ISSN 1814-4225 (print)
ISSN 2663-2012 (online)

UDC 004.056.53(045) **doi: 10.32620/reks.2025.2.15**

Oleksandr KORCHENKO[1, 2], Anna KORCHENKO[1,3], Serhii ZYBIN[4], Kyrylo DAVYDENKO[3]

[1] ***University of the National Education Commission, Krakow, Poland***
[2] ***State University of Information and Communication Technologies, Kyiv, Ukraine***
[3] ***National Technical University Dnipro Polytechnic, Dnipro, Ukraine***
[4] ***National Aviation University, Kyiv, Ukraine***

AN APPROACH FOR CLASSIFYING SOCIOTECHNICAL ATTACKS

*The primary research **goal** is to develop a method for constructing a classification model of modern approaches to implementing sociotechnical attacks, to systematize and integrate existing classifications of relevant approaches, with the possibility of expanding with new characteristic features. The development of information technology and data exchange creates new threats to cyber security, including cyber attacks and frauds. Social networks and artificial intelligence contribute to the improvement of sociotechnical methods. Analyzing the data of leading studies, certain methods are identified that social engineers use most often, but these publications do not form a set of signs that characterize the approaches to implementation of the corresponding attacks, which will make it possible to formalize the process of their classification from a systemic standpoint. The research is aimed at solving the following **tasks**: toconstruct a model for classifying sociotechnical attacks in which it is possible to develop a generalized hierarchical model; to form a generalized set of features, criteria, and sub-criteria, which allows us to select and develop appropriate means of countering sociotechnical attacks from a systemic perspective; and to carry out the modelling of a corresponding cyberattack for a systematic understanding of actions and countermeasures. Given this, the analysis and classification of modern approaches to the implementation of sociotechnical attacks is an important component of a cyber security strategy to ensure protection against ever-growing threats and is an urgent scientific task. **Results and conclusions.** Based on the multi-theoretical approach, a method is proposed, in which, due to the stages of determining the set: identifiers of signs, criteria, and sub-criteria, it is possible to develop a generalized hierarchical model for classifying socio-technical attacks according to the characteristic principle. Based on the proposed model and the analyzed literature, a generalized set of features, criteria, and sub-criteria has been formed, such as: time aspect, industry affiliation, interaction with security policy, remoteness, initialization, tools, manipulation, violation of characteristics, relational signs, severity level, type of attacked source, type of access, type of appeal, type of sociotechnical technique, and scale, which allows us to select and develop appropriate means of countering sociotechnical attacks from a systemic perspective. The example of conducting a sociotechnical attack is considered, in which, taking into account the MAISA classification model and such steps of their implementation as: target research, preparation of a sociotechnical attack, performing of the attack, exploitation of the information received, hiding traces, made it possible to approach the understanding of the actions of a sociotechnician when implementing a phishing attack from a systemic perspective for the further development of appropriate countermeasures. In addition, based on the obtained criteria, it is possible to develop a method for assessing personnel readiness to counter various classes of sociotechnical attacks.*

Keywords: *cyber security; data protection; information security; sociotechnical attacks; sociotechnical attack methods; social engineering.*

1. Introduction

1.1. Motivation

The rapid development of information technologies and the intensive exchange of data via the Internet create new opportunities and threats to security. With the use of advanced technologies, offenders can perform cyber attacks on corporate information resources, industrial systems, critical infrastructure, etc. The demand for digital services and products has given rise to new types of cybercrime such as fraud, identity theft, phishing and others. The rapid data exchange over the Internet creates unique opportunities for cyber-espionage, when, for example, private information can be stolen or intercepted, which leads to a violation of such basic security characteristics such as privacy [1]. Violators can use IT infrastructure to conduct cyber-terrorist acts, for example, by exploiting vulnerabilities in critical infrastructure management systems.

In addition, new methods and opportunities for social engineering application have recently emerged. For example, social networks and artificial intelligence can be used by offenders to gather information about

potential victims and conduct attacks. The behaviour and online habits of users are constantly changing. Therefore, cybercriminals are constantly looking for new ways to implement attacks and improve their methods.

The most vulnerable element in the cyber security system is the human being, therefore the main attention of violators is directed at the use of sociotechnical methods.

A systemic attitude toward the formation of classification and understanding modern approaches to the implementation of sociotechnical attacks will allow the development of effective security measures for users and organizations.

In connection with the above, the analysis and classification of modern approaches to the implementation of sociotechnical attacks (MAISA) is an important component of the cyber security strategy to ensure protection against ever-growing threats and is an urgent scientific task.

This study is dedicated to developing a model for classifying sociotechnical attacks.

The remainder of this article is organized as follows. Section 1: discusses the motivation underlying this study; provides an overview of sociotechnical attacks methods to obtain information or gain unauthorized access; and offers an analysis of leading studies. Section 2 describes the appropriate model, which is based on the specified criteria for classifying approaches to the implementation of sociotechnical attacks and consists of three stages. Section 3 presents discussion the analysis results of modern approaches to the implementation of sociotechnical attacks and sets of criteria when performing a sociotechnical cyber attacks. Section 4 presents conclusions based on the research results, focusing on the set of signs that allow selection and development of appropriate countermeasures against sociotechnical attacks from systemic positions.

1.2. State of the art

Social engineering is the process of manipulating people in order to obtain information with limited access or to gain unauthorized access to information system resources (ISR). Violators use psychological manipulation and exploit human credulity, fear, inattention, and ignorance to achieve their goals [2, 3]. That is, this type of attack is primarily aimed at not the hardware or software component of the information system but at its personnel and users – the "weakest link". Although this task may seem complex and technically sophisticated, it can often be a simple and effective approach to the implementation of attacks because techniques from psychology, social sciences, and interpersonal interactions are used.

The implementation of sociotechnical attacks comprises several stages. At the initial stage (research stage), the offender conducts reconnaissance in order to obtain information about the target organization or person, for example, the organizational structure, roles of employees, their behaviour, etc. Information can be collected through company websites, social media, or even personal visits. Next, during the planning stage, the offender uses the received information in order to choose an attack method and develop a strategy. They also identify specific messages or scripts to manipulate targeted individuals. In the final stage, the attacker typically implements the attack by sending specially crafted messages via e-mail or other online channels. Some attacks require active interaction with the victim, whereas others can be automated and activated, for example, by clicking on malicious links.

Analyzing the leading studies [4, 5], we can distinguish the following methods that are most often used in social engineering attacks: phishing, watering hole, whaling attack, pretexting, baiting and quid pro quo, vishing, honeypot, backdoor, pharming, smishing, spear phishing, and whaling [6, 7]. However, for example, in the mentioned publications [8, 9], the sets of signs that characterize approaches to the implementation of sociotechnical attacks are not formed, which makes it possible to formalize the process of their classification from a systemic point of view.

The use of social engineering affects users of sociotechnical systems due to existing vulnerabilities. Among them are distinguished characteristics such as weaknesses, needs, passions, and hobbies. The manipulation of these vulnerabilities [10, 11] is aimed at encouraging users to a new model of behaviour and, as a result, gaining unauthorized access to information. In [10, 12], it was stated that manipulation of information is a process of influencing the beliefs of other people by simplifying, inventing, or distorting facts or events and can consist of methods such as disinformation, fabrication, and distortion of facts. However, in the above-mentioned sources, research on a specific set of criteria by which modern sociotechnical methods of detecting attacks can be characterized has not been conducted.

In [4], the main types of attacks and scenarios of social engineering were proposed, as well as an approach that uses the synergy of existing methods aimed at training users to protect personal information and data [13]. In [14], a study was presented that uses attacks such as fake access points and phishing pages, and a method of countering social engineering on information activity objects was suggested [7, 9]. However, in these papers, sociotechnical methods are not considered in relation to the possibility of forming a set of sub-criteria by which they can be identified.

In [11, 15], the psychological mechanisms that are used to influence people and can be used in sociotechnical attacks were studied. These mechanisms are used to

ISSN 1814-4225 (print)
ISSN 2663-2012 (online)

manipulate emotions, beliefs, or psychological pressures in order to gain access to confidential information or perform certain actions in favour of the offender. However, in these studies, attention is not concentrated on a set of possible signs of sociotechnical methods, such as time aspect, sectoral affiliation, interaction with security policy, remoteness, initialization, toolkit, violation of characteristics, relational signs, degree of difficulty, type of the attacked source, type of access, type of addressing, type of social engineer, scale, etc.

In [16], state-of-the-art methods of social engineering testing to determine an organization's vulnerabilities to appropriate attacks were presented, and a methodology that can be used to conduct an ethical social engineering test is presented, but the paper lacks a specific study on the formation of a set of sub-criteria for categorizing approaches to implementation of these attacks.

In [5, 6] are analyzed some methods of countering social engineering, for example the method of penetration testing which is focused on identifying and preventing the use of human vulnerabilities. Some ways of implementation of the mentioned methods are described, and a classification of the signs of sociotechnical attacks is presented. However, this classification does not reveal the proposed methods according to signs such as time aspect, sectoral affiliation, remoteness, degree of difficulty, type of attacked source, type of access, type of addressing, type of social engineer, scale, etc.

In [17, 18], the main approaches of social engineering at the enterprise are shown, namely methods built on human weaknesses, in particular, on the use of the "curiosity" and "trust" instincts. Mechanisms have been proposed that make it possible to promptly monitor and detect social engineering signs in the early stages, to warn against cyber threats at the enterprise, and to counter social hacking [19, 20]. However, these techniques and methods do not provide a conceptual understanding of the entire possible set of signs by which modern social technicians can be characterized.

Paper [21] shows the use of fuzzy directed social graphs to create a model for analyzing the vulnerabilities of sociotechnical systems to the effects of social engineering, but it does not consider a set of existing characteristics of relevant attacks, such as time aspect, sectoral affiliation, interaction with security policy, remoteness, initialization, toolkit, violation characteristics, relational signs, degree of severity, type of the attacked source, type of access, type of addressing, and scale.

In [22], an algorithm for executing social technicians' actions was considered. Techniques used to manipulate people and obtain information remotely through remote means of communication, communication channels such as e-mails, phone calls, messages in social networks, and Internet fraud, have also been presented [23, 24]. However, these papers do not reveal the general set of signs and criteria for the selection and classifying approaches to implementing sociotechnical attacks.

Papers [25, 26] have revealed the impact of sociotechnical attacks on a person in cyberspace and offer an appropriate classification of attacks, but the study lacks an analysis of the criteria and sub-criteria that characterize modern sociotechnical approaches to identifying relevant attacks.

In [20, 27], a fairly deep classification of sociotechnical attack methods was conducted; however, due to the rapid progress in modern information technologies, such attacks have become more common and complex, and combinational approaches and techniques are used for their implementation. For successful development and implementation of effective countermeasures against sociotechnical attacks, it is necessary to expand the list of modern methods and supplement their characteristics with new criteria. However, unfortunately, in these studies, no certain sets of signs, for example, time aspect, sectoral affiliation, and scale of the attack for approaches characterizing sociotechnical actions have been formed.

1.3. Objectives and tasks

Considering the above mentioned, the purpose of the work is to develop a method for constructing a classification model of modern approaches to implementing sociotechnical attacks, to systematize and integrate existing classifications of relevant approaches [27, 28] with the possibility of expanding with new characteristic features. This makes it possible to train personnel to resist sociotechnical threats from a systemic standpoint.

In addition, based on the conducted research, it is possible in the future to design new methods of assessing personnel readiness to counter sociotechnical attacks.

To achieve the set goal, the following tasks must be solved:

1. Based on the multi-theoretical approach, it is necessary to propose a method for developing a model for classifying sociotechnical attacks, in which it is possible to develop a generalized hierarchical model.

2. Based on the proposed model and the analyzed literature, a generalized set of features, criteria, and subcriteria should be formed to allow us to select and develop appropriate means of countering sociotechnical attacks from a systemic perspective.

3. A sociotechnical attack example should be considered.

2. Materials and methods of research

Considering the results of known studies and their further generalization, an analysis and classification of

MAISA was carried out according to the following criteria: time aspect, sectoral affiliation, interaction with security policy, initialization, type of requests, toolkit, violation of characteristics, degree of severity, relational features, type of the attacked source, type of access, remoteness, manipulation, type of the social engineer, and scale (Fig. 1).

The appropriate model is based on the specified criteria and sub-criteria for classifying modern approaches to the implementation of sociotechnical attacks.

The model development method consists of the following stages:

Stage 1 – defining a set of identifiers of signs for classifying of approaches to implementation of sociotechnical attacks.

Stage 2 – defining a set of criteria for classifying approaches to the implementation of sociotechnical attacks.

Stage 3 – defining a set of sub-criteria for classifying of approaches to implementation of sociotechnical attacks.

2.1. Developing stages

Stage 1. Let us introduce a set of identifiers of signs S of all possible identifiers for classifying of approaches implement sociotechnical attacks

$$S = \{\bigcup_{i=1}^{n} S_i\} = \{S_1, S_2, ..., S_n\}, \ (i = \overline{1,n}), \qquad (1)$$

where S_i – i-th identifier of the signs for classifying of approaches to implementation of sociotechnical attacks, and n – their number.

