KnE Social Sciences

XXIII International Conference
Culture, Personality, Society in the Conditions of Digitalization:
Methodology and Experience of Empirical Research Conference
Volume 2020

Knowledge E
enriching | engaging | empowering

Conference Paper

Paternalism and Self-Reliance on Personal Security in the Information and Communication Environment

A. A. Krivoukhov

Kursk State Agricultural Academy named after I.I. Ivanov, Kursk, Russian Federation

Abstract

The research is devoted to the study of the personal security level in the information and communication environment. The purpose of this work is to determine the citizens' subjective opinion about the information security level in the information and communication environment and the role of the state in these processes. The study is based on data of sociological survey conducted in 2019 among the population of the Kursk region as a subject of the Russian Federation. The sample included 1000 respondents aged 16 and over living in urban and rural settlements in the region. Based on the understanding of the information and communication environment as an anthropo- sociotechnical phenomenon, the author concludes that personality is one of the key elements of information security in the triad (man — communications — technology). The study has fixed that users assess their life in the information and communication environment as dangerous. But at the same time, despite the fact that citizens face with the attackers' actions, a significant part of them are in no hurry to recognize the Internet as criminal. The study has determined that issues of personal cybersecurity and self-reliance prevail over paternalism. Network users should not only be aware of possible types and schemes of fraud, but also of software protection methods and anti-virus products.

Keywords: information and communication environment, cybercrime, personal cybersecurity, information and telecommunication technologies, state.

Corresponding Author:
A. A. Krivoukhov
anatka@rambler.ru

Published: 21 January 2021

Publishing services provided by Knowledge E

Selection and Peer-review under the responsibility of the XXIII International Conference Conference Committee.

1. Introduction

Universal informatization has significantly increased the dependence of the society effectiveness on the condition of the information and communication environment. The intensification and globalization of information interactions dictate different requirements for the security of the information and communication environment, which updates the urgent need for in-depth scientific analysis of the security problem in the environment.

The information and communication environment is a poorly structured system in which a plurality of citizens carry out joint activities in the storage, transfer and processing of information through information and telecommunication technologies. At the same time, three sides can be distinguished in the structural organization of this environment [2]. The first side is the technical side that reflects the capabilities of computer systems for registering, recording, processing and transmitting information. The second one is socio-cultural, reflecting the movement of knowledge and cultural meanings in the system of technically mediated social communications. And finally, the third notion is man himself / herself.

Therefore, it can be argued that this environment has an anthropological and sociotechnical character, since it consists of people, social communications, and information and telecommunications technologies. All its elements complement each other. This makes it possible to consider the security of the information and communication environment as the individual's security, the security of communications and the security of information and telecommunication technologies.

It should be noted that the key problem should be recognized as the problem of respect for the individual's interests in the information and communication environment. The interests of the individual should include the exercise of his or her constitutional rights of information access, the use of information for the purpose of carrying out activities not prohibited by law, physical, spiritual and intellectual development, as well as the protection of information ensuring personal security [1, 5, 6]. Therefore, the concept of information security of the individual seems reasonable to highlight (more precisely — separate from the general) the concept of information security, shifting the emphasis on the issue of personal security when specifying the concept.

Under the individual cybersecurity should be understood as the state and condition of the individual's life, in which there is a lack of or minimized threat of harm to the private space of the individual's communications and the information that he possesses.

It is the sociological analysis of personal cybersecurity in modern conditions that becomes the most important need of the scientific society. The purpose of this work is to determine the citizens 'subjective opinion about the level of cybersecurity in the information and communication environment and the role of the state in ensuring it.

2. Methodology and Methods

The survey was conducted among the population of the Kursk region as the median subject of the Russian Federation in terms of Informatization. In the course of the survey,

1000 respondents were surveyed, with quotas based on gender, age, and place of residence. The results of the study were systematized and analyzed.

3. Results and Discussion

According to the survey, respondents generally note (see Figure 1) that as a result of the introduction of information and telecommunication technologies their life's activity becomes more dangerous or more dangerous in modern society (as 17.6% respondents and 40.1% respondents, respectively).

