SOCIAL PROBLEMS OF MODERN RUSSIA

RESEARCH ARTICLE

DOI: 10.21684/2587-8484-2018-2-4-42-58 **UDC** 316.334.4

Social networking sites as a platform for fraud

Alexandra I. Kukhto[1], Anna V. Maltseva[2]

[1] Undergraduate Student, Department of Social Analysis and Mathematical Methods in Sociology, Saint Petersburg State University (Saint Petersburg, Russian Federation) a-kuh@bk.ru

[2] Dr. Sci. (Soc.), Associate Professor, Department of Social Analysis and Mathematical Methods in Sociology, Saint Petersburg State University (Saint Petersburg, Russian Federation) annamaltseva@rambler.ru

Abstract. This article studies the use of social networks as new forms of virtual social space, which allows realizing different types of fraud. The issue is especially urgent due to the actions of users and organizations on social networks and their insufficient level of information literacy about computer security. This research aims to provide a social analysis of computer criminality before devising any effective actions for increasing security level of interactions in social networks and preventing Internet crime. This article depicts some general principles, including negative and positive features of user interactions on social networks, accounting for real public relations and government regulations in Internet security and computer crime. The results of the research have revealed the contemporary distinctive conditions for implementing, increasing, and developing computer crime on social networks, its specifics, aims, and technological components. The authors describe different kinds of criminal acts on social networks, their typology, and the fraudulent methods. This research emphasizes the deficiency of knowledge on information security, demonstrated by the Internet users. Based on the data acquired during social analysis, the authors recommend a number of personal, legal, and public actions for protecting user personal data and preventing computer crime on the Internet and social networks.

Keywords: social networks, Internet, information, Internet fraud, cybercrime, information threats, information security.

Citation: Kukhto A. I., Maltseva A. V. 2018. “Social networking sites as a platform for fraud”. Siberian Socium, vol. 2, no 4, pp. 42-58. DOI: 10.21684/2587-8484-2018-2-4-42-58

INTRODUCTION

The end of the 20th century was marked by the penetration of digital technologies into all spheres of human life. They rapidly changed them and contributed to the emergence of qualitatively new types of social relations. The Internet has given people almost unlimited possibilities for transferring and processing information and performing transactions that were previously made only in the physical world, for example banking.

However, not all activity in the Internet can be viewed as positive. Certain activities within the network can lead to negative consequences and impacts on certain spheres of life.

The relative novelty of the social relations realized through the social networks in the Internet and the deficiency of legal and regulatory framework give rise to problems and risks associated with cyber-crime. The popularity and continuous development of social networks in the Internet promote new types of socially dangerous actions and transform traditional crimes.

Internet fraud is one of the most frequently encountered crimes manifesting themselves in various forms online. Despite the fact that online fraud was first reported a long time ago, as the Internet is becoming more accessible every year, more and more types of online fraud are appearing. However, the measures of fraud prevention and correction are mainly contradictory and fragmented. They can hardly address the newest forms of criminality.

High-quality legal and regulatory environment in the Internet-based social networks requires an interdisciplinary study of all emerging threats on their platforms. Fraud is one of the most frequent and possibly dangerous threats. This paper attempts to address the problem of development of quality measures for online fraud protection and prevention using the sociological analysis.

MAIN PART

The social network as a sociological concept appeared as far back as in the middle of the twentieth century. However, over more than sixty years it has undergone a great transformation of meanings. The first websites did not suppose any connection either between the user and the network administrator, or between the users. Users remained anonymous consumers of the content offered by the administrators. Various feedback tools appeared gradually with new technological advancements. Initially, there were functions of voting and commenting; then communication services developed in the form of conferences, chats, etc. [15, p. 111]. Thus, gradually, websites began to turn into sort of virtual social networks.

In general, virtual social networks are a form of virtual social space which can be defined as a virtual social structure populated with virtual social groups, virtual personalities, and virtual individuals. Therefore, any online community where users communicate and exchange information can be considered as a social network. These communities are most often formed on the basis of common interests, outlooks, and values.

In the second half of the 20th century, scientists, primarily Western, initiated multiple studies of social networks to better understand online interactions. They ana-

lyzed the structure of the relationships in social networks and the actions of users who create and modify these structures. Such studies were even more popular at the beginning of the twenty-first century. (See, for example, the works by B. Hogan) [7], D. M. Boyd (1) and many others.). Ten years ago, N. G. Fielding and R. M. Lee edited the fundamental *Handbook of Online Research Methods* [5]. Therefore, it is difficult to disagree with A. A. Morozova that complete theories have been produced from social network analysis stating that websites are one of the attributes of the information society, that they form a special communicative space with its own characteristics and differences from real world interaction [9, p. 201-202].

The interaction on social networking sites is a series of contacts between user profiles, implemented in the social network as "friendship". Ye. G. Efimov rightly points out that these contacts "allow network users to create public or semi-public profiles within the limits imposed by the system, define groups of other users with whom they can communicate and share information, view and link their contacts, messages, likes, etc." [4, p. 27].

Despite all the specifics of virtual relationships, they still remain the relationship between man and man, man and group or group and group, to which human laws and rules [12, p. 128-129], behavioral attitudes and needs still apply [14]. In addition, despite the advantages of social networks, their main drawbacks are anonymity and impersonality, which can entail dangers and risks of various kinds, including various fraudulent activities.

A rather large amount of personal information voluntarily placed in online social networks brings to the fore the problem of information security and protection against unlawful attacks on the data stored in such networks, as well as intellectual, financial and physical property.

The importance of information security threats is emphasized by the Doctrine of Information Security of the Russian Federation, which defines the following "main types of threats:

- to constitutional human and civil rights and freedoms with regard to the receipt and use of information; privacy in the use of information technologies, … interaction between the State and civil society; as well as applying information technologies for the preservation of cultural, historical, spiritual and moral values of the multi-ethnic people of the Russian Federation;
- to the sustainable and smooth operation of the information infrastructure, primarily of the critical information infrastructure of the Russian Federation;
- to the development of the sector of information technologies and electronics in the Russian Federation and improving the performance of production, research and scientific and technological community to develop, produce, and operate information security means and provide information security services meeting the needs of the domestic market and entering the world market, as well as ensuring the accumulation, preservation, and efficient use of domestic information resources;
- threats to the security of information and telecommunication means and systems, both deployed and in the process of creation on the territory of Russia"[2].

