The Model of Secure Social Networks Activity Based on Graph Theory

Pavlo Shchypanskyi, Vitalii Savchenko, Volodymyr Akhramovych, Tetiana Muzshanova, Svitlana Lehominova, Volodymyr Chegrenets

***Abstract:** The article deals with social networks parameters that describe individuals within network. The basic idea is based on an assumption that individuals with common characteristics are likely to communicate with each other. This is a kind of epidemical model with the chance of sending some information, as a functions of distance between source and potential destination. The main approach in the article is based on clustering of local characteristics of network. They characterize degree of interaction between the closest neighbors of current graph node. For the most networks if a node A is connected to node B and node B – to node C, then, there is a big chance of the fact, that node A is connected to node C (friends of our friends are also our friends). Depending on the graph structure, between two nodes there are often a few different paths. Distribution of nodes degree is a distribution with "long tail" and is modelled with degree distribution. It means, that in such networks, there are a lot of nodes, that has 1-3 neighbors, but a little of nodes, which has thousands of neighbors. A modelling of parameters (possible quantity of graph edges, clustering coefficient, connection of new node, shortest and average path, residual lifetime of chain, node interactions, average degree of node etc.) of social networks is taken. Calculations are illustrated with graphical materials. Relevant equations are represented.*

***Keywords:** social network, graph, node interaction, information security, modelling.*

Revised Manuscript Received on February 28, 2020.
***** Correspondence Author

Pavlo Shchypanskyi, PhD, Professor, Deputy Head of Ivan Cherniakhovskyi National Defense University of Ukraine, Kyiv, Ukraine. Email: info@nuou.org.ua

Vitalii Savchenko*, Doctor of Technical Science, Professor, Director of the Institute of Information Protection, State University of Telecommunications, Kyiv, Ukraine. Email: savitan@ukr.net +38067-5046012

Volodymyr Akhramovych*, PhD, Associated Professor, Institute of Information Protection, State University of Telecommunications, Kyiv, Ukraine. Email: 12z@ukr.net

Tetiana Muzhanova, PhD in Public Administration, Associated Professor, Institute of Information Protection, State University of Telecommunications, Kyiv, Ukraine. Email: muzanovat@gmail.com

Svitlana Lehominova, Doctor of Economics, Associated Professor, Institute of Information Protection, State University of Telecommunications, Kyiv, Ukraine. Email: chiarasvitlana77@gmail.com

Volodymyr Chegrenets, PhD, Associated Professor, Institute of Information Protection, State University of Telecommunications, Kyiv, Ukraine. Email: vovkacheg@ukr.net

I. INTRODUCTION

It's known that in the base of functioning of all social networks (SN) is a phenomenon of social network communication. Users of SN create a system of nodes, that are connected between themselves with data transfer channels.

As users are able to establish connections with other users or virtual communities, we can state about distributed character of connections between nodes.

Nowadays social networks in the Internet has a huge amount of threats to security and privacy [1], which can lead to irreversible loss of confidential data, and so, to the loss of money and reputation.

In the work [1] V. Akhramovych consider the methods of protection in Internet-social networks. In [2] V. Akhramovych M. and V. Chegrenec explore privacy data protection in social networks. N. Gusarova [3] consider questions, that are connected to base terms in analysis of social network, such as complex networks, static distribution laws, random graphs, small world and other.

In [16] Y. Zhongmei et al. consider a modeling of heterogeneous changes of users and local stability of unstructured networks P2P. D. Sade [14] reveals centrality of N-path in networks. B. Markovsky et al. [11] highlight energy relation in networks. Works of N. Friedkin [8], P. Bonacich [4], M. Newman [12], L. Freeman [7] and S. Borgatti [6] are dedicated to the theory of centrality in social network. In [10] C. Hubbell and P. Bonacich in [5] are considering the theory of clicks. M. Newman [13] considers a general theory of networks. T. Hoivik and N. Gleditsch P. [9] explore structure parameters of graph. Despite all the existing work, now there is no single model of activity in social networks in terms of information security.

The purpose of the article is creating the Model of social networks activity based on Graph Theory for further use in information and privacy data security.

II. THE MAIN PART

A. Calculation of possible quantity of social network edges

Graph edge – is a term in graph theory, a line, that connects a couple of adjacent vertices of graph. Oriented edge of graph, is one, for which one vertex is considered as beginning, other – as end, is called an arc. Fig. 1 represents a full graph [9].

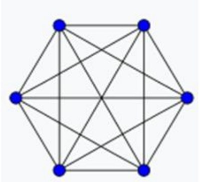

Fig. 1 Full graph example

Using formula of sum of degrees for graph G = (V,E) ∑(v∈V), deg(v)=2|E|, so sum of degrees of vertices of any graph equals doubled number of its edges [12].

In addition, from formula, it's clear that in any graph has a pair number of vertices of odd degrees. Given statement is known as lemma about handshake. A name comes from known mathematical problem: we need to prove that in any group, number of people handshake an odd number of others.

