Social engineering in the context of ensuring information security

1 Introduction

The practice of human-machine interaction (HMI) makes increasingly high demands on the level of information security. This process is like an eternal dispute - what is stronger, a sword or a shield. The evolution of information protection methods reflects the evolution of unauthorized data access methods [1].

Nowadays people are actively embedding computers in their environment; they are trying to make the computer more "human", the level of computer dependence on the outside world also increases with the development of networks [2, 3]. On the other hand, the human factor continues to be the least controlled element of HMI [4], which, in turn, according to the modern information and communication technologies development creates not only new opportunities, but also new risks [5]. As a result, the number of information security [6] vulnerability factors increases.

Someday, a computer will learn how to evaluate human behavior [7,8] and make decisions based on the results of cognitive processes analysis, considering the value and semantic aspects of personality behavior. Consequently, we are waiting for a new evolutionary leap in the confrontation of "sword and shield". But, so long as a person is only understandable by the other person, the social engineering knowledge will be in demand [9].

2Introduction to the problem

A review of research papers on the research topic showed that the theoretical, methodological and applied aspects of the problem of social engineering evolved in a certain way.

First, it should be recognized that the attitude towards the threat of social engineering has radically changed. Previously, there was a trend of systematically increasing the protective and preventive potential of corporate IT systems. This trend was a response to a threat or breach of information security. Therefore, remedies were actively developed, as well as means to prevent attacks and minimize the consequences of the social engineer actions. Scientists generalized the trajectory of social engineering and classified actions of the social engineer. Thus, requirements for data transfer protocols and information security policy [Abraham, S; Mills, D], profile settings [Alim, S], software development and information systems architecture [Penserini, L] were formed. The social nature of information security threats is being actively studied [Dalpiaz, F], and means are proposed against the influence of the human factor [Luo, X], Pritchard, M]. As result, training programs, procedures and policies were formed. Approaches to testing information systems [Pavkovic`, N; Sandouka, H] and testing methodology [Dimkov, T] have been developed. As a result, various protection strategies [Gonzalez, J], user guides and practical scenarios [Jansson, K; Kampthan, P.] were developed. Social engineering was considered as a fraudulent “low-tech” approach to the high-tech world of the Internet [Manske, K]. According to it, the social engineer exploited the vulnerabilities of the Internet environment, but human ethics and personality psychology were as before pressure points. However, this approach has evolved along with the evolution of the high-tech world of the Internet. On the one hand, the taxonomy of social engineering, as the practice of systematization of a complex system, remains the same - it still is and is perceived as a type of fraud. Three taxonomies are often used in literature: Cialdini’s principles of influence, Gragg’s psychological triggers, and Stajano’s principles of scams [Ferreira, A.]. Thus, we are now dealing with high-tech fraud, which is taking global forms. The social engineer manipulates the patterns of thinking in the digital environment, using data on the results of online interaction between users and group behavior, including cultural values

*

[Karamanian, A]. Methods of protection from social engineering also become global. An example is the use of machine learning to detect attacks in the results of identify questions, to commands, dialogs [Sawa, Y]. The effectiveness of the use of artificial intelligence to protect against social engineering depends on the work on the knowledge bases of cybersecurity in human capital, prototyping risks, environmental structuring [Aldawood, H].

It should also be noted that protection methods become gradient depending on the level and limit of attack [Kaushalya, S]. Modern protection methods are aimed at point and dosed counteraction [Fathollahi-Fard, A.] and characterize the tendency to save effort and meaningful actions to counteract social engineering. This tendency develops up to the acceptance as a variant of the norm social engineering within reasonable limits. Manipulations of lower categories in the hierarchy of social communities can be justified if they are understood as part of an individual obligation to participate in the community [Hatfield, J.].

