http://doi.org/10.35784/iapgos.7754

received: 16.05.2025 | revised: 20.12.2025 | accepted: 02.01.2026 | available online: 30.03.2026

METHOD FOR ASSESSING THE RISK OF USER COMPROMISE BASED ON INDIVIDUAL SECURITY PROFILE

Svitlana Lehominova, Mykhailo Zaporozhchenko, Tetiana Kapeliushna, Yuriy Shchavinsky, Tetiana Muzhanova

State University of Information and Communication Technologies, Department of Cybersecurity and Information Protection Management, Kyiv, Ukraine

Abstract. *This article presents a method for assessing the risk of user compromise in corporate information systems caused by social engineering cyberattacks. The approach integrates an evaluation of the individual security profile of each user – based on psychological, organizational, technical, and information influence factors – with graph-based modelling of internal interactions within the organization. Unlike most existing methods that focus solely on isolated user characteristics or assume a single-stage (direct) cyberattack scenario, the proposed method accounts for the propagation of cyberattacks through multi-stage trajectories in communication networks. A formalized four-phase model of social engineering cyberattack implementation is developed, with each phase described as a function of interacting factors. Conditional probabilities are estimated using dynamic coefficients that reflect both the base value and the contextual impact of modifying factors. A graph-based procedure is introduced to calculate the probability of multi-stage compromise based on the structure and intensity of user interactions (e.g., project participation, communication frequency, hierarchical relationships, and shared access to information assets). The proposed method was validated through individual user security profiling, followed by scenario-based modeling of multi-stage social engineering attack propagation on a representative subset. Results show that users with strong individual protection can remain vulnerable due to their position in critical communication chains. The visualization of trajectories exceeding a defined probability threshold supports the identification of high-risk paths and intermediary nodes that require prioritized protection measures. The main scientific contribution lies in combining individualized risk assessment with system-level propagation modelling using interpretable and adaptable mathematical constructs. The method does not require large volumes of empirical data, which ensures its practical applicability even in conditions of limited access to internal information. Future research will focus on automating data collection for factor assessment, adapting the model for real-time operation, and extending it through advanced modelling of behavioral attack scenarios.*

Keywords: information and cybersecurity, social engineering, cyberattack, risk management, user vulnerability, threat modeling

METODA OCENY RYZYKA NARUSZENIA BEZPIECZEŃSTWA UŻYTKOWNIKA NA PODSTAWIE INDYWIDUALNEGO PROFILU BEZPIECZEŃSTWA

Streszczenie. *W niniejszym artykule przedstawiono metodę oceny ryzyka naruszenia bezpieczeństwa użytkowników w korporacyjnych systemach informatycznych spowodowanego cyberatakami wykorzystującymi socjotechnikę. Podejście to łączy ocenę indywidualnego profilu bezpieczeństwa każdego użytkownika – opartą na czynnikach psychologicznych, organizacyjnych, technicznych i informacyjnych – z modelowaniem opartym na grafach wewnętrznych interakcji w organizacji. W przeciwieństwie do większości istniejących metod, które koncentrują się wyłącznie na izolowanych cechach użytkownika lub zakładają scenariusz cyberataku jednoetapowego (bezpośredniego), proponowana metoda uwzględnia rozprzestrzenianie się cyberataków poprzez wieloetapowe trajektorie w sieciach komunikacyjnych. Opracowano sformalizowany czterofazowy model realizacji cyberataku socjotechnicznego, w którym każda faza jest opisana jako funkcja współdziałających czynników. Prawdopodobieństwa warunkowe są szacowane przy użyciu współczynników dynamicznych, które odzwierciedlają zarówno wartość bazową, jak i kontekstowy wpływ czynników modyfikujących. Wprowadzono procedurę opartą na grafach w celu obliczenia prawdopodobieństwa wieloetapowego naruszenia bezpieczeństwa w oparciu o strukturę i intensywność interakcji użytkowników (np. udział w projekcie, częstotliwość komunikacji, relacje hierarchiczne i wspólny dostęp do zasobów informacyjnych). Proponowana metoda została zweryfikowana poprzez indywidualne profilowanie bezpieczeństwa użytkowników, a następnie modelowanie oparte na scenariuszach wieloetapowego rozprzestrzeniania się ataków socjotechnicznych na reprezentatywnej podgrupie. Wyniki pokazują, że użytkownicy posiadający silną indywidualną ochronę mogą pozostawać podatni na zagrożenia ze względu na swoją pozycję w krytycznych łańcuchach komunikacyjnych. Wizualizacja trajektorii przekraczających określony próg prawdopodobieństwa pomaga w identyfikacji ścieżek wysokiego ryzyka i węzłów pośrednich, które wymagają priorytetowych środków ochrony. Główny wkład naukowy polega na połączeniu zindywidualizowanej oceny ryzyka z modelowaniem propagacji na poziomie systemu przy użyciu interpretowalnych i adaptowalnych konstrukcji matematycznych. Metoda nie wymaga dużych ilości danych empirycznych, co zapewnia jej praktyczną przydatność nawet w warunkach ograniczonego dostępu do informacji wewnętrznych. Przyszłe badania będą koncentrować się na automatyzacji gromadzenia danych do oceny czynników, dostosowaniu modelu do działania w czasie rzeczywistym oraz rozszerzeniu go poprzez zaawansowane modelowanie scenariuszy ataków behawioralnych.*

Słowa kluczowe: informacje i cyberbezpieczeństwo, inżynieria społeczna, cyberataki, zarządzanie ryzykiem, podatność użytkowników, modelowanie zagrożeń

Introduction

In the context of rapid digitalization and the increasing dependence of business processes on information systems, social engineering cyberattacks have evolved into a systemic threat to corporate security that extends beyond the technical perimeter. Their effectiveness lies in the attackers' ability to exploit users' cognitive and organizational vulnerabilities while bypassing conventional technical defenses. Incident statistics involving phishing, Business Email Compromise (BEC), and targeted manipulative influence indicate the limited efficiency of traditional technical and administrative countermeasures, which often fail to account for the complex nature of the human factor [14, 15].

Most existing approaches to user vulnerability assessment rely on analyzing only isolated aspects, such as psychological susceptibility to manipulation, technical literacy, or participation in cybersecurity training. However, such models disregard the interaction between these factors and do not allow for the evaluation of a user as an element of a complex sociotechnical system, in which an attack can propagate through trust-based, hierarchical, or functional connections. In particular, the mechanisms of attack transmission via internal communication channels – which form a latent network for the spread of social engineering influence within the corporate structure – remain insufficiently explored.

