Henryk NOGA
henryk.noga@uken.krakow.pl
https://orcid.org/0000-0001-7073-3443
Tetiana KONRAD
tetiana.konrad@uken.krakow.pl
https://orcid.org/0000-0001-6283-1967
University of the National Education Commission, Krakow
Institute of Technical Sciences
Viktoriia TROFYMCHUK
trofymchukviktoria@gmail.com
https://orcid.org/0000-0002-9756-0244
Viktoriya VOLKOGON
State University «Kyiv Aviation Institute»/ Department of Software Engineering
https://orcid.org/0000-0002-6813-5724
Agnieszka GAJEWSKA
https://orcid.org/0000-0002-4620-0222
Kamila KLUCZEWSKA-CHMIELARZ
https://orcid.org/0000-0003-4301-7438
University of the National Education Commission, Krakow/ Institute of Technical Sciences
https://doi.org/10.34739/dsd.2025.02.08

MODELING THE RISKS OF SOCIOENGINEERING ATTACKS ON THE INFORMATION SYSTEM BASED ON THE METHOD OF COGNITIVE MAPPING

ABSTRACT: The article explored the key methods of social attacks, including phishing, vishing, spear phishing, and trust manipulation, which allow attackers to bypass even the most sophisticated defense mechanisms. Special attention is focused on analyzing the human factor as a critical element of security. The research shows that about 70% of incidents are related to the actions of users themselves, who may be unaware, psychologically vulnerable, or subject to external influence. The practical significance of the study is to develop strategies to minimize the risks of social engineering. The proposed measures include comprehensive staff training, the use of multi-level authentication, restriction of access rights, implementation of software monitoring of suspicious actions, and threat modeling based on cognitive analysis. The presented results may be useful for security policy makers, information security professionals, and researchers in the field of cyber defense.

KEYWORDS: social engineering, information security, human factor, cognitive mapping, mathematical modeling

MODELOWANIE RYZYKA ATAKÓW SOCJOINŻYNIERYJNYCH NA SYSTEM INFORMATYCZNY W OPARCIU O METODĘ MAPOWANIA KOGNITYWNEGO

ABSTRAKT: W artykule przeanalizowano kluczowe metody ataków społecznościowych, w tym phishing, vishing, spear phishing i manipulację zaufaniem, które pozwalają atakującym ominąć nawet najbardziej wyrafinowane mechanizmy obronne. Szczególną uwagę skupiono na analizie czynnika ludzkiego jako krytycznego elementu bezpieczeństwa. Badania pokazują, że około 70% incydentów jest związanych z działaniami samych użytkowników, którzy mogą być nieświadomi, podatni psychologicznie lub podlegać wpływom zewnętrznym. Praktyczne znaczenie badania polega na opracowaniu strategii minimalizujących

ryzyko inżynierii społecznej. Proponowane środki obejmują kompleksowe szkolenia personelu, stosowanie wielopoziomowego uwierzytelniania, ograniczanie praw dostępu, wdrażanie oprogramowania monitorującego podejrzane działania oraz modelowanie zagrożeń w oparciu o analizę kognitywną. Przedstawione wyniki mogą być przydatne dla osób odpowiedzialnych za politykę bezpieczeństwa, specjalistów ds. bezpieczeństwa informacji i badaczy w dziedzinie cyberobrony.

SŁOWA KLUCZOWE: inżynieria społeczna, bezpieczeństwo informacji, czynnik ludzki, mapowanie kognitywne, modelowanie matematyczne

INTRODUCTION

In today's digital environment, information security is becoming a critical issue for any organization or individual user[1]. One of the most dangerous methods of gaining unauthorized access to data is social engineering, which is based on the manipulation of human psychology and behavioral traits. Unlike traditional attack methods, such as exploiting software vulnerabilities or using malware, social engineering bypasses technological safeguards by forcing users to disclose confidential information or perform actions that threaten system security[2].

Research into social engineering is relevant due to the rapid growth in the number of attacks that exploit the human factor as a weak link in cybersecurity systems. According to statistics, about 70% of information security incidents are caused by social attacks rather than technical vulnerabilities. Attackers use a variety of methods, including phishing (manipulation via email)[3], vishing (attacks via voice)[4], spear phishing (targeted attacks on specific individuals), as well as more sophisticated techniques that include long-term information gathering and psychological influence on the victim[5].

---

[1] A. Gajewska, H. Noga, M.K. Grzegorzewska, *Bezpieczeństwo i porządek publiczny w systemie funkcjonowania państwa na przykładzie działań w dzielnicy Kraków Nowa Huta jako wyzwania edukacji dla bezpieczeństwa*, "Edukacja Ustawiczna Dorosłych", 2023(2), s.167–175; A. Gajewska, H. Noga, T. Piotrowski, *Kompetencje funkcjonariuszy Policji w zakresie bezpieczeństwa i porządku publicznego na przykładzie dzielnicy Kraków Nowa Huta wobec wyzwań edukacji dla bezpieczeństwa*, "Edukacja Ustawiczna Dorosłych", 2022(4), s. 95–105; S. Bałuszyński, K. Kluczewska-Chmielarz, D. Lis, *Contemporary Hazards for Drivers*, „Zeszyty Naukowe Wyższej Szkoły Finansów i Prawa w Bielsku-Białej", 2024 28(4), s. 40-46; P. Czaja, Kamila Kluczewska-Chmielarz, J. Porębska, H. Noga, B. Szczypka-Brodzińska, *Techniki informacyjne w zarządzaniu szkołą*, "Edukacja Ustawiczna Dorosłych", 2024, 2, s. 79-95.

