doi: 10.31470/2309-1797-2019-26-1-199-215 UDC 81'23

Psycholinguistic Aspects of Humanitarian Component of Cybersecurity

Психолінгвістичні аспекти гуманітарного компоненту кібербезпеки

Yuliya Krylova-Grek
Ph.D. in Psychology,
Assistant Professor

Юлія Крилова-Грек
кандидат психологічних наук,
доцент

E-mail: doca123@ukr.net
orcid.org/0000-0002-2377-3781

Kyiv State University of Telecommunications
✉ 7, Solomyanska Str.,
Kyiv, Ukraine, 02000

Київський університет телекомунікації
✉ вул. Соломенська, 7,
Київ, Україна, 02000

Original manuscript received November 15, 2018
Revised manuscript accepted September 15, 2019

ABSTRACT

Introduction. *The paper focuses on language means exploited by social engineers in their activities in terms of humanitarian aspects of cybersecurity. The* ***goal*** *of this research is to analyze the methods and techniques employed by social engineers in their malicious activity and its features from a psycholinguistic point of view for further development of counteraction mechanisms.*

Methods. *To obtain results we used the following methods: primary source analysis, analysis of spoken and written speech and speech products, and intent analysis.*

Results. *The activity theory has been successfully applied to consider the key features of social engineers' work. On the base of AT we presented a three-component model which we may consider only in the case of a social engineer's successful attack (action).*

Based on the analysis of the sources, we distinguished the types of spoken and written communication actions (these types correspond to direct and indirect actions),

used by social engineers to affect the cognitive processes for retrieving «sensitive data» and confidential information. Besides, we also categorized psychological and language means, which social engineers evidently apply in their activities. We stress that in most cases social engineers' activities are aimed at a) affecting the person's emotions and feelings; b) blocking rational and critical thinking; c) manipulating moral and ethic values, and d) using positive incentives that have an interest to a user. Taking into account the abovementioned types of communication, psychological and language means, we systematized and described the general techniques of using oral and written forms of language and technologies: 1) techniques related to the use of spoken speech; 2) techniques related to the use of written speech; 3) techniques related to the use of USB flash drives, applications, and program software.
The findings are applicable for developing a mechanism to counter social engineers' attacks and contribute to improving the level of cyber literacy.

Key words: *psycholinguistics, spoken and written language, social engineering, cybersecurity, influence.*

Introduction

Psycholinguistics and its methods contribute to solving problems related to a wide range of issues, including the analysis of the humanitarian aspects of cybersecurity and social engineering. As a technique in communication, social engineering involves human interaction, manipulation, and persuasion through either oral or written communication to succeed in affecting a person's behavior. However, examining social engineering is not as simple as it looks. Since spoken and written language samples are one of the few materials available for the study, thus, in our opinion, psycholinguistics offer an important means for identifying speech patterns of an individual engaged in a social engineering activity, the impact on the behavior and consciousness of the object of attack and developing counteraction mechanisms against complex social engineering strategies.

Social engineering is one of the biggest challenges facing cybersecurity as it exploits the natural human tendency to trust. The annual reports and documents of the world's leading organizations and many experienced security experts emphasize the given fact According to statistics, social engineering attacks are on the rise, accounting for 43% of data breaches (Actual cyber threats – 2018. Trends and forecasts, https; UN Documents. Creation of a Global Culture of Cybersecurity:

Resolution Adopted by the General Assembly, http). It evidences the importance of comprehensive consideration of this issue and confirms the view that human factor still remains the weakest link of any security system (Yan et al., 2018).

The prevalence of social engineering methods can be explained by the fact that social engineers always take advantage of human emotions and psychology which are more vulnerable than protective technologies, so cyber criminals find it much easier to ain access to private data through communication than by breaking down the security system. In this regard, understanding the psycholinguistic aspects of cybersecurity is the basis for protecting sensitive data and practicing cyber defense tactics, even if a person is not a cybersecurity specialist.

Human-based social engineering attacks are sophisticated and hard to detect, making their study necessary. The abovementioned is a key reason to consider the social engineering-related psycholinguistic aspects of cybersecurity, which can be applied to develop counteracting and data protecting mechanisms.

Currently, a great deal of research from pedagogy, psychology, and philology has covered cybersecurity in humanitarian contexts. At the same time, psycholinguistic aspects of cybersecurity have never been investigated before.

V.Y. Bykov, O.Y. Burov, N.P. Dementievska (2019), G. Li et al. (2019) address the pedagogical basis in the designing of cybersecurity educational courses suited to a broad target audience, since people are not trained to prevent cyberattacks.