One of the main types of online crimes most often committed on social networking sites and directly connected with the security of information and personal data is internet-fraud. With the development of information technologies and the emergence of social networking sites as the main platforms for interaction on the Internet, fraudulent actions have changed their nature based on certain properties and functions of the virtual environment.

Social networking sites attract various kinds of fraudsters because their audience is constantly and rapidly growing. Their users are free to spread information remaining anonymous. Site administrators have practically no control over the users which means that communication on the website is almost unregulated.

In addition, these sites are characterized by a number of features which together form a set of favorable conditions for online crime growth. They include:

1. First, anonymity which can be created with certain (often quite simple and basic) skills and knowledge. The opportunities for anonymous access to social networks not only generate a large amount of dangerous information, spam and advertising, but also a sense of freedom and impunity, encouraging fraudulent schemes within the network.
2. Secondly, the speed of actions and information transfer provided by social networks. It allows fast delivery of messages, electronic payments and commercial operations. The speed and easy access to such operations applies virtually to the entire Internet space and creates a delay from the moment a criminal act is committed until the user realizes that s/he has become a victim. This, in turn, can imply that there will be no consequences for the perpetrator.
3. Thirdly, the lack of effective legal regulation and security of Internet payments and Internet banking including cyber payment services and transfers.
4. Fourthly, the cross-border nature of social networks and, hence, the crimes committed on their platforms. The fraud perpetrator and their victims may be located in different cities, regions and countries. The differences in the legislation and territories can complicate capturing of the criminal and let him/her commit more crimes in several places at the same time.

Thus, social networks create a favorable environment for fraud perpetrators who use increasingly sophisticated methods of committing criminal offences. Currently, the punishment for online fraud is provided for by art. 159 of the Criminal Code of the Russian Federation. Nevertheless, fraud incidents are widespread and continue to increase in frequency.

Fraud is generally defined in modern scholarly publications as:

> "any deprivation of another person's property by deception, betrayal of public trust, misappropriation, embezzlement and property damage through deception or abuse of trust using computer hardware" [6, p. 445];
>
> "unlawful intentional distortion, alteration or disclosure of data with the purpose of obtaining benefits (usually in cash) using a computer system that is used to commit or cover a single or serial crimes" [8, p. 62],

etc. Each existing definition reveals certain aspects of this type of online crime.

This type of crime in social networks is the result of the interaction within the most unprotected sphere of public relations. Unlike any other type of computer related crimes, fraudulent actions are most noteworthy because, in essence, they are directed neither at the computer or other means of transmitting information, but directly at the person. Most fraudsters aim at monetary gain by deception or abuse of trust. Most often, criminals commit such actions that are almost impossible to distinguish from the goods and services offered on the Internet by legal entrepreneurs and firms. Thus, they not only cause damage to users, but also undermine the reputation and credibility of legitimate commercial activities on the Web.

Fraud on social networking sites has, according to I. A. Nikitina, two components: technological and communicative. The first implies plotting a crime and using the Internet environment to cover it up (for example, creating anonymity) and receiving money from the user without directly contacting him or her. The second includes putting the potential victim under psychological pressure and making him/her act in the interests of the fraudster [11, p. 122].

An important aspect of information security is to prevent and counter the use of social networking sites for fraudulent purposes. This becomes a daunting task in the modern dynamically developing world. Researchers believe that today there are no effective measures to prevent fraud on the Internet. Therefore the responsibility to exercise reasonable caution lies with the users who want to make their actions on the Internet as secure as possible [3].

Among the possible measures aimed at protecting social network users, we can distinguish three categories: measures taken by the administrators of social networks; measures taken by commercial organizations that may incur risks in the event of fraud; and measures that ordinary users can take [10, p. 71].

Based on the foregoing, fraud on social networking sites can be considered one of the most common and dangerous illegal actions in the Internet environment. It has various forms and features and changes with the development of technology creating threats for both ordinary users and commercial organizations. It has become a problem at the national and even international levels. In addition, it has a dangerous social and psychological impact on the users who have encountered it.

We conducted a sociological survey of Internet users in order to study their awareness and attitude to fraudulent actions on social networking sites. The sample for this survey included those Internet users who are registered on the websites of the following social networks: VKontakte, Odnoklassniki, Instagram, YouTube, Facebook, and Twitter. The so-called instant messengers—instant messaging systems for text, audio and video messaging (for example, Telegram, WhatsApp)–were not taken into account in the study.

The number of the users of the social network VKontakte (488,810,000) in accordance with the *Catalog of VKontakte users* [16] was considered as the volume of the entire population since almost all Russian users of social networks are registered in this network. In this case, with a confidence interval of 5 and a confidence probability of 95%, the minimum sample size of the respondents must be 385 respondents in order to get reliable and representative results. The calculation of the

sample took into account the age distribution of the users. In addition, the questionnaire included questions formulated to identify the reason for registering and using the social networking sites, the level of user confidence in the interlocutors and site administrators and the relevance of the problem of fraud.

During the empirical study, 428 people were interviewed. The survey was launched on the Google Forms platform which is an online service for creating feedback forms that include questionnaires, surveys, online testing, and registration forms.

