Method of Determining Trust and Protection of Personal Data in Social Networks

Laptiev O.[1], Savchenko V.[1], Kotenko A.[1], Akhramovych V.[1], Samosyuk V. [1], Shuklin G[1], Biehun A.[2]

[1]Institute of Information Protection, State University of Telecommunications, Kyiv, Ukraine
[2]Institute of Information and Communication Technologies and Systems, Vadym Hetman Kyiv National University of Economics, Kyiv, Ukraine

Abstract: The analysis of parameters of social networks (information transfer to other users, traffic density, probability of network construction) is carried out. Three variants of solving the equation near the steady state of the system are considered. The protection of personal data increases from the growing factors of trust in information.
Mathematical modeling of the dependence of personal data protection on trust is performed. The results obtained in the article showed that the protection of personal data is directly proportional to the reliability and trust, with constant security parameters. The protection of personal data increases with the growth of trust parameters.

Keywords: social network, user, parameter, transmission, information, metrics, density, cycle.

1. Introduction

In today's world, almost everyone has valuable electronic information, whether it is your personal data or working documents - a financial report, a plan to work with a prospective client or a strategy for the development of the company's services. Such information needs reliable protection: from unauthorized access and distribution, accidental deletion or alteration. All developed European countries are concerned about the problem of information security, as well as the protection of personal data of citizens. This is due to the fact that informatization and digitization of information have become widespread in all areas of human activity, including the storage of personal and work data.
At the current level of technology development, social networks are one of the main methods of communication, search for connections and exchange of both publicly available and confidential information. Social networks, which make up an ever-growing share of shared networks, the network itself acquires new properties, acting as a separate factor (in addition to factors such as interface, network node and connections between nodes).
Because information in the global network exists outside of space and time, the network itself becomes an active agent of influence on the person, keeping, above all, large amounts of data publicly available. Any user can log in to the network (legally or illegally) and access the nodes he needs (when using cloud tools, specific nodes may be unknown to the average user), also changing their content (for example, Wiki-object) according to the allowed rules.
In recent years, the vision of the problem of cybersecurity has begun to change significantly, as people increasingly cease to be the subject of cybercrime, becoming an object in itself, and not only its financial and economic interests and capabilities. More and more analysts are pointing out that the main causes of incidents in Internet resources are related to the action of the human factor, the mass hacking of IoT devices and cloud services. This problem is especially exacerbated by the strengthening of the digital humanistic nature of education, the growing role of social networks in human life in general.
Thus, according to KPMG International, which conducted a global study in the banking sector [1,4,25-27] in the period from November 2018 to February 2019, 2365 million customer data and records became publicly available. The study addresses the risks of fraud in the banking sector, includes investigations and surveys of security professionals on trends in fraud typologies, challenges faced by banks in minimizing internal and external threats in the period 2016-2018 and was conducted in 43 retail banks, 13 of which are located in the countries of the Asia-Pacific region, 5 - in America and 25 - in Europe, the Middle East and Africa (EMA). According to the Center for Combating Internet Crime Complaints, which is under the jurisdiction of the FBI, published in June 2018, the amount of damage caused by BEC schemes is more than 12 billion US dollars In [2,28].
Therefore, the problem of studying the parameters of social networks for their further use in solving problems of information and personal data protection is very relevant.

2. Literature Survey and problem statement

Modern social networks have significantly changed the consideration of the issue - researchers now have a «free» resource to search, and the rapid spread of online social services and the development of Big Data technology, have aroused interest in using information from social networks in various fields. The exchange of structural and thematic data potentially allows the use of social networks to address a wide range of data protection issues.
In [3,5] the standards, attributes and characteristics of the «actor» profile are considered and the method of revealing signs of manipulation of public opinion in social networks on the basis of construction of information security profiles of «actors» of social Internet services which is based on gradient strengthening of binary trees is offered, which allowed to automate the procedures for early detection of threats.
In [6] analyzes the features of the airline network, which shows that the main threats to information security are related to the use of regional communication networks. To ensure the proper level of information security and its control

in the real conditions of the airline, it is proposed to use a software switch that allows you to restrict access to networks. To obtain in the analytical form of the sensitivity functions of the system used in solving the problem of increasing reliability, applied the methods of harmonic analysis.

In [7] only the problems of interaction of trust parameters are considered, but the set of parameters of threat in social networks from loss of trust between users is not considered. Therefore, the problem is not fully resolved.