[2] A.A. Melnychenko, *The Problem of the Relationship Between Social Engineering and Social Management: A Philosophical Reflection*, "Bulletin of NTUU "KPI". Philosophy. Psychology. Pedagogy", 2008, (1)22, p. 40-43; A. Naz, M. Sarwar, M. Kaleem, M.A. Mushtaq, S. Rashid, *A comprehensive survey on social engineering-based attacks on social networks*, "International Journal of Advanced and Applied Sciences", 2024, 11(4), p. 139–154; M.A. Siddiqi, W. Pak, M. Siddiqi, *A Study on the Psychology of Social Engineering-Based Cyberattacks and Existing Countermeasures*, "Applied Sciences" 2022, 12(12), 6042;

[3] M. Butavicius, K. Parsons, M. Pattinson, A. McCormac, *Breaching the human firewall: Social engineering in phishing and spear-phishing emails*, "Computers & Security", 2016, 57, p. 70–87; P. Unchit, S. Das, A. Kim, L.J. Camp, *Quantifying susceptibility to spear phishing in a high-school environment using signal detection theory*, "Journal of Cybersecurity", 2020, 6(1); M. Schmitt, I. Flechais, *Digital deception: Generative artificial intelligence in social engineering and phishing*, "Artificial Intelligence Review", 2024, 57, 324; F. Salahdine, Z. El Mrabet, N. Kaabouch, *Phishing attacks detection: A machine learning-based approach*, "Computers & Security", 2022, 118, 102720.

[4] A. Triantafyllopoulos, et al., *Vishing: Detecting social engineering in spoken communication — A first survey & urgent roadmap to address an emerging societal challenge*. Computer Speech & Language, 2025, 94, 101802; F. Toapanta, et al., *AI-Driven Vishing Attacks: A Practical Approach*, Engineering Proceedings 2024, 77(1), p. 15.

[5] M.A. Siddiqi, W. Pak, M. Siddiqi, *A Study on the Psychology of Social Engineering-Based Cyberattacks and Existing Countermeasures*, "Applied Sciences" 2022, 12(12), 6042; A.A. Melnychenko, *Social Engineering as*

Despite the development of security technologies[6], any security system cannot guarantee complete protection against attacks that exploit human weaknesses. The concept of "candy security," which implies strong external protection with a weak internal structure, illustrates a real problem in modern organizations: even the most advanced encryption and access control systems can be useless if employees or users are not aware of the risks and do not follow security rules[7].

This article discusses not only the methods of social attacks, but also suggests ways to model and analyze them mathematically. Particular attention is paid to cognitive mapping of the impact of social engineering on users, which allows visualizing and assessing the cause-and-effect relationships between behavioral factors and the probability of attack success. The use of cognitive maps allows not only to predict the vulnerability of the system to attacks, but also to develop strategies to minimize risks.

In addition, the article proposes a probabilistic model for assessing the risks of social engineering attacks, which takes into account such parameters as the level of user awareness, attacker skills, and the availability of technical means of protection. The author analyzes critical risk factors and opportunities for implementing effective countermeasures, including staff training, implementation of multi-level authentication, development of corporate security policies, and use of specialized software and hardware solutions.

In summary, the goal of this research is to identify the mechanisms of social engineers' influence on information systems, assess the risks of such attacks, and develop effective methods of counteraction. The presented results may be useful for cybersecurity professionals,

---

a Factor in Ensuring the Sustainable Development of Social Systems, "Bulletin of NTUU "KPI" Political Science. Sociology. Law", 2012, (1)13, p. 73-78; V.V. Vyshnovskyi, L.M. Tkachuk, *Social Engineering as a Means of Influencing Human Consciousness*, XLVII Scientific and Technical Conference of the Institute for Integration of Learning with Production, https://studies.in.ua/lekcii-sociologija/4443-socalna-nzhenerya.html; R. Montañez-Rodriguez, E. Golob, S. Xu, *Social engineering cyberattacks and human cognition: A psychology perspective*, "Frontiers in Psychology", 2020, 11, 1755; M. Sh. Tsauri, *Human Vulnerabilities to Social Engineering Attacks: A Systematic Literature Review for Building a Human Firewall*. "Journal of Applied Informatics and Computing (JAIC)", 2025, 9(4), pp. 1127-1136.

[6] T. Darbek, A. Mukasheva, A. Bissembayev, S. Gnatyuk, D. Mukammejanova, *Research and development of two-factor authentication methods using neural networks*, Proceedings of the IEEE 4th International Conference on Smart Information Systems and Technologies (SIST 2024), 2024, pp. 340-345; Z. Avkurova, S. Gnatyuk, B. Abduraimova, K. Makulov, *Targeted Attacks Detection and Security Intruders Identification in the Cyber Space*, "International Journal of Computer Network and Information Security", 2024, 16(4), pp. 144-153; S. Gnatyuk, R. Berdibayev, M. Aleksander, et al., *Software System for Cybersecurity Events Correlation and Incident Management in Critical Infrastructure*, "Lecture Notes on Data Engineering and Communications Technologies", 2024, vol. 213, pp. 247-269; R. Ziubina, G. Litawa, R. Szklarczyk, P. Biel, O. Veselska, J. Nikodem, *Detection of viruses using machine learning method*, In: Proceedings of the Pacific Asia Conference on Information Systems (PACIS 2020) (Paper 9). Association for Information System, https://aisel.aisnet.org/pacis2020/9; M. Kasianchuk, M.P. Karpinski, R.V. Kochan, V. Karpinskyi, G. Litawa, I. Shylinska, I. Yakymenko, *Developing symmetric encryption methods based on residue number system and investigating their cryptosecurity*, "IACR Cryptology ePrint Archive", 2020, 589, https://eprint.iacr.org/2020/589.

