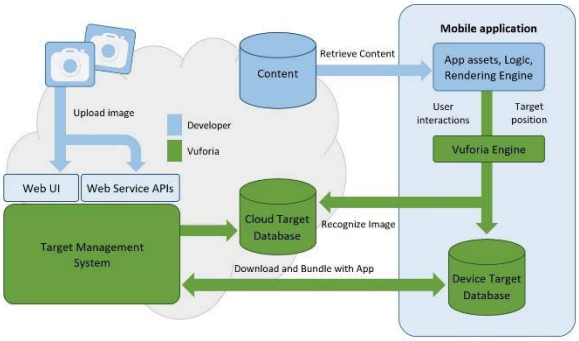


Figure 2: Development of a mobile application using the Vuforia platform

Vuforia Cloud Recognition is ideal for applications that use many targets or targets that need to be updated frequently, as is the case with museum exhibits. The free Vuforia license allows to use Cloud Recognition and recognize up to a thousand targets each month.

2.3. Implementation of the mobile application «Find ARt»

The mobile application «Find ARt» is designed for devices based on Android OS. Despite the fact that the official integrated development environment (IDE) for Android is Android Studio, Unity was chosen. Unity is a cross-platform application development environment developed by the American company Unity Technologies. Android Studio is not focused on developing applications using augmented reality (AR) technologies, but the leading platforms for working with AR (such as Hololens, Oculus, Vuforia, etc.) are designed for Unity. To use Vuforia in Unity, the Vuforia Engine AR package needs to be installed in the project through the Package Manager. We use Vuforia Engine version 8.1.12, which is the approved version for Unity 2019.4. After installing the package, an ARCamera object needs to be added to the appropriate scene. ARCamera is a Unity gaming camera feature that includes VuforiaBehavior to support augmented reality applications for both portable devices and digital glasses. The default camera can be deleted as ARCamera contains its own Camera component.

Vuforia offers three types of databases for storing target images: Device, Cloud, and VuMark. Due to the need to store a large number of target images for the application and constantly add data, it was decided to use Cloud database to store the application targets. To do this, a Cloud database needs to be created on the Vuforia developer portal through the Target Manager. CloudRecognition and ImageTarget objects are nedded to be added to the scan scene. ImageTarget is an image that Vuforia Engine can detect and track.

A C# script needs to be attached to the CloudRecognition object. This script initializes a CloudRecoBehavior object. This is a basic behavior class that encapsulates Cloud Recognition behavior. It will initialize the target finder and will wait for new results. Status changes and new recognition results are tracked using the OnNewSearchResult() method.

The developer can add target images to the cloud database through the Target Manager on the Vuforia Engine developer portal. Target images are detected based on natural features that are extracted from the target image and then compared to the camera image in real time. Target ratings can range from 1 to 5 stars. For best results, it's best to use targets with 4 or 5 stars.

Each target cloud image may additionally have associated metadata. Target metadata is user-defined data that can be associated with a target and populated with special information up to the permitted limits (up to 2 MB per target). Metadata can contain a simple text message that will be displayed on the device screen when a target is detected; a simple URL string that points to a special network location where other content, such as a 3D model, video, image, or any other user data, is stored; some special text that the program can process and use to perform certain actions, such as presenting an object in JSON format. Metadata can be loaded with the

target image when creating a target in the Cloud database, or developer can update the metadata of an existing goal later through the goal manager, but this can take up to several minutes. Therefore, it was decided to store image data not as target image metadata in the Vuforia cloud database, but in the Firebase Database cloud database.

Firebase Realtime Database stores data in JSON format [14]. The database contains data about paintings (title, author ID, year of writing, museum ID, additional information if necessary, total number of recognitions, etc.), authors, museums and users of the application (recognition statistics and ID of paintings added to Favorites). In our case using a NoSql database is more convenient than relational databases. When storing data in JSON format, you can not worry about determining the complete structure of each element or the interaction of the stored data types. For example, not all Artwork objects may have a description field. Materials or sizes of the original may be unknown. The year of creation can be specified in numbers or in text, for example, «before 1715».

The implemented software allows to recognize paintings and immediately displays brief information about them on the screen. In the message that appears, user can click "Details" and go to the page with full information about the painting, which contains the name, author, size, year of creation, materials used, a brief description and the museum in which it is located. There is the ability to log in to save user's favorite pictures to the "Favorites" and share information about them with friends through social networks or messengers. From the main page user can view the expositions of the museums of Odessa and the works of popular artists. The application has a minimalist light design (fig. 3).

3. Conclusions

In this work, a mobile application «Find ARt» was developed for convenient and quick obtaining information about objects of art using augmented reality (AR) technologies. The Vuforia Engine platform was used to implement AR technologies.

Vuforia Engine is considered to be the leading tool in this field and the most complete SDK with a wide range of features for AR applications: identification and tracking of target images, English texts and 3D objects in real time; placement of virtual objects, such as 3D models, in a real environment, etc.

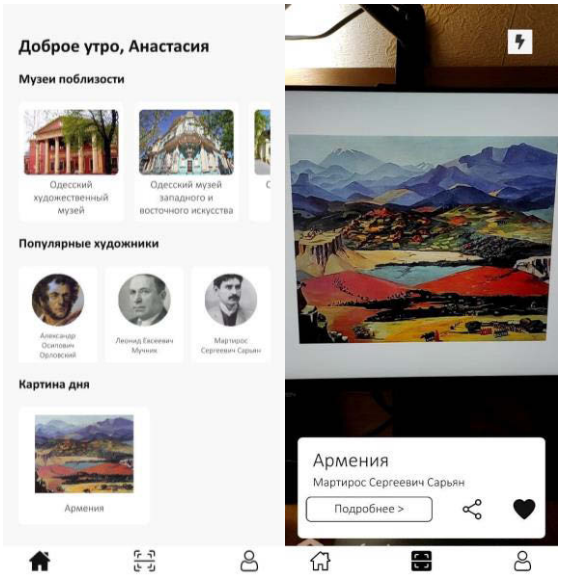


Figure 3: «Find ARt» interface

Due to the need to store a large number of target images for the application and constantly add data, it was decided to use Cloud database to store the application targets.

Due to the need to store a large number of target images for the application and constantly add data, the Vuforia cloud database was used to store the FindARt application targets. Vuforia Cloud Recognition allows to store images and metadata in a cloud database and then recognize them in the application. This service is free, but has some limitations.

4. References

[1] Loureiro S.M.C. (2021) The Use of Augmented Reality to Expand the Experience of Museum Visitors. In: Geroimenko V. (eds) Augmented Reality in Tourism, Museums and Heritage. Springer Series on Cultural Computing. Springer, Cham. https://doi.org/10.1007/978-3-030-70198-7_8

[2] Han, D. I., Jung, T., & Gibson, A. (2013). Dublin AR: Implementing augmented reality in tourism. In Information and communication technologies in tourism 2014 (pp. 511-523). Springer, Cham.

[3] Claudia tom Dieck, M., & Jung, T. (2018). A theoretical model of mobile augmented

reality acceptance in urban heritage tourism. Current Issues in Tourism, 21(2), 154-174.
[4] Siang, Tan & Ab. Aziz, Kamarulzaman & Ahmad, Zauwiyah & Suhaifi, Syazani. (2019). Augmented Reality Mobile Application for Museum: A Technology Acceptance Study. 1-6. 10.1109/ICRIIS48246.2019.9073457.
[5] Azuma, R. T. (1997). A survey of augmented reality. Presence: Teleoperators & Virtual Environments, 6(4), 355-385.
[6] Boes K, Buhalis D, Inversini A (2016) Smart tourism destinations: ecosystems for tourism destination competitiveness. Int J Tour Cities 2(2):108–124. https://doi.org/10.1108/IJTC-12-2015-0032
[7] Procházka, David & Stencl, Michael & Popelka, Ondřej & Stastny, Jiri. (2011). Mobile Augmented Reality Applications. Mendel.
[8] Carmigniani, Julie et al. "Augmented reality technologies, systems and applications." Multimedia Tools and Applications 51 (2010): 341-377.
[9] Abou El-Seoud, Samir; Taj-Eddin, Islam. An Android Augmented Reality Application for Retail Fashion Shopping. International Journal of Interactive Mobile Technologies (iJIM), [S.l.], v. 13, n. 01, p. pp. 4-19, jan. 2019. ISSN 1865-7923. doi:http://dx.doi.org/10.3991/ijim.v13i01.9898.
[10] Dorfmüller K. (1999) An Optical Tracking System for VR/AR-Applications. In: Gervautz M., Schmalstieg D., Hildebrand A. (eds) Virtual Environments '99. Eurographics. Springer, Vienna. https://doi.org/10.1007/978-3-7091-6805-9_4
[11] Augmented reality (AR). URL: https://www.it.ua/ru/knowledge-base/technology-innovation/dopolnennaja-realnost-ar.
[12] Cloud Recognition Documentation. URL: https://library.vuforia.com/articles/Training/Cloud-Recognition-Guide.html.
[13] Developing with Vuforia. URL: https://developer.vuforia.com/resources/dev-guide/getting-started.
[14] Firebase Documentation. URL: https://firebase.google.com/docs/guides.

The Mersenne Twister Output Stream Postprocessing

Yurii Shcherbyna [1], Nadiia Kazakova[2], Oleksii Fraze-Frazenko[3]

1 National University "Odesa Law Academy", Rishelievska st., 28, Odesa, 65011, Ukraine
[2,3] Odesa State Environmental University, 15 Lvivska str., Odesa, 65016, Ukraine

Abstract

Today, pseudo-random number sequence generators are actively used to solve a large number of applied problems of statistical and simulation modeling in such areas as telecommunications networks, automated control systems for production processes and infrastructure, security systems and others. Such generators have serious requirements for the sequence of numbers that they generate at their outputs. These are, first of all, the requirements for their randomness. The original sequences should be almost indistinguishable from the truly random ones. And, most importantly, they must also ensure a high uniformity of probability distribution of the original numbers. It is shown that the non-uniformity of numbers at the output of the primary generator significantly affects the quality of modeling of stochastic processes that take place in systems for which computer models are built. Tests on a linear congruent generator and a Mersenne twister (MT) generator have shown that the flow of decimal real numbers at their outputs does not fully meet the needs of modern computer modeling. The vast majority of tests of such flows using the Pearson chi-square test gives an unsatisfactory result. Based on the analysis of post-processing methods of numerical sequences, it is proposed to perform preliminary thinning of the input in relation to the model of the numerical flow by removing elements that do not fit into the uniform distribution. The expected sum of random real numbers to be included in each of the segments of the random number distribution histogram is chosen as the thinning criterion. It is shown that the use of this method of post-processing of the primary generator does not require extra computing resources of the system.

Keywords

Simulation, linear congruent generator, Mersenne twister generator, inverse function method, Pearson chi-square test, post-processing of numerical flow.

1. Introduction

If in the second half of the last century modeling was considered a secondary stage in the design of complex systems, today the modern development of computer technology significantly increases its importance in the study of stochastic processes that occur in modern production, infrastructure management and economic activity.

Usually the modeling of random processes takes place in two stages: first a sequence of random variables evenly distributed on the interval [0, 1] is created, and only then a sequence of numbers is formed from them, which corresponds to the given probability distribution law. Because computing devices are deterministic automata, they can only output pseudo-random numbers (PRN) with a limited repetition period of T. For efficient modeling, PRN generation algorithms must provide high speed, long repetition periods, and good statistics. [1].

Libraries of modern programming languages already contain PRN generators with a uniform distribution law, which return the number U_i from the finite set $\{0, 1, \dots, T-1\}$. It is also possible to connect external libraries offered by different developers. Most traditional PRN generators are well described by Donald Knuth in [2], where he concludes that they are of insufficient quality and unsuitable for research needs.

The vast majority of PRN cryptographic generators developed in recent decades have been described in detail by Bruce Schneier in [3], but they are hardly suitable for computer simulation. First, their use requires significant computing

EMAIL: shcherbinayura53@gmail.com (A. 1); kaz2003@ukr.net (A. 2); frazenko@gmail.com (A. 3)
ORCID: 0000-0003-3885-6747 (A. 1); 0000-0003-3968-4094 (A. 2); 0000-0002-2288-8253 (A. 3)

resources, which significantly reduces their efficiency, and secondly, they ensure uniform distribution at the binary level. As shown in [4], the transformation of a binary sequence into a decimal format and its subsequent scaling leads to a significant loss of uniformity.

Recently, an algorithm known as the Mersenne Twister (MT) has been proposed for modeling purposes, which provides an extremely long repetition period $2^{19937} - 1$ [5]. It, together with the linear congruent generator (LCG) [6], is part of the libraries of almost all known specialized software environments designed to solve research and engineering problems.

The two-stage modeling scheme is very sensitive to the uniform distribution of numbers at the output of the selected generator. As shown by checking the flow of real numbers generated by LCG and MT using Pearson's χ^2-test, up to half of the samples, regardless of their size, are not tested for uniformity.

Since the choice of PRN generator is extremely limited for researchers, this problem should be solved by upgrading the numerical flow at the output of the PRN generator.

2. The aim of the study

To check the quality of pseudo-random number generators, a large number of test packets were created [7,8] and all of them perform the analysis of the output stream at the binary level. This is due to the fact that they are mainly intended for testing cryptographic generators focused on the performance of quenching operations, which are performed bit by bit. Divided into bytes and converted to a decimal sequence of real numbers, a binary sequence does not necessarily remain evenly distributed. In most cases, it is necessary to perform its post processing [9], choosing a method that would give a satisfactory simulation result and, at the same time, was effective in terms of the use of computing resources. In view of this, the aim of the study is to select and justify an additional method of converting a sequence of pseudo-random numbers at the output of the MT generator to ensure a given level of uniformity of their distribution.

3. Methods of post-processing

The general idea of additional processing of numbers at the output of the generator was formulated long ago, when the main source of random numbers were physical noise occurring in electronic devices, such as electronic lamps, quantum generators and the like. Its essence is to sacrifice a certain number of numbers at the output of the generator for the sake of obtaining an output stream that would satisfy the conditions. Later, von Neumann remarked on the inadmissibility of using physical generators in computer technology, because due to technical difficulties the possibility of re-implementing the obtained sample of random numbers at that time was absent and, therefore, proposed algorithms for generating pseudo-random numbers as the method of mean squares [10] and the linear congruent method. But, as shown by D. Knuth [4], they also did not provide the necessary uniformity of the formed numerical flow. Since it is almost impossible to make an ideal generator, the idea of post-processing for both real random number generators and PRN generators remains relevant.

At the moment, we can identify the following four methods of post-processing: [9].

1. Ad hoc simple correctors.
2. Whitening with hash functions.
3. Extractor algorithms.
4. Resilient functions.

The general requirement for all methods of post-processing is the minimization of resources for their implementation.

An example of a simple corrector is the corrector described by von Neumann in [10] where he proposes to combine a pair of bits obtained from independent sources on the principle: if the bits match (00 or 11), the bits are canceled, the combination of bits 01 corresponds to 0-th the output bit, and the combination 10 corresponds to the 1st output bit. The maximum efficiency of such an algorithm is on average 4 input bits per 1 output bit. It was in this work that von Neumann emphasized the difficulty of generating random decimal numbers.

Later, other, more advanced versions of similar correctors were proposed, but they also work at the bit level.

Whitening is a method that reduces the correlation of symbols at the output of the entropy source and increases the homogeneity and uniformity of the distribution of symbols in the output stream. It is usually performed using hash algorithms, such as MD5, SHA-1, SHA-2, SHA-256 or SHA-512. This processing is a deterministic algorithm that converts input blocks of characters of arbitrary length into a fixed size string. In [11] it was shown that bleaching does

not increase entropy and therefore the main task of ensuring randomness should be solved by the PRN generator, and not by the post-processing algorithm. It should be noted that the term randomness means the absence of a noticeable analytical relationship between the symbols at the output of the PRN generator. But, in contrast to cryptographic problems, in modeling it is important to ensure the uniformity of the distribution of the original numerical flow.

Randomity extractors are algorithms that convert a low-quality stream of input values into an almost uniform stream of numeric characters with a small number of guaranteed random bits. Formally, the method of such a transformation is described in the work of Luke Trevisan [12]. To characterize weak sources of chance, the author introduces the concept of minimum entropy, which characterizes the non-uniform distribution of the quantity X in the range $\{0,1\}^n$, where n is a binary combination at the source output. In the case of a perfectly uniform distribution, all combinations will be equally probable and the entropy will be maximum, otherwise it will be smaller. If the minimum entropy of such a source has a value of at least k, then for each $x \in \{0,1\}^n$ the condition $\Pr[X = x] \leq 2^{-k}$ is fulfilled. The task of the extractor is to convert the flow X into almost uniform. To quantify the output flow, the concept of statistical difference ϵ between two random variables X and X in the range $\{0,1\}^n$ is used, which is defined as:

$$|p[T(X) = 1]| - |p[T(Y) = 1]| \leq \epsilon \qquad (1)$$

In the general case, the (k, ϵ) -extractor converts the flow of random variables X into an almost uniform flow by the rule:

$$Ext : \{0,1\}^n \times \{0,1\}^t \rightarrow \{0,1\}^m, \qquad (2)$$

where the random variable X has a minimum entropy k, and U_t is a uniformly distributed quantity on $\{0,1\}^t$. The mechanism of operation of the randomness extractor is shown in Figure 1.

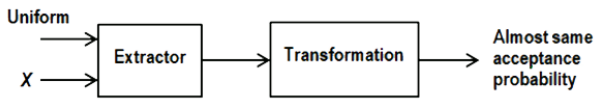


Figure 1: The mechanism of the extractor

In [12], another method of amplifying the randomness of the output flux of the PRN generator, which is based on its postfiltration through some deterministic process, is considered. His idea is to use the use of elastic functions to divide the original characters into random and "not random enough". In [13], the elastic function F is defined as the (n, m, k) -function $f : F^n \rightarrow F_m$, which forms each output k-bit combination of fixed input bits directly, and the others $n - k$ bits are selected randomly. Such functions were created exclusively for the needs of cryptographic transformations.

From the above we can conclude that the work on creating generators of random and pseudo-random numbers is mainly focused on cryptographic needs. At the heart of such generators is a complex computational process, the implementation of which requires significant computing resources. For modeling purposes, either LCG or MT generators are typically used, which have unsatisfactory uniformity in the distribution of the source symbols, but can be subject to post-processing methods such as combining streams from multiple sources and thinning them by removing symbols that look like " not random enough ".

4. Post-processing of a numerical stream from the MT generator

Computer simulation of random processes such as request flows in telecommunication systems [1], flows of attacks on information system resources [14], or failures of technical equipment in computer systems, involves the use of procedures containing elements of randomness implemented using built based on number theory and numerical analysis of optimally selected deterministic systems. Such systems are understood as arithmetic generators of pseudo-random numbers, which are based on recurrent relations. This means that each subsequent number at the output of the generator is determined by one or more pre-formed numbers and the flow of such numbers will be repeated regularly with period T. Despite this dependence, the numbers generated by the generator should look independent throughout the period. only in the case of their absolutely uniform distribution. Such numbers, evenly distributed on the interval $[0,\ 1]$, are most often used for modeling purposes. They must meet the following requirements:

1. the sequence must have the properties of uniform distribution of random numbers in the interval $[0,\ 1]$ throughout the repetition period T;

2. each fragment of the sequence within the period T, from the output of the generator must have the properties of uniform distribution.

The first condition is not met by the definition of PRN, but this shortcoming developers are trying to compensate by creating algorithms for generating numbers with too long a repetition period. Both LCG and MT generators have fairly long periods. The problem for them is the need to initialize them with a real random number, but it is quite simply solved by forming such a number from the current time.

The second condition can be formally described as follows. The general sequence $x_1, x_2, \ldots$ can be considered completely uniformly distribute (CUD), if for any $s \geq 1$ part of this sequence $(x_n, x_{n+1}, \ldots, x_{n+s+1})$ $n = 1, 2, \ldots$ will also be evenly distributed.

In [6] it was shown that the LCG developers tried to provide satisfactory generator characteristics with the optimal ratio of the coefficients a, c, m of the recurrent ratio

$$X_{n+1} = (aX_n + c) \, mod \, m. \qquad (3)$$

As practice shows, the function **rand()** is built into most modern programming environments and uses as a module m 32-bit machine bit word, which provides a period of repetition of numbers T at the output of the generator, which does not exceed the value of $m = 2^{32}$. As for the uniformity of the distribution of the output stream, it remains extremely low.

Figure 2 shows an example of a histogram of the distribution of numbers at the output of the LCG, obtained using the function **rand()**, which is part of the library C ++. The value of the sample N is 1024 numbers, and the number of intervals of the histogram is 16.

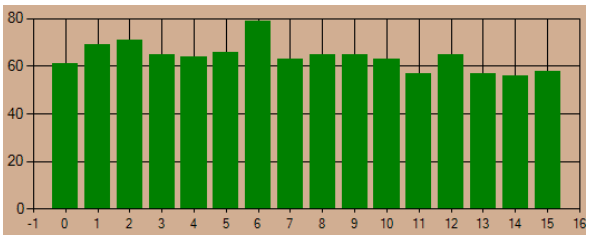


Figure 2: Histogram of the distribution of PRN obtained by the function **rand()**

A check of the quality of the distribution using the χ^2 –test showed that more than two-thirds of the samples do not meet the requirements of uniformity. Figure 3 shows the distribution of the number of hits in each of the 16 intervals of the histogram, Figure 2. Here are the limits of the intervals of the histogram (*Xmin, Xmax*), the probability of hitting the number in the interval (*Pi*), the number of hits in the interval (*Ni*) and components indicator χ^2 –-test (*Hi*), for each specific interval of the histogram.

N	Xmin	Xmax	Ni	Hi
1	0	0,0625	61	0,1406
2	0,0625	0,125	69	0,3906
3	0,125	0,1875	71	0,7656
4	0,1875	0,25	65	0,0156
5	0,25	0,3125	64	0
6	0,3125	0,375	66	0,0625
7	0,375	0,4375	79	3,5156
8	0,4375	0,5	63	0,0156
9	0,5	0,5625	65	0,0156
10	0,5625	0,625	65	0,0156
11	0,625	0,6875	63	0,0156
12	0,6875	0,75	57	0,7656
13	0,75	0,8125	65	0,0156
14	0,8125	0,875	57	0,7656
15	0,875	0,9375	56	1
16	0,9375	1,0625	58	0,5625

Figure 3: Boundaries of histogram intervals and distribution of sample numbers between them

The total quality index according to Pearson's χ^2 –-test is calculated by the formula

$$\chi^2 = \sum_{i=1}^{k} \frac{(n_i - N_i^*)^2}{N_i^*}, \qquad (4)$$

where k – this is the number of segments of the histogram, n_i and N_i^* – the number of random numbers of the output stream that actually fell in the i-th interval and their expected number, respectively. The expected number with uniform distribution N_i^* is defined as N/k and for the given example is 64.