In [8,9] the mechanism of application of correlation of potential crisis situations for an estimation of average and total level of criticality of a current situation in information sphere is considered. The mechanism is based on methods of expert evaluation and fuzzy logic. A correlation mechanism is proposed to determine the correlation coefficient of each dependent identification of potential crisis situations with the main one, which determines the interdependencies between them. The obtained correlation coefficients can be used to calculate the average and total levels of criticality of a situation that has arisen under the influence of several interrelated and simultaneous potential crisis situations. Correlation coefficients determine the common features of the impact of each of the incidents on the system or environment being protected, and are determined by comparing the parameters of assessing the level of criticality of each, identifying potential crises. Only information correlation problems are considered.

In [10, 34-36] developed a structural-parametric model of information security risk assessment system which, due to the structural components of subsystems, the formation of primary and secondary data, as well as their components modules of initialization of input data, formation and conversion of reference values, weighing evaluation parameters and their adjustment, risk assessment and report generation, in which the proposed methods are implemented, assessment based on vulnerability databases, incrementing and decrementing the order of linguistic variables, allows to provide high flexibility and convenience in assessing information security risks without the participation of experts in the subject area.

Based on the proposed structural-parametric model, developed a basic algorithm and a corresponding software tool for evaluation in the form of an application software system - «RISK-CALCULATOR», which uses CVSS values (versions 2.0 and 3.0) of indicators presented in the relevant databases and allows to implement information risk assessment. real time security.

In [11,12] only issues of information security presented in CVSS databases (versions 2.0 and 3.0) are considered. The threat of loss of trust between users is not considered, the number of parameters of threats in social networks is limited and incomplete, so the integrated indicator of loss trust between users is not considered. Therefore, the solution to the problem has not been completed.

In [13,29] considered the qualitative-quantitative method of analysis and assessment of information security risks by modifying the procedures for determining many parameters of risk assessment and assessment of current values of parameters with the ability to integrate CVSS values, which are presented in the relevant databases. To do this, it is proposed to use appropriate vulnerability databases, which represent their quantitative estimates, such as the National Vulnerability Database (USA); information security threat data bank (Russian Federation); Open Sourced Vulnerability Database (USVDB); IBM X-Force Vulnerability Database (US), US-CERT VND Vulnerability Record Database (US), SecurityFocus Vulnerability Database (US), etc. The basic component of such databases is CVSS (Common Vulnerability Scoring System).

In [14,37] only information security issues are considered, which are really presented in the databases of CVSS indicators, but the set of threat parameters in social networks is not complete, so the threat of loss of trust between users is not considered. Therefore, the problem is not completely solved and needs further testing.

In [15,17,38] the methodology of construction of the system of information security of banking information in automated banking systems (ABS) is considered, which is based on the first proposed three-level model of strategic management of information technology security. It is based on the first introduced synergetic model of information security information threats, while taking into account information security threats and banking information security threats in the ABS. Hybrid crypto-code constructions on unprofitable codes are offered, which are based on cryptographic transformations of noise-tolerant and unprofitable coding, which allowed to guarantee security services at the set probabilistic indicators. Thus, the speed of crypto-transformations is provided at the level of BES, crypto-stability at the level of 1025-1035 group operations, the probability of transferring banking information to the ABS through open communication channels is not lower than RP 10-9-10-12.

In [16,18-20] only issues of information security are considered, without taking into account technical parameters and problems of trust between users. Therefore it is complex. the overall indicator of the threat of loss of trust between users is not considered. The solution to the problem has not been completed.

The aim of the article is to study the whole set of parameters of threats in social networks from the loss of trust between users for their further use in solving problems of information and data protection.

The exchange of structural and thematic data potentially allows the use of social networks to address a wide range of information issues, including data protection. Therefore, the issue of developing new methods for assessing the dependence of personal data protection on trust in social networks is very relevant.

The purpose of this study is to develop a new method for assessing the dependence of personal data protection on trust in social networks.