[7] M. Sh. Tsauri. *Human Vulnerabilities to Social Engineering Attacks: A Systematic Literature Review for Building a Human Firewall*, "Journal of Applied Informatics and Computing (JAIC)", 2025, 9(4), pp. 1127-1136.; V.L. Buryachok, V.B. Tolubko, V.O. Khoroshko, S.V. Tolyupa, *Information and Cybersecurity: A Socio-Technical Aspect: A Textbook*. Kyiv 2015; Y.O. Nikitina, D.S. Timofeev, *Social Engineering in the Information Security System*, Youth: Science and Innovation – 2017: Proceedings of the V All-Ukrainian Scientific and Technical Conference of Students, Postgraduates, and Young Scientists (Dnipro, November 28-29, 2017), Dnipro 2017.

business executives, and researchers in the field of information security. Understanding the principles of social engineering and methods of protection against it will significantly reduce the risks of compromising information resources and increase the overall level of cyber resilience of organizations.

OBJECT, SUBJECT, GOAL AND OBJECTIVES OF THE RESEARCH

Object of research: the process of targeted influence on a person for the purpose of unauthorized access to information resources.

Subject of research: forms and methods of influence of a social engineer on the user of an information system.

Goal of the research: to determine the factors that lead to violations of information security by employees under the influence of actions (methods) by a social engineer.

Objectives of the research:

1. Analysis of the boundaries of the subject area of social engineering.
2. Defining the roles of "social engineer" and "information system user" within the subject area.
3. Identification of tactical tasks and opportunities for the use of social engineering.
4. Analysis of forms and methods of attacks, in particular attacks aimed at the qualities of human nature.
5. Analysis of the stages of social engineer's actions.
6. Building a cognitive map of the impact on the object using social engineering methods.

RESEARCH METHODS

The research of social engineering requires an interdisciplinary approach[8], that combines knowledge in the fields of information security, social psychology, cognitive science, and cybernetics. Given the complexity of the phenomenon, the study uses a comprehensive

[8] S. Sageer, et al., *An interdisciplinary view of social engineering: A call to action*, "Computers & Security", 2021, 114, 102556, https://doi.org/10.1016/j.cose.2021.102556.

methodology that includes literature analysis, cognitive modeling[9], mathematical modeling[10], and empirical research[11].

The main goal of the methodology is:

- systematization of mechanisms of social engineering influence;
- mathematical modeling of attack risks;
- assessing the vulnerability of users to social engineering attacks;
- development of strategies to minimize risks and increase cyber resilience of information systems.

The following research methods have been used to achieve the set objectives:

- At the first stage of the study, we analyzed the literature on social engineering and its methods. The main focus is on the following aspects:
- Theoretical foundations of social engineering in the field of information security.
- The concept of "weak security", which explains why the external protection of information systems can be reliable, while the internal structure remains vulnerable.
- Methods of social manipulation based on cognitive biases and psychological characteristics of a person.
- Mathematical models for assessing the risks of social engineering attacks.
- The analysis of the literature allowed us to form a knowledge base for building mathematical models for assessing the risks of attacks.

Cognitive mapping of social engineering

To visualize the mechanisms of influence of social engineering, a cognitive map has been developed that allows assessing the cause-and-effect relationships between the attacker's actions and the victim's reaction.

Stages of cognitive mapping:

Key concepts are identified:

- Victim of the attack (user, employee of the organization).
- Attacker (social engineer, cybercriminal).
- Methods of influence (phishing, vishing, trust manipulation, social pressure).

[9] K. Yesypovych, *The Phenomenon of Cognitive Mapping in the Modern Linguistic Paradigm*, „Studia Linguistica", 2013 (7), 254-257; D.G. Udochukwu, A. Bode-Asa, *An overview of social engineering: The role of cognitive biases towards social engineering-based cyber-attacks, impacts and countermeasures*, Preprint on ResearchGate.

[10] A. Sandor, G. Tonț, E. Simion, *A mathematical model for risk assessment of social engineering attack*, „SSRN Electronic Journal", 2021; J. Meyer, O. Levin, *Using machine learning to predict social engineering susceptibility*, „Behaviour & Information Technology", 2022, 41(3), p. 321–338; T. Konrad, O. Pysarchuk, H. Noga, A. Gajewska, V. Volkogon, D. Baran, *Method of Multifactor Analysis of the Alternatives Using the Example of Multicriterial Selection of the Optimal Cargo Transportation Route*, In: Proceedings of Ninth International Congress on Information and Communication Technology. ICICT 2024 2024, Lecture Notes in Networks and Systems, London, Volume 6, p. 73-85; V. Volkogon, T. Konrad, O. Kolganova, L. Tereshchenko, *Situational Synthesis of Algorithmic Support of Regional Transport Systems based on Expert System*, In: *Proceedings of the International Workshop on Advances in Civil Aviation Systems Development* (Kyiv, May 30, 2023), Kyiv, 2023, p. 100-114.

[11] V. Greavu-Şerban, C. Floredana, N. Sabina-Cristiana, E*xploring heuristics and biases in cybersecurity: A factor analysis of decision-making in social engineering contexts*, "Systems", 2025, 13(4), p. 280.

- Vulnerability factors (low level of cyber literacy, stressful situations, lack of security protocols).
- Consequences of an attack (compromise of information, financial losses, reputational risks).
- A cognitive model of the interaction between a social engineer and a victim is created that reflects the dynamics of the attacker's influence and the weaknesses of users.
- Graph analysis methods are used to determine the most critical points of influence, which allows to estimate the probability of a successful attack.

This research considers social engineering as an interdisciplinary phenomenon that combines sociological, psychological and information technology aspects of influencing users to obtain confidential information. According to the concept developed by one of the founders of social engineering, K. Popper, this approach in applied social sciences is focused on modifying behavioral attitudes, adapting social systems and solving social problems. In the modern scientific discourse, social engineering is developing in two directions: as a mechanism for the formation and improvement of social institutions and as a tool for manipulating information security[12].

