Human Factor as a Cause of Risks in Electronic Banking Services

Pavel V. Revenkov
Department of Information Security
Financial University under the Government
Moscow, Russian Federation
pavel.revenkov@mail.ru

Alexander A. Berdyugin
Department of Information Security
Financial University under the Government
Moscow, Russian Federation
a40546b@gmail.com

***Abstract*— Intended for stealing confidential information, social engineering is manipulation of people's actions without any technical means, playing upon biases of the human factor. In finance and banking, it causes breaches in data protection that threaten to the business continuity and security. This subject arises from the improper preparation of customers using electronic financial services that results in thefts from bank accounts. The research explores the mutual relation of actions undertaken by data generating functions. We also analyze social engineering techniques for swindling a victim, and undertaking appropriate countermeasures. We also devise methods to reinforce cybersecurity. This research involves mathematical computations and methods of a systems analysis of scientific literature on theoretical and applied researches. We also applied a pedagogical approach to studying and summarizing the existing experience. The article analyzes the cause-and-effect relations from cybercriminal–victim perspectives. We refer to particular examples of social engineering crimes and countermeasures and examine these entangled challenges. We substantiate the importance of conventional training for countering cybercrimes. We devise intellectual development methods, organizational and legal methods for countering social engineering. The article describes how the user's social engineering legitimacy correlates with information security violations.**

Keywords*— *RBS, cybersecurity, risks, human factor, commercial bank, social engineering, information protection

I. INTRODUCTION

Successful results of technological development are actively used for simplify access to savings and improve the efficiency of financial services. The most significant achievement in the banking business over the past 20 years can be called a large-scale introduction of remote banking service (RBS) technology. RBS allows customers to make banking transactions with using various telecommunications channels (network “Internet” in the case of Internet banking and cellular communication for mobile payment services) [1].

Banking experience of customers will increasingly integrate with existing technologies. Instead sign on a paper document, the client can sign with electronic pen on the tablet, use face recognition technology or compare a fingerprint for an identity card [2]. The main deterrent to the more dynamic development of RBS technology in Russia remains people's anxiety about security.

According to statistics of the Bank of Russia, nearly 6.7 billion rubles were stolen by cybercriminals from the country's financial system in 2016. (Table I[2]). For comparison: minimal amount of labour payment since July 2016 was 7500 rubles per month.

Thus, in 2016 in Russia hackers stolen $(6.86 \cdot 10^9) / (7.5 \cdot 10^3) \approx 915\,000$ of salaries. Credit and financial organizations will need serious technology to protect against computer attacks and direct physical hacking of devices. However, the protection of information is not only the prerogative of specialists, but also the task of RBS users.

Number of incidents with accounts of individuals and legal entities (for example, download malicious software onto user's computer and theft of digital money) with the use of RBS is constantly increasing and cybercrime is continuously developing. It is necessary to improve methods of protecting banking information for both the credit organizations and their clients (social engineering methods are using against clients).

TABLE I. FINANCIAL LOSSES OF RUSSIA IN 2016, BILLION RUBLES

	Stolen	**Saved**	**Total**	**Effectiveness of thefts. %**
Individuals	1.23	1.24	2.48	50
Legal entities	0.38	1.12	1.51	26
AWS of BRC[3]	1.20	1.67	2.87	42
Total:	2.82	4.04	6.86	41

II. RELATED WORK

Consider the fundamental interpretations of social engineering in manuscripts of foreign authors. Most information security researchers provides social engineering as technique that uses influence and persuasion to deceive people, manipulate them and convince them that social engineer is expert in some sphere [3, 4]. As a result the victim of social engineer unwittingly becomes source of confidential

[1] The article follows results of researches financed as part State Job of the Financial University under the Government of the Russian Federation in 2017.

[2] The Central Bank prepares banks for computer and information attacks. URL: http://www.vedomosti.ru/finance/articles/2016/12/07/668512-tsb-otrazheniyu-atak#/galleries/140737493044801/normal/1.

[3] Automated workstation of the Bank of Russia client’s.

information with or without use of technologies.

The article “Advanced social engineering attacks” [5] social engineering is describes as art of attracting users to compromise information systems. Instead of technical attacks on banking systems, social engineers receive private information through manipulation by users to disclose confidential information or commit malicious attacks to their accounts through influence and persuasion. Technical protection measures are usually ineffective against such attacks. In addition, people usually believe that they are well versed in such attacks. However, studies show that victims are ill-prepared to detect lies and deceit.