Effective assessment of a user's compromise risk requires the integration of individual security profile analysis with modeling of the interaction structure among employees. This enables the identification of potential trajectories for the propagation of a social engineering cyberattack within a corporate information system. Such an approach allows not only for the evaluation of the likelihood of a user's initial compromise but also for forecasting the risk of further threat propagation through internal organizational communications.

A critical requirement in this context is minimizing dependence on large volumes of historical or training data, which are typically essential for machine learning-based methods. While such approaches may yield high accuracy in large organizations with extensive logging infrastructures, they are of limited applicability in environments where incident data are scarce or where comprehensive monitoring systems are absent.

Unlike existing methods, this work proposes a formalized method for assessing the risk of user compromise, which maintains high adaptability and allows analysis even under conditions of partial information transparency. The method integrates the evaluation of individual user characteristics with the structure of their interactions within the corporate environment, enabling the assessment of not only primary compromise but also the potential propagation of an attack through the internal network of connections.

The aim of this study is to develop a formalized method for assessing the risk of user compromise resulting from a social engineering cyberattack by integrating individual users' characteristics with the structure of their interactions within the corporate environment. The proposed approach is based on constructing a mathematical model that combines the evaluation of four key factor groups – psychological disposition, organizational safeguards, technical security level, and external informational influence – with graph-based analysis of internal interrelations among employees. This integration enables a well-founded quantitative assessment of the likelihood of a specific user's compromise, taking into account not only their individual security profile but also the systemic context of potential threat propagation within the corporate information system.

The scientific novelty of the proposed method lies in three key aspects and differs from existing approaches, which typically assess only isolated influencing factors, consider only primary compromise, or require large datasets for training:

- the user security profile is formalized as an integrated conceptual model that encompasses four interrelated factor groups: psychological characteristics, organizational environment, level of technical protection, and external destabilizing conditions;
- the risk assessment is conducted using a probabilistic model of social engineering cyberattack propagation within a corporate environment, which accounts not only for the primary compromise of the user but also for potential multi-stage propagation scenarios through a network of professional, communicative, and hierarchical connections;
- the model is implemented as a formalized system of mathematical procedures, combining probabilistic modeling (including Monte Carlo simulation), expert-based methods (such as the Analytic Hierarchy Process), and adaptive parameterization based on the nature of user interactions.

This enables a balance between analytical rigor and the practical applicability of the proposed method for integration into corporate decision-support systems in the field of information and cybersecurity – particularly for prioritizing protection resources, identifying critical nodes within the organizational structure, and simulating social engineering cyberattack scenarios based on the actual dynamics of user interactions within the corporate environment.

The study is structured as follows. Section 1 presents a review of current scientific approaches to assessing the risk of user compromise due to social engineering cyberattacks, with an emphasis on the limitations of existing methods. Section 2 outlines the developed models and formalizes the mathematical framework for calculating the probability of user compromise. Section 3 presents the results of numerical simulations, demonstrates a case study using a test user structure, and provides interpretation of key patterns. Section 4 offers conclusions regarding the practical applicability of the proposed method. Section 5 outlines prospects for future research, including the automation of data collection, adaptation to dynamic environments, and model extension through behavioral scenario modeling.

1. Literature review

A review of scientific literature shows that the majority of current approaches to assessing the risk of user compromise resulting from social engineering cyberattacks are focused on single-stage scenarios, in which the user is treated as an isolated object of analysis. These models typically consider psychological characteristics, behavioral patterns, cybersecurity awareness, frequency of operations, technical literacy, and the presence of protective technologies.

In studies [4, 5], multi-factorial models have been proposed for estimating the likelihood of user compromise within social networks. These models incorporate indicators such as user engagement, motivation, and competence. While these approaches offer a degree of flexibility, their applicability is largely limited to social media environments and does not reflect the specificities of corporate information systems – particularly the level of implemented countermeasures and the dynamic nature of risk shaped by professional and functional interactions among employees.

Study [13] presents a framework for profiling users of cloud services based on operation frequency and cybersecurity awareness. While the model employs a quantitative approach to risk assessment, it disregards psychological factors, external influences, and social connections among users – significantly limiting its applicability in the context of multi-stage attacks.

A separate group of studies focuses on leveraging machine learning algorithms to evaluate user vulnerability. In [10], demographic, technical, and psychological characteristics are incorporated to enable personalized risk assessments. However, the model is based on experimental data and does not consider the influence of external conditions, reducing its applicability in real-world environments. In [7], the emphasis is placed on technical parameters, omitting behavioral and socio-psychological factors. As such, while the model demonstrates potential as a tool for evaluating users' technical protection levels, it fails to provide a comprehensive risk assessment. Study [9] implements an artificial intelligence-based method for phishing detection using natural language processing and behavioral modeling. Nevertheless, the model is critically dependent on regular updates, which poses challenges to its deployment in dynamic operational environments.

In [2], a combination of attack trees and Markov models is proposed, incorporating threat frequency and the effectiveness of manipulative techniques. The model enables classification of threats based on risk levels; however, it omits users' cognitive characteristics and external destabilizing factors. Moreover, it is built on static data, which limits the model's adaptability to dynamic changes.

An alternative line of research is presented in studies [3, 6], which attempt to integrate social engineering threats into attack graph structures. Study [3] introduces a vulnerability assessment framework for social network users that accounts for psychological, behavioral, and emotional characteristics; however, its applicability is restricted to social media interactions. In [6], social and technical vulnerabilities are combined into a unified threat model. While the graph-based approach enables quantitative evaluation of attack propagation trajectories, it fails to capture the nature of internal communications among employees.

A common limitation of the aforementioned approaches is their focus on isolated risk factors – primarily individual user characteristics or the technical context – without accounting for the systemic interactions among elements within a corporate information system. Additionally, they largely neglect the influence of the informational environment shaped by external political, economic, and social conditions. As a result, such models exhibit limited adaptability to real-world organizational environments, where the dynamics of threats are determined not only by internal vulnerabilities but also by external destabilizing influences.

Therefore, there is a pressing need to develop a comprehensive method for evaluating the risk of user compromise that integrates individual security characteristics, organizational context, external informational influence, and the nature and intensity of internal interactions. This method must also enable a systemic analysis of potential trajectories of social engineering cyberattack propagation within the corporate information infrastructure.

2. Method for assessing the risk of user compromise due to a social engineering cyberattack

2.1. Formalization of the user security profile

To accurately assess the risk of user compromise due to a social engineering cyberattack, it is necessary to represent the individual level of user protection through a formalized, multifactor model. The user security profile model proposed in this study is based on four key and interrelated groups of factors, each representing a distinct dimension of influence on the likelihood of a successful attack: psychological characteristics, the organizational environment, technical protection infrastructure, and external informational influences.