In cybersecurity terms, social engineering is interpreted as a method of gaining unauthorized access to information systems through psychological influence on users. The use of manipulative technologies allows attackers to bypass technical security measures by exploiting human weaknesses, cognitive biases, and lack of awareness of information security.

Key aspects of social engineering in information security

The main factor that determines the vulnerability of a system to social engineering attacks is the human factor. The study identified the following critical aspects[13]:

- Psychological influence and manipulation – exploitation of the victim's trust, fear, desire for gain, or uncertainty.
- Use of deception and persuasion – creating scenarios that force users to disclose confidential data or perform harmful actions.
- Understanding of cognitive biases – the use of natural features of information perception, such as the effect of authority, the principle of social proof, or cognitive laziness.
- Knowledge of information technology is a combination of psychological influence and modern technological tools to collect information and prepare attacks.

Social engineering is implemented through various forms of interaction with the victim, which fall into three main categories:

1. Physical methods – manipulation through personal contact, creating situations that force the victim to act in favor of the attacker.
2. Psychological methods – influence on the emotional state of the victim through fear, trust, urgency or a sense of gain.
3. Technical methods – the use of fake web resources, emails, phishing attacks, etc.

[12] A.A. Melnychenko, *Social Engineering as a Factor in* …, op. cit.
[13] V.V. Vyshnovskyi, L.M. Tkachuk, *Social Engineering as a Means of Influencing…,* op. cit.

The success of each of these methods is determined by two variables: the level of training of the attacker (A) and the level of awareness of the victim (R).

The study found that social engineering can be used not only to directly gain access to information, but also as an intelligence tool. The main tasks of this area are:

- Research of complex social and sociotechnical systems to identify potential weaknesses in cybersecurity.
- Studying the impact on the human factor as the main tool of social engineers' attacks.

To accomplish these tasks, various methods of information collection are used:

1. Intelligence of information systems – open source research (OSINT), metadata analysis, identification of vulnerabilities in corporate infrastructure.
2. Network intelligence and cyber intelligence – searching for vulnerabilities in security systems through automated or manual means of collecting information.
3. Analysis of user behavioral factors – assessment of interaction patterns with the system to predict potentially dangerous scenarios.

According to the results obtained, from 35% to 95% of confidential information can be collected without the use of technical means of hacking, which confirms the high efficiency of social engineering methods[14].

The role of the human factor and cognitive vulnerabilities[15]:

One of the most important elements in the context of social engineering is the human factor, which determines the effectiveness of attacks. To assess the vulnerability of users, the following aspects are analyzed:

- Values and moral principles – determine the user's willingness to comply with security policies.
- Level of knowledge and awareness – affects the likelihood of error when interacting with an attacker.
- Social skills and attitudes – can help or hinder the detection of social attacks.

The main psychological mechanisms of manipulation used by social engineers include:

1. Building trust – using elements of external attributes, fake accounts, imitation of well-known individuals or organizations.
2. Creating emotional pressure – using fear, urgency, threats or benefits to accelerate the adoption of wrong decisions.
3. Manipulation of weaknesses – the use of human greed, naivety or desire for personal gain.

[14] V.L. Buryachok, V.B. Tolubko, V.O. Khoroshko, S.V. Tolyupa, *Information and Cybersecurity: A Socio-Technical Aspect*…, op. cit.
[15] M. Sh. Tsauri. *Human Vulnerabilities to Social Engineering Attacks: A Systematic Literature Review for Building a Human Firewall*…, op. cit.

MATHEMATICAL MODEL OF SOCIOENGINEERING ATTACK

The probability of a successful attack P can be represented as an equation:

$$P = \frac{A}{A+R+S} \quad \mathrm{P} = \frac{\mathrm{A}}{\mathrm{A+R+S}} \tag{1}$$

where:

A – is the attacker's skill level (0 - 1),

R – level of victim's security (0 - 1),

S is the level of use of protective technologies (0 - 1).

If $P>0.5$, the attack is considered successful, if $P<0.5$, the victim resisted.

The article discusses the methods of influence of a social engineer and the threat of corporate information leakage.

Social engineering is a tool of manipulative influence based on the peculiarities of human psychology and natural behavioral reactions. The influence of a social engineer is aimed at exploiting the basic social and psychological mechanisms that determine the interaction between people and their propensity to trust.

The main methods of influence include the following key factors:

Submission to authority - the use of status, job titles or other factors that create the illusion of authority for the victim, forcing them to comply with requests without further verification.

Social kinship – establishing a trusting relationship by demonstrating common interests, views or artificially creating a sense of similarity with the victim.

The principle of reciprocity – encouraging the victim to unconsciously comply with requests by providing previous “services” or offering assistance.

Responsibility and obligations – using the principle of fulfilling promises or job duties to manipulate behavior.

Social validation – creating the illusion that a certain action is generally accepted or expected in a particular organization or social group.

Urgency factor – putting the victim in a state of stress by creating a situation of urgency or the need to make a quick decision, which reduces the criticality of information assessment.

All of these mechanisms are used to form the victim's unconscious consent to disclose confidential information or perform harmful actions.

Goals of social engineer attacks: requests for critical information

The main goal of a social engineer is to obtain data that can be used for further attacks or commercial/political blackmail. The most common requests are:

Authentication data – passwords, access keys, pin codes, passwords, secret answers.

Organizational structure - internal departments, their functions, contact details of employees.

Technical information – IP addresses, server configurations, software, data processing algorithms.

Personal information of employees – phone numbers, passport data, financial information.

Confidential business information – strategic plans, software source codes, customer bases, financial reports.

In addition to information requests, social engineers can encourage victims to perform dangerous actions, including

- opening attachments in suspicious emails containing malware;
- changing passwords or transferring them to a “trusted person”;
- making changes to the configuration of a computer network or software;
- launching third-party applications or installing “necessary updates”;
- providing remote access to corporate systems.

