The OSCAR PUBLISHING Services
American Journal of Applied Science and Technology

VOLUME Vol.05 Issue 10 2025
PAGE NO. 37-42
DOI 10.37547/ajast/Volume05Issue10-09

Assessment Of Social Engineering Attack Traces In Information Systems

Obidjon Bekmirzaev
Tashkent State University of Economics, International Nordic University, Uzbekistan

Zafarbek Soipov
Student at "Rahimov School" Tashkent, Uzbekistan

Received: 19 August 2025; **Accepted:** 15 September 2025; **Published:** 17 October 2025

Abstract: The article examines social engineering attacks in information systems and issues related to detecting and assessing their traces. Using social-graph models, the interactions between users and the propagation paths of attacks are analyzed. Alongside the probability of attack success, the expected level of damage to the organization is also taken into account. The proposed approach enables a more realistic assessment of information security and facilitates effective planning of preventive measures.

Keywords: Social engineering, information security, social graph, attack traces, criticality assessment.

INTRODUCTION:

Social engineering attacks are among the most dangerous and widespread threats in the field of information security. Their relevance is explained by several factors. It is often easier to deceive a person than to defeat technical controls. Many organizations deploy strong passwords, encryption technologies, firewalls and other protective measures. However, if a user makes a simple mistake or falls for an attacker's deception, all those systems can be bypassed. According to statistics, recent international cybersecurity reports note that the success rate of social engineering attacks in recent years is around 70–80%. This indicates that despite technical protections, the human factor remains the weakest link. The wide spread of phishing and spear-phishing also increases the danger of these attacks. Fake messages, links or documents sent by e-mail deceive users and force them to disclose confidential information. In particular, spear-phishing attacks targeted at specific individuals pose a significant risk. The rise of social networks is another important factor. Open information about users on platforms such as Facebook, Telegram and LinkedIn gives attackers convenient opportunities to manipulate them. The issue of financial losses is also pressing: social engineering attacks cause companies to lose billions of dollars. For example, in 2017 such attacks caused losses of 600 billion roubles in Russia. Increasingly sophisticated attack techniques further complicate the fight for security. In addition to simple phishing, more elaborate methods such as pretexting, baiting and quid pro quo are being used more widely [1-10].

Recent international cybersecurity reports emphasize that social engineering attacks are considerably more successful than many other types of attacks. Research shows that the success rate of such attacks is 70–80 percent. These figures demonstrate that, despite technical defenses, the human factor remains the weakest link in information security. A single mistake or lapse by an ordinary user can sharply reduce the security level of an entire corporate system. Therefore, the high effectiveness of social engineering attacks justifies treating them as a topical and dangerous threat.

No matter how advanced information security systems are, user behavior continues to be the weakest link. Even when strong passwords, multi-factor authentication, encryption technologies and firewalls are in place, users' inattention or lack of skills can render those protections ineffective. For example, clicking a link from an unknown source, disclosing personal information, or trusting a fake message can

give attackers easy access to systems. Hence, alongside technical measures, it is necessary to regularly train users, foster a culture of security, and increase awareness of social engineering techniques [11,12].

The main aim of this article is to assess the traces of social engineering attacks by taking into account not only the probability of an attack but also the potential level of damage it may cause. Practical studies show that some attacks, although highly probable, may result in relatively minor damage, whereas rare attacks can produce major financial losses or substantial data loss. Therefore, analyzing attacks solely by probability does not provide a full picture. In the proposed approach, a "criticality level" is determined for each attack vector as the product of its probability and damage metrics, thereby identifying the most dangerous paths. This method enables organizations to allocate resources more effectively, to plan security policies more precisely, and to minimize real risks [13-16].

Ijtimoiy muhandislik hujumlarini baholash bo'yicha olib borilgan tadqiqotlar orasida avvalo xorijiy olimlarning ishlari alohida o'rin tutadi. Masalan, K. Mitnick o'zining "The Art of Deception" nomli maqolasida inson psixologiyasidan foydalanishga asoslangan hujumlarni tahlil qilgan hamda foydalanuvchilarning xatti-harakati texnik himoyadan ham ko'ra ko'proq zaiflik keltirib chiqarishini ta'kidlagan. Ushbu ishda hujumlarning amalga oshish ehtimolligi muhokama qilingan bo'lsa-da, ular keltirib chiqaradigan zarar miqdori chuqur ko'rib chiqilmagan[17,18].