This technical tool is easy to use and has a number of advantages for conducting empirical research:

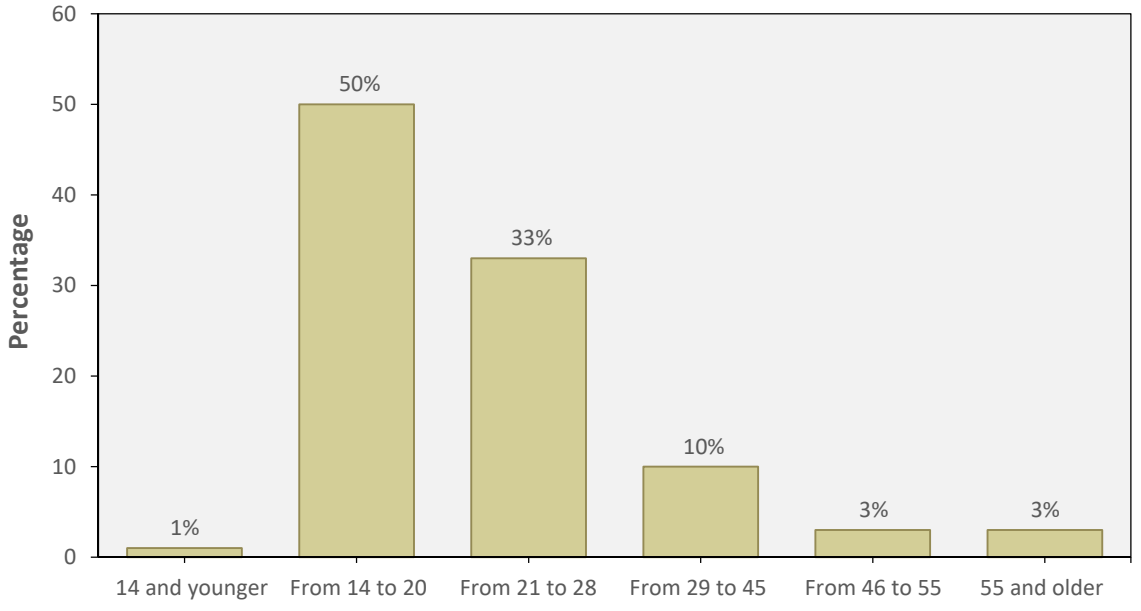
— simplicity and clarity of the interface for the respondents;
— free of charge and round-the-clock access to the data from various devices;
— possibility to publish links on various platforms, including social networking sites;
— providing possibility to download the received data in various formats suitable for Microsoft Excel and the statistical data processing package–SPSS.

Altogether, 1 093 Internet users took part in the survey in May 2018.

The results of the sociological survey can be divided into four parts: basic information, personal data, threats of fraud and the influence of the user's field of education.

The age distribution of the majority of the respondents is 14–28, which corresponds to the official statistics of the user audience of the social networks presented in the survey. Thus, the sample can be considered as representative [11] (Fig. 1).

Fig. 1. Age distribution of social networks' users



Almost all respondents are registered on various social networking sites. The overwhelming majority did it on their own, and only a small portion of the respondents admitted that they entrusted this process to their relatives and friends.

However, even the presence of this aggregate (less than 5%) may indicate that a certain percentage of users of social networking sites are more susceptible to dangers and risks of hacking, since registration by an outsider often leads to sharing of passwords and makes the user vulnerable to cybersecurity threats such as social and psychological pressure (Fig. 2).

The most popular among the Russian users of social networking sites is *VKontakte*. The second place goes to YouTube – a social media platform built on the principle of a social network. The social network for sharing photos and videos Instagram ranks third in popularity. Given the specifics of the social media and networks aimed at visual data, it can be assumed that, during registering on these sites, anonymity is more difficult to maintain than on the classic examples of social networking sites such as VKontakte, Facebook or Odnoklassniki (Table 1).

The survey revealed the information related to personal data by asking questions aimed at identifying the data which users most frequently post on the networks taking into account the degree of privacy of their user profiles and information disclosure behavior in relation to the other users of this network or the Internet.

The most pertinent information, which most often enters the network through voluntary publication, is photographs (which is not surprising, given the large number of Instagram users). However there is a large percentage of those people who do not publish any data in open access. This can be explained both by the lack of need and by the desire to maintain complete anonymity on the network (Tables 2-3).

Fig. 2. Distribution of users registered in social networks according to the survey results

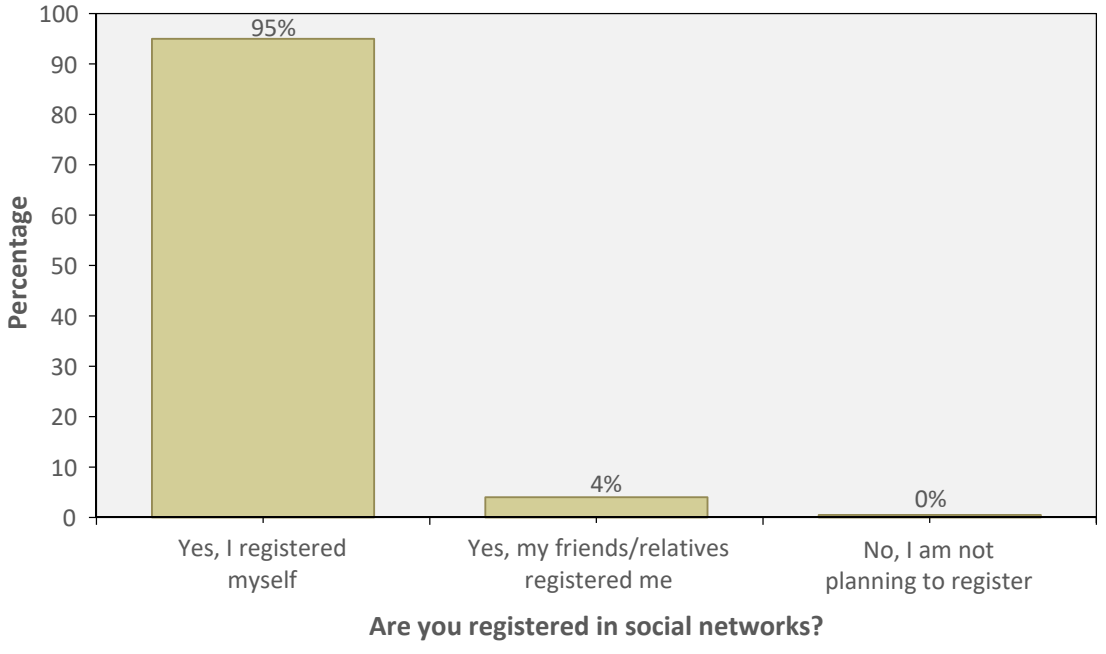


Table 1. Popularity of social networks among users

Which social network do you use?	**% of observations**
Facebook	10
VKontakte	96
Twitter	21
Tumblr	8
Odnoklassniki	4
LiveJournal	0
Ask.fm	7
Instagram	47
YouTube	62
Use none	0

