An Empirical Analysis of Phishing Simulation to Mitigate Social Engineering Attacks

Adilet Abdykerimov *, Ruslan Isaev, Ruslan Amanov

Posted Date: 24 November 2025

doi: 10.20944/preprints202511.1827.v1

Keywords:

phishing simulation; social engineering; email-based attacks; employee susceptibility; phishing; cybersecurity awareness; open-source tools; information security training

 doi:10.20944/preprints202511.1827.v1

Article

An Empirical Analysis of Phishing Simulation to Mitigate Social Engineering Attacks

Adilet Abdykerimov [1,*], Ruslan Isaev [2] and Ruslan Amanov [1]

[1] Faculty of Engineering and Informatics, Ala-Too International University, Bishkek, Kyrgyzstan
[2] Faculty of ICT, Paragon International University, Phmom Penh, Cambodia
* Correspondence: adilet.abdykerimov@alatoo.edu.kg

Abstract

Phishing remains one of the most prevalent and damaging forms of cyberattacks, exploiting human behavior rather than technical vulnerabilities. Despite technological advancements in email filtering, anomaly detection, and two-factor authentication, phishing continues to succeed by manipulating trust, authority, and urgency cues in unsuspecting users [1,5,14]. This study presents an empirical analysis of a phishing simulation conducted in a university setting to assess user susceptibility and promote security awareness. A simulated phishing email was sent to 35 staff members, with 80% opening the message and 40% clicking the embedded link. Behavioral responses—such as fear of reprimand and avoidance—indicated cultural and psychological barriers to effective awareness [4,9,18]. In addition to field experimentation, a technical comparison of open-source phishing tools—GoPhish, King Phisher, Phishery, and Evilginx2 — was conducted to evaluate their practicality, usability, and deployment complexity [7,11,13]. Drawing on recent literature in cybersecurity education and behavioral science, this paper highlights the need for psychologically safe, culturally sensitive, and role-specific training to reduce long-term phishing risk [3,6,8,12,17]. Our findings support the integration of simulated phishing campaigns with structured, non-punitive feedback and adaptive educational interventions to foster more resilient digital behavior.

Keywords: phishing simulation; social engineering; email-based attacks; employee susceptibility; phishing; cybersecurity awareness; open-source tools; information security training

1. Introduction

Phishing attacks are among the most enduring threats in the cybersecurity landscape, accounting for a large%age of breaches in both private and public sectors [1,18]. Unlike malware or system-based exploits, phishing operates through psychological manipulation, deceiving users into revealing credentials, clicking malicious links, or downloading harmful attachments. The sophistication of modern phishing campaigns—including AI-generated emails and advanced spoofing techniques—makes them particularly difficult to detect, even by experienced users [13,15].

While technical controls such as spam filters, browser warnings, and authentication systems provide baseline defense, they cannot eliminate the human factor. Studies show that users often ignore security cues under pressure or when influenced by authority or emotional appeals [5,6,9]. Parsons et al. [5] and Burda et al. [9] highlight that phishing susceptibility is often tied to cognitive overload, poor training design, or organizational fear culture—where users are afraid to report mistakes.

In this context, awareness programs and phishing simulations have become essential components of cyberdefense. When conducted correctly, simulations do more than test vulnerability—they act as learning tools, helping users recognize threat patterns and reinforcing good security habits [3,4,10]. However, simulations can also backfire if they induce shame or punishment, especially in cultures with hierarchical structures or low digital literacy [17,20].

This paper presents an empirical case study from Ala-Too International University (AIU), where a phishing simulation was sent to 35 staff members using the GoPhish platform. Alongside the

 doi:10.20944/preprints202511.1827.v1

behavioral results, we compare four popular open-source tools for phishing training and analyze how different technical and educational strategies intersect. Drawing from the cybersecurity literature—including work on social engineering cognition [9], deception-based defenses [12], and machine learning detection [2,8] — this paper argues for an integrated, human-centered approach to phishing mitigation that accounts for both technical efficacy and emotional safety.

2. Literature Review

Phishing attacks have evolved from simplistic mass emails to highly targeted, sophisticated campaigns that exploit both technical loopholes and psychological weaknesses. The literature reveals a multifaceted challenge that requires both technological innovation and behavioral intervention.

2.1. The Psychological and Behavioral Dimensions of Phishing

Human behavior plays a central role in the susceptibility to phishing. Several studies emphasize that most successful attacks are not the result of advanced malware, but rather clever manipulation of user trust, urgency, and authority.