N. Oligfer and V. Oligfer, in their scholarly work "Компьютерные сети. Принципы, технологии, протоколы", elucidate the general theoretical foundations of network security; however, the issue of detecting traces of social engineering attacks is not covered there in sufficient depth [19-23].

Among recent international studies, the paper by M. Huber et al., "Social engineering: A survey of techniques, tools, and social implications," is noteworthy: the authors classify widely used social engineering methods and attempt to assess their societal impact. Nevertheless, their research does not place emphasis on modeling attack traces using graph-based approaches[24].

Among local researchers, O. Bekmirzayev's study entitled "A Model for Searching Attack Traces in Information Systems" was published in the journal Digital Transformation and Artificial Intelligence. Although the study analyzes attack traces based on an algorithmic approach, it does not sufficiently address the issue of jointly assessing damage and probability [25-27].

Similarly, the article by B. Jorayev and D. Karimov titled "Social Engineering Attacks and Their Impact on Corporate Security" was published in the scientific journal Information Security and Cryptography, where practical examples of attacks such as phishing and spear-phishing are presented. However, this article also does not consider analyzing attack vectors using a graph-based approach or determining their criticality level [28,29].

This literature review shows that existing studies have mainly focused on calculating attack probabilities or classifying attack methods. The application of a social-graph approach in identifying attack traces — while jointly assessing potential damage and probability — has not been sufficiently explored, which highlights the scientific and practical relevance of this topic.

METHODS

In the proposed approach, users within the information system and their mutual interactions are represented using a graph model. In this model each user is treated as a node, while their relationships — such as information exchange, access rights, or dependencies — are depicted by edges. This graph-based representation proves effective for detecting traces of social engineering attacks because it enables step-by-step tracking of the propagation process from one user to another.

Each node in the graph not only represents a user role but also takes into account that user's level of access to documents and the relative importance of those documents. Edges express the probability of an attack propagating from one user to another. Using a model constructed in this way, it is possible to evaluate attack paths, their likelihoods, and the potential magnitude of the damage they may cause.

This methodology provides a more realistic reflection of real-world conditions when analyzing social engineering attacks, since user behavior, access privileges, and interpersonal relationships are decisive factors in whether an attack will succeed.

Mathematical Formulations for Estimating Attack Likelihood and Expected Damage.

Below are the main formulas used to calculate attack probability, damage (impact), and criticality based on the social-graph model:

– $G = (V, E)$ graph where $V -$ is the set of users (nodes) and, $E -$ is the set of connections (edges).

– For each edge, the propagation probability of an attack is $p_{uv} \in [0,1]$ $(u \to v)$.

– D_v – the set of documents (resources) belonging to user v or which can be exfiltrated via v.

– For a document (resource) $d \in D_v$ its value (damage) is $D_d > 0$.

1) Path-based attack probability.

Let there be a path $\pi = (s = v_0, v_1, \dots, v_k = t)$ from an initial node s to a target node t consisting of consecutive edges. Assuming the edges are independent, the probability of a successful attack along this path is:

$$P(\pi) = \prod_{i=0}^{k-1} p_{v_i v_{i+1}}$$

Let $\{\pi_j\}$ be the set of all (independent) paths leading from s to t. The probability that at least one of these paths succeeds can be written using the inclusion–exclusion principle. A commonly used simplified form (assuming path-level independence) is:

$$P_{s \to t} = 1 - \prod_j (1 - P(\pi_j))$$

2) Node-level attack (access) probabilities in the network.

Given an initial set of compromised nodes $S \subseteq V$ we denote by q_v the probability that node v is reached.

Under the single-path assumption: $$q_v = \max_{\pi \in \mathrm{Paths}(S \to v)} P(\pi)$$

Under the multi-path (combined influence) assumption:

$$q_v = 1 - \prod_{\pi \in \mathrm{Paths}(S \to v)} (1 - P(\pi))$$

To stabilize the calculation, a logarithmic form is also applied:

$$w_{uv} = -\ln p_{uv} \ (\geq 0), \text{ shunda } \arg\max P(\pi) \equiv \arg\min \sum w_{uv}$$

(“Finding the “most probable path” is done using the Dijkstra algorithm).

3) Calculation of Damage (Impact).