In this model, there are two parameters – *n* (number of nodes) and *p* – chance of the fact, that any randomly chosen couple of nodes is connected with edge. If p = 0, then there are no edges in graph, and if p = 1, we receive a full graph, all nodes are connected with edges. Then, number of edges - is a random number, that has mathematical chance (5). Number of edges.

$$\langle m\rangle = p\cdot\frac{n(n-1)}{2} \qquad (1)$$

where *m* – quantity of edge.

Graphical interpretation of dependency (1) is represented in Fig. 2 (modelling is performed in MathCad 13 environment). On picture there are accepted notation, for example, in parentheses (0, 0.1, 1) means, that parameter vary from minimum value, in current case, from 0 to maximum value, in current – to 1, with step 0.1.

B. Calculation of clustering coefficient

Clustering is a local characteristic of network [3]. It characterizes degree of interaction between the closest neighbors of current graph node. In most networks, if a node A is connected to node B, and node B – to node C, then, there is a big chance of the fact, that node A is connected to node C (friends of our friends are also our friends) [14]. Coefficient of clustering of current node is a chance of two closest neighbors of current node are themselves closest neighbors [15]. Coefficient C responds to a relation of real number of connections between its neighbors and their potentially possible number. Coefficient of clustering may be averaged to any part of network, or to network in general, becoming its integral characteristic: $C=\frac{1}{n}\sum_{i=1}^{n}C_i$.

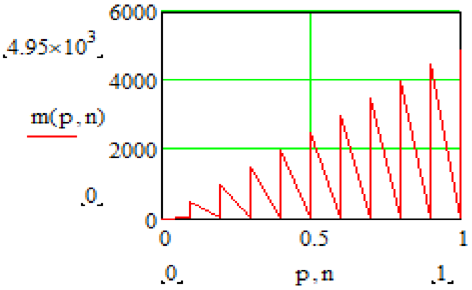

Fig. 2,a Number of graph edges: p = (0, 0.1, 1), n = (10, 20, 100)

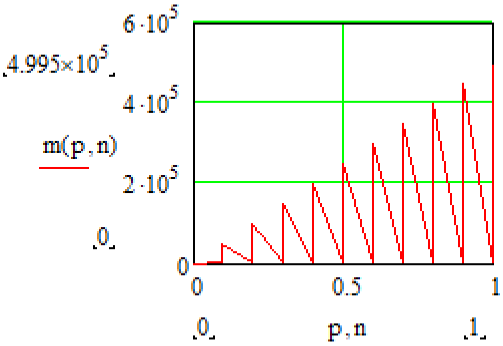

Fig. 2,b Number of graph edges: p = (0, 0.1, 1), n = (100, 200, 1000)

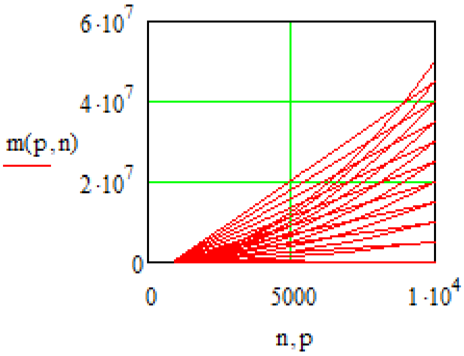

Fig. 2,c Number of graph edges: p = (0, 0.1, 1), n = (1000, 2000, 10000)

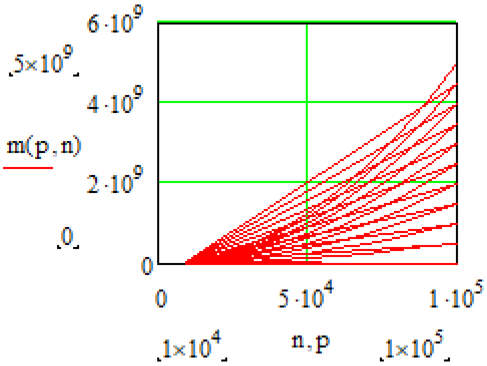

Fig. 2,d Number of graph edges: p = (0, 0.1, 1), n = (10000, 20000, 100000)

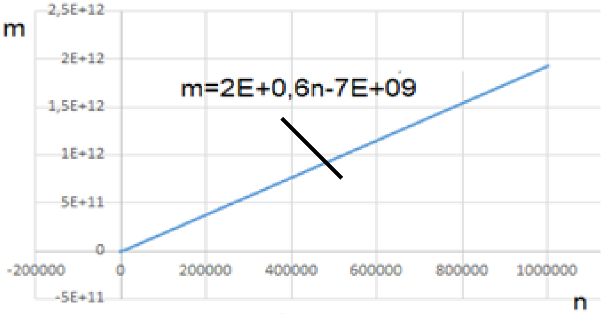

Fig. 2,e Number of graph edges dependence of quantity of full graph edges from quantity of nodes

Coefficient of clustering– is a metric, that is more effective than its density, and it's used more and more often in social sciences [6]. Coefficient of clustering– is a degree, that defines how many nodes are willing to clustering [16]. For example, in the network of friends it's chance of two of my friends are friends between themselves. So, this is some assessment of network fragmentation. With high clustering, you can expect, that virus will be shared only in some subgroup (cluster) [9]. With low clustering there is a high chance of fast spreading of virus within whole network.