Hong [1] laid the foundation for understanding the psychology of phishing, illustrating how deceptive email cues influence user decision-making. Based on this, Parsons et al. [5] conducted scenario-based experiments and found that participants often clicked on phishing links despite having basic awareness, due to cognitive overload and task-switching errors.

Burda et al. [9] performed a large-scale review of empirical social engineering studies and identified three major psychological factors behind the susceptibility to phishing: fear of authority, lack of cybersecurity culture, and emotional urgency. Pfleeger and Caputo [6] argue that cybersecurity awareness must be reframed using behavioral science principles, with training programs tailored to actual user behavior rather than theoretical risks.

2.2. The Role of Training and Awareness Programs

Awareness campaigns have become a cornerstone of phishing prevention. Chatchalermpun et al. [3] and Carroll et al. [18] show that regular training, especially when gamified or role-specific, reduces click-through rates in simulations by up to 40

However, Carroll et al. [18] highlight that even trained users are susceptible to well-crafted messages, especially when emotional triggers are used. Jackson [8] suggests integrating training with real-time behavioral monitoring to personalize interventions. Additionally, Jumalieva [20] argues that digital literacy and information security must be built into broader public sector transformation strategies in regions like Kyrgyzstan. Modern social-engineering attacks, including advanced phishing, can be formally modeled using game theory and probabilistic decision trees [21]. In Central Asian universities, phishing remains the most commonly exploited vulnerability according to local security surveys [22]. Machine-learning models originally developed for urban resilience monitoring are increasingly repurposed for real-time phishing detection [23]. Hybrid detection approaches combining permission analysis with user-behavior profiling show promise for evaluating phishing-training effectiveness [24]. CTF competitions organized for Kyrgyz schoolchildren in 2024 significantly improved participants' ability to identify phishing attempts [26]. Non-punitive, simulation-based training is particularly effective in educational settings, where fear of punishment otherwise discourages reporting [25].

Yet, not all training programs succeed. According to Eshetu et al. [17], cultural context, language barriers, and institutional fear of punishment often reduce participation in simulations.

2.3. Phishing Simulations and User Behavior Studies

Phishing simulations are widely used to test user behavior and deliver "teachable moments." Doe et al. [4] and Montañez Rodriguez and Xu [10] present simulation frameworks that record user interaction with phishing emails to understand patterns.

In the case of Ala-Too International University, a real-world simulation found that 80% of staff opened a phishing email, and 40% clicked the link. Only 3 participants completed the post-simulation

 doi:10.20944/preprints202511.1827.v1

survey. These findings echo those in Parsons et al. [5], showing that even low-stakes scenarios trigger avoidance and fear, especially where organizational cultures are perceived as punitive.

Burda et al. [9] emphasize the need for "psychological safety" in training environments, where users feel they can make and learn from mistakes without consequence.

2.4. Open-Source Tools for Phishing Simulation

Several open-source tools are available to support phishing simulation: GoPhish is frequently cited as the most accessible, especially for educational use [7]. King Phisher offers comprehensive features but has a steep installation curve [11]. Phishery is lightweight and fast, ideal for document-based payload generation [7]. Evilginx2 is more suited for red-team simulations involving token interception and 2FA bypass [13]. Gokkaya et al. [7] provide a broader review of security tooling challenges in open-source environments, including the importance of secure defaults and proper documentation.

2.5. Summary

Finally, national-level strategies play a role in shaping phishing defense. The Kyrgyz Republic Cybersecurity Strategy [19] outlines several strategic priorities, including incident response, digital literacy, and regulatory support. Jumalieva [20] adds that fostering public trust is essential to any transformation involving user data and government digital services. The literature strongly supports a multi-layered phishing defense strategy, combining:

- Continuous, behavior-driven training
- Real-world phishing simulations
- Use of open-source tools
- Cultural sensitivity and emotional safety Engagement at the Policy-level and public trust building

3. Methodology

This study used a mixed-methods research design that combined an empirical phishing simulation with a comparative technical analysis of open-source phishing tools. The goal was to evaluate both user susceptibility to phishing attacks and the practical utility of simulation platforms for training and awareness.

3.1. Phishing Simulation Design

To assess phishing awareness in a real-world setting, a simulated phishing campaign was conducted at Ala-Too International University targeting a sample group of 35 staff members, primarily administrative and academic support staff (guidance counselor). These individuals were selected because of their frequent interaction with digital communication systems, but relatively limited exposure to cybersecurity training.

