ISSN 2347 - 3983
Volume 8. No. 2, February 2020
International Journal of Emerging Trends in Engineering Research
Available Online at http://www.warse.org/IJETER/static/pdf/file/ijeter05822020.pdf
https://doi.org/10.30534/ijeter/2020/05822020

# Analysis of Social Network Parameters and the Likelihood of its Construction

**Vitalii Savchenko[1], Volodymyr Akhramovych[2], Alina Tushych[3], Irina Sribna[4], Ihor Vlasov[5]**
[1]Director of Information Security Institute, State University of Telecommunication, Kyiv, Ukraine, savitan@ukr.net
[2]Associate Professor, Department of Information and Cybersecurity Systems, State University of Telecommunication, Kyiv, Ukraine, 12z@ukr.net
[3]Senior Lecturer, Department of Information Systems and Technologies, State University of Telecommunication, Kyiv, Ukraine, alinatushych@gmail.com
[4]Associate professor, Department of Information Systems and Technologies, State University of Telecommunication, Kyiv, Ukraine, isribnaya@gmail.com
[5]Head of Logistic Educational Department, Ivan Chernyakhovsky National Defense University of Ukraine, Kyiv, Ukraine, igor.vlas1969@gmail.com

## ABSTRACT

The article explores the problem of the analysis of social network parameters e.g. user strength, information transfer to other users, graph density, network building probability. There are a few approaches for determination the central users. At first, central users comply a tops of network, which have a lot of ribs, they have the biggest extent. Second point, a central top is a top, which have a minimal distance to other tops of network. As a result, a way from central users to other users is the most simple, the central users have large probability obtain information, which circulates in a network, and control distribution this information. The third measure of centrality is the distance or degree of involvement this user in routes between other users. In this case, the central user is the user, who can control the largest number of paths in the social network between individual users and between their groups. All suggested parameters as well as the likelihood of social network construction are substantiated by modeling.

**Key words :** graph, parameter, probability, social network.

## 1. INTRODUCTION

Last decades modern social networks have significantly changed with rapid spread of social online services and the development of Big Data technology. Such approaches have sparked an interest to the use of information from social networks in various fields. The sharing of structural and thematic data potentially allows to use a social networks for address a wide range of information and data protection problems [1].

Graphs can be used to illustrate good and bad relationships between people [2]. Edges with positive weight between two nodes indicate a positive relationship (friendship, kinship, relationships), and edges of negative weight between two nodes indicate a negative relationship [4] (hatred, anger). Marked graphs of social networks can be used for prediction of the graph development in the future [3]. Some social networks can use the concepts of "balanced" and "unbalanced" cycles [5]. Underbalanced cycle means a cycle in which the result for all labels is positive. Balanced graphs represent a group of people whose members do not want to change their opinion of other group members [6]. Unbalanced graphs represent a group of people whose members can easily change their opinion about other group members [9].

V. Akhramovich [1] and Leucio Antonio Cutillo [13] discuss network settings for the protection of personal data. D. Gubanov, D. Novikov, A. Chhartishvili [2], A. Zuev, D. Fedyanin [4] consider the parameters of influence, counteraction between users in networks. V. Davydenko, G. Romashkina, S. Chukanov, L. Maslyuk [3] consider network parameters in a general way without resorting to detailed analysis. L. Levkovich-Maslyuk [5], K. Slavnov [8], M. Yudina [9], L. Freeman [10], U. Kang, S. Papadimitriou, J. Sun, H. Tong consider centralities in Large Networks [11]: analyze, network parameters, including node centrality, graph density. Leucio Antonio Cutillo, Re-k Molva, and Thorsten Strufe [12] analyze the network performance of the complex without indicating the impact of each characteristics.

Some approaches for building secure social networks can be taken from technical networks. So, Dr. Sasi Bhanu *et al*. [14] consider combinatorial techniques based on neural networks model. Janus Jade A. Basa *et al*. [15] analyze wireless sensor network for smart inventory management system**.** Sri

Lakshmi *et al*. [16] analyze of defense techniques for various network topologies. Such approaches are useful for understanding the issues of information flow but very simplified for processes and understanding social network behavior.