The psychological factor (P) encompasses the user's individual cognitive and behavioral traits that determine susceptibility to manipulation and the tendency to interact with malicious content without critically evaluating the associated risks [12].

The organizational factor (O) reflects the effectiveness of information security procedures implemented within the organization, such as incident response policies, training initiatives, and internal regulations. These measures shape the user's awareness and behavior in the context of potential cyber threats [8].

The technical factor (T) characterizes the level of technical protection available to the user against social engineering influence. It includes the presence and effectiveness of mechanisms such as email filtering, access control, intrusion detection, and containment of malicious actions. These technical tools may either prevent the delivery of malicious content or stop the cyberattack after initial user interaction [11].

The informational influence factor (I) represents the external environment in which the user operates. Destabilizing conditions – such as political tension, economic instability, information overload, or disinformation campaigns – can significantly reduce both the user's individual response capability and the effectiveness of organizational security measures [1].

Each of the user security profile factors is determined based on a set of parameters that define the corresponding dimension of influence (Fig. 1).

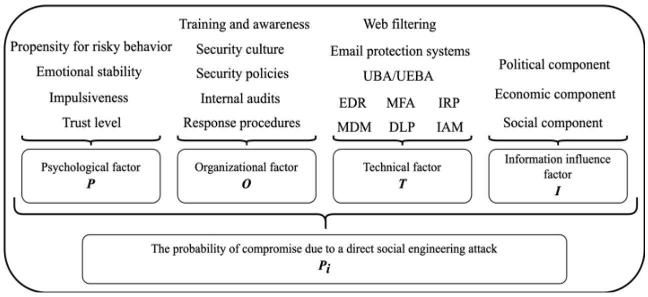


Fig. 1. Evaluated parameters within the user security profile

Within the proposed model, the individual user security profile is defined as a vector:

$$\vec{S} = \{P, O, T, I\} \tag{1}$$

where each component is normalized within the range [0; 1], reflecting the level of protection from minimal (0) to maximal (1).

The values of these components can be obtained through either quantitative or qualitative assessment, based on expert analysis, structured surveys, scenario-based testing, security audits, or the application of analytical models adapted to the organization's specific context. These evaluation methods ensure both flexibility and reproducibility of results, making them applicable across various corporate environments with differing levels of data availability and organizational maturity.

This formalized representation provides a unified foundation for implementing subsequent procedures of user compromise risk modeling. It also enables the integration of individual user characteristics into a network-based model of social engineering influence propagation within the corporate environment.

2.2. Single-stage social engineering cyberattack risk modeling based on the user security profile

Based on the formalized structure of the user security profile, this study proposes a method for assessing the probability of user compromise resulting from a single-stage (direct) social engineering cyberattack. The approach is grounded in the analysis of four key phases of attack development:

1) delivery of malicious content to the user;
2) user interaction with the malicious content;
3) detection of the threat by the user during interaction;
4) technical blocking of the attack before compromise occurs.

A cyberattack is considered successful only if the first two phases (delivery and interaction) are realized, and the detection and technical blocking mechanisms fail. Accordingly, the overall probability of compromise for the i-th user is modeled as a function of four conditional probabilities:

$$P_i = P_{del} \cdot P_{int} \cdot \bar{P}_{det} \cdot \bar{P}_{block} \tag{2}$$

where P_{del} – delivery probability, P_{int} – interaction probability, P_{det} – detection probability, P_{block} – technical blocking probability.

The first phase – delivery of malicious content to the user is modeled by accounting for both the level of technical protection of communication channels and the stability of the external environment. The proposed model considers that even with a high configuration of technical defenses, their effectiveness may be partially undermined by destabilizing external conditions – such as information overload, large-scale crises, or heightened distrust in digital channels. The corresponding mathematical dependency formalizes this assumption by modifying the influence of the technical factor in relation to the information environment:

$$P_{del} = 1 - T \cdot e^{k_{I,T}(I-1)} \tag{3}$$

where T and I denote the values of the technical factor and the informational influence factor, respectively, while $k_{I,T}$ represents the interaction coefficient that captures the impact of the information environment on the effectiveness of technical controls.

Under stable conditions ($I = 1$) protection mechanisms operate at full efficiency, and the probability of malicious content being delivered depends solely on the technical security level. However, in destabilized environments ($I < 1$) a degradation effect is observed in the performance of preventive mechanisms. This phenomenon is reflected in the model through the interaction coefficient $k_{I,T}$.

The second phase – user interaction with malicious content – is modeled with a dominant emphasis on the user's individual psychological characteristics. However, within a real-world corporate environment, psychological vulnerability does not function in isolation but is shaped by contextual factors that significantly influence user risk behavior.

Firstly, the organizational context – such as insufficient awareness, weak security culture, and lack of formalized policies – can considerably amplify pre-existing individual susceptibilities. Secondly, the external informational environment – characterized by societal crises, disinformation campaigns, and cognitive overload – negatively affects a user's ability to respond consciously and interpret messages adequately.

In the model, these effects are captured through a formalized dependency where the baseline probability of user interaction, determined by the psychological factor, is adjusted by parameters reflecting the influence of both the organizational environment and external conditions under which user behavior is formed:

$$P_{int} = 1 - P \cdot e^{k_{O,P}(O-1)+k_{I,P}(I-1)} \tag{4}$$

where $k_{O,P}$ and $k_{I,P}$ denote the influence coefficients of the organizational context and the external informational environment, respectively, on the user's psychological vulnerability.

The third phase – the detection of a social engineering cyberattack by the user prior to its execution – is interpreted as the user's conscious recognition of potentially malicious interaction and the initiation of an appropriate response, such as reporting to the information security department or terminating the communication.

The primary factor influencing the likelihood of successful threat detection is the organizational factor, which reflects the degree of formalization of internal procedures, the consistency and quality of user security training, the presence of feedback mechanisms, and the general user awareness regarding response protocols to suspicious activities.

However, the effectiveness of organizational measures is significantly modified by individual psychological characteristics. Specifically, a low level of attentiveness, high trust in authoritative sources, or a predisposition to risky behavior can reduce the likelihood that a user will interpret anomalous activity as a potential threat. Additionally, this process is influenced by external informational influences – such as cognitive overload, crisis situations, and stress factors – which may lead to cognitive fatigue or a diminished motivation to follow security protocols.