Similar tests were performed for the MT generator. Unlike the LCG generator, it has a much longer repetition period, which is equal to $T = 2^{19937} - 1$ bits, and the algorithm embedded in it provides very little correlation between two samples from the original sequence of numbers. The developers of the generator claim that it passes the tests of the DIEHARD package [8]. However, all the declared positive qualities of such a generator are valid for a binary sequence. Tests of real numbers distributed in the interval $[0, 1]$ using the χ^2 –test showed that only $10 \div 15$

percent of samples from the output stream from the MT generator give a positive test result.

Figure 4 shows an example of a histogram of the distribution of numbers at the output of MT, obtained using the function **uniform_real_distribution<> mersenne(0, 1)** from the library C ++ <cmath.h>

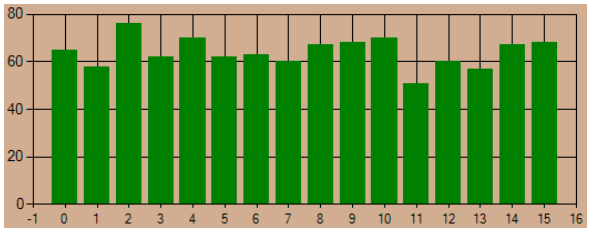


Figure 4: Histogram of the PRN distribution obtained using the function **uniform_real_distribution<> mersenne(0, 1)**

The sample size *N*, as in the case of the LCG generator, was equal to 1024 real decimal numbers, and the number of intervals of the histogram k was also equal to 16.

To model stochastic processes, the method is most often used, the essence of which is that on the basis of the conditions of inverse functions and the theorem according to which a continuous random variable x, with an arbitrary distribution having a probability distribution function $F(x)$, determines a continuous uniformly distributed on the interval [0, 1], the random variable $\gamma = F^{-1}(\gamma)$ [15]. This method works well when the process can be described analytically and the inverse function $F^{-1}(x)$ exists for it.

To evaluate the numbers distribution uniformity influence at the output of the MT generator on the quality of the simulation, consider the example of creating a numerical flow, which is described by the Weibull function with two parameters. It looks like this:

$$F(x, \alpha, \beta) = 1 - e^{-(x/\beta)^{\alpha}}. \quad (5)$$

where α – is a scale parameter, β – form parameter, a x – variable. α i β – are fixed values for which the conditions $\alpha > 0$, $\beta > 0$ must be met. In case if $\beta = 1$, Weibull's distribution coincides with the exponential distribution.

The inverse function looks like:

$$F^{-1}(x) = \beta[-\ln(1 - x)]^{1/\alpha}. \quad (6)$$

We assume that at the output of the MT generator there is a flow of numbers $y_1, y_2, \ldots$ which express the probability of events of the random Weibull process. Then, using relation (6), we can obtain a stream of numbers $x_1, x_2, \ldots$, which in accordance with this principle, is determined by relation (5) and expresses the argument of the distribution function.

Next, we construct a histogram, on the basis of which we calculate the quality index by the χ^2-test. The choice of this criterion is determined by the fact that, firstly, its use is not limited to the type of distribution and, secondly, if this criterion is not met, then all other criteria, too, are unlikely to be met.

A separate issue in the special literature is the choice of the number of segments of the histogram. They should be sufficient so that the shape of the histogram in its form as close as possible to the form of the Weibull distribution density function described by the expression:

$$p(x) = \frac{\alpha}{\beta^{\alpha}} x^{\alpha-1} e^{-(x/\beta)^{\alpha}}. \quad (7)$$

On the other hand, the number of segments should not be too large so as not to lose the filtering capabilities of the histogram, as is the case with signal quantization. Today there are several different ways to determine their number and the most popular is the formula proposed in 1926 by Sturges [16]

$$k = 1 + \lfloor log_2 N \rfloor \quad (8)$$

where k number of histogram segments, and N – the number of characters in the random number sample. This formula is derived from the binomial distribution and implicitly assumes work with the normal distribution.

There are other formulas that also allow you to determine the approximate number of segments. A good option is the formula proposed in 1981 by Freedman and Diaconis [17], which gives the length of the segment h, expressed in terms of interquartile range (the distance between the end of the first and the beginning of the last quartile of the IQ sample)

$$h = 2 \cdot (IQ) \cdot N^{-1/3}, \quad (9)$$

where the number of segments can be defined as

$$k = \frac{y_{max} - y_{min}}{h}. \quad (10)$$

where y_{max} and y_{min} are, respectively, the maximum and minimum values of the members of the sample variation series.

All the proposed methods for calculating the number of segments of the histogram were

determined based on the problem of finding the type of distribution based on the accumulated statistical material and, each time, the researchers proceeded from the features of the process to be evaluated. That is why there are so many ways to determine the value of k. As for the simulation, the inverse problem is solved here, when the method of distribution of random variables is known and, therefore, the value of the number of segments is not so critical and can be determined arbitrarily.

If the inverse function method converts a sequence of random numbers from the MT generator into a random Weibull process with the parameters $\alpha = 1.3$, $\beta = 0.1$, it will look like Figure 5.

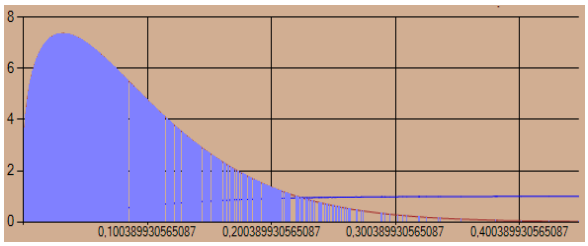


Figure 5: The result of modeling a random Weibull process by the inverse function method

An additional problem that arises when estimating an asymmetric random process is that, taking into account the peculiarities of formula (4), very few random numbers n_i fall into the last segments of the "tails" of the distribution and, therefore, these components of the indicator χ^2-test contributes the lion's share to the error, which brings its value closer to the critical value $\chi^2_{\text{кр}}$. In [2] D. Knuth points out that the sample size N must ensure that each interval of the histogram hits at least 5 random numbers. To avoid this problem, and since the histogram segments do not have to be the same size, we will combine the last intervals with less than 6 numbers into one common interval. For the example shown in Figure 5, 16 segments of the histogram will be filled as follows

The table in Figure 6 shows the boundaries of the intervals of the histogram (*Xmin, Xmax*), the probability of hitting the number in the interval (*Pi*), the number of hits in the interval (*ni*), the expected number of hits in the interval (*Ni*) and the component indicator χ^2-test (*Hi*).

N	Xmin	Xmax	Pi	ni	Ni	Hi
1	0	0,0331	0,211148	193	216	2,449074
2	0,0331	0,0661	0,231187	248	237	0,510549
3	0,0661	0,0992	0,185829	196	190	0,189474
4	0,0992	0,1322	0,134426	135	138	0,065217
5	0,1322	0,1653	0,091082	83	93	1,075269
6	0,1653	0,1984	0,058813	62	60	0,066667
7	0,1984	0,2314	0,036541	38	37	0,027027
8	0,2314	0,2645	0,02198	31	23	2,782609
9	0,2645	0,2975	0,012855	11	13	0,307692
10	0,2975	0,3306	0,007332	17	8	10,125
11	0,3306	0,3636	0,004089	3	4	0,25
12	0,3636	0,3967	0,002234	2	2	0
13	0,3967	0,4298	0,001197	1	1	0
14	0,4298	0,4628	0,00063	1	1	0
15	0,4628	0,4959	0,000326	0	0	не число
16	0,4959	0,562	0,000166	2	0	∞

Figure 6: Boundaries of histogram intervals and their filling for Weibull distribution

From the table shown in Figure 6, it is seen that the segments 12 to 16 do not allow to calculate the corresponding components of the indicator χ^2, and therefore they are combined into one interval, for which $n_i = 9$, and $n_i^* = 8$. At the level of five percent error ($\lambda = 0.05$) for the given example, its value is $\chi^2 = 17.723577$, which is more than the critical value $\chi^2_{\text{кр}} = 7.290644$, and this means dissatisfaction with the simulation result. This result is confirmed in the vast majority of subsequent tests and, thus, it can be concluded that it is necessary to correct the numerical flux at the output of the MT generator by post-processing.

As can be seen from the above analysis of post-processing methods, the vast majority of them were developed for cryptography and, therefore, are unacceptable for the correction of the numerical flow at the output of the MT generator due to their excessive complexity. The solution to the problem should not burden the computer system with significant additional resources.

Given the admissibility of such operations as combining numerical streams, their "bleaching" or "sieving", as well as the use of Pearson's χ^2-test to assess the uniformity of number distribution, we will try to "align" it by removing from its composition "extra" elements .

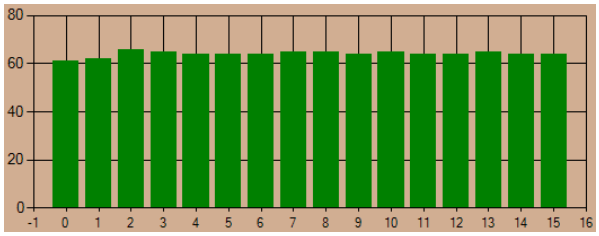


Figure 7: Histogram of the PRN distribution obtained at the output of the MT generator after post-processing

It is expected that in the case of uniform distribution in each segment of the histogram should fall the same number of random numbers equal to $N_i^* = N/k$. The mathematical expectation of a quantity to be included in a segment bounded by the conditions $x_{min} \le x_i < x_{max}$ is defined as $m_i = (x_{min} + x_{max})/2$. Then the number of numbers that fall into the i-th segment S_i, will be approximately equal to the value of $S_i^* = N_i^* m_i$. Of course, each time this sum will be either less than S_i^*, or more than S_i^*, but there will be no significant difference. This makes it possible to formulate such an algorithm. If the sum of the numbers S_i that fall into the i-th segment of the histogram exceeds the value of S_i^*, then all other numbers that fall into it are skipped. Of course, the number of numbers in the segments will remain different, but the unevenness of the sample will be smaller.

N	Xmin	Xmax	Ni	Hi
1	0	0,0625	61	0,1406
2	0,0625	0,125	62	0,0625
3	0,125	0,1875	66	0,0625
4	0,1875	0,25	65	0,0156
5	0,25	0,3125	64	0
6	0,3125	0,375	64	0
7	0,375	0,4375	64	0
8	0,4375	0,5	65	0,0156
9	0,5	0,5625	65	0,0156
10	0,5625	0,625	64	0
11	0,625	0,6875	65	0,0156
12	0,6875	0,75	64	0
13	0,75	0,8125	64	0
14	0,8125	0,875	65	0,0156
15	0,875	0,9375	64	0
16	0,9375	1	64	0

Figure 8: Boundaries of histogram intervals and their filling with numbers from the output of the MT generator after post-processing

Figure 7 shows the test results of a sample of length $N = 1024$ real decimal pseudo-random numbers at the output of the MT generator after post-processing as described, and the filling of histogram segments is shown in Figure 8 Now, for $\lambda = 0.05$ $\chi^2 = 0.3438$, which is less than critical value $\chi^2_{\text{кр}} = 7.2609$..

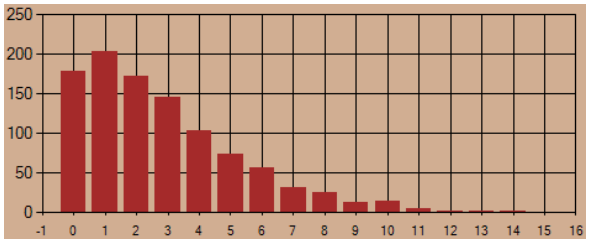


Figure 9: Histogram of the Weibull process, based on the table in Figure 8

The Weibull process formed by the method of the inverse function of the numbers from the MT generator after their post-processing gives significantly better results. The histogram constructed on the basis of such flow is shown in figure 9.

The table in Figure 10 shows the distribution of numbers in the segments of the histogram shown in Figure 9 and the components of the χ^2-test.

N	Xmin	Xmax	Pi	ni	Ni	Hi
1	0	0,0275	0,17037	178	176	0,022727
2	0,0275	0,055	0,19828	203	204	0,004902
3	0,055	0,0825	0,172518	172	178	0,202247
4	0,0825	0,11	0,136571	146	141	0,177305
5	0,11	0,1375	0,102121	104	105	0,009524
6	0,1375	0,1651	0,073283	74	76	0,052632
7	0,1651	0,1926	0,050908	57	52	0,480769
8	0,1926	0,2201	0,034422	32	35	0,257143
9	0,2201	0,2476	0,022739	26	23	0,391304
10	0,2476	0,2751	0,014715	13	15	0,266667
11	0,2751	0,3026	0,009348	14	10	1,6
12	0,3026	0,3301	0,00584	5	6	0,166667
13	0,3301	0,3576	0,003592	2	4	1
14	0,3576	0,3851	0,002178	2	2	0
15	0,3851	0,4126	0,001303	2	1	1
16	0,4126	0,4677	0,000769	0	1	1

Figure 10: Boundaries of histogram intervals and distribution of numbers between them for Weibull distribution after post-processing

For the given example for $\lambda = 0.05$, $\chi^2 = 4.10807$, which is less than the critical value $\chi^2_{\text{кр}} = 7.260944$.

Subsequent tests showed that the use of the proposed method of "thinning" the input stream

from the MT generator, gives significantly better simulation results in terms of their reliability.

5. Conclusions

The experience of modern computer modeling shows that the use of specialized software packages such as Boost, Glib, C ++, Python, Ruby, R, PHP, MATLAB and Autoit requires significant computing resources and therefore the simulation of stochastic processes is better performed using common tools programming in languages that allow you to create economical program code. Modern C ++ programming environments, such as Visual Studio and QT5, are a good option. They include a large number of additional libraries containing various PRN generators.

Such generators are built on the basis of recurrent algorithms and do not provide a given level of uniformity of distribution of real numbers in the output stream and, therefore, their use for modeling significantly affects its quality.

The problem of improving the quality of modeling can be solved by supplementing the algorithm for calculating operations that provide pre-randomization of the input stream. As such operations, you can use the removal of the original numbers, the presence of which violates the uniformity of the distribution of the primary generator. One way to implement such an algorithm is to limit the number of characters in each segment of the histogram by the value of the expected sum of random numbers, which is determined by the mathematical expectation of the number in the segment and the expected number of numbers in the segment. Tests show that the unevenness of the primary generator with this method of post-processing has almost no effect on the quality of modeling.

6. References

[1] Averill M. Law. Simulation modeling and analysis, 5th. ed., McGraw-Hill Education, 2 Penn Plaza, New York, 2015. URL: https://industri.fatek.unpatti.ac.id/wp-content/uploads/2019/03/108-Simulation-Modeling-and-Analysis-Averill-M.-Law-Edisi-5-2014.pdf

[2] D. E. Knuth, The Art of Computer Programming, Volume 2: Seminumerical Algorithms, 3rd. ed., Boston, Mass, USA : Addison-Wesley, Longman Publishing, Addison-Wesley, Reading, Mass, 1998. URL: https://doc.lagout.org/science/0_Computer%20Science/2_Algorithms/The%20Art%20of%20Computer%20Programming%20%28vol.%202_%20Seminumerical%20Algorithms%29%20%283rd%20ed.%29%20%5BKnuth%201997-11-14%5D.pdf

[3] Bruce Schneier, Applied Cryptography, Second Edition: Protocols, Algorthms, and Source Code in C, 20. ed., Boston, Mass, USA : Addison-Wesley, Longman Publishing, Addison-Wesley, Reading, Mass, 1998. doi:10.1002/9781119183471 URL: https://lost-contact.mit.edu/afs/adrake.org/usr/rkh/Books/books/Schneier%20-%20Applied%20Cryptography%202ed%20-%20Wiley.pdf.

[4] J. H. Ahrens, U. Dieter, A. Grube, Pseudo-random numbers. Computing 6 (1970) 121-138). URL: https://doi.org/10.1007/BF02241740.

[5] Saito, M. An Application of Finite Field: Design and Implementation of 128-bit Instruction-Based Fast Pseudorandom Number Generator. Dept. of Math. Graduate School of Science, February 9th, 2007. URL: http://www.math.sci.hiroshima-u.ac.jp/~m-mat/MT/SFMT/M062821.pdf.

[6] Niederreiter H. Quasi-Monte Carlo methods and pseudo-random number. doi: https://doi.org/10.1090/S0002-9904-1978-14532-7. URL: https://www.ams.org/journals/bull/1978-84-06/S0002-9904-1978-14532-7/S0002-9904-1978-14532-7.pdf.

[7] A Statistical Test Suite for Random and Pseudorandom Number Generators for Cryptographic Applications. SP 800-22 Rev. 1a, April 2010. URL: https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-22r1a.pdf.

[8] The Marsaglia Random Number CDROM including the Diehard Battery of Tests of Randomness, 1995. URL: http://ftpmirror.your.org/pub/misc/diehard/.

[9] Mario Stipčević, True Random Number Generators. Open Problems in Mathematics and Computational Science, Open Problems in Mathematics and Computational Science 275-315) doi:10.1007/978-3-319-10683-0_12 URL: https://www.researchgate.net/publication/29

9824248_True_Random_Number_Generators.
[10] J. von Neumann. Various techniques for use in connection with random digits. Applied Math Series, Notes by G. E. Forsythe, in National Bureau of Standards, Vol. 12, 36 – 38, 1951. URL: https://mcnp.lanl.gov/pdf_files/nbs_vonneumann.pdf.
[11] Sunar, B. Martin, W. J. Stinson, D. R. A Provably Secure True Random Number Generator with Built-in Tolerance to Active Attacks doi:10.1109/TC.2007.250627 URL: https://cs.uwaterloo.ca/~dstinson/papers/rng-IEEE.pdf.
[12] Trevisan L. Extractors and Pseudorandom Generators 1999. Journal of the ACM URL: http://theory.stanford.edu/~trevisan/pubs/extractor-full.pdf
[13] Reshef, Yakir. On Resilient and Exposure-Resilient Functions. 2009. URL: https://www.math.harvard.edu/media/reshef.pdf.
[14] Shcherbyna, Y. Analysis of attacks in modern cyberphysical systems , Kazakova, N. , Fraze-Frazenko, O., Parchuts, L. , Schneider, S. CEUR Workshop Proceedings, 2019, 2683, pp. 12-14
[15] Ross S. A First Course in Probability. 8th Edition. 2010. ISBN-13: 978-0136033134 URL: http://julio.staff.ipb.ac.id/files/2015/02/Ross_8th_ed_English.pdf
[16] Sturges, H. (1926) The choice of a class-interval. J. Amer. Statist. Assoc., 21, P. 65–66. URL: https://www.tandfonline.com/doi/abs/10.1080/0162
[17] Freedman, D. and Diaconis, P. (1981) On this histogram as a density estimator: L2 theory. Zeit. Wahr. ver. Geb., 57, 453–476. URL: https://bayes.wustl.edu/Manual/FreedmanDiaconis1_1981.pdf

Model And Method For Identification Of Functional Security Profile

Anatolii Davydenko[1], Oleksandr Korchenko[2], Olena Vysotska[3], Ihor Ivanchenko[4]

[1,2,3,4] National Aviation University, Liubomyra Huzara ave. 1, Kyiv, 03058, Ukraine
[1] Pukhov Institute for modeling in energy engineering of NAS of Ukraine, General Naumov str. 15, Kyiv, 03164, Ukraine

Abstract

One of the key tasks during the state examination is the identification of the functional security profile. During the examination, the types of information that is processed and the risks of its loss, modification or disclosure are evaluated. For this, the functional security profile is being built. To solve the problem of identifying the functional security profile, it is necessary to: determine the levels of functional security services, implemented comprehensive information security systems of the object of examination; determination of the completeness and consistency of the profile; identification of the description of the functional security services in the source documents. The paper proposes a model of parameters for identifying the functional security profile in computer systems. A definition is given for the sets of criteria, their elements and levels. All this made it possible in a formal form to form the necessary set of quantities for the implementation of the identification of functional security profile in the computer systems. The development of these works is the development of a method for identifying functional security profile. This will automate the determination of the requirements of the regulatory document regarding the protection functions (security services) and guarantees, which will be done in subsequent articles.

Keywords

comprehensive information security systems state examinations, functional security profile, information security criteria, computer systems.

1. Introduction

One of the key tasks during the state examination is to identify the functional security profile. During examination evaluated the types of information [1-8], which is processed in the system and the risk of its loss, modification or disclosure. For this purpose, a functional security profile (FSP) is built which contains the lists of functional security service (FSS) and levels that are needed to ensure an acceptable level of information security.

Exactly FSP is the key element of public examinations and its analysis on accordance to the normative document is one of major tasks.

For the decision of task of FSP authentication, it is necessary to carry out: determination of FSS levels, implemented FSP examination object; determine completeness and consistency profile; FSS describe the identification in the original documents. To determine the completeness and consistency of rules to consider construction of FSP (see [9]), and automation of this process contacts with corresponding rules.

For the decision of task proposed model parameters for identifying the FSP in computer system (CS) and FSP identification method.

2. Determining the criteria set

As it's known [9], the criteria reflect methodological framework for determining requirements of information security in of computer systems against unauthorized access, the creation of protected CS and protection against unauthorized access, evaluation of information security in the CS and its suitability for the treatment of critical information (information that requires defense).

Given the above, let's form the set of all criteria for information security

$$\mathrm{MK} = \left\{ \bigcup_{q=1}^{w} \mathrm{MK}_q \right\} = \{ \mathrm{MK}_1, \mathrm{MK}_2, .., \mathrm{MK}_w \}, \quad (1)$$

where $\mathrm{MK}_q \subseteq \mathrm{MK}$ $(q = \overline{1,w})$ – q-th element of set of criteria MK, and w - its count.

EMAIL: davidenkoan@gmail.com (A. 1); icaocentre@nau.edu.ua (A. 2); lek_vys@ukr.net (A. 3); igor-p-l@ukr.net (A. 4)
ORCID: 0000-0001-6466-1690 (A. 1); 0000-0003-3376-0631 (A. 2); 0000-0002-9543-1385 (A. 3); 0000-0003-3415-9039 (A. 4)

3. Determining of element of the criteria set

Next, on the basis of (1) we define the elements of the $МК_q$ -th set of criteria

$$МК_q = \left\{\bigcup_{e=1}^{w_q} МК_{q,e}\right\} = \left\{МК_{q,1}, МК_{q,2}, .., МК_{q,w_q}\right\}, \quad (2)$$

where $МК_{q,e} \subseteq МК_q$ $(e = \overline{1,w_q})$ – e-th element $МК_q$ - th set of criteria, and w_q its count.