In other publications, social engineering is a technique used by intruders to access the desired information by using flaws in human logic, known as cognitive biases [6], 7]. This is the use of social masks, linguistic ruses and psychological tricks that allow computer users to help hackers in their illegal intrusion or use of computer systems and networks [8, 9].

Social engineering is one of the most powerful tools in the arsenal of hackers and malicious programmers. Because it is much easier to deceive someone that he furnishes his password for any positive result than to spend time and efforts on breaking protected information system [10, 11].

Illustration of social engineering is such example. English researchers sent letters to employees of one large corporation as if from the system administrator of their company. This letters were contained request to provide their passwords, as check of equipment is planned. 75% of the company's employees responded to this letter and reported their password in the letter [12].

This example shows an employee's inattentive can cause serious insider incident when bank secrecy is at stake. Information leakage can not only seriously affect, but even destroy the business of the credit institution, without exaggeration. Thus, in a number of cases, careless employee can be called an accomplice of computer criminal.

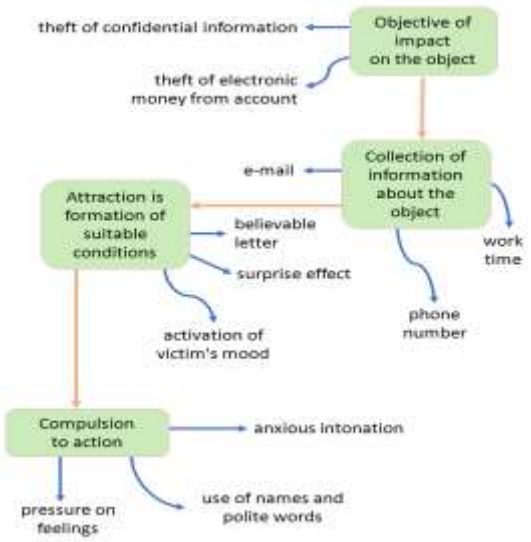

Fig. 1. Social engineering: impact on victims. Compiled by authors

III. Problem Formulation

The core of technologies is information. The most vulnerable link in the automated banking system is a people. He has flaws and the imagination of fraudster, who specializing in the search for weaknesses of the human factor, is unlimited [13]. But all fraudulent scenarios are subject to the same scheme (see Fig. 1). Information security is of great importance in optimizing technology and dissemination of Internet services. Computer crime increases information risks and stimulates development of information security. But ensuring security of information is not only prerogative of specialists, but also the task of users [14]. Sites of social networks represent a space where users unconcerned communicate with friends and relatives. Such media resources cybercriminals use for their own purposes to steal personal data. To carry out fraud, not only technological, but also psychological methods are used [15, 16]. Suppose a person places photos of luxurious interior or purchased car on his personal web-page. Then he tells the so-called “friends” and “followers” that in a week he will go on vacation. True friends equate this frankness with information noise. Attackers gather information sufficient to create forged documents. After that, the robber disruptions the security of the target apartment and/or, with credit card information, to take a large loan in the name of the victim [17].

It is worth emphasizing that the definition of cybersecurity goes beyond traditional information security and includes protection not only of information resources, but also of other assets, including the life of the person. The human factor aspect has ethical implications for society as a whole, since protection and attack on certain vulnerable groups (for example, children and pensioners) represents social responsibility [18]. Here we have in mind digital vandalism, cyber espionage, extortion (through the encryption of the contents of the hard disk) and propaganda (obsessive mailing of knowingly false representations). Thus, to the peculiarities of crimes in the information sphere with using human factor’s errors one can attribute high latency of cybercrimes (from Latin “latentis” is hidden, invisible) and, as a consequence of that, impunity of cybercriminals [7]. Also insufficient awareness by state authorities at the federal and especially regional levels of possible political, economic, moral and legal consequences of computer crimes also is peculiarity of crimes.

In this way, it is recommended to strengthen measures of administrative and criminal prosecution for computer crimes where the human factor and social engineering methods are used to obtain confidential information.

IV. Vigilance and Protection

For implementation of many computer crimes, social engineering techniques are actively used. Scammers are increasingly attracted by bank accounts with remote access, opened in credit organizations of Russia. Dynamics of accounts is shown in statistics of the Bank of Russia[4] (Table II).

There is a tendency to increase of the total number of open accounts from 27722.6 thousand in January 2008 to 172529.0 thousand in July 2017. Increase of 6.2 times in 9.5 years.