In the proposed model, this is represented through a formalized function, where the organizational factor serves as the base value, adjusted by influence coefficients that reflect the modifying effects of psychological and external contextual variables. This allows the model to capture scenarios in which even a high level of organizational preparedness may be offset by cognitive or environmental limitations:

$$\bar{P}_{\text{det}} = 1 - O \cdot e^{k_{P,O}(P-1)+k_{I,O}(I-1)} \tag{5}$$

where $k_{P,O}$ and $k_{I,O}$ are the coefficients representing the influence of the user's psychological profile and the external informational environment, respectively, on the effectiveness of technical protection measures.

The fourth phase – technical blocking of the attack prior to user compromise – is conceptualized as the final defense barrier capable of halting the execution of a cyberattack regardless of user behavior.

The primary factor determining the probability of successful blocking is the technical component of the user security profile, which reflects the presence, coverage, and operational effectiveness of deployed security technologies. However, the performance of these mechanisms in a real-world environment can be significantly influenced by two additional factors.

First, user psychology – such as ignoring warnings, engaging in risk-prone behavior, or actively circumventing security controls – can undermine the efficiency of technical tools even when they are correctly configured and operational. Second, external informational conditions – including increased attack intensity, delayed system updates, or resource limitations during crises – may degrade the functional reliability of technical protection systems.

Within the proposed model, this relationship is formalized through a functional expression in which the baseline value of technical protection is adjusted using coefficients that account for the potential adverse effects of both the psychological factor and the external informational environment:

$$\bar{P}_{block} = 1 - T \cdot e^{k_{P,T}(P-1)+k_{I,T}(I-1)} \tag{6}$$

where $k_{P,T}$ and $k_{I,T}$ represent the influence coefficients of the user's psychological profile and the informational environment, respectively, on the overall effectiveness of technical security mechanisms.

To reflect the complex interplay between factors in the user security profile and ensure sensitivity to fluctuations in external conditions, the model introduces influence coefficients defined as:

$$k_{cor,main} = d_{cor,main} - s_{cor,main} \tag{7}$$

where $d_{cor,main}$ denotes the dynamic component, which adapts based on the values of the main and correcting factors, while $s_{cor,main}$ is the static component determined through expert evaluation under boundary condition analysis.

The dynamic component enables the model to respond effectively to combinations of low factor values that reflect conditions of maximum system vulnerability:

$$d_{cor,main} = \min(cor, main)^{\max(1-cor,1-main)} \tag{8}$$

This mechanism ensures an exponential amplification of influence under adverse circumstances (Fig. 2). Such an approach allows the model to capture not only the isolated values of individual factors but also the nature of their interaction, enhancing the realism and sensitivity of the risk assessment.

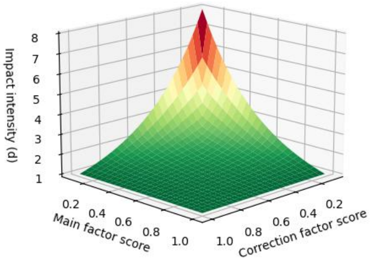


Fig. 2. Dependence of the dynamic component of the influence coefficients on the factor values

The static component serves as a compensatory mechanism that stabilizes the model's behavior under boundary conditions and ensures its consistency with expected limits when input parameters are fixed.

The combination of dynamic and static elements enables an adaptive yet balanced risk assessment that remains robust to fluctuations in individual factors while remaining responsive to high-risk scenarios.

Fig. 3 illustrates the impact of combining the dynamic and static components on the distribution of the user's interaction probability with malicious content: the left panel shows the model using only the dynamic component, while the right panel presents the result when both components are taken into account.

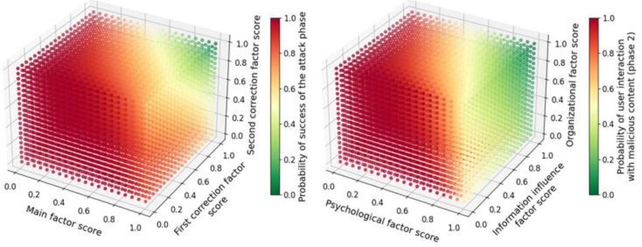


Fig. 3. The impact of the combined use of dynamic and static components on the probability distribution of attack phases (on the example of user interaction with malicious content)

Thus, the proposed method for evaluating the individual risk of user compromise based on the security profile enables a step-by-step analysis of each phase of a social engineering cyberattack. The use of formalized dependencies that incorporate both dynamic and static components of influence coefficients ensures the model's adaptability to contextual changes, factor interdependencies, and evolving threat levels. This approach not only provides a quantitative assessment of risk for a specific user but also allows the identification of critical factors contributing to heightened vulnerability, thereby forming a foundation for the development of targeted countermeasures.

2.3. Multi-stage social engineering cyberattack risk modeling

While the likelihood of a single-stage social engineering cyberattack is primarily determined by a user's individual and organizational protection characteristics, the probability of a multi-stage attack propagating within a corporate information system is largely influenced by the structure of interpersonal interactions – specifically, the intensity of communication and the users' roles within the organizational hierarchy.

Unlike initial attacks that originate externally, further propagation via already compromised users faces significantly lower detection thresholds, as attackers gain several strategic advantages, including:

- the ability to mimic authentic communication patterns through access to message history, characteristic language structures, and established interaction timelines;
- a high degree of trust in the source, due to the use of legitimate corporate accounts;
- exploitation of trusted internal communication channels, which are not always subject to rigorous monitoring or filtration;
- utilization of internal knowledge (such as company structure, active projects, job functions, and interpersonal relationships) to enhance the personalization and targeting precision of subsequent attacks.

Under these conditions, the intensity and nature of interactions between users become critical for forecasting threat propagation trajectories. To quantitatively assess the probability of further user compromise, the following structural interaction indicators are proposed:

- participation in joint projects;
- regular communication (e.g., via email or internal platforms);
- hierarchical relationships within the organizational structure;
- shared access to critical assets.

The "joint projects" criterion reflects the degree of professional collaboration, which may indicate functional interdependence and a high level of trust – factors that facilitate attack propagation. The evaluation is based on project management system data over a defined observation period and involves normalization of the number of shared projects between each user pair. This approach eliminates the influence of organizational scale and ensures comparability of the indicators across different user groups.

The "communication" criterion accounts for the frequency of contact as a factor that shapes a persistent interpersonal context, thereby reducing the likelihood of detecting an attack. Interaction intensity is measured by the number of contacts over a specified period, based on data from corporate communication platforms. Message content is not analyzed, preserving user confidentiality.