For example, for $n = 15$ according to (1) in Fig. 1, the set S can be represented as:

$$S = \{\bigcup_{i=1}^{15} S_i\} = \{S_1, S_2, ...S_{15}\} =$$
$$= \{S_{TA}, S_{SA}, S_{SP}, S_I, S_{ADD}, S_{ST}, S_{VC}, S_{DS}, S_{RS}, S_{AS}, S_{ACC}, S_R, S_M, S_{SE}, S_S\} =$$
$$= \{TA, SA, SP, I, ADD, T, VC, DS, RS, AS, ACC, R, M, SE, S\},$$

CLASSIFICATION SIGNS (CRITERIA) OF IMPLEMENTATION OF SOCIOTECHNICAL ATTACKS

1. BY THE TIME ASPECT	2. BY SECTORAL AFFILIATION	3. BY INTERACTION WITH SECURITY POLICY	4. BY INITIALIZATION		5. BY ADDRESSING
SP-attacks	CS-attacks	PTP-methods	C-attacks	CA-attacks CP-attacks	OVS-methods
PP-attacks	PI-attacks	DP-methods	UC-attacks		RVS-methods

6. BY THE TOOL	7. BY VIOLATION OF CHARACTERISTICS	8. BY DEGREE OF SEVERITY	9. BY THE RELATIONAL SIGN	10. BY THE TYPE OF THE ATTACKED SOURSE	11. BY THE TYPE OF ACCESS
SW-methods	CV-methods	SPL-attacks	MN-attacks	ED-attacks	OS-attacks
HW-methods	IV-methods	CPX-attacks	PN-attacks	CFP-attacks	COS-attacks
AT-methods	AV-methods	SYST-attacks	MPL-attacks	CD-attacks	CIS-attacks
			PPL-attacks	OP-attacks	SIS-attacks

12. BY REMOTENESS							13. BY MANIPULATION	14. BY THE TYPE OF THE SOCIAL ENGINEER		15. BY SCALE
Local				Remote			AB-manipulation	H-performed	RT-performed	LL-attacks
LC-attacks	LWP-attacks	LW-attacks	LDA-attacks	TB-attacks	NT-attacks	RPT-attacks	FB-manipulation	PT-performed	SL-performed	
							MB-manipulation	SP-performed	RC-performed	
							RB-manipulation	ITT-performed	PS-performed: GO-performed	WW-attacks
							SB-manipulation	DE-performed	PS-performed: MP-performed	
							LB-manipulation	F-performed	PS-performed: PSY-performed PS-performed: LWR-performed	

Fig. 1. Classification criterion (sign) of modern approaches to implementation of sociotechnical attacks

ISSN 1814-4225 (print)
ISSN 2663-2012 (online)

where $S_1 = S_{TA} = TA$, $S_2 = S_{SA} = SA$, $S_3 = S_{SP} = SP$, $S_4 = S_I = I$, $S_5 = S_{ADD} = ADD$, $S_6 = S_T = T$, $S_7 = S_{VC} = VC$, $S_8 = S_{DS} = DS$, $S_9 = S_{RS} = RS$, $S_{10} = S_{AS} = AS$, $S_{11} = S_{ACC} = ACC$, $S_{12} = S_R = R$, $S_{13} = S_M = M$, $S_{14} = S_{SE} = SE$, $S_{15} = S_S = S$ are the identifiers of the signs "BY THE TIME ASPECT", "BY SECTORAL AFFILIATION", "BY INTERACTION WITH SECURITY POLICY", "BY INITIALIZATION", "BY ADDRESSING", "BY TOOL", "BY VIOLATION OF CHARACTERISTICS", "BY DEGREE OF SEVERITY", "BY RELATIONAL SIGNS", "BY THE TYPE OF THE ATTACKED SOURCE", "BY THE TYPE OF ACCESS", "BY REMOTENESS", "BY MANIPULATION", "BY THE TYPE OF THE SOCIAL ENGINEER", "BY SCALE" respectively.

Stage 2. Let us define $S_i \subseteq S$ $(i = \overline{1,n})$ as

$$S_i = \{\bigcup_{j=1}^{m_i} C_{ij}\} = \{C_{i1}, C_{i2}, ..., C_{im_i}\}, \ (j = \overline{1,m_i}), \qquad (2)$$

where $C_{ij} \subseteq S_i$ is a set of criteria of the i-th identifier of the j-th criterion in the classification of approaches to implementation of sociotechnical attacks, and m_i – their number.

Next, taking (2) into account, expression (1) can be presented in the form:

$$S = \{\bigcup_{i=1}^{n} S_i\} = \{\bigcup_{i=1}^{n}\{\bigcup_{j=1}^{m_i} C_{ij}\}\} = \{\{C_{11}, C_{12}, ..., C_{1m_1}\}, \{C_{21}, C_{22}, ..., C_{2m_2}\}, ..., \{C_{n1}, C_{n2}, ..., C_{nm_n}\}\}. \qquad (3)$$

Further, for example, for $i = 14$, $m_{14} = 10$, and taking account of the characteristics shown in Fig. 1, the set $S_i = S_{14} = S_{TC}$ takes the following form

$$S_{14} = \{C_{14,1}, C_{14,2}, ..., C_{14,10}\} = \{C_{SE,H}, C_{SE,PT}, C_{SE,SP}, C_{SE,ITT}, C_{SE,DE}, C_{SE,F}, C_{SE,RT}, C_{SE,SL}, C_{SE,RC}, C_{SE,PS}\} = \{H, PT, SP, ITT, DE, F, RT, SL, RC, PS\},$$

where $C_{14,1} = C_{SE,H} = H$, $C_{14,2} = C_{SE,PT} = PT$, $C_{14,3} = C_{SE,SP} = SP$, $C_{14,4} = C_{SE,ITT} = ITT$, $C_{14,5} = C_{SE,DE} = DE$, $C_{14,6} = C_{SE,F} = F$, $C_{14,7} = C_{SE,RT} = RT$, $C_{14,8} = C_{SE,SL} = SL$, $C_{14,9} = C_{SE,RC} = RC$, $C_{14,10} = C_{SE,PS} = PS$ are the criteria "PERFORMED BY HACKERS", "PERFORMED BY PENETRATION TESTERS", "PERFORMED BY SPIES", "PERFORMED BY IDENTITY THIEVES", "PERFORMED BY DISSATISFIED EMPLOYEES", "PERFORMED BY FRAUDS", "PERFORMED BY RECRUITERS", "PERFORMED BY SELLERS", "REMOTE COMBINATIONS", "PARTICULAR SECTOR" respectively.

Stage 3. For each C_{ij} it is necessary to introduce a set of sub-criteria $SC_{ijk} \subseteq C_{ij}$ of classification of all possible approaches to the implementation of sociotechnical attacks, where, with respect to the j-th criterion, we can apply an array of r_j sub-criteria, which is represented by the subset:

$$C_{ij} = \{\bigcup_{k=1}^{r_j} SC_{ijk}\} = \{SC_{ij1}, SC_{ij2}, ..., SC_{ijr_j}\}, \ (k = \overline{1,r_j}), \qquad (4)$$

where SC_{ijk} is the k-th identifier of the sub-criteria of the j-th criterion of the i-th identifier of the signs of classification of approaches to implementation of sociotechnical attacks, and r_j is their number.

Next, considering of (3) and (4), expression (1) can be represented in the following form

$$S = \{\bigcup_{i=1}^{n} S_i\} = \{\bigcup_{i=1}^{n}\{\bigcup_{j=1}^{m_i} C_{ij}\}\} = \{\bigcup_{i=1}^{n}\{\bigcup_{j=1}^{m_i}\{\bigcup_{k=1}^{r_j} SC_{ijk}\}\}\} = \{\{\{SC_{111}, SC_{112}, ..., SC_{11r_1}\}, \{SC_{121}, SC_{122}, ..., SC_{12r_2}\}, ..., \{SC_{1m_1 1}, SC_{1m_1 2}, ..., SC_{1m_1 r_{m_1}}\}\}, \{\{SC_{211}, SC_{212}, ..., SC_{21r_1}\}, \{SC_{221}, SC_{222}, ..., SC_{22r_2}\}, ..., \{SC_{2m_2 1}, SC_{2m_2 2}, ..., SC_{2m_2 r_{m_2}}\}\}, ..., \{\{SC_{n11}, SC_{n12}, ..., SC_{n1r_1}\}, \{SC_{n21}, SC_{n22}, ..., SC_{n2r_2}\}, ..., \{SC_{nm_n 1}, SC_{nm_n 2}, ..., SC_{nm_n r_{m_n}}\}\}\}, \qquad (5)$$

where, for example, for $n = 15$, $m_1 = m_2 = m_3 = m_4 = m_5 = m_{12} = m_{15} = 2$, $m_6 = m_7 = m_8 = 3$, $m_9 = m_{10} = m_{11} = 4$, $m_{13} = 6$, $m_{14} = 10$, $r_{1,1} = r_{1,2} = r_{2,1} = r_{2,2} = r_{3,1} = r_{3,2} = r_{4,2} = r_{5,1} = r_{5,2} = r_{6,1} = r_{6,2} = r_{6,3} = r_{7,1} = r_{7,2} = r_{7,3} = r_{8,1} = r_{8,2} = r_{8,3} = r_{9,1} = r_{9,2} = r_{9,3} = r_{9,4} = r_{10,1} = r_{10,2} = r_{10,3} = r_{10,4} = r_{11,1} = r_{11,2} = r_{11,3} = r_{11,4} = r_{13,1} = r_{13,2} = r_{13,3} = r_{13,4} = r_{13,5} = r_{13,6} = r_{14,1} = r_{14,2} = r_{14,3} = r_{14,4} = r_{14,5} = r_{14,6} = r_{14,7} = r_{14,8} = r_{14,9} = r_{15,1} = r_{15,2} = 0$, $r_{4,1} = 2$, $r_{12,1} = 4$, $r_{12,2} = 3$, $r_{14,10} = 4$ and considering the characteristics in Fig. 1, expression (5) can be represented as:

$$S = \{\bigcup_{i=1}^{15} S_i\} = \{\bigcup_{i=1}^{15}\{\bigcup_{j=1}^{m_i} C_{ij}\}\} = \{\bigcup_{i=1}^{15}\{\bigcup_{j=1}^{m_i}\{\bigcup_{k=1}^{r_j} SC_{ijk}\}\}\} =$$

$$= \{SC_{1,1,1}, SC_{1,2,1}\},\ \{SC_{2,1,1}, SC_{2,2,1}\},\ \{SC_{3,1,1}, SC_{3,2,1}\},\ \{\{SC_{4,1,1}, SC_{4,1,2}\},\ \{SC_{4,2,1}\}\},\ \{SC_{5,1,1}, SC_{5,2,1}\},$$

$$\{SC_{6,1,1}, SC_{6,2,1}, SC_{6,3,1}\},\ \{SC_{7,1,1}, SC_{7,2,1}, SC_{7,3,1}\},\ \{SC_{8,1,1}, SC_{8,2,1}, SC_{8,3,1}\},\ \{SC_{9,1,1}, SC_{9,2,1}, SC_{9,3,1}, SC_{9,4,1}\},$$

$$\{SC_{10,1,1}, SC_{10,2,1}, SC_{10,3,1}, SC_{10,4,1}\},\ \{SC_{11,1,1}, SC_{11,2,1}, SC_{11,3,1}, SC_{11,4,1}\},\ \{\{SC_{12,1,1}, SC_{12,1,2}, SC_{12,1,3}, SC_{12,1,4}\},$$

$$\{SC_{12,2,1}, SC_{12,2,2}, SC_{12,2,3}\}\}, \{SC_{13,1,1}, SC_{13,2,1}, SC_{13,3,1}, SC_{13,4,1}, SC_{13,5,1}, SC_{13,6,1}\},$$

$$\{SC_{14,1,1}, SC_{14,2,1}, SC_{14,3,1}, SC_{14,4,1}, SC_{14,5,1}, SC_{14,6,1}, SC_{14,7,1}, SC_{14,8,1}, SC_{14,9,1}, \{SC_{14,10,1}, SC_{14,10,2}, SC_{14,10,3}, SC_{14,10,4}\}\},$$

$$\{SC_{15,1,1}, SC_{15,2,1}\} = \{SC_{TA,SP,SP}, SC_{TA,PP,PP}\},\ \{SC_{SA,CS,CS}, SC_{SA,PI,PI}\},\ \{SC_{SP,PTP,PTP}, SC_{SP,DP,DP}\},$$

$$\{\{SC_{I,C,CA}, SC_{I,C,CP}\},\ SC_{I,UC,UC}\},\ \{SC_{ADD,OVS,OVS}, SC_{ADD,RVS,RVS}\}, \{SC_{T,SW,SW}, SC_{T,HW,HW}, SC_{T,AT,AT}\},$$

$$\{SC_{VC,CV,CV}, SC_{VC,IV,IV}, SC_{VC,AV,AV}\},\ \{SC_{DS,SPL,SPL}, SC_{DS,CPX,CPX}, SC_{DS,SYST,SYST}\},$$

$$\{SC_{RS,MN,MN}, SC_{RS,PN,PN}, SC_{RS,MPL,MPL}, SC_{RS,PPL,PPL}\},\ \{SC_{AS,ED,ED}, SC_{AS,CFP,CFP}, SC_{AS,CD,CD}, SC_{AS,OP,OP}\},$$