3. Proposed Methodology

In the classical approach to the problem of personal data protection, there are many threats of loss of trust between users, which can be represented as a dependence [21 - 23,29 - 32]:

$$T_i = \left[D_j, D_n, D_m, D_k \right], \qquad (1)$$

where:

T_i - the set of threats of loss of trust between users;

D_j - trust in the provision of services (a person trusts the party in the provision of quality services or resources by the provider);

D_n - delegation trust describes the trust in the user (representative), who acts and makes decisions on behalf of the party he trusts;

D_m - access trust describes the trust on the part (provider) to the user who is granted access to resources. This is access control. Used in authentication systems;

D_k - contextual trust determines the degree of the participant's faith in the necessary systems and institutional mechanisms that support transactions and ensure network security.

Loss of such a quality as trust is a process that has a time interval [24]. Denote the amount of information in the system - I. The flow of information outside the information system through dI -, the rate of change of this flow - $\frac{dI}{dt}$. It is logical that if the flow and the rate of change of flow are zero, then there is no leakage of information:

$$dI = 0; \frac{dI}{dt} = 0 . \quad (2)$$

What can the leakage of information depend on? First of all, from the security of the system, the measures taken to neutralize threats to the security of personal data.

Z - indicator of information system security. Let's make the equation:

$$\frac{dI}{dt} = Z_p Z + (C_v + C_k) I , \quad (3)$$

where:

Z_p - coefficient reflecting the impact of information protection measures;

Cv - coefficient that reflects the impact of the rate of leakage of personal data;

C_k - factor that reflects the impact of the amount of personal data on their leakage.

This equation can be interpreted as follows. Information leakage depends on:

- from the size of the information system (hence, to some extent, from the amount of personal data);
- from the speed of leakage of personal data;
- information leakage is suspended by the security of the system (measures to neutralize information security threats).

Next, consider what determines the security of the system - Z. Define the security of the system as the ability of the system to resist unauthorized access to the confidentiality of personal data. Therefore, the security of the system will depend on [25]:

- system size (as well as the amount of personal data);
- information security threats from loss of trust between users.

Let's make the equation:

$$\frac{dZ}{dt} = D_i - I(C_{d2} + C_{d1}) , \quad (4)$$

where: D_i - coefficient that reflects the impact of threats to the security of personal data from the loss of trust between users on the security of the information system;

C_{d2} - coefficient that reflects the impact of system size on security;

C_{d1} – factor that reflects the impact of security on the leakage of personal data.

Combine equations (2.3) and (2.4) into a system:

$$\begin{cases} \frac{dI}{dt} = Z_p Z + (C_v + C_K) I \\ \frac{dZ}{dt} = D_i - I(C_{d2} + C_{d1}) \end{cases} . \quad (5)$$

Find the stationary position of the system described by equations (5). Stationary conditions. Therefore:

$$dI = 0; \frac{dI}{dt} = 0 . \quad (6)$$

From the second equation of the system it follows that:

$$\bar{I} = \frac{D_i}{(C_{d2} + C_{d1})} . \quad (7)$$

Next, from the first equation of the system of equations (6) we find $\bar{Z}$.

$$Z_p \bar{Z} - \frac{(C_v + C_K) D_i}{(C_{d2} + C_{d1})} = 0 , \quad (8)$$

$$\bar{Z} = \frac{(C_v + C_K) D_i)}{(C_{d2} + C_{d1}) Z_p} . \quad (9)$$

Since the reliability of the protection system depends on the value of trust parameters between users of the social network, it is necessary to analyze the parameters of trust in social networks (develop mathematical models) and develop ways to improve them.

Therefore, the conditions of the position of the stationary system:

$$\begin{cases} \bar{I} = \frac{D_i}{C_{d2} + Z_p} \\ \bar{Z} = \frac{(C_v + C_K) D_i}{(C_{d2} + C_{d1}) Z_p} \end{cases} . \quad (10)$$

Solve the system of equations (5) by the method of «small deviations» $I = \bar{I} + I; D = \bar{D} + D$ and then, the system of equations will take the form:

$$\begin{cases} \bar{I} = \frac{D_i}{C_{d2} + Z_p} \\ \bar{Z} = \frac{(C_v + C_K) D_i}{(C_{d2} + C_{d1}) Z_p} \end{cases} , \quad (11)$$

$$\begin{cases} \frac{dI}{dt} = (C_{d1} + C_{d2}) Z - (C_v + C_K) I \\ \frac{dZ}{dt} = -I(C_{d2} + D_i) \end{cases} \quad (12)$$