Thus, (1) with respect to (2) we present in the following form:

$$\begin{aligned} МК &= \left\{\bigcup_{q=1}^{w} МК_q\right\} = \left\{\bigcup_{q=1}^{w}\left\{\bigcup_{e=1}^{w_q} МК_{q,e}\right\}\right\} = \\ &= \left\{\left\{МК_{1,1}, МК_{1,2}, ..., МК_{1,w_1}\right\}, \right. \\ &\left\{МК_{2,1}, МК_{2,2}, ..., МК_{2,w_2}\right\}, ..., \\ &\left.\left\{МК_{w,1}, МК_{w,2}, ..., МК_{w,w_w}\right\}\right\}. \end{aligned} \quad (3)$$

4. Determination of levels of elements of the set criteria

Next, on the basis of (3) we define the level of each element $МК_{q,e}$ - th element $МК_q$ - th set criteria.

$$МК_{q,e} = \left\{\bigcup_{y=1}^{w_{q,e}} МК_{q,e,y}\right\} = \left\{МК_{q,e,1}, МК_{q,e,2}, .., МК_{q,e,w_{q,e}}\right\}, \quad (4)$$

where $МК_{q,e,y} \subseteq МК_{q,e}$ $(y = \overline{1,w_{q,e}})$ – y-th level $МК_{q,e}$-th element $МК_q$ - th set criteria and $w_{q,e}$ its maximum level.

Thus, (3) with respect to (4) has the form:

$$\begin{aligned} МК &= \left\{\bigcup_{q=1}^{w} МК_q\right\} = \left\{\bigcup_{q=1}^{w}\left\{\bigcup_{e=1}^{w_q} МК_{q,e}\right\}\right\} = \\ &= \left\{\bigcup_{q=1}^{w}\left\{\bigcup_{e=1}^{w_q}\left\{\bigcup_{y=1}^{w_{q,e}} МК_{q,e,y}\right\}\right\}\right\} = \\ &= \left\{\bigcup_{q=1}^{w}\left\{\bigcup_{e=1}^{w_q}\left\{МК_{q,e,1}, МК_{q,e,2}, ..., МК_{q,e,w_{q,e}}\right\}\right\}\right\} = \\ &\left\{\bigcup_{q=1}^{w}\left\{\left\{МК_{q,1,1}, МК_{q,1,2}, ..., МК_{q,1,w_{q,1}}\right\}\right\}\left\{МК_{q,2,1}, МК_{q,2,2}, ..., МК_{q,2,w_{q,2}}\right\}, \right. \\ &\left., \left\{МК_{q,w_q,1}, МК_{q,w_q,2}, ..., МК_{q,w_q,w_{q,w_q}}\right\}\right\}\right\} = \\ &= \left\{\left\{\left\{МК_{1,1,1}, МК_{1,1,2}, ..., МК_{1,1,w_{1,1}}\right\}, \left\{МК_{1,2,1}, МК_{1,2,2}, ..., МК_{1,2,w_{1,2}}\right\}, .., \right.\right. \\ &\left\{МК_{1,w_1,1}, МК_{1,w_1,2}, ..., МК_{1,w_1,w_{1,w_1}}\right\}\right\}, \left\{\left\{МК_{2,1,1}, МК_{2,1,2}, ..., МК_{2,1,w_{2,1}}\right\}, \\ &\left\{МК_{2,2,1}, МК_{2,2,2}, ..., МК_{2,2,w_{2,2}}\right\}, .., \left\{МК_{2,w_2,1}, МК_{2,w_2,2}, ..., МК_{2,w_2,w_{2,w_2}}\right\}\right\}, \\ &..., \left\{\left\{МК_{w,1,1}, МК_{w,1,2}, ..., МК_{w,1,w_{w,1}}\right\}, \left\{МК_{w,2,1}, МК_{w,2,2}, ..., МК_{w,2,w_{w,2}}\right\}, \right. \\ &\left.\left.\left., \left\{МК_{w,w_w,1}, МК_{w,w_w,2}, ..., МК_{w,w_w,w_{w,w_w}}\right\}\right\}\right\}. \end{aligned} \quad (5)$$

5. Formation of the method of identification of FSP

Step 1. Formation of the primary set of functional security services.

As previously described, the levels of the elements of the sets of criteria are determined by $МК_{q,e,y}$ where $y = \overline{1,w_{q,e}}$ – y-th level of $МК_{q,e}$-th element of $МК_q$ - th set criteria and $w_{q,e}$ its maximum level. Thus, we define the primary set (PS) of functional security services (FSS) as the union of elements of sets of criteria defined by the expert:

$$ПМ_p = \left\{\bigcup_{f=1}^{k} ПМ_{p,f}\right\} = \left\{ПМ_{p,1}, ПМ_{p,2}..., ПМ_{p,k}\right\}, \quad (6)$$

where k - the number of primary projects [2] identified by the expert.

Step 2. Formation of secondary sets of functional security services.

Next, we form an FSSSS, which consists elements of a set of criteria $МК$, that have levels that characterize the FSS according to [9]. In turn, the FFP function is intended to display from a set of PS into one or more elements of the set $МК$ by means of which can form a set of all possible functions from the elements, $ПМ_f$, $f = \overline{1,k}$. We define the number of SS of the FSS:

$$\begin{aligned} ВМ_p &= \left\{\bigcup_{f=1}^{k} ВМ_{p,f}\right\} = \left\{\bigcup_{f=1}^{k} ФВП(ПМ_{p,f})\right\} = \\ &= \left\{ВМ_{p,1}, ВМ_{p,2}, ..., ВМ_{p,k}\right\} = \\ &= \left\{ФВП(ПМ_{p,1}), ФВП(ПМ_{p,2}), ..., ФВП(ПМ_{p,k})\right\}, \end{aligned} \quad (7)$$

where k - respectively, the number of secondary

functional security services of the project and mapping from the set of PS to one or more elements of the $\mathbf{МК}$ set of the project.

Step 3. Formation of a basic FSP**.**

The Basic Functional Security Profile (FSP), given the expertise and facility requirements to ensure the safe flow of information, consists of a set of primary (PS) and secondary (SS) FSS. Let us define the FSP:

$$\text{БЗ}_\text{р} = \left\{\left\{\bigcup_{\text{f}=1}^{\text{k}} \text{ФВП}(\text{ПМ}_{\text{p,f}})\right\}, \left\{\bigcup_{\text{f}=1}^{\text{k}} \text{ВМ}_{\text{p,f}}\right\}\right\} =$$

$$= \left\{\left\{\text{ФВП}(\text{ПМ}_{\text{p,1}}), \text{ФВП}(\text{ПМ}_{\text{p,2}}), .., \text{ФВП}(\text{ПМ}_{\text{p,k}})\right\},\right.$$

$$\left.\left\{\text{ВМ}_{\text{p,1}}, \text{ВМ}_{\text{p,2}}, .., \text{ВМ}_{\text{p,k}}\right\}\right\},$$

where $\text{БЗ}_\text{р}$ – basic functional profile of protection of the project.

Step 4. Forming a set of order by element indices $\text{МК}_{\text{q,e,y}}$

Using (6), taking into account [9], we form a set of order by indices:

$$\text{БЗ}_{\text{ПМЕ}} = \{\text{МК}_{1,1,4},\ \text{МК}_{1,2,4},\ \text{МК}_{1,3,2},\ \text{МК}_{2,1,4}, \text{МК}_{2,2,4},$$
$$\text{МК}_{2,3,2}, \text{МК}_{2,4,3},\ \text{МК}_{3,1,3}, \text{МК}_{3,2,3},\ \text{МК}_{3,3,3}, \text{МК}_{3,4,3},$$
$$\text{МК}_{4,1,5}, \text{МК}_{4,2,2}, \text{МК}_{4,3,2}\ , \text{МК}_{4,4,3}, \text{МК}_{4,5,3}, \text{МК}_{4,6,2},$$
$$\text{МК}_{4,8,1},\ \text{МК}_{4,9,1}\} = \{\text{КД-4, КА-4, КО-1, КК-2, КВ-4,}$$
$$\text{ЦД-4, ЦА-4, ЦО-2,ЦВ-3, ДР-3, ДС-3, ДЗ-3, ДВ-3,}$$
$$\text{НР-5, НИ-2, НК-2, НО-3, НЦ-3,НТ-2, НА-1,}$$
$$\text{НП-1, НВ-2, НА-1, НП-1}\}$$

Step 5. Minimizing the basic FSP

Using (7) taking into account [9] we minimize the basic FPP by the highest y-th index:

$$\text{БЗ}_\text{р}^{\min} = \left\{\bigcup_{\text{q}=1}^{\text{w}} \left\{\bigcup_{\text{e}=1}^{\text{w}_\text{q}} \left\{\bigvee_{\text{y}=1}^{\text{w}_{\text{q,e}}} \text{МК}_{\text{q,e,y}}\right\}\right\}\right\} =$$

$$= \left\{\bigcup_{\text{q}=1}^{\text{w}} \left\{\bigcup_{\text{e}=1}^{\text{w}_\text{q}} \left\{\text{МК}_{\text{q,e,1}} \vee, \text{МК}_{\text{q,e,2}} \vee, ..., \vee \text{МК}_{\text{q,e,w}_{\text{q,e}}}\right\}\right\}\right\} =$$

$$= \left\{\bigcup_{\text{q}=1}^{\text{w}} \left\{\left\{\text{МК}_{\text{q,1,1}} \vee, \text{МК}_{\text{q,1,2}} \vee, ..., \vee \text{МК}_{\text{q,1,w}_{\text{q,1}}}\right\}\right.\right.$$
$$\left\{\text{МК}_{\text{q,2,1}} \vee, \text{МК}_{\text{q,2,2}} \vee, ..., \vee \text{МК}_{\text{q,2,w}_{\text{q,2}}}\right\}, ..,$$
$$\left.\left.\left\{\text{МК}_{\text{q,w}_\text{q},1} \vee, \text{МК}_{\text{q,w}_\text{q},2} \vee, ..., \vee \text{МК}_{\text{q,w}_\text{q},\text{w}_{\text{q,w}_\text{q}}}\right\}\right\}\right\} =$$

$$= \left\{\left\{\left\{\text{МК}_{1,1,1} \vee, \text{МК}_{1,1,2} \vee, ..., \vee \text{МК}_{1,1,\text{w}1,1}\right\},\right.\right.$$
$$\left\{\text{МК}_{1,2,1} \vee, \text{МК}_{1,2,2} \vee, ..., \vee \text{МК}_{1,2,\text{w}1,2}\right\}, .., \qquad (8)$$
$$\left.\left\{\text{МК}_{1,\text{w}1,1} \vee, \text{МК}_{1,\text{w}1,2} \vee, ..., \vee \text{МК}_{1,\text{w}1,\text{w}1,\text{w}1}\right\}\right\},$$
$$\left\{\left\{\text{МК}_{2,1,1} \vee, \text{МК}_{2,1,2} \vee, ..., \vee \text{МК}_{2,1,\text{w}2,1}\right\},\right.$$
$$\left\{\text{МК}_{2,2,1} \vee, \text{МК}_{2,2,2} \vee, ..., \vee \text{МК}_{2,2,\text{w}2,2}\right\}, ...$$
$$\left.\left\{\text{МК}_{2,\text{w}2,1} \vee, \text{МК}_{2,\text{w}2,2}, \vee ..., \vee \text{МК}_{2,\text{w}2,\text{w}2,\text{w}2}\right\}\right\}, ...,$$
$$\left\{\left\{\text{МК}_{\text{w},1,1} \vee, \text{МК}_{\text{w},1,2} \vee, ..., \vee \text{МК}_{\text{w},1,\text{w}_{\text{w}},1}\right\},\right.$$
$$\left\{\text{МК}_{\text{w},2,1} \vee, \text{МК}_{\text{w},2,2} \vee, ..., \vee \text{МК}_{\text{w},2,\text{w}_{\text{w}},2}\right\}, ..,$$
$$\left.\left.\left\{\text{МК}_{\text{w},\text{w}_{\text{w}},1} \vee, \text{МК}_{\text{w},\text{w}_{\text{w}},2} \vee, ..., \vee \text{МК}_{\text{w},\text{w}_{\text{w}},\text{w}_{\text{w}},\text{w}_{\text{w}}}\right\}\right\}\right\},$$

As a result, I have developed a system that analyzes the input documents for the presence of a FSP and its identification by the formal characteristics of the [9].

In case of errors, corrects FSP. The system is implemented on the .NET platform in C# programming language using the Microsoft Visual Studio development environment.

The implementation of a software module for identifying a functional security profile is intended to assist the expert in identifying the FSP in a Microsoft Word document, and to assist the expert in the analysis of the FSP. The main purpose of this software module is to assist the expert in the creation of the FSP and to control compliance with the conditions set out in the regulatory document [9], namely: determination of integrity control; takeovers by the highest FSS of lower ones; checking the correlation of the FSS.

The software module is written in C# programming language in VisualStudio 2005. In the written code technology used MSOffice'sCOMInterop, namely Microsoft.Office.Interop.Word library and basic libraries of programming language C#.

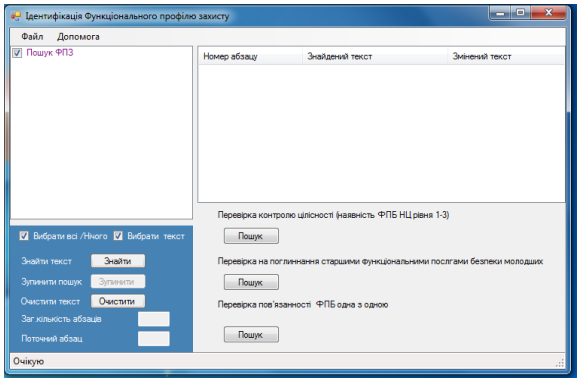


Figure 1: Program interface

The interface of the program module (Fig. 1) is a window application, which is implemented in the form of a GUI program, in which there are the following controls: a window box type "Listbox" search for a functional security profile; buttons: "Find", "Stop", "Clear"; the right part of the screen has a window of type "ListView", which displays the paragraph number where the FPP was found and the security profile found; three buttons to search for compliance of the FPP with the terms of the regulatory document [9]; two textboxes of type "TextBox" in one of which the total number of paragraphs of the document is displayed, and in the other field the current paragraph when processing the document; a «statusStrip» type window with three positions: "Pending", "Search started", "Search is complete"; two window boxes of the type "CheckedBox" in one of which there is a possibility to deselect or select the search of the FSP, and in the other field there is an opportunity to go to the specified part of the FSP search text; window menu type "menuStrip", which contains two tabs: "File", "Help".

Microsoft Word is a specialized hierarchical, COM-oriented data warehouse - Structured Storage. A document can contain different types of data: structured text, graphics, mathematical expressions, organizational charts, etc. The concept of structured repository is an integral part of the modern programming paradigm based on the Component Object Model (COM). In fact, structured storage is the technology of combining objects (files) of objects with different nature and properties into one logical unit of storage. COM technology offers the standard implementation of the concept of structured storage in the form of a compound file (Compound File): a file system inside the file. The COM repository is a hierarchical structure of collections of objects of two types: Storage and Stream, to which directories and files correspond in the traditional file system. This approach can significantly reduce the storage costs in a single file of objects of different nature.

The implementation of the program includes methods of regular expressions: comparison of strings; suffix tree; approximating patterns; patterns with which multiple choices can be made, partial patterns. It is shown that technologies that combine the properties of approximating patterns and patterns by which multiple choice can be made, solve the problems of FSP analysis and can be used to build a system.

Testing of the program module was carried out in the process of the state examination of the CISS Grid site. The work of the software module resulted in the fulfillment of the tasks for the search of the FSP and analysis of the FSP for compliance with the three conditions. Performance analysis using the software module showed a multiple increase in the speed of document processing in the absence of errors, namely - the software module eliminated the repetition of the FSS, performed a check of integrity and completeness. The analysis of execution with the help of the program showed many increase of speed of processing of the document at 100% absence of errors, namely, the program excluded inclusion in the FPP of the same type of services, performed the check of integrity and completeness. Approximate time of processing of documents was: Technical task - 17 sec; Explanatory note to the technical project - 43 seconds; Act of inspection - 7 sec .; Information Security Policy - 12 sec. The program was run on a workstation with the following specifications: Intel Core i5-4670 CPU with 3.4 GHz; RAM - 8 GB.

The volume of the document is 8635 words. The average speed of reading in Ukrainian in an adult is within 150-200 words per minute [10], according to experimental studies, the average speed is 201 words per minute (with scatter of values from 60 to 378) with an average percentage of mastering 52 words per minute. Table 1 summarizes the time required for the expert to process the standard inputs of the CISS examination. It is only 43 minutes to read the “Terms of Reference”. Analysis time depends on the experience of the expert and can not be less than reading time. Therefore, the acceleration of processing will be at about fifteen thousand percent.

Table 1
Time required to process documents

Document Name	The total number of words	Minimum Read Time (min)
Terms of Reference	8635	43
Explanatory note to technical project	22641	113
Inspection Act	2235	11
Information Security Policy	5206	26

Let's consider software features. Software Components:

1. Knowledge base;
2. User interface;
3. Software module "Meaning constants";
4. Software module "FSP Identification";
5. Software module "Determination of FSP";

Meaning Constants module. The module should ensure that semantic constants are extracted from the input documents by forming a set of defined constants in the knowledge base and inserting these constants into the output document templates by a defined algorithm.

The Subsystem of Meaning Constants module performs the following functions:

• selection of semantic constants from input documents;

• formation of knowledge base of semantic constants;

• Completing source document templates.

Module « FSP Determination» ensures that the FSP complies with the three criteria of RD STPI 2.5.004-99 [9]. The subsystem "Determination of FSP" ensures the following functions:

The FSP is obliged to include the control of the integrity of the STPI:

• the connection of the FSP to each other according to the RD STPI 2.5.004-99;

• if the service has any too FSS or more, then FSP can include only one functional security service.

FSP Identification Module

The module should ensure the formal compliance of the PSP with the format of the FSS description, as well as give the expert, in an interactive mode, the possibility to analyze the FSP in accordance with the normative document of the RD STPI 2.5.004-99.

The subsystem "Determination of FSP" must ensure the following functions:

• check the description of the FSP;

• provide the expert with the opportunity to receive extended information about the service in an interactive mode at events of type mouse focus.

According to testing methods, one can classify, for example, as black box testing or behavioral testing - a strategy (method) for testing the functional behavior of an object (program, system) from the point of view of the outside world, in which knowledge about the internal structure of the tested object is not used. Strategy refers to systematic methods for selecting and creating tests for a test suite. The behavioral test strategy is based on technical requirements and their specifications [2]. The "black box" refers to the object of study, the internal structure of which is unknown. The concept of a "black box" was proposed by Ashby, William Ross. In cybernetics, it allows you to study the behavior of systems, that is, their reactions to a variety of external influences and at the same time abstract from their internal structure. Manipulating only with inputs and outputs, it is possible to conduct certain studies. In practice, the question always arises of how the black box homomorphism reflects the adequacy of its studied model, that is, how fully the basic properties of the original are reflected in the model. The description of any control system in time is characterized by a picture of the sequence of its states in the process of moving toward its goal. The transformation in the control system can be either one-to-one and then it is called isomorphic, or only unambiguous, in one direction. In this case, the transformation is called homomorphic. The "black" box is a complex homomorphic model of a cybernetic system in which diversity is respected. It is only then a satisfactory system model when it contains such an amount of information that reflects the diversity of the system. It can be assumed that the greater the number of perturbations acting on the inputs of the system model, the greater the variety the regulator should have. Currently, two types of "black" boxes are known. The first type includes any "black" box, which can be considered as an automaton, called finite or infinite. The behavior of such "black" boxes is known. The second type includes such "black" boxes, whose behavior can be observed only in the experiment. In this case, a hypothesis is expressed explicitly or implicitly about the predictability of the behavior of the black box in a probabilistic sense. Without a preliminary hypothesis, any generalization is

impossible, or, as they say, it is impossible to draw an inductive conclusion based on experiments with the black box. To designate the model of the "black" box, N. Wiener proposed the concept of a "white" box. The "white" box consists of known components, that is, known X, Y, δ, λ. Its contents are specially selected to implement the same dependence of the output on the input as the corresponding "black" box. In the process of research and generalizations, hypotheses and establishing patterns, it becomes necessary to adjust the organization of the "white" box and change models. In this regard, when modeling, the researcher must necessarily repeatedly refer to the scheme of relations "black" - "white" box. Creating a mathematical description of a black box is a kind of art. In some cases, it is possible to form an algorithm in accordance with which the "black" box responds to an arbitrary input signal. The main methods of testing a black box are: – equivalent partition; – analysis of boundary values; – analysis of cause and effect relationships; – assumption of error. A tester with extensive experience seeks out errors without any methods, but at the same time, he unconsciously uses the method of assuming an error. This method is largely based on intuition. The main idea of the method is to make a list that lists possible errors and situations in which these errors could occur. Then, based on the list, tests are compiled.It's possible that it's more correct to talk about different degrees of transparency, and maybe even generally about different colors of the box, rather than testing using the black method and the white box method. The only important thing is what information we take into account when designing tests. Either we use information about the internal structure of the program, or we do not use it. The following CISS components were subject to testing:

1) OS protection and administration tools;

2) security features (security services) of middleware;

3) means of increasing accessibility;

4) organizational measures to protect information, software and hardware;

5) documentation on CISS according to the list defined by the requirements of TR.

The purpose of the CISS tests are:

- verification of the implementation and sufficiency of organizational measures of protection given in the documentation;

- verification of compliance with the requirements of section 10 "Criteria of guarantees" RD STPI 2.5-004-99 for the level of guarantees of the correct implementation of the G2 security functions in relation to the CIS architecture, CIS development environment, CIS development sequence, CIS functioning environment, documentation and tests of CIS.

Verification of compliance with the conditions for the implementation of information security services is carried out in accordance with the FSP:

3.КЦД = {КА-2, КД-2, КВ-1, ЦА-1 , ЦД-1, ЦВ-1, ДС-1, ДЗ-2, ДВ-1, НР-2, НИ-2, НК-1, НО-1, НЦ-2, НТ-2, НВ-1}

6. Conclusion

The paper offers a model of parameters which due to the theoretical and multiple representation of certain sets of criteria for information security, their elements and corresponding levels, allowed to formally form the necessary set of values for the implementation of the identification of FSP in the CS. In addition, a method for identifying the FSP was developed which made it possible to automate the process of determining requirements [9] for security features (security services) and guarantees. As a result, a software module was created that eliminates the repetition of the FSS, performed integrity and completeness checks.

7. References

[1] About information: Law of Ukraine of October 2, 1992 No. 2657-XII, ed. Law No. 2938 – VI of 13.01.2011. OVR, № 32, Art. 313 (2011.) (in Ukrainian).