The purpose of the article is to investigate the parameters of social networks for their further use in information and data protection.

## 2. MAIN PART

### 2.1. User power

There are a few approaches for determination the central users. At first, central users comply a tops of network, which have a lot of ribs, they have the biggest extent [7]. Second point, a central top is a top, which have a minimal distance to other tops of network [8]. As a result, a way from central users to other users is the most simple, the central users have large probability obtain information, which circulates in a network [10], and control distribution this information [9]. The third measure of centrality is the distance or degree of involvement this user in routes between other users [12]. In this case, the central user is the user, who can control the largest number of paths in the social network between individual users and between their groups. The power of the user is determined from the formula: $GPI=1^{n-1}p$ (Figure. 1):

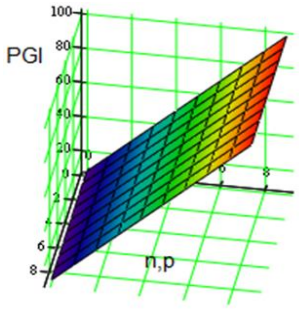


**Figure 1,a**: The user's power k=(1, 0.1, 2) p=(10, 10, 100)

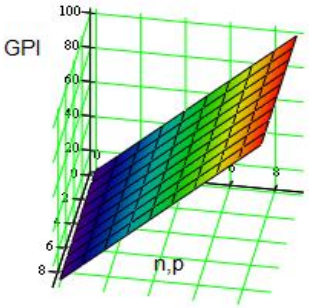


**Figure 1,b**: The user's power k=(1, 2, 10) p=(10, 10, 100)

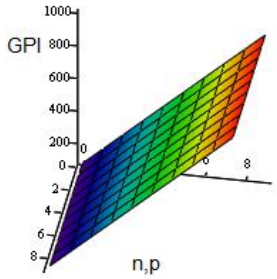


**Figure 1,c**: The user's power k=(1, 2, 10) p=(100, 100 1000)

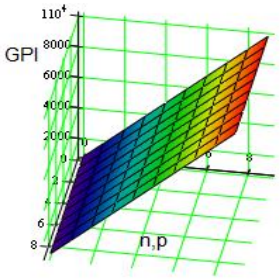


**Figure 1,d**: The user's power k=(1, 2, 10) p=(1000, 1000, 10000)

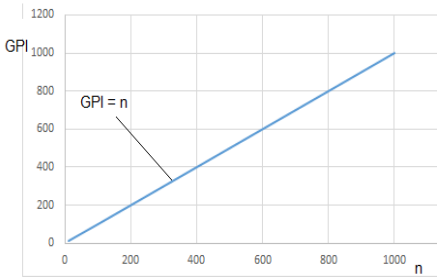


**Figure 1,e**: The user's strength depend on the number of edges

### 2.2. The transmission of information to another user

Information which is interesting for any individual depends largely on the characteristics of the latter. Moreover, individuals with similar characteristics tend to communicate with each other [11]. Imagine an epidemic model with a probability of transmission of certain information as a function of distance between source and potential target. Next, we will show that this epidemic model has no borders network, but has a limiting threshold, which means the spread of information is limited [6].

The probability that the neighbor m will give this information to the person, who is in contact with him, is defined as: $y=t(r+1)–f$ (Figure 2).

In Figure 2: $f>0$, r is the number of users which may share the user information, t – the network user is located on a particular node.

When the primary node $t(0) = t$ and at large distances of the environment t goes to zero.