In particular, (Bykov, Burov & Dementievska, 2019: 313–331) draw attention to the necessity of introducing cyber defense training into the e-learning environment. Since cybersecurity is a complex problem, the protection of sensitive data should include legal, technical, informational, organizational, and psychological measures.

G. Li et al. (2019) point out that the lack of cybersecurity awareness can lead to a cyberattack. The authors propose to introduce online courses to work at a number of training models aimed at developing competencies and skills to detect unauthorized access to closed systems.

J. Dawson and R. Thomson (2018), R. Dreibelbis, J. Martin, M. Coovert, and D. Dorsey (2018), Z. King et al. (2018), etc. discuss

the crucial role of psychology in understanding cybersecurity and examine the behavioral aspects of cybersecurity.

J. Dawson and R. Thomson focus on the importance of cognitive abilities for the cybersecurity workforce. The authors believe that alongside technical and engineering skills cybersecurity experts need to develop social, communication skills that they can be constantly trained on (Dawson & Thomson, 2018).

Social psychologists R. Dreibelbis and J.Martin explain that the rapid changes in cyberspace require I-O psychology intervention from organizational psychology. They insist on including special tasks targeted at the development of sustainability and adaptability into the corporate personnel training system (Dreibelbis et al., 2018).

Contemporary researchers have made significant efforts to develop a holistic approach that could describe the human-factor risks in the cybersecurity system. Researchers examined cyberattackers' behavior and analyzed the motives behind insider threats and user profiles. The analysis data formed the basis for a scale that includes a set of characteristics and assessment tools, which can be used in the future to identify potential patterns of cybercrime behavior (King et al., 2018).

Since computer security is not just about technology and systems, but it is also about the people who use these systems, so scholars repeatedly highlight the extreme importance of human factors in cybersecurity systems (Quigley, 2015; Hadlington, 2017; Marble et al., 2015; Yan et al., 2018, and etc.).

Particularly, K. Quigley (scrutinizes communication problems between technical experts and laypersons, for instance, blame-shifting in case the system is being attacked. The survey demonstrates that professional communication has a number of disadvantages that are associated with over- and underestimation of the risks, which may affect the critical infrastructure (Quigley, 2015).

L. Hadlington brought into focus the correlation between employees' attitudes towards cybersecurity and risky online behaviors. He notes that Internet addiction and impulsivity are the indicators of an employee's tendency for risky behavior on the network that threatens the organization's cybersecurity (Hadlington, 2017).

J. Marble et al. (2015) analyze the role of cyberattack participants (attackers and defenders). The authors emphasize that the lack of awareness of cyberthreats by users and the complexity of the new cyber

environment are the key reasons for successful cyberattacks. In this regard, they suppose that studying the psychology of users as potential targets of cyberattacks can help to create a safer cyber environment. Finally, the authors conclude that the human factor poses a threat not only to the individual but also to the nationwide security system in general. The complexity of the problem needs further research and development of cyberthreats counteraction mechanisms (Marble et al., 2015).

L. Ermakova's and Yu. Aidarov (2009) and work carries out a linguistic analysis of spam emails, which may help hackers to gain access to user's sensitive data. Paying special attention to their grammatical, lexical, and syntactic features, the authors, however, come to the conclusion that junk mail is more likely to be a channel to advertise obnoxious and intrusive services and goods. The conclusions made by the authors do not allow to systematize and identify linguistic patterns of junk mail and to take action against it. In addition, spam emails, unlike social engineers' activity, do not harm personal sensitive data. Unfortunately, the given study suggests a rather limited application, it contains little practical information on what steps users should undertake to protect themselves from receiving junk mails and does not consider other psycholinguistic aspects of the problem.

O. Vanyushicheva et al. (2011) cogitate about psychological peculiarities of user vulnerability as a potential object of socio-engineering attack. The authors allude to the user's personal and social factors that affect the degree of his vulnerability. Moreover, the authors mention the correlation between the user's vulnerability and psychological profile. Nevertheless, the given work focuses on the individual object of attack, while the psycholinguistic aspects of the social engineer's activity and his interaction with the object of attack have not been subject to research so far.

The ways in which individuals manipulate or influence other persons were considered by G. Grachev and I. Melnik (2002), R. Cialdini (2015), and others. These studies refer to the psychology of persuasion in general, paying no particular attention to the psychological and linguistic aspects of social engineering as a vital problem of cybersecurity.