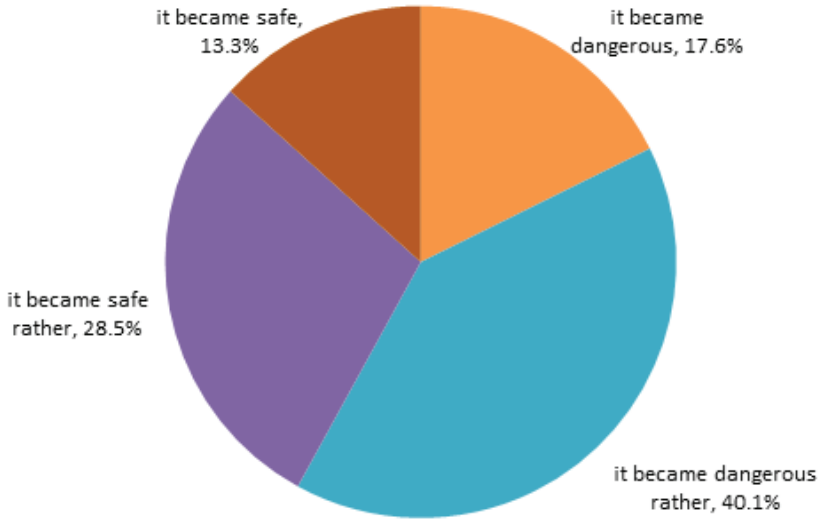

Figure 1: Respondents' opinion on their Life's activity in modern society due to the introduction of information and telecommunication technologies

Note: Without taking into account the position "Not sure".

The change in feelings of personal security in the information and communication environment in recent years is presented in Figure 2.

For 38.3% of the respondents in the region there is an increase in the feeling of insecurity in the information and communication environment. At the same time, the loss of sense of security on the Internet can be related to the fact that it becomes a breeding ground of crime [6]. The Internet not only increases the efficiency of human activity, but also creates a new electronic platform for cybercrime as a spectrum of crimes implemented through information and telecommunication technologies in cyberspace [5]. On object of the offense researches allocate the following groups of cybercrimes [7]: computer crimes against the personal rights and inviolability of the private sphere, economic computer crimes, computer crimes against public and state interests. In this

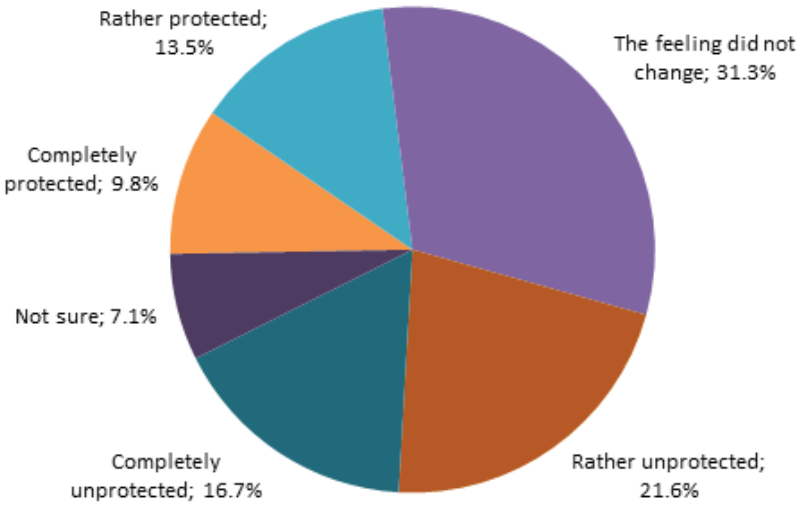

Figure 2: Respondents' opinion on the question referring to their sense of personal security in the information and communication environment, in %

classification, computer crimes against personal rights and privacy are of interest for research purposes.

Our survey has shown that today a certain part of the population has faced such crimes. As can be seen from the data of Table 1, citizens are most often faced with spam, that is, with sending correspondence to persons who have not expressed a desire to receive it. Such information is advertising most often, but the anonymity of spam creates ideal conditions for various kinds of fraud. For example, intruders send spam that lures money from trusting e-mailbox users.

The second highest incidence is viruses that block a browser or computer. 78.7% of respondents note this problem. Finally, in third to fourth place is phishing (as an attempt to unauthorized access to logins and passwords) and its particular case — breaking and stealing pages on social networks.

But at the same time, the survey data do not allow us to attribute crime in the information and communication environment to the key problems of personal security (Figure 4). In General, 51.4% of respondents feel protected from criminal attacks when working on the Internet (14.2% completely and 37.2% partially), while 36.6% do not feel protected from crime in the Network (10.1% completely and 26.5% partially).

In today's society, the problems of personal cybersecurity do not put on the back burner, just the Internet user learns to live in conditions of constant information threats. This provision is confirmed by the distribution of respondents' opinions on who should ensure human security in the information and telecommunications environment (Figure 5). More than 2/3 of respondents believe that everyone should take care of their own security on the Internet and social networks.