Local coefficient of clustering. Local clustering coefficient (clustering coefficient) is a measure of how well the neighbors of this node are interconnected. Local clustering coefficient is calculated as number of connections between neighbors of current node / possible number of connections between neighbors.

In indirect graph, the clustering coefficient c(v) of node v with deg(v) edges is determined as quantity of existing connections between those nodes, marked as, $e_{deg(v)}$ divided on quantity of all possible links, which provided

$$\frac{e_{deg(v)}\left(e_{deg(u)}\right)^{-1}}{2} \qquad (2).$$

That's why we have:

$$C(v)=\frac{2e_{deg(v)}}{e_{deg(v)}\left(e_{deg(u)}\right)^{-1}} \qquad (3)$$

Clustering coefficient of general graph, marked as C (G), is defined as average clustering coefficient of all nodes of graph, so:

$$C(G)=\frac{\sum_{v\in V} c(v)}{\|V\|}. \qquad (4)$$

Calculation or evaluation of clustering coefficient (Fig. 3,4) may give a representation about influence of dissemination of unauthorized information by malicious users on friendship with nodes [5].

After, malicious node η is added to contact list v, η can get an access to sensitive data of v, and disclose them without filtration, using social network resources, such as creating a post, publication of pictures and so on. In particular, if η user, that is using professional trust, all sensitive data, that v share with η, will be disclosed [10]. Such influence can be measured by calculating the average relation of Q_v of friends v, that can get confidential information, that is disclosed by malicious η, so:

$$Q_v = p_v c(v). \qquad (5).$$

From this equation we can say that degree of distribution is proportional to clustering coefficient. The bigger number of friends – the wider distribution of confidential data to user contacts [12].

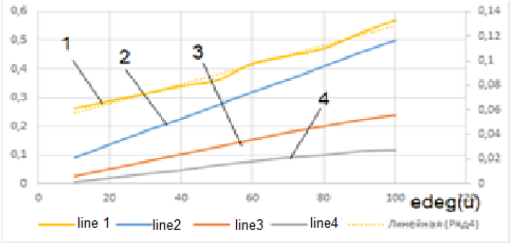

Fig. 3 Clustering coefficient:

line 1 – while e $\deg(v)$ =(1, 1, 2), scale ordinates on the left, equation (G)=0,0034 edeg(u) +0,2132;
line 2 while e $\deg(v)$ =(1, 1.5, 5) ordinate scale on the right, equation C(G)=0,0011 edeg(u)+0,0106;
line 3 while e $\deg(v)$ =(1, 2, 10) ordinate scale on the right, equation C(G)=0,0006 edeg(u)+0,012;
line 4 while e $\deg(v)$ =(1, 2, 20) ordinate scale on the right, equation C(G)=0,0003 edeg(u)-0,0006.

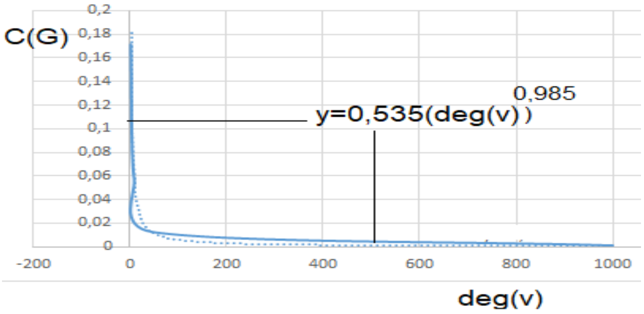

Fig. 4 Dependence of clustering coefficient from deg(v) while e_deg = (1, 100, 1000)

C. Calculating of possible accession of new node

In the model of Mediation driven attachment (MDA) new node comes with *m* edges, for what, an existing linked node is chosen randomly and new node connects not only with this randomly chosen node, and also with *m* of his neighbors, that are also chosen randomly [13].

Let $U_i \subset$ G – is a community of nodes and let CS (t) = U_i where U_i – is a totality of all existing communities (CS, communities) at the moment of time t with $U_i \cap U_j = \emptyset$ for $i \neq j$. On the beginning (t = t_0) graph consists of one community $U_0 = CS(t_0)$. If to graph in moment t + 1 will be added a new node *u*, *u* will add a chance P(X ≥ N) to existing community $U_i \subseteq$ CS (t). With chance P (X <N), u creates new community U_i + 1 and becomes a new member of it. We have CS(t+1) = $CS(t)UU(i+1)$ – parameter of model configuration, and value *N* responds to the chance of forming a new community. The smaller the choice N, the smaller communities exist. Chance of new node creates a new community U_i + 1 and connects with existing node $v \in U_i$, is calculated with equation (6).

$$P_{U_i+1}\left(deg(v)X\right)=P\left(deg(v)\right)P\left(X<N\right), \qquad (6)$$

where deg(v) – number of edges that come to vertex v.