[2] Beiser B.: Black Box Testing. Technology functional testing software and systems. Peter, p. 320 (2004). (in Russian)

[3] Zegzhda D.P., Ivashko A.M.: Fundamentals of security of information systems. Textbook manual for universities, p.451 (2000). (in Russian)

[4] Korchenko O.G, Davydenko A.M, Shaban M.R.: Model of parameters for identification of functional protection profile in computer systems. Security of Information. vol. 25, No.2, pp. 122-126 (2019). (in Ukrainian). DOI: https://doi.org/10.18372/2225-5036.25.13844

[5] Vysotska O., Davydenko A.: Keystroke Pattern Authentication of Computer Systems Users as One of the Steps of Multifactor Authentication. In: Hu Z., Petoukhov S.,

Dychka I., He M. (eds). Advances in Computer Science for Engineering and Education II. ICCSEEA 2019. Advances in Intelligent Systems and Computing, vol. 938, pp. 356-368 (2019). DOI: https://doi.org/10.1007/978-3-030-16621-2_33

[6] Kazmirchuk, S., Ilyenko A., Ilyenko S.: Digital signature authentication scheme with message recovery based on the use of elliptic curves In: Hu Z., Petoukhov S., Dychka I., He M. (eds). Advances in Computer Science for Engineering and Education II. ICCSEEA 2019. Advances in Intelligent Systems and Computing, vol. 938, pp. 279–288 (2019). DOI: https://doi.org/10.1007/978-3-030-16621-2_26

[7] Zadeh L.: Fuzzy sets. Inform. Control, vol. 8, no. 3, pp. 338-353 (1965)

[8] Lakhno V., Kazmirchuk S., Kovalenko Y., Myrutenko L., Zhmurko T.: Design of adaptive system of detection of cyber-attacks, based on the model of logical procedures and the coverage matrices of features. Eastern-European Journal of Enterprise Technologies, vol. 3, Issue 9 (81), pp. 30–38 (2016). DOI: https://doi.org/10.15587/1729-4061.2016.71769

[9] RD STPI 2.5-004-99 Criteria for evaluation of information security in computer systems against unauthorized access, approved by the Order of the Department of Special Telecommunication Systems and Information Protection of the Security Service of Ukraine dated April 28, 1999, No. 22. (in Ukrainian).

[10] Korchenko O.G., Davydenko A.M., Shaban M.R.: A decomposition model for the representation of semantic constants and variables for the implementation of expertise in the field of STPI. Information Security, vol. 21, No.2, pp. 88-96 (2019). (in Ukrainian). DOI: https://doi.org/ 10.18372/2410-7840.21.13766

Information Support For Making Strategic Decisions On The Development Of An Industrial Enterprise

Iryna Otenko [1], Marharyta Podorozhna[2], Vasyl Otenko [3]

[1,2,3] *Simon Kuznets Kharkiv National University of Economics, ave. Nauki, 9-A, Kharkiv, 61166 Ukraine*

Abstract

Support of strategic decisions on the development of enterprise by information technology provides an opportunity to study in more detail each source of information and draw conclusions. The main role is played by the completeness, timeliness and reliability of information. There are high requirements for it. The clarity of the tasks, data analysis, efficiency of processing the results depend on the qualifications of the staff and technologies used in the enterprise. Strategic decisions reflect the interaction of the campaign and the external environment. Therefore, the company needs to adapt to the external environment, which is constantly changing.

Keywords

strategy, strategic decisions, support, information, information support, information technology.

1. Introduction

Information support for making strategic decisions on enterprise development involves the accumulation and storage of information, ensuring access to it for all stakeholders in the innovative development of the enterprise. Innovative employees must be technologically and market-aware, which will form the necessary information base to create not only product, but also organizational and marketing innovative ideas. Thus, such information base should include knowledge of past experience and promising areas of development in such important areas as: features of corporate business strategy, its possible changes; application of effective management methods; significance and features of the implemented information technologies; changes in the organizational structure of the enterprise, the distribution of powers and responsibilities, as well as the goals that must be achieved through these changes; features of application of modern quality control systems, certification of goods, works and services; introduction of modern systems of logistics and supply of raw materials, materials, components; creation and activity of specialized divisions on carrying out of researches and developments, practical realization of scientific and technical achievements; implementation and operation of corporate knowledge management systems; available staff development activities; the degree of use of third-party services by the enterprise (consulting, outsourcing, etc.); information on technical characteristics of products, their range and nomenclature, the degree of diversification of production; advantages and disadvantages (technical and economic parameters of competitiveness) of enterprise products; introduced and promising significant changes in the design of goods and services; implemented and planned changes in the packaging of goods; results of implementation of marketing strategies, actual and perspective market shares, key market segments of consumers; the results of the use of old and new methods of promoting goods; data on the efficiency of existing distribution and sales channels; features of pricing strategies of the enterprise and the results of their implementation. [1,2,3,4].

The accuracy, completeness and timeliness of the necessary information play an important role in these

EMAIL: otenkoip@gmail.com.ua (A. 1); rita.margarita0398@gmail.com (A. 2); ovi@hneu.edu.ua (A. 3)
ORCID: 0000-0001-7849-2381 (A. 1); rita.margarita0398@gmail.com (A. 2); 0000-0002-5979-1084 (A. 3)

processes. There are high requirements for it. The clarity of the tasks, data analysis, efficiency of processing the results depend on the qualifications of the staff and the technologies used (Table 1).

Table 1
Content of works on information support of strategic decision-making

Stages	Contents of works
Data preparation and analysis	- data acquisition and preparation: observation and search; data acquisition and perception; data filtering and presentation; situation detection; − problem statement: identification and formulation of the problem situation; determining the structure of the problem situation
Problem setting and development of alternatives	- problem statement: qualification of connection factors; definition of goals and criteria; determination of conditions; coordination and evaluation of task components; task formulation, − model development, search, development and selection of problem solving method; − development of alternatives, grouping of alternatives by goals / criteria and conditions / resources; − forecasting and evaluation implementation of alternatives
Making a strategic decision	- definition (refinement) of selection criteria: definition of selection profiles; generalization of the manifestation of the criteria of preference for selection; − selection of criteria; − design of the decision: interpretation and evaluation of the results of the choice (decision); development and issuance of directives for the implementation of the decision

2. Presentation of the main material

Problems of strategic decision-making are called problems of unique choice, when the new object of choice or the situation in which it is implemented is new during its implementation [5]. The basis for highlighting the existing problems of formation of information and analytical support for strategic decision-making in machine-building enterprises were the methods of questionnaires, observation and expert evaluation. The study of problems of information and analytical support for strategic decision-making was conducted during 2017-2018 at 18 machine-building enterprises in the Kharkiv region [6]. In order to study the relevance of the issue of formation of information and analytical support for strategic decision-making, its importance for the enterprise was assessed. Thus, 14 enterprises out of 18 surveyed stated the high importance of having a modern system of information and analytical support. The main requirements for information and analytical support of strategic decision-making in the enterprise are presented in table 2.

Table 2
Basic requirements for information and analytical support of strategic decision-making at the enterprise

Requirements	Explanation
Openness and ease of access to information	Mobility − scalability of applications, portability to other objects. Binding applications to a specific manager and specific computing and operating systems. Configuration of functionality and user interfaces in a distributed structure
Compliance with the basic principles of document support	Regulated automated document management. Unity of accounting, control and storage of documents. Unity of substantive and

	formal accounting. Unity of synthetic and analytical accounting. Multicurrency.
Creating a single information space	Spatial distribution of users. Real-time information system operation. Expanding global telecommunications capabilities. Intra-system information connectivity. Multiple interfaces
Preference for specific management characteristics and user managers, user interface specifications	Description of structure, composition of functions and powers. Integrated system data transmission for various communication schemes. Configuration of services (including information protection and interaction regulations). Configuration of intersystem interfaces.
Reliability, security and safety	Redundancy, including technical and information duplication. Multiple levels of protection. Authorization and control of access to the system for individual operations.
Ensuring the controllability of the control object	Management of development strategy and tactics. Analysis of the state of the external and internal environment. Consolidation of networks of branches and subsidiaries and their management. Management of resources, portfolios of assets and liabilities. Administration of electronic document management, rights and responsibilities.
Unified regulations for documentation, maintenance and modification	
Multi-level system of analysis and preparation of decision-making with a flexible graphical user interface.	

But in fact, from the point of view of employees of enterprises, the system of information and analytical support for strategic decision-making exists in 6 out of 18 surveyed enterprises (30%). From this we can conclude that in general there is a need for information and analytical support for strategic decision-making, but such a need is not met in domestic enterprises. Moreover, the relationship between the need for information and analytical support and the actual use is low (table 3). This is confirmed by the calculation of the contingency ratio for dichotomous variables (K = 0.013), the low value of which indicates the lack of connection between the need and the actual implementation of the system of information and analytical support for strategic decision-making.

Table 3

The results of the survey on the importance and availability of information and analytical support for strategic decision-making (IAZ AKP) in the studied machine-building enterprises

Indicator	**Importance of IAZ AKP (high / low)**	**There is a problem with the implementation of IAZ AKP (exists / does not exist)**
Number of enterprises out of 18 surveyed	14/4	6/12
Contingency ratio	0,013	

The research conducted at the selected enterprises was aimed at identifying the need for information and analytical support for strategic decision-making and analysis of information on the existing problems of formation and use of such support. Selected problems of strategic decision-making in enterprises are presented in table. 4. The peculiarity of the selected problems is that in the current management of the enterprise they are almost not felt − because for the current

management of information support, strategic decision-making itself is often not of particular value, looks like an abstraction or refers to the future. But this does not diminish the importance of the problem in the context of strategic development management.

Table 4
Problems of formation and use of information-analytical support of strategic decision-making (IAZ AKP) on development of researched enterprises

Problems of formation and use of information-analytical support of AKP	Number of enterprises out of 18 surveyed in which such a problem exists	The importance of the problem for enterprise management
1. IAZ AKP is not formed at all	6	4,8
2. The company does not have specialized IT tools (software) for the formation of IAZ AKP	11	3,6
3. The company has no specialized units and specialists with IAZ AKP	9	2,2
4. Elements and separate information of IAZ AKP are realized by various divisions which activity concerning IAZ AKP is not coordinated	9	2,4
5. The company does not allocate funds for IAZ AKP	8	4,6
6. The company's staff (including top management) has no information on current capabilities on the tools of IAZ AKP	10	4,2
7. The company uses some elements of IAZ AKP, which are not complete and integrated into the management system	5	3,5
8. IAZ AKP is formed, but information flows are not consistent with each other	4	3,8
9. The existing elements of the IAZ AKP do not meet the information needs of information users	10	4,6
10. The existing elements of IAZ AKP are realized inertially	4	2,4
11. The results are qualitative, but do not find full use in AKP	3	2,0

Table 4 shows the number of enterprises that have these problems and provides an assessment of the importance of such a problem for strategic decision-making in the enterprise. The number of enterprises appears as a discrete quantity and varies from 1 to 18 (total sample size). The importance of the problem appears as a subjective interval value, which is estimated by an expert on the basis of the involvement of the company's specialists for evaluation on a five-point scale, followed by averaging on the basis of arithmetic mean. The number of expert groups for each of the

surveyed enterprises is different and varies from 3 to 11 people. The resulting importance of the problem for enterprise management is calculated as the arithmetic mean of estimates of the importance of such a problem for all enterprises for which such a problem exists. From this point of view, it is possible to distribute the presented problem issues (Table 4) according to two criteria − "importance" and "frequency" of the problem (according to the number of the stated problem question). According to these estimates, we can conclude that among the most serious issues in the formation of information and analytical support for strategic decision-making and are the most typical (as they occur quite often) include: paragraph 1, the lack of formation of IAZ AKP; item 2 lack of specialized tools; item 5 absence or insufficiency of actual financing of IAZ AKP; item 6 ignorance of the personnel of the enterprise concerning use and possibilities of IAZ AKP; Clause 9 inconsistency of IAZ AKP elements (if any) with the needs of information users.These issues should be the first focus of managerial attention in the case of trying to solve the problem of forming information and analytical support for strategic decision-making in the enterprise.

3. Conclusion

Important in managing the development of the enterprise, but the frequency of its occurrence can be considered partial rather than universal. On the contrary, the problems of the lack of specialists with IAZ AKP, as well as the low coordination of actions for the formation of IAZ AKP are quite common, but their importance is relatively insignificant. Problems of weak connection of elements of IAZ AKP with strategy of development of the enterprise and needs of users, insufficient use of the received results, despite their theoretical significance, from the subjective point of view of managers of researched enterprises are not too frequent and have rather small importance for enterprise development management. Therefore, in addition to providing information support for strategic decision-making, the problem of forming their organizational support is relevant.

4. References

[1] The use of IT in marketing. URL: https://sites/googl/com

[2] Voronkova AE, Kalyuzhna NG, Otenko VI Management decisions in ensuring the competitiveness of the enterprise: organizational aspect: monograph. Kharkiv: VD "INZHEK", 2008. 512 pp.

[3] Sectoral export strategy of mechanical engineering. Analytical reference. URL: http://ref.org.ua/upload/iblock/d96/Analitical_Report_Machinery_Sector_Ukr_27.11.2018_edit_03.12.2018_VK.doc

[4] Managing change. Harvard Business Review: Bill Munck, Robert Kegan, Lisa Laskow Lahe, Debra E. Meyerson, Donald Sull, Katherine M. Hudson, Paul F. Levy. "Alpina Publisher", 2016.

[5] Gamie AM Methodical support of research of organizational development of the enterprise. Modeling of the regional economy: coll. Science. wash. Ivano-Frankivsk: Precarpathian National University. Vasily Stefanik, 2016. № 2 (28). Pp. 165–173.

[6] Hamie AM, Otenko VI Tools for making strategic decisions in the business activities of industrial enterprises. Business Inform. 2020. № 12. S. 417–422.

Real-time Cybersecurity Risk Assessment

Oleksandr Korchenko [1], Svitlana Kazmirchuk [1], Tetiana Panivko-Babenko [1], Stanislav Milevskyi [2] and Volodymyr Aleksiyev [2]

[1] *National Aviation University, Liubomyra Huzara ave., Kyiv, 03058, Ukraine*
[2] *Simon Kuznets Kharkiv National University of Economics, Nauki ave., 9a, Kharkiv, 61166, Ukraine*

Abstract

The structural solution of the real-time information security risks assessment system is developed, which, due to the structural components of the subsystems of primary and secondary data generation, as well as their components of input data initialization modules, formation and conversion of reference values, weighing evaluation parameters and their adjustment, evaluation of risk degree and report generation, in which the proposed method is implemented, allows to provide certain properties of adaptability and efficiency in risks assessment in real time.

Keywords

Information security, risks assessment, risk degree, software, report

1. Introduction

Often in the risks analysis and assessment (RAA) it is not always possible to involve relevant specialists, and there are situations in which the expert can not always unambiguously assess a particular vulnerability of information systems resources (ISR). It is proposed to use appropriate databases (DB) of vulnerabilities (in which their quantitative estimates are presented), such as the National Vulnerability Database (NVD), Open Sourced Vulnerability Database (OSVDB), IBM X-Force, US-CERT VND, SecurityFocus and etc. The basic component of such databases is CVSS - indicators that can be used as an alternative to expert estimates.

In practice, for example, there may be situations where it is necessary to carry out operational assessment and monitoring (real-time) of risks without the involvement of these experts, and the available methods and tools of RA do not provide such an opportunity.

On this basis, we will develop a method of risk assessment (RA), which will implement an alternative RA using known databases without the involvement of experts in the relevant field.

Use only styles embedded in the document. For paragraph, use Normal. Paragraph text. Paragraph text. Paragraph text. Paragraph text.

2. Method of assessing information security risks based on open databases of vulnerabilities

Let's consider in details its work, which is based on 11 steps.

Step 1 (Determining the complete set of RIS identifiers and vulnerabilities)

The first step determines the complete set of identifiers of all RIS, ie

$$\boldsymbol{RIS} = \{\bigcup_{rs=1}^{r} RIS_{rs}\} \quad (rs = \overline{1,r}),$$

where r – the number of all resources (and, accordingly, their identifiers), as well as the full set of vulnerabilities

$$\boldsymbol{V} = \{\bigcup_{uz=1}^{n} V_{uz}\} \quad (uz = \overline{1,n}),$$

where n – the number of all vulnerabilities (and, accordingly, their identifiers). Based on and experts can identify sets of RIS and vulnerabilities

EMAIL: oleksandr.korchenko@npp.nau.edu.ua (A. 1); sv.kazmirchuk@nau.edu.ua (A. 2); pani.tasha@gmail.com (A. 3); Stanislav.Milevskiy@hneu.net (A. 4); aleksiyev@gmail.com (A. 5)
ORCID: 0000-0003-3376-0631 (A. 1); 0000-0001-6083-251X (A. 2); 0000-0003-2085-3783 (A. 3); 0000-0001-5087-7036 (A. 4); 0000-0001-6767-7524 (A. 4)

by object of assessment. To create appropriate sets (as a basis), for example, a known database of NVD vulnerabilities can be used.

Step 2 (Determining the set of RIS identifiers and vulnerabilities for the object of evaluation)

Here, based on the set $\boldsymbol{RIS}$ for a specific object of evaluation, experts determine the required set of RIS (and, accordingly, their identifiers) $\boldsymbol{RISO}$ ($\boldsymbol{RISO} \subset \boldsymbol{RIS}$), that is

$$\boldsymbol{RISO} = \{\bigcup_{rs=1}^{ro} RISO_{rs}\} \ (rs = \overline{1, ro}),$$

where ro – the number of assessed RIS at the facility. Next for every $RISO_{rs}$ the sets of their vulnerabilities are determined $\boldsymbol{V}_{rs} \subset \boldsymbol{V}$ (and, accordingly, their identifiers), ie

$$\{\bigcup_{rs=1}^{ro} \boldsymbol{V}_{rs}\} = \{\bigcup_{rs=1}^{ro} \{\bigcup_{uz=1}^{n_{rs}} V_{rs,uz}\}\} \ (rs = \overline{1, ro}, \ uz = \overline{1, n_{rs}}),$$

where n_{rs} – possible number of identified vulnerabilities rs- of the estimated RIS $(RISO_{rs})$.

Step 3 (Determining the set of risk assessment parameters)

Here we introduce a set of risk assessments $\boldsymbol{LR}$ for the defined in the second step $\boldsymbol{RISO}$, ie at $rs = \overline{1, ro}$

$$\exists \boldsymbol{LR} = \{\bigcup_{rs=1}^{ro} LR_{rs}\} = \{LR_1, ..., \ LR_{rs}\}.$$

So, for RE for each vulnerability reflected by the identifier $V_{rs,uz}$ introduce sets $\boldsymbol{LRV}_{rs}$ at $rs = \overline{1, ro}$ and $uz = \overline{1, n_{rs}}$, ie

$$\exists \{\bigcup_{rs=1}^{ro} \boldsymbol{LRV}_{rs}\} = \{\bigcup_{rs=1}^{ro} \{\bigcup_{uz=1}^{n_{rs}} LRV_{rs,uz}\}\},$$

where $LRV_{rs,uz}$ – quantitative risk assessment for each *uz*-th vulnerability of *rs*-th PIC on yhe object. To display the result of the RA, we will use the LV "RISK DEGREE" (***RD***), presented in the form of a tuple.

Further, to ensure the evaluation process, indicators are taken as a basis CVSS [1] with NVD. To do this, define the required sets of parameters $\boldsymbol{EP}_i$, $(i = \overline{1, g})$, used for evaluation, ie $\boldsymbol{EP} = \{\bigcup_{i=1}^{g} \boldsymbol{EP}_i\} = \{EP_1, EP_2, ..., \ EP_g\}$, where g – the number of sets of such parameters.

Note that for version 3 estimations of CVSS [1], in which, unlike version 2.0, the metrics of operation (***AC, AV, PR, UI***) calculated for the vulnerable component, and impact metrics (***C, I, A***) for the attacker. This makes it possible to distinguish between vulnerable and attacking components, for example, when g = 3 can be determined by the following sets of values –

$$\{\bigcup_{i=1}^{3} \boldsymbol{EP}_i\} = \{\boldsymbol{EP}_1, \boldsymbol{EP}_2, \boldsymbol{EP}_3\} = \{\boldsymbol{B}, \ \boldsymbol{T}, \ \boldsymbol{E}\}$$

$$(i = \overline{1,3}),$$

where:

$\boldsymbol{B}$ – **basic (Base) estimations**, which are presented as a set

$$\boldsymbol{B} = \{\bigcup_{uz=1}^{n_{rs}} B_{uz}\} \ (uz = \overline{1, n_{rs}}),$$

whose members are formed on the basis of a group of sets of parameters $\boldsymbol{AV}_{uz}$, $\boldsymbol{AC}_{uz}$, $\boldsymbol{PR}_{uz}$, $\boldsymbol{S}_{uz}$, $\boldsymbol{UI}_{uz}$, $\boldsymbol{C}_{uz}$, $\boldsymbol{I}_{uz}$, $\boldsymbol{A}_{uz}$ $(uz = \overline{1, n_{rs}})$, where:

$\boldsymbol{AV}_{uz}$ – cyber-attack vector, which is represented as a set

$$\boldsymbol{AV}_{uz} = \{\bigcup_{av=1}^{4} AV_{uz,av}\}$$

$$= \{AV_{uz,1}, ..., AV_{uz,4}\} = \{N, A, L, P\}$$

$(uz = \overline{1, n_{rs}}, av = \overline{1,4})$, where: N – «Network» = 0,85; *A* – «Connected network» = 0,62; *L* – «Local access» = 0,55; *P* – «Physical access» = 0,2,

$\boldsymbol{AC}_{uz}$ – the complexity of the cyber-attack, represented by the set

$$\boldsymbol{AC}_{uz} = \{\bigcup_{ac=1}^{2} AC_{uz,ac}\}$$

$$= \{AC_{uz,1}, AC_{uz,2}\} = \{L, H\}$$

$(uz = \overline{1, n_{rs}}, ac = \overline{1,2})$, where: *L* – «Low» = 0,77; *H* – «High» = 0,44,

$\boldsymbol{PR}_{uz}$ – compliance with the authority represented by the plural

$$\boldsymbol{PR}_{uz} = \{\bigcup_{pr=1}^{3} PR_{uz,pr}\} =$$

$$\{PR_{uz,1}, PR_{uz,2}, PR_{uz,3}\} = \{N, L, H\}$$

$(uz = \overline{1, n_{rs}},\ pr = \overline{1,3})$, where: N – «Absent» = 0,85;

$$L - \text{«Low»} = \begin{cases} 0,62 \ at \ S_{uz,1} = U, \\ 0,68 \ at \ S_{uz,2} = C, \end{cases}$$ with

$\boldsymbol{S}_{uz}$ – action scope, which can be represented as a set

$$\boldsymbol{S}_{uz} = \{\bigcup_{s=1}^{2} S_{uz,s}\} = \{S_{uz,1}, S_{uz,2}\} = \{U, C\}$$

$(uz = \overline{1, n_{rs}}, s = \overline{1,2})$, where: U – «No changes»; C – «Changing»);

$$H - \text{«High»} = \begin{cases} 0,27 \ at \ S_{uz,1} = U, \\ 0,50 \ at \ S_{uz,2} = C, \end{cases}$$