Table 2. Published average data by sample

The data published by the users	**% of observations**
photo	65
telephone number	12
address	3
location	10
family status	6
Information about their work	12
Do not post anything	31

Table 3. Published data by different age groups

The published data	**Up to 14**	**14-20**	**21-28**	**29-45**	**46-55**	**56 and older**
photo	1	33	24	5	2	1
telephone number	0	5	5	1	1	0
address	0	1	1	1	0	0
location	0	4	4	1	1	1
family status	0	2	1	1	0	0
Information about their work	0	4	6	2	1	0
Do not post anything	0	16	9	4	1	1

Also, in most cases, users leave their profiles on the social network open. However, older users tend to grant selective or restricted access to their profiles (Fig. 3), which may indicate their greater caution and can be explained by previous online fraud experiences (Fig. 4).

To learn about the users' perception of fraud threats on social networking sites, we asked questions about their attitudes to this phenomenon and relevant personal experience (what threats affect the users' activities on the network; the users' experience of social media fraud; whether they consider themselves protected).

Most users are disturbed by threats of both human and technological nature (Fig. 5). However, the percentage of people who noted threats related to human activities and directed at the users (for example, fraud) is almost twice the percentage of those who chose technological threats aimed at destroying their computer system (e.g. viruses) (Fig. 6).

When distributed by age categories, the value of the "technological threats" variable begins to decrease and the value of the variable that says that users are not worried about any of the listed types of threats (Fig. 5) rises. This situation may be associated with a lower awareness of the older generation of the users in comparison with the younger ones who get access to social networks at an early age.

