

The role of social engineering in modern Russian society

K.P. Stozhko^{1,*}, *D.K. Stozhko*², *A.V. Shilovtsev*^{1,3}, *S.N. Nekrasov*¹ and *T.N. Makarova*¹

¹ FSBEI HE Ural State Agrarian University, city of Yekaterinburg, Russia

² FSBEI HE Ural State University of Economics, city of Yekaterinburg, Russia

³ FSBEI HE Ural Federal University named after the first President of Russia B.N. Yeltsin

Abstract. The article analyzes the role and content of modern social engineering in the conditions of increasing macroeconomic instability and the spread of unfair competition. The reasons for the development of the negative nature and orientation of modern social engineering technologies are revealed. The theses on the expediency of considering social engineering in "broad" and "narrow" meanings, as well as on the development of "special social engineering" and its techniques as carrying asocial or antisocial content are put forward and substantiated. Recommendations are formulated to ensure the necessary level of information security of economic entities.

1 Introduction

Modern society is at the same time an "information society" (Zh. Baudrillard) and "risk society" (U. Beck). The role of information technology is only increasing over time, as evidenced by the emergence and spread of so-called social engineering technologies. In the context of the global socio-economic crisis and steadily growing political and macroeconomic turbulence, the role, nature, and content of social engineering are changing significantly, which is increasingly turning from a constructive mechanism of social interaction into another kind of unfair competition.

The purpose of this study is to identify and assess the causes and factors of the transformation of the nature and content of modern social engineering in conditions of growing social instability and uncertainty.

The research objectives are: first, to determine the essence of social engineering in a "broad" and "narrow" meaning; second, to identify the format of special social engineering as carrying negative social content; third, to substantiate the need to study social engineering techniques in courses on information security, social communications, and social psychology in high school.

* Corresponding author: a.shilovtsev@mail.ru

2 Materials and Methods

The study uses structural-functional and program-target approaches, methods of analysis, synthesis, axiology, and hermeneutics to study problematic issues of the state and organization of modern social engineering.

3 Research results

It is legitimate to consider the term "social engineering" in a "broad" and "narrow" sense. In a "broad" sense, social engineering is an "interdisciplinary scientific and practical activity of people associated with the formation and transformation of systems of different complexity levels" [1]. Nevertheless, in any particular case, such formation and transformation acquires its own objectivity and character. There are, for example, different directions, methods, and levels of social engineering [2; 3; 4]. In addition, in the conditions of a particular society and within the framework of a specific historical stage of its development, social engineering acquires its own special features and reflects the main ideological, cultural, political and economic features of the current moment.

Thus, the phenomenon of social engineering becomes concrete and for its realistic and adequate understanding should be considered in a near sense. Just as more general concepts are represented in more specific concepts (music in a symphony, sonata, sonatina, fugues; furniture in tables, chairs, beds, deck chairs, etc.), social engineering can be represented in its strict sense in the form of special social engineering, which alone, if it is considered in the context of information security, it refers to psychological manipulation of people to collect information, fraud, or gain access to the system [5].

The variety of modern forms of social engineering is quite wide. Among its relatively new (innovative) forms in the economy there are such as *outsourcing*, *outstaffing*, *blockchain*, *insourcing*, *crowdfunding*, *crowdivesting*, *crowdlending*, *crowdstaffing*, *crowdtesting*, *crowdsourcing*, *catering*, *freelancing*, etc. In the educational sphere, coaching, case studies, trainings, asphatronics, synectics, bricolage, heutagogy, etc. can be noted. In the field of social relations, mobbing, bullying, hype, standing, etc. But the most innovative forms of social engineering are in computer science, which is due to digitalization and modern scientific and technological revolution. In each subject area, social engineering acquires its own specific innovative forms.

At the same time, the main task of social engineering remains to change a specific system for the purposes of either the system itself or an external (third-party) customer of such changes, as which the system may not act. Hence, it is legitimate to distinguish two main archetypes of social engineering: endogenous (organic) one, conditioned by the internal needs of the transformed system and based on regulatory regulation; and exogenous one, i.e. artificial, determined by external factors and organized with violations of nominative legal requirements. The latter archetype is dominant in the conditions of growing political, macroeconomic, cultural, and ideological instability and uncertainty and the spread of unfair social competition. This, in turn, leads to a violation of the entire system of social security in society: informational, economic, environmental, political, etc.