$\boldsymbol{UI}_{uz}$ – user interaction, represented by the set

$$\boldsymbol{UI}_{uz} = \{\bigcup_{ui=1}^{2} UI_{uz,ui}\} = \{UI_{uz,1}, UI_{uz,2}\} = \{N, R\}$$

$(uz = \overline{1, n_{rs}}, ui = \overline{1,2})$, where: N – «No need» = 0,85; R – «Is required» = 0,62,

$\boldsymbol{C}_{uz}$ – impact on privacy, defined as a set

$$\boldsymbol{C}_{uz} = \{\bigcup_{c=1}^{3} C_{uz,c}\} = \{C_{uz,1}, C_{uz,2}, C_{uz,3}\} = \{N, L, H\}$$

$(uz = \overline{1, n_{rs}}, c = \overline{1,3})$, where: N – «Absent» = 0; L – «Low» = 0,22; H – «High» = 0,56,

$\boldsymbol{I}_{uz}$ – influence on integrity, which is represented by the set

$$\boldsymbol{I}_{uz} = \{\bigcup_{in=1}^{3} I_{uz,in}\} = \{I_{uz,1}, I_{uz,2}, I_{uz,3}\} = \{N, L, H\}$$

$(uz = \overline{1, n_{rs}}, in = \overline{1,3})$, where: N – «Absent» = 0; L – «Low» = 0,22; H – «High» = 0,56,

$\boldsymbol{A}_{uz}$ – the impact on availability, which can be represented by the plural

$$\boldsymbol{A}_{uz} = \{\bigcup_{ai=1}^{3} A_{uz,ai}\} = \{A_{uz,1}, A_{uz,2}, A_{uz,3}\} = \{N, L, H\},$$

$(uz = \overline{1, n_{rs}}, ai = \overline{1,3})$, where: N – «Absent» = 0; L – «Low» = 0,22; H – «High» = 0,56;

$\boldsymbol{T}$ – **temporal estimates**, which in accordance with paragraph 4.6 are presented as a set

$$\boldsymbol{T} = \{\bigcup_{uz=1}^{n_{rs}} T_{uz}\} \ (uz = \overline{1, n_{rs}}),$$

whose members are determined by a group of sets of parameters: $\boldsymbol{EX}_{uz}$, $\boldsymbol{RL}_{uz}$, $\boldsymbol{RC}_{uz}$ $(uz = \overline{1, n_{rs}})$, where:

$\boldsymbol{EX}_{uz}$ – usability, which can be displayed as a set

$$\boldsymbol{EX}_{uz} = \{\bigcup_{ex=1}^{5} EX_{uz,ex}\} = \{EX_{uz,1}, ..., EX_{uz,5}\} = \{X, U, POC, F, H\}$$

$(uz = \overline{1, n_{rs}},\ ex = \overline{1,5})$, where: X – «No data» = 1; U – «Theoretical (no evidence)» = 0,91; POC – «Experimental» = 0,94; F – «Functional» = 0,97; H – «High» = 1,

$\boldsymbol{RL}_{uz}$ – the level of correction (indicator of the degree of readiness of the decision), which is determined as a set

$$\boldsymbol{RL}_{uz} = \{\bigcup_{rl=1}^{5} RL_{uz,rl}\} = \{RL_{uz,1}, ..., RL_{uz,5}\} = \{X, OF, TF, W, U\}$$

$(uz = \overline{1, n_{rs}}, rl = \overline{1,5})$, where: X – «No data» = 1; OF – «Official patch» = 0,95; TF – «Interim solution» = 0,96; W – «Solutions based on tips and tricks» = 0,97; U – «Absent» = 1,

$\boldsymbol{RC}_{uz}$ – the reliability of the report (an indicator of the degree of reliability of information), which is represented by the set

$$\boldsymbol{RC}_{uz} = \{\bigcup_{rc=1}^{4} RC_{uz,rc}\}$$

$$= \left\{RC_{uz,1}, ..., RC_{uz,4}\right\} = \{X, U, R, C\}$$

$(uz = \overline{1, n_{rs}},\ rc = \overline{1,4})$, where: X – «No data» = 1; U – «Undefined» = 0,92; R – «Justified» = 0,96; C – «Confirmed» = 1;

E – **environmental metrics (Environmental)**, presented as a set

$$\boldsymbol{E} = \{\bigcup_{uz=1}^{n_{rs}} E_{uz}\} \ \ (uz = \overline{1, n_{rs}}),$$

whose members are determined by a group of sets of parameters: $\boldsymbol{CR}_{uz}$, $\boldsymbol{IR}_{uz}$, $\boldsymbol{AR}_{uz}$, $\boldsymbol{MS}_{uz}$, $\boldsymbol{MAV}_{uz}$, $\boldsymbol{MAC}_{uz}$, $\boldsymbol{MPR}_{uz}$, $\boldsymbol{MUI}_{uz}$, $\boldsymbol{MC}_{uz}$, $\boldsymbol{MI}_{uz}$, $\boldsymbol{MA}_{uz}$ $(uz = \overline{1, n_{rs}})$, where:

$\boldsymbol{CR}_{uz}$ – confidentiality requirements defined as a set

$$\boldsymbol{CR}_{uz} = \{\bigcup_{cr=1}^{4} CR_{uz,cr}\} =$$

$$\left\{CR_{uz,1}, ..., CR_{uz,4}\right\} = \left\{X, L, M, H\right\}$$

$(uz = \overline{1, n_{rs}},\ \ cr = \overline{1,4})$, where: X – «Undefined» = 1; L – «Low» = 0,5; M – «Medium» = 1; H – «High» = 1,5,

$\boldsymbol{IR}_{uz}$ – integrity requirements represented by the set

$$\boldsymbol{IR}_{uz} = \{\bigcup_{ir=1}^{4} IR_{uz,ir}\} = \{IR_{uz,1}, ...,$$

$$IR_{uz,4}\} = \left\{X, L, M, H\right\}$$

$(uz = \overline{1, n_{rs}},\ ir = \overline{1,4})$, where: X – «Undefined» = 1; L – «Low» = 0,5; M – «Medium»= 1; H – «High» = 1,5,

$\boldsymbol{AR}_{uz}$ – accessibility requirements, presented in the form of a set

$$\boldsymbol{AR}_{uz} = \{\bigcup_{ar=1}^{4} AR_{uz,ar}\} =$$

$$\left\{AR_{uz,1}, ..., AR_{uz,4}\right\} = \left\{X, L, M, H\right\}$$

$(uz = \overline{1, n_{rs}},\ \ ar = \overline{1,4})$, where: X – «Undefined» = 1; L – «Low» = 0,5; M – «Medium» = 1; H – «High» = 1,5,

$\boldsymbol{MS}_{uz}$ – modified action scope, which can be represented as a set

$$\boldsymbol{MS}_{uz} = \{\bigcup_{ms=1}^{3} MS_{uz,ms}\}$$

$$= \left\{MS_{uz,1}, MS_{uz,2}, MS_{uz,3}\right\} = \left\{X, U, C\right\}$$

$(uz = \overline{1, n_{rs}},\ ms = \overline{1,3})$, where: X – «Undefined»; U – «Unchanged»; C – «Changing»,

$\boldsymbol{MAV}_{uz}$ – modified cyber-attack vector, which is represented as a set

$$\text{Medium } \boldsymbol{MAV}_{uz} = \{\bigcup_{mav=1}^{5} MAV_{uz,mav}\}$$

$$= \left\{MAV_{uz,1}, ..., MAV_{uz,5}\right\} =$$

$$\left\{X, N, A, L, P\right\}$$

$(uz = \overline{1, n_{rs}},\ mav = \overline{1,5})$, where: X – «Undefined» = 1; N – «Network» = 0,85; A – «Connected network» = 0,62; L – «Local access» = 0,55; P – «Physical access» = 0,2,

$\boldsymbol{MAC}_{uz}$ – modified complexity of a cyberattack determined by the set

$$\boldsymbol{MAC}_{uz} = \{\bigcup_{mac=1}^{3} MAC_{uz,mac}\} =$$

$$\left\{MAC_{uz,1}, MAC_{uz,2}, MAC_{uz,3}\right\}$$

$$= \left\{X, L, H\right\}$$

$(uz = \overline{1, n_{rs}},\ mac = \overline{1,3})$, where: X – «Undefined» = 1; L – «Low» = 0,77; H – «High» = 0,44,

$\boldsymbol{MPR}_{uz}$ – modified compliance with the authority represented by the set

$$\boldsymbol{MPR}_{uz} = \{\bigcup_{mpr=1}^{4} MPR_{uz,mpr}\} =$$

$$\{MPR_{uz,1}, MPR_{uz,2},$$

$$MPR_{uz,3}, MPR_{uz,4}\} = \left\{X, N, L, H\right\}$$

$(uz = \overline{1, n_{rs}},\ \ mpr = \overline{1,4})$, where: X – «Undefined» = 1; N – «Absent» = 0,85;

$$L \text{ – «Low»} = \begin{cases} 0,62 \ at \ MS_{uz,1} = U, \\ 0,68 \ at \ MS_{uz,2} = C; \end{cases}$$

$$H - \text{«High»} = \begin{cases} 0,27 \; at \; MS_{uz,1} = U, \\ 0,50 \; at \; MS_{uz,2} = C, \end{cases}$$

$\boldsymbol{MUI}_{uz}$ – modified interaction with the user, represented by the set

$$\boldsymbol{MUI}_{uz} = \{\bigcup_{mui=1}^{3} MUI_{uz,mui}\} = \{MUI_{uz,1}, MUI_{uz,2}, MUI_{uz,3}\} = \{X, N, R\}$$

$(uz = \overline{1, n_{rs}}, mui = \overline{1,2})$, where: X – «Undefined» = 1; N – «No need» = 0,85; R – «There is a need» = 0,62,

$\boldsymbol{MC}_{uz}$ – modified impact on privacy determined by the set

$$\boldsymbol{MC}_{uz} = \{\bigcup_{mc=1}^{4} MC_{uz,mc}\} = \{MC_{uz,1}, MC_{uz,2}, MC_{uz,3}, MC_{uz,4}\} = \{X, N, L, H\}$$

$(uz = \overline{1, n_{rs}}, mc = \overline{1,4})$, where: X – «Undefined» = 1; N – «Absent» = 0; L – «Low» = 0,22; H – «High» = 0,56,

$\boldsymbol{MI}_{uz}$ – modified effect on the integrity determined by the set

$$\boldsymbol{MI}_{uz} = \{\bigcup_{min=1}^{4} MI_{uz,min}\} = \{MI_{uz,1}, MI_{uz,2}, MI_{uz,3}, MI_{uz,4}\} = \{X, N, L, H\}$$

$(uz = \overline{1, n_{rs}}, min = \overline{1,4})$, where: X – «Undefined» = 1; N – «Absent» = 0; L – «Low» = 0,22; H – «High» = 0,56,

$\boldsymbol{MA}_{uz}$ – modified effect on availability, represented by the set

$$\boldsymbol{MA}_{uz} = \{\bigcup_{mai=1}^{4} MA_{uz,mai}\} = \{MA_{uz,1}, MA_{uz,2}, MA_{uz,3}, MA_{uz,4}\} = \{X, N, L, H\}$$

$(uz = \overline{1, n_{rs}}, mai = \overline{1,4})$, where: X – «Undefined» = 1; N – «Absent» = 0; L – «Low» = 0,22; H – «High» = 0,56.

Next, we introduce the logical variable (LV) "LEVEL OF EVALUATION PARAMETER $\boldsymbol{EP}_i$" ($\boldsymbol{K}_{EP_i}$), which is determined by the tuple [2, 3] $< \boldsymbol{K}_{EP_i}, \underset{\sim}{T}_{K_{EP_i}}, \boldsymbol{X}_{EP_i} >$, where the base term sets are initialized by m-terms $\underset{\sim}{\boldsymbol{T}}_{K_{EP_i}} = \bigcup_{j=1}^{m} \underset{\sim}{T}_{K_{EP_i j}}$, for which, respectively, determine their intervals of values for each $\boldsymbol{EP}_i$, $(i = \overline{1, g})$ – $[k_{EP_i 1};\ k_{EP_i 2}[$, $[k_{EP_i 2};\ k_{EP_i 3}[$, …, $[k_{EP_i j-1};\ k_{EP_i j}[$, $[k_{EP_i j};\ k_{EP_i j+1}[$, …, $[k_{EP_i m};\ k_{EP_i m+1}]$.

Next, using the appropriate method [4], which is implemented using four stages, the conversion of intervals into fuzzy numbers (FN) – $\underset{\sim}{T}_{K_{EP_i j}} = (ai_j; bi_{1j}; bi_{2j}; ci_j)$.

To do this, we modify the expression of the method using the following redefinitions [4]: $a_j = b_{2j}$, $c_j = b_{1j}$, where $j = \overline{1, m}$, (m – number of term sets) $a_1 = b_{11} = 0$ i $c_m = b_{2m} = k_{m+1}$.

Significance assessment of $\boldsymbol{EP}_i$ is performed using parameters from the set $\boldsymbol{LS} \in \{LS_i\}$ $(i = \overline{1, g})$, and estimation of the current value of the estimation parameter – by means of set $\boldsymbol{ep} \in \{ep_{uz,i}\}$ $(uz = \overline{1, n_{rs}}, i = \overline{1, g})$.

Step 4 (Determining the number of term sets)

The number of term sets that will be used in the RA process is determined. If necessary, the initial number of term sets can be changed. For this purpose, for the equivalent transformation of m-dimensional terms of FN LV $\boldsymbol{DR}^{(m)}$ in $\boldsymbol{DR}^{(m-n)}$ or $\boldsymbol{DR}^{(m+n)}$ and $\boldsymbol{K}_{EP_i}^{(m)}$ in $\boldsymbol{K}_{EP_i}^{(m-n)}$ or $\boldsymbol{K}_{EP_i}^{(m+n)}$ it is proposed to use methods of realization of function of transformation of LV standards [5].

Step 5 (Assessment of the evaluation parameters significance level). This step is interrelated with a similar step of the method described in [5].

Step 6 (Determination of reference values of the risk degree).

In this step, the reference values for LV ***DR*** are determined, that is, the number of terms in the base term set is specified $\underset{\sim}{\boldsymbol{T}}_{DR}$, where they correspond to a given range of values in the range from dr_{min} to dr_{max}.

Step 7 (Determination of evaluation parameters reference values).

Experts determine the standards of parameters for LV $\boldsymbol{K}_{EP_i}$, that is, the number of terms in the term set $\underset{\sim}{\boldsymbol{T}}_{K_{EP_i}}$ is specified.

To convert intervals into FN, we use the method proposed in [5], which is implemented using four stages. For convenience of estimation parameters display through FN tab. 1 was used.

Table 1

Determination of FN values of estimation parameters

$\boldsymbol{EP}_i$	FN $\underset{\sim}{T}_{K_{EP_i j}} = (a_j, b_{1j}, b_{2j}, c_j)_{LR}$ for $\underset{\sim}{T}_{K_{EP_i 1}}$ – $\underset{\sim}{T}_{K_{EP_i m}}$, ($j = \overline{1,m}$)				
	$\underset{\sim}{T}_{K_{EP_i 1}}$	…	$\underset{\sim}{T}_{K_{EP_i j}}$	…	$\underset{\sim}{T}_{K_{EP_i m}}$
$\boldsymbol{EP}_1$	($a1_1$; $b1_{11}$; $b1_{21}$; $c1_1$)	…	($a1_j$; $b1_{1j}$; $b1_{2j}$; $c1_j$)	…	($a1_m$; $b1_{1m}$; $b1_{2m}$; $c1_m$)
…	…	…	…	…	…
$\boldsymbol{EP}_i$	(ai_1; bi_{11}; bi_{21}; ci_1)	…	(ai_j; bi_{1j}; bi_{2j}; ci_j)	…	(ai_m; bi_{1m}; bi_{2m}; ci_m)
…	…	…	…	…	…
$\boldsymbol{EP}_g$	(ag_1; bg_{11}; bg_{21}; cg_1)	…	(ag_j; bg_{1j}; bg_{2j}; cg_j)	…	(ag_m; bg_{1m}; bg_{2m}; cg_m)

Step 8 (Estimation of current parameter values)

For each evaluation parameter

$$\{\bigcup_{i=1}^{3} \boldsymbol{EP}_i\} = \{\boldsymbol{EP}_1, \boldsymbol{EP}_2, \boldsymbol{EP}_3\} = \{ \boldsymbol{B},\ \boldsymbol{T},\ \boldsymbol{E} \}\ (i = \overline{1,3})$$

determined $ep_{uz,i}$ $\forall V_{rs,uz}$, ($rs = \overline{1,ro}$, $uz = \overline{1,n_{rs}}$), that is $\{ep_{uz,i}\} = \{ep_{uz,\boldsymbol{B}}, ep_{uz,\boldsymbol{T}}, ep_{uz,\boldsymbol{E}}\}$.

The value of each of the parameters can be taken from known databases or determined by appropriate formulas [1]:

$$B_{uz} = \begin{cases} 0 \ \ at\ IM_{uz} \le 0, \\ roundUp_1(\min[(IM_{uz} + EXb_{uz}), 10])\ at\ S_{uz,1} \\ roundUp_1(\min[1{,}08 \cdot (IM_{uz} + EXb_{uz}), 10])\ a \end{cases}$$

where $roundUp_1(\,)$ – function for rounding to the first decimal place (for example, 3,822 will be rounded to 3.8);

$$IM_{uz} = \begin{cases} 6{,}42 ISC_{uz}\ at\ S_{uz,1} = U, \\ 7{,}52(ISC_{uz} - 0{,}029) - \\ -3{,}25(ISC_{uz} - 0{,}02)^{15} \\ at\ S_{uz,2} = C, \end{cases}$$

where

$$ISC_{uz} = 1 - ((1 - C_{uz,c})(1 - I_{uz,in})(1 - A_{uz,ai})),$$

values $S_{uz,s}$, $C_{uz,c}$, $I_{uz,in}$, $A_{uz,ai}$ we obtain on the basis of step 3 of this method, and

$$EXb_{uz} = 8{,}22 AV_{uz,av} AC_{uz,ac} PR_{uz,pr} UI_{uz,ui},$$

$$T_{uz} = roundUp_1(B_{uz} EX_{uz,ex} RL_{uz,rl} RC_{uz,rc}),$$

where the values $EX_{uz,ex}$, $RL_{uz,rl}$ i $RC_{uz,rc}$ also obtained on the basis of step 3 of the method;

$$E_{uz} = \begin{cases} 0 \qquad\qquad\qquad at\ MIM_{uz} \le 0, \\ roundUp_1(\min[(MIM_{uz} + MEXb_{uz}) \\ EX_{uz,ex} RL_{uz,rl} RC_{uz,rc}, 10]) \\ \qquad\qquad\qquad at\ MS_{uz,1} = U, \\ roundUp_1(\min[1{,}08(MIM_{uz} + MEXb_{uz}) \\ EX_{uz} RL_{uz,rl} RC_{uz,rc}, 10]) \\ \qquad\qquad\qquad at\ MS_{uz,1} = C, \end{cases}$$

where:

$$MIM_{uz} = \begin{cases} 6,42(MISC_{uz}) \; at \; MS_{uz,1} = U, \\ 7,52(MISC_{uz} - 0,029) - \\ -3,25(MISC_{uz} - 0,02)^{15} \\ at \; MS_{uz,2} = C, \end{cases}$$

a $MEXb_{uz} = 8,22MAV_{uz,mav} \; MAC_{uz,mac} \; MPR_{uz,mpr} MUI_{uz,mui}$ i

$$MISC_{uz} = \min[(1-(1-MC_{uz,mc}CR_{uz,cr}) \; (1-MI_{uz,min}IR_{uz,ir}) \; (1-MA_{uz,mai}AR_{uz,ar})), \; 0,915],$$

while values $MS_{uz,ms}$, $MAV_{uz,mav}$, $MAC_{uz,mac}$, $MPR_{uz,mpr}$, $MUI_{uz,mui}$, $MC_{uz,mc}$, $CR_{uz,cr}$, $MI_{uz,min}$, $IR_{uz,ir}$, $MA_{uz,mai}$, $AR_{uz,ar}$ pre-defined in step 3 of this method. Here E_{uz} is a corrective evaluation parameter that determines B_{uz} and T_{uz}.

For clarity, the results of the calculations are entered in table. 2, where $\lambda_{uz,ij}$ – the level of affiliation of the carrier $ep_{uz,i}$ to the fuzzy subset $\underset{\sim}{T}_{K_{EP_i}j}$.

Similar transformations are carried out for all $V_{rs,uz}$.

Table 2

Classification of current values of evaluation parameters

EP_i	$\lambda_{uz,ij}$ for $\underset{\sim}{T}_{K_{EP_i}j}$ $(uz=\overline{1,n_{rs}}, \; i=\overline{1,g}, \; j=\overline{1,m})$				
	$\underset{\sim}{T}_{K_{EP_i}1}$	…	$\underset{\sim}{T}_{K_{EP_i}j}$	…	$\underset{\sim}{T}_{K_{EP_i}m}$
EP_1	$\lambda_{uz,11}$	…	$\lambda_{uz,1j}$	…	$\lambda_{uz,1m}$
…	…	…	…	…	…
EP_i	$\lambda_{uz,i1}$	…	$\lambda_{uz,ij}$	…	$\lambda_{uz,im}$
…	…	…	…	…	…
EP_g	$\lambda_{uz,g1}$	…	$\lambda_{uz,gj}$	…	$\lambda_{uz,gm}$

Step 10 (Risk degree assessment)

This step calculates the risk indicators for each vulnerability reflected by the identifier $V_{rs,uz}$ according to the formula

$$LRV_{rs,uz} = \sum_{j=1}^{m}\left(K_{lr_j} \sum_{i=1}^{g}(ks \cdot LS_i)\lambda_{uz,ij} \right),$$

where K_{lr_j} = 90 – 20(*m* – *j*), $ks = \dfrac{1}{(LS_1 + ... + LS_i)}$ – rationing factor, $\lambda_{uz,ij}$ $(uz=\overline{1,n_{rs}}, \; i=\overline{1,g}, \; j=\overline{1,m},)$ determined for each $V_{rs,uz}$ $(rs=\overline{1,ro}, \; uz=\overline{1,n_{rs}})$, and *LS*$_i$, $(i=\overline{1,g})$ depending on the significance of the parameter.