Diverse issues of social engineering are mostly the focal point of popular books, written by experts in this field. These books include real stories and social engineering cases (Mitnick & Saymon, 2004;

Kaspersky, 2005; Kuznetsov, 2007; Mason, Watson & Ackroyd, 2014; Hadnagy, 2018; Binks, 2019, etc.).

M. Workman (2007), F. Mouton et al. (2016), C.J. Mansfield-Devine (2017), and J. Hatfield (2018) recognize social engineering as an extremely urgent problem and one of the greatest security threats facing both individuals and organizations.

The SANS Institute that specializes in information security identifies four social engineer attack vectors based on the following human psychological vulnerabilities: 1) careless attack vector, which exploits user's indifference to take corresponding defensive countermeasures; 2) comfort zone attack vector that is aimed at intruding the environment the user feels comfortable in; 3) helpful attack vector, which employs the user's natural desire to be in assistance; 4) fear attack vector that manipulates the user's fears (Lively & Charles, 2003). Though describing the main attack vectors, this study, unfortunately, does not analyze the means used by social engineers to influence the behavior of an object of attack.

From our perspective, discussing the phenomenon of social engineering is impossible without mentioning the global cybersecurity culture, which, according to Resolution adopted by the General Assembly, includes such components as (a) awareness; (b) responsibility; (c) response; (d) ethics; (e) democracy; (f) risk assessment; (g) security design and implementation; (h) security management; (i) reassessment (UN Documents. Creation of a Global Culture of Cybersecurity: Resolution Adopted by the General Assembly, http).

It is worth to note that existing research does not address the issues of social engineering, their psycholinguistic aspects, and the way these aspects can be used to create a common system of personal data protection.

Moreover, this problem has not been investigated in psycholinguistics as well: there are no studies trying to analyze or sort out the impact of spoken and written speech on the user's behavior and the mechanisms developed to counteract such impact.

Based on the abovementioned, we suppose that the formation of the cybersecurity culture associated with cyberattack counteraction mechanisms at the human-factor level should be considered by various fields of scientific study, including psycholinguistics. In this regard, psycholinguistics examines what words, phrases, and expressions

social engineers exploit to influence and manipulate user's behavior and cognitive processes. The results obtained will be very useful for generating techniques to counter social engineering attacks.

In a two-stage design, we will analyze social engineers' activities in terms of using morphological, lexical, syntactical, etc. forms to intervene and influence the user's consciousness (the psycholinguistic aspect of the problem), then we will develop countermeasure mechanisms, based on the data obtained at the first stage.

The paper manifests the results of the first stage of the conducted study, i.e. the analysis of typical methods applied by social engineers in their work and scrutiny of how they use language to influence user's thought and action.

The goal of this paper is to analyze the methods and techniques employed by social engineers in their malicious activity and its features from a psycholinguistic point of view for further development of counteraction mechanisms.

Methods and Techniques of Research

In the study, we used the following research methods: primary source analysis, analysis of spoken and written speech and speech products, and intent analysis.

Considering the psycholinguistic aspects of social engineering, we emphasize that this type of cyberthreat is based on manipulations in the communication process and is widely used by attackers to influence the user's cognitive processes (critical thinking, logic, situation analysis, etc.) forcing him to perform their desired actions.

The distinctive feature of the social engineer's activity is the lack of face-to-face interaction with another person. Taking the abovementioned into account, we will interpret social engineer's activity as a subject-object interaction in terms of Alexei Leontiev's (1975) classical activity theory and Lev Vygotsky's (2005) cultural-historical activity theory.

The practical applicability of the activity theory is the main reason for exercising it to analyze the social engineer's actions. Indeed, many fields of knowledge use the activity theory to analyze, determine problems and improve the work of particular branches. Despite the activity theory is mainly theoretical in domestic science, it

has gained huge popularity in the practical studies of foreign scientists and has proven to be an effective tool for analyzing the activities of both individuals and organizations. For example, in the early 1990s, it was intensively used to create user-friendly interfaces to optimize and improve performance in computer-related industries (human-computer interaction). Yrjö Engeström, based on the cultural-historical activity theory, constructed the empirical activity triangle and summarized the principles to analyze the activity in an organization. Cultural-historical activity theory helps to understand the relationship between human and material, social and cultural environment (Cole, 1996; Cole & Engeström, 1993; Wertsch, 1993, 1994; Engeström, 1999).

Hence, time-tested activity theory has proven to be an effective tool able to identify the general patterns of activity, tools, and ways of its implementation, as well as the motives, objectives, and means used to achieve the goal.