Chance of new node u joins the existing community U$_i$(CS(t) and connects with existing node $v \in U_i$, is calculated with equation

$$P_{U_i}\left(deg\left(v\right)X\right) = P\left(deg\left(v\right)\right)P\left(X \geq N\right). \quad (7)$$

In that way, preferential access is connected with a condition for joining a specific community [11]. Forming a new connection. Let's say, that we have community of nodes and let CS(t) = i U_i – a totality of all existing communities in the moment of time t with $U_i \cap U_j = \emptyset$ for $i \neq j$. u and v are added to graph, and it's made with chance P(X$\geq$0), for u, $v \in U_i$ and $U_i \subset$ CS (t). From chance P (X<0), $u \in U_i$ and $v \in U_j$ we've chosen from U_i, U_i (CS(t), $i \neq j$. Chance of forming one new edge (u, v) between two nodes $u \in U_i$ and $v \in U_i$ formed from common friends com (u, v), is calculated with equation

$$P_{U_{i=j}}\left(com\left(u,v\right)X\right) = P\left(com\left(u,v\right)\right)P\left(X \leq 0\right). \quad (8)$$

Chance of new edge e (u, v) creates between two nodes u ∈ Ui and v ∈ Uj for i/= j with com (u, v) common friends, is calculated using equation

$$P_{U_{i\neq j}}\left(com\left(u,v\right)X\right) = P\left(com\left(u,v\right)\right)P\left(X > 0\right). \quad (9)$$

Choice of two nodes in accordance to Newman's clusterization is connected, in such way, with condition of membership in one community. Results of modelling are represented in Fig. 5.

D. Calculating of the shortest path

Depending on the graph structure, between two nodes u and v there are often a few different paths. Path, that is taken from u to node v in minimal quantity of steps is called the shortest, or the distance [11]. To refer to the shortest path between two nodes u and v, a designation d(u, v) is used.

Average shortest path dkP(G) of graph is an average shortest distance between all possible disjointed combinations of two nodes u and v.

It is calculated with equation

$$\text{dkP}\left(G\right) = \frac{\sum\limits_{v\neq u\in V} d\left(u,v\right)}{\left|V\right|}, \quad (10)$$

where d(u,v) – sum of all distances between nodes u,v, V – an infinite nodes of u.

Results of modelling are represented in Fig. 6. Radius Rad(G) of graph G responds to the length of shortest paths between any combination between two disjointed nodes u and v. Radius is calculated with equation

$$\text{Rad}\left(G\right) = \min_{u\neq v\in V} d\left(u,v\right). \quad (11).$$

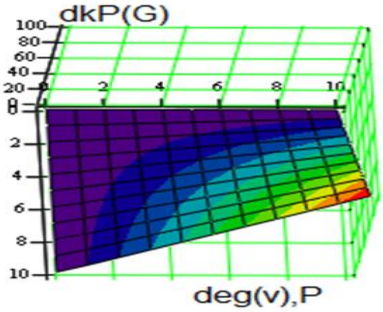

Fig. 5,a Chance of new connections to network: P (deg(v) = (0, 10, 100), P = (0, 0.1, 1)

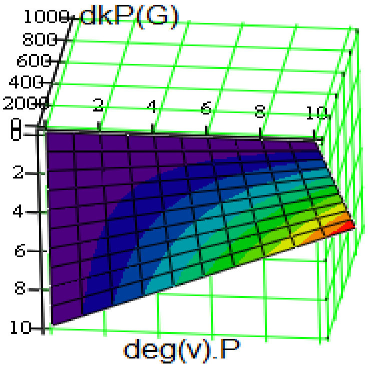

Fig. 5,b Chance of new connections to network: P (deg(v) = (0, 100, 1000), P = (0, 0.1, 1)

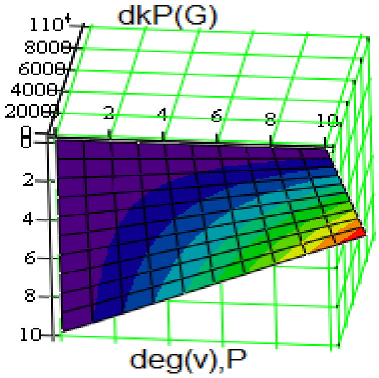

Fig. 5,c Chance of new connections to network: P (deg(v) = (0, 1000, 10000), P = (0, 0.1, 1)

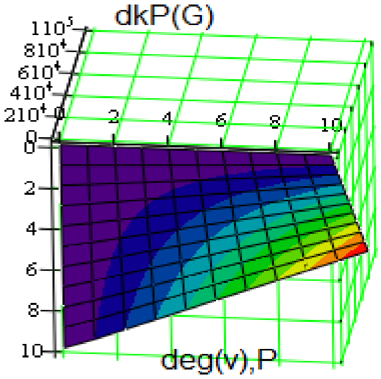

Fig. 5,d Chance of new connections to network: P (deg(v) = (0, 10000, 100000), P = (0, 0.1, 1)

According to results of modelling $\text{Rad}(G) = 1$.