Fig. 3. Profile privacy specifics by age

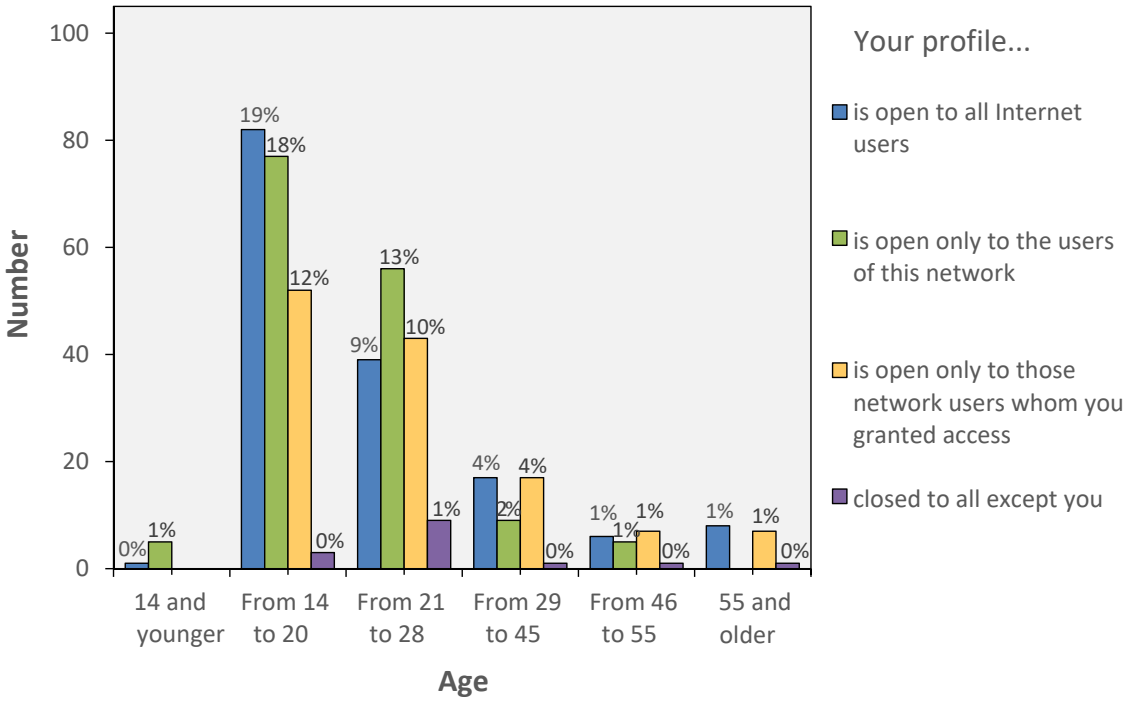


Fig. 4. Respondents' perceptions of the impact of threats depending on the age

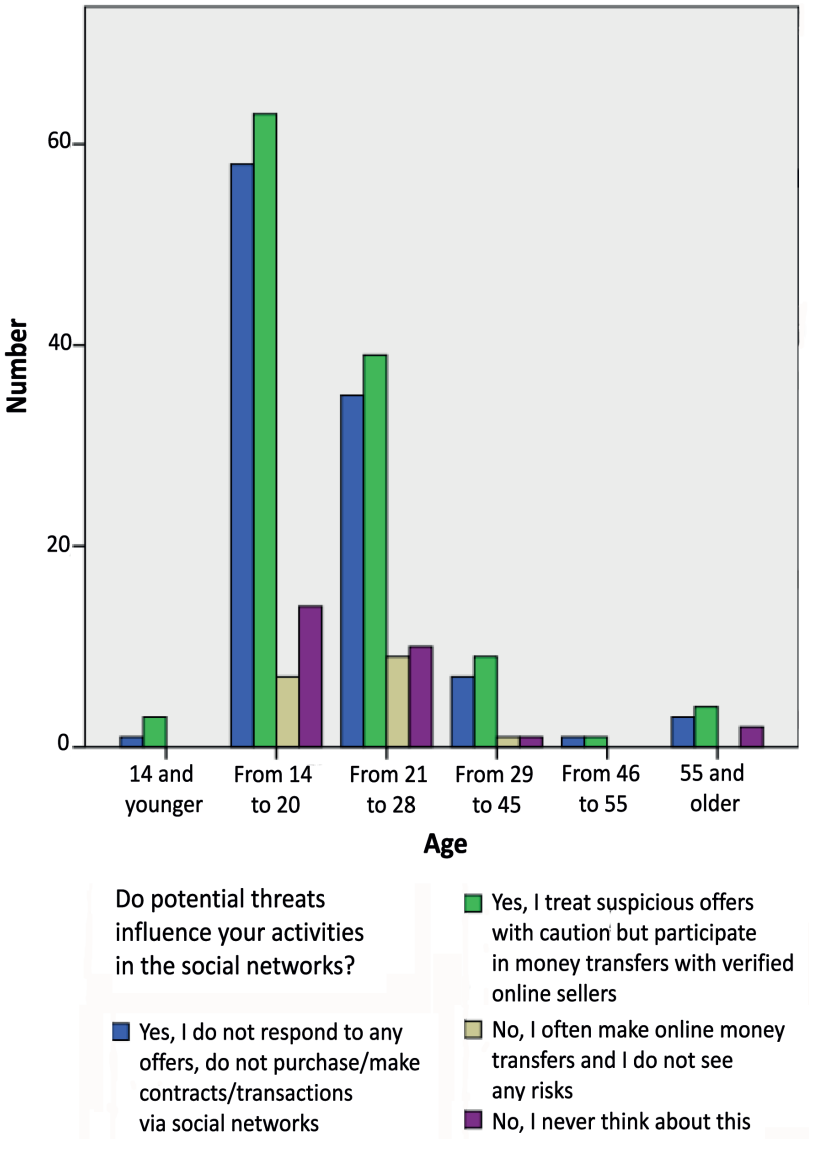


Fig. 5. Respondents' perceptions about the fraudulent threats' economic impact on user activity on social networks

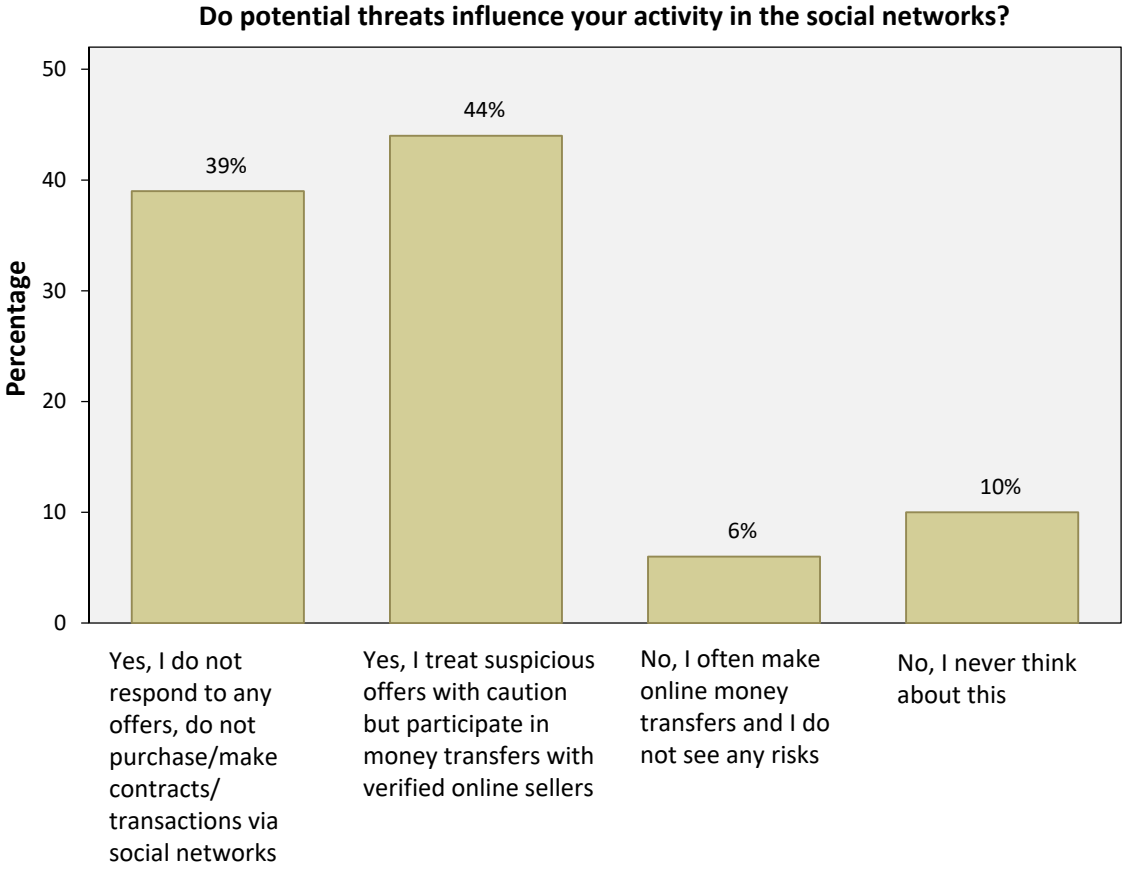


Table 4. Distribution of threats depending on the social network, preferred by a respondent