Among the most obvious factors contributing to the spread of negative content of modern social engineering, the following can be named:

- deepening of socio-economic inequality in modern society, drop in real incomes of the population, which causes a desire on the part of certain individuals to solve their problems by criminal means;
- development of information and digital technologies, automation and computerization, thanks to which new technical tools for criminal actions of individual "social engineers" appear;

- regime of self-isolation of the population in the conditions of Covid-pandemic, contributing to the weakening of vigilance and caution of citizens in communicating with unknown persons – subjects of social engineering;

- insufficient level of control by the state (in particular, the "K" Department of the Ministry of Internal Affairs of the Russian Federation) in the information services market, including the work of the main services and actors, as evidenced by the steady growth of cybercrimes: 11 thousand in 2014, 66 thousand in 2016, 180 thousand in 2019, 320 thousand for the first 7 months of 2021 [6].

- insufficient level of effectiveness of protective means offered on the Russian information market by the main developers (Kaspersky Lab, Anti-Phishing, System Software, etc.).

Although the effectiveness of security measures to protect confidential information increases over time, people nevertheless remain susceptible to manipulation, the human factor remains the weakest link. Just as in the well-known model – the "Karpman triangle", three participants function – the victim, the chaser, the rescuer, something similar happens in the information space. The aggressor (the persecutor) chooses a victim and puts a chaser on her; the victim feels helpless and either gives up or expects help from the outside. The rescuer (the state) is either unable to help her in a timely manner, or provides inadequate assistance, which is why his role is not fully realized. Thus, in this model of relations, their intoxication occurs, which leads to a social balance violation.

This is also facilitated by the widespread practice of manipulation of public and personal people consciousness, which has developed in recent decades due to the spread of unfair competition: outright lies, discrediting, destruction of symbols, policy of silence, information asymmetry, destruction of morality core, etc. [7, p.511]

Considered more generally, from the management point of view, especially Event-management, social engineering is a whole set of organizational and practical measures to form a new reality in which the person is most often assigned the role of a blind performer or an ordinary consumer. For him, all issues, from catering, training, career advancement, and ending with family planning issues are solved by external actors – specialized institutions (companies).

Thus, modern Event-management is directly connected not only with the positive events of our life, but also with the negative events that often happen to us. Understanding the nature, character, and possibilities of managing such events is an important element of Event-management.

The most important aspect for a full-scale and adequate understanding here is the fact that on the basis of social engineering, the so-called unreal sector has formed in the Russian economy, which has its own unreal economic environment and specific (very far from market) ways and methods of competition: economic espionage, practice of "hit-and-run", black PR, various "setups" [8, p.69]. This can also include price discrimination, raiding, lobbying, counterfeiting, logrolling, racketeering, cartelization, redistribution, smuggling, etc.

The problems of modern social engineering are actively discussed in modern literature. It is the subject of research by both Russian [9; 10; 11] and foreign authors [12; 13; 14].

Unfortunately, under the conditions of unfair competition and a high monopolism level of the Russian economy, social engineering turns out to be a negative rather than a positive factor [15; 16]. While the security services of corporations and various institutions install new antivirus software, develop a complex identification and authentication system, attackers penetrate the network with the help of insiders, employees of educational organizations, as well as unsuspecting students.

When accessing the network, one of the most popular hacking mechanisms is used, which can be defined as *special social engineering*, and to which, so far, they pay clearly

insufficient attention. Special social engineering is formed on the basis of personalized (targeted) management (manipulation) of a person when his personal qualities, strengths, and weaknesses, personal data are used (considered and taken into development). This is done by third parties (usually anonymous or fake) to achieve their desired goals: fear, curiosity, greed, superiority, generosity, pity, gullibility, laziness, etc. – everything goes into business for the sake of profit, revenue, income at the expense and to the detriment of the "victim". Although all methods of social engineering are based on specific parameters of human character and are a prerequisite for making certain managerial decisions, special social engineering has a special focus: it abuses the information received (often simply by illegal means) and turns the weaknesses of potential customers to the service of third parties and to the detriment of the customers.

Carrying out a kind of diagnostics and forecasting, a specialist in social engineering methodologies, as it were, constructs a scenario of his behavior, which is based on the principle of freedom from responsibility. But if a doctor, a teacher, or an author of a literary work are personally responsible for their actions and for the quality of their product, then a "social engineer" acting on the condition of anonymity frees himself from such responsibility. Thus, his activities turned out to be in the field of the "shadow economy" and are often of a criminal nature or a "gray schemes" nature.