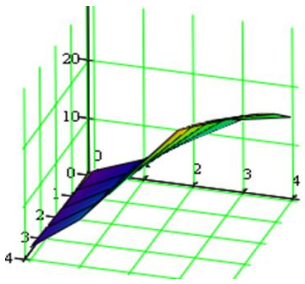

**Figure 2,a**: The reliability of the communication of information to other users f=0,6, r=(1, 2, 5), t=(1, 3, 10)

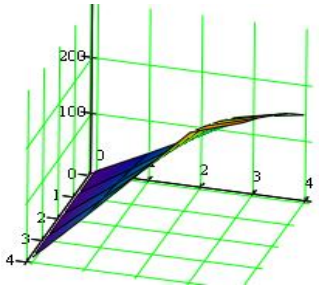

**Figure 2,b:** The reliability of the communication of information to other users f=0,6, r=(1, 2, 5), t=(10, 30, 100)

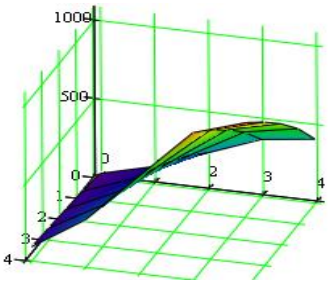


**Figure 2,c**: The reliability of the communication of information to other users f=0,6, r= (10, 20, 50), t=(10, 30, 100)

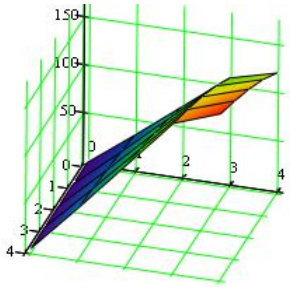


**Figure 2,d:** The reliability of the communication of information to other users f=0,3, r= (10, 20, 50), t=(10, 30, 100)

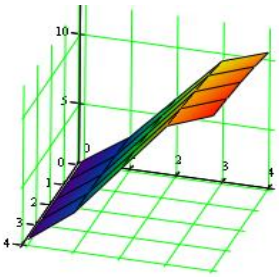


**Figure 2,e**: The reliability of the communication of information to other users f=0,1, r= (10, 20, 50), t=(1, 3, 10)

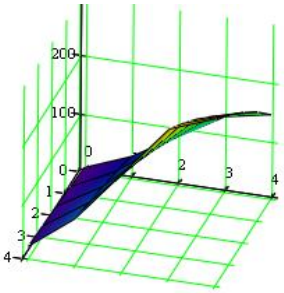


**Figure 2,f:** The reliability of the communication of information to other users f=0,6, r= (1, 2, 5), t=(1, 6, 20)

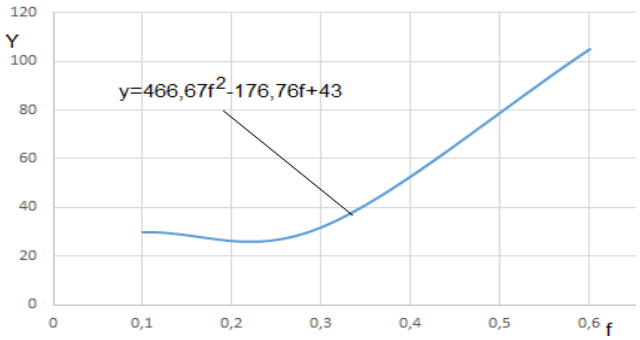


**Figure 2,g**: dependence of information transfer on degree f, while r= (1, 2 5), t=(10, 30, 100)

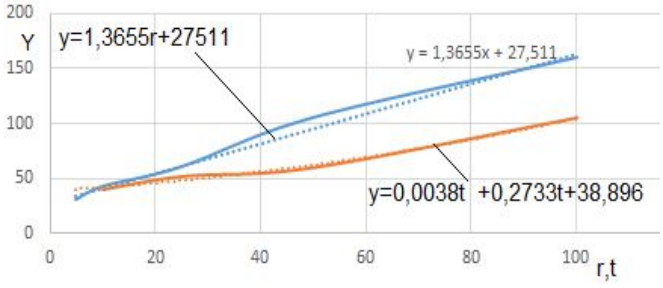


**Figure 2,h:** dependence of information transfer on degree f=0,6

### 2.3. The density of the graph

Density is the ratio of the number of available edges of this graph to the maximum number of edges of this graph. Density is a common metric and it is used primarily when comparing graphs of the same size, or when comparing a graph with itself over time. It is calculated by the formula: m (n,p) = n existing bonds / n maximum possible m (n, p) = 2 * p * n / (n * (n-1)) - where p * n is a number of connections, p is the probability of connections, and n is the number of vertices in the graph (Figure 3).