Differentiating the first equation of system (12) we obtain:

$$\frac{d^2I}{dt^2} = -I(C_{d1} + C_{d2})(Z_p + D_i) - (C_v + C_K)\frac{dI}{dt}\ , \qquad (13)$$

$$\frac{d^2I}{dt^2} + (C_v + C_K)\frac{dI}{dt} + (C_{d1} + C_{d2})(Z_p + D_i)I = 0\ . \qquad (14)$$

Equation (14) is the equation of a harmonic oscillator with a decaying amplitude, where:

$$\omega_0 = \sqrt{(C_{d1} + C_{d2})(Z_p + D_i)}\ , \qquad (15)$$

$$\omega = \sqrt{(C_{d1} + C_{d2})(Z_p + D_i) - \frac{(C_v + C_K)^2}{4}}\ , \qquad (16)$$

$$T = \frac{2\pi}{\sqrt{(C_{d1} + C_{d2})(Z_p + D_i) - \frac{(C_v + C_K)^2}{4}}}\ , \qquad (17)$$

$$\beta = \frac{(C_v + C_K)}{2}\ . \qquad (18)$$

The solution of the equation of a harmonic oscillator is divided into three cases.
The first case when:

$$\beta \prec \omega_0 : I = A_0 \exp(-\frac{(C_v + C_K)}{2}\cos\times \times(\sqrt{(C_{d1} + C_{d2} + Z_p + D_i) - \frac{(C_v + C_K)^2}{4}}t + \varphi_0) \qquad (19)$$

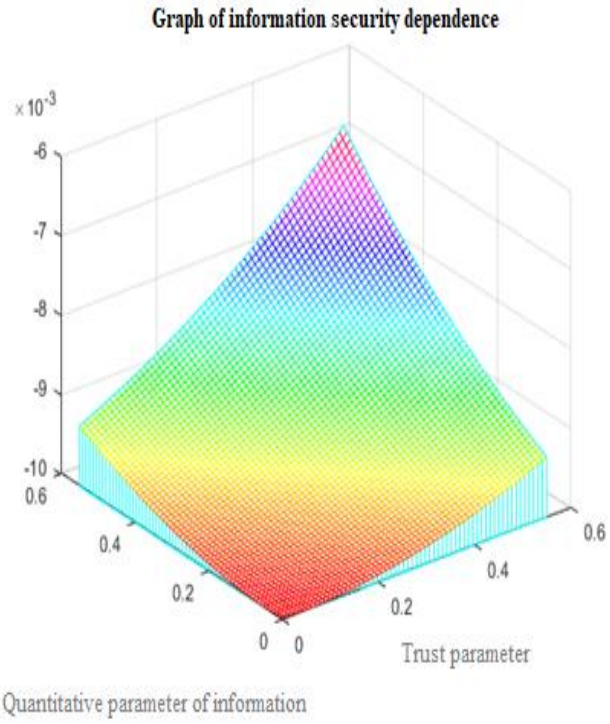

Figure 1. Dependence of personal data protection on trust between users for the first case

The second case when:

$$\beta = \omega_0 : I = (A_0 + B_0 t\exp(-\frac{(C_v + C_K}{2}t) \qquad (20)$$

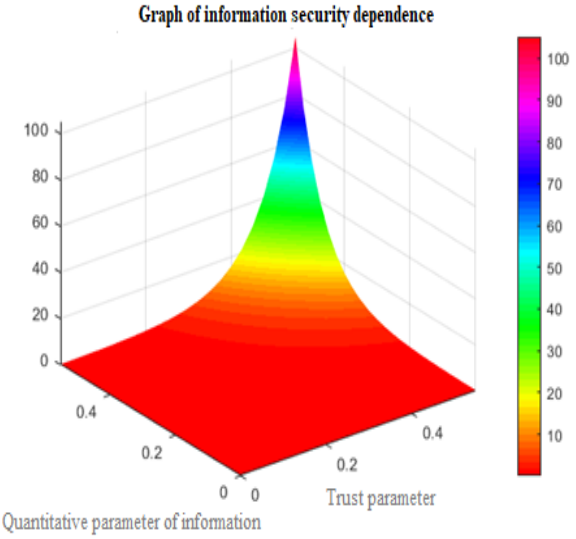

Figure 2. Dependence of protection of personal data on trust between users for the second case

The third case when:

$$\beta \succ \omega_0 : I = A_0 \exp(-y_1 t) + B_0 \exp(-y_2 t)$$

$$\partial e \qquad (21)$$

$$y_{12} = \beta \pm \sqrt{\frac{(C_v + C_K)^2}{4} - (C_{d1} + C_{d2} + Z_p + D_i)}$$