The negative aspects of such special social engineering were especially widely seen and felt by Russian citizens during the Covid-pandemic, when telephone fraud increased exponentially, frankly false advertising flourished, and all sorts of "standing" and "hype" became fashionable. In conditions of self-isolation, many categories of citizens, especially the elderly ones (pensioners, sick people, disabled, etc.) have changed certain types of their activities and their habits. But, most importantly, they also turned out to be in a certain distorted and modified information environment, in which the traditional informing of the population has increasingly been subjected to new tests of strength by the so-called "specialists" in social engineering. It comes to the point that people sometimes do not know who should pay for housing and communal services, open the doors of their apartments to service gas equipment, etc. In such conditions, people's social well-being suffers, their social security, self-esteem, and self-identification decrease. Society as a whole is being irreparably harmed.

Special social engineering is the most severe type of various kinds of information attacks on a person, regarding protection against them. The person is not able to be completely protected from such attacks only by hardware or software. Intrusive calls, numerous letters to an email address, SMS messages, sometimes with threats (for example, to initiate criminal prosecution and transfer materials to court for an imaginary debt or to terminate utilities for a minor delay in paying for housing and communal services, etc.) – all this is not just evidence of the lack of economic culture of specific economic entities, but also the result of their use of special social engineering (technologies of suggestion, zombification, recruitment, manipulation of consciousness). People are first scared, then "warned up", then they make some "guiding hints", then they offer "help". And all the fraudulent chains of the so-called "*special social engineering*" are closed. As a result, a person either loses money, remains without funds, or faces a deterioration in health, and in the "easiest" case - reputational losses, becomes a mock, etc.

Successful protection against such "special social engineering" requires the state and society to organize a unified system of effective information security, starting with the security policy at enterprises, organizations, and institutions, security in the content of various kinds of "guidance documents" (orders, directions, job descriptions, etc.), and ending with the assessment of vulnerability, risk, threats to specific categories of citizens, specific officials.

It is known that "if you're drowning, you're on your own". In the conditions of the Covid pandemic, independent (initiative) civil (public) mutual assistance groups organized by employees of a particular enterprise, residents of a particular microdistrict, village, apartment building, etc. can play a special role. Of course, special state social institutions, which role in extreme conditions is higher than ever before [17, p.37].

We have to admit that currently up to 30% of all hacking and illegal use of personal data of citizens comes from "outsiders", i.e. from people who do not work in the organization. This means that 70% of violators are inside the organization. They are the ones who prepare their recommendations on "social engineering" for corporate management: for example, they offer to conduct face-to-face training sessions in educational institutions in conditions of the spread of a new coronavirus strain "Omicron", or they either demand or cancel the practice of QR codes. All this happens in the absence of strict personal responsibility for such initiators and "activists".

Today, social engineering is recognized as one of the greatest threats to social (economic, informational, reputational, and other) security facing organizations. If successful, many social engineering attacks allow attackers to gain legitimate, authorized access to confidential information and cause sometimes irreparable damage to organizations and their employees. Among the most common techniques of modern special social engineering, we note such as *pretexting*, *phishing*, *vishing*, *farming*, *exchaining*, *Trojan horse*, *road apple*, *reverse social engineering*, *garbage analysis*, *collecting information from open sources*, etc. Almost all of these technologies are criminal or semi-criminal. For example, a "road apple" is an attack in which attackers stick a company logo on a physical medium (pre-infected), leave it in places frequented by employees, and wait for the victim to find it. An employee can find it and insert it into the computer or return it to the company.

There are other techniques of social engineering: *instant messaging systems*, *visual contact*, *"personal" approaches*, *"pump-and-pump"*, *"type-squatting"*, etc., the appearance of which is associated with the regime of self-isolation and the general increase in the volume of information attacks on private and legal entities [18, p.61]. According to official data, social engineering accounts for up to 83.3% of the total number of information attacks on individuals in the Russian Federation [19].

4 Conclusions

Modern social engineering has long moved to the Internet. At the same time, the peculiarities of the behavior of social managers and consumers in the Internet environment were formed. A wide variety of Internet platforms and online wallet services serve as a tool for a variety of modern social engineering technologies, as well as for the promotion and commercialization of innovative goods and services [20, pp.67-68]. A wide arsenal of special social engineering indicates that organization and special training are needed to counteract its techniques and methods in educational institutions. Courses on "information security", "social management", "social psychology", "communication" (communication techniques), etc. can contribute to the formation of a higher level of social competencies of students, their stress resistance and high-quality preparation for successful work in an active and even aggressive social environment. This, by the way, corresponds to the decision of the Ministry of Education of the Russian Federation on the introduction of courses in the educational process to improve the information literacy of students [21].

Another important direction in regulating the content and role of social engineering is the improvement of the legislative framework, including Russian laws: FZ-98 "On Trade Secrets" (2004), FZ-149 "On Information, Information Technologies and Information Protection" (2006), FZ-152 "On Personal Data Protection" (2006), etc. Here, the most

relevant are the strengthening of technological control by the state over the work of subjects of social engineering and the tightening of administrative and criminal responsibility against the latter for illegal actions.