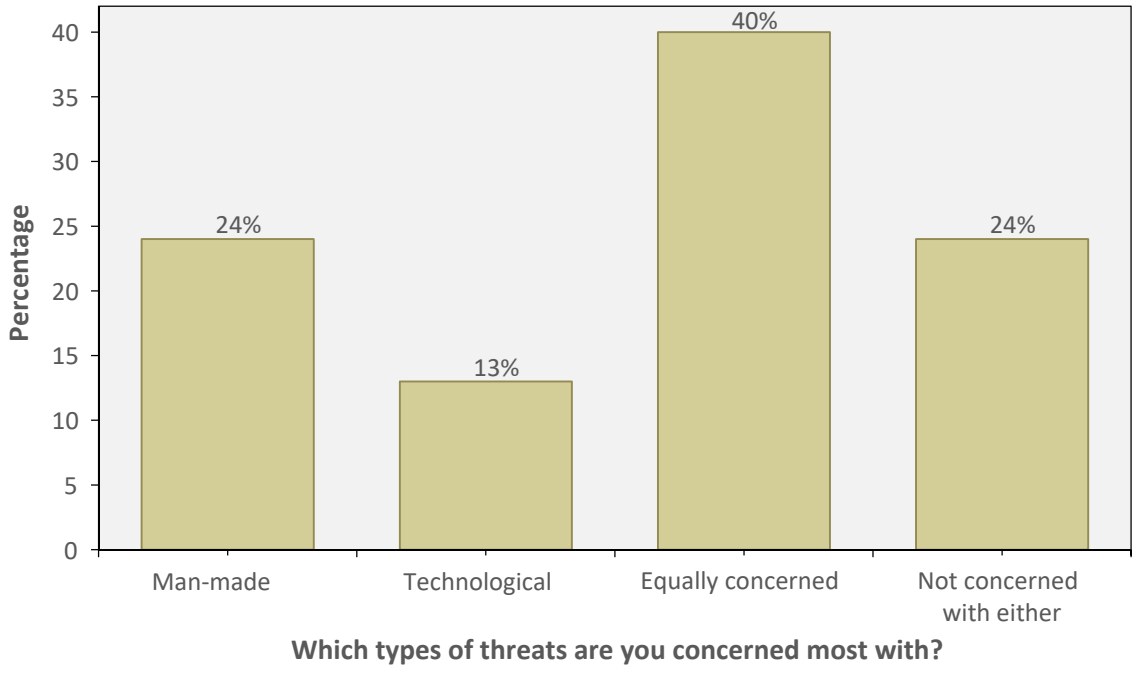
Social network	Types of threats				
	Concerned about man made threats	Concerned about technological threats	Concerned equally about both types of threats	Are not concerned	Total
Facebook	25	14	39	23	100
VKontakte	24	13	39	23	100
Twitter	21	12	49	17	100
Tumblr	17	20	46	17	100
Odnoklassniki	20	13	53	13	100
LiveJournal	0	0	0	100	100
Ask.fm	3	17	73	7	100
Instagram	26	13	44	17	100
YouTube	26	11	39	24	100
Use none	0	50	0	50	100

The distribution of the user attitudes towards threats depending on their preferred social networking sites (Table 4) is also quite interesting. In this case, the number of the people who have noted man-made threats also prevails for almost all the social networks. The only exceptions are the users of Tumblr and Ask.fm, which can be explained by the greater openness of these networks and fewer data security technologies (for example, registration confirmation via e-mail is not necessary for registering on the Ask.fm network).

When comparing the percentage of the users who have encountered fraud during their activity in the social networks (Fig. 7), one can see no direct correlation. The number of the respondents who have personally encountered online fraud and are now worried or not worried about the problem of human threats is approximately the same.

From the charts described above, it can be noted that, in general, regardless of the age, preferred social network or fraud experience, the majority of the users are worried about threats from human activities. This indicates that fraud prevention on social networking sites is a common growing concern and site administrators together with the authorities and the users themselves shall deal with the problem. Since the legislation in the area in question is underdeveloped, as well as the technology solutions to fight cybercrime, the dialogue seems to be the most successful strategy.

Fig. 6. Distribution of respondents' views on the nature of threats



Threats associated with the loss of financial resources are called an urgent problem by a third of the social networks users (Fig. 8). Figure 9 shows an interesting distribution of the values: 26% of the respondents consider the problem of fraud in social networks relevant; they encountered it personally; 37% of the respondents personally experienced fraud, but they believe that it was an accident and ignore the risks; 12% have never been fraud victims, but assessed the risks as relevant. This group is most secure. Many of them treat online payment services and platforms offered by various social networks with caution; 25% of the respondents, in our opinion, constitute a risk group, since these users have not personally encountered the problem and do not consider it critical, which may result in reckless online behavior (Fig. 9).

Despite the high frequency of fraud on the social networking sites as well as the fraud-related negative experience of some users, for most it is not relevant, which may again be due to the respondents' low awareness of the potential online dangers (Fig. 9).

Among the respondents who have experienced fraud on the social networking sites, the majority believe that they were poorly protected against various kinds of criminal actions (identity theft or breach of trust) by the site administrators (Fig. 10).

This empirical study allowed us to identify a number of trends in the users' attitude to this phenomenon and its influence on their activities within the social network.

First, the majority of the users tend to consider human threats within the social networks to be the most dangerous for themselves. Obviously, the problem of technological threats is being gradually and successfully solved through the creation and improvement of various technologies (for example, antivirus or cleaning programs). The problems of fraud and breach of trust have not been much elaborated on and are currently requiring further investigation and solution.

Secondly, a significant number of the users encountered fraudulent activities on the social networking sites directly or indirectly, which implies that the phenomenon is common on the Internet and on various platforms, regardless of the country of origin and the attempts of the social network administrators to mitigate risks. Fraud is a transnational phenomenon, therefore, in order to find a solution to this problem, there is a need for consistency between the law enforcement and governmental systems of different countries.

Thirdly, the potential threats associated with money transfers do not allow the respondents to use freely all the features and services of the social networks.

Fourth, despite the widespread occurrence of fraud on the social networking sites, more than 60% of the users do not consider the problem of online fraudulent activities relevant to themselves. They tend to reason like "it will not affect me". Based on these statistics we can assume low user awareness, literacy, and information culture. Thus, it is important to timely disseminate information related to certain types of fraud and fraud prevention on the social networking sites.