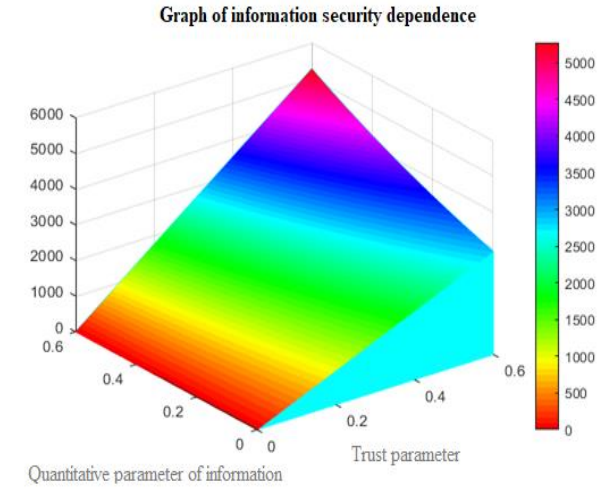

Figure 3. Dependence of personal data protection on trust between users for the third case

Considering three options for solving the equation near the steady state of the system, we can conclude that, based on the conditions of the ratio of dissipation and natural frequency, the attenuation of the latter to a certain value is carried out periodically, with decaying amplitude, or exponential attenuation law. But the protection of personal data is growing from the growing factors of trust in information.

In general, we obtained the results, in general: the dependence of personal data protection on trust is directly proportional to the constant parameters of protection (Figure 4), and increases with increasing factors and parameters of trust.

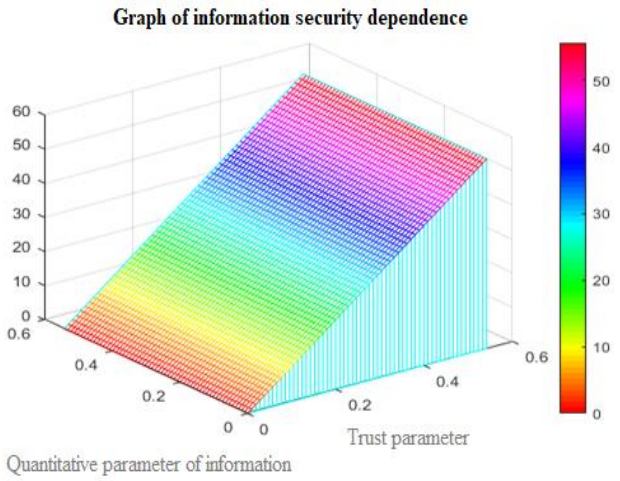

Figure 4. Dependence of protection of personal data on trust between users (at all other values of parameters equal to unit)

The obtained graphic simulation materials according to the proposed method of determining the protection of personal data from trust in social networks, fully confirm the theoretical calculations. This indicates the adequacy of our proposed methods.

4. Conclusions

A method for assessing the dependence of personal data protection on trust in social networks is proposed.
Carried out simulations for three different types of changes in confidence parameters. All three variants of solving the equation near the steady state of the system proved that, based on the conditions of the ratio of dissipation and natural frequency of confidence, and the attenuation of the latter to a certain value is carried out periodically, with damped amplitude, or exponentially decaying law. The obtained graphic materials fully showed that the protection of personal data increases with the growth of factors of trust in information. The dependence of personal data protection on trust is directly proportional to other constant protection parameters.

References

[1] Perera R. Recent Advancesin Natural Language Generation: AS urvey and Classification of the Empirical Literature. Computing and Informatics, vol. 36, pp. 1–32, 2017.

[2] Kravchenko Y. Evaluating the effectiveness of cloud services. 2019 IEEE 1th International Scientific-Practical Conference Problems of Infocommunications Science and Technology, PIC S&T`2019, Kyiv, pp.120–124, 2019.

[3] Pennington J. Socher R.., Manning C. D., Glove: Global vectors for word representation. EMNLP, vol. 14, pp. 1532–43, 2014.

[4] Kiros, R., Zhu Y., Salakhutdinov R. R. Skip-thought vectors. Advances in Neural Information Processing Systems, pp.3276– 3284, 2016.