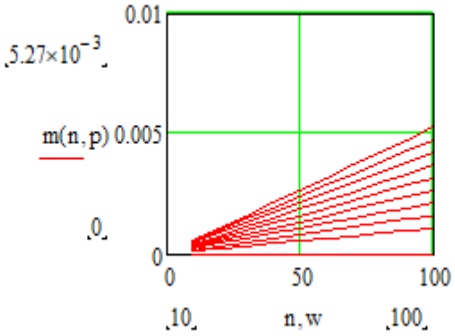


**Figure 3,a:** The density of graph p = (0, 0.1, 1), n = (10, 10, 100)

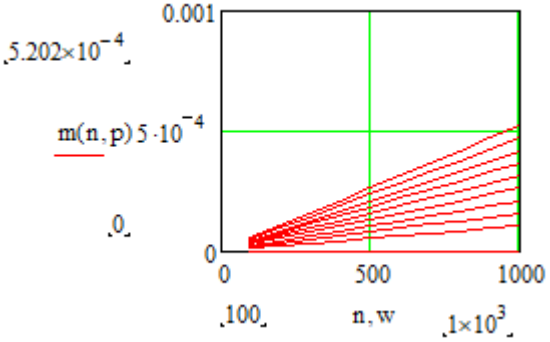


**Figure 3,b:** The density of graph p = (0, 0.1, 1), n = (100, 100, 1000)

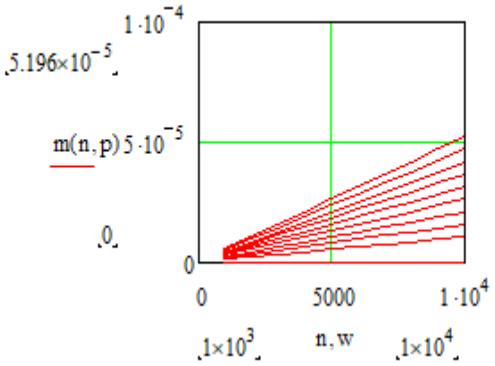


**Figure 3,c:** The density of graph p = (0, 0.1, 1), n = (1000, 1000, 10000)

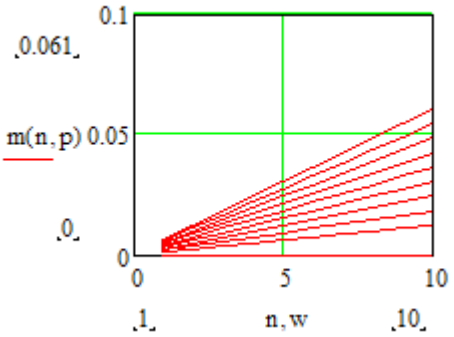


**Figure 3,d:** The density of graph p = (0, 0.1, 1), n = (1, 2, 10)

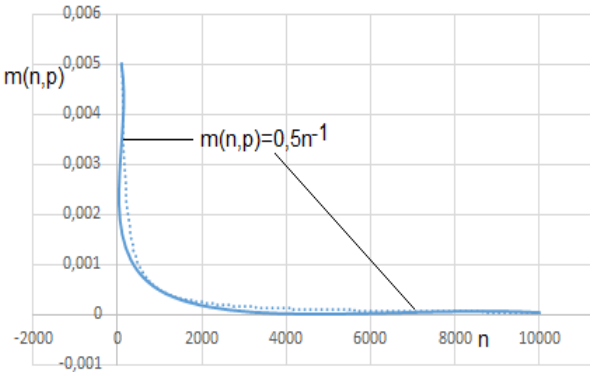


**Figure 3,e:** The dependence of the density of the graph on the number of vertices at p = 1.

### 2.4. The probability of constructing spherical surfaces with depth h

Based on the probability of constructing a single circuit, because of m mirrors can only be reliable node contacts, f users should be online, the probability of constructing spherical surfaces with depth h is calculated as:

$$P_{mart} = \sum_{i=1}^{\vec{f}} \left( \frac{\vec{f}}{i} \right) p^i (1-p)^{\vec{f}-1} \left[ \sum_{i=m}^{\vec{f}-1} \left( \frac{\vec{f}-1}{j} \right) p^j (1-p)^{\vec{f}-j-1} \right]^{h-1}$$