If node v is compromised, the impact is given as the aggregate (cumulative) damage of the documents D_v that are associated with or can be accessed via v:

$$I_v = \sum_{d \in D_v} C_d$$

If documents can be accessed through multiple nodes, to avoid double counting, a document-centric accounting approach is used (for example, applying the “first accessed node” rule for each document or using submodular aggregation).

4) Kutilayotgan zarar (Expected Loss).

When spreading from the initial source, the expected total damage across the entire network is:

$$\mathbb{E}[\text{Zarar}] = \sum_{v \in V} q_v I_v.$$

If a more precise calculation is required at the document level:

$$\mathbb{E}[\text{Zarar}] = \sum_d \Pr\{\text{d hujjat ochiladi}\} C_d,$$

Here, Pr{document d is accessed} represents the combination of the probabilities of reaching the nodes that can provide access to the document (for example, for OR-logic)

$$1 - \prod_{v \in \mathcal{V}(d)} (1 - q_v))$$

5) Criticality (Risk/Criticality) Criterion.

The main criterion used in the article: Criticality = Probability × Damage.

Path-based evaluation:

$$\mathrm{Crit}\,(\pi) = P\,(\pi) \times \left(\sum_{v \in \pi} I_v \right),$$

Global assessment across the network:

$$\mathrm{Crit}_{\mathrm{global}} = \mathbb{E}\,[\mathrm{Zarar}] = \sum_{v \in V} q_{v I_v}.$$

6) Sorting and prioritization.

The most probable path.: $\pi^{\star} = \arg\max_{\pi} P\,(\pi).$

The most damaging path: $\pi^{\diamond} = \arg\max_{\pi} \sum_{v \in \pi} I_v.$

The most critical path: $\pi^{\dagger} = \arg\max_{\pi} \mathrm{Crit}\,(\pi) = \arg\max_{\pi} \left[P\,(\pi) \cdot \sum_{v \in \pi} I_v \right].$

Practical rule: relying only on probability (π^{*}) often underestimates the risk; the criticality criterion, however, also identifies paths that are less probable but potentially highly damaging.

If you wish, I can also create a small sample graph (with 2–3 paths and 4–5 nodes) and prepare a step-by-step calculation table based on these formulas, formatted in Word.

Dijkstra and Bellman–Ford algorithms for determining the most probable path. In the assessment of social engineering attacks, the probability of propagation from one user to another is represented as a graph. A success probability is assigned to each edge, and based on these probabilities it is necessary to determine the path by which an attacker can most easily reach the target. For this purpose, the Dijkstra and Bellman–Ford algorithms can be used.

The Dijkstra algorithm is typically applied to find the shortest path in graphs with nonnegative weights. When analyzing probabilities for social engineering attacks, the weight of each edge is taken as the negative logarithm of the attack probability. As a result, paths with higher probabilities become the “shortest paths.” Using this approach, the attacker’s most probable path can be computed quickly and efficiently.

The Bellman–Ford algorithm, on the other hand, can be applied to graphs that allow negative weights and provides a more flexible approach. It computes reachability to all nodes step by step, so it is appropriate for multi-stage attacks or when the graph structure is complex.

In general, while Dijkstra is faster in terms of performance, Bellman–Ford yields correct results under more complex conditions. Therefore, to determine the most probable path of a social engineering attack, these algorithms are used to process the user-to-user propagation probabilities and identify the attacker’s route to the target. This approach shows the organization which users or communication links are the weakest.

Selecting the most critical path using the expected-damage metric. In assessing social engineering attacks, not only the probability of an attack but also the potential damage it may cause are important. Some paths may have a high probability of success but relatively minor consequences; conversely, some less probable paths may cause substantial financial or informational losses. Therefore, relying solely on probability does not provide a complete picture when choosing the most dangerous path.

To address this, the expected-damage metric is applied. For each attack path, the attack probability (P) and the possible damage (C) are estimated, and the overall risk level is determined as their product:

$$\mathrm{Risk\ (Criticality)} = \mathrm{P} * \mathrm{C}$$

As a result, the most critical path is chosen as the path with the highest value according to this criterion. This approach more accurately reflects the organization’s actual risk because it takes into account not only the probability of an attack but also its consequences. Thus, when developing security policies, it becomes possible to identify the weakest points that demand the most resources and to prioritize attention to them.