We describe social engineering through activities that involve the subject or the attacker (the social engineer himself), the object or the user (any person the social engineer communicates with), and the mediators. Since the social engineer's activity is as a subject-object interaction, mediators are represented by tools and/or signs (Vygotsky, 2005). Tools include computers, cell phones, USB flash drives, program software, etc., while signs are psychological factors, language, speech, concepts, and symbols (Carrol, 2003: 291–324). It should be noted that specified subject-object interaction will be scrutinized through the prism of external factors (cultural, historical, mental, and social) and the environment.

Thus, this study is based on the activity theory and explanation of cultural mediators within the framework of Lev Vygotsky's cultural-historical activity theory that serves as a methodological foundation for investigating the social engineer's activity. Our task is to identify and analyze the methods applied by social engineers in their work and to examine the speech and language tools used to manipulate and influence the user's consciousness and mental state (Vygotskyi, 2005).

Results and Discussions

The interaction between subject and object and various aspects of their behavior leads to the formation of an entire structure, so the survey

of individual manifestations of activities and actions can be considered as just a single stage of a comprehensive study. The key motive of each social engineer's action is to divulge confidential information, which can be successful or vice versa. The social engineer's attack is apparently a hierarchically organized triad including motive – specific actions and operations – final result. The analysis of the products of oral and written speech allows to determine the main directions of communicative activity and to visualize the system picture, which contains linguistic, psychological, social, and cultural factors. Based on Alexei Leontiev's activity theory and clarification of cultural mediators within the framework of Lev Vygotsky's cultural-historical activity theory (2005), we worked out a scheme depicting subject-object interaction during a successful social engineer's attack (Fig. 1).

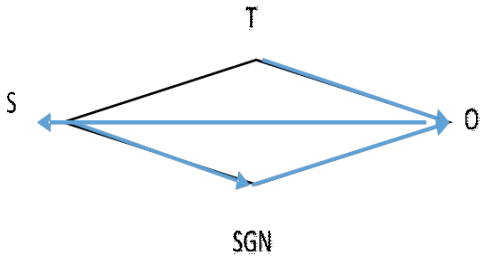

Fig. 1. *Interaction scheme of a successful social engineer's cyberattack*
S – subject, O – object, T – tools, SGN – signs

The subject (attacker) influences the object (user) using modern telecommunication technologies and either written or verbal means of language. According to the scheme, the subject's primary goal is to obtain the necessary data through communication to manipulate the object's behavior. The attacker usually develops certain communication strategies depending on the current situation, the user's individual characteristics (determined by analyzing his responses, reactions, and pauses), cultural, historical, mental, social factors, and the environment of his activity.

After scrutinizing a wide array of social engineering-related cases, it is possible to conclude that the subject's (attacker/social engineer) main actions performed to influence the object are connected with the use of oral and written products, apps, program software or USB flash drives.

Based on the type of communication involved, we divided the social engineer's main actions (attacks) into direct (oral) and indirect (written).

I. Actions through written speech (indirect attacks).

Indirect communication is related to provoking mechanical actions like opening a file, connecting an unknown USB flash drive to your computer, downloading program software or an application. Besides, the indirect attack includes a preliminary collection of data about the user and his environment. Indirect communication implies the selection of written language means able to induce the user to provide cybercriminals with access to «sensitive data» (private emails and messages, passwords, bank accounts, etc.).

II. Actions through spoken speech (direct attack).

Direct communication is the process of exchanging information through oral speech.

As for the social engineer's activity, oral or written text is a reflection of the subject's activity structure, his objectives, motives, and the means used to achieve the goal. The techniques exploited to influence user's cognitive processes are based on the distinctive features of spoken and written speech, linguistic factors, object's psychological characteristics, and the environment he lives in, historical and cultural aspects of a certain society. By conducting a comprehensive analysis of primary sources and systematically examining the subjects' speech activity at different communicative levels, we have singled out *methods of social engineer's influence* on the user's cognitive processes, involving direct and indirect actions:

a) one of the principal methods is to affect the emotional and sensual sphere by creating texts or messages able to provoke a certain reaction and manipulate the object's consciousness. For instance, overly-positive or overly-angry post has an emotional effect on social network users being shared, commented, and liked. The given fact can be easily explained by psychology and physiology. The use of verbal constructs that elicit mental images and situations appeals to a person's emotional-affective sphere and blocks the rational zones of the cognitive-rational sphere. According to J.G. Nicholls, A.R. Martin, B.G. Wallace, and P.A. Fuchs, it is primarily connected with the major action of adrenaline and noradrenaline that being released prepare a person for «fight or flight» response in stress, vigorous or sudden action (Nicholls, Martin,