In this equation, we assume that the friends of each node are selected independently. However, there is a chance to choose a friend who is already involved in spherical surfaces. Therefore, building Pmart, we introduce a new parameter $(f_i)^{\rightarrow}$ which corresponds to the average of friends of one node in shells one. Then we have:

$$P_{mart} = \sum_{i=1}^{\vec{f}} \left( \frac{\vec{f}}{i} \right) p^i (1-p)^{\vec{f}-1} \prod_{i=1}^{h-1} \left[ \sum_{i=m}^{\vec{f}} \left( \frac{\vec{f}}{i} \right) p^j (1-p)^{\vec{f}-j} \right].$$

So, Pmart depends on p, h, and $m(f_i)^{\rightarrow}$. Assessment $(f_i)^{\rightarrow}$ is not trivial; however, we distinguish between the best and worst result, taking into account the ratio of overlapping between friend lists. In the best case, no overlap of friends lists, we have $(f_i)^{\rightarrow} = f-1$, and in the worst case with full overlapping between friend lists $(f_i)^{\rightarrow} = f-ml$. The probability Pmart is evaluated through some experiments, when the probability of the Internet is set to p = 0,53 (based on data from Skype). The number of friends is estimated as f = 130, illustrating the best case, when the friends lists have no overlap, Pmart does not depend on h, so the equation can be simplified to:

$$P_{mart} = \sum_{i=1}^{\vec{f}} \left( \frac{\vec{f}}{i} \right) p^i (1-p)^{\vec{f}-i}.$$

On the contrary, in the worst case, h plays a significant role. Thus, the influence of the overlap between the lists of friends has a large effect on performance (Figure 4).