Fig. 7. Distribution of the nature of threats according to the personal user experience

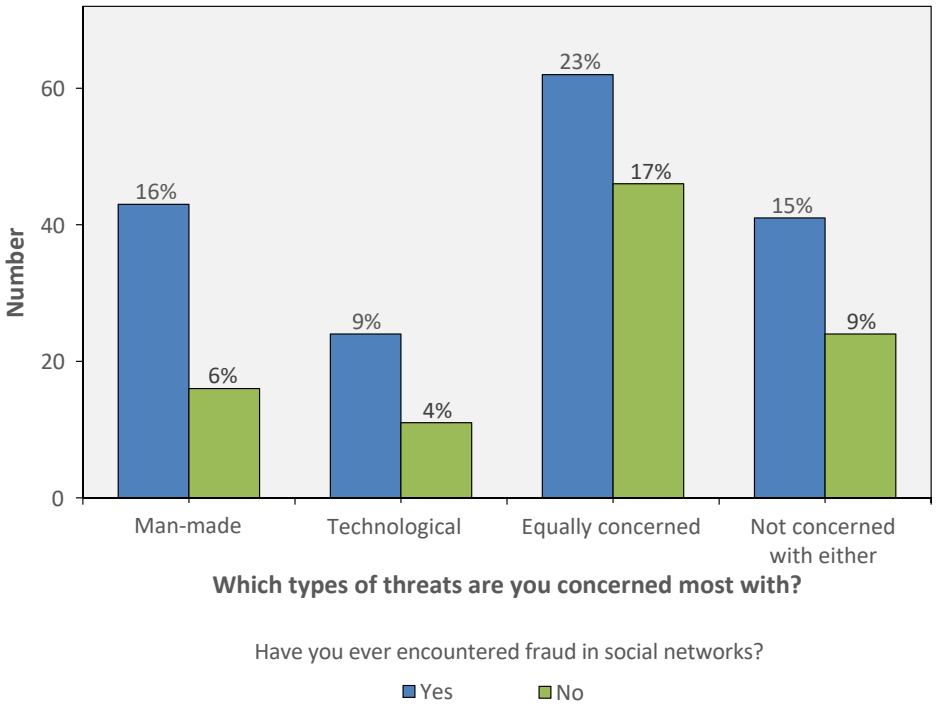


Fig. 8. The relevance of the problem of fraud for users

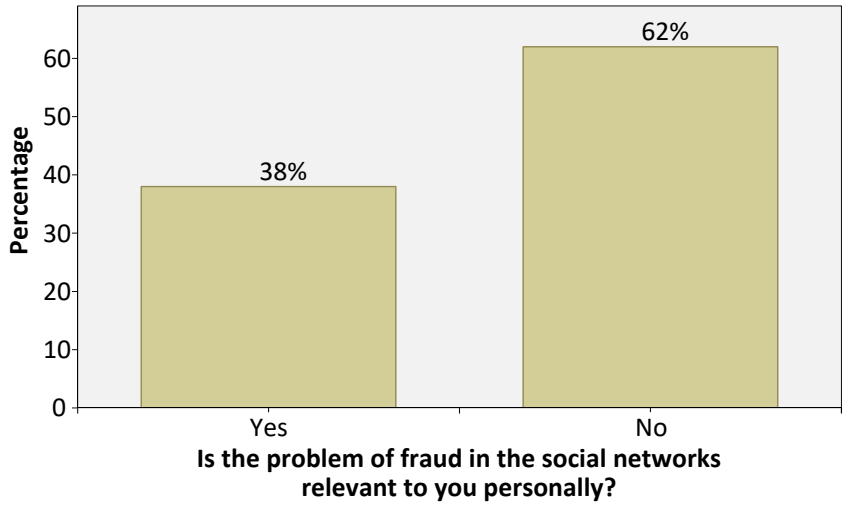


Fig. 9. Distribution of user opinions on the urgency of fraud according to their personal experience

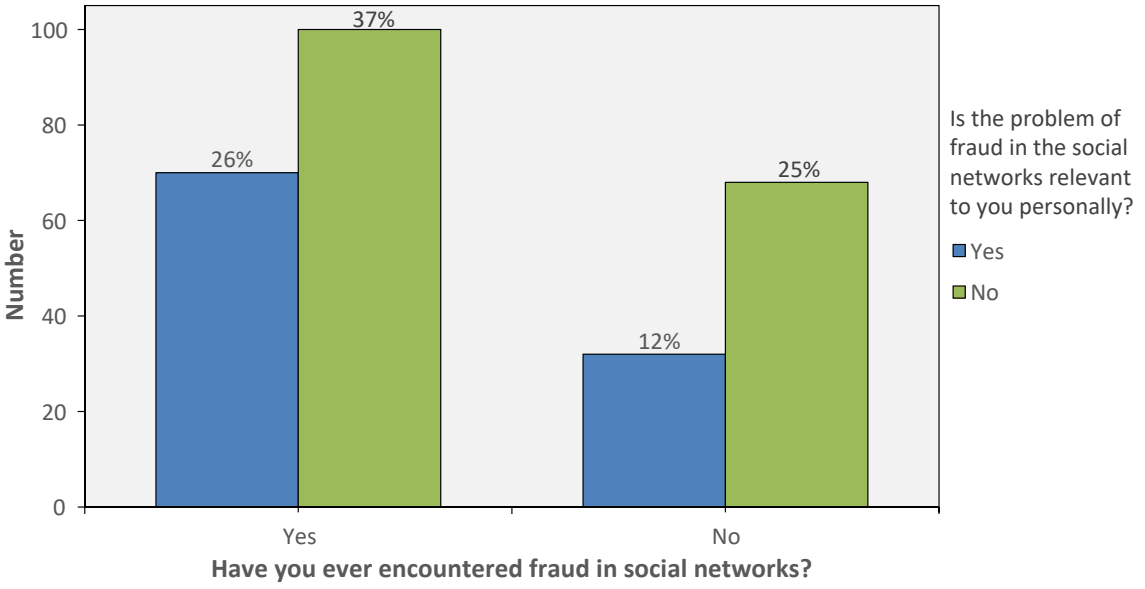
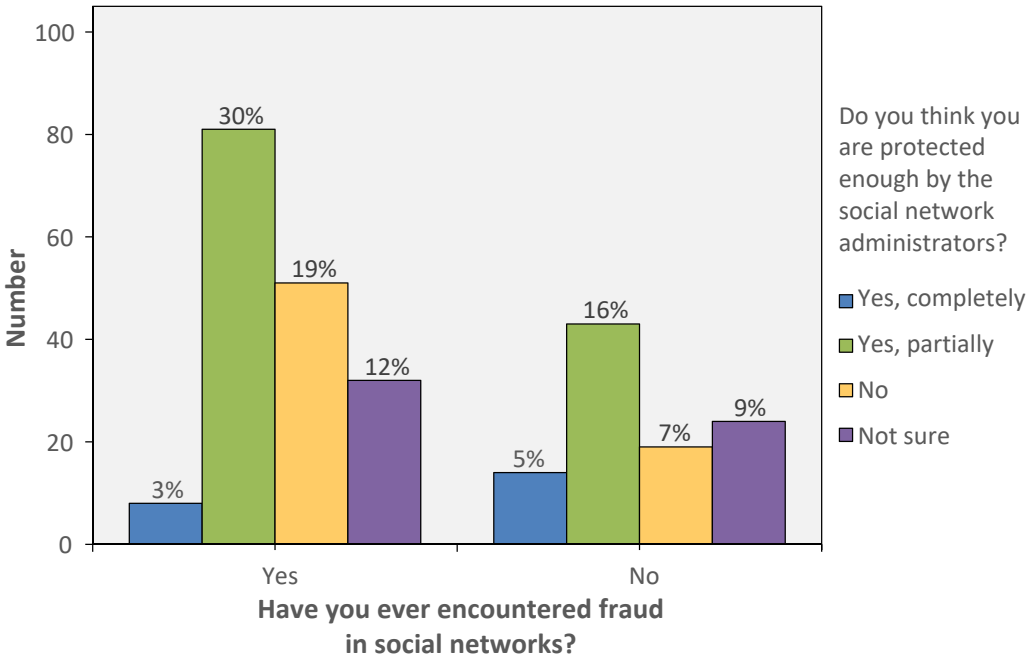