Wallace & Fuchs, 2008). From the point of view of psychology, the social engineer's activity must first and foremost have an impact on the emotional sphere. A.R. Damasio (2001), T.E. Nygren et al. (1996), and other researchers accentuate that the emotional and sensual sphere is an important chain that influences the result of the activity. When the social engineer and the user converse with each other, be it a direct or telephonic conversation, the communication process helps to reveal the user's distinctive psychological features and traits developed under the influence of cultural and historical peculiarities of the given society and organizational principles of an enterprise he works at;

b) methods of influence aimed at creating situations that limit the user's critical perception by drawing his attention to details he might be interested in (for example, a «Salary»– scripted USB flash drive which obviously causes a desire to open it immediately);

c) methods of influence that help to block the cognitive processes of rational and critical thinking. Such methods do not allow the user to analyze and critically evaluate events and find solutions in a non-standard situation (for instance, the urgency of the situation, authoritative sources of information to convince the recipient in something, etc.). In this case, social engineers select linguistic means able to cause anxiety and stress, to limit the time for deliberating over the situation, to create a sense of urgency or fear in victims;

d) speech actions which contain positive incentives that have an interest to a user, like «promotion», «win», «positive impression», etc. Social engineers widely exploit lexical and stylistic devices to formulate a request, praise, encouragement, and so on. Such attacks are targeted at manipulating user's moral attitudes (the desire to assist, to be helpful).

Depending on the type of communication and the methods of influencing the user's cognitive process, we have categorized the general *techniques* applied by social engineers as follows:

1) techniques related to the use of spoken speech;
2) techniques related to the use of written speech;
3) techniques related to the use of USB flash drives, applications, and program software.

Techniques related to the use of verbal speech include actions that block the cognitive processes of rational and critical thinking and persuade the object to make wrong decisions, thereby providing

access to his sensitive data (phishing, vishing, smishing, creating limited-time situations).

Techniques related to the use of written language aimed at forming lexical and conceptual structures able:

– to provoke the subject to perform certain actions (for example, to open a file, to fill in a form containing personal data);

– to block rational thinking zones (for instance, when the object is forced to focus on events that evoked a particular emotion, no matter positive or negative (joy of winning, worrying about a family member);

– to influence the emotional and affective sphere (for example, phishing using SMS, threatening letters, virus warning emails, etc.).

Techniques related to the use of USB flash drives, applications, and program software exploit special words or phrases to make the user download the desired apps or program to his PC, for example, an antivirus update message or «Bonus» written on a «lost» USB flash drive, which definitely may arouse user's interest or curiosity.

The wide application of the abovementioned methods, actions, and techniques results in the leakage of personal data and confidential («sensitive») information, downloading harmful, spyware or viral files (apps and programs) to a computer.

Conclusion

Therefore, cybersecurity cannot be viewed only as a set of security measures to preserve the confidentiality of information, since it involves communication-related activities. In this regard, it is crucial to teach people to recognize and confront the techniques used by social engineers to get access to «sensitive» data and to improve their information security awareness.

In this paper, social engineering is considered as a negative socio-technological phenomenon, which poses a threat to the personal confidential data of both individuals and corporations. Commonly, social engineering implies communication between the attacker (subject/social engineer) and the user (object of attacks) that invokes fear, urgency, anger or positive emotions, leading the user to reveal confidential information, open a malicious file or click a malicious link.

We proved that social engineers widely employ oral and written texts or deep knowledge in psychology to influence and manipulate

the user. Having analyzed the actions (attacks) and techniques used by social engineers, we singled out speech and language means able to affect the user's cognitive processes and alter his behavior. Depending on the type of communication, the principal actions (attacks) of social engineering can be divided into 1) direct (oral) and 2) indirect (written) ones. In addition, we came to the conclusion that common methods of influence exploited by social engineers are aimed at governing the consciousness of the object of attack and his emotional-affective sphere, as well as blocking the processes of rational and critical thinking, manipulating person's moral and ethical attitudes. Furthermore, resting on the type of communication and the methods of influencing the user's cognitive process, we systematized the general techniques applied by social engineers to the objects of their attacks, explaining the prevailing psychological and linguistic aspects of this impact.