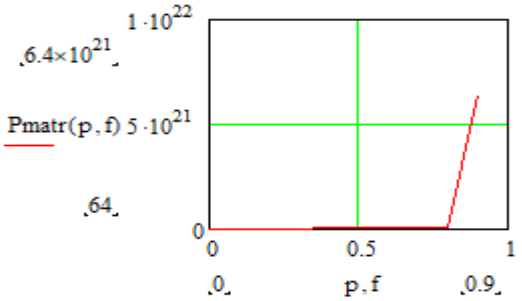


**Figure 4,a:** The probability of constructing spherical surfaces
f = 1, p = (0, 0.1, 1), h = 5

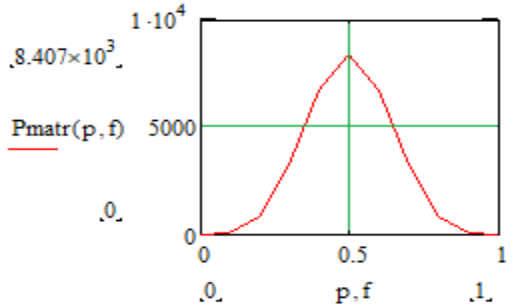


**Figure 4,b:** The probability of constructing spherical surfaces
f = 5, p = (0, 0.1, 1), h = 5

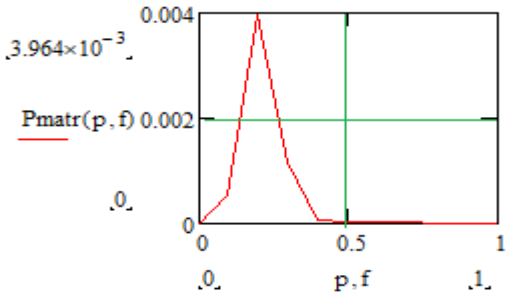


**Figure 4,c:** The probability of constructing spherical surfaces

f = 10, p = (0, 0.1, 1), h = 5

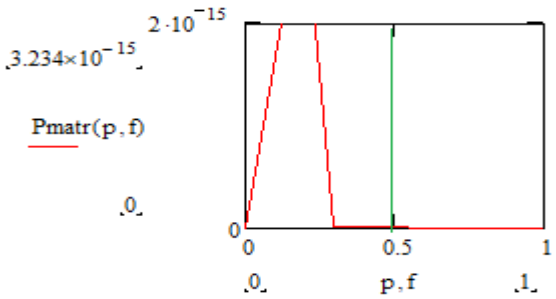


**Figure 4,d:** The probability of constructing spherical surfaces
f = 20, p = (0, 0.1, 1), h = 5

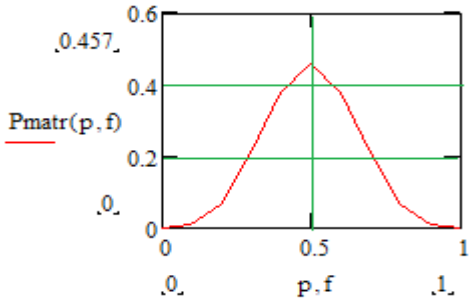


**Figure 4,e:** The probability of constructing spherical surfaces
f = 5, p = (0, 0.1, 1), h = 0

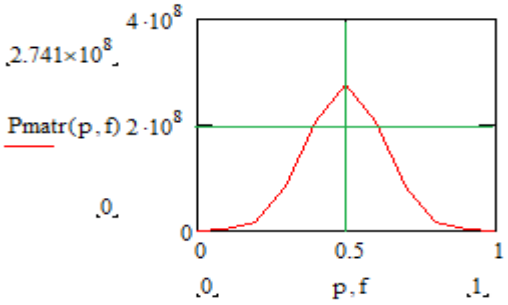


**Figure 4,f:** The probability of constructing spherical surfaces
f = 5, p = (0, 0.1, 1), h = 10

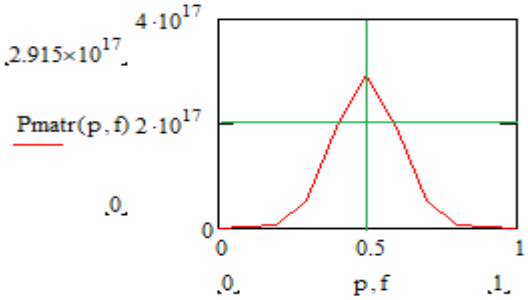


**Figure 4,g:** The probability of constructing spherical surfaces
f = 5, p = (0, 0.1, 1), h = 20

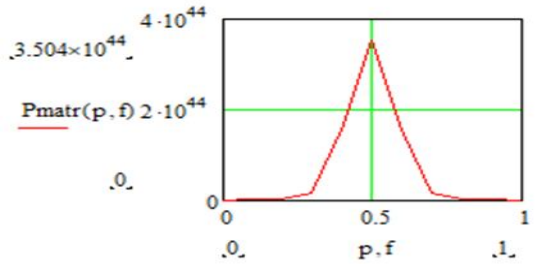


**Figure 4,h:** The probability of constructing spherical surfaces
f = 5, p = (0, 0.1, 1), h = 50

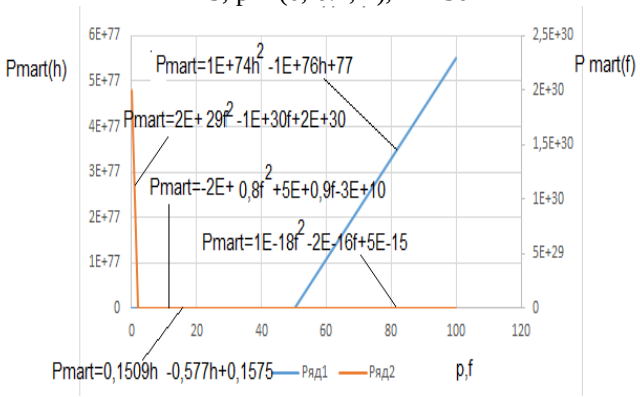


**Figure 4,i:** The dependence of the probability of construction of spherical surfaces on the number of mirrors and the depth of construction p = 1.

## 3. CONCLUSION

All social network parameters explored directly or indirectly affect the security of user information and personal data. For example, the lower the strength of the user and its interaction with other users, the reliability of the information transmission, the greater the positive or negative impact it can have on other users and as a consequence on network security. The density of the network graph affects the productivity and speed of interaction. So, the field of the future research has to cover different aspects of Social Networks modeling with respect to dependence of security parameters from total network parameters.