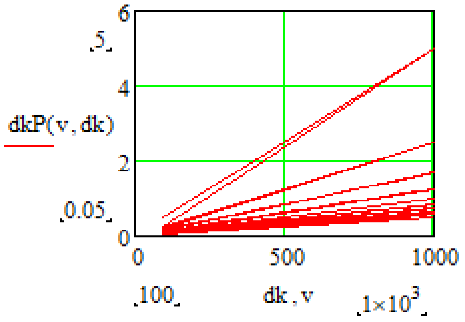

Fig. 6,a Dependency of shortest path from quantity of connections – 1000 connections.

Diameter Dia(G) of graph equals to the length of the longest of shortest paths between any combination of disjointed nodes u and v. Diameter is calculated with equation

$$\text{Dia}(G) = \max_{u \neq v \in V} d(u,v). \qquad (12)$$

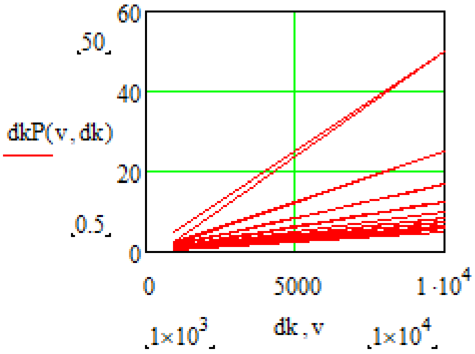

Fig. 6,b Dependency of shortest path from quantity of connections – 10000 connections.

E. Calculation of residual lifetime of chain, while which the data search is performed

Let's S_{on}, S_{off} are random variables, conducted distributions $O_{n(x)}$, $O_{ff(x)}$ in online mode and O sessions of one node accordingly, and R is a random variable from residual resource of distribution Res(x). Authors [7] where chance to achieve a lifetime t determined it with next equation

$$P_r = \frac{1}{ES}\int_0^t \left(\left(1-P_r\right)S\right)dt\,, \qquad (13)$$

where Pr [·] chance of argument p (·);
E [X] is expected value of random number X.

As all nodes in one chain are accepted simultaneously in the network, we define residual lifetime of R_{ch} chain (h-1) -hops, as minimum residual term of service R_{ni} between all h nodes, that are taking part in this chain. From here:

$$R_{ch} = \min\{R_{n1} \ldots R_{nh}\}. \qquad (14)$$

In work [6] authors made some measurements of online and repeated sessions of users work using program Skype. In Fig. 8 graphs of residual resource, that suits to (13) basing on these real number of data: as R is stochastic greater than Son, lifetime of new arrival, likely will be lower that residual lifetime of online-node. We calculate chance of online-node p, as it's determined in [7]:

$$p = \frac{E\left[S_{on}\right]}{E\left[S_{on}\right]+E\left[S_{off}\right]}. \qquad (15)$$

Basing on this equation and length h of chain we evaluate residual lifetime of chain, using simple Monte-Carlo methods on distribution Res (x). In Fig. 7 the result of modelling values of residual lifetime, while data search is running, is shown.

F. Calculation of nodes interaction

Chance P (deg (u)), that node u is chosen for initiating of interaction is calculated using equation

$$P_{(deg(u))} = \frac{deg(u)}{\sum\limits_{u \in V} deg(v)}. \qquad (16)$$

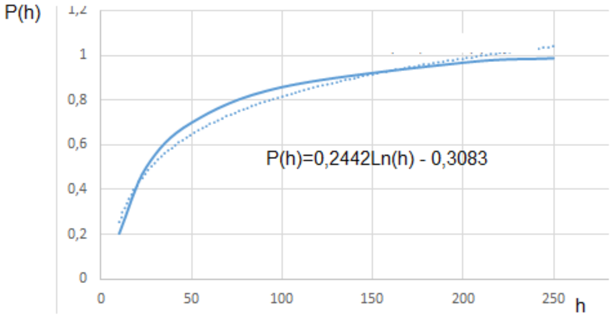

Fig. 7 Residual lifetime of chain, while search E = (0.1, 0.1 1), Pr= (0.1, 0.1 1), t=0, 200, 1000), S = (0, 10, 100)

This part of interactive module represents distribution of network interactions. Results of modelling are represented on Fig. 8, 9.

G. Calculation of average degree of node

Distribution of degree of nodes, meaning, a proportion of nodes, is a distribution with "long tail" and is modelled with degree distribution. It means, that in such networks, there are a lot of nodes, that has 1-3 neighbors, but a little of nodes, which has thousands of neighbors [4]. Example – distribution of websites in Internet [7].