Protecting an organization's information assets involves classifying data depending on their level of criticality. According to I. A. Eremichev's approach, corporate information can be divided into protected and low-protected.

Protected information

This category includes data that is restricted by law or internal company policies. It includes:

- confidential commercial information (financial statements, contracts, customer bases);
- internal documents of the organization containing strategic plans and management decisions;
- data on the company's economic activities;
- protected software source codes;
- intellectual property, patents, know-how.

The leakage of such information can lead to serious financial losses, loss of competitive advantages or legal consequences for the company.

Information with little protection

This category includes data that is not classified as confidential, but if it were to be leaked, it could create risks for the organization. Such data includes:

- internal structure of the company, names of departments, positions of employees;
- internal terminology of the organization;
- contact details of employees (office phone numbers, email addresses);
- data on the technical equipment used;
- information about work processes and regulations that does not contain critical details.

Although the leakage of this information may seem insignificant, social engineers use it as a basis for preparing targeted attacks, allowing them to impersonate internal employees and gain access to protected data.

The research considers information sources for the activities of a social engineer, including[7]:

- social bookmarking, which forms a list of bookmarks or popular websites and is used to find users with common interests (Delicious);

- social cataloging, focused on the scientific field for working with databases, citations from scientific articles (Academic Search Premier, LexisNexis, Academic University, CiteULike, Connotea);
- social libraries that contain links to books, audio recordings with a rating system (discogs.com, IMDb.com);
- social networks of webmasters that contain links to posts, appeals, etc. and often have ratings or recommendations;
- Massively Multiplayer Online Games, which simulate virtual worlds with different systems of winners and losers (World of Warcraft);
- geosocial networks that contain geolocation data, such as GPS to determine the user's location;
- professional social networks for job search, development of business relations (LinkedIn, MarketingPeople, etc.)
- age- and gender-specific social networks for relevant users.

There are three consecutive stages to each attack:

Stage I - is research. A social engineer must know which of the company's employees has access to the information he is interested in, who works in which department, where the departments are located, what software is installed on corporate computers, etc. A social hacker must be familiar with the terminology and know the internal procedures of the targeted company.

Stage II - development of an attack plan.

Stage III - is the implementation of the attack. The most common attacks are: obtaining, transmitting or unauthorized change of passwords; creating accounts (with user or administrator rights); launching malware; obtaining information on ways to remotely access the corporate information network; unauthorized granting of additional rights and opportunities to registered users of the system; transfer or dissemination of confidential information[16].

Development of a cognitive map of influence on an object using social engineering methods.

For a formalized description and the possibility of further modeling of changes in a complex or poorly structured system under the influence of a social engineer, it is proposed to describe factors (concepts) using the cognitive mapping technique.

Cognitive mapping is an applied analytical methodology for studying and demonstrating the characteristics of individual (group) thinking, which allows to predict with a high degree of probability the choices made by a person[28]. In accordance with the cognitive mapping methodology, a cognitive model (cognitive map) is built, which is displayed as an oriented weighted graph in which the set of vertices symbolizes the concepts of a complex system, and arcs symbolize the cause-and-effect relationships between the constituent elements of the system. The main initial vertex, whose value is studied and optimized, is called a privileged (target) vertex.

[16] M.A. Siddiqi, W. Pak and M. Siddiqi, *A study on the psychology of social* …, op. cit.

The further cognitive modeling on the basis of the created model (map) reproduces various scenarios of system development, in particular, identifying changes that will occur if a certain parameter increases (or decreases), and vice versa - what should be changed to maximize or minimize the target vertex.

Based on the analysis of general methods of social engineering, forms of attacks, social engineering methods of influence aimed at the qualities of human nature and actions of a social engineer, a cognitive map of the social engineer's influence on the object, which is a complex information system, is constructed.

The following components were used to build the cognitive map:

Privileged (target) vertex - System resistance to attacks;

Basic concepts – factors that lead to information security violations by employees under the influence of actions (methods used) by a social engineer:

1. "Working conditions" – optimal, acceptable, harmful, dangerous.
2. "Social protection" – social security package.
3. "Remuneration for work" – wages.
4. "Security" – a feeling of anxiety, fear, etc. caused by external circumstances.
5. "Mode/specificity of work" – work schedule, confidentiality, secrecy policy, etc.
6. "Document" – access levels, complexity of processing.
7. "Technical devices and equipment" – the requirement of skills and abilities, cyber hygiene.
8. "Software" – the requirement of skills and abilities, cyber hygiene, differentiation of access to authorized users.
9. "Training" – opportunities for learning and development.
10. "Experience" – requirements for work experience, in particular with a particular software, device, document, etc.
11. "Professional development" – opportunities for professional self-improvement.
12. "Career growth" – opportunities for promotion.
13. "Motivation" – support, leadership, mutual respect, bonus system.
14. "Methods of personnel management" – economic, organizational and administrative, and social and psychological.
15. "Psychological comfort" – the psychological microclimate within the organization.
16. "Staff turnover" is the movement of personnel in an organization caused by employee dissatisfaction.

A cognitive map of the impact on the object by social engineering methods is shown in Fig. 1.