$$\{SC_{ACC,OS,OS}, SC_{ACC,COS,COS}, SC_{ACC,CIS,CIS}, SC_{ACC,SIS,SIS}\},\ \{\{SC_{R,L,LC}, SC_{R,L,LWP}, SC_{R,L,LW}, SC_{R,L,LDA}\},$$

$$\{SC_{R,RM,TB}, SC_{R,RM,NT}, SC_{R,RM,RPT}\}\},\ \{SC_{M,AB,AB}, SC_{M,FB,FB}, SC_{M,MB,MB}, SC_{M,RB,RB}, SC_{M,SB,SB}, SC_{M,LB,LB}\},$$

$$\{SC_{SE,H,H}, SC_{SE,PT,PT}, SC_{SE,SP,SP}, SC_{SE,ITT,ITT}, SC_{SE,DE,DE},\ SC_{SE,F,F}, SC_{SE,RT,RT},\ SC_{SE,SL,SL},\ SC_{SE,RC,RC},$$

$$\{SC_{SE,PS,GO},\ SC_{SE,PS,MP},\ SC_{SE,PS,PSY},\ SC_{SE,PS,LWR}\}\},\ \{SC_{S,LL,LL}, SC_{S,WW,WW}\} =$$

$$\{(TA, SP, SP), (TA, PP, PP)\},\ \{(SA, CS, CS), (SA, PI, PI)\},\ \{(SP, PTP, PTP), (SP, DP, DP)\},$$

$$\{\{(I, C, CA), (I, C, CP)\},\ (I, UC, UC)\},\ \{(ADD, OVS, OVS), (ADD, RVS, RVS)\},$$

$$\{(T, SW, SW), (T, HW, HW), (T, AT, AT)\},\ \{(VC, CV, CV), (VC, IV, IV), (VC, AV, AV)\},$$

$$\{(DS, SPL, SPL), (DS, CPX, CPX), (DS, SYST, SYST)\},$$

$$\{(RS, MN, MN), (RS, PN, PN), (RS, MPL, MPL), (RS, PPL, PPL)\},$$

$$\{(AS, ED, ED), (AS, CFP, CFP), (AS, CD, CD), (AS, OP, OP)\},$$

$$\{(ACC, OS, OS), (ACC, COS, COS), (ACC, CIS, CIS), (ACC, SIS, SIS)\},$$

$$\{\{(R, L, LC), (R, L, LWP), (R, L, LW), (R, L, LDA)\},\ \{(R, RM, TB), (R, RM, NT), (R, RM, RPT)\}\},$$

$$\{(M, AB, AB), (M, FB, FB), (M, MB, MB),\ (M, RB, RB), (M, SB, SB), (M, LB, LB)\},$$

$$\{(SE, H, H), (SE, PT, PT), (SE, SP, SP), (SE, ITT, ITT), (SE, DE, DE),\ (SE, F, F), (SE, RT, RT),\ (SE, SL, SL),$$

$$(SE, RC, RC), \{(SE, PS, GO), (SE, PS, MP),\ (SE, PS, PSY),\ (SE, PS, LWR)\}\},\ \{(S, LL, LL), (S, WW, WW)\}.$$

Thus, based on the proposed method, we have built a set theory model for classifying of approaches to the implementation of sociotechnical attacks, which, taking into account the created characteristics (signs, criteria see Fig. 1), reflects the current state of sociotechnical threats, the graphic interpretation of which is presented in Fig. 2.

Considering the proposed generalized set theory model for the interpretation of MAISA classification, an analysis of such attacks was conducted. This analysis contributes to a deeper understanding of various aspects of social engineering and helps in the development of appropriate countermeasures. According to the proposed model and the characteristics shown in Fig. 1, each attack class is revealed.

2.2. Attack classification

1. According to the time aspect ($S_1 = S_{TA} = TA$), MAISA are divided into spontaneous attacks (SP-attacks – $C_{1,1} = C_{TA,SP} = SP$) and previously planned attacks (PP-attacks – $C_{1,2} = C_{TA,PP} = PP$).

SP-attacks occur suddenly and without prior planning. They are difficult to predict and prevent. They can be implemented at any time to cause damage or gain control over ISR. This kind of attack can be directed at any object, system, or random targets that are vulnerable at the time of attack. They usually exploit existing vulnerabilities or capabilities that appear without warning. For example, such exploits can be used as a result of automatic network scanning, or, for example, attackers can use approaches to manipulate people to make them involved in a spontaneous physical attack.

PP-attacks require advanced preparation and detailed planning and can be very complex and sophisticated. Offenders conduct a detailed analysis of potential targets and individualize their actions to maximize success. They can examine organizational structures, security schemes, personnel activities, and other aspects to identify weaknesses.

ISSN 1814-4225 (print)
ISSN 2663-2012 (online)

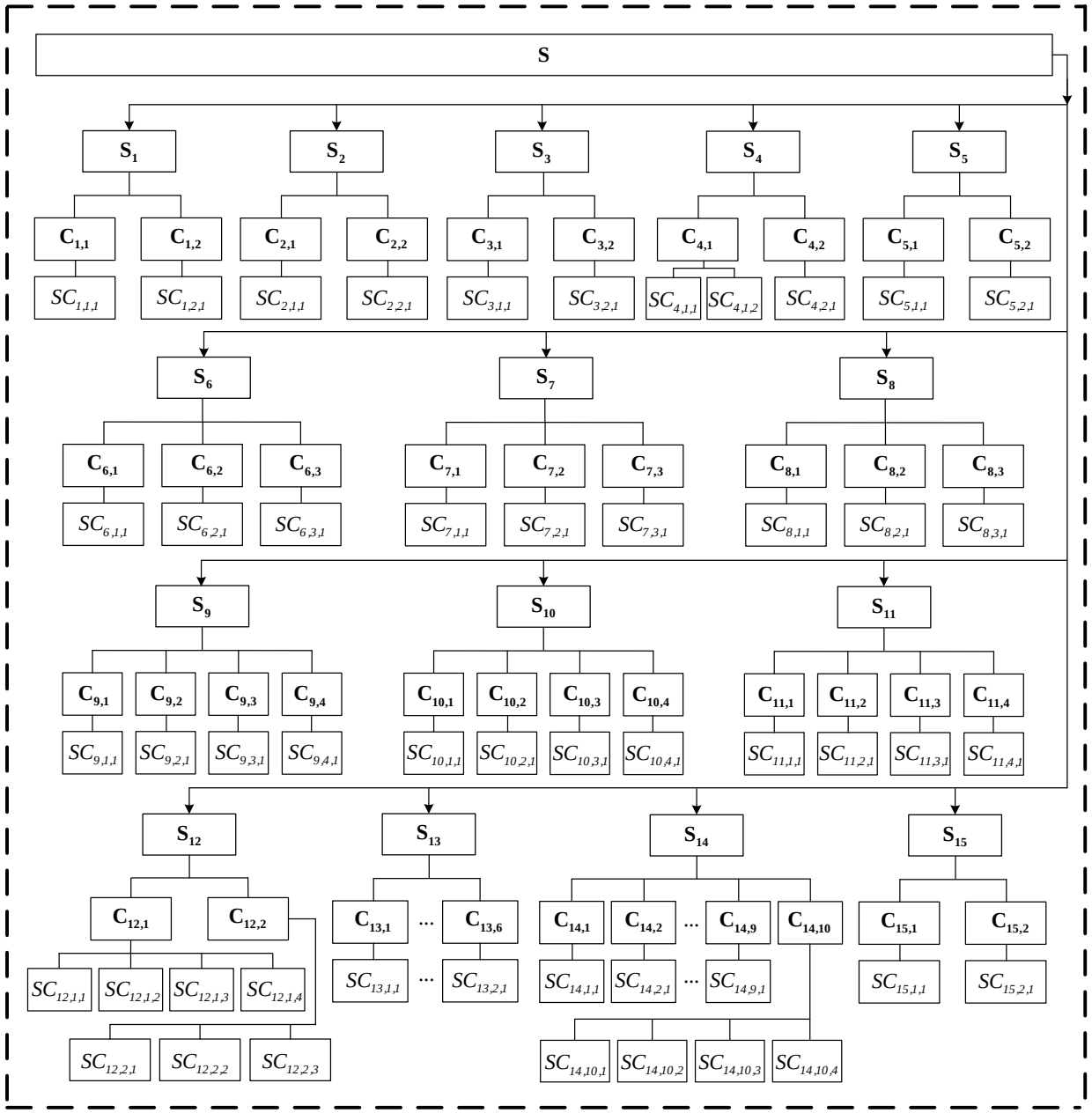

Fig. 2. The graphical interpretation of the set of signs, criteria and sub-criteria regarding classification of sociotechnical attack implementation approaches

Offenders create a detailed plan of the attack, including identifying possible attack methods, developing sociotechnical scenarios and choosing the optimal time to carry out the attack. In this study, advanced social and psychological techniques to manipulate victims and gain access to various ISRs were used. Attacks can be aimed at hacking infrastructure, including networks, servers, databases, and other resources, to gain access to critical information or gain control over certain systems. A preplanned attack may require significant effort and resources but may have the greatest potential to cause serious damage [14, 16].

2. According to sectoral affiliation ($S_2 = S_{SA} = SA$) MAISA are divided into attacks on the corporate sector (CS-attacks – $C_{2,1} = C_{SA,CS} = CS$) and on public institutions (PI-attacks – $C_{2,2} = C_{SA,PI} = PI$).

CS-attacks are aimed at enterprises and organizations for obtaining useful information or profit. For example, when engaging in business information espionage, offenders may attempt to obtain restricted information about a company's products, manufacturing processes, development plans, or other competitive advantages, such as stealing customer databases and demanding a ransom for their return. Such information is used to gain a competitive advantage, create financial losses and reduce the company's reputation. To protect against cyberattacks in the corporate sector, companies

can employ targeted cybersecurity strategies that include network and software security measures, staff training, appropriate security policies, and incident response procedures.

PI attacks target public institutions that are key to providing services and ensuring the functioning of society. These bodies are responsible for managing a country or region, making decisions, and implementing certain policies. These attacks often target government agencies and administrations, the judiciary, social services, police, municipal, educational, energy, and medical institutions. These institutions can have serious consequences because they usually have access to a large amount of confidential information, play an important role in society and are responsible for security. Attacks can target critical infrastructures, such as power grids, telecommunications systems, and financial institutions, causing significant disruption or damage. In addition, insiders or former employees of public institutions can be used to perform attacks from the inside using their access and knowledge of the organization's processes for illegal purposes. When protecting, both a comprehensive approach to ensuring the security of all its components and cooperation with other institutions and organizations to exchange information on cyber threats and joint response to them are important [29, 30].

3. According to interaction with security policy ($S_3 = S_{SP} = SP$), MAISA are divided into post politicized methods (PTP-methods – $C_{3,1} = C_{SP,PTP} = PTP$) and depoliticized methods (DP-methods – $C_{3,2} = C_{SP,DP} = DP$).

PTP-methods are based on the use of flaws in the existing security policy and can be implemented during the operation of the system and during inactivity of its individual components. For example, such shortcomings can be incorrectly constructed rules of access mediation, use of software and hardware with an insufficient level of security, errors in blocking information leakage channels with limited access, and prohibition of personnel to provide information about the source of a request that is not reliably identified [8, 31].

DP-methods involve errors and negligence that occur during the implementation of measures related to the enforcement of the existing security policy. The main reasons for this are human factors, insufficient administrative support, improper performance of protection functions and untimely response to emergencies. For example, if personnel do not comply with the requirements of security measures when requesting information with limited access from the top management of the company. If attacks are implemented using different methods, then a combined approach can be used, combining post-politicization and depoliticization methods and using flaws in both existing policies and emergency situations [32, 33].

4. By initialization ($S_4 = S_I = I$), MAISA are divided into conditional attacks (C-attacks – $C_{4,1} = C_{I,C} = C$) and unconditional attacks (UC-attacks – $C_{4,2} = C_{I,UC} = UC$). C-attacks arise as a result of a certain event provoked, for example, by the use of a logic bomb. C-attacks are divided into conditionally active attacks (CA-attacks – $SC_{4,1,1} = SC_{I,C,CA} = CA$) and conditionally passive attacks (CP-attacks – $SC_{4,1,2} = SC_{I,C,CP} = CP$).

C-attacks monitor the state of individual resources when a certain change occurs, an attack start signal is generated, for example, in the case of the disconnection of a session with a certain user's server. Such an attack can be initiated in case of going to a link to a fake page and entering confidential information on it. CP-attacks can involve the transmission of a request of a certain type from a potential target, which becomes a condition for the attack to begin.

UC-attacks do not require any particular conditions for their launch, do not depend on specific changes in the state of the ISR, and are determined by the source of the attack. They can be initiated by an offender regardless of the actions or reactions of the offender. For example, phishing attacks, where the offender sends spam messages to obtain confidential information, are examples of UC attacks [34].

5. According to the type of addressing ($S_5 = S_{ADD} = ADD$), MAISA are divided into obverse methods (OVS-methods – $C_{5,1} = C_{ADD,OVS} = OVS$) and reverse methods (RVS-methods – $C_{5,2} = C_{ADD,RVS} = RVS$).