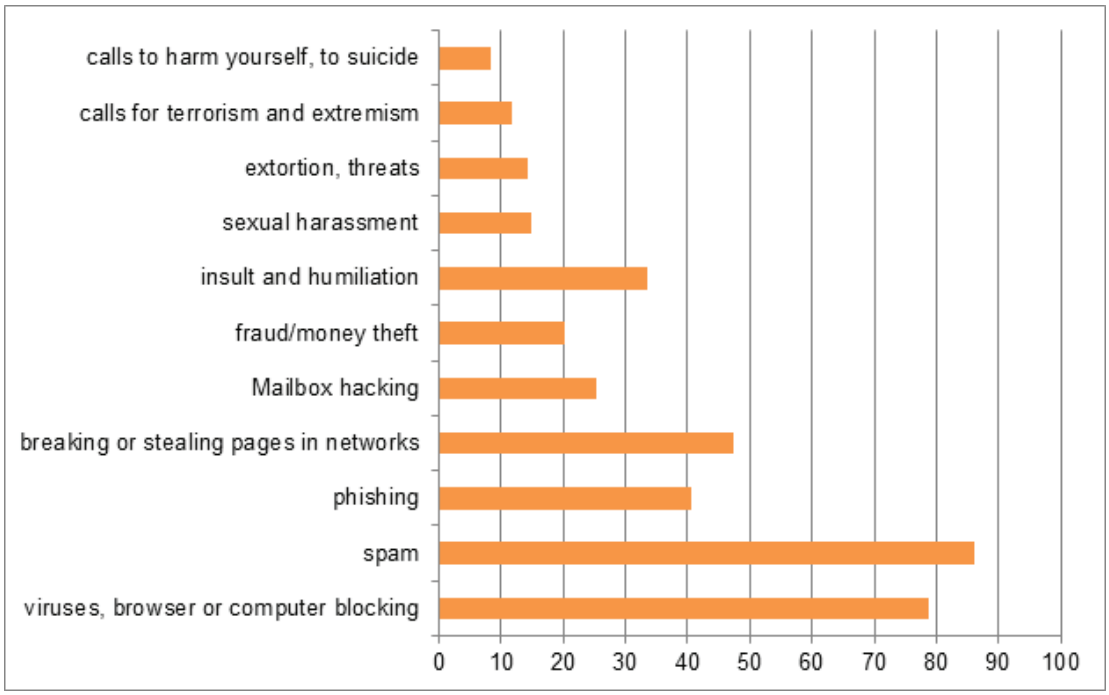

Figure 3: Respondents' opinion on the question referring their practice of using Internet resources, in %

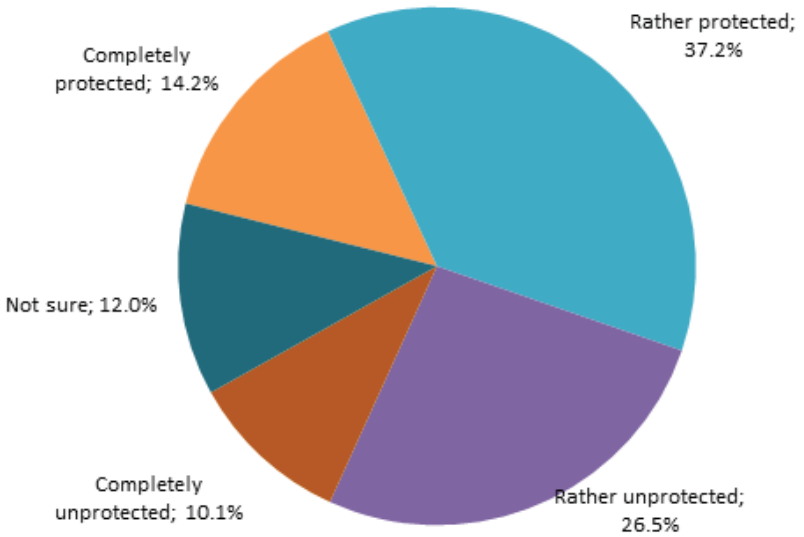

Figure 4: Respondents' opinion on their feel of protection or exposure to criminal attacks when working on the Internet generally, in %

Under these conditions, it is up to the user to have a concept of information security and its means of providing it. Users of the network should not only be aware of possible types and schemes of fraud, but also methods of software protection, anti-virus products, as well as timely updating of all applications, browsers and systems.