Hierarchical relationships between users are considered a distinct criterion affecting the probability of social engineering cyberattack propagation in cases of direct subordination. The existence of a formal "supervisor-subordinate" link significantly increases risk by fostering compliance with atypical requests without critical assessment. The data are sourced from HRM systems, and the evaluation is performed in binary form: presence or absence of hierarchical dependency.

The "shared access to critical assets" criterion is based on the assumption that users with equivalent access rights exhibit a higher level of functional interaction, which may facilitate chain compromise. Assessment is conducted using data from identity and access management systems and is performed by normalizing the volume of commonly accessible resources.

Collectively, these criteria enable the quantitative evaluation of the probability of social engineering cyberattack propagation from a compromised user to other system participants, taking into account the specific characteristics of the organizational structure. The model is grounded in the assumption that a greater number of interaction types and higher interaction intensity between users correlates with an increased risk of compromise. The probability of attack transmission is calculated for each user pair and reflects both the intensity of interactions and the baseline compromise probabilities associated with each type of interaction, which represent the risk of attack propagation under maximum interaction conditions:

$$S_{i,j} = 1 - \prod_{t=1}^{n}(1 - p_t)^{in_t^{i,j}} \tag{9}$$

where p_t denotes the baseline probability of compromise for t-th interaction type, and $in_t^{i,j}$ represents the intensity of the t-th interaction type between users i and j.

The baseline probabilities of compromise can be tailored to the specifics of a particular corporate environment based on empirical data or expert analysis, thus ensuring the model's flexibility and its applicability across diverse organizational structures.

The described model for estimating the probability of attack propagation between user pairs is local in nature and reflects only the likelihood of a direct transmission from one user to another. However, a multi-stage social engineering cyberattack is not limited to interactions between just two users – it is executed as a sequence of transitions through multiple nodes, forming an attack trajectory within the network of interactions.

Each trajectory is represented by an ordered set of users $\{U_{n1}, U_{n2}, \dots, U_{nm}\}$. The probability of realizing a specific trajectory is defined as the product of the probability of compromising the initial node and the probabilities of propagation across all subsequent pairs:

$$T_{n_1,\dots,n_m} = P_{n_1} \cdot \prod_{k=1}^{m-1} S_{n_k,n_{k+1}} \tag{10}$$

When modeling a multi-stage social engineering cyberattack targeting a specific user, it is important to account for the potentially large number of propagation trajectories that may lead to the target node. For instance, in the case of user U_5, possible attack paths include both short sequences (e.g., $U_1 \to U_5$, $U_2 \to U_5$), and extended chains (e.g., $U_2 \to U_3 \to U_7 \to U_6 \to U_5, U_{10} \to U_8 \to U_1 \to U_5$). Each trajectory is characterized by its own probability of successful propagation, which depends on the individual compromise risk of the initial node and the transmission probabilities along each step of the path.

However, exhaustively evaluating all possible trajectories is not only computationally intensive but also leads to artificial overestimation of risk due to duplication of low-probability paths. Even when the individual probabilities are small, the cumulative effect of numerous similar trajectories (e.g., $U_2 \to U_3 \to U_7 \to U_5,; U_4 \to U_1 \to U_7 \to U_5;\ U_{10} \to U_8 \to U_7 \to U_5$) can inflate the overall risk, resulting in systematic overestimation of the user's probability of compromise.

To optimize the model, a risk aggregation approach through the penultimate node is proposed. Instead of accounting for all possible trajectories leading to the target user, the model considers only the maximum attack probability originating from each immediate predecessor – the node that directly precedes the target in any trajectory. As a result, the integral probability of compromise for user j is defined as follows:

$$C_j = 1 - \prod_{l=1}^{N}\left(1 - T_{l,j}^{max}\right) \tag{11}$$

where $T_{l,j}^{max}$ is the maximum probability of attack propagation from user l to j across all possible trajectories in which l is the penultimate node.

This approach reduces the computation to N independent multiplicative terms for a system with N users, striking a balance between model accuracy and computational efficiency. It eliminates redundant risk duplication while maintaining the relevance and interpretability of the resulting compromise probability.

3. Results and analysis

To validate the functionality of the proposed model and assess its practical applicability, an experimental study was conducted with the objective of quantitatively estimating the probability of user compromise in a corporate information system under direct and multi-stage social engineering attack scenarios. The study involved a population of 83 users representing different organizational roles and hierarchical levels.

At the first stage, individual security profiles were constructed for all users in the population. These profiles provide quantitative estimates of the probability of compromise resulting from a single-stage social engineering attack and serve as initial parameters for subsequent modeling of attack propagation. A subset of the obtained security profile values is presented to illustrate the distribution of user vulnerability within the analyzed population (Table 1).

At the second stage, a subset of users was randomly selected from the general population for scenario-based modeling of multi-stage social engineering attack propagation. The selection aimed to construct a minimally sufficient sample for exploratory modeling under conditions of limited data availability. The minimum required sample size was estimated using a standard formula for a finite population:

$$n = \frac{N \cdot z^2 \cdot p(1-p)}{(N-1) \cdot e^2 + z^2 \cdot p(1-p)} \tag{12}$$

where N denotes the population size, z is the standard normal quantile corresponding to the confidence level, p is the assumed population proportion, and e is the acceptable margin of error. Assuming $N = 83$, a confidence level of 0.95 $z = 1.96$, a conservative estimate $p = 0.5$, and an acceptable error margin of $0.25 \le e \le 0.3$, the minimum required sample size was estimated as $n \approx 10$.

To further assess the consistency of the selected subset with the overall population, the homogeneity of the distributions of key security profile parameters was evaluated using non-parametric statistical tests. The results did not reveal statistically significant differences between the selected subset and the general population ($p > 0.05$), indicating the absence of systematic sampling bias and confirming the suitability of the subset for scenario-based modeling.