OVS-methods (or direct communication methods) involve the actions of a social engineer attempting to gain access to information by addressing the victim directly with a fictional scenario or problem. Appropriate attacks can use specialized software to exploit the carelessness of the attacker to achieve their goals. An attacker uses approaches such as contact by telephone, e-mail, or face-to-face meetings to convince the attacked person of his/her authenticity and obtain the necessary information. An example of OVS-methods of social engineering attacks is the use of a phone call; that is, a social engineer can call an employee and introduce himself/herself as a member of the company's technical support. He/she can report possible technical problems in the work of the employee's computer and request his/her ID and password to solve the problem. Under this guise, a social engineer gains access to confidential information that can be used for malicious purposes.

RVS-methods or feedback methods for sociotechnical attacks consist of creating a situation where attacked himself/herself and turns to the attacker to solve a

ISSN 1814-4225 (print)
ISSN 2663-2012 (online)

certain problem. It may also involve the attacked party recognizing the attack and taking action to obtain information about the attacker. For example, offenders may impersonate the ISP's technical support and inform victims of possible connection problems to gain access to their computer. In such a case, the attacked party turns to the attacker for help, not suspecting that he/she is the violator.

If attacks include different approaches to interaction, the result will be a combination of methods using both forward and reverse communication, for example, an obverse-reverse type when using the two types of communication [28].

6. According to the tool ($S_6 = S_T = T$), MAISA are divided into software methods (SW-methods – $C_{6,1} = C_{T,SW} = SW$), hardware methods (HW-methods – $C_{6,2} = C_{T,HW} = HW$) and atypical methods (AT-methods – $C_{6,3} = C_{T,AT} = AT$).

SW-methods use software, espionage technologies, phishing attacks, attack fragments and other software tools to manipulate target persons and obtain necessary information.

HW-methods are based on the use of various devices, such as hidden cameras, audio recorders, electronic devices for eavesdropping or data copying, and mechanical, electrical, electromechanical, electronic, or combined devices, which help attackers perform various tasks and obtain confidential information.

AT-methods include the use of non-standard means such as explosives, radioactive materials, chemicals, or even physical threats, to obtain information.

If attacks use different types of tools, for example, the first and third of the abovementioned tools, then the result is a combined method that combines software and non-typical tools to achieve the goal [35].

7. According to violation of security characteristics ($S_7 = S_{VC} = VC$) MAISA are divided into three types: confidentiality violation methods (CV-methods – $C_{7,1} = C_{VC,CV} = CV$), integrity violation methods (IV-methods – $C_{7,2} = C_{VC,IV} = IV$) and accessibility violation methods (AV-methods – $C_{7,3} = C_{VC,AV} = AV$).

CV-methods are aimed at violating the confidentiality of information when social engineers gain access to confidential data without having the right to do so. For example, access to names, addresses, phone numbers, passwords, financial, and corporate data. The interception of private information through sociotechnical attacks can be performed using various methods and their combination; for example, the use of psychological and social methods unauthorized access to data. These attacks often rely on human manipulation rather than technical means. The most common methods are phishing, trust engineering, masking techniques, diversionary manoeuvers, Internet espionage, and identity theft. These attacks can be effective because they use the human factor, which is often a weak link in information security. To protect against such attacks, it is important to train staff to recognize suspicious situations, provide instructions on how to protect privacy, and establish appropriate security policies and procedures.

IV-methods are aimed at violation of information integrity by a social engineer. An example of an information integrity attack may include an attack on a website or application to modify or corrupt data stored on or transmitted through it. For example, a social engineer can modify the content of a website or application to introduce malicious code or false information. Let us imagine that a hacker attacks a bank's website and changes the information on the money transfer page. Instead of transferring the money to the recipient's account, as is usually done, the social engineer implements a script that redirects the money to his own account. Users who try to transfer through this site do not notice any suspicious changes, as the website interface may remain unchanged, but their funds end up in the hands of the offender. This example shows how an attack on information integrity can have serious consequences by distorting or disrupting data that users perceive as true.

IV-methods are aimed at violation of information integrity by a social engineer. An example of an information integrity attack is an attack on a website or application to modify or corrupt data stored on or transmitted through it. For example, a social engineer can modify the content of a website or application to introduce malicious code or false information. Let us imagine that a hacker attacks a bank's website and changes information on the money transfer page. Instead of transferring the money to the recipient's account, as is usually done, the social engineer implements a script that redirects the money to his/her own account. Users who attempt to transfer through this site do not notice any suspicious changes, as the website interface may remain unchanged; however, their funds end up in the hands of the offender. This example demonstrates how an attack on information integrity can have serious consequences by distorting or disrupting data that users perceive as true.

AV methods are aimed at violating accessible information, for example, the violation of this characteristic. These are so-called DDoS attacks where social engineers try overloading servers or the network in order to block user access to a certain resource or service. For ex-

ample, social engineers use a botnet network of previously infected computers with malicious software. They can direct these botnets to a website or online platform and launch an attack by sending several requests to the servers of that system. Because of such an attack, servers become overloaded, resulting in the temporary termination or restriction of user access to websites or services. This can have serious implications for a business or organization if it depends on an online platform to operate [16, 34]. In addition, it should not be excluded that during an attack, various security characteristics are violated and obtaining, for example, confidential information through interception can occur in various contexts, including communication networks, technical data transmission channels, and physical access to devices or systems. Then, in this case, a combination of these methods may take place, for example, MAISA CV-IV-AV activities, simultaneously violate the confidentiality, integrity, and availability of information.

8. According to the degree of severity ($S_8 = S_{DS} = DS$) MAISA are divided into simple attacks (SPL-attacks – $C_{8,1} = C_{DS,SPL} = SPL$), complex attacks (CPX-attacks – $C_{8,2} = C_{DS,CPX} = CPX$) and system attacks (SYST-attacks – $C_{8,3} = C_{DS,SYST} = SYST$).

SPL-attacks require only a few steps or readily available means to achieve their goal. For example, to obtain the name of an employee of a certain department at an enterprise, a social engineer can simply go to the company's website to obtain the contact number of the support service and request the necessary information.

CPX-attacks require a combination of multiple steps, algorithms, detailed planning, or the use of complex technical methods to achieve the goal. For example, a "fingerprinting" attack, where an attacker collects information about the target person, such as his/her daily activities and habits, in order to use this information in an insidious way. Or, a phishing attack, where the attacker sends an email that looks like a letter from a well-known company and invites you to access a personal account by clicking on a link and entering a password. If the goal of the attack is to obtain users' passwords, then a social engineer can first perform reconnaissance to determine the names of these users and then use the appropriate method to obtain their passwords.

SYST-attacks are based on complex algorithms with complex branched processes and cyclical feedback. These may include the use of various technologies and psychological methods. These attacks are used to obtain important information that is not accessible by trivial methods. For example, to gain access to security system servers, an unauthorized party can develop a complex algorithm that uses various methods and techniques [28, 34].

9. According to relational signs ($S_9 = S_{RS} = RS$) MAISA are divided into four types: mononomial attacks (MN-attacks – $C_{9,1} = C_{RS,MN} = MN$), polynomial attacks (PN-attacks – $C_{9,2} = C_{RS,PN} = PN$), monopoltic attacks (MPL-attacks – $C_{9,3} = C_{RS,MPL} = MPL$), and polypolitic attacks (PPL-attacks – $C_{9,4} = C_{RS,PPL} = PPL$).

MN attacks indicate that one attacker directs actions during an attack. An example of such an attack could be a situation where a social engineer pretending to be a representative of the company's technical support calls an employee asking for their password to "check the correctness of the account." In this case, the attacker directs his actions to a single target person.

PN-attacks occur when several attackers (two or more) affect one attack. An example of such an attack is a situation in which a group of social engineers sends e-mails on behalf of different colleagues or friends to the same target person. These emails may contain links to phishing web pages or malicious attachments intended to gain access to sensitive data or account information. Such attacks use the interaction of several attackers with one target person to achieve their goal, i.e., obtaining confidential information or even installing malicious software on the computer of the target person.

MPL-attacks occur when one attacker affects two or more attacked. For example, a social engineer contacts two or more different people who work in the same company or have access to certain information to obtain confidential information (which cannot be provided by one employee). He can use different approaches in communicating with each of them, perhaps even spreading different stories or promises to obtain the data he needs from each one.

PPL-attacks combine both polynomial and monopolistic methods when several attackers influence several attacks. An example of a relevant attack may involve the actions of a group of social engineers who interact with several different individuals or groups of people to obtain certain information. For example, this group may simultaneously send emails, make phone calls, and use social media to influence several different individuals or groups of individuals to commit fraud or obtain confidential information.

Such differentiation of methods allows a better understanding of how sociotechnical influence can be directed at individuals or groups of people depending on their relationships and properties [28, 36].

10. According to the type of the attacked source ($S_{10} = S_{AS} = AS$) MAISA are divided into four types: expert-directed attacks (ED-attacks – $C_{10,1} = C_{AS,ED} = ED$), attacks against a carefree person

ISSN 1814-4225 (print)
ISSN 2663-2012 (online)

(CFP-attacks – $C_{10,2} = C_{AS,CFP} = CFP$), contactee-directed attacks (CD-attacks – $C_{10,3} = C_{AS,CD} = CD$), attacks against an occasional person (OP-attacks – $C_{10,4} = C_{AS,OP} = OP$), the type of the attacked source being determined depending on the level of awareness of the person under attack [28].

ED attacks are targeted at experts with deep knowledge and contacts in a certain area. These attacks are aimed at obtaining valuable information that is usually considered reliable. The information provided by the expert is based on his/her professional knowledge and experience and includes various aspects related to the psychology of people, interpersonal interactions, and methods of influence. The obtained data can be useful for making decisions, solving problems, or developing strategies according to the user's needs or requests. This information may relate to methods of manipulating or persuading people, techniques of psychological influence, analysis of behavioural patterns and other aspects that help to understand and effectively use human behaviour to achieve certain goals. An example of such an attack could be a situation in which a social engineer conducting research in the field of cyber security turns to a well-known expert in this area. Communicating with him/her during a conference or through specialized forums, he/she learns about new attacks methods, weaknesses in security systems, or potential threats to companies. An expert who is trying to help a colleague may accidentally reveal confidential information or share valuable knowledge about the technical details of data protection. As a result, social engineers can use this information to create sophisticated and effective attack methods or to prepare more successful social engineering scenarios.

CFP-attacks are directed to a frivolous person who, in informal conversations, discloses certain facts in a business or friendly conversation. The relevant information may have value although it is possible that it is a simple lie or deliberate misinformation. An example of this attack can be a situation when a social engineer communicates with a colleague at a work event or during a coffee break. During the conversation, the person inadvertently extracts information about the processes or projects that the colleague is working on, under the guise of curiosity or simple conversation. This information can be valuable to social engineers who can use it to further attack or gain an advantage.

CD attacks are directed at people who have contact with the object of the social engineer's research, whether they are business partners, relatives, or acquaintances. They can help access valuable information. An example of a relevant attack is a situation where a social engineer contacts a colleague who had previously worked in the information security department in order to obtain confidential information. The social engineer can use the previous relationship with this colleague to establish a trusting contact and inventing an attractive reason for communication. During the conversation, he/she can test the colleague's reaction to certain questions or topics related to the confidential information and try to extract this information by presenting himself/herself as an interested or trustworthy person. This contact can facilitate the obtaining of important information for social engineers.

OP attacks target individuals who are not considered potential sources of information but may have important data. Social engineers do not count on them but try to obtain as much necessary information as possible. An example of such an attack can be a situation when a social engineer accidentally meets a company employee at a social event or in a cafe. Even if this employee is not considered a key source of information, he/she may have access to important data that may be of interest to the social engineer. By deftly using general topics of conversation or maintaining a friendly mood, social engineers can try to learn more about a person's work responsibilities, access to information, or even use subterfuges to obtain confidential information. This type of attack can be particularly effective because the individual does not suspect that he/she is the target of the attack and therefore does not take the necessary precautions.

If different types of attacked sources are used, a combined type of attack can be achieved. For example, an attack combining the aspects of an expert and a frivolous person can be referred to as an ED-CFP attack.

11. According to the type of access to information ($S_{11} = S_{ACC} = ACC$) MAISA are divided into attacks on open sources (OS-attacks – $C_{11,1} = C_{ACC,OS} = OS$), attacks on conditionally open sources (COS-attacks – $C_{11,2} = C_{ACC,COS} = COS$), attacks on confidential information sources (CIS-attacks – $C_{11,3} = C_{ACC,CIS} = CIS$) and attacks on secret information sources (SIS-attacks – $C_{11,4} = C_{ACC,SIS} = SIS$) [28].

OS-attacks are related to information that is available for public viewing and use. It can be published in open source such as newspapers, magazines, books, websites, and social networks. People are free to obtain, use, and distribute this information without restrictions or special permissions. In other words, data can be accessed by anyone who has access to the relevant source where it is located. For example, a social engineer can obtain information from news on the Internet, public documents, and public data.

COS-attacks are related to information that is also contained in open sources or may be available to the general public, but requires protection and restriction of access due to its significance for a person, society, or state,

i.e., information important for the organization, the violation of integrity or availability of which may lead to losses. For example, a social engineer obtains access to documents inside an organization that may be available to employees but requires authorization permission for access by outsiders.