Average degree of node is calculated with dependency:

$$\langle k \rangle = \frac{1}{n}\sum_i k_i = \frac{2\langle m \rangle}{n} = p(n-1) \approx pn\,. \qquad (17)$$

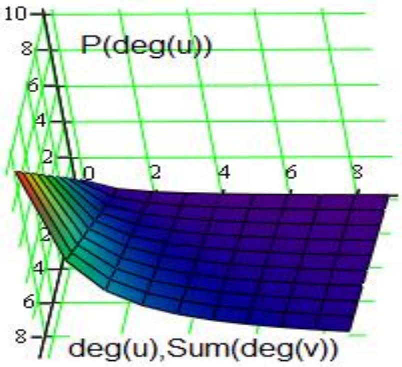

Fig. 8,a Interaction of nodes in network while deg(u) (1, 1, 10), deg(v) (1, 1, 10)

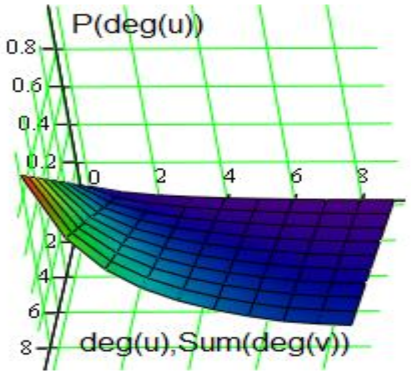

Fig. 8,b Interaction of nodes in network while deg(u) (1, 1, 10), deg(v) (5, 10, 50)

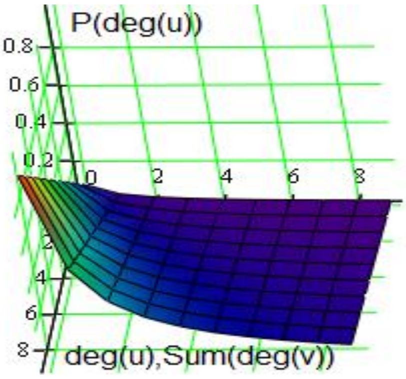

Fig. 8,c Interaction of nodes in network while deg(u) (1, 1, 10), deg(v) (10, 10, 100)

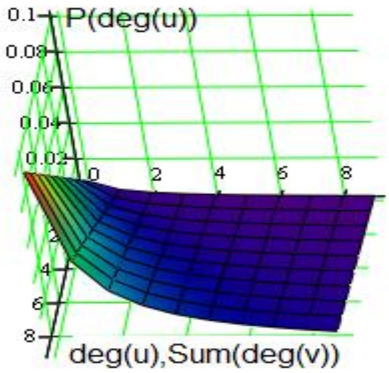

Fig. 8,e Interaction of nodes in network while deg(u) (1, 1, 10), deg(v) (100, 100, 1000)

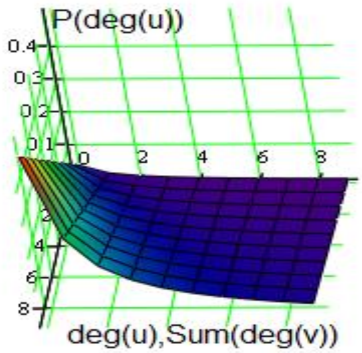

Fig. 8,d Interaction of nodes in network while deg(u) (5, 5, 50), deg(v) (100, 100, 1000)

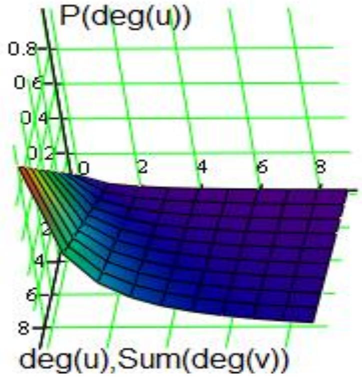

Fig. 8,f Interaction of nodes in network while deg(u) (10, 10, 100), deg(v) (100, 100, 1000)

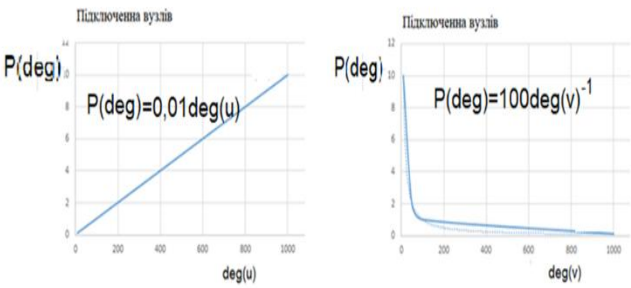

Fig. 9 Graph of equation of dependency of possible maximum connection of nodes from a) deg(u), deg(v)= (100, 100 1000), b) deg(v), deg(u), (1, 1, 10).

For random graph it's easy to calculate distribution function of degrees of nodes: it's described with Bernulli's formula:

$$P\left(k_i = k\right) = P\left(k\right) = C_{n-1}^{k} p\left(1-p\right)^{n-1-k}. \qquad (18)$$

It's known that in Bernoulli distribution there is a marginal case: if n → α, but n→∝, while fix average value k=pn=λ then, it's distribution of Poisson

$$P\left(k\right) = \frac{k^k e^{-k}}{k!} = \frac{\lambda^k e^{-\lambda}}{k!}. \qquad (19)$$

Results of modelling are represented in Fig. 10.

This distribution is discrete, meaning k has an integer value. From graph in Fig. 10,c we can see, that distribution function of degree of node from λ is close to normal distribution at large values λ and has a function with disruption (Fig. 10,b) in dependency of k change.