The findings will be used for developing social engineering defense mechanisms and counteracting strategies. In our viewpoint, the combination of critical thinking skills with Internet safety rules is an effective tool to reduce the risk of «sensitive data» leakage.

A better understanding of social engineering methods and actions is a powerful tool that can be used for developing cyberattacks countermeasures and increasing cybersecurity literacy.

References

Actual cyber threats – 2018. Trends and forecasts (2018). Positive Technologies. Retrieved from: https://www.ptsecurity.com/upload/corporate/ru-ru/analytics/Cybersecurity-threatscape-2018-rus.pdf [in Russian].

Binks, A. (2019). The art of phishing: past, present and future. *Computer Fraud & Security*, 4, 9–11. https://doi.org/10.1016/S1361-3723(19)30040-5

Bykov, V.Y., Burov, O.Y., & Dementievska, N.P. (2019). Cyber security in a digital learning environment. *Information Technologies and Learning Tools*, *70*(2), 313–331. https://doi.org/10.33407/itlt.v70i2.2876

Carrol, J.M. (2003). *HCI Models, Theories, and Frameworks: Toward a Multidisciplinary Science.* Morgan Kaufmann Publishers Inc. San Francisco, CA, USA.

Chaldini, R.B. (2015). Psihologiya vliyaniya [Psychology of Influence]. Sant-Petersburg: Izd. Piter [in Russian].

Cole, M. (1996). *Cultural Psychology: A Once and Future Discipline*. MA: Cambridge University Press.

Cole, M., Engeström, Y. (1993). A cultural-historical Approach to Distributed Cognition. In Salomon, G. (Ed.), *Distributed Cognitions: Psychological and Educational* Considerations (pp. 1–46). New York: Cambridge University Press.

Damasio, A.R. (2001). Emotion and the Human Brain. *Annals of the New York Academy of Sciences, 935,* 101–106. https://doi.org/10.1111/j.1749-6632.2001.tb03475.x

Dawson, J., & Thomson, R. (2018). The Future Cybersecurity Workforce: Going Beyond Technical Skills for Successful Cyber Performance. *Frontiers in Psychology*, *9*, 744. https://doi.org/10.3389/fpsyg.2018.00744

Dreibelbis, R.C., Martin, J., Coovert, M.D., & Dorsey, D.W. (2018). The Looming Cybersecurity Crisis and What It Means for the Practice of Industrial and Organizational Psychology. *Industrial and Organizational Psychology*, *11*(02), 346–365. https://doi.org/10.1017/iop.2018.3

Engeström, Y. (1999). Activity theory and individual and social transformation. In Y. Engeström, R. Miettinen, & R.-L. Punamäki (Eds.), *Perspectives on Activity Theory* (pp. 19–38). https://doi.org/10.1017/CBO9780511812774.003

Ermakova, L., & Aidarov, Yu. (2009). Lingvistika protiv sotsialnoy inzhenerii. [Linguistics Versus Social Engineering]. *Otkrytyie sistemyi. SUBD – Open systems. SUBD.* Retrieved from: https://www.researchgate.net/publication/307855981 [in Russsian].

Grachev, G.V., & Melnik, I.K. (2002). *Manipulirovanie lichnostyu: organizatsiya, sposobyi i tehnologii informatsionno-psihologicheskogo vozdeystviya. [Manipulation of Personality: Organization, Methods and Technologies of Information and Psychological Impact]*. Moscow: Izd. Algoritm [in Russian].

Hadlington, L. (2017). Human factors in cybersecurity; examining the link between Internet addiction, impulsivity, attitudes towards cybersecurity, and risky cybersecurity behaviours. *Heliyon, 3*(7). https://doi.org/10.1016/j.heliyon.2017.e00346

Hadnagy, Chr. (2018). *Social Engineering: The Science of Human Hacking* (2nd ed.). https://doi.org/10.1002/9781119433729

Hatfield, J.M. (2018). Social engineering in cybersecurity: The evolution of a concept https. *Computers & Security*, *73,* 102–113. https://doi.org/10.1016/j.cose.2017.10.008

Kasperski, K. (2005). *Sekretnoe oruzhie sotsialnoy inzhenerii [The Secret Weapon of Social Engineering]*. Kompaniya AyTi [in Russian].

King, Z.M., Henshel, D.S., Flora, L., Cains, M.G., Hoffman, B., & Sample, C. (2018). Characterizing and Measuring Maliciousness for Cybersecurity Risk Assessment. *Frontiers in Psychology*, *9,* 39. https://doi.org/10.3389/fpsyg.2018.00039

Kuznetsov, M. (2007). Sotsialnaya inzheneriya i sotsialnyie hakeryi [Social Engineering and Social Hackers]. Peterburg: «BHV-Peterburg» [in Russian].