CIS-attacks are related to information that is not classified; however, access to such information is controlled and limited by individuals or organizations responsible for its preservation and confidentiality. For example, a social engineer obtains access to employee personal data, such as salary information, medical information, or other private data that are subject to protection from unauthorized access, as well as internal company documents containing financial information, strategic plans, and sensitive data about products or services, which are for internal use only.

SIS-attacks are related to information that has a seal of secrecy, and only a certain circle of persons or organizations may have access to such information. This information may contain important government and commercial secrets, military plans, critical technology, other sensitive data, secret access codes, or the latest developments to which access is restricted for security reasons. For example, a social engineer gains access to classified cybersecurity data containing important information about potential threats, attacks, critical systems that require special protection, or classified government documents containing data on national security, intelligence, or important foreign policy decisions. In addition, this can include the company's trade secrets, such as manufacturing technologies, patents, research and development, strategic partnerships, and business expansion plans.

When attacks are aimed at accessing different types of information, it is possible to combine classes; for example, a COS-CIS-attack is aimed at conditionally open and confidential information.

12. According to remoteness ($S_{12} = S_R = R$), MAISA are divided into local attacks (L-attacks – $C_{12,1} = C_{R,L} = L$), which may be local attacks from a controlled area (LC-attacks – $SC_{12,1,1} = SC_{R,L,LC} = LC$), local attacks within a premise (LWP-attacks – $SC_{12,1,2} = SC_{R,L,LWP} = LWP$), local attacks from a workplace (LW-attacks – $SC_{12,1,3} = SC_{R,L,LW} = LW$), local attacks with access to the data area (LDA-attacks – $SC_{12,1,4} = SC_{R,L,LDA} = LDA$) and remote attacks (RM-attacks – $C_{12,2} = C_{R,RM} = RM$), which may be telephone-based attacks (TB-attacks – $SC_{12,2,1} = SC_{R,RM,TB} = TB$), attacks using network technologies (NT-attacks – $SC_{12,2,2} = SC_{R,RM,NT} = NT$), and remote attacks using registering or profiling tools (RPT-attacks – $SC_{12,2,3} = SC_{R,RM,RPT} = RPT$).

L-attacks are carried out through direct individual communication between a social engineer and a potential victim. The intrusion method uses physical access to premises, systems, or objects to obtain commercial information or perform certain actions. Such attacks can be particularly effective because they use not only technological but also social and psychological aspects to achieve their goals. For example, if the victim is an employee of the company (including system users, personnel maintaining technical facilities, managers at various levels of the job hierarchy, employees of the software development and maintenance department, technical personnel maintaining the premises), then the social engineer may present himself/herself as an employee, supplier, or employee of a partner company, a support service representative, etc., and ask for help. Local attacks can occur in different places and are divided into the following categories:

LC-attacks, which are carried out from a controlled area (CA) without requiring access to premises.

LWP-attacks, which are carried out within a premise (WP) without access to the technical facilities of the system.

LW-attacks, which are carried out from the workplaces (W) of the end users of the system.

LDA-attacks, which are carried out with access to the data area (DA) or control area of the protection system security tools.

Such attacks can be aimed at observing and analyzing the behaviour of the personnel, using public events to gain access to facilities or information, forging access cards, and impersonation. For example, social engineers can use techniques of masking or impersonation to gain access to protected premises or information. Violators may impersonate organization employees, contractors, or other trusted individuals to gain access to facilities. To gain access to premises via local methods, various lock means can be used, such as locks, skeleton keys, electronic master keys, motion detectors, alarms, and others. There is a wide range of such classic keys. In the case of using different types of local attack methods, a combined approach can be used, for example, the LC-LWP-type approach, where the attack is first carried out from a controlled area without access to the premises, and then penetration is carried out inside the premises without access to the technical means of the system on different stages of the attack [23, 24].

RM-attacks are implemented using various means of communication, such as telephone, fax, e-mail, and virtual computer networks. In most cases, they are carried out without the need for access to a controlled territory. These attacks can be classified as TB-attacks (performed by phone), NT-attacks (using different types of commu-

ISSN 1814-4225 (print)
ISSN 2663-2012 (online)

nication and network technologies), and RPT attacks (using registering or profiling tools).

TB-attacks are based on phone use, and they are the most common method of sociotechnical attacks.

They are based on the use of authority, status, or manipulation skills to influence other people by persuading them to act in certain ways or adopt certain views in order to gain access to information or perform actions that would not be available to the average user. Influence can occur in various ways, including persuasion, argumentation, simple frustration, and admiration. A number of psychological techniques are used to reinforce the influence of personality through authoritative sources. This method is especially effective in large corporations, where it is difficult to track of all employees and control new ones. Specialists in sociotechnical attacks pay special attention to the creation of a psychological environment favourable for performing an attack. Regardless of the method used, the main goal is to convince the disclosing person that the social engineer is a reliable entity to whom the relevant information can be entrusted [12].

Today, in the era of mobile and cellular phones, VoIP, and telephone servers, the possibilities of a social engineer to use the telephone have greatly expanded. Every day, businesses receive much calls for various reasons, which requires a significant amount of skill from the attacker to successfully attack the phone. Since everyone has a cell phone, people can have personal conversations in any public place, making the cell phone an important tool for social engineers. Ability to listen to or call on mobile devices opens additional levers for obtaining information that was previously unavailable. With the rise of smartphones and other mobile devices, more and more people are storing personal data on their phones, making them attractive targets for criminals. In addition, people who are always in touch are often ready to provide information quickly if approached with certain criteria, making their requests more believable. For example, if the phone number indicates that the call is from a corporate headquarters or a well-known online bank, many people will provide the information without verification. The quality of caller ID spoofing phone apps has become impressive, giving social engineers access to tools that simulate calls from anywhere on Earth for relatively little cost. For example, with apps like SpoofApp – https://www.spoofcard.com, a social engineer can fake calls that look like they are coming from any location and pretend to be a remote office worker, new employee, supplier, or software manufacturer by offering to update it.

NT-attacks are used to manipulate people and obtain information remotely through remote means of communication, various network technologies, communication channels such as e-mails, various types of viruses and other malicious software, messages in social networks. This method can be particularly effective in settings where remote access to the target organization is possible and physical contact is limited or impossible. Such social engineering can include phishing e-mails, spam phone calls, spam in social networks, Internet fraud [23, 24]. For example, a request or call to perform a certain action on behalf of management or colleagues can be sent through e-mail. For example, a social engineer can send a request to the finance department to provide a report for the month to management, while using a phishing e-mail address. Another example of NT-remote MAISA may be sending along with the letter or application software viruses or malicious software, or providing the address of an Internet resource for them. For example, an attacker can send an email attachment or attachment to a downloader with malicious software. Also, a social engineer can send a letter to the attacked person with a message that a new useful utility has been found, and provide a link to the address where he/she places the malicious program or virus. The offender can use known sources with a very similar but different from the real address of the Internet resource to trick the victim into providing personal data. By creating a sufficiently similar graphical interface, a social engineer can create a situation where the victim unknowingly registers by specifying his ID, password or email address, or tries to log in as an already registered user. In addition, a social engineer can carry out an NT-attack using a fake pop-up window, where addresses of Internet resources, forms for additional registration, windows for downloading malicious software that look like useful applications, and other insidious elements can be placed.

RPT-attacks are based on the application of registering or profiling tools, which results in the creation of a profile of the target of the attack and the execution of a certain part or achievement of the final goal. The modern market offers a variety of registering devices, such as cameras in various forms, hidden in items or objects, such as pens, pieces of clothing, or watches. Social engineers often use GPS trackers to track the whereabouts of targets outside the office. In addition to profiling tools that help collect profiles and passwords, social engineers develop profile questionnaires to target an attack and begin creating a list of possible passwords to attempt access. Password selection using a profiling tool can take time. Every year, many people fall victim to simple attacks despite numerous warnings and security measures. Many individuals publish personal information about themselves, their family, and their personal lives online on social media pages. By combining these data with the

information available on social networks through profiling tools, social engineers can recreate a person's complete life. Many people use the same or easily guessed passwords; thus, this method is very effective. For example, the following software Common User Password Profiler (CUPP), CeWL, can be used for this purpose. Information gathering tools play a key role in social engineering and successful attacks. Without proper attention to information gathering, an attack may fail. Today, there are many tools available that help in collecting, processing, and using collected data. These tools can significantly affect the way an infringer uses information available on the Internet, such as Maltego, SET: Social Engineer Toolkit, Whois, and search engines.

If attacks are carried out using different types of remote methods, the result can be a combined method, for example, the TB-RPT-remote type that uses phone calls and registering tools. In the case of attacks using different types of remote methods (both local and remote), the result can be a combined method, for example, LC-local-NT-remote. This method is used in attacks from a controlled area without access to premises and employs network technologies.

13. According to manipulation ($S_{13} = S_M = M$), MAISA are divided into six categories that include features of human nature, such as: authority (authority-based manipulation (AB-manipulation – $C_{13,1} = C_{M,AB} = AB$), favour (favour-based manipulation (FB-manipulation – $C_{13,2} = C_{M,FB} = FB$)), mutuality (mutuality-based manipulation (MB-manipulation – $C_{13,3} = C_{M,MB} = MB$)), responsibility (responsibility-based manipulation (RB-manipulation – $C_{13,4} = C_{M,RB} = RB$)), sociality (sociality-based manipulation (SB-manipulation – $C_{13,5} = C_{M,SB} = SB$)) and limitation (limitation-based manipulation (LB-manipulation – $C_{13,6} = C_{M,LB} = LB$)). Information manipulation is the process of influencing the beliefs, perspectives, or behaviour of other people by simplifying, inventing, or distorting facts or events. This method can be used to achieve specific goals, such as changing attitudes, beliefs, or decision-making.

AB-manipulation is based on authority, when people's tendency to follow the directions or recommendations of a person with power or authority. For example, a social engineer may attempt to obtain information by acting as a management or other influential person, which automatically instils a certain level of trust in the potential victim.

FB-manipulation is based on favour, it is aimed at creating a sense of commonality or similarity of interests between the social engineer and the target person. The social engineer may attempt to obtain information by impersonating someone with similar interests or concerns to the target, thereby inducing them to be more likely to cooperate or provide information.

MB-manipulation is based on the perception of reciprocity between people, where one party feels obligated to respond to requests or gifts given by another party; that is, it is based on a person's tendency to reciprocate a favour received, especially when it is not expected. For example, a social engineer can introduce himself/herself as an employee of the IT department and inform that some of the company's computers are infected with a new, dangerous virus, offering to solve this problem. After that, the attacker can ask the attacked person to test the new utility to change passwords.

RB-manipulation consists in giving a person responsibility for the performance of certain actions or events, which can stimulate him/her to a certain behaviour, and is also based on the habit of fulfilling promises to maintain trust and not seem to be a person who does not keep his/her word. For example, a social engineer may advise a new employee to read the company's security policy, emphasizing the need to adhere to the agreement. After several discussions, the manager can ask for the employee's password or other personal data to verify the agreement and then provide recommendations for creating a password in the future.

SB-manipulation relies on social norms and expectations that influence a person's behaviour and uses the attacked person's belonging to a certain social group as a guarantee of truth in the matter of behaviour. The attacker can present himself/herself as a security inspector by naming other people from the attacked department who have already passed the inspection procedure. This allows the attacker to ask various questions, including the user's ID and password used by the victim.

LB-manipulation is based on the belief that the attacked object will share information that others claim or that this information is available only at a particular moment. For example, the attacker could send emails promising a free e-album for any artist to anyone who signs up for a new entertainment site by the end of the week. During registration, the employee may unknowingly provide his/her ID, password, email, etc. By exploiting the fact that many people use the same passwords and IDs, an attacker can gain access to various resources of the attacker.

When a sociotechnical attack includes combined features of the description of human nature, the result will be an aggregation of different methods, for example, the use of authority and favour (AB-FB-manipulation) [10, 28].

ISSN 1814-4225 (print)
ISSN 2663-2012 (online)

14. According to the type of social engineer ($S_{14} = S_{SE} = SE$), MAISA are divided into methods performed by hackers (H-performed – $C_{14,1} = C_{SE,H} = H$), penetration testers (PT-performed – $C_{14,2} = C_{SE,PT} = PT$), spies (SP-performed – $C_{14,3} = C_{SE,SP} = SP$), identity thefts (ITT-performed – $C_{14,4} = C_{SE,ITT} = ITT$), dissatisfied employees (DE-performed – $C_{14,5} = C_{SE,DE} = DE$), frauds (F-performed – $C_{14,6} = C_{SE,F} = F$), recruiters (RT-performed – $C_{14,7} = C_{SE,RT} = RT$), sellers (SL-performed – $C_{14,8} = C_{SE,SL} = SL$), methods using remote combinations (RC-performed – $C_{14,9} = C_{SE,RC} = RC$) and methods aimed at a particular sector (PS-performed – $C_{14,10} = C_{SE,PS} = PS$), which are ranked according to the specifics of the activity and are aimed at government officials (GO-performed – $SC_{14,10,1} = SC_{SE,PS,GO} = GO$), medical professionals (MP-performed – $SC_{14,10,2} = SC_{SE,PS,MP} = MP$), psychologists (PSY-performed – $SC_{14,10,3} = SC_{SE,PS,PSY} = PSY$), lawyers (LWR-performed – $SC_{14,10,4} = SC_{SE,PS,LWR} = LWR$) [28, 31].