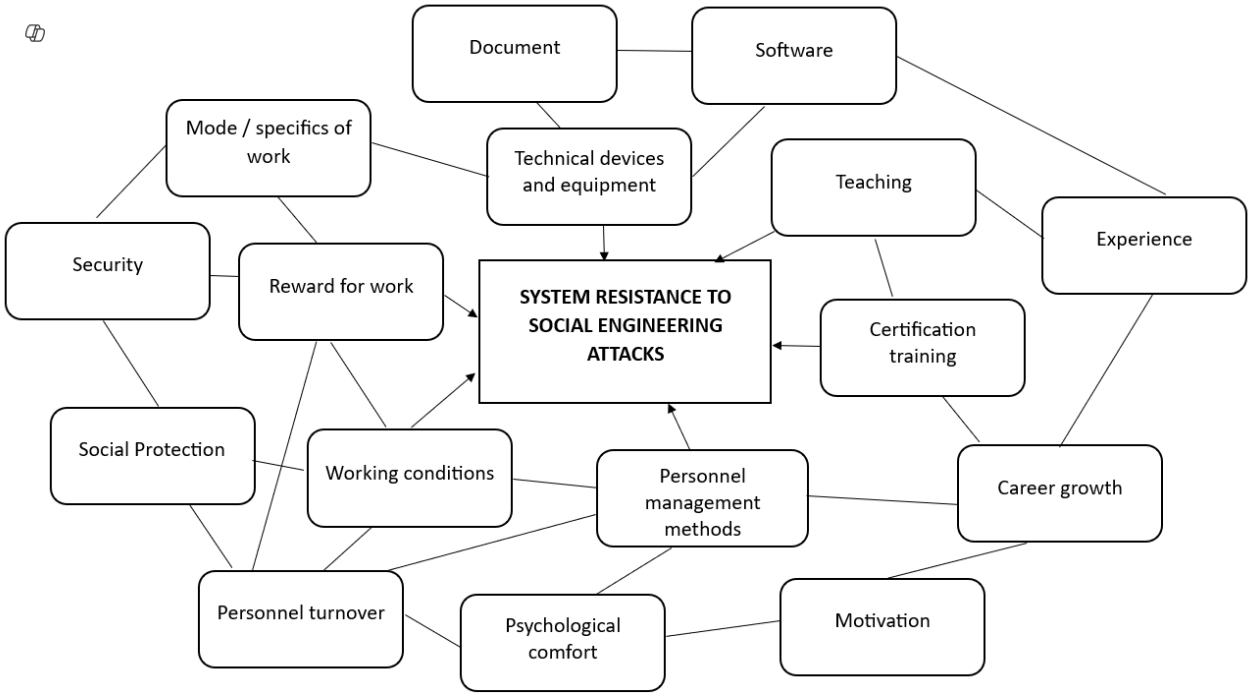

Fig. 1. Cognitive map of impact on an object by social engineering methods
Source: Own study.

To protect users from the actions of social engineers, it is recommended to use both organizational (at the level of an institution, organization) and software and hardware tools.

Organizational means of ensuring information protection currently include organizational and technical (preparation of premises taking into account access restriction requirements, etc.) and organizational and legal (requirements of national legislation, etc.) means. Their advantage is due to the possibility of solving various problems, ease of implementation and unlimited possibilities for modification and development.

Technical (hardware) means include various types of devices that either prevent physical penetration of an intelligence object (security alarms, etc.) or detect and block potential information leakage channels (noise generators, surge protectors, scanning radios, etc.). Their advantages are reliability, independence from subjective factors, and high resistance to modification. The main disadvantage is usually the cost aspect. Software tools include programs for user identification, access control, information encryption, temporary file extraction, etc.

MATHEMATICAL CALCULATIONS FOR A COGNITIVE IMPACT MAP

To model the impact of social engineering on a system, we will use the method of cognitive analysis. Let the system be represented as a set of factors $F\{F_1, F_2, F_n\}$, where each factor characterizes a certain aspect of the system's stability. The influence of the factors on each other can be represented as a matrix of relations W, where W_{ij} determines the strength of the influence of the factor F_i on F_j .

The dynamics of system changes is described by the equation:

$$F(t+1) = W\ (F(t)) \tag{2}$$

Where $(F(t)$ is the vector of the system state at time *t, W,* is the influence matrix.

To determine the critical factors, we introduce the sensitivity coefficient C_i , which is calculated as follows:

$$C_i = \sum_{j=1}^{n} |W_{ij}| \tag{3}$$

A high value of C_i means that the factor F_i has a significant impact on the entire system.
Risk minimization algorithm

To reduce the risk of social attacks, it is recommended to:

1. Increase the level of cyber literacy of users (increase).
2. Use multi-level authentication (increase).
3. Regularly test staff for vulnerability to social attacks.
4. Analyze critical factors to determine priority security measures.

Implementation of this risk minimization algorithm will significantly reduce the likelihood of successful social engineering attacks, ensure a higher level of user awareness, and increase the overall resilience of the organization to cyber threats. An integrated approach to protecting information systems includes both staff training and implementation of technical solutions, as well as the formation of a cybersecurity culture, which is a key factor in the modern digital environment.

PRACTICAL APPLICATION OF THE RESULTS

The proposed methods can be used to increase the resilience of organizations to social engineering attacks. They are effective for both government agencies and the private sector, where information security issues are critical.

PERSPECTIVES FOR FURTHER DEVELOPMENT

Further research can be aimed at:

- development of more sophisticated attack prediction models that take into account changing user behavioral patterns;
- integrating machine learning and artificial intelligence methods to detect threats in real time;
- creation of adaptive security systems that will automatically respond to attempts of social attacks;
- studying the effectiveness of various staff training strategies in the context of preventing social attacks;

– introducing new cryptographic security mechanisms to reduce the risks of social engineering.

CONCLUSIONS

The research has examined social engineering as a multidimensional phenomenon that combines methods of psychological influence, information technology, and social manipulation. The main mechanisms of attacks, such as phishing, vishing, and spear phishing, are analyzed and their effectiveness in the context of modern cyber threats is considered. Particular attention is paid to the role of the human factor as a key vulnerability in information systems, which is confirmed by statistics on a significant share of attacks made possible by insufficient user awareness.