Table 1. Estimated probabilities of user compromise under direct social engineering attacks

User	*P*	*O*	*T*	*I*	P_{del}	P_{int}	$\overline{P}_{det}$	$\overline{P}_{block}$	P_i
$User_1$	0.88	0.73	0.67	0.28	0.65	0.52	0.7	0.7	0.17
$User_2$	0.9	0.78	0.67	0.28	0.65	0.49	0.7	0.7	0.15
$User_3$	0.96	0.8	0.67	0.28	0.65	0.42	0.63	0.7	0.12
$User_4$	0.73	0.75	0.61	0.28	0.71	0.67	0.71	0.76	0.26
$User_5$	0.67	0.71	0.61	0.28	0.71	0.73	0.75	0.77	0.3
$User_6$	0.84	0.69	0.61	0.28	0.71	0.57	0.74	0.75	0.23
$User_7$	0.69	0.64	0.51	0.28	0.79	0.72	0.8	0.84	0.38
$User_8$	0.59	0.64	0.51	0.28	0.79	0.8	0.81	0.85	0.44
$User_9$	0.53	0.62	0.51	0.28	0.79	0.84	0.83	0.86	0.48
$User_{10}$	0.43	0.57	0.51	0.28	0.79	0.9	0.88	0.87	0.55
…									
$User_{81}$	0.87	0.61	0.51	0.28	0.69	0.55	0.79	0.82	0.29
$User_{82}$	0.91	0.68	0.67	0.28	0.65	0.49	0.74	0.7	0.17
$User_{83}$	0.38	0.57	0.51	0.28	0.79	0.92	0.89	0.88	0.58

For the selected users, a directed interaction graph with weighted edges was constructed, where edge weights represent the probabilities of attack transition between users, determined by the intensity and directionality of their interactions (Fig. 4). The individual security profile values were used as input parameters for the multi-stage attack realization model.

To quantitatively assess the psychological factor, a standardized survey was conducted using scenario-based tests designed to identify typical user responses to manipulative influences. Each component of the psychological factor was evaluated based on 10 situational questions simulating various aspects of behavior under information pressure. Respondents provided answers on a five-point scale.

The integral assessment of the psychological factor was calculated as the arithmetic mean of the evaluated components. The resulting value was scaled to the [0; 1] interval, where a score of 1 corresponded to maximum resistance to manipulation, and 0 indicated complete vulnerability.

The organizational factor was assessed based on the analysis of internal security policies, practices, and procedures. This evaluation utilized information security audit reports, employee surveys, and a review of internal documentation, training plans, and incident response procedures.

The components of the organizational factor were evaluated using a six-level scale (ranging from 1 to 0.05), which reflects the maturity of practices, as well as the quality and regularity of implemented measures. The criteria for each level were developed based on international standards, particularly ISO/IEC 27001 and ISO/IEC 27004, and were adapted to the corporate context.

The overall score for the organizational factor was calculated using a multiplicative model with weighted coefficients determined through the Analytic Hierarchy Process, allowing for the differential impact of individual components on the total level of user protection to be taken into account.

The technical factor was evaluated based on the implementation level of key security controls applied to relevant personnel categories within the information system. A graded evaluation scale was developed for these controls, reflecting their functional capabilities, compliance with modern standards, and integration with other components of the security architecture. The assessment was conducted through the analysis of technical documentation, internal audit reports, surveys of responsible personnel, and verification of service contracts for corresponding security tools.

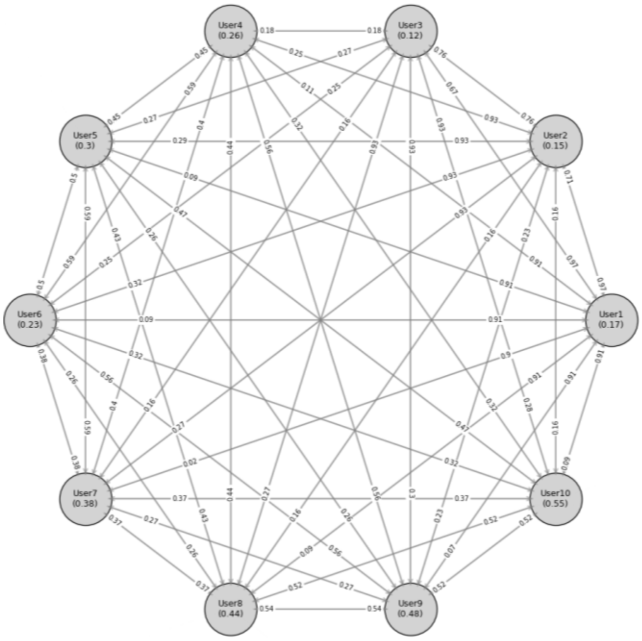


Fig. 4. Complete corporate information system users' interaction graph

Within each user category, the level of technical protection was assessed across several directions. The final score for the technical factor was calculated as a weighted average, with weights determined by expert judgment according to the effectiveness of each technology in counteracting different phases of a social engineering cyberattack. This approach reflects the relative independence of individual security tools, where deficiencies in one component may be partially offset by the presence of others.

The target scale for results was normalized to the interval [0; 1], where a value of 1 corresponded to the full implementation of modern security technologies with a high level of automation and integration, while a value of 0 reflected a complete absence of technical protection or the use of outdated solutions with high vulnerability.

The evaluation of the information influence factor was carried out based on three components, each of which included several assessment levels spanning from full stability to critical degradation. The scale ranged from 1 (a maximally favorable environment) to 0.05 (deep crisis) and was constructed using external open sources. These included data from international analytical institutions, reports from think tanks and governmental bodies, as well as aggregated indicators of macroeconomic and social conditions – such as inflation, levels of civil unrest, crime rates, and the intensity of disinformation campaigns.

The overall value of the information influence factor was calculated using a multiplicative model with weighting coefficients determined through the Analytic Hierarchy Process. This approach made it possible to account for the disproportionate impact of certain components under crisis conditions, where even minor political or social destabilization can significantly affect the overall level of informational vulnerability.

Based on the obtained evaluations, the following were calculated for each user:

1) the probability of compromise as a result of a single-stage social engineering cyberattack P_i (Fig. 5);
2) the integral probability of compromise C_i, taking into account potential propagation within the corporate interaction structure.

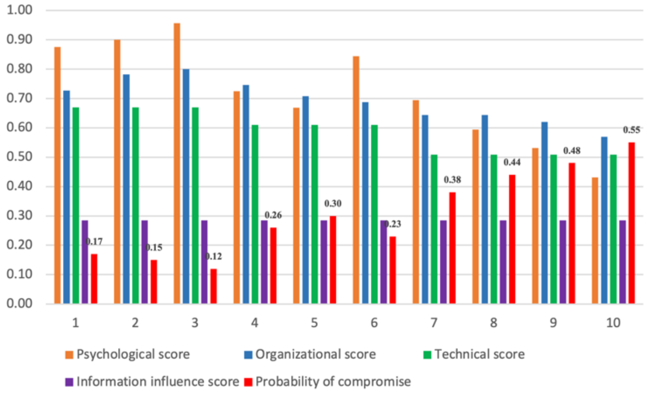
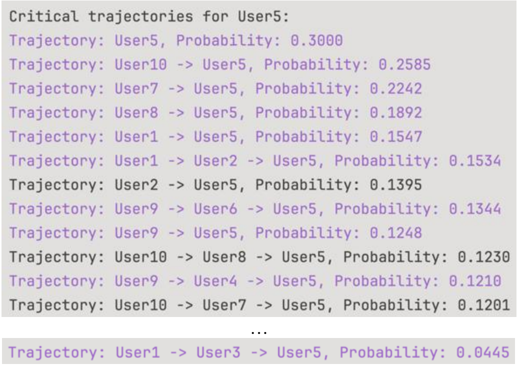