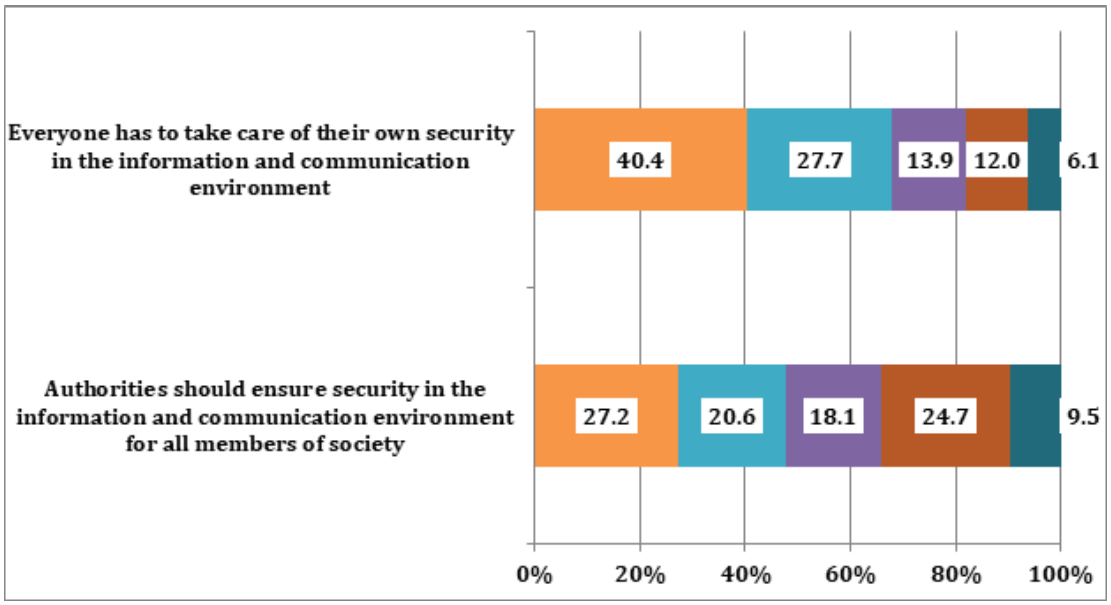

Figure 5: Respondents' opinion on citizens' safety in the information and telecommunications environment

4. Conclusions

Unfortunately, if the information and communication environment is considered as an anthropological and sociotechnical system, its weakest link is the terminal user. Assessment of information security, obtained during a survey of the population, allows us to conclude that users evaluate life's activity in modern society as dangerous. But at the same time, despite the fact that a significant part of the population fell under the influence of cybercriminals, the latter is in no hurry to recognize the Internet as criminal and blames the person for network security.

This study has fixed that citizens are ready to live in conditions of increasing risks and threats in the information and communication environment. In these conditions, the state can take upon itself the financing of the process to improve the tools for ensuring the personal cybersecurity. And since the successful use of such tools is associated with the end user, who must have the skills to use them, another state task is the formation of appropriate competence through the education system, including further education.

References

[1] Krivoukhov, A. A. (2018). Assessment of Information Security of the Internet Environment by the Users of Social Networks. *Communicology (Russia),* vol. 6, issue 1, pp. 107-117.

[2] Krivoukhov, A. A. and Zotov. V.V. (2017). Information Security as Anthroposociotechnical Phenomenon. *Communicology (Russia)*, vol. 2, issue 2, p. 71-81.

[3] Nomokonov, V. A. and Tropina, T. L. (2012). Cybercrime as a New Criminal Threat. *Criminology: Yesterday, Today, Tomorrow*, vol. 1, issue 24, pp. 45-55.

[4] Serieva, M. M. (2017). Cybercrime as a New Criminal Threat. *New Law Gazette,* vol. 1, pp. 104-106.

[5] Shoricheva, A. Y. (2014). Information Security of a Person in a Communication Network. *Innovative Technologies: Theory, Tools, Practice*, vol. 2, pp. 180-182.

[6] Tereshov, A. V. and Tereshova, O. A. (2016, May). Modern Problems of Ensuring Information Security of the Person on the Internet. Presented at *Problems of Combating Cybercrime in Modern Society: Collection of Materials of the First All-Russian Conference*. Tambov: Publishing House of Pershina R.V., pp. 23-28.

[7] Zhang, K., Zhao, L. and Cao, H. Q. (2014). Research on the Computer Network Crime and Information Security. *Applied Mechanics and Materials*, vol. 687-691, pp. 1806-1809.