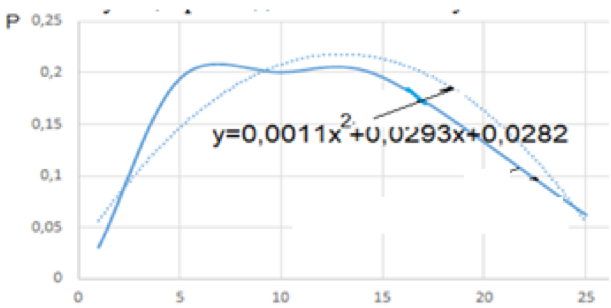

Fig.10,a Distribution function of degree of node with λ k=25

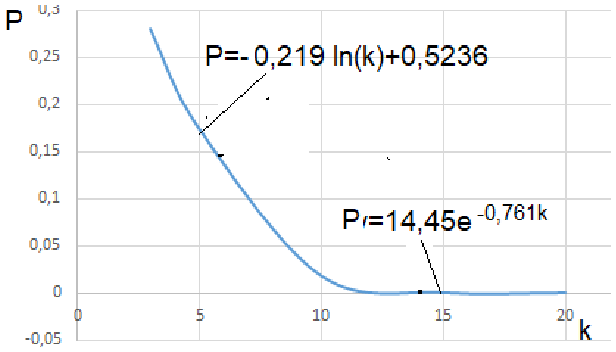

Fig.10,b Distribution function of degree of node with λ, from k λ=5, function has a disruption in point k=12

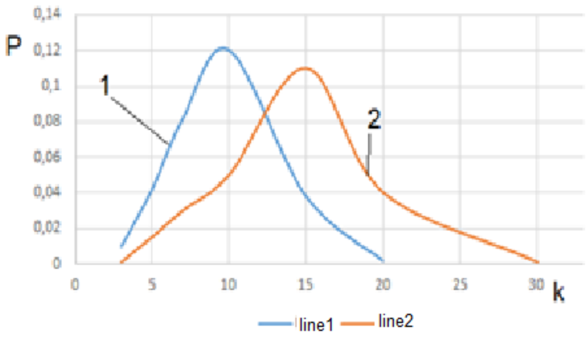

Fig.10,c Distribution function of degree of node with λ, from k curve 1 - λ=10, curve 2 - λ=15

Research function P=0,219ln(k)+0,5236 and P=14,45e$^{-0,761k}$ for continuity.

These functions are undefined in points x=12. So, function has a disruption in point x=12. To define the type of disruption, let's count single side margins in these points. Limp → -0,219ln12+0,5236 = 0,219*2,484907+0,5236 = -0,02059, limP → 14,45e$^{-0,761*12}$ = 14,45*0,000658 = 0,0095. Such point is a disruption point of first kind.

III. CONCLUSION

Continuous transformation of social and cultural reality requires understanding of modern communicative situation and producing of new relevant strategies; management tactics of communication processes, ability of community to interpret and construct communicative innovations, actively take part in its realization. Penetration of communication in all areas of community life, appearing and development of new kind of quality of communicative structures requires deep rethinking of communicative nature of social reality, that actualizes problem of network communication in modern humanitarian knowledge.

Problem of researching a role and place of social networks on communicative space of modern society is also conducted with, the fact, that networks became a global coordination center of social connections, because they can compensate not only normative vacuum, but also regulate communicative processes in social systems.

In this article we made a modelling of main parameters of social networks, that are influencing security parameters directly, or indirectly.

Summing above, we can say that analysis of social network – is a powerful and important instrument, that provides information for optimization if it's work, and also, provides security support. Complexity of processes that are flowing inside of network makes us use the special methods and analysis algorithms, which were not used earlier. Further research should be devoted to new regularities in parameters of social networks in scope of information security.