Step 11 (Formation of a structured risk parameter)

Based on the calculated value of $LRV_{rs,uz}$ and constructed standards form a structured parameter of the risk degree ***RD*** by expression:

$$SP_{uz} = \begin{cases} (LRV_{rs,uz}; \underset{\sim}{T}_{DR_j}) \\ at \; \mu_j(LRV_{rs,uz}) = 1; \\ (LRV_{rs,uz}; \underset{\sim}{T}_{DR_j}(\mu_j(LRV_{rs,uz})); \\ \underset{\sim}{T}_{DR_{j+1}}(\mu_{j+1}(LRV_{rs,uz}))) \\ at \; \mu_j(LRV_{rs,uz}) \neq 1 \wedge \mu_{j+1}(LRV_{rs,uz}) \neq 1, \end{cases}$$

where $(LRV_{rs,uz}; \underset{\sim}{T}_{DR_j})$ verbally interpreted as – «The risk degree $\underset{\sim}{T}_{DR_j}$ with a numerical equivalent $LRV_{rs,uz}$», and $(LRV_{rs,uz}; \underset{\sim}{T}_{DR_j}(\mu_j(LRV_{rs,uz}));$ $\underset{\sim}{T}_{DR_{j+1}}(\mu_{j+1}(LRV_{rs,uz})))$, as – «The risk degree with a numerical equivalent $LRV_{rs,uz}$, which borders $\underset{\sim}{T}_{DR_j}$ and $\underset{\sim}{T}_{DR_{j+1}}$ along the border

$\underset{\sim}{T}_{DR_j}$ – $\mu_j(LRV_{rs,uz})$ and $\underset{\sim}{T}_{DR_{j+1}}$ – $\mu_{j+1}(LRV_{rs,uz})$».

With the help of ***RD*** both the numerical value of the degree of risk and its linguistic interpretation can be obtained.

Also, can be calculated the average value LR_{rs} by estimation resource:

$$LR_{rs} = (\sum_{uz=1}^{n_{rs}} LRV_{rs,uz}) / n_{rs}.$$

Thus, the presented method of assessing the risks of IS based on open database vulnerabilities by modifying the procedures for determining the set of RA parameters and estimating the current values of parameters with the possibility of integration (as an alternative to expert estimates) of CVSS values (version 3.0) presented in NVD distinguish between vulnerable and offensive components, and also allows for the implementation of operational assessment and monitoring (real-time) of risks without the involvement of experts in the relevant subject area.

3. Information security risks assessment system

On the basis of the developed method the corresponding system of IS RA which due to use of structural components of subsystems of formation of primary and secondary data, and also components of their modules of initialization of input data, formation and transformation of reference values, weighing of estimation parameters and their adjustment, estimation of RD and generation of report, which implemented the proposed method, allows to provide certain properties of adaptability and efficiency in RA of RIS security in real time. Such a system, using CVSS metrics, allows to perform RA in real time, as well as at the request of the user to transform the reference LV without the involvement of specialists in the relevant field. In addition, the system provides the function of editing these metrics, using the built-in CVSS-calculator version 3.0 [1].

The structural solution of the proposed system (Fig. 1) consists of two basic components that reflect the subsystems of primary (SPDP) and secondary data (SSDP) processing. We describe the composition of each of the subsystems.

The SPDP subsystem is intended for primary processing of initial values and includes the module of input data initialization (MDI), and also modules of formation (MFR) and conversion (MCR) of reference values.

The SSDP subsystem, using CVSS metrics, performs the transformation of the primary parameters coming from the SPDP in order to form the final estimates of the RD. It consists of a module for weighing evaluation parameters (MWP) and their adjustment (MAP), as well as modules for estimating RD (MRD) and generating a report (MGR).

Let's consider the functional purpose of each of the modules of the subsystems. Thus, MDI is designed to form and identify many RIS and vulnerabilities of the evaluation object.

Here based on the set ***RIS*** for the specified object experts determine the required set of ***RIS*** (and, accordingly, their identifiers) $\boldsymbol{RISO} = \{\bigcup_{rs=1}^{ro} \boldsymbol{RISO}_{rs}\}$ $(rs = \overline{1, ro})$, where ro – the number of assessed ***RIS*** at the facility.

Next, for every $\boldsymbol{RISO}_{rs}$ determined the sets of their vulnerabilities $\{\bigcup_{rs=1}^{ro} \boldsymbol{V}_{rs}\} = \{\bigcup_{rs=1}^{ro}\{\bigcup_{uz=1}^{n_{rs}} V_{rs,uz}\}\}$ $(rs = \overline{1, ro},\ uz = \overline{1, n_{rs}})$, where n_{rs} – the possible number of identified vulnerabilities of rs-th estimated RIS $(\boldsymbol{RISO}_{rs})$.

As input for the MDI can be used, for example, the results of the program to check the system for penetration (Penetration test).

Such software, as a rule, analyzes the specified object, searching for vulnerabilities of its RIS in cyberspace (according to ISO / IEC 27032: 2012, cyberspace can be understood as a complex entity that actually exists as a global set of processes of interaction of people, software and Internet services in networks (including technological equipment connected to them), but which does not manifest itself in any known, material form).

Thus, a list is formed in the form of a set of RIS vulnerabilities of the studied object. To obtain a set of RIS and a set of relevant vulnerabilities in MDI, performed the processing

of the corresponding report obtained from specialized software (level - Penetration test), which contains information about RIS and vulnerabilities with the specified CVSS metrics.

Next, the list of vulnerabilities and RIS is initialized for further transmission to the MFR. As a result of the work of the MDI, all identified MFRs arrive at the entrance $\boldsymbol{RISO}_{rs}$, $\boldsymbol{V}_{rs}$ and their CVSS metrics.

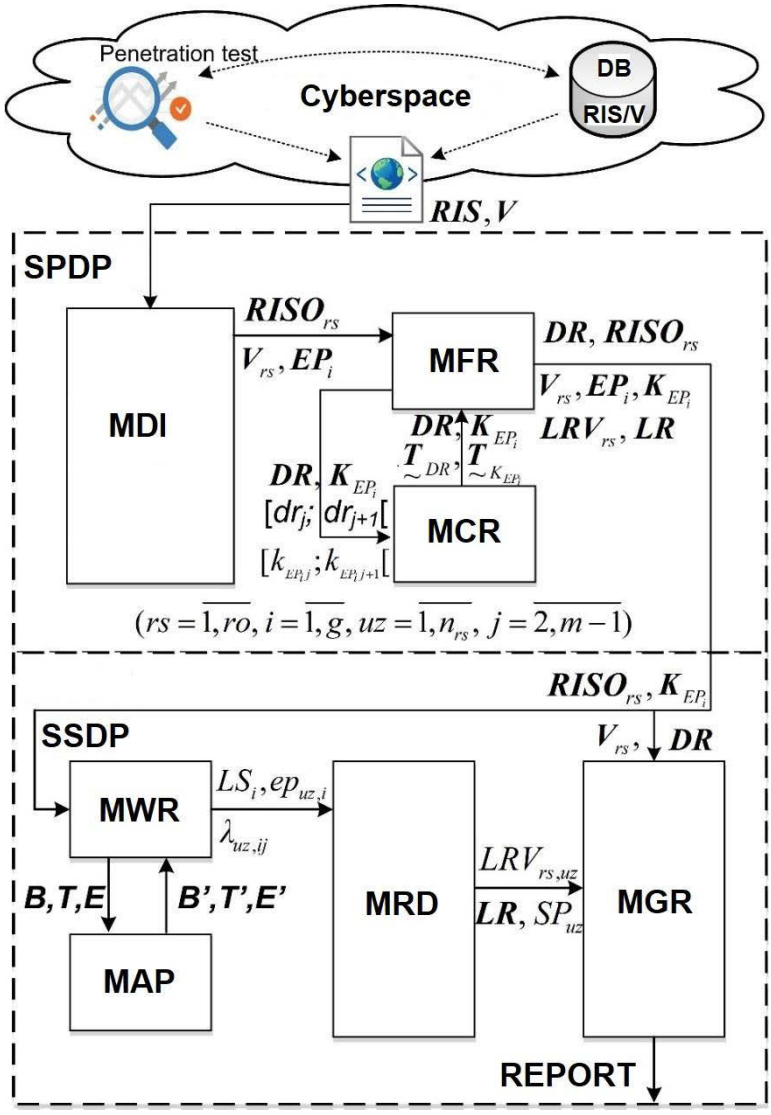


Figure 1: Structural solution of the IS RA system in real time

Next, the MFR performs the formation of a set of parameters:

– $\boldsymbol{LR} = \{\bigcup_{rs=1}^{ro} \boldsymbol{LR}_{rs}\}$ $(rs = \overline{1,ro})$,

where $\boldsymbol{LR}_{rs}$ – quantitative risk assessment of rs – th RIS on object (used for $\boldsymbol{RISO}_{rs}$);

– $\boldsymbol{LRV} = \{\bigcup_{rs=1}^{ro} \boldsymbol{LRV}_{rs}\} = \{\bigcup_{rs=1}^{ro} \{\bigcup_{uz=1}^{n_{rs}} LRV_{rs,uz}\}\}$ $(rs = \overline{1,ro}, uz = \overline{1,n_{rs}})$, where $LRV_{rs,uz}$ – quantitative risk assessment for each uz – th vulnerability of rs – th RIS on the object (used for the RA for each vulnerability reflected by the identifier $V_{rs,uz}$);

– $\boldsymbol{DR}$, where LV «RISK DEGREE» is represented as a corresponding tuple <$\boldsymbol{DR}$, $\underset{\sim}{T}_{DR}$, $\boldsymbol{X}_{DR}$> (is used to display the RA result);

– $\boldsymbol{EP} = \{\bigcup_{i=1}^{g} \boldsymbol{EP}_i\}$ $(i = \overline{1,g})$,

where g – number of sets of evaluation parameters

(used to ensure the evaluation process, based on CVSS indicators);

– $\boldsymbol{K}_{EP_i}$, where LV «LEVEL OF EVALUATION PARAMETER $\boldsymbol{EP}_i$» determined by the tuple $<\boldsymbol{K}_{EP_i}, \underset{\sim}{T}_{K_{EP_i}}, \boldsymbol{X}_{EP_i}>$ (used to display evaluation results using CVSS metrics).

Formed LVs ***DR*** and $\boldsymbol{K}_{EP_i}$ are transmitted to the input of the MCR, where for each of the terms $\underset{\sim}{T}_{DR_1}, \ldots, \underset{\sim}{T}_{DR_j}, \ldots, \underset{\sim}{T}_{DR_m}$ i $\underset{\sim}{T}_{K_{EP_i1}}, \underset{\sim}{T}_{K_{EP_i2}}, \ldots,$ $\underset{\sim}{T}_{K_{EP_ij-1}}, \underset{\sim}{T}_{K_{EP_ij}}, \ldots, \underset{\sim}{T}_{K_{EP_im}}$ the transformation is implemented according to the specified range of values $[dr_1; dr_2[, \ldots, [dr_j; dr_{j+1}[, \ldots, [dr_m; dr_{m+1}]$ i $[k_{EP_i1}; k_{EP_i2}[, [k_{EP_i2}; k_{EP_i3}[, \ldots, [k_{EP_ij-1}; k_{EP_ij}[, [k_{EP_ij}; k_{EP_ij+1}[, \ldots, [k_{EP_im}; k_{EP_im+1}]$ to FN. Also in MCR the procedure of variation by the order of LV is implemented. Thus, for the equivalent transformation of *m*-dimensional terms of FN LV $\boldsymbol{DR}^{(m)}$ to $\boldsymbol{DR}^{(m-n)}$ or $\boldsymbol{DR}^{(m+n)}$ and $\boldsymbol{K}_{EP_i}^{(m)}$ to $\boldsymbol{K}_{EP_i}^{(m-n)}$ or $\boldsymbol{K}_{EP_i}^{(m+n)}$ in MCR methods of transformation of LV standards are used. As a result of transformations on output of SPDP arrive $\boldsymbol{RISO}_{rs}$, $\boldsymbol{V}_{rs}$ and their CVSS metrics, $\boldsymbol{EP}_i$, LV ***DR*** and $\boldsymbol{K}_{EP_i}$, as well as formed sets $\boldsymbol{LR}$ i $\boldsymbol{LRV}_{rs}$ for RA.

Significance levels of estimation parameters are defined in MWP SSDP $LS_i \ (i=\overline{1,g})$ and their current values $\boldsymbol{ep}_{uz,i}$ from SPDP, for example, $\{\bigcup_{i=1}^{3} \boldsymbol{EP}_i\} = \{\boldsymbol{EP}_1, \boldsymbol{EP}_2, \boldsymbol{EP}_3\} = \{$ $\boldsymbol{B}, \boldsymbol{T}, \boldsymbol{E}\} \ (i=\overline{1,3})$.

Then, with the help of reference values, the process of fasification is carried out, which is associated with the determination of affiliation of $\boldsymbol{ep}_{uz,i}$ to a given FN, after which values $\lambda_{uz,ij}$ are formed. Also in MWP the graphic interpretation of estimation parameters is carried out ***B, T*** and ***E***.

If necessary, it is possible to adjust the CVSS metrics using the MAP, which implements their redefinition due to the built-in CVSS-calculator (see Fig. 2). Adjusted parameters ***B'***, ***T'*** and ***E'*** are transferred back to the MWP.

Data from MWP LS_i, $\boldsymbol{ep}_{uz,i}$ and $\lambda_{uz,ij}$ enter the MSP, where for each vulnerability reflected by the identifier $V_{rs,uz}$, SR evaluation is implemented $LRV_{rs,uz}$, and the average value is calculated $\boldsymbol{LR}_{rs}$ for RIS.

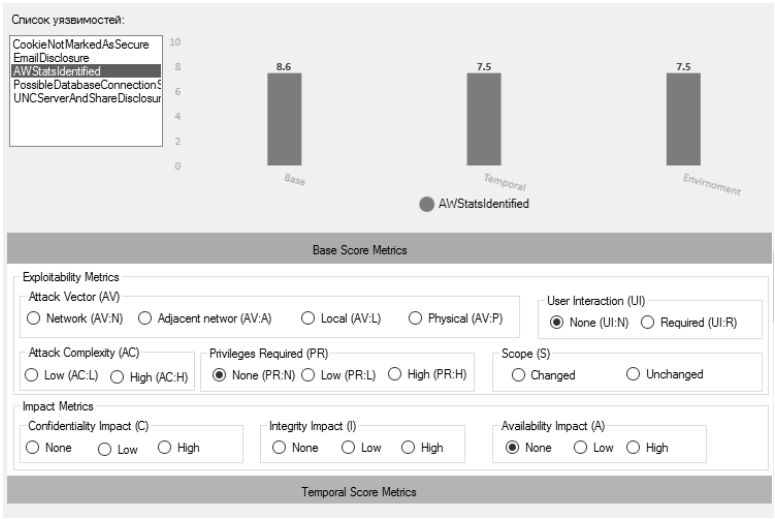


Figure 2: Built-in CVSS-calculator with graphical interpretation of CVSS metrics

Next, based on the calculated value $LRV_{rs,uz}$, $\boldsymbol{LR}_{rs}$ and constructed standards in the SPDP, the process of defasification, which is associated with the formation of a structured parameter of the RD SP_{uz}, which allows to obtain numerical values of RD and its linguistic interpretation.

On the basis of MGR, taking into account the results of SPDP and SSDP, a report is generated on the estimates of the RD (see Fig. 3), which

contains $\boldsymbol{RISO}_{rs}$, $\boldsymbol{V}_{rs}$, $LRV_{rs,uz}$, $\boldsymbol{LR}_{rs}$, their linguistic equivalents and graphical interpretation of the results.

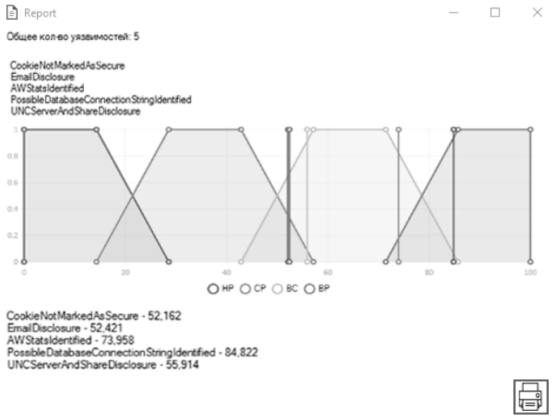


Figure 3: Example of the generated report

The proposed real-time IS RA system, for example, can be implemented programmatically and work on the basis of the proposed basic algorithm (Fig. 4).

According to this algorithm, the operation of the system begins with the initialization of the list of vulnerabilities and CVSS ratings (top 1) using a specialized program to check the system for penetration (Penetration test).

This procedure in the software implementation can, for example, be performed by the function OpenXMLFile (), which opens the file in XML format and implements its parsing. XML file parsing is used to initialize (fill in) fields in the Vulnerability class with the following structure:

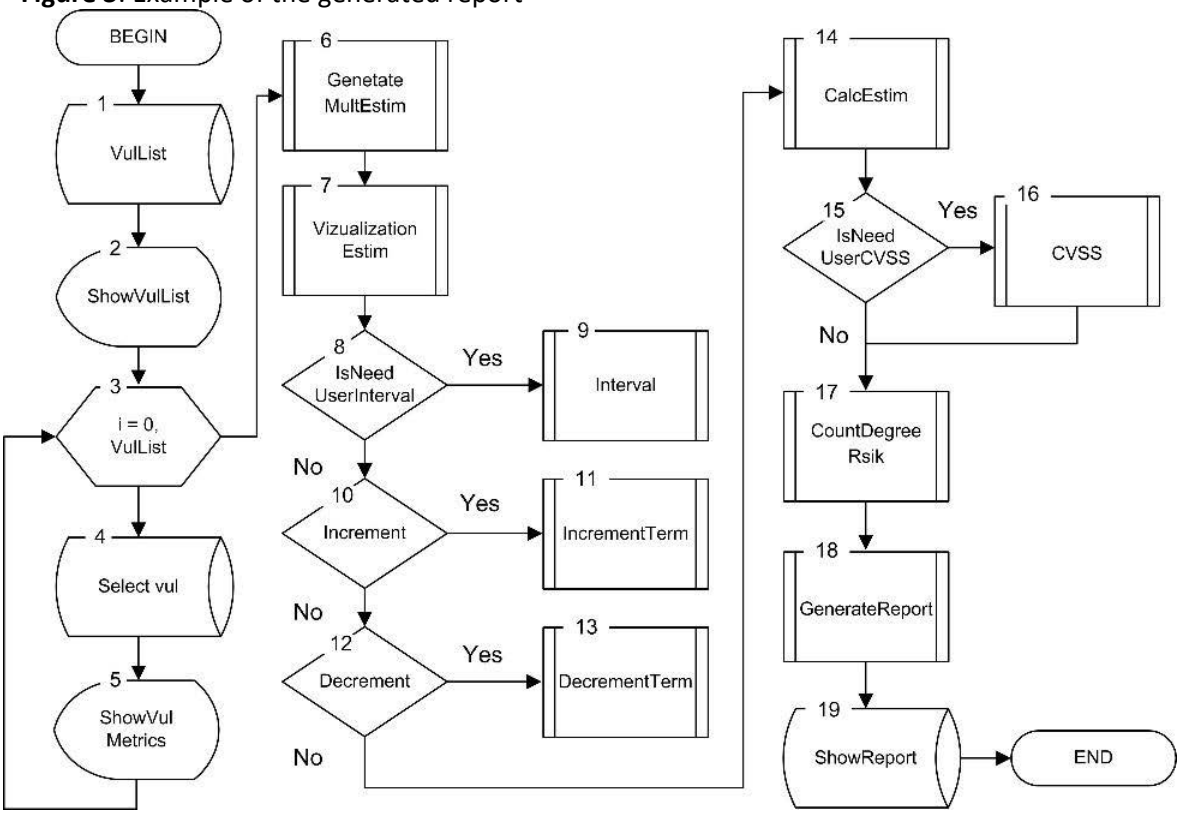


Figure 4: Basic algorithm of IS RA system operation

```
class Vulnerability
  {
    public string Id { get; set; }
    public string Description { get; set; }
    public string VulClass { get; set; }
    public string vectorCVSS { get; set; }
    public Metrics metrics;
    public Vulnerability()
    {
      metrics = new Metrics();
    }}.
```

After identifying the next vulnerability (Vulnerability class), its characteristics are entered into the List container, resulting in the formation of a structure – List <Vulnerability>. Next, after generating a list of vulnerabilities (vertex 2), its contents are written to the ListBox component with $\boldsymbol{RISO}_{rs}$, $\boldsymbol{V}_{rs}$ and their CVSS estimates.

Next, in the loop (vertex 3) performs a selection of vulnerabilities (vertex 4) from the ListBox (Select Vul) and their graphical interpretation (vertex 5) CVSS metrics (Fig. 2). This process provides the appropriate event handler - the lbVul CVSS_

SelectedIndexChanged function. The moment the SelectedIndexChanged event occurs when the index of the selected ListBox component changes. The lbVulCVSS_SelectedIndexChanged function graphically displays CVSS metrics based on the LiveChart library. CVSS metrics are displayed in the form of a bar chart (see Fig. 2), which is achieved using the following block of program listing:

```
chartCVSS.Series.Add(new ColumnSeries()
        {
          Title =
vulList[lb.SelectedIndex].Description,
          Values = new
ChartValues<ObservableValue>()
          {
            new
ObservableValue(vulList[lb.SelectedIndex].metri
cs.baseVector.CommonScore),
            new
ObservableValue(vulList[lb.SelectedIndex].metri
cs.tempVector.CommonScore),
            new
ObservableValue(vulList[lb.SelectedIndex].metri
cs.envirVector.CommonScore)
          },
          DataLabels = true});
```

Next, with the help of a predetermined process (vertex 6) is the formation of LV $\boldsymbol{K}_{EP_i}$ and ***DR***, and sets are initialized for subsequent estimates $\boldsymbol{LR}$ and $\boldsymbol{LRV}_{rs}$.

After the formation of the necessary linguistic terms, the conversion of the given intervals into FN is performed, linguistic standards are formed and their graphical interpretation is realized (vertex 7). For clarity, the obtained CVSS metrics for each vulnerability are displayed on a graph with reference values $\boldsymbol{EP}_i$ (see Fig. 5).

Representation of terms of LV $\boldsymbol{K}_{EP_i}$ in graphical form (in accordance with the software implementation of the system) is provided by the structure of TrapezeCreator, which may have, for example, such fields:

```
struct Trapeze
  {
    public string degreeRisk;
    public double a { get; set; }
    public double b11 { get; set; }
    public double b21 { get; set; }
    public double c { get; set; }
  }.
```

The intervals that will be used to convert to FN are described by the Interval structure, which consists of the following fields:

```
struct Interval
  {
    public double a { get; set; }
    public double b { get; set; }
  }.
```

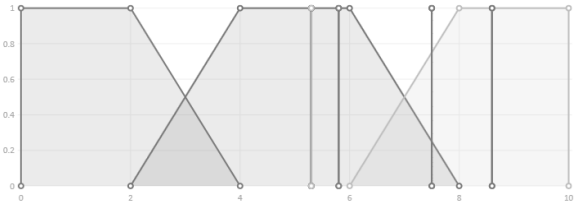


Figure 5: Graphical interpretation of the obtained CVSS metrics and standards of evaluation parameters

Graphical interpretation of the obtained results (according to the proposed software implementation) is carried out using the function List <Trapeze> CreateTrapezeList (double lengthAsixX, int countTrap, params double [] intervalArr). Next, with the help of subroutines Interval, IncrementTerm, DecrementTerm and conditional vertices (vertices 8-13), which are used to control the need for additional data processing, ie converting the specified intervals into FN, the process of decrementing and incrementing the order of LV.