[4] Number of remote access accounts opened with credit organizations. https://www.cbr.ru/statistics/p_sys/print.aspx?file=sheet009.htm&pid=psrf&sid=ITM_39338 (circulation date December 4, 2017).

TABLE II. NUMBER OF REMOTE ACCESS ACCOUNTS OPENED WITH CREDIT ORGANIZATIONS (THOUSANDS)

As of date	Total number of accounts	Of which opened by:		X^2	Y^2	XY
		Legal entities (X)	Individuals (Y)			
01.07.2017	172 529.00	4 562.30	167 966.70	20 814 581.29	28 212 812 308.89	766 314 475.41
01.04.2017	152 025.20	4 177.80	147 847.40	17 454 012.84	21 858 853 686.76	617 676 867.72
01.01.2017	191 961.50	4 522.90	187 438.70	20 456 624.41	35 133 266 257.69	847 766 496.23
01.10.2016	174 623.80	4 249.90	170 373.90	18 061 650.01	29 027 265 801.21	724 072 037.61
01.07.2016	155 280.60	4 022.80	151 257.70	16 182 919.84	22 878 891 809.29	608 479 475.56
01.04.2016	137 632.80	3 749.10	133 883.70	14 055 750.81	17 924 845 125.69	501 943 379.67
01.01.2016	162 833.20	4 026.40	158 806.80	16 211 896.96	25 219 599 726.24	639 419 699.52
01.10.2015	147 801.60	3 875.30	143 926.30	15 017 950.09	20 714 779 831.69	557 757 590.39
01.07.2015	137 738.60	3 544.20	134 194.40	12 561 353.64	18 008 136 991.36	475 611 792.48
01.04.2015	122 924.90	3 239.70	119 685.20	10 495 656.09	14 324 547 099.04	387 744 142.44
01.01.2015	125 776.30	3 460.50	122 315.80	11 975 060.25	14 961 154 929.64	423 273 825.90
01.10.2014	110 791.50	3 292.20	107 499.20	10 838 580.84	11 556 078 000.64	353 908 866.24
01.07.2014	101 694.60	3 000.30	98 694.30	9 001 800.09	9 740 564 852.49	296 112 508.29
01.04.2014	93 459.60	2 826.10	90 633.50	7 986 841.21	8 214 431 322.25	256 139 334.35
01.01.2014	111 879.50	3 042.00	108 837.50	9 253 764.00	11 845 601 406.25	331 083 675.00
01.10.2013	102 872.90	2 938.20	99 934.70	8 633 019.24	9 986 944 264.09	293 628 135.54
01.07.2013	93 723.90	2 786.30	90 937.60	7 763 467.69	8 269 647 093.76	253 379 434.88
01.04.2013	82 500.90	2 629.30	79 871.70	6 913 218.49	6 379 488 460.89	210 006 660.81
01.01.2013	99 885.50	2 798.50	97 087.00	7 831 602.25	9 425 885 569.00	271 697 969.50
01.10.2012	87 992.10	2 657.70	85 334.40	7 063 369.29	7 281 959 823.36	226 793 234.88
01.07.2012	79 225.60	2 482.80	76 742.80	6 164 295.84	5 889 457 351.84	190 537 023.84
01.04.2012	68 069.60	2 275.80	65 793.90	5 179 265.64	4 328 837 277.21	149 733 757.62
01.01.2012	79 261.90	2 404.20	76 857.70	5 780 177.64	5 907 106 049.29	184 781 282.34
01.10.2011	68 397.30	2 224.60	66 172.70	4 948 845.16	4 378 826 225.29	147 207 788.42
01.07.2011	58 226.90	2 081.30	56 145.60	4 331 809.69	3 152 328 399.36	116 855 837.28
01.04.2011	50 311.50	1 905.60	48 405.90	3 631 311.36	2 343 131 154.81	92 242 283.04
01.01.2011	59 042.70	2 006.40	57 036.30	4 025 640.96	3 253 139 517.69	114 437 632.32
01.10.2010	52 586.90	1 877.70	50 709.20	3 525 757.29	2 571 422 964.64	95 216 664.84
01.07.2010	46 016.70	1 812.70	44 204.00	3 285 881.29	1 953 993 616.00	80 128 590.80
01.04.2010	40 099.30	1 662.80	38 436.50	2 764 903.84	1 477 364 532.25	63 912 212.20
01.01.2010	46 715.40	1 791.40	44 924.00	3 209 113.96	2 018 165 776.00	80 476 853.60
01.10.2009	41 895.60	1 706.80	40 188.70	2 913 166.24	1 615 131 607.69	68 594 073.16
01.07.2009	37 537.50	1 612.70	35 924.80	2 600 801.29	1 290 591 255.04	57 935 924.96
01.04.2009	32 592.80	1 488.50	31 104.30	2 215 632.25	967 477 478.49	46 298 750.55
01.01.2009	38 862.00	1 591.10	37 270.90	2 531 599.21	1 389 119 986.81	59 301 728.99
01.10.2008	33 228.10	1 461.00	31 767.10	2 134 521.00	1 009 148 642.41	46 411 733.10
01.07.2008	28 914.60	1 355.70	27 558.90	1 837 922.49	759 492 969.21	37 361 600.73
01.04.2008	24 495.20	1 235.50	23 259.70	1 526 460.25	541 013 644.09	28 737 359.35
01.01.2008	27 722.60	1 290.00	26 432.70	1 664 100.00	698 687 629.29	34 098 183.00
Σ	3 479 130.20	103 668.10	3 375 462.20	312 844 324.73	376 509 190 437.64	10 737 078 882.56