H-performed methods are implemented by highly experienced, highly qualified IT specialists-hackers who have deep knowledge in the field of information technologies. With the development of software, vendors are increasingly improving measures to protect against infringers. These specialists make extensive use of both hardware and software solutions, as well as the capabilities of social engineering to increase the effectiveness of attacks. An example of such an activity is when an experienced hacker uses hardware and software tools to breach the security of a company's web server. He/she can use various methods, such as password capture, software vulnerabilities, and password hashing attacks, can be used to gain access to the server. It can then delete or modify important data, cause damage, or even demand a ransom for its recovery.

PT-performed methods are implemented by expert penetration testers who use and learn techniques similar to those used by attackers with the aim of ensuring client security. This category of specialists never uses the information obtained for personal purposes or to cause harm; in most cases, they are internal testers or external consultants. An example of such a method is penetration testing of an enterprise's network infrastructure. A penetration tester can attempt to gain access to a system by exploiting vulnerabilities in network protocols and applications. For example, a hacker can use cracked passwords or intercept network traffic to gain access to confidential company information. After that, the researcher analyses the test results and recommends measures to eliminate the identified vulnerabilities and increase the level of network security.

SP-performed methods are based on the ability to apply social engineering as a key aspect of spies' lives. They skilfully use each sociotechnical component and are experts in the relevant field. Spies of all levels and qualifications learn various deception methods by pretending to be someone they are not. In addition to mastering the art of social engineering, they also exploit the victim's trust, especially if they have some knowledge or even significant information about the business or government they are trying to attack. For example, a spy posing as a technical support engineer can email a company employee offering help in solving a computer problem. The email may contain a link to malware that attacks the user's computer under the guise of fixing the problem. The victim, confident in the authority and help of the "engineer", can open the link, which will lead to the infection of his computer with malicious code.

ITT-performed methods involve identity theft and use of identification information, often by offenders who use techniques to steal data such as names, bank account numbers, addresses, dates of birth, or social security numbers without the owner's permission. These crimes include impersonation or the use of false uniforms to impersonate others, or more sophisticated types of fraud. Identity thieves use various social engineering methods, and over time, they become more confident and indifferent to the consequences of their actions. For example, identity thieves may send an email or call pretending to be a bank or other organization and ask the potential victim to confirm their personal details, such as card numbers and other sensitive information, under the pretence of needing to verify an account or prevent potential theft.

DE-performed methods are implemented by disgruntled employees, and this applies to situations where employees who feel dissatisfied or offended by their employer can take actions against him. This situation is often one-sided because employees usually try to hide their level of dissatisfaction in order to keep their jobs. However, growing dissatisfaction can lead to theft, vandalism, the distribution of confidential information, or other crimes. For example, a disgruntled employee who was promised a raise but his expectations were not met may decide to compensate by stealing office equipment or performing other malicious acts against the company.

F-performed methods are used by fraudsters who exploit greed and other human principles to mislead, change people's beliefs, and induce them to make money or receive other privileges. Scammers have learned the art of understanding people. They know how to detect their weak points and use tricks to induce them to take certain actions that seem profitable. They also create

situations that seem like unbeatable opportunities for personal gain. An example of this technique is when fraudsters send an email from a fictitious company that resembles a well-known existing technology organization. This email may contain instructions that the sender is performing a security audit or system maintenance free of charge, and requests access to certain systems or confidential information for "audit." A potential victim, by trusting the appearance of the email and the data presented in it, can give fraudsters access to their information or computer system, which can lead to security breaches and data loss.

RT-performed methods are implemented by recruiters who have extensive experience in understanding people and their motivations, thanks to the study of the psychological principles of social engineering. They use this knowledge for effective recruitment and have extensive experience in this area. For example, an executive recruiter can use various methods and techniques to persuade a potential candidate to accept a job offer, using apt psychological strategies and persuasive arguments that match their motivations and goals.

SL-performed methods are often used by salespeople who must possess various interpersonal skills. Many experts in the field of sales emphasize that a successful salesperson is not based on manipulating people, but skilfully uses his/her skills to identify the needs of customers and evaluate the possibilities of their satisfaction. The art of selling requires understanding aspects such as gathering information, identifying needs, influencing customers, and using psychological principles and other skills. For example, a salesperson in a hardware store can use appropriate sociotechnical methods to persuade customers to purchase additional products or services. It emphasizes how an optional accessory or extended warranty service can increase the performance or lifespan of the purchased product. The seller may also use psychological techniques, such as creating the impression that the buyer will receive more value or convenience if he or she buys additional products in addition to the main product. Thus, the seller uses social engineering to encourage the buyer to purchase additional goods or services.

RC-performed methods represent a separate category of techniques and methods used to determine certain signs and characteristics of attacks. These can be executable scripts or programs that allow offenders to gain access to the system by running them through servers, remotely over the Internet, or other methods. For example, an executable script can be created to automatically identify vulnerabilities in a network application. It can scan network nodes for open ports and perform vulnerability analysis to identify possible intrusion paths. Another example is to create a script to automatically back up data from the server to an external drive. This script can be programmed to regularly make copies of important files and store them in a safe place with minimal user intervention.

PS-performed methods are directed to a specific sector and the specific activity of a person. They can be divided by sectoral affiliation and targeted at government officials (GO-performed), medical professionals (MP-performed), psychologists (PSY-performed), and lawyers (LWR-performed). For example, government officials, doctors, psychologists, or lawyers may apply their own methods according to their professional needs and tasks.

GO-performed methods are based on the actions of government officials and include various strategies designed to achieve certain goals in the sector. For example, government officials can use social engineering to shape messages and control communications with the public and subordinates. This type of attack is not always negative, as some messages from the government are intended for the greater good, and the use of social engineering elements can make these messages more attractive and effective. Psychological and communication strategies can increase the level of understanding and support among citizens, which will contribute to the successful implementation of various programs or initiatives.

MP-performed methods are based on the actions of doctors; for example, they can use social engineering to increase the level of trust and cooperation of patients in performing medical procedures or accepting treatment recommendations. They can use empathy, the ability to communicate effectively, and create a positive environment for patients to ensure successful treatment outcomes and improve their overall health.

PSY-performed methods are based on the actions of psychologists; for example, they may include the use of psychological techniques to influence people's behaviour in certain situations. This may include developing consumer motivation programs, psychological testing in advertising campaigns, or using persuasive techniques to influence customer decisions.

LWR-performed methods are based on the actions of lawyers who can use psychological and legal knowledge to influence the behaviour of parties in legal proceedings or to conclude agreements. They can apply techniques such as negotiation, mediation, argumentation, and the use of legal knowledge to achieve their goals or protect clients.

15. According to scale ($S_{15} = S_S = S$), MAISA are divided into local (LL-attacks – $C_{15,1} = C_{S,LL} = LL$) and world-wide (WW-attacks – $C_{15,2} = C_{S,WW} = WW$) attacks.

LL-attacks are aimed at a particular region, group of persons, or may occur within a specific network or

ISSN 1814-4225 (print)
ISSN 2663-2012 (online)

organization. They can be implemented using several sociotechnical methods. They are particularly dangerous because they can be carried out inside an institution where protection against external threats is weaker. For example, attackers can target employees with high privileges to access restricted information in order to gain access to systems or data. In addition, manipulative techniques enable access to areas or information to which no unauthorized party would normally have access. To protect against local cyberattacks, security measures, such as regular staff training, monitoring network activity, using access control systems, limiting access privileges to information and systems, and implementing security policies and incident response procedures, are important. In addition, an organization can regularly audit its systems and network to identify vulnerabilities and ensure that they are addressed in a timely manner.

WW-attacks. This type of cyber-attacks has an international or large-scale nature and is aimed at a large number of individuals and organizations with a potentially wide range of influence through the use of the Internet and other global technologies. Attacks can be performed using various methods and means, including technical, social, and organizational aspects. For example, offenders use mass communication channels to spread fake news and manipulate public opinion and influence political processes and elections in different countries by using social networks, disinformation, and other methods to manipulate voters. In addition, hackers may attempt to break into the systems and networks of large corporations or government agencies in order to obtain restricted information or cause other harm. Such global sociotechnical attacks can have a serious impact on society, economy and political processes. To protect against such attacks, it is important to develop and implement comprehensive cyber security strategies covering technical, organizational and legal measures. It is also important to constantly improve your means of detecting and responding to threats [34].

3. Results and Discussion

Based on the MAISA analysis and the set of criteria, the implementation of a sociotechnical cyber attack, such as phishing, was investigated.

There is a general description of the process of implementing a sociotechnical attack, which may have its own unique features depending on the goals, methods and tools of the social engineer, and includes the following stages:

Stage 1. Target research. The social engineer begins by researching his or her target – a company, an individual, or an organization. It collects information about the target person or organization, such as contact details and the organization's social media profile.

Stage 2. Attack preparation. The social engineer develops a strategy to influence the target person. This may include creating fake emails, social media accounts, or websites.

Stage 3. Attack execution. The social engineer executes the planned attack, which includes sending phishing emails demanding sensitive information, intercepting data, or using social engineering techniques to gain access to the system.

Stage 4. Using the obtained information. After a successful attack, the social engineer can use the obtained information for various purposes, such as stealing sensitive data, using the target systems to carry out further attacks, or even demanding a ransom to regain access to the compromised systems.

Stage 5. Hiding the tracks. In the final stage, the social engineer usually covers his tracks to avoid detection and responsibility for the attack.

Based on the above general presentation, a sociotechnical attack has been described, the purpose of which is to obtain personal data and access his/her accounts with the help of duplicate sites (phishing attack). The object of the attack is the seller of the product.

For example, today it is possible to buy or sell online, thanks to online platforms where free and commercial trade ads are posted. One of the most popular resources for this is the classifieds service OLX (https://www.olx.ua).

Stage 1. The social engineer begins the attack by analysing his/her target (the OLX Internet platform), collects various information about the structure of the site, the principle of its operation, the mechanism of the implementation of the agreement, methods of payment and delivery of goods.

In the first stage, the following MAISA classes are implemented:

– PP-attacks (detailed planning and preliminary preparation of fraudulent actions is carried out, the OLX service is analyzed according to such indicators as: operating principle, agreement implementation mechanism, methods of payment, delivery of goods, etc.);

– SPL-attacks (simple actions and tools are used to collect and analyze the necessary information); and

– MN-attacks (the attacker studies and collects information to perform illegal actions on a certain victim);

– OS-attacks (information about the service published in open sources and is available for general review and use);

– SP-performed methods (using social engineering principles for collecting information and its further aggregation);

– LL-attacks (collection of information and subsequent actions aimed at a local group of people).

Stage 2. Next, the social engineer creates a website (duplicate site) that looks as similar as possible to the

OLX site, for which purpose he/she uses a similar design, logo, and other elements to make it as authentic as possible. In addition, the unauthorized party creates a fake account for themselves on the real site (usually the corresponding accounts are "fresh" and have a recently created date), and advertisements are used to enhance the "presence effect" to mislead the victim.

Stage 2 is based on such MAISA classes:

– PP-attacks (a detailed attack plan is created, including the definition of attack methods and development of sociotechnical scenarios);

– MN-attacks (the social engineer develops special solutions aimed at a certain person to obtain confidential information); and

– COS-attacks (information about the operation of the service, for example, a link to pay for the product);

– LL-attacks (solutions aimed at a certain person are developed).

Stage 3. The social engineer chooses the victim who has already placed an ad with the product for sale.

It starts with a friendly and light conversation. First, the fraudster sends private messages to the personal account in which he/she is allegedly interested in the product. He/she uses various methods of influence and unobtrusive pressure. He/she is ready to buy the product very quickly.

Sometimes, for "convenience" and speed of communication, the fraudster suggests switching to a messenger app, for example, WhatsApp or Viber.

After that, he/she asks about the possibility of placing an order thanks to "OLX Delivery" or "New Mail", promising to bear the costs.

Next, the product is "paid", where a link to the site is sent along with a notification of its confirmation. The "buyer" (social engineer) asks to confirm the receipt of funds by clicking on a special link, which is a fake site and looks almost like the real OLX service (which was developed in advance). Also, to strengthen the effect of the "authenticity of the deal" to the seller of the goods, an employee of the OLX service can call the mobile phone from a fake phone to confirm the deal and make sure that the sale operation will now be carried out and the money will be credited to his/her bank card.

The main difference is the link address. The seller of the product follows it, after which an alleged order placement appears with a form (a fake "secure agreement" questionnaire) in which he/she has to fill in personal data on a bank plastic card (16 card digits, the CVV code and/or the card expiration date) to transfer the money to. The "victim" fills out the form and enters private information.