RESULTS

To test the proposed approach in practice, a simple experiment was conducted. As an example, three users

and three documents of different criticality levels were considered. Each user's access rights to the documents and the probabilities of attack propagation via them were represented using a graph model. The documents were assigned different importance levels: one was rated as low-value, the second as medium-value, and the third as a high-value document that could cause significant damage if accessed.

The calculations showed that under a probability-only approach, the path with the highest probability is identified as the most dangerous. However, when the expected-damage criterion is applied, a path with a lower probability but which provides access to the highest-value document is selected as the most critical. This empirically confirms the necessity of accounting for damage magnitude alongside probability when assessing social engineering attacks.

The conclusion drawn is that, when developing security policies, organizations should consider not only frequently occurring attack paths but also less likely paths that may cause substantial harm. In this way resources can be allocated more effectively and attention focused on eliminating the most dangerous routes.

DISCUSSION

The main advantage of the proposed approach is that it accounts not only for attack probability but also for the expected damage when assessing attacks. This provides a clearer picture of actual risk and enables an organization to direct resources toward the weakest links. Such an approach is important for effective security policy planning, prioritised mitigation of the most dangerous attack paths, and improving overall security posture.

At the same time, the approach has certain limitations. In particular, accurately quantifying the value of documents in practice is a complex process, since it often depends on subjective factors. In addition, computing attack probabilities and expected damages in large-scale systems can require substantial computational resources.

In future research, to further refine the method, it is planned to account for hierarchical document structures, model complex information flows, and develop comprehensive risk-assessment systems. This will allow for deeper analysis of traces of social engineering attacks and the development of more effective protective measures against them.

CONCLUSION

Analyses show that relying solely on attack probability when assessing traces of social engineering attacks is insufficient, because in some cases low-probability paths can inflict very large damage. Therefore, a complete assessment of attacks requires jointly considering both probability and expected damage metrics. The proposed approach takes this into account and produces effective results for determining the criticality levels of attacks. This method enables organizations to plan security policies more precisely, prioritize resource allocation, and minimize real risks. Thus, in defending against social engineering attacks, not only technical measures but also scientifically grounded assessment approaches are important.

REFERENCES

1. Nuralievich, B. O., & Boltaevich, M. B. (2021, November). Method of Detection and Elimination of Tracks of Attacks in the Information System. In 2021 International Conference on Information Science and Communications Technologies (ICISCT) (pp. 1-2). IEEE.
2. Nuralievich, B. O., Boltaevich, M. B., & Ugli, B. U. B. (2022, September). The Procedure for Forming a List of Sources of Attack in the Information System. In 2022 International Conference on Information Science and Communications Technologies (ICISCT) (pp. 1-4). IEEE.
3. Bekmirzaev O., Shirinov B. An Algorithm for Viewing Node State Events Under Attack for Information Systems // AIP Conference Proceedings., 2024, 3147(1), 050003. DOI: 10.1063/5.0210404
4. Bekmirzaev O., Samarov H. A Method of Evaluating the Effectiveness of Information System Protection // AIP Conference Proceedings., 2024, 3147(1), 050004. DOI: 10.1063/5.0210405
5. Muminov, B., & Bekmirzaev, O. (2022). Structure and algorithms of online discussion information system. Scientific Collection «InterConf», (114), 373-384.
6. Мўминов, Б., & Бекмирзаев, О. (2022). Построение узлов о событиях под влиянием атаки в информационной системе. Scientific Collection «InterConf», (114), 388-396.
7. Bekmurodov, O. (2023). Ахборот тизимларида ҳужум манбалари рўйхатини шакллантириш процедураси. Digital Transformation and Artificial Intelligence, 1(3), 129-136.
8. Samarov, H. K., & Bekmirzayev, O. N. (2023). Masofaviy o'qitish tizimlarida mavjud risklar va ularni minimallashtirish istiqbollari. Research and Education, 2(4), 146-155.
9. Bekmirzayeva, M. (2024). Vizuallashtirish tizimlarida yomg'ir va qor muammolarini tasvirga dastlabgi ishlov berish yordamida bartaraf etish.

Digital Transformation and Artificial Intelligence, 2(1), 120-124.