Research on the social nature of social engineering has also evolved. If previously the personal qualities of the object (the victim) were put at the forefront in assessing the human factor, now the factor of openness of personal data is key when evaluating such social engineering methods as persuasion, fabrication and data collection [Tetri, P.]. Denoting data openness as a vulnerability, scientists complement it by pointing out the risks of networking, citing social networks as an example [Algarni, A.]. Spreading and infecting a botnet poses a threat to both users and the social network as a whole [Li, S.]. Thus, the object of social engineering is no longer a specific user, but the users of the entire social network.

Phishing technologies have also evolved [Bhakkta, R.; Krombholz, K; Gupta, S.]. This was facilitated by the development of collaboration formats (BYOD - bring your own device), which creates prerequisites for attacks such as phishing, and a variety of communication tools, which increases the risks of network attacks, in particular, the creation fake versions of existing web pages or phishing emails.

3 Models and methods

Social engineering is a set of approaches of applied social sciences, or applied sociology, purposeful change of organizational structures positive aspect of the applied nature of social engineering is to increase the effectiveness of the control function in the human-machine interaction system. The result of the control function is commonly understood as an increase in labor productivity and

- fraud (fraud, breach of trust);
- crimes in the field of information technologies;
- dissemination of unlawful information;
- malicious interference through computer networks in the work of various systems. As a result, access to information that is protected, confidential and closed will be considered. We specifically operate with criminal law1 categories in order to emphasize the unlawful (harmful) nature of the social engineer actions [12]. The question arises: is it right to call a subject a social engineer, who is using social engineering techniques for his own benefit consciously and with understanding of the wrongfulness of his actions? After all, not every social engineer uses techniques to influence human behavior in this way. It may be appropriate to use other semantically close concepts associated with a breach of information security - a hacker or an information intelligence agent. However, by prioritizing the used techniques of social engineering and perceiving human-machine interaction as a conditional environment, in relation to (and not inside) which the subject carries out his actions, we identify this person as a social engineer.

The key features of a social engineer, regardless of the nature of his actions, are: conscious behavior, active mode of action, purposeful influence [11]. The area of impact is the human-machine interaction environment on which the social engineer makes organizational changes. Such changes are not carried out independently, but through the establishment of behavioral control over objects - a person, people, using their involvement in the environment of human-machine interaction. The object can be the information owner, the information producer, the user (consumer) or the information holder.

All the above describes an abstract category “social engineer”. The establishment of the unlawful (malicious) nature and consequences of the activity is possible through determining the target setting of the social engineer actions [13, 14]. In other words, determining why (for what purpose) a social engineer performs such actions, we will establish their character.

4 Results and discussion

Achieving the goals is determined by the method of access to the information when methods of human-machine interaction interested the social engineer directly or in connection with the person (persons), interacting with them. If the method of information access violates the status of protected, confidential, confidential information, the actions of the social engineer should be considered as unlawful.

1 Resolution of the Plenum of the Supreme Court of the Russian Federation of 30.11.2017 No. 48 "On judicial practice in cases of fraud, embezzlement and embezzlement"; "Guidelines for

*

We focus our attention on one provocative moment. If, as a result of applying methods of influence, a social engineer has gained access to confidential information, the analogue of which is publicly available, but using manipulating models of human behavior and is caused damage, his actions are illegal. However, if the damage did not cause, the actions of the social engineer do not violate the law, although it blame for non-compliance with ethics [15]. In a situation where a social engineer obtained (or made an attempt to obtain) access to confidential information, even without using it and not causing damage by his actions, the actions are unlawful due to the impact applied to the object [16].

To illustrate the qualifying attributes of social engineering, a matrix was drawn up by which it can be established in which combinations the actions of the social engineer are unlawful (harmful) in nature (Table 1). Filling out the

Table 1. Matrix of qualifying attributes of social engineering.