Leontiev, A.N. (1975). *Deyatelnost. Soznanie. Lichnost [Activity. Consciousness. Personality]*. Moscow: «Politizdat» [in Russian].

Li, G, Shen, Yu., Zhao, P., Lu, X., Liu, J., Liu, Ya., & Hoi, S. (2019). Detecting cyberattacks in industrial control systems using online learning algorithms. *Neurocomputing, 364,* 338–348. https://doi.org/10.1016/j.neucom.2019.07.031

Lively, Charles, E.Jr. (2003). Psychological Based Social Engineering. *GSEC.* Option 1, version 1.4b. Retrieved from: https://www.giac.org/paper/gsec/3547/psychological-based-social-engineering/105780

Mansfield-Devine, S. (2017). Bad Behaviour: Exploiting Human Weaknesses. *Computer Fraud & Security*, *1,* 17–20. https://doi.org/10.1016/S1361-3723(17)30008-8

Marble, J., Lawless, W., Mittu, R., Coyne, J., Abramson, M., & Sibley, C. (2015). The Human Factor in Cybersecurity: Robust & Intelligent Defense. In *Cyber*

Warfare: Building the Scientific Foundation (pp. 173–206). Springer International Puplishing. https://doi.org/10.1007/978-3-319-14039-1_9

Mitnik, K., & Saymon, V. (2004). *Iskusstvo obmana [The Art of deception].* Kompaniya AyTi [in Russian].

Mouton, F., Leenen, L., & Venter, H.S. (2016). Social engineering attack examples, templates and scenarios. *Computers & Security*, *59,* 186–209. https://doi.org/10.1016/j.cose.2016.03.004

Nicholls, J.G., Martin, R.A., Bruce, W., & Fuchs, P.A. (2001). *From Neuron to Brain*. *Cellular and Molecular Approach to the Function of the Nervous System, Fourth Edition.* Sinauer Associates (4th ed.).

Nygren, T.E., Isen, A.M., Taylor, P.J., & Dulin, J. (1996). The influence of positive affect on the decision rule in risk situations: Focus on outcome (and especially avoidance of loss) rather than probability. *Organizational Behavior and Human Decision Processes*, *6.1*, 59–72. https://doi.org/10.1006/obhd.1996.0038

Quigley, K. (2015). 'Cyber Gurus': A rhetorical analysis of the language of cybersecurity specialists and the implications for security policy and critical infrastructure protection. *Government Information Quarterly, 32*(2), 108–117, https://doi.org/10.1016/j.giq.2015.02.001

UN Documents. Elements for Creating a Global Culture of Cybersecurity. Retrieved from: http://www.un.org/ru/documents/decl_conv/conventions/elements.shtml]

Vanyushicheva, O.Yu., Tulupeva, T.V., Paschenko, A.E., & Tulupev, A.L. (2011). Klassifikatsiya psihologicheskih osobennostey sostavlyayuschih osnovu uyazvimostey polzovatelya pri ugroze sotsioinzhenernyih atak [Classification of Psychological Features that Form the Basis of User Vulnerabilities in Case of Threat of Social Engineering Attacks]. *Trudy SPIIRAN – SPIIRAS Proceedings,* 17, 70–99 [in Russian].

Vygotskiy, L.S. (2005). *Psihologiya razvitiya cheloveka [Psychology of Human Development].* Moscow: Izd-vo «Smyisl; Eksmo» [in Russian].

Watson, G., Mason, A., & Ackroyd, R. (2014). *Social Engineering Penetration Testing: Executing Social Engineering Pen Tests, Assessments and Defense*. Boston. doi.org/10.1016/B978-0-12-420124-8.00011-9

Wertsch, V. James (1993). *Voices of the Mind. Sociocultural Approach to Mediated Action.* Harvard University Press.

Wertsch, V. James (1994). The Primacy of Mediated Action in Sociocultural Studies. *Mind, Culture, and. Activity, 1*(4), 202–208.