[5] Dukhnovska K.K. Formuvannya Posukovy dynamical vector space.Shtunniy intertekt, no3.4, pp. 28-36, 2016.

[6] Barabash O.V., Open'ko P.V., Kopiika O.V., Shevchenko H.V., Dakhno N.B. Target Programming with Multicriterial Restrictions Application to the Defense Budget Optimization. Advances in Military Technology, vol. 14, no. 2, pp. 213 – 229 , 2019.

[7] Kreines M.G., Kreines E.M. Control model for the alignment of the quality assessment of scientific documents based on the analysis of content-related context. JCSSI, vol. 55, no. 6, pp. 938–947,2016.

[8] Musienko A.P., Serdyuk A.S. Lebesgue-type inequalities for the de la Valée-Poussin sums on sets of analytic functions . Ukrainian Mathematical Journal, Volume 65, Issue 4, pp. 575 – 592, September 2013.

[9] Musienko A.P., Serdyuk A.S. Lebesgue-type inequalities for the de la Vallée poussin sums on sets of entire functions. Ukrainian Mathematical Journal, Volume 65, Issue 5, pp. 709 – 722, October 2013.

[10] Grigoryan D.S. Cogerent data processing in tasks of spectral analysis of super resolution radar signals. Journal of Radio Electronics" Electronic Journal, 2012. № 3 http://jre.cplire.ru/jre/mar12/1/text.html.

[11] Bakiko V.M., Popovich P.V.,. Shvaichenko V.B. Determination of noise immunity of a communication channel in case of accidental interference. Bulletin of the National tech. University "KhPI": Coll. Science. Kharkiv: NTU "KhPI", № 14 (1290). P. 7 – 10, 2018.

[12] 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. 4/9 (100). pp. 6–19, 2019.

[13] Lubov Berkman, Oleg Barabash, Olga Tkachenko , Andri Musienko, Oleksand Laptiev, Ivanna Salanda. The Intelligent Control System for infocommunication networks. International Journal of Emerging Trends in Engineering Research (IJETER) Volume 8. No. 5, pp.1920 – 1925, May 2020.

[14] Vitalii Savchenko, Oleh Ilin, Nikolay Hnidenko, Olga Tkachenko, Oleksander 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, Scopus Indexed - ISSN 2347 – 3983. pp.2019 – 2025, May 2020.

[15] Olexandr Laptiev, German Shuklin, Spartak Hohonianc, Amina Zidan, Ivanna Salanda. Dynamic model of Ceber Defence Diagnostics of information Systems with the Use of Fozzy Technologies IEEE ATIT 2019 Conference Proceedings Kyiv, Ukraine, December 18 - 20, pp.116-120, 2019.

[16] Sweta Srivastav, Sangeeta Gupta. Results with Matlab coding of Middle Graph of Cycle and its related graphs in context of Sum Divisor Cordial International Journal of Innovative Technology and Exploring Engineering (IJITEE), Volume-8 Issue-2, pp. 398 – 401, February 2020.

[17] V. Savchenko, V. Zaika, M. Trembovetskyi, G. Shuklin, L. Berkman, K. Storchak, I. 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, , pp. 2246-2251, September - October 2019.

[18] Mashkov O.A., Sobchuk V.V., Barabash O.V., Dakhno N.B., Shevchenko H.V., Maisak T.V. Improvement of variational-gradient method in dynamical systems of automated control for integro-differential models. Mathematical Modeling and Computing, Vol. 6, No. 2, pp. 344 – 357, 2019.

[19] Barabash O., Dakhno N., Shevchenko H., Sobchuk V. 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). 16-18 October, National Aviation University, Kyiv, Ukraine. pp. 94 – 97, 2018.

[20] Ihor Ruban, Nataliia Bolohova, Vitalii Martovytskyi, Nataliia Lukova-Chuiko , Valentyn Lebediev. Method of sustainable detection of augmented reality markers by changing deconvolution. International Journal of Advanced Trends in Computer Science and Engineering (IJATCSE).Volume 9, No.2, pp.1113-1120, March-April 2020.

[21] Lubov Berkman, Oleg Barabash, Olga Tkachenko , Andri Musienko, Oleksand Laptiev, Ivanna Salanda. The Intelligent Control System for infocommunication networks. International Journal of Emerging Trends in Engineering Research (IJETER) Volume 8. No. 5, Scopus Indexed - ISSN 2347 – 3983. pp.1920 – 1925. May 2020.