Stage 3 comprises the following MAISA classes:

– PP-attacks (a potential victim is defined, and the optimal attack time is selected). Advanced social and psychological techniques are used to manipulate the victims to gain access to information);

– PTP-methods (the social engineer who is not reliably identified can take actions for his/her own benefit and at the same time bear no responsibility);

– DP-methods (insufficient administrative support, incorrect performance of protection functions and untimely reaction to unusual situations, for example, the site does not fully filter personal links);

– CP-attacks (a (phishing) link to a potential target is transferred, which becomes a condition for starting the attack);

– OVS-methods (the social engineer attempts to gain access to the information (bank card) by contacting the target directly according to the planned scenario);

– SW-methods (a phishing link is sent to manipulate the target persons); and

– CV-methods (using combined techniques of manipulation, the victim enters his/her personal data, as a result of which the social engineer gains access to confidential information without having the right to do so);

– CPX-attacks (the social engineer sends an electronic link that looks like a real one and offers to fill out a form by clicking on it and entering personal information); and

– MN-attacks (the attacker directs his/her actions at the defined person attacked);

– CFP-attacks (directed at a frivolous or uninformed person who may reveal confidential information in a personal conversation);

– OP-attacks (targeted at random persons, but the social engineer tries to get as much necessary information as possible);

– CIS-attacks (a request is sent to receive information, access to which is limited to private individuals);

– NT-attacks (used to manipulate people and obtain information remotely by sending a phishing e-mail);

– RB-manipulation (after the social engineer has convinced the victim that he/she is purchasing the product, the former offers, by sending a phishing link (giving the person responsibility for performing certain actions), to fill in personal information for crediting the corresponding funds); and

– SP-performed methods (having specific knowledge and information, and using a whole set of deception methods, the social worker enters into trust and offers to perform certain actions);

– ITT-performed methods (using the principles of imitation, the social engineer can make a call on behalf of a legitimate service to confirm the purchase of a product, which is associated with further theft of personal data);

– LL-attacks (actions aimed at a specific target).

Stage 4. After the corresponding data are entered, the funds on this bank card will be immediately stolen. If it is a credit plastic bank card, then the amount of the

ISSN 1814-4225 (print)
ISSN 2663-2012 (online)

fraudster's benefit will increase by the entire credit limit of the seller's card.

Stage 4 is based on the following MAISA classes:

– PP-attacks (pre-planned social and psychological techniques are applied to manipulate the victim and gain control over the data); and

– SW-method (using a phishing link, the social engineer receives the necessary information); and

– CV-methods (private information is intercepted and access to a bank card is obtained);

– CPX-attacks (in the received link, the victim enters his confidential data, which are sent to an unauthorized party for illegal actions);

– MN-attacks (the actions of the social engineer are aimed at a predetermined goal);

– ACIS-attacks (receiving and using information that is controlled by the owner of the relevant information and data);

– NT-attacks (implemented using network technology through personal messages by receiving a corresponding request and a call to perform certain actions on behalf of the site);

– ITT-performed methods (methods of stealing personal data and identification information are used);

– LL-attacks (a certain person's information and data are improperly used).

Stage 5. At the final stage, the goal has been achieved (the attack has been carried out) and the money is already in the account of the social engineer. The social engineer tries to hide his/her presence (traces) that he/she used for the attack in order to avoid detection of his/her role in this attack. The social engineer "throws" the buyer's phone into the black list, changes the SIM card, turns off the phone, blocks the seller's account, or deletes his/her own.

In stage 5, such MAISA is realized as follows:

– PP-attacks (a PP-attack is completed by causing serious damage (losses) and hiding (according to the pre-prepared scenario) the traces of the social engineer);

– AV-methods (the social engineer performs necessary actions to hide his/her presence on the site and removes all information about himself/herself);

– LL-attacks (personal information is deleted within the defined service).

According to the given example, the implementation of a sociotechnical attack was implemented based on the following MAISA classes: PP-attacks – $C_{1,2}$, PTP-methods – $C_{3,1}$, DP-methods – $C_{3,2}$, CP-attacks – $SC_{4,1,2}$, OVS-methods – $C_{5,1}$, SW-methods – $C_{6,1}$, CV-methods – $C_{7,1}$, AV-methods – $C_{7,3}$, SPL-attacks – $C_{8,1}$, CPX-attacks – $C_{8,2}$, MN-attacks – $C_{9,1}$, CFP-attacks – $C_{10,2}$, OP-attacks – $C_{10,4}$, OS-attacks – $C_{11,1}$, COS-attacks – $C_{11,2}$, CIS-attacks – $C_{11,3}$, NT-attacks – $SC_{12,2,2}$, RB-manipulation – $C_{13,4}$, SP-performed – $C_{14,3}$, ITT-performed – $C_{14,4}$ and LL-attacks – $C_{15,1}$.

In addition, based on the set-theory model of MAISA and considering the characteristics shown in Fig. 1 and Fig.2, the above-mentioned sociotechnical attack can be graphically interpreted, as shown in Fig. 3.

This is only one example of how a phishing attack can occur on the OLX site. Such attacks may vary the methods and techniques used by attackers.

It is worth noting that the proposed method provides a generalized approach to building a classification model of modern approaches to the implementation of sociotechnical attacks. The proposed model expands the capabilities of the constructed model by introducing additional criteria and sub-criteria. The introduction of additional criteria is performed in the event of the emergence of new criterion (sign) characteristics that may appear in the event of the emergence of new threats and vulnerabilities in information systems.

For example, when a new criterion characterizing sociotechnical attacks is discovered, the general appearance of the model is preserved but leads to an increase in the number of identifiers when constructing a specific classification.

According to the proposed classification (Fig. 1), for example, the detection of a single new criterion leads to an expansion of the number of identifiers (an increase of 1, i.e. $n=16$, $i=\overline{1,16}$).

Further, an additional set of criteria and sub-criteria can be formed for the classification of the new 16th feature. Here, if the number of criteria is equal 3 and the sub-criteria is equal 0, then $m_{16}=3$, $j=\overline{1,m_{16}}$, and $r_{16,1}=r_{16,2}=r_{16,3}=0$, $\left(k=\overline{1,r_j}\right)$.

4. Conclusions

1. Based on the multi-theoretical approach, a method is proposed, in which, due to the stages of determining the set: identifiers of signs, criteria, and sub-criteria, it is possible to build a generalized hierarchical model for classifying socio-technical attacks according to the characteristic principle.

2. Based on the proposed model and the analyzed literature, a generalized set of features, criteria and sub-criteria has been formed, such as: time aspect, industry affiliation, interaction with security policy, remoteness, initialization, tools, manipulation, violation of characteristics, relational signs, severity level, type of attacked source, type of access, type of appeal, type of sociotechnical technique and scale, which allows us to select and develop appropriate means of countering sociotechnical attacks from a systemic perspective.

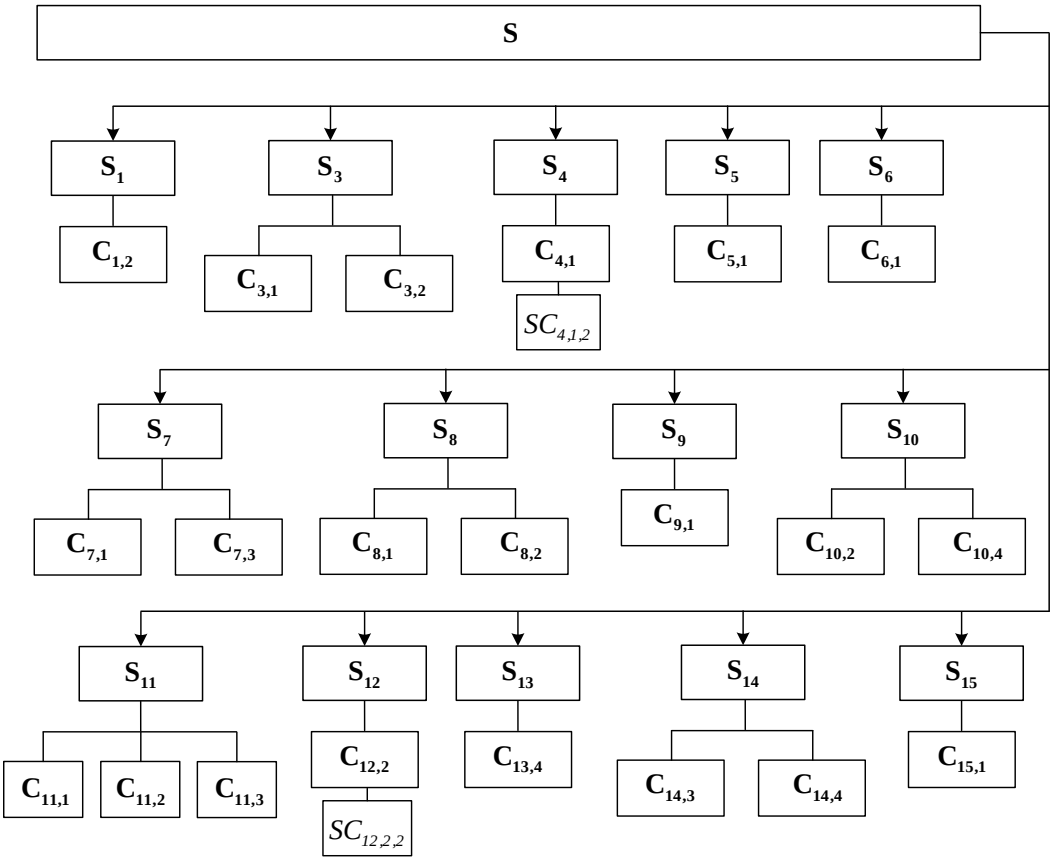

Fig. 3. An example of interpretation of implementation of a sociotechnical attack of the phishing type

3. The example of conducting a sociotechnical attack is considered, in which, taking into account the MAISA classification model and such steps of their implementation as: target research, preparation of a sociotechnical attack, performing of the attack, exploitation of the information received, hiding traces, made it possible to approach the understanding of the actions of a sociotechnician when implementing a phishing attack from a systemic perspective for the further development of appropriate countermeasures.

In addition, based on the obtained criteria, it is possible to develop a method for assessing personnel readiness to counter different classes of sociotechnical attacks. The method for building a model for classifying of sociotechnical attacks has been developed. Using this method at the expense of the stages of defining identifier sets: signs, criteria, and sub-criteria for the classifying of approaches to the implementation of sociotechnical attacks, a generalized model of the theoretical-multiple interpretation of the MAISA classification has been developed.

Based on the proposed model and the analyzed literature, the generalized set of signs, criteria and sub-criteria has been formed, such as: time aspect, sectoral affiliation, interaction with security policy, remoteness, initialization, toolkit, manipulation, violation of characteristics, relational signs, degree of severity, type of the attacked source, type of access, type of addressing, type of social engineer and scale, which allows selection and development of appropriate countermeasures against sociotechnical attacks from systemic positions.

The example of a sociotechnical attack has been considered, in which, taking into account the MAISA classification model and such stages of their implementation as: target research, preparation of a sociotechnical attack, execution of the attack, exploitation of the received information, concealment of traces, made it possible to approach the understanding of the social engineer's actions during the implementation of phishing from a systemic point of view, attacks for further development of appropriate countermeasures.

In addition, based on the obtained criteria, it is possible to develop a method for assessing personnel readiness to counter various classes of sociotechnical attacks.

Contributions of authors: conceptualization – **Oleksandr Korchenko**, **Anna Korchenko;** ideas, hypotheses, and problems statements – **Anna Korchenko**, **Serhii Zybin;** formulation of tasks, analysis – **Oleksandr Korchenko**, **Anna Korchenko;** analysis of results, visualization – **Serhii Zybin**, **Kyrylo Davydenko**; writing original draft – **Anna Korchenko, Kyrylo Davydenko;** review and editing – **Serhii Zybin.**

ISSN 1814-4225 (print)
ISSN 2663-2012 (online)

Conflict of Interest

The authors declare that they have no conflict of interest concerning this research, whether financial, personal, authorship or otherwise, that could affect the research and its results presented in this paper.

Financing

This study was conducted without financial support.

Data Availability

The manuscript contains no associated data.

Use of Artificial Intelligence

The authors confirm that they did not use artificial intelligence methods while creating the presented work.

Acknowledgments

This paper was prepared using the results of research conducted by the Scientific School of Cybersecurity at the National Aviation University, the Department of Information Technology Security (Kyiv, Ukraine).

All the authors have read and agreed to the published version of this manuscript.

References

1. Babak, A., & Ben, B. *Combatting Cybercrime and Cyberterrorism. Challenges, Trends and Priorities*. Springer International Publishing, 2016. 321 p.

2. Breda, F., Barbosa, H., & Morais, T. Social engineering and cyber security. *International Technology, Education and Development Conference*, 2017, pp. 4204–4211. DOI: 10.21125/inted.2017.1008.

3. Wang, Z., Sun, L., & Zhu, H. Defining Social Engineering in Cybersecurity. *IEEE Access*, 2020, vol. 8, pp. 85094-85115. DOI: 10.1109/ACCESS.2020.2992807.

4. Mahmood, S., Chadhar, M., & Firmin, S. Addressing Cybersecurity Challenges in Times of Crisis: Extending the Sociotechnical Systems Perspective. *Appl. Sci.*, 2024, vol. 14, iss. 24, article no. 11610. DOI: 10.3390/app142411610.

5. Nakhal Akel, A. J., Di Gravio, G., Fedele, L., & Patriarca, R. Learning from Incidents in Socio-Technical Systems: A Systems-Theoretic Analysis in the Railway Sector. *Infrastructures*, 2022, vol. 7, iss. 7, article no. 90. DOI: 10.3390/infrastructures7070090.

6. Mokhor, V. V., Tsurkan, O. V., Herasymov, R. P., & Tsurkan, V. V. Information Security Assessment of Computer Systems by Socio-engineering Approach. *Selected Papers of the XVII International Scientific and Practical Conference Information Technologies and Security*, Kyiv, 2017, pp. 92-98.