Fig. 10. Distribution of the sense of security according to the personal experience of users



CONCLUSION

Social networking sites are becoming an integral part of people's lives. Their importance is continuously growing in all spheres of modern social life. However, the influence of social networks on social development remains ambiguous. On the one hand, online networks facilitate active communication between people, rapid transfer of information and access to the resources necessary for the successful life of the individual and meeting his/her needs. On the other hand, virtual communication is different from the real one. It is less subject to control and regulation, which can give rise to all sorts of risks and threats associated with the loss of personal data and formation of various deviant behavior patterns in individuals.

Interaction on social networking sites remains one of the most unprotected types of human relationships, creating ever new security threats, both technical and, to a greater extent, man-made. Despite the development of technology and knowledge society, the overall level of erudition and education, which should be increasing every year, is not high enough. At the moment not all social network users are competent in the field of information literacy and personal data protection. Many of them do not consider it necessary to restrict public access to their personal information which can be used by criminals for gaining money profit or against the owners themselves. In addition, a large number of the users believe online fraud and overall cyber security do not have anything to do with them personally.

Computer fraud today is massive; and in most cases fraudulent actions through direct interaction with the user mean the attacker's expected outcome will be positive. Fraud on social networking sites develops dynamically, is geographically distributed and has a latent character, which makes legal regulation difficult and forces the average user to take full responsibility for protecting their own personal data and finances.

REFERENCES

1. Boyd D. M., Ellison N. B. 2008. "Social network sites: definition, history, and scholarship". Journal of Computer-Mediated Communication, no 13, pp. 210-230.
2. Doctrine of Information Security of the Russian Federation (approved by the RF President's Decree No 646 of 5 December 2016). [In Russian]
3. Dremlyuga R. I. 2008. Internet Crime. Vladivostok: Izdatelstvo Dalnevostochnogo universiteta. [In Russian]
4. Efimov E. G. 2015. Social Internet Networks (Research Methodology and Practice). Volgograd: Volgogradskoye nauchnoye izdatelstvo. [In Russian]
5. Fielding N. G., Lee R. M., Blank G. (eds.). 2008. Sage Handbook of Online Research Methods. Thousand Oaks, CA: Sage. DOI: 10.4135/9780857020055
6. Fomina N. A. 2015. "The use of social engineering methods for fraud in social networks". Proceedings of the Conference "Informatsionnaya bezopasnost' i voprosy profilaktiki kiber·ekstremizma sredi molodezhi" (9-12 October), pp. 443-453. [In Russian]
7. Hogan B. 2008. "Analysis of social networks on the Internet". In: Fielding N., Lee R. M. Blank G. (eds.). Sage Handbook of Online Research Methods. Thousand Oaks, CA: Sage.
8. Kolikov N. L. 2011. "Professional computer crime and fraud". Vestnik Yuzhno-Ural'skogo gosudarstvennogo universiteta. Seriya: Pravo, no 28, pp. 61-64. [In Russian]
9. Morozova A. A. 2017. "Social network: on the issue of user security". Znak: problemnoye pole mediaobrazovaniya, no 3, pp. 201-205. [In Russian]
10. Nenashev S. M. 2016. "Information-technological and information-psychological safety of the user of social networks". Voprosy kiberbezopasnosti, no 5, pp. 65-72. [In Russian]
11. Nikitina I. A. 2010. "Financial fraud on the Internet". Vestnik Tomskogo gosudarstvennogo universiteta, pp. 122-124. [In Russian]
12. Selezenev R. S., Skripak E. I. 2013. "Social networks as a phenomenon of the information society and specificity of social connections in their environment". Vestnik Kemerovskogo gosudarstvennogo universiteta, no 2 (54), pp. 125-131. [In Russian]
13. Sergeeva Yu. "Social networks in 2018: global studies". https://www.web-canape.ru/business/socialnye-seti-v-2018-godu-globalnoe-issledovanie/ [In Russian]
14. Shilkina N. E. 2014. "What is the difference between a 'careerist' and a 'killer'? Social adaptation in a computer-simulated virtual world". Kazanskaya nauka, no 1, pp. 266-268. [In Russian]
15. Vinnik D. V. 2012. "Social networks as a phenomenon of the organization of society: the essence and approaches to the use and monitoring". Filosofiya nauki, no 4 (55), pp. 110-126. [In Russian]
16. VKontakte. "Users' catalogue". https://vk.com/catalog.php [In Russian]