Initialization of a new interval in the program is realized by means of the following block of program listing (verses 8-9):

```
double[] interval = new
double[intervalList.Count * 2];
for (int i = 0, k = 0; i < interval.Length; i++,
k++)
        {
          interval[i] = intervalList[k].a;
          interval[++i] = intervalList[k].b;}.
```

Intervals are formed from a pre-formed list of intervalList, having the type List <Interval>, and are filled using the following block of program listing:

```
private void bSetInterval_Click(object sender,
EventArgs e)
        {
          string[] arrInterval = interval.Split(':');
          double a =
Convert.ToDouble(arrInterval[0]);
          double b =
Convert.ToDouble(arrInterval[1]);
          intervalList.Add(new Interval() { a = a,
b = b });}.
```

The procedure of incrementing (vertices 10-11) or decrementing (vertices 12-13) can be carried out, for example, using the developed functions List <Trapeze> IncrementTrapezeList (List <Trapeze> trapList, double lengthAsixX) or List <Trapeze> DecrementTrapezeList (List <Trapeze > trapList, double lengthAsixX).

On the basis of the received CVSS metrics the estimation (top 14) is realized LS_i and classification of $\lambda_{uz,ij}$ obtained $\boldsymbol{ep}_{uz,i}$ (fasification).

If necessary (vertex 15) CVSS metrics are adjusted ***B***, ***T*** and ***E*** (vertex 16). Next, using the data obtained LS_i and $\lambda_{uz,ij}$, estimated RD $LRV_{rs,uz}$ (vertex 17) for each vulnerability reflected by the identifier $V_{rs,uz}$, and the average value is calculated $\boldsymbol{LR}_{rs}$. Here, based on the received $LRV_{rs,uz}$, $\boldsymbol{LR}_{rs}$ and constructed standards in the PDP, the structured parameter RD is formed SP_{uz} (dephasification).

As a result of the calculations performed by the method of IS RA (vertex 18) a report is formed on the estimates of the RD (Fig. 6), which contains $\boldsymbol{RISO}_{rs}$, $\boldsymbol{V}_{rs}$, $LRV_{rs,uz}$, $\boldsymbol{LR}_{rs}$, their linguistic equivalents, as well as a graphical interpretation (vertex 19) of the results (Fig. 3). To verify the work of the developed software (see Fig. 6), a corresponding experimental study was conducted.

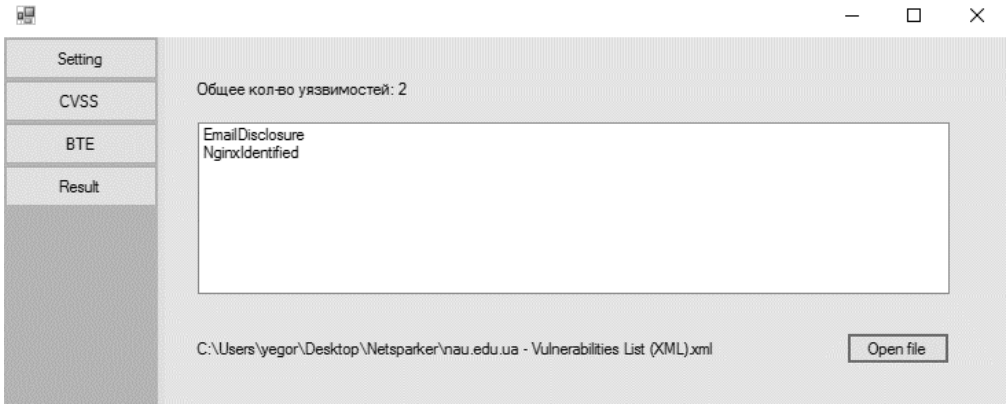


Figure 6: Fragment of the software system interface

To test the object of assessment for penetration used software to test the system for vulnerabilities - "Netsparker" (Fig. 7).

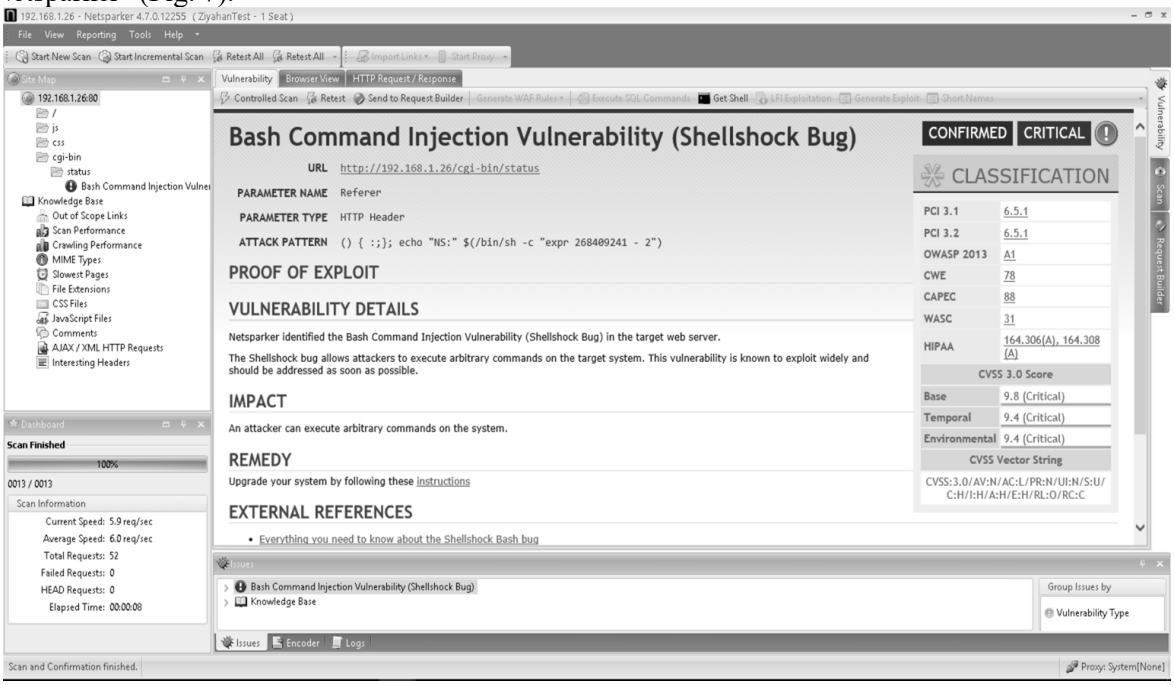


Figure 7: Interface part of the vulnerability scanning program «Netsparker»

As a result of scanning the XML file with the list of RIS and their vulnerabilities (fig. 8) was formed for the further use as input data of the developed system of IS RA.

xml-vul.txt — Блокнот

Файл Правка Формат Вид Справка

```
<classification>
        <OWASP2013></OWASP2013>
        <WASC>45</WASC>
        <CWE>200</CWE>
        <CAPEC>224</CAPEC>
        <PCI31></PCI31>
        <PCI32></PCI32>
        <HIPAA></HIPAA>
        <OWASPPC>C6</OWASPPC>

                <CVSS>
                        <vector>CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N</vector>

                        <score>
                                <type>Base</type>
                                <value>7.5</value>
                                <severity>High</severity>
                        </score>
                        <score>
                                <type>Temporal</type>
                                <value>7.5</value>
                                <severity>High</severity>
                        </score>
                        <score>
                                <type>Environmental</type>
                                <value>7.5</value>
                                <severity>High</severity>
                        </score>

                </CVSS>
</classification>
```

Figure 8: XML file with a list of vulnerabilities

Next, the input data is initialized as a list of vulnerabilities in the ListBox.

In fig. 9 and fig. 10, respectively, visualized examples of the implementation of the function of transforming the order of LV ***DR,*** which is performed at the request of the user by activating the process of increment and decrement.

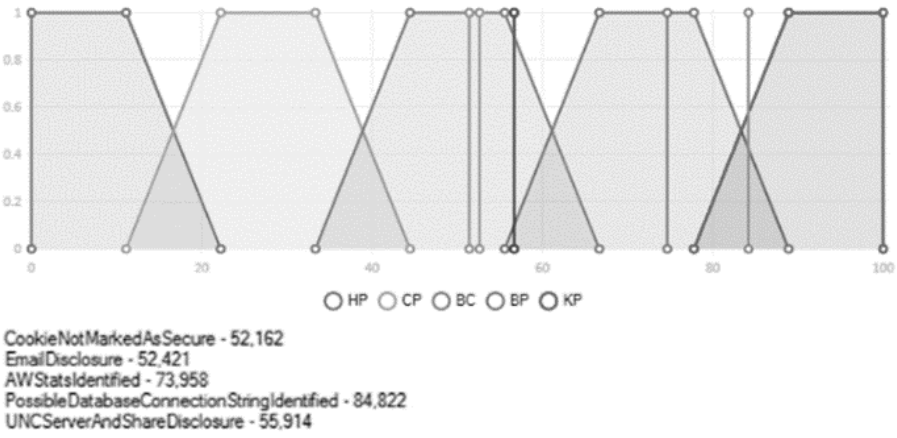


Figure 9: The result of incrementing the order of LV ***DR***

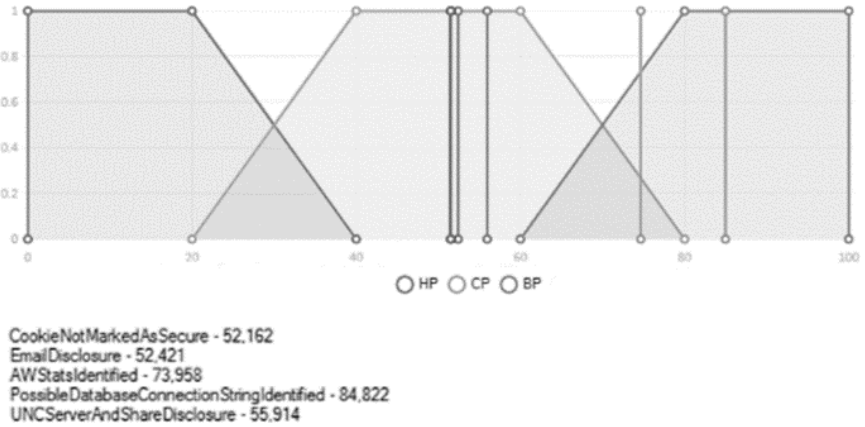


Figure 10: The result of decrement of LV ***DR***

Based on the obtained information about the assessment components and vulnerabilities, the system implements the calculation (vertex 17) of the RD for each vulnerability and with the help of a subprogram (vertex 18) that implements the functions of the MGR, performs a graphical interpretation of the vulnerability of the LV ***DR*** at m=4 (see Fig. 11). All the obtained results are recorded in the report generated by MGR.

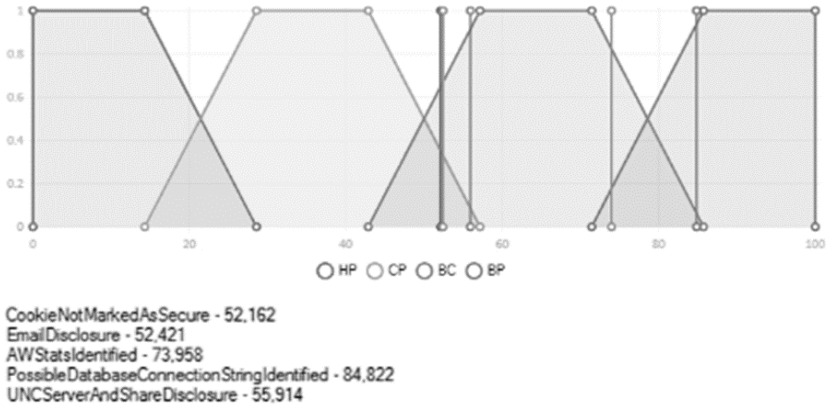


Figure 11: The result of the calculation of the RD for the identified vulnerabilities at the object of assessment

4. Conclusions

Thus, the structural solution of the real-time IS RA system is developed, which, due to the structural components of the subsystems of primary and secondary data generation, as well as their components of input data initialization modules, formation and conversion of reference values, weighing evaluation parameters and their adjustment, evaluation of RD and report generation, in which the proposed method is implemented, allows to provide certain properties of adaptability and efficiency in RA security of RIS in real time.

Also on the basis of the offered structural decision the basic algorithm and the corresponding software for estimation in the form of application software system of RA which unlike known uses values of CVSS (versions 2.0 and 3.0) of the indicators presented in the corresponding databases and allows real-time risk assessment of RIS security.

5. References

[1] «Common Vulnerability Scoring System v3.0: User Guide» [Electronic resource], *Forum of Incident Response and Security Teams*, Morrisville, 2016, [Online]. Access mode: http://www.first.org/cvss/user-guide.

[2] A. Korchenko, A. Arkhypov, S. Kazmyrchuk, Analyz y otsenyvanye ryskov ynformatsyonnoi bezopasnosty. Monohrafyia, Kyev: OOO «Lazuryt-Polyhraf», 2013, s. 275. (А. Корченко, А. Архипов, С. Казмирчук, *Анализ и оценивание рисков информационной безопасности*. *Монография*, Киев: ООО «Лазурит-Полиграф», 2013, с. 275).

[3] A. Korchenko, Postroenye system zashchyty ynformatsyy na nechetkykh mnozhestvakh. Teoryia y praktycheskye reshenyia, K.: MK-Press, 2006, s.320. (А. Корченко, *Построение систем защиты информации на нечетких множествах. Теория и практические решения*, К.: МК-Пресс, 2006, с.320).

[4] A. Korchenko, S. Kazmyrchuk, «Metod preobrazovanyia yntervalov v nechetkye chysla dlia system analyza y otsenyvanyia ryskov», Pravovoe, normatyvnoe y metrolohycheskoe obespechenye systemы zashchyty ynformatsyy v Ukrayne, № 1(31), S. 57-64, 2016. (А. Корченко, С. Казмирчук, «Метод преобразования интервалов в нечеткие числа для систем анализа и оценивания рисков», *Правовое, нормативное и метрологическое обеспечение системы защиты информации в Украине*, № 1(31), С. 57-64, 2016).

[5] Korchenko O.H, Kazmirchuk S.V., Akhmetov B.B., Prykladni systemy otsiniuvannia ryzykiv informatsiinoi bezpeky, Monohrafiia. – K.: TsP «Komprynt», 2017. – 435 s. (Корченко О.Г, Казмірчук С.В., Ахметов Б.Б., Прикладні системи оцінювання ризиків інформаційної безпеки, Монографія. – К.: ЦП «Компринт», 2017. – 435 с.).

Development of an Automated Passenger Transport Management System Using Microservices Architecture

Mykyta Dermenzhi[1], Svitlana Kuznichenko[2], Tetiana Tereshchenko[3], Iryna Buchynska[4], Viktoriia Klepatska[5]

[1, 2, 3, 4, 5]*Odessa State Environmental University, 15 Lvivska Str, Odesa, 65016, Ukraine*

Abstract

The paper presents applied aspects of the design and development of an automated passenger transportation management system for any transport company. A flexible architecture of the transport system (TS) is proposed, which is built according to the microservice methodology and simplifies the synchronization processes between drivers and operators. Vehicle information is updated via GPS. The proposed design approaches allow to customize the TS to the individual needs and initiatives of customers and quickly expand functionality and add new features and services. In addition, the system can be used as an intermediate node for embedding in an existing system to collect information and provide a graphical user interface for operators.

Keywords

Transport system, automated system, GPS, microservices architecture.

1. Introduction

Transport is one of the most important branches of social production and it is designed to meet the needs of the population in transportation. In Ukraine, most bus services are provided by small private enterprises. Their fleet of vehicles provides urban, long-distance and international transportation in Europe and the CIS. A feature of the work of private operators is the difficulty of control and the lack of a single system for monitoring vehicles on routes, which is often an obstacle to making operational decisions to optimize the operation of transport. In this regard, there is a need to create an automated passenger traffic management system with the following capabilities: 1

- Storage and management of information about vehicles and their technical characteristics;
- Driver information management: current position during the trip, contact details, the vehicle to which they are assigned;
- Ability to expand locations on the map and update them: location is a material point, which is added by the operator to establish a point of repair, parking, stopping, etc.;
- Keeping records of reference data on emergency repair and synchronization of data from external resources;
- Creating routes using external APIs, using software to store information in internal repositories and caching this data for the fastest response from the server;
- Systematize available information for planning future transportation;
- Automatic processing of the vehicle's arrival to the final stop and the ability to adjust the time in case of trip delays.

In recent years, researchers have shown great interest in the public transport system. This is largely due to the growth of cities and transport development of territories [1]. The principles of creation and features of transport systems (TS) architecture are widely discussed, which can provide important programs and services to improve the safety and mobility of passenger traffic, as well as to optimize transport resources and time [2-4]. The article [5] discusses public transport management systems for future smart cities built using Internet of Things (IoT) systems. TS is actively used in the architecture based on the joint use of IoT and geographic information systems (GIS), which have great potential to support decision-making in various

EMAIL: nikita.dermenzhi@gmail.com (A. 1); skuznichenko@gmail.com (A. 2); tereshchenko.odessa@gmail.com (A. 3); buchiskayira@gmail.com(A. 4); victoria.klepatska@gmail.com(A. 5)
ORCID: 0000-0003-3564-9806 (A.1); 0000-0001-7982-1298 (A. 2); 0000-0001-7691-6996 (A. 3); 0000-0002-0393-2781 (A. 4); 0000-0001-5613-6546 (A. 5);

fields of human activity [6-8], including public transport. Thus, in [9] a project of emergency management system for public transport networks was presented, which uses IoT technologies for traffic monitoring, as well as GIS to facilitate situational awareness and emergency operations. This work [10] explores how to develop an extremely flexible and comprehensive architecture for TS that can use the latest technologies, such as cloud computing and the subscribe-publish communication model.

However, despite the large number of publications related to the development of transport management systems, it is important to consider the applied aspects of the development of their infrastructure and implementation stages of design solutions.

In addition, one of the main problems associated with TS are external and internal integration processes, such as: the implementation of data dependencies and tracking their changes, tracking cars using intermediate services, and so on.

Thus, the main goal of this project is to develop an automated passenger transportation management system of the transport company with the ability to: systematize data obtained during trips, receive instructions for creating and installing new services, infrastructure preparation (ease and speed of deployment, integration of customer data, etc.), the ability to use the system on any platform and support for gadgets from phone to computer.

2. Presentation of the main research material

The main non-functional requirements (NFR) for the project are:

- completeness of information and technical specifications;
- availability of the service regardless of time;
- the ability to expand the content;
- dynamic cartography, independence from the map provider;
- confidentiality of customer data;
- security of obtaining data on synchronization of movements of system objects;
- service of operators and drivers in real time with minimal delays;
- design flexibility and ease of use by end customers;
- the ability to scale the system and the number of services during support;
- the possibility of the system deployment process on different platforms;
- support for data integration using resources and sources implemented by the customer;
- possibility of constant logging and data recovery;
- simplification of visualization on mobile devices and tablets, to maintain the full consistency of data, as well as the use of the platform by operators in cases of inability to use a computer;
- fast conversion of content with translation into other languages;
- dynamic specifications (vertical expansion): CPU speed, memory, disk space, network performance.

In addition, to determine the progress of the project, functional sections were introduced, which in turn build the system as a whole: Models, Vehicles, Drivers, Contacts, Locations, Cities / Regions / Countries, Routes, Schedules, Trips, System Settings.

2.1. Prerequisites for the implementation of the system

With each passing day, the implementation or sequential integration of artificial intelligence (AI) according to [11] research is becoming an increasingly important process in information systems. Such services can allow you to build trips more accurately, help resolve conflicts, and more. This project is integrated with TomTom systems, which provide AI API for building and calculating trips. Such routes are close to real, and it becomes easier for drivers and operators to coordinate actions.

Most modern systems use the Global Positioning System (GPS), which allows you to get the coordinates of vehicles and place marks on a virtual map [12].

It should be noted that the developed system also implements this approach and deepens it. This is an optimization model, when information is provided in small portions, and the user while navigating the virtual map loads updated or changed data. This reduces the load on the server and facilitates display on the client application.

Additionally, the system provides the ability to automatically calculate and build routes, simplify the workflow for operators and synchronize statuses for system users. In addition, the system can be used as an intermediate node to integrate into an existing system and used to gather information and provide a graphical interface for operators. This approach saves time on reporting and allows you to use the data recorded in the system as automatically generated reports. This increases the level of security and also reduces the risk of error on the part of the operator. All current data: vehicle location, rerouting, trip status update, adding or deleting locations and system users, are stored at the information store level.

Note that most of the existing logistics systems are tied only to the construction of vehicle tracking without the possibility of integration into this process of other users of the system, such as operators, administrators, persons who provide parking and repair facilities, etc. This project solves the main problem of transport companies: combining all operators, drivers and intermediate users of the system in a single application and saving current data for sequential analysis.

Project consumers can choose their own configuration and use integration processes to enter existing data (drivers, locations, automotive objects, routes, etc.) using an external integration service. This allows you to not disrupt the technological processes of the business and make it easy to combine two or more projects in one ecosystem.

It is assumed that the consumer is a self-employed person or a commercial group who is interested in saving time and money on late shipments, and instead wants to use systematization, storing important data on travel and drivers for further analysis. Data analysis of this type can provide an understanding of how employees perform their work and will allow them to track problems without direct contact with operators.

2.2. Implementation of constant vehicle tracking

There are several basic approaches to obtaining information from external resources [13]:

- Long Polling;
- WebSockets;
- Server-Sent Events.

All of them allow you to get up-to-date information using external systems.

WebSocket is a computer communication protocol that provides full-duplex communication channels over a single TCP connection. It is synchronous, which gives a high level of correctness, but connecting a large number of connections can lead to poor performance of the module.

Server-sent events (SSEs) are a one-way communication channel where events are transmitted only from the server to the client. Events sent by the server allow browser clients to receive the stream of events from the server over an HTTP connection without constant polling.

It was decided to use a combined approach to connect the system to the constant updating of vehicles via the GPS system: to create an intermediate module that will use web sockets, and to receive synchronous information.

As soon as the socket sends a new message from the vehicle tracker, this message is transmitted to the asynchronous queue. Thus, the queue will use the SSE approach, which sends messages to all system subscribers (authenticated users) through other communication channels (Fig. 1).

2.3. Architectural approaches during implementation

The project is based on the principles of the structure of micro-services, as shown in Fig. 2. The first service is a graphical user interface (GUI) layer what is a web application. The next mechanism in the system that provides most of the data changes and external resource providers is called the micro-service pool. A microservice is a small piece of system that can reside on different servers or even be embedded in a partition of an application, and works with external APIs, data warehouses, or prepares scheduling events.