A proposed cognitive model for analyzing social attacks is used to assess the relationship between the level of user security, behavioral factors, and the probability of attack success. The research has confirmed that the main triggers of successful attacks are trust, fear, hasty decision-making and lack of critical thinking in interaction with information resources.

The use of probabilistic modeling of social engineering attacks allowed us to identify critical parameters that affect their effectiveness. The proposed risk assessment model confirmed that increasing the level of user awareness by 30% can reduce the success of attacks by 2 times, and the introduction of multi-level authentication and minimum privilege policies significantly complicates the implementation of attack scenarios.

Based on the results obtained, an algorithm for minimizing the risks of social engineering has been developed, which includes:

– increasing the level of cyber literacy of users through training programs and regular testing;
– use of multi-level authentication and adaptive access control methods;
– analysis of critical risk factors to develop individualized protection measures;
– implementation of technologies for detecting anomalous behavior and anti-phishing systems;
– creating a security culture in the organization through motivational measures and information campaigns.

The research results confirm that the human factor is the most vulnerable component in modern security systems, and its manipulation through social engineering remains one of the most effective strategies for gaining unauthorized access to information resources.

In summary, the models and approaches proposed in this study can be used as a basis for developing new cyber defense strategies, security policies, and training programs. Further research can be aimed at automating the processes of detecting socio-engineering attacks, analyzing the behavioral characteristics of users, and developing adaptive protection methods based on artificial intelligence.

The results are of practical importance for organizations seeking to reduce the risks of social engineer attacks and can be used to improve the overall level of cybersecurity in government and corporate structures.

REFERENCES

Avkurova Zhadyra, Gnatyuk Sergiy, Abduraimova Bayan, Makulov Kaiyrbek. 2024. "Targeted Attacks Detection and Security Intruders Identification in the Cyber Space". International Journal of Computer Network and Information Security 16(4): 144-153.

Bałuszyński Sławomir, Kluczewska-Chmielarz Kamila, Lis Dawid. 2024. „Contemporary Hazards for Drivers". Zeszyty Naukowe Wyższej Szkoły Finansów i Prawa w Bielsku-Białej (28)4: 40-46. DOI: 10.19192/wsfip.sj4.2024.6.

Buryachok Volodymyr Leonidovych, Tolubko, Volodymyr Borysovych, Khoroshko Volodymyr Oleksiyovych, & Tolyupa Serhii Vasylovych. 2015. Information and Cybersecurity: A Socio-Technical Aspect: A Textbook. Kyiv: DUT.

Butavicius Marcus, Parsons Kathryn, Pattinson Malcolm, McCormac Agata. 2016. "Breaching the human firewall: Social engineering in phishing and spear-phishing emails". Computers & Security 57: 70–87. https://doi.org/10.1016/j.cose.2015.12.006.

Czaja Piotr, Kluczewska-Chmielarz Kamila, Porębska Joanna, Noga Henryk, Szczypka-Brodzińska Beata. „Techniki informacyjne w zarządzaniu szkołą". Edukacja Ustawiczna Dorosłych (2): 79-95. DOI: 10.34866/6nxf-qx89.

Darbek Temirkhan, Mukasheva Assel, Bissembayev Alibek, Gnatyuk Sergiy, Mukammejanova Dinargul. 2024. Research and development of two-factor authentication methods using neural networks In Proceedings of the IEEE 4th International Conference on Smart Information Systems and Technologies, 340-345, (SIST 2024), Almaty.

Gajewska Agnieszka, Noga Henryk, Piotrowski Tomasz. 2022. „Kompetencje funkcjonariuszy Policji w zakresie bezpieczeństwa i porządku publicznego na przykładzie dzielnicy Kraków Nowa Huta wobec wyzwań edukacji dla bezpieczeństwa". Edukacja Ustawiczna Dorosłych 2(4): 95–105. DOI: 10.34866/13ab s288.

Gajewska, Agnieszka, Noga Henryk, Grzegorzewska, Maria Katarzyna. 2023. „Bezpieczeństwo i porządek publiczny w systemie funkcjonowania państwa na przykładzie działań w dzielnicy Kraków Nowa Huta jako wyzwania edukacji dla bezpieczeństwa". Edukacja Ustawiczna Dorosłych (2): 167–175. DOI: 10.34866/3930 0504.

Gnatyuk Sergiy, Berdibayev Rat, Aleksander Marek. et al. "Software System for Cybersecurity Events Correlation and Incident Management in Critical Infrastructure, Lecture Notes on Data". Engineering and Communications Technologies (213): 247-269.

Greavu-Şerban Valerică, Floredana Constantin, Sabina-Cristiana Necula. 2025. Exploring heuristics and biases in cybersecurity: A factor analysis of decision-making in social engineering contexts. Systems, 13(4), 280. https://doi.org/10.3390/systems13040280.

Islam Abdalla Mohamed Abass. 2018. "Social Engineering Threat and Defense: A Literature Survey". Journal of Information Security, (9): 257-264 http://www.scirp.org/journal/jis.

Kasianchuk Mykhailo, Karpinski Mikołaj, Kochan Roman, Karpinskyi Volodymyr, Litawa Grzegorz, Shylinska Inna, Yakymenko Igor. 2020. Developing symmetric encryption

methods based on residue number system and investigating their cryptosecurity. IACR Cryptology ePrint Archive, 2020/589. https://eprint.iacr.org/2020/589.

Konrad Tetiana, Pysarchuk Oleksij, Noga Henryk, Gajewska Agnieszka, Volkogon Viktoriya, Baran Danylo. 2024. Method of Multifactor Analysis of the Alternatives Using the Example of Multi-criterial Selection of the Optimal Cargo Transportation Route. In: Proceedings of Ninth International Congress on Information and Communication Technology. ICICT 2024 2024 (6), 73-85, Lecture Notes in Networks and Systems, London, DOI: https://doi.org/10.1007/978-981-97-3299-9_6.