REFERENCES

1. Ahramovych V.M. Problems of playback of attacks on sensitive data and security methods in internet-social networks. *Sciences of Europe*, Praha, Czech Republic.2019/ VOL 4, No 44. P. 31-38. www.european-science.org
2. Ahramovych V.M., Chegrenec V.M. Research of science-methodical apparat of sensitive data protection in social networks. *Sciences of Europe*, Praha, Czech Republic.2019/ VOL 1, No 46(2019). Pp. 36-39. www.european-science.org
3. Gusarova N.F. Analysis of social networks. *Main terms and metrics*. Spb: University ITMO, 2016. – 67 p.
4. Bonacich P. F. Power and centrality: A family of measures. *Amer. J. Sociol*. 1987. V. 92. P. 1170-1182.
5. Bonacich P. F. Simultaneous group and individual centralities. *Soc. Networks*. 1991. V. 13. P. 155-168.
6. Borgatti S. P. Identifying sets of key players in a network. *Computational, Mathematical and Organizational Theory*. 2006. V. 12, iss. 1. P. 21-34. 34.
7. Freeman L. C., Borgatti S. P., White D.R. Centrality in valued graphs: A measure of betweenness based on networkow. *Soc. Networks.* 1991. V. 13. P. 141-154.
8. Friedkin N. E. Theoretical foundations for centrality measures. *Amer. J. Sociol.* 1991. V. 96. P. 1478-1504.
9. Hoivik T., Gleditsch N. P. Structural parameters of graphs: a theoretical investigation. In *Quantitative sociology*. N.Y.: Academic Press, 1975. P. 203-223.
10. Hubbell C. H. An input-output approach to clique identication. *Sociometry*. 1965. V. 28. P. 377-399.
11. Markovsky B., Willer D., Patton T. Power relations in exchange networks. *Amer. Sociol. Rev*. 1988. V. 53. P. 220236.
12. Newman M. E. J. Networks. An introduction. N.Y.: *Oxford University Press*, 2010.
13. Newman M. E.. A measure of betweenness centrality based on random walks *Soc. Networks*. 2005. V. 27. P. 39-54.
14. Sade D. S. Sociometrics of macaca mulatta III: N-path centrality in grooming networks *Soc. Networks*. 1989. V. 11. P. 273-292.
15. Saikat Guha, Neil Daswani, and Ravi Jain. An experimental study of the skype peerto-peer voip system. In *Proceedings of The 5th International Workshop on Peer-to-Peer Systems*, IPTPS '06, pages 16, Santa Barbara, CA, February 2006.
16. Zhongmei Yao, Derek Leonard, Xiaoming Wang, and Dmitri Loguinov. Modeling heterogeneous user churn and local resilience of unstructured p2p networks. In *Proceedings of the 14th IEEE International Conference on Network Protocols*, ICNP '06, pages 32-41, Santa Barbara, California, 2006. IEEE Computer Society.

AUTHORS PROFILE

Pavlo Shchypanskyi, Major General, PhD, Professor, Deputy Head of Ivan Cherniakhovskyi National Defense University of Ukraine, Kyiv, Ukraine.
Graduated from the Military School of Air Defense. Served in the Air Force and Air Defense of Ukraine. Has a considerable practical experience in military service. Many times participated in combat firing of air defense systems. Began to study science in 1998. Was a lecturer at the Military Academy and head of the Air and Air Defense Institute. In 2002 received Ph.D. in military sciences. The author of 80 scientific publications on military topics and has 15 patents for inventions.

Vitalii Savchenko, Doctor of Technical Science, Professor, Director of the Institute of Information Protection, State University of Telecommunications, Kyiv, Ukraine.
In 1990 graduated from the Military Aviation Engineering School and served in the Air Force of Ukraine in the meteorological service. In 2000 began to engage in science. In 2005 received a PhD in Navigation and in 2012 got a Doctors degree in Information Technology. In 2017 resigned from the Armed Forces. Retired Colonel. Field of Interest: navigation, information technology, cybersecurity. The author of 5 computer models for teaching students and the author of more than 150 scientific publications. Teaches disciplines on protecting objects from unauthorized access, searching for hidden bugs, methods of counteracting technical radio intelligence.

Volodymyr Akhramovych, PhD in Technical Science, Associated Professor, Institute of Information Protection, State University of Telecommunications, Kyiv, Ukraine.
Has been working in the field of higher education for more than thirty years. Author of over 150 scientific publications and 14 patents.

The sole author of four textbooks, co-authored with two textbooks and three workshops. Teaches the following courses: Methods of transmission in information security systems; Methods of receiving and processing signals in information security systems; Cyber security of banking and commercial structures; Theory of information resources protection with limited access; Licensing, certification and certification in the security field of information activity objects; Organization of science and research.

Tetiana Muzhanova, PhD in Public Administration, Associated Professor, Institute of Information Protection, State University of Telecommunications, Kyiv, Ukraine. Experienced scientist in social engineering and information security of the state. Has many years of work in the field of counteracting information influence on public administration processes. Is the author of social networking research and agent interaction across networks. Develops models of influence of social groups on social behavior of the individual. Has publications on the use of graphs to model social processes. Author of over 30 scientific publications. Teaches the courses: Information Security, Information Warfare, Information Security Management.

Svitlana Lehominova, Doctor of Economics, Associated Professor, Institute of Information Protection, State University of Telecommunications, Kyiv, Ukraine. Email: chiarasvitlana77@gmail.com Experienced scientist in the field of economic security of the state. The author of economic models of cybersecurity. Develops the theoretical foundations of protecting the economy in cyberspace. Has many years of work in the field of counteracting information influence on public administration processes. Is the author of social networking research and agent interaction across networks. Teaches courses: Information Security in Economics; Enterprise protection management; Social engineering in cybersecurity. Author of over 80 scientific publications.

Volodymyr Chegrenets, PhD in Technical Science, Associated Professor, Institute of Information Protection, State University of Telecommunications, Kyiv, Ukraine. Graduated from the Radio Engineering Faculty of the Air Force Military College. Served in aviation units as a radio engineer and electronics engineer. Has many years of experience in information security research. Is a developer of information security technology. Investigates the properties of electromagnetic devices in the development of information security. Determines the required parameters of information leakage control devices. Author of over 50 scientific publications. Teaches the courses: Physical security; Microelectronic elements in cybersecurity systems; Technical devices of Cybersecurity.