## 4. REFERENCES

1. Akhramovych V.M., Chegrenets V.M. **Research of the scientific and methodological apparatus of personal data protection on social networks.** *Sciences of Europe*, Praha, Czech Republic.2019 / VOL 1, No 46 (2019). Ex. 36-39. http://www.european-science.org.
2. D.A. Gubanov, D.A. Novikov, A.G. Chhartishvili. **Social networks: models of information influence, management and confrontation**. Moscow: Publishing

House of Physical and Mathematical Literature, 2010. - 228 p.

3. V.A. Davydenko, G.F. Romashkina, S.N. Chukanov. **Social networking modeling. Report towards the grant "Sociological and mathematical modeling of social networks"** - *Bulletin of the Tomsk State University* - http://www.tmnlib.ru/resources/books/pdf/Romashkina_3.pdf.
4. Zuev A.S., Fedyanin D.N. **Models of managing the agents' opinions on social networks.** *Electronic scientific journal: management of economic systems*, 2011. 37 p.
5. Levkovich-Maslyuk L. **Mathematics of these networks - Computer** No. 35 dated September 28, 2005. - http://www.kinnet.ru/cterra/607/230222.html.
6. Parinov A.V. **Analysis and regulation of content distribution processes on social networks digg, slashdot, bibsonomy.** A.V. Parinov, E.I. Kulakov, V.V. Kolmakov, A.V. Ocheret, E.S. Sokolova, R. Babakanov, Ostapenko A.A., Tikhonova S.S. *Information and security*. 2017. Vol. No. 2 (4). P. 273-284.
7. Razgonyaev A.N. **Social twitter network: structural and functional analysis of content distribution processes.** A.N. Razgonyaev, E.S. Sokolova, S. Kulikov, D.N. Rakhmanin, and Yu. Stefanovich. *Information and Security*. 2017. T. 20. № 4 (4). P. 508-515.
8. Slavnov K. A. **Analysis of social graphs.** 2015. http://www.machinelearning.ru/wiki/images/6/60/2015_417_SlavnovKA.pdf .
9. M.N. Yudina, **Nodes of social networks: measures of centrality and role in network processes**. Omsk Scientific Bulletin, 2016, 161 p.
10. Freeman L.C. **Centrality in social networks: Conceptual clarification**. *Social Networks*. 1978. №1. P. 215-239. https://doi.org/10.1016/0378-8733(78)90021-7
11. Kang U., Papadimitriou S., Sun J., Tong H. **Centralities in Large Networks: Algorithms and Observations** // *Proceedings of the 2011 SIAM International Conference on Data Mining*. 2011. P. 119-130. https://doi.org/10.1137/1.9781611972818.11
12. Leucio Antonio Cutillo, Re-k Molva, and Melek Önen. **Analysis of privacy in online social networks from the graph theory perspective.** *In GLOBECOM 2011, Selected Areas in Communications Symposium*, Social Networks Track, Houston, Texas, USA, December 2011.
13. Leucio Antonio Cutillo, Re-k Molva, and Thorsten Strufe. **Safebook: a privacy preserving online social network leveraging on real-life trust**. *IEEE Communications Magazine, Consumer Communications and Networking Series*, 47(12), December 2009.International Conference on Wireless On-demand Network Systems and Services, Snowbird, Utah, USA, February 2009. https://doi.org/10.1109/MCOM.2009.5350374
14. Dr. Sasi Bhanu et al. **Generating Test cases for Testing Embedded Systems using Combinatorial Techniques and Neural Networks based Learning Model.** *International Journal of Emerging Trends in Engineering Research*. Volume 7, No. 11 November 2019. p. 417-429. https://doi.org/10.30534/ijeter/2019/047112019
15. Janus Jade A. Basa et al. **Smart Inventory Management System for Photovoltaic-Powered Freezer Using Wireless Sensor Network.** *International Journal of Emerging Trends in Engineering Research*. Volume 7, No. 10 October 2019. p. 393-397. https://doi.org/10.30534/ijeter/2019/057102019
16. N. V. V. N. J. Sri Lakshmi et al. **Study and Analysis of Defense Techniques for Various Network Topologies.** *International Journal of Emerging Trends in Engineering Research*. Volume 7, No. 11 November 2019. p. 481-496. https://doi.org/10.30534/ijeter/2019/137112019