	Status "protected information": yes	Status "protected information": no	Status "access granted": yes	Status "access granted": no	The fact of "damage when gaining access": yes	The fact of "damage when gaining access": no	Status "information used": yes	Status "information used": no	The fact of "damage caused by using ": yes	The fact of "damage caused by using ": no
Status "protected information": yes	+		+	+	+	+	+	-	+	-
Status "protected information": no		-	-	-	+	-	+	-	+	-
Status "access granted": yes	+	-	+		+	+	+	-	+	
Status "access granted": no	+	-		-	+	-				
The fact of "damage when gaining access": yes	+	+	+	+	+		+	-	+	-
The fact of "damage when gaining access": no	+	-	+	-		-				
Status "information used": yes	+	+	+		+	+	+		+	+
Status "information used": no	-	-	-		-	-		-		
The fact of "damage caused by using ": yes	+	+	+		+		+		+	
The fact of "damage caused by using ": no	-	-	-		-		+		-	-

The results of qualification signs comparison showed that the most significant signs are the status of the information and the damage caused on accessing the information. To assess the impact effect of social engineers on the object the risk map was compiled. Table 2 presents the identified information security risks according to the results of the constructed scenario of a risk situation. The risk situation was modelled by determining the causal relationship between the actions of the social engineer and the response of a normally functioning security system in the organization. The identified risks are consolidated by stages of social engineering. Scenarios for the occurrence of a risk situation are ranked in

*

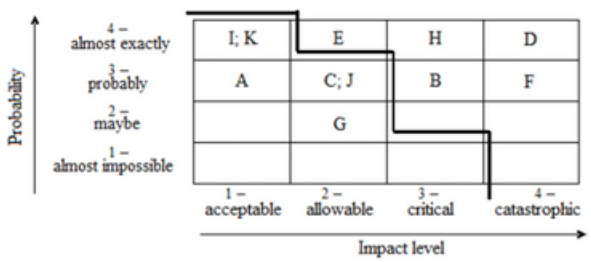
qualitative terms of "probability" and "impact" on the risk object dispersed in an ascending order.

Table 2. Distribution of information security risks from social engineer actions.

Name of the social engineering stage	Social engineer action	Ranking code
Preparatory stage	object data collection	A
	introduction to the area of the facility	B
	request for feedback from the object	C
	imposing actions on an object	D
Stage of access to the information	hacking devices	E
		F
	object action programming	G
	provocation	the H
Stage of using received information	commercialization of information received	
	distribution of malicious content	I
	interference with devices	systems, J
	dissemination of information	illegal K

Placing risks on the map (Figure 1) in accordance with the parameters of "probability" and "impact" is the final step of building a risk map and, at the same time, the starting point for the beginning of the operational risk management process.

As the risk map shows, the greatest threat to information security is created by the actions of a social engineer, activating the human factor and associated with the active actions of an object that has fallen under the influence of a social engineer. Above all at zone of risk is the protection of information access, the owner (holder) of which is the object of manipulation itself. If there is an element between the social engineer and data access where the human factor is minimized, then such risk situations are shown on the map below the risk tolerance limit. Such an element can be an authorized access system, a system of distributed access rights, a storage system, data updates, a data coding system, and so on. With respect to such risks, the information security system provides for the operation of algorithms that limit the capabilities of the social engineer or the effect of its impact. Although for this group of risks, the influence of the human factor should be taken into account.



By correcting the risk map fields due to changes in the initial data and practices of a particular organization, it is possible to increase the steadiness of the information security system to social engineering techniques.

Conclusion

The given results fit into the logic of the modern approach to social engineering and its global distribution - they are beyond the scope of management of corporate risk caused by the social engineer actions and the impact assessment on the psychology of the individual. It has been possible by shifting the focus from the object of social engineering to the subject - directly to the social engineer and the harmful nature of his

actions.

Consequently, the proposed solutions can be applied for assessing the threat of social engineering in the context of the vulnerability of the human factor, but without reference to a specific technology of social engineering.

The research was supported by grant of the President of the Russian Federation according to state support of leading scientific schools (grant № NSh-5449.2018.6).