Fig. 5. Results of the assessment of user compromise probability due to a single-stage social engineering cyberattack

For each user, all possible attack trajectories were identified and ranked in descending order of probability. The trajectories included in the calculation of the integral probability of compromise are highlighted in color (Fig. 6).



```
Critical trajectories for User5:
Trajectory: User5, Probability: 0.3000
Trajectory: User10 -> User5, Probability: 0.2585
Trajectory: User7 -> User5, Probability: 0.2242
Trajectory: User8 -> User5, Probability: 0.1892
Trajectory: User1 -> User5, Probability: 0.1547
Trajectory: User1 -> User2 -> User5, Probability: 0.1534
Trajectory: User2 -> User5, Probability: 0.1395
Trajectory: User9 -> User6 -> User5, Probability: 0.1344
Trajectory: User9 -> User5, Probability: 0.1248
Trajectory: User10 -> User8 -> User5, Probability: 0.1230
Trajectory: User9 -> User4 -> User5, Probability: 0.1210
Trajectory: User10 -> User7 -> User5, Probability: 0.1201
…
Trajectory: User1 -> User3 -> User5, Probability: 0.0445
```

Fig. 6. List of compromise trajectories for User$_5$

The calculated probabilities of user compromise are presented in Fig. 7. The analysis of the results demonstrates that users with high individual protection scores may appear more vulnerable in scenarios involving internal propagation of attacks, particularly when they are actively involved in the corporate communication network.

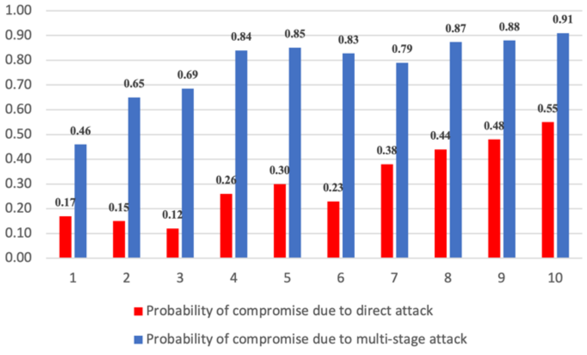


Fig. 7. Comparison of compromise probabilities from single-stage and multi-stage social engineering cyberattacks

This highlights the critical role of the socio-technical context in risk modeling: even in the presence of a well-developed individual security profile, the intensity of information exchange within the corporate environment can significantly increase the probability of compromise as a result of multi-stage social engineering cyberattack.

To support effective risk management of multi-stage social engineering attack propagation, the proposed method enables the visualization of critical attack trajectories based on predefined probability thresholds. This approach focuses analytical attention only on those trajectories that pose a substantial threat from the standpoint of the specified risk level, excluding low-impact paths from consideration. For instance, Fig. 8 presents all attack trajectories with a realization probability exceeding 0.2.

Analysis of this visualization allows the identification of users who act as key intermediaries in the propagation of social engineering attacks within the organizational structure. These users may not be the most vulnerable in terms of individual security profiles, yet their position in the communication network – such as simultaneous involvement in critical projects, access to shared resources, and active cross-departmental collaboration – creates conditions for the effective spread of an attack following the compromise of a preceding node.

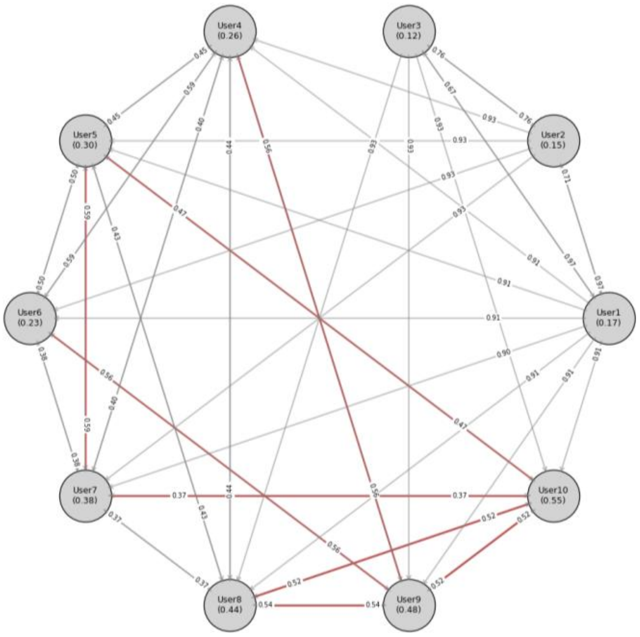


Fig. 8. Communication links between users involved in social engineering cyberattack trajectories with a probability above 0.2

The results of the analysis can be used to identify topologically vulnerable attack routes, enabling targeted risk mitigation strategies tailored to the actual structure of corporate communications. In particular, the findings support informed decision-making related to the reconfiguration of communication flows, access control adjustments, or the implementation of personalized security awareness measures for users situated on high-risk trajectories.

By visualizing the most probable paths of attack propagation within the organizational structure, the proposed approach enhances situational awareness for security teams and facilitates proactive identification of users whose network position makes them critical intermediaries.

4. Conclusions

The article presents a method for assessing the risk of user compromise in a corporate information system due to a social engineering cyberattack, incorporating both the individual security profile and the structure of internal user interactions. A formalized model is proposed, combining four key influencing factors – psychological profile, organizational protection, technical security level, and external informational influence – with probabilistic graph-based modeling of attack propagation scenarios.

The model enables the estimation of not only the probability of a direct attack on each user, but also the cumulative risk of compromise through multi-stage propagation within the interaction network. A trajectory aggregation mechanism based on key nodes was introduced, ensuring a balance between computational efficiency and predictive accuracy. The results indicate that users with high individual protection scores may still be vulnerable if they are embedded in critical communication routes, highlighting the need for a comprehensive approach to risk modeling.

The practical value of the proposed method lies in its applicability to real-world environments, as it does not require large volumes of empirical data, unlike machine learning approaches, and offers a high level of adaptability to specific corporate contexts.

5. Future works

A promising direction for further research involves the automation of data collection for assessing user security factors and interaction patterns based on information extracted from corporate systems. Special attention will be given to adapting the method for real-time application and integrating it with security monitoring systems to enable dynamic risk analysis.