It is still considered almost impossible to completely protect yourself from social engineering attacks, but it is possible to minimize threats and risks on its part. To do this, you need to follow some rules, thanks to which you can achieve very high results, and which are as follows:

1. Constantly study and apply new and more advanced methods of information protection to strengthen information security.
2. Follow a certain behavior scenario in which to increase your vigilance, accuracy, responsibility and not trust outsiders.
3. Do not disclose confidential information by phone or email, unless it is prescribed in the security policy.
4. Properly handle documents and physical media in accordance with the instructions and protocol.

Together, work in these areas will reduce the negative content of modern social engineering and the practice of unfair actions of information services market participants.

References

1. A.V. Veselov, Social engineering: the essence and paradigm methodology. Autoref. diss. cand. ph. scien. 09.00.11. Moscow: MGIU, 32 (2012)
2. S.P. Teplyakov, A.S. Timokhovich, Social engineering. Analysis and methods of protection, Academy, **7(34)**, (2018) URL: <https://cyberleninka.ru/article/n/sotsialnaya-inzheneriya-analiz-i-metody-zaschity>
3. E.N. Volkov, Human transformation: critical reflection of social engineering versus naive reflexivity of trust in oneself and "one's own", Transformation of human potential in the context of the century. Materials of the III All-Russian Scientific Forum "Science of the future – the science of the young". Nizh. Novgorod, Publishing House of NISOC, 229-233 (2017)
4. O.A. Urzha, Social engineering as a methodology of management activity, Sociological research, **10**, 87-96 (2017)
5. O.G. Laminina, Possibilities of social engineering in information technologies, Humanities, socio-economic and social sciences, 2 (2017) <https://cyberleninka.ru/article/n/vozmozhnosti-sotsialnoy-inzhenerii-v-informatsionnyh-tehnologiyah/viewer>
6. The number of cybercrimes in Russia <https://www.tadviser.ru/index.php>
7. S.G. Kara-Murza, Manipulation of consciousness, Moscow: Eksmo, 832 (2005)
8. O.S. Cheremnykh, S.V. Cheremnykh, Strategic management: a process-cost approach to business management, Moscow: Finance and Statistics, 736 (2005)
9. V.A. Achkasova, M.V. Metkin, Public relations as social engineering, Moscow: Yurayt (2021) <https://www.ozon.ru/product/svyazi-s-obshchestvennostyu-kak-sotsialnaya-inzheneriya-2-e-izd-ispr-i-dop-uchebnik-dlya-141367305/?sh=wHW8awAAAA>
10. M. Kuznetsov, I. Simdyanov, Social engineering and social hackers, St. Petersburg: BHV-Petersburg, 358, (2007)
11. M.O. Yangaeva, Social engineering as a way of committing cybercrimes, Bulletin of the Siberian

12. K.D. Mitnik, V.L. Saimon, *The Art of Deception: translated from English*, Moscow: Ai-Ti Company, 360 (2004)
13. K.D. Mitnik, V.L. Saimon, *The ghost is online. Memoirs of the greatest hacker: translated from English*, Moscow: Eksmo, 416 (2012)
14. K.D. Mitnik, V.L. Saimon, *The Art of Invasion: translated from English*, Moscow: DMK-Press, 280 (2005)
15. N. Artemov, *Social engineering – hacking technology* <https://emisare.medium.com/socialnaya-ingeneria-9f16e0ba7fa5>
16. *What is social engineering: history, methods* <http://www.reg.ru/blog/chto-takoe-sotsialnaya-inzheneriya/>
17. D.A. Bistyakina, T.V. Solovyova, E.G. Pankova, *Social well-being of elderly people during the self-isolation regime*, *Social policy and Sociology*, **19(3 (136))**, 33-39 (2020)
18. V.Yu. Yevglevsky, M.M. Putyato, A.S. Makaryan, I.V. Volodin, *Research of social engineering mechanisms and analysis of counteraction methods*, *Scientific works of the Kuban State Technical University*, **2**, 57-68 (2021)
19. *Actual cyber threats* <https://www.ptsecurity.com/ru-ru/research/analytics/cybersecurity-threatscape-2020-q2/>
20. V.G. Boikov, *Marketing features of the promotion of innovative products on Internet sites, Economy: yesterday, today. Tomorrow*, **7(3A)**, 64-74 (2017)
21. *Russian schools will supplement the lessons of Health and Safety with courses on cybersecurity* <https://4pda.ru/2020/01/09/366366/>