We perform correlation analysis of tabular data. Number of values is $n = 39$. Let's calculate the mean values of random variables X and Y:

$$\bar{x} = 103668.10 / 39 \approx 2568.16 \quad (1)$$

$$\bar{y} = 3375462.20 / 39 \approx 86550.31 \quad (2)$$

Let's find the mean square deviations $\sigma^2(x) = \Sigma (X^2) / n - \bar{x}$ and $\sigma^2(y) = \Sigma (y^2) / n - \bar{y}$:

$$\sigma^2(x) = 312844324.73 / 39 - 2568.16^2 \approx 1426203.57 \quad (3)$$

$$\sigma(x) = \sqrt{1426203.57} \approx 1194.24 \quad (4)$$

$$\sigma^2(y) = 376509190437.6 / 39 - 86550.3^2 \approx 2163127376 \quad (5)$$

$$\sigma(y) = \sqrt{2163127376} \approx 46509.43 \quad (6)$$

Therefore, covariance is $Cov(x, y) = \Sigma (X \cdot Y) / n - \bar{x} \cdot \bar{y}$:

$$Cov(x, y) = 10737078882.56 / 39 - 2568.16 \cdot 86550.31 \approx 275309714.94 - 222275044.13 \approx 53034670.81 \quad (7)$$

Positive value of covariance indicates unidirectional change in the value of number remote access accounts of individuals and legal entities.

The correlation coefficient is $r_{xy} = Cov(x, y) / (\sigma(x) \cdot \sigma(y))$.

$$r_{xy} = 53034670.81 / (1194.24 \cdot 46509.43) \approx 0.955 \quad (8)$$

Its value implies a very high direct connection between the random variables X and Y, as well as a strong compression of the data cloud with its main axis.

The coefficient of variation is ratio $V_x = \sigma(x) / \bar{x} \cdot 100\%$ and $V_y = \sigma(y) / \bar{y} \cdot 100\%$:

$$V_x = 1194.24 / 2568.16 \cdot 100\% \approx 46.5\% \quad (9)$$

$$V_y = 46509.43 / 86550.31 \cdot 100\% \approx 53.7\% \quad (10)$$

The degree of data dispersion is not uniform in both cases. Data is far from each other and from its middle axis [19].

A "digital person" more and more uses devices that record information about his whereabouts and activities. Therefore, risks of violating cybersecurity are constantly increasing. On the diagram is depicted relationship of actions and services producing new data about the "digital person" (see Fig. 2). This information can be used by hackers for computer crimes.

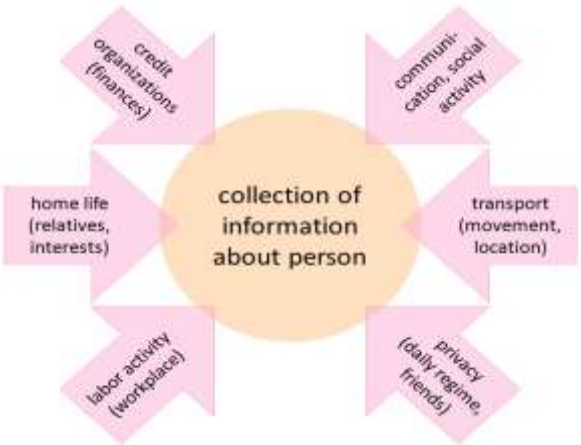

Fig. 2. Actions and services producing information.