Melnychenko Anatolii Anatolievich. 2008. "The Problem of the Relationship Between Social Engineering and Social Management: A Philosophical Reflection". Bulletin of NTUU "KPI". Philosophy. Psychology. Pedagogy (1)22: 40-43.

Melnychenko Anatolii Anatolievich. 2012. "Social Engineering as a Factor in Ensuring the Sustainable Development of Social Systems". Bulletin of NTUU "KPI" Political Science. Sociology. Law (1)13: 73-78.

Montañez-Rodriguez Rosana, Golob Edward, Xu Shouhai. 2020. "Social engineering cyberattacks and human cognition: A psychology perspective". Frontiers in Psychology, 11, 1755. https://doi.org/10.3389/fpsyg.2020.01755.

Muhammad Shofian Tsauri. 2025. "Human Vulnerabilities to Social Engineering Attacks: A Systematic Literature Review for Building a Human Firewall". Journal of Applied Informatics and Computing (JAIC) 9(4): 1127-1136.

Murtaza Ahmed Siddiqi, Wooguil Pak and Moquddam Siddiqi. 2022. "A Study on the Psychology of Social Engineering-Based Cyberattacks and Existing Countermeasures". Applied Sciences 12(12), 6042. https://doi.org/10.3390/app12126042

Naz Anam, Sarwar Madiha, Kaleem Muhammad, Mushtaq Muhammad Azhar, Rashid Salman. 2024. "A comprehensive survey on social engineering-based attacks on social networks". International Journal of Advanced and Applied Sciences 11(4): 139–154. https://doi.org/10.20474/ijaas-11.4.3.

Salahdine Fatima, El Mrabet Zakaria, Kaabouch Naima. 2022. "Phishing attacks detection: A machine learning-based approach". Computers & Security, 118, 102720. https://doi.org/10.1016/j.cose.2022.102720.

Sandor Andrei, Tonț Gabriel, Simion Eduard. 2021. "A mathematical model for risk assessment of social engineering attacks". SSRN Electronic Journal. https://doi.org/10.2139/ssrn.4180646.

Schmitt Marc, Flechais Ivan. 2024. "Digital deception: Generative artificial intelligence in social engineering and phishing". Artificial Intelligence Review (57) 324. https://doi.org/10.1007/s10462-024-10973-2.

Siddiqi Murtaza Ahmed, Pak Woguil, Siddiqi Moquddam A. 2022. "A study on the psychology of social engineering-based cyberattacks and existing countermeasures". Applied Sciences 12(12), 6042. https://doi.org/10.3390/app12126042.

Toapanta, Fabricio, Belén Rivadeneira, Christian Tipantuña, and Danny Guamán. 2024. "AI-Driven Vishing Attacks: A Practical Approach". Engineering Proceedings 77(1): 15. https://doi.org/10.3390/engproc2024077015.

Triantafyllopoulos Andreas, Anika Spiesberger, Iosif Tsangko, Xin Jing, Verena Distler, Felix Dietz, Florian Alt, Björn Schuller. 2025 Vishing: Detecting social engineering in spoken

communication — A first survey & urgent roadmap to address an emerging societal challenge. Computer Speech & Language (94). 101802. https://doi.org/10.1016/j.csl.2025.101802

Udochukwu David G., Bode-Asa Ayomide. 2023. An overview of social engineering: The role of cognitive biases towards social engineering-based cyber-attacks, impacts and countermeasures. Preprint on ResearchGate. https://doi.org/10.13140/RG.2.2.12421.12003.

Unchit Plot, Das Sanchari, Kim Andrew L., Camp L. Jean. 2020. "Quantifying susceptibility to spear phishing in a high-school environment using signal detection theory". Journal of Cybersecurity 6(1). https://doi.org/10.48550/arXiv.2006.16380.

Volkogon Viktoriia, Konrad Tetiana, Kolganova Olena, Tereshchenko Lidiia. 2023. Situational Synthesis of Algorithmic Support of Regional Transport Systems based on Expert System. In: Proceedings of the International Workshop on Advances in Civil Aviation Systems Development, 100-114, Kyiv.

Vyshnovskyi Vyacheslav Viktorovych, Tkachuk Lyudmyla Mykolaivna. 2018. Social Engineering as a Means of Influencing Human Consciousness. XLVII Scientific and Technical Conference of the Institute for Integration of Learning with Production. In https://ir.lib.vntu.edu.ua//handle/123456789/20485?utm_source=chatgpt.com,

Yesypovych, Kateryna Petrivna. 2013. "The Phenomenon of Cognitive Mapping in the Modern Linguistic Paradigm". Studia Linguistica (7): 254-257.

Yichiet Aun, Ming-Lee Gan, Nur Haliza Binti Abdul Wahab, Goh Hock Guan. 2023. „Social Engineering Attack Classifications on Social Media Using Deep Learning". Computers, Materials & Continua 74(3): 4917–4931. https://doi.org/10.32604/cmc.2023.032373

Yueqiang Cheng, Zhi Zhang, Yansong Gao, Zhaofeng Chen, Shengjian Guo, Qifei Zhang Rui Mei, Surya Nepal, Yang Xiang. 2022. „Meltdown-type attacks are still feasible in the wall of kernel page-Table isolation". Computers & Security, Volume 113, 102556 https://doi.org/10.1016/j.cose.2021.102556

Ziubina Ruslana, Litawa Grzegorz, Szklarczyk Rafał, Biel Patryk, Veselska Olga, Nikodem Joanna J. 2020. "Detection of viruses using machine learning method. In Proceedings of the Pacific Asia Conference on Information Systems (PACIS 2020) (Paper 9). Association for Information Systems. In https://aisel.aisnet.org/pacis2020/9.