Workman, M. (2007). Gaining Access with Social Engineering: An Empirical Study of the Threat. *Information Systems Security, 16*(6), 315–331. https://doi.org/10.1080/10658980701788165

Yan, Zh., Robertson, T., Yan, R., Sung, Yo.P., Bordoff, S., Chen, Q., & Sprissler, E. (2018). Finding the weakest links in the weakest link: How well do undergraduate students make cybersecurity judgment? *Computers in Human Behavior,* 84, 375–382. https://doi.org/10.1016/j.chb.2018.02.019

АНОТАЦІЯ

Вступ. *У статті розглянуто гуманітарні аспекти кібербезпеки з точку зору мовленнєвих та мовних засобів, які використовує соціальний інженер у своїй діяльності.* ***Мета статті*** *– проаналізувати методи та прийоми роботи*

соціального інженера та її особливості з психолінгвістичної точки зору для подальшого вироблення механізмів протидії.

Методи. *У дослідженні використано наступні методи: аналіз джерел, аналіз продуктів мовленнєвої та мовної діяльності, інтент-аналіз.*

Результати. *Діяльність соціального інженера розглядаємо з позиції діяльнісного підходу, яку ми представили її у вигляді трикомпонентної схеми: суб'єкт, об'єкт, медіатори. Ми зауважуємо, що дана схема є валідною за умови успішної атаки (дій) соціального інженера. На основі аналізу джерел виокремлено засоби усного та писемного мовлення (прямі та непрямі дії), які використовуються соціальним інженером для впливу на когнітивні процеси об'єкта, задля отримання доступу до «чутливих» даних та конфіденційної інформації. Виділено психологічні та лінгвістичні засоби, які використовує в своїй роботі соціальний інженер. Ми зазначаємо, що основні методи роботи соціального інженера скеровані а) на емоційно-чуттєву сферу, б) на блокування процесів раціонального та критичного мислення, в) маніпулювання морально-етичними установками особистості, г) використання позитивних стимулів для заохочення об'єкта атаки.*

Ґрунтуючись на виокремлених методах роботи соціального інженера та типах комунікаційних дій (прямі-непрямі), систематизовано та описано загальні прийоми, пов'язані з використанням усного та писемного мовлення та технологіями: 1) прийоми, пов'язані з використанням усного мовлення; 2) прийоми, пов'язані з використанням писемного мовлення; 3) прийоми, пов'язані з використанням флеш-накопичувачів, додатків та ПЗ.

Зазначені результати дослідження є корисними для розробки механізмів протидії атакам соціального інженера та сприяють підвищенню загального рівня грамотності в питаннях кібербезпеки.

Ключові слова: *психолінгвістика, мова, мовлення, соціальна інженерія, кібербезпека, вплив.*

Крылова-Грек Юлия. Психолингвистические аспекты гуманитарного компонента кибербезопасности

АННОТАЦИЯ

Вступление. *В статье рассмотрены гуманитарные аспекты кибербезопасности с точки зрения деятельности социального инженера.* ***Цель статьи*** *– проанализировать методы и приёмы работы социального инженера и её особенности с точки зрения психолингвистики что даст в дальнейшем возможность разработать механизмы противодействия данному явлению.*

Методы. *В исследовании использованы следующие методы: анализ источников, анализ продуктов устной и письменной деятельности, интент-анализ.*

Результаты. *Мы рассматриваем деятельность социального инженера с точки зрения деятельностного подхода. Она представлена в виде трёхкомпонентной схемы: субъект, объект, медиаторы. Основываясь на анализе источников, мы выделили средства прямых и непрямых (средства устной и письменной речи)*

действий (атак) социального инженера. Данные средства используются с целью воздействия на когнитивные процессы объекта для получения доступа к «чувствительным» данным и конфиденциальной информации.

В работе мы обозначили психологические и лингвистические методы роботы социального инженера. Обращаем внимание на то, что основные методы работы направлены: а) на эмоционально-чувственную сферу; б) на блокирование процессов рационального и критического мышления; в) манипулирование морально-этическими установками объекта; г) использование позитивных стимулов для поощрения ожидаемых действий от объекта атаки.

Основываясь на выделенных методах роботы социального инженера и типах коммуникационных действий (прямые-непрямые), мы систематизировали и описали типичные приёмы в соотношении с используемыми языковыми средствами и технологиями: 1) приёмы, соотнесенные с устной речью, 2) приёмы, соотнесенные с письменной речью, 3) приёмы, соотнесенные с использованием флеш-накопителей, приложений и ПО.

Результаты исследования возможно использовать при анализе ситуаций и разработке механизмов противодействия атакам социального инженера, а также для повышения общего уровня грамотности в вопросах кибербезопасности.

Ключевые слова: *кибербезопасность, социальная инженерия, язык, речь, психолингвистика, влияние.*