For increase of observance level of information security it is need to bring clients and employees to the history of cybercrime by financial institutions. After all, as said the Russian historian V.O. Klyuchevsky "*history is not a teacher, but a warder: she does not teach, but severely punishes for ignorance of her lessons*." We can explanation of this phenomenon with words of V.S. Stepin (philosopher and organizer of science), who believes that a person, beginning with his birth, is gradually included in the system of historically established social ties and relations. The higher the person ascends in his historical development through civilization's levels, the more he rises above the dominant influence of direct biological stimuli to regulate his relations with other people[5]. Biological needs predominant over moral norms usually. It is prompt people to violate security (territorial security, information security, economic security, etc.).

V. CONCLUSIONS

Conducted research of social engineering in electronic banking shows that in the long term it is necessary to create not only system of supervision in the virtual space, but also to raise culture of behavior in it of all participants of information exchange to prevent external and internal cyberthreats.

The value and novelty of this research are that it provides recommendations for elevating users' literacy with respect to remote banking so to mitigate cybercrime risks. The findings can be used by financial and educational institutions to corroborate the dependence of cybercrimes on the users' literacy and intellectual development methods. After all modern banking business will strive to expand RBS.

Subscriber can trust his interlocutor only if the subscriber is an active party. If caller did a call, introduced himself as bank employee and was asked to name any Personal Identification Number (PIN) or password, then the subscriber is a passive party. Therefore, the subscriber must not do anything that interlocutor wants from him. If an interlocutor offered to call back on some other phone and the subscriber call this phone, then he is again a passive party. In general, if interlocutors were presented by the bank's employees, it is necessary to call back, but only by the official phone number, which is on the bank card or the official website.

Scammers use original techniques to weaken human vigilance, invade his psyche and obtain valuable information. All these techniques are based on lies[6]. Therefore, before the present time there is no perfect way to confront the information-psychological impact.

Blogs of information security services of banks and groups in social networks are excellent source of information about new cyberthreats, malicious software, methods of fraudulent and ways to counteract. Often the reason for disclosure of information is excessive credulity and negligence of people (customers and employees).

To educate the critical perception of incoming information in realize of social engineering methods, it is necessary to improve the teaching of humanitarian disciplines in programs of secondary and higher education, namely, Russian history,

[5] Stepin V.S. History and philosophy of science: Textbook for graduate students and applicants of the scientific degree of Candidate of Science. Moscow, Academic Project, 2014, 424 p.

[6] Sun Tzu. The Art of War, Chiron Academic Press, 2015, 108 p.

financial literacy and methodology of cybersecurity [20].

It is necessary to raise financial literacy of citizens and to explain attractiveness of non-cash transactions for customers. Nevertheless, talking about raising financial literacy in isolation from general education is completely wrong. An educational institution must to choose an audience where the workplaces of “administrators at RBS”, “hackers” and “customers” will be deployed. This will allow the students to take training the algorithms of action for provide of information protection [14]. Forewarned is forearmed.

After all, being financially literate is a necessity dictated by time. The invulnerability of human's savings will be reward for his knowledge and vigilance [21].

ACKNOWLEDGMENT

The article follows results of researches financed as part State Job of the Financial University under the Government of the Russian Federation in 2017.

Authors would like to express special gratitude to colleagues and friends for their helpful comments and critical remarks concerning this article: Sergey Vladimirovich Dvoryankin [13], Grigory Olegovich Krylov [19], co-author's mother Ekaterina Vasilievna Berdyugina, etc.

REFERENCES

[1] Chris Skinner. Digital bank: Strategies to Launch or Become a Digital Bank. Singapore, Marshall Cavendish International (Asia), 2014, 300 p.

[2] Dorofeev A.V., Markov A.S., Tsirlov V.L. Social media in identifying threats to ensure safe life in a modern city. Communications in Computer and Information Science. 2016. Vol. 674. pp 441-449. DOI: 10.1007/978-3-319-49700-6_44.

[3] Yudenkov Yu.N. Internet-related technologies in banking business: outlooks and risks: workbook. Moscow, KnoRus Publ., 2014, 318 p.

[4] Travis J. Wiltshire, Samantha F. Warta, Daniel Barber, Stephen M. Fiore. Enabling robotic social intelligence by engineering human social-cognitive mechanisms. Cognitive Systems Research, Volume 43, June 2017, pp. 190-207. DOI: https://doi.org/10.1016/j.cogsys.2016.09.005.