The basic access service (BDS) is a common component for connecting to the data access level (DAL) and some necessary plug-ins: mapping, service data, etc. An internal database is an abstract layer that can be switched between providers and has a single interface. The only limitation is the need to have entities that are used in the main application and stored procedures. This type of abstraction makes it possible to choose the most convenient provider

for the database and absolutely provides a connection to the structure, as separate as possible from dependencies. This principle is the principle of GRASP, Low Coupling & High Cohesion [14]. To understand below (Fig. 3), the main set of micro-services in system architecture is presented.

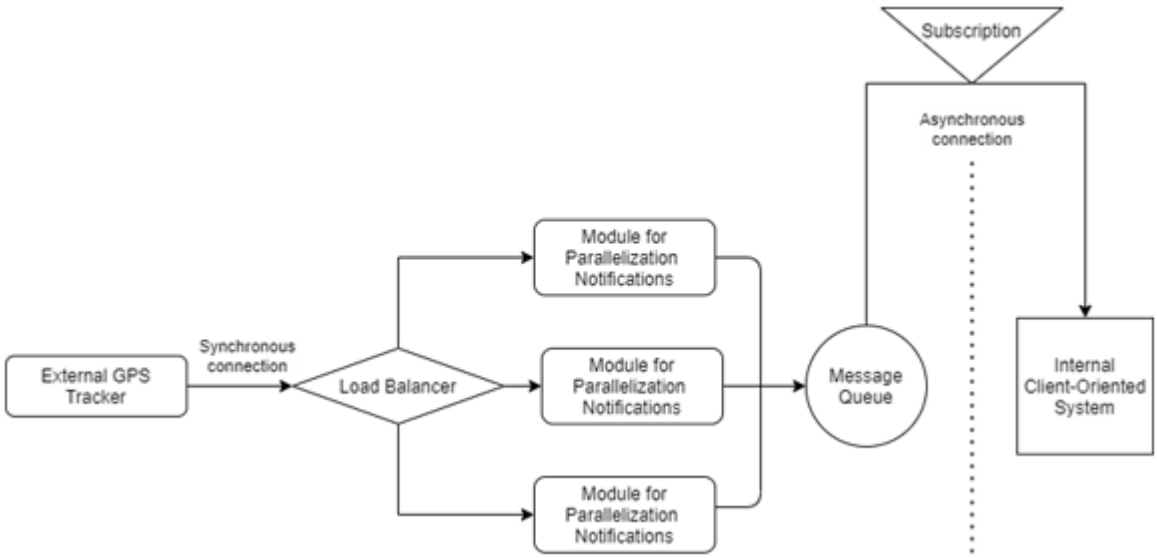


Figure 1: Combined approach to sending messages

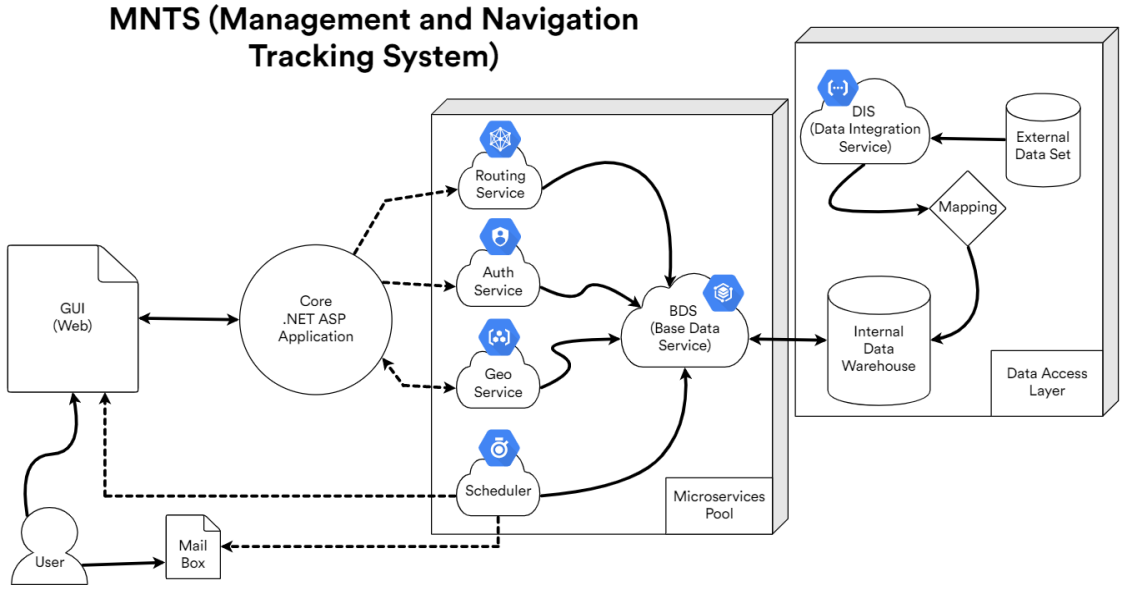


Figure 2: Diagram of micro-service architecture

Figure 3: Micro-services in the system

.

External datasets will be processed by the Data Integration Service (DIS), which will then be passed to a mapping process, where the data is converted to an internal model. Authentication service (AS) is a modern generation of token systems called JWT (JSON Web Token). This service allows you to authenticate and then identify moderators using only a hash with metadata sealed in it. The Geolocation Service (GS) is the "core" of the project and its main part. This means that the GS directly affects the data, in addition, it must build linked lists and include some additional data about places and objects.

It should be noted another pattern that was used during the implementation of the system: the Routing Service (RS) is based and configured using the TomTom API. To reduce requests, a Proxy template [15] has been implemented, which envelops this functionality and saves data to reduce the number of requests, thus reducing the cost of services (Fig. 4).

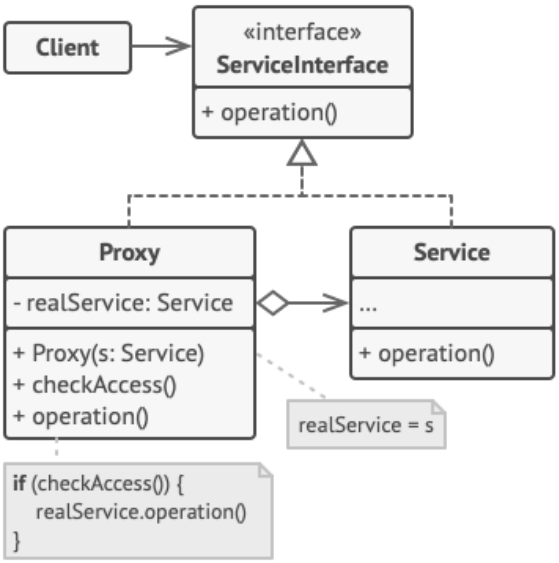


Figure 4: Proxy Pattern

For example, if a route has the same location, the system will use the saved data instead of making a new request.

The scheduler is the only module that can be either a separate service or a built-in part of the developed system. For the data warehouse, SQL Server was chosen, which provides the best connection experience and many features, such as triggers to schedule or even save data analysis if necessary.

2.4. Internal processes of the system

To explain the implementation, consider the Use-Case diagram in the Fig. 5, which presents the two main users of the system: the administrator and the driver.

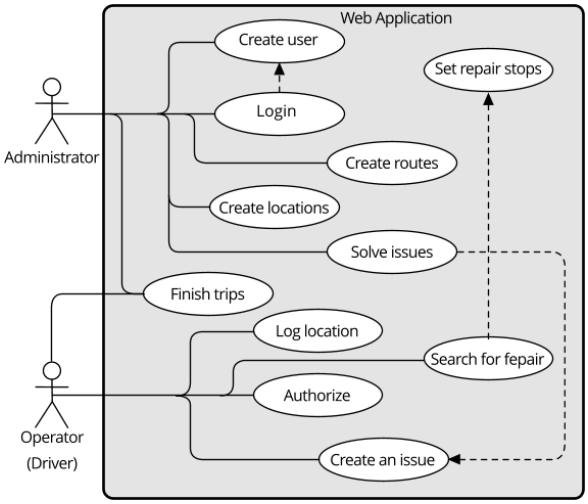


Figure 5: Use-Case diagram

As can be seen from the diagram, the driver has the following functionalities: go through the process of authorization and authentication, has automatic logging of its location and display in the application for administrators, can create requests to solve problems during trips, search for parking or repair; register intermediate statuses and terminate trips automatically or manually.

In turn, the administrator monitors the capabilities and responsibilities of drivers, confirming actions, as well as coordinates and solves problems as needed: creates new administrators and moderators, drivers, logs in the system, creates locations, fills in new information for system users, sets stop for repairs and parking, solves problems and problems of drivers during trips, creates new routes and manages trips.

The next step of implementation is the functions of creating new entities of the system, as shown below in the activity diagrams: the processes of creating a new driver, creating and making changes to routes and locations, creating a trip and accompanying processes during its execution.

As shown in the Fig. 6 - the process of creating a driver begins with filling out a questionnaire and then it branches into two parallel processes, which can be asynchronous,

which means the possibility of their delayed completion. If necessary, a separate entry is created for the driver with a new bus or an existing one is selected. After filling out the questionnaire, you can additionally fill in the contact details. Finally, all processes are synchronized and sent to the database.

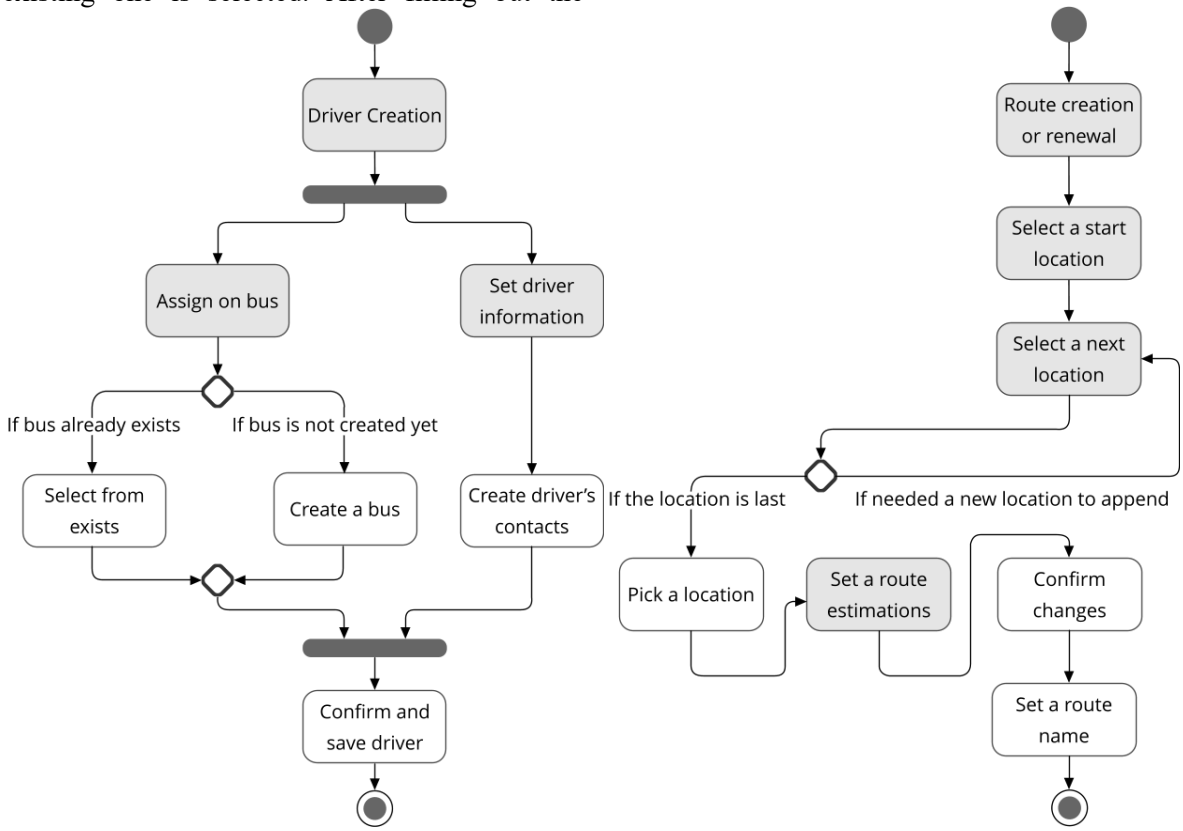


Figure 6: Activity diagram. Creating a driver and route

.

Creating and updating routes begins with a modal window that offers to specify or redefine the starting point, if this has been done or the route already has a starting position, the user can select new intermediate stops or change existing ones. The final step is the process of specifying the last location, which cannot be changed after. The system automatically offers estimates of time and route length based on data obtained during route calculation.

In order to start a trip, you need to create a new schedule or choose an existing one, after which the algorithm branches into two parallel processes: creating a system of stops with time intervals, setting metadata for a specific trip, as in Fig. 7. The system also has an automatic time calculation, which determines how much real time is required to travel the distance based on the geolocation of data. The process of creating metadata takes responsibility for specifying which bus, driver will perform the trip, as well as adjusting such parameters as date and time, etc.

Finally, we note the life cycle of the entire system through a state diagram (Fig. 8), which indicates the process, starting from the creation of the user, ending with the trip process and logging its final destination.

3. Conclusions

The developed system and the conducted researches introduce the service methodology for creation or integration into the existing systems for simplification of processes of synchronization between drivers and operators. The proposed approaches allow you to customize the system to individual customer needs and allow you to quickly expand the functionality regardless of existing ones.

As mentioned in the sections, each function or micro-service corresponds to an independent micro-service, which helps to increase the stability of the system. Despite the fact that the system already has a lot of services to address the basic needs of customers, it has and will

expand in commercial projects. This project solves the problem of bureaucracy when generating reports, analyzing trips, creating plans, etc. But the most important aspect it covers is the need to synchronize information between operators and drivers.

As every professional employer wants to provide good working conditions, and in the transport industry there is a growing demand for personnel management, and the staff is expanding every year, there is a need to quickly form trip schedules to avoid conflicts. Conflict situations mean overlapping schedules of routes, as well as emergencies. .

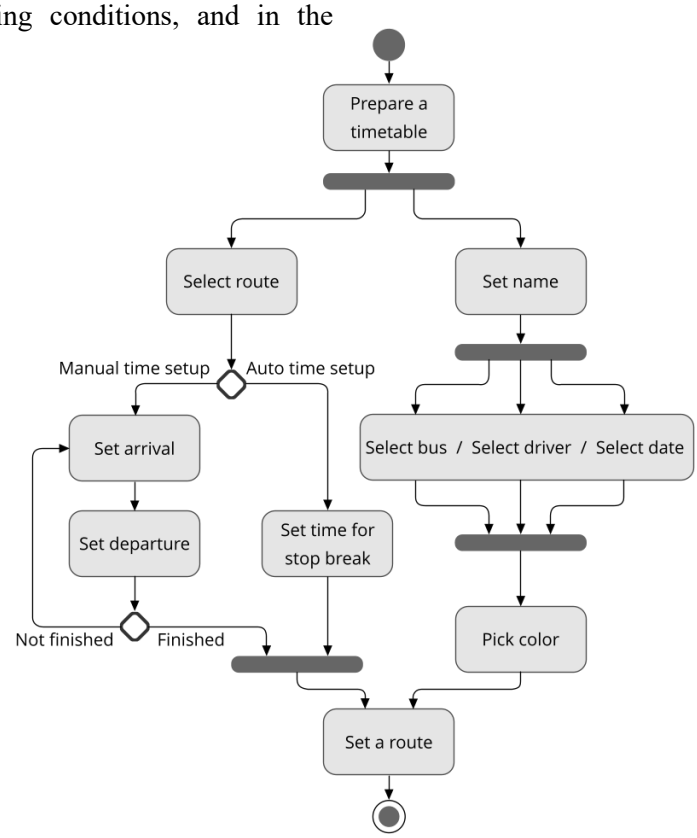


Figure 7: Activity diagram for creating a new schedule

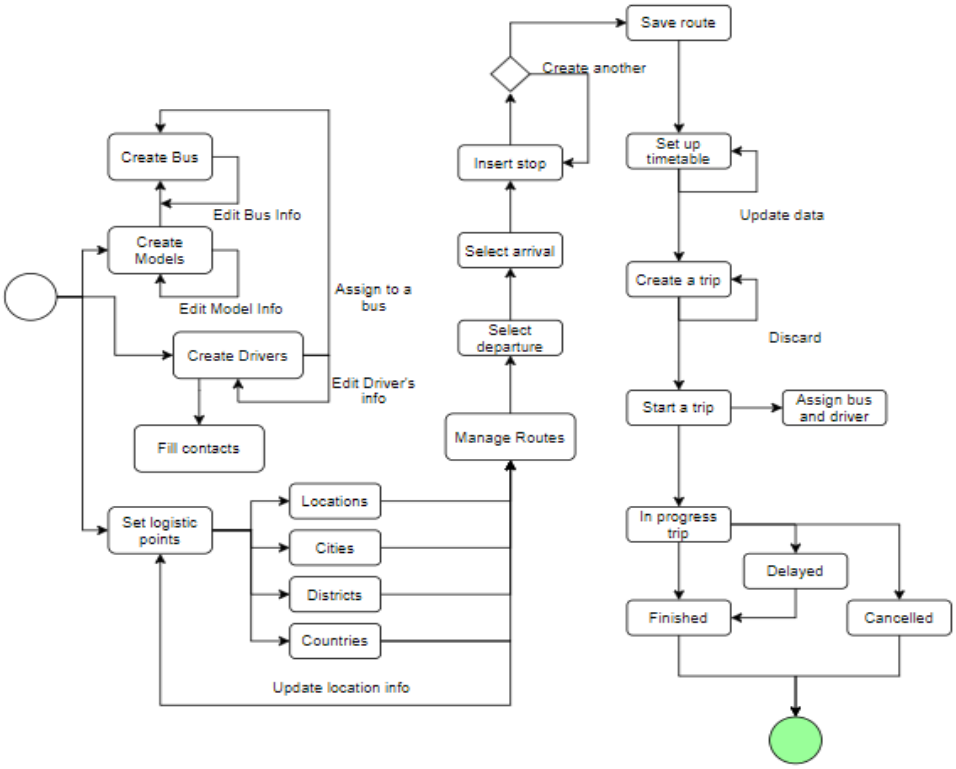


Figure 8: Life cycle. State diagram

It should also be noted that iterative operations were performed to increase optimization and correctness of the system, which led to an increase in possible connections to the tracking. All locations are stored in chunks, and when the client moves, it receives a new image with new data and cached previous ones, which saves memory and makes the application faster. Each route created by the user will be saved in the repository, and when the user tries to build a new route with multiple repetitive routes, this will result in retrieving the saved data instead of calling the API. This saves the client money and affects the performance of the application.

4. References

[1] M. Karpinski, S. Kuznichenko, N. Kazakova, O. Fraze-Frazenko, D. Jancarczyk.. Geospatial Assessment of the Territorial Road Network by Fractal Method. Future Internet. 12. 201 (2020). DOI:10.3390/fi12110201.

[2] Z. Cortes, J. Andres; A. Serna, M. Dario and A. Gomez.(2013). Information systems applied to transport improvement. Dyna rev.fac.nac.minas. vol.80, n.180. ISSN 0012-7353

[3] Alam, Muhammad & Ferreira, Joaquim & Fonseca, José. (2016). Introduction to Intelligent Transportation Systems. 10.1007/978-3-319-28183-4_1.

[4] A. Nuzzolo and A. Comi, "Advanced public transport and intelligent transport systems: New modelling challenges," Transp. A, Transp. Sci., vol. 12, pp. 674–699, Sep. 2016.

[5] Dinh Dung, Nguyen & Rohács, József & Rohacs, Daniel & Boros, Anita. (2020). Intelligent Total Transportation Management System for Future Smart Cities. Applied Sciences. 10. 8933. 10.3390/app10248933.

[6] Kuznichenko, S.,Buchynska, I.,Kovalenko, L.,Tereshchenko, T. Integrated information system for regional flood monitoring using internet of things. CEUR Workshop Proceedings, 2019, 2683, стр. 1–5

[7] Kuznichenko, S., Kovalenko, L., Buchynska, I., Gunchenko, Y. , Development of a multi-criteria model for making decisions on the location of solid waste landfills. Eastern-European Journal of Enterprise Technologies, 2018. Vol.2, No. 3(92). P. 21–31. DOI: 10.15587/1729-4061.2018.129287

[8] S. Kuznichenko, I. Buchynska, L. Kovalenko, Y. Gunchenko. Suitable site selection using two-stage GIS-based fuzzy multi-criteria decision analysis. Advances in Intelligent Systems and Computing, 2020, 1080 AISC, стр. 214–230
[9] P. Du, J. Chen, Z. Sun, and Y. Li, "Design of an IoT-GIS emergency management system for public road transport networks," in Proc. 1st ACM SIGSPATIAL Int. Workshop GIS Emergency Manage., Bellevue, WA, USA, Nov. 2015, p. 12.
[10] Robayet Nasim. Architectural Evolution of Intelligent Transport Systems (ITS) using Cloud Computing. Licentiate thesis. Karlstad University Studies, 2015:2. ISSN 1403-8099
[11] Ricardo Salazar-Cabrera, Álvaro Pachón de la Cruz, Juan Manuel Madrid Molina, Sustainable transit vehicle tracking service, using intelligent transportation system services and emerging communication technologies: A review, Journal of Traffic and Transportation Engineering, Vol.7, Issue 6, 2020, P. 729-747, ISSN 2095-7564, https://doi.org/10.1016/j.jtte.2020.07.003.
[12] Kamel, Mohammed B.. (2015). Real-Time GPS/GPRS Based Vehicle Tracking System. International Journal Of Engineering And Computer Science. 10.18535/ijecs/v4i8.05.
[13] Long Polling vs WebSockets vs Server-Sent Events, 2019. URL: https://medium.com/system-design-blog/long-polling-vs-websockets-vs-server-sent-events-c43ba96df7c1
[14] Design model: Use-Case realization with GRASP patterns, 2001. URL: https://www.pearsonhighered.com/assets/samplechapter/0/1/3/0/0130925691.pdf
[15] Design Patterns: Elements of Reusable Object-Oriented Software 1st Edition, Kindle Edition, by Gamma Erich, Helm Richard, Johnson Ralph, Vlissides John,

Наукове електронне видання

МІЖНАРОДНА НАУКОВО-ПРАКТИЧНА КОНФЕРЕНЦІЯ
“ІНФОРМАЦІЙНА БЕЗПЕКА ТА ІНФОРМАЦІЙНІ ТЕХНОЛОГІЇ”
13-19 вересня 2021
Харків–Одеса, Україна
МАТЕРІАЛИ КОНФЕРЕНЦІЇ
(українською та англійською мовою)

Видавець і виготовлювач
видавництво ХНЕУ ім. С. Кузнеця, 61166,
м. Харків, пр. Науки, 9А
Свідоцтво суб’єкта видавничої справи
Дк№481 від 13.06.2001