7. Wolert, R., & Rawski, M. Email Phishing Detection with BLSTM and Word Embeddings. *Intl journal of electronics and telecommunications*, 2023, vol. 69, no. 3, pp. 485–491. DOI: 10.24425/ijet.2023.146496.

8. Mouton, F., Leenen, L., & Venter, H. Social engineering attack examples, templates and scenarios. *Computers & Security*, 2016, vol. 59, pp. 186-209. DOI: 10.1016/j.cose.2016.03.004.

9. Krombholz, K., Hobel, H., Huber, M., & Weippl, E. Advanced social engineering attacks. *Journal of information security and applications*, 2015, vol. 22, pp. 113–122. DOI: 10.1016/j.jisa.2014.09.005.

10. Talishinsky, E. Manipulation as a form of information-psychological war. *Universidad y Sociedad*, 2023, vol. 15, no. 5, pp. 143-150.

11. Wang, Z., Zhu, H., & Sun, L. Social Engineering in Cybersecurity: Effect Mechanisms, Human Vulnerabilities and Attack Methods. *IEEE Access*, 2021, vol. 9, pp. 11895-11910. DOI: 10.1109/ACCESS.2021.3051633.

12. Konstankevych, I., Kostusiak, N., & Shulska, N. Media Manipulation as a Tool of Information Warfare: Typology Signs, Language Markers, Fact Checking Methods. *AD ALTA*, 2022, vol. 2, Spec. iss. XXIX (12), pp. 224-230.

13. Ebers, M. *Privacy, Data Protection and Data-driven Technologies*. Routledge, 2024. 430 p. DOI: 10.4324/9781003502791.

14. Alotaibi, B. Cybersecurity Attacks and Detection Methods in Web 3.0 Technology: A Review. *Sensors*, 2025, vol. 25, iss. 2, article no. 342. DOI: 10.3390/s25020342.

15. Al-Thani, N. A. Adolescents' and social engineering: The role of psychometrics factors in determining vulnerability and designing interventions. *2022 9th International Conference on Behavioural and Social Computing (BESC)*, Matsuyama, Japan, 2022, pp. 1-5. DOI: 10.1109/BESC57393.2022.9995705.

16 Conheady, S. *Social Engineering in IT Security: Tools, Tactics, and Techniques*. New York, McGraw-Hill Education, 2014. 254 p.

17. Momoh, I., Adelaja, G., & Ejiwumi, G. *Analysis of the Human Factor in Cybersecurity: Identifying and Preventing Social Engineering Attacks in Financial Institution*. IEEE, 2023. DOI: 10.13140/RG.2.2.35640.52489.

18. Ghafir, I., Prenosil, V., Alhejailan, A., & Hammoudeh, M. Social engineering attack strategies and defence approaches. *2016 IEEE 4th International Conference on Future Internet of Things and Cloud (FiCloud)*, Vienna, Austria, 2016, pp. 145-149. DOI: 10.1109/FiCloud.2016.28.

19. *ISO/IEC 27032:2023 Cybersecurity - Guidelines for Internet security*. Available at:

https://www.iso.org/standard/76070.html (accessed 22 April 2025)

20. Breda, F., Barbosa, H., & Morais, T. *Social engineering and cyber security*, 2017, pp. 4204–4211. DOI: 10.21125/inted.2017.1008.

21. Malatji, M., Marnewick, A., & von Solms, S. Validation of a socio-technical management process for optimising cybersecurity practices. *Computers & Security*. 2020, vol. 95, article no. 101846. DOI: 10.1016/j.cose.2020.101846.

22. Hadnagy, C. *Social Engineering: The Science of Human Hacking*. John Wiley & Sons, Inc., 2018. 362 p.

23. Edwards, L., Zahid Iqbal, M., & Hassan, M. A multi-layered security model to counter social engineering attacks: a learning-based approach. *International Cybersecurity Law Review*, 2024, vol. 5, pp. 313–336. DOI: 10.1365/s43439-024-00119-z.

24. Moraitis, G., Sakki, G.-K., Karavokiros, G., Nikolopoulos, D., Tsoukalas, I., Kossieris, P., & Makropoulos, C. Exploring the Cyber-Physical Threat Landscape of Water Systems: A Socio-Technical Modelling Approach. *Water*, 2023, vol. 15, iss. 9, article no. 1687. DOI: 10.3390/w15091687.

25. Borowiec, Ł., Demidowski, K., Pecka, M., & Jonarska, A. The analysis of social engineering methods in attacks on authentication systems. *Advances in Web Development Journal*, 2023, vol. 1, no. 7, pp. 83–106.

26. Ruffo, G., Semeraro, A., Giachanou, A., & Rosso, P. Studying fake news spreading, polarisation dynamics, and manipulation by bots: A tale of networks and language. *Computer Science Review*, 2023, vol. 47, article no. 100531. DOI: 10.1016/j.cosrev.2022.100531.

27. Korchenko, O. H., Patsira, Ye. V., & Pukha, D. A. Klasyfikatsiya metodiv sotsial′noho inzhynirynhu [Classification of social engineering methods]. *Zakhyst informatsii – Ukrainian Information Security Research Journal*, 2007, vol. 9, no. 4(36), pp. 37-45. DOI: 10.18372/2410-7840.9.4129. (In Ukrainian).

28. Korchenko, O. H., Hornitska, D. A., & Hololobov, A. Yu. Rozshyrena klasyfikatsiyia metodiv sotsialnoho inzhenirynhu [Extended classification of methods of social engineering]. *Bezpeka informatsii – Ukrainian Scientific Journal of Information Security*, 2014, vol. 20, iss. 2, pp. 197-205. Available at: http://jrnl.nau.edu.ua/index.php/Infosecurity (accessed 10.02.2025) (In Ukrainian).

29. Koyun, A., & Al Janabi, E. Social Engineering Attacks. *Journal of Multidisciplinary Engineering Science and Technology*, 2017, vol. 4, iss. 6, pp. 7533-7538. Available at: https://scholar.archive.org/work/rtexlf6nyrgjtgc76gzorss6aq (accessed 10.02.2025)

30. Troyer, L. *Expanding sociotechnical systems theory through the trans-disciplinary lens of complexity theory*. Transdisciplinary Perspectives on Complex System, Springer, Cham, 2017, pp. 177–192. DOI: 10.1007/978-3-319-38756-7_7.

31. Hadnagy, C. *Social Engineering. The art of Human Hacking*. Wiley Publishing, Inc., 2011. 477 p.

32. Somepalli, S. H., Tangella, S. K. R., & Yalamanchili, S. Information Security Management. *HOLISTICA – Journal of Business and Public Administration*, 2020, vol. 11, iss. 2, pp. 1-16. DOI: 10.2478/hjbpa-2020-0015.

33. Goutam, R. *Cybersecurity Fundamentals: Understand the Role of Cybersecurity, Its Importance and Modern Techniques Used by Cybersecurity Professionals*. BPB Publications,2021. 260 p.

34. Lewandowski, B., Paffenroth, R., & Campbell, K. Improving Network Intrusion Detection Using Autoencoder Feature Residuals. *4th International Conference on Data Intelligence and Security (ICDIS)*, Shenzhen, China, 2022, pp. 31-39. DOI: 10.1109/ICDIS55630.2022.00013.

35. Rabii, A., Assoul, S., Touhami, K., & Roudies, O. Information and cyber security maturity models: a systematic literature review. *Information & Computer Security*, 2020, vol. 28, no. 4, pp. 627-644. DOI: 10.1108/ICS-03-2019-0039.

36. Parhizkari, S. *Anomaly Detection - Recent Advances, AI and ML Perspectives and Applications*, 2024. 168 p. DOI: 10.5772/intechopen.110988.

Received 17.03.2025, Accepted 20.05.2025

ПІДХІД ДО КЛАСИФІКАЦІЇ СОЦІОТЕХНІЧНИХ АТАК

О. Г. Корченко, А.О. Корченко, С.В. Зибін, К.О. Давиденко

Основною метою дослідження є розробка методу побудови моделі класифікації сучасних підходів до реалізації соціотехнічних атак, систематизація та інтеграція існуючих класифікацій відповідних підходів з можливістю розширення новими характерними ознаками. Розвиток інформаційних технологій та обміну даними створюють нові загрози кібербезпеці, включаючи кібератаки та шахрайство. Соціальні мережі та штучний інтелект сприяють удосконаленню соціотехнічних методів. Аналізуючи дані провідних досліджень, визначено певні методи, які соціальні інженери використовують найчастіше, але ці публікації не формують сукупність ознак, що характеризують підходи до реалізації відповідних атак, що дозволить формалізувати процес їх класифікації з системної точки зору. Дослідження спрямоване на вирішення **наступних завдань**: побудувати модель класифікації соціотехнічних атак, в якій можна розробити узагальнену ієрархічну модель; сформувати узагальнений набір ознак, критеріїв та підкритеріїв, що дозволяє вибрати та розробити відповідні

ISSN 1814-4225 (print)
ISSN 2663-2012 (online)

засоби протидії соціотехнічним атакам з системної точки зору; здійснити моделювання відповідної кібератаки для систематичного розуміння дій та контрзаходів. З огляду на це, аналіз та класифікація сучасних підходів до реалізації соціотехнічних атак є важливою складовою стратегії кібербезпеки для забезпечення захисту від постійно зростаючих загроз та є актуальним науковим завданням. **Результати та висновки.** На основі мультитеоретичного підходу запропоновано метод, в якому завдяки етапам визначення набору: ідентифікаторів ознак, критеріїв та підкритеріїв, можливо розробити узагальнену ієрархічну модель класифікації соціотехнічних атак за характеристичним принципом. На основі запропонованої моделі та проаналізованої літератури сформовано узагальнений набір ознак, критеріїв та підкритеріїв, таких як: часовий аспект, галузева приналежність, взаємодія з політикою безпеки, віддаленість, ініціалізація, інструменти, маніпуляції, порушення характеристик, реляційні ознаки, рівень серйозності, тип атакованого джерела, тип доступу, тип звернення, тип соціотехнічної техніки, масштаб, що дозволяє вибрати та розробити відповідні засоби протидії соціотехнічним атакам із системної точки зору. Розглянуто приклад проведення соціотехнічної атаки, в якому врахування моделі класифікації MAISA та таких кроків їх реалізації, як: дослідження цілі, підготовка соціотехнічної атаки, виконання атаки, використання отриманої інформації, приховування слідів, дозволило підійти до розуміння дій соціотехніка під час реалізації фішингової атаки із системної точки зору для подальшої розробки відповідних контрзаходів. Крім того, на основі отриманих критеріїв можна розробити метод оцінки готовності персоналу до протидії різним класам соціотехнічних атак.

Ключові слова: кібербезпека; захист даних; інформаційна безпека; соціотехнічні атаки; методи соціотехнічних атак; соціальна інженерія.

Корченко Олександр Григорович – член-кореспондент НАН України, Senior Member, IEEE, д-р техн. наук, проф., проф. каф. комп'ютерної інженерії та кібербезпеки Інституту безпеки та інформатики Університету Комісії Національної Освіти, Краків, Польща;
перший проректор Державного університету інформаційно-комунікаційних технологій, Київ, Україна.

Корченко Анна Олександрівна – д-р техн. наук, проф., проф. каф. комп'ютерної інженерії та кібербезпеки Інституту безпеки та інформатики Університету Комісії Національної Освіти, Краків, Польща;
проф. каф. безпеки інформації та телекомунікацій, Національний технічний університет "Дніпровська політехніка", Дніпро, Україна.

Зибін Сергій Вікторович – д-р техн. наук, проф., проф. каф. технічного захисту інформації, Національний Авіаційний Університет, Київ, Україна.

Давиденко Кирило Олександрович – асист. каф. захисту інформації та телекомунікацій Національного технічного університету "Дніпровська політехніка", Дніпро, Україна.

Oleksandr Korchenko – Corresponding Member of the National Academy of Sciences of Ukraine, Senior Member, IEEE, D.Sc., Professor, Professor at the Department of Computer Engineering and Cybersecurity of the Institute of Security and Informatics, University of the National Education Commission, Krakow, Poland;
First Vice-Rector of the State University of Information and Communication Technologies, Kyiv, Ukraine,
e-mail: agkorchenko@gmail.com, ORCID: 0000-0003-3376-0631, Scopus Author ID: 57217960494.

Anna Korchenko – D.Sc., Professor, Professor at the Department of Computer Engineering and Cybersecurity of the Institute of Security and Informatics, University of the National Education Commission, Krakow, Poland;
Professor at the Department of Information Security and Telecommunications at the National Technical University "Dnipro Polytechnic", Dnipro, Ukraine,
e-mail: annakor@ukr.net, ORCID: 0000-0003-0016-1966, Scopus Author ID: 56029291400.

Serhii Zybin – D.Sc., Professor, Professor at the National Aviation University, Kyiv, Ukraine,
e-mail: zysv@ukr.net, ORCID: 0000-0002-2670-2823, Scopus Author ID: 57202220667.

Kyrylo Davydenko – Teaching Assistant at the Department of Information Security and Telecommunications, National Technical University Dnipro Polytechnic, Dnipro, Ukraine,
e-mail: kirilldavy@gmail.com, ORCID: 0009-0001-9209-1274.