[5] Katharina Krombholz, Heidelinde Hobel, Markus Huber, Edgar Weippl. Advanced social engineering attacks. Journal of Information Security and Applications, 2015, vol. 22, pp. 113-122. DOI: https://doi.org/10.1016/j.jisa.2014.09.005.

[6] Francois Mouton, Louise Leenen, H.S. Venter. Social engineering attack examples, templates and scenarios. Computers & Security, 2016, vol. 59, pp. 186-209. DOI: https://doi.org/10.1016/j.cose.2016.03.004.

[7] Lyamin L.V. Application of electronic banking technologies: risk-oriented approach. Moscow, KnoRus Publ., 2011, 336 p.

[8] Nader Sohrabi Safa, Rossouw von Solms, Lynn Futcher. Human aspects of information security in organisations. Computer Fraud & Security, 2016, vol. 2016, no. 2, pp. 15-18. DOI: https://doi.org/10.1016/S1361-3723(16)30017-3.

[9] Hossein Siadati, Toan Nguyen, Payas Gupta, Markus Jakobsson, Nasir Memon. Mind your SMSes: Mitigating social engineering in second factor authentication. Computers & Security, Volume 65, March 2017, Pages 14-28. DOI: https://doi.org/10.1016/j.cose.2016.09.009.

[10] David Tayouri. The Human Factor in the Social Media Security – Combining Education and Technology to Reduce Social Engineering Risks and Damages. Procedia Manufacturing. Volume 3, 2015, Pages 1096-1100. DOI: https://doi.org/10.1016/j.promfg.2015.07.181.

[11] Joseph M. Hatfield. Social engineering in cybersecurity: The evolution of a concept. Computers & Security, Volume 73, March 2018, Pages 102-113. DOI: https://doi.org/10.1016/j.cose.2017.10.008.

[12] Christopher Hadnagy, Paul Wilson. Social Engineering: The Art of Human Hacking. Indianapolis, Wiley Publishing, Inc., 2011, 416 p.

[13] Minaev V.A., Dvoryankin S.V. Modeling the dynamics of information and psychological influence on mass consciousness. Voprosy kiberbezopasnosti *[Cybersecurity issues]*, 2016, iss. 5 (18), pp. 56-64. DOI: 10.21681/2311-3456-2016-5-56-64.

[14] Revenkov P.V., Berdyugin A.A. Social Engineering as a Source of Risks in Online Banking Services. National Interests: Priorities and Security, 2017, vol. 13, iss. 9, pp. 1747–1760. DOI: https://doi.org/10.24891/ni.13.9.1747.

[15] Francois Mouton, Mercia M. Malan, Kai K. Kimppa, H.S. Venter. Necessity for ethics in social engineering research. Computers & Security, 2015, vol. 55, pp. 114–127. DOI: https://doi.org/10.1016/j.cose.2015.09.001

[16] Shamraev A.V. International and foreign financial regulation: institutes, transactions, infrastructure: monograph. Moscow, KnoRus Publ., 2014, 640 p.

[17] Matthew Edwards, Robert Larson, Benjamin Green, Awais Rashid, Alistair Baron. Panning for gold: Automatically analysing online social engineering attack surfaces. Computers & Security, 2017, vol. 69, pp. 18-34. DOI: https://doi.org/10.1016/j.cose.2016.12.013.

[18] Shailendra Rathore, Pradip Kumar Sharma, Vincenzo Loia, Young-Sik Jeong, Jong Hyuk Park. Social network security: Issues, challenges, threats, and solutions. Information Sciences, Volume 421, December 2017, Pp. 43-69.DOI: https://doi.org/10.1016/j.ins.2017.08.063.

[19] Denisenko A.S., Krylov G.O. Application of principal components analysis results in visual network analysis. Biosciences Biotechnology Research Asia. 2015. Vol. 12. Iss 1. Pp. 609-617. DOI: 10.13005/bbra/1704.

[20] Sveta K. Berdibayeva, Aiman M. Kalmatayeva, Sholpan A. Tulebayeva. Research of Formation of Personal-Professional Capacities at Higher Education Institutes Students of Pedagogical Specialties. Procedia – Social and Behavioral Sciences, Volume 69, 24 December 2012, Pages 1174-1177. DOI: https://doi.org/10.1016/j.sbspro.2012.12.048.

[21] Sheremet I. A. Augmented Post Systems: The Mathematical Framework for Data and Knowledge Engineering in Network-centric Environment. Berlin, 2013. 395 p.