Future developments also include the enhancement of behavioral modeling for social engineering cyberattack scenarios and the expansion of the input parameter set influencing the probability of social engineering propagation.

References

[1] Abdollahbeigi, B., & Salehi, F. (2019). The Effect of External Environment Characteristics on Effective IT Governance through Organizational Performance. *Journal of Technology Management and Technopreneurship (JTMT)*, *7*(1), 19–28. https://jtmt.utem.edu.my/jtmt/article/view/5566

[2] Aijaz, M., & Nazir, M. (2024). Modelling and analysis of social engineering threats using the attack tree and the Markov model. *International Journal of Information Technology*, *16*(2), 1231–1238. https://doi.org/10.1007/s41870-023-01540-z

[3] Albladi, S. M., & Weir, G. R. S. (2018). User characteristics that influence judgment of social engineering attacks in social networks. *Human-Centric Computing and Information Sciences*, *8*(1), 5. https://doi.org/10.1186/s13673-018-0128-7

[4] Albladi, S. M., & Weir, G. R. S. (2019). A Conceptual Model to Predict Social Engineering Victims. *2019 IEEE 12th International Conference on Global Security, Safety and Sustainability (ICGS3)*, 212–212. https://doi.org/10.1109/ICGS3.2019.8688352

[5] Albladi, S. M., & Weir, G. R. S. (2020). Predicting individuals' vulnerability to social engineering in social networks. *Cybersecurity*, *3*(1), 7. https://doi.org/10.1186/s42400-020-00047-5

[6] Beckers, K., Krautsevich, L., & Yautsiukhin, A. (2015). Using Attack Graphs to Analyze Social Engineering Threats: *International Journal of Secure Software Engineering*, *6*(2), 47–69. https://doi.org/10.4018/IJSSE.2015040103

[7] Bohonko, O., & Lysenko, S. (2023). Social engineering attacks detection approach. Herald of Khmelnytskyi National University. Technical Sciences, 327(5(2), 231-236. https://doi.org/10.31891/2307-5732-2023-327-5-231-236

[8] Cletus, A., Weyory, B., & Opoku, A. (2022). Improving Social Engineering Awareness, Training and Education (SEATE) using a Behavioral Change Model. *International Journal of Advanced Computer Science and Applications*, *13*(5). https://doi.org/10.14569/IJACSA.2022.0130572

[9] Fakhouri, H. N., Alhadidi, B., Omar, K., Makhadmeh, S. N., Hamad, F., & Halalsheh, N. Z. (2024). AI-Driven Solutions for Social Engineering Attacks: Detection, Prevention, and Response. *2024 2nd International Conference on Cyber Resilience (ICCR)*, 1–8. https://doi.org/10.1109/ICCR61006.2024.10533010

[10] Huseynov, F., & Ozdenizci Kose, B. (2024). Using machine learning algorithms to predict individuals' tendency to be victim of social engineering attacks. *Information Development*, *40*(2), 298–318. https://doi.org/10.1177/02666669221116336

[11] Lopes, A., Mamede, H. S., Reis, L., & Santos, A. (2024). Common Techniques, Success Attack Factors and Obstacles to Social Engineering: A Systematic Literature Review. *Emerging Science Journal*, *8*(2), 761–794. https://doi.org/10.28991/ESJ-2024-08-02-025

[12] Wang, Z., Sun, L., & Zhu, H. (2020). Defining Social Engineering in Cybersecurity. *IEEE Access*, *8*, 85094–85115. https://doi.org/10.1109/ACCESS.2020.2992807

[13] Ye, Z., Guo, Y., Ju, A., Wei, F., Zhang, R., & Ma, J. (2020). A Risk Analysis Framework for Social Engineering Attack Based on User Profiling: *Journal of Organizational and End User Computing*, *32*(3), 37–49. https://doi.org/10.4018/JOEUC.2020070104

[14] 2024 Data breach investigations report. *Verizon Business*, https://www.verizon.com/business/en-gb/resources/reports/2024/dbir/2024-dbir-data-breach-investigations-report.pdf

[15] Cost of data breach report 2024. *IBM Corporation*. https://table.media/wp-content/uploads/2024/07/30132828/Cost-of-a-Data-Breach-Report-2024.pdf

Prof. Svitlana Lehominova
e-mail: s.legominova@duikt.edu.ua

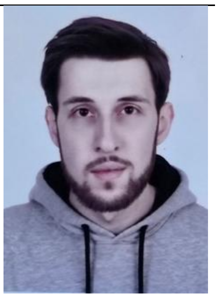
Doctor of Sciences (economics), professor, Head of the Department of Cybersecurity and Information Protection Management, State University of Information and Communication Technologies, Kyiv, Ukraine.
Research interest: information security audit, project management in information security, strategic communications, enterprise cybersecurity management.

https://orcid.org/0000-0002-4433-5123

Ph.D. Mykhailo Zaporozhchenko
e-mail: m.zaporozhchenko@duikt.edu.ua

Ph.D. in cybersecurity, associate professor, Department of Cybersecurity and Information Protection Management, State University of Information and Communication Technologies, Kyiv, Ukraine.
Research interest: auditing of information security management systems; information security risk management; testing personnel susceptibility to social engineering; cybersecurity awareness.

https://orcid.org/0000-0003-0182-9497



D.Sc. Tetiana Kapeliushna
e-mail: t.kapeliushna@duikt.edu.ua

Doctor of Sciences (economics), associate professor, Department of Cybersecurity and Information Protection Management, State University of Information and Communication Technologies, Kyiv, Ukraine.
Research interest: enterprise security, economic security of the enterprise, enterprise information security management, enterprise cybersecurity management, enterprise information security.

https://orcid.org/0000-0001-7490-6751

Ph.D. Yuriy Shchavinsky
e-mail: y.shchavinskyi@duikt.edu.ua

Candidate of Technical Sciences, associate professor, Department of Cybersecurity and Information Protection Management, State University of Information and Communication Technologies, Kyiv, Ukraine.
Research interest: management automation, decision support systems, application of artificial intelligence in cybersecurity management, formation of competencies of cybersecurity specialists.

https://orcid.org/0000-0002-2319-8983

Ph.D. Tetiana Muzhanova
e-mail: t.muzhanova@duikt.edu.ua

Candidate of Sciences in public administration, associate professor, Department of Cybersecurity and Information Protection Management, State University of Information and Communication Technologies, Kyiv, Ukraine.
Research interest: best practices of information and cyber security management, personnel security, information and psychological security, information security of a state, strategic communications.

https://orcid.org/0000-0002-7435-0287