10. Bekmirzayev, O., & Sabirov, X. (2023). “Kompyuter arxitekturasi” fanini o ‘qitish samaradorligini oshirishda zamonaviy pedagogik texnologiyalarning interfaol usullaridan foydalanish. Science and Innovation, 2 (Special Issue 14), 549-551.
11. Muminov, B., Bekmirzaev, O., & Al-Khwarizmi, M. (2022). Classification and analysis of network attacks in the category of “denial of service” information system. central asian journal of education and computer sciences (CAJECS), 1, 7-15.
12. Бекмирзаев О., Турсунов Ж. Алгоритмы системы одностороннего межсетевого взаимодействия и система обнаружения вторжений //Digital Transformation and Artificial Intelligence. – 2023. – Т. 1. – №. 4. – С. 135-145.
13. Axmedova, N., & Bekmirzaev, O. (2022). Analysis of methods of fighting against network attacks of the “denial of service” category on information systems. central asian journal of education and computer sciences (CAJECS), 1, 5.
14. Bekmirzayev, O., & Muminov, B. (2024). The Role and Application of Artificial Intelligence in Identifying Threats to Information Systems. DTAI–2024, 1(DTAI), 85-90.
15. Bekmirzayev, O. (2024). Algorithm for Constructing and Configuring Parameters of a Model for Searching for Traces of Attacks in an Information System. DTAI–2024, 1(DTAI), 171-174.
16. Bekmurodov, O., Usmanbayev, D., & Eshonqulov, N. Z. (2024). Kompyuter tarmoqlarini ddos hujumlaridan himoya qiluvchi dasturiy vositalarning qiyosiy tahlili. Digital Transformation and Artificial Intelligence, 2(2), 46-50.
17. Bekmirzayev, O., & Kumushbibi, G. U. (2024). Korxona tizimlarda ma’lumotlarni saqlash va uzatishda foydalanuvchi maxfiyligi. Digital Transformation and Artificial Intelligence, 2(6), 207-213.
18. Bekmirzayev, O. N., & Bekmirzayeva, M. S. (2016). Recognize faces by the selecting degree of security. In Информатика: проблемы, методология, технологии (pp. 3-7).
19. Ташев, К. А., & Бекмирзаев, О. Н. (2015). К вопросу анализа проблем информационной безопасности. In Информатика: проблемы, методология, технологии (pp. 211-214).
20. Турапов, У. У., & Бекмирзаев, О. Н. (2015). Системный подход при обеспечении информационной безопасности в информационно-библиотечных сетях. In Информатика: проблемы, методология, технологии (pp. 219-224).
21. Beknazarova, S., & Bekmirzaeva, M. (2024). Analysis of Filters for Processing Video Images. DTAI–2024, 1(DTAI), 224-227.
22. Safibullaevna, B. S., Qizi, J. M. K., Shaimardanova, B. M., & Erkinovna, A. M. (2020). Adaptive Method For Eliminating Noise Of Image. The American Journal of Engineering and Technology, 2(12), 59-66.
23. Islomov, S. Z., Bekmirzayev, O. N., Shodmonova, X., & Karimov, A. A. (2017). Threats and protection ways of mobile networks. In Информатика: проблемы, методология, технологии (pp. 213-216).
24. Bekmirzayeva M., Norqulova Z., Bekmirzayev O. Yomg‘ir izlarini olib tashlash algoritmlari tahlili //DIGITAL TRANSFORMATION AND ARTIFICIAL INTELLIGENCE. – 2025. – Т. 3. – №. 3. – С. 26-32.
25. Bekmirzaev O., Gulomova K., Mukhamadiev S. Research on New Trends and Development Prospects of Enterprise Resource Planning (ERP) Systems //European International Journal of Multidisciplinary Research and Management Studies. – 2025. – Т. 5. – №. 03. – С. 50-54.
26. Boltaevich M. B., Nuralievich B. O. STRUCTURE AND ALGORITHMS OF ONLINE DISCUSSION INFORMATION SYSTEM //EDITOR COORDINATOR. – С. 373.
27. Bekmirzaeva M., Bekmirzaev O. Methods of visual quality improvement of images and the video under adverse weather conditions //AIP Conference Proceedings. – AIP Publishing LLC, 2025. – Т. 3377. – №. 1. – С. 060001.
28. Bekmirzayeva M. S. Removing rain tracks from images using image processing algorithms //Sun’iy Intellekt Nazariyasi va Amaliyoti: Tajribalar, Muammolar va Istiqbollari. – 2024. – С. 272-278.
29. Beknazarova S. S., Bekmirzayeva M. S. Study of the Degree of Influence of Fog on Images in Visualization Systems. – 2024.