[22] Aaron Don M. Africa, Lourdes Racielle Bulda, Matthew Zandrick Marasigan, Isabel Navarro. Binary Phase Shift Keying Simulation with MATLAB and SIMULINK International Journal of Innovative Technology and Exploring Engineering (IJITEE), Volume-8 Issue-2, February 2020.

[23] Barabash Oleg, Laptiev Oleksand, Tkachev Volodymyr, Maystrov Oleksii, Krasikov Oleksandr, Polovinkin Igor. 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, Indexed- ISSN: 2278 – 3075. pp 4133 – 4139, August 2020.

[24] 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, pp 8725-8729, September - Oktober 2020

[25] Wahyul Amien Syafei, Yosua Alvin Adi Soetrisno and Agung Budi Prasetijo.Smart Agent and Modified Master-Backup Algorithm for Auto Switching Dynamic Host Configuration Protocol Relay through Wireless Router/ International Journal of Communication Networks and Information Security (IJCNIS) Vol. 12, No. 2, pp 248–255, August 2020.

[26] Oleg Barabash, OleksandrLaptiev, 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, pp 5713–5718. September 2020.

[27] .M. Rakushev, O. Permiakov, S. Tarasenko, S. Kovbasiuk, Y. Kravchenko, O. Lavrinchuk “Numerical Method of Integration on the Basis of Multidimensional Differential-Taylor Transformations”, International Scientific-Practical Conference Problems of Infocommunications Science and Technology, PIC S&T`2019, Proceedings. pp.675–678.

[28] Y. Kravchenko, K. Herasymenko, V. Bondarenko, O. Trush, M. Tyshchenko, O. Starkova, “Model of Information Protection system database of the mobile terminals information system on the territory of Ukraine (ISPMTU)”, IEEE International Scientific-Practical Conference Problems of Infocommunications Science and Technology, PIC S&T`2020 – Proceedings, in press.

[29] Pichkur, V. V., Sasonkina, M. S.: Maximum set of initial conditions for the problem of weak practical stability of a discrete inclusion. J. Math. Sci. 194, 414-425 (2013)

[30] Garashchenko, F.G., Pichkur, V.V.: On Properties of Maximal Set of External Practical Stability of Discrete Systems. Journal of Automation and Information Sciences. 48(3), pp. 46-53.2016.

[31] Pichkur, V.: On practical stability of differential inclusions using Lyapunov functions. Discrete and Continuous Dynamical Systems. Series B. 22, pp.1977 – 1986, 2017.

[32] 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, 2020.

[33] Barabash O.V., Open’ko P.V., Kopiika O.V., Shevchenko H.V. and Dakhno N.B. Target Programming with Multicriterial Restrictions Application to the Defense Budget Optimization. Advances in Military Technology. 2019. Vol. 14, No. 2, pp. 213 – 229. ISSN 1802-2308, eISSN 2533-4123. DOI 10.3849/aimt.01291, 2019.

[34] Smelyakov K., Chupryna A., Hvozdiev M., Sandrkin D., Martovytskyi V. Comparative efficiency analysis of gradational correction models of highly lighted image. 2019 IEEE International Scientific-Practical Conference Problems of Infocommunications, Science and Technology (PIC S&T), 8-11 Oct. 2019, Kyiv, Ukraine. pp. 703–708, 2019

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

[36] S. Khan, K. K.. Loo. Real time cross layer flood detection mechanism. Elsevier Journal of Network Security, Vol. 16, No. 5, pp. 2–12, 2009.

[37] Maha Abdelhaq, Raed Alsaqour, Noura Albrahim, Manar Alshehri, Maram Alshehri1, Shehana Alserayee, Eatmad Almutairi, Farah Alnajjar.The Impact of Selfishness Attack on Mobile Ad Hoc Network. International Journal of Communication Networks and Information Security (IJCNIS).Vol. 12, No. 1, April 2020, pp.42 – 46, 2020.

[38] Abdullah Shakir, Raed Alsaqour, Maha Abdelhaq, Amal Alhussan, Mohd Othman, Ahmed Mahdi. Novel Method of Improving Quality of Service for Voice over Internet Protocol Traffic in Mobile Ad Hoc Networks. International Journal of Communication Networks and Information Security (IJCNIS). Vol. 11, No. 3, December 2019, pp.331–341, 2019.