The phishing email was crafted to appear official and credible, styled as an internal memo concerning "updated organizational guidelines." It included a phishing link leading to a fake login page hosted via the open-source GoPhish platform. No credentials were collected; instead, the system recorded whether emails were opened and whether links were clicked.

This method aligns with prior studies that have used realistic phishing simulations to evaluate user behavior in organizational contexts [4,5,10]. The decision to use GoPhish was based on its ease of deployment, robust tracking features, and suitability for educational environments [7,11].

3.2. Ethical Considerations and Participant Privacy

Participants were not informed in advance to maintain realism, but debriefing followed shortly after the campaign. A follow-up survey and informal interviews were conducted to assess emotional and cognitive reactions. These included questions about whether the participant identified the message as suspicious, how they reacted, and whether they felt comfortable reporting such messages in the future.

 doi:10.20944/preprints202511.1827.v1

This approach was influenced by the work of Burda et al. [9], who emphasize the importance of understanding user' emotional responses and the cultural dynamics of shame and fear in reporting cybersecurity incidents. Similarly, Pfleeger and Caputo [6] stress the need for psychologically safe environments when conducting behavior-based security research.

3.3. Tool Comparison Approach

In parallel, a technical review of four open-source phishing tools was performed to understand their potential for scalable, repeatable awareness training. The tools evaluated were:

- GoPhish
- King Phisher
- Phishery
- Evilginx2

Each tool was installed and tested in a virtual lab environment using Ubuntu Linux and Windows 10 systems. The evaluation criteria included the following: primary use, license, latest development activity (as per 2025), ease of use, template quality, campaign management capabilities, tracking and reporting granularity, ability to bypass two-factor authentication, scalability, community support, and most suitable application scenario Table 1.

Table 1. Comparison of Open-Source Phishing Frameworks.

Criterion	GoPhish	King Phisher	Phishery	Evilginx2
Primary use	Training campaigns	Multi-channel sim	Basic Auth harvest	2FA bypass (AiTM)
License	MIT	BSD-3	MIT	BSD-3 (core)
Latest activity (2025)	Active	Unmaintained†	Low	Active + Pro version
Ease of use	Very high	Medium	Medium	Medium–High
Template quality	High	High	Low	Medium (phishlets)
Campaign management	High	High	None	Medium (w/ GoPhish)
Tracking & reporting	High	Medium	Low	High (tokens/cookies)
2FA/MFA bypass	No	No	No	High
Scalability	High	High	Low	Medium
Community support	Very strong	Limited	Minimal	Strong + paid Pro
Best for	Awareness training	Flexible attacks	Word doc phishing	Advanced red-teaming

This process was informed by earlier reviews of open-source cybersecurity tools such as Gokkaya et al. [7] and Rahman et al. [11], who advocate for systematic, usability-focused assessments of open-source security platforms. Particular attention was paid to usability vs. power trade-offs, as King Phisher and Evilginx2 are known to offer advanced features but at the cost of installation complexity and learning curve [13,15].

The comparative results were recorded in structured tables to highlight differences and support implementation decisions in low-resource environments.

3.4. Data Collection and Analysis

For the phishing simulation:

- Data collected included email open rates, link click-through rates, and survey responses.
- Click and open events were timestamped and anonymized.
- Behavioral observations from informal interviews were coded thematically.

 doi:10.20944/preprints202511.1827.v1

For the tool comparison:

- Usability and functionality were scored using a 5-point Likert scale.
- Screenshots and logs were used to document performance and bugs.

This mixed-methods design allows for triangulation of findings—linking quantitative metrics (click rates, usability scores) with qualitative insights (emotional reactions, tool deployment experience). This follows a framework similar to that proposed by Montañez Rodriguez and Xu [10], who advocate a cyber kill-chain approach to map social engineering attack stages and defense strategies.

3.5. Limitations

Several limitations are acknowledged:

- The small sample size (35 users) may not be statistically generalizable.
- Self-report bias could affect the accuracy of the survey responses.
- Tool evaluations were subjective, although multiple testers were involved to reduce individual bias.

Nevertheless, the study offers valuable insights into real-world user behavior and tool viability, especially in contexts where technical capacity is limited, and organizational cybersecurity culture is still maturing [17,20].

4. Case Insight: Phishing Awareness Exercise at Ala-Too International University

To better understand how staff respond to real phishing threats, a phishing simulation was conducted at Ala-Too International University in Bishkek. This case provides practical insight into user behavior, emotional reactions, and institutional readiness to handle social engineering risks. The simulation was not only a means of testing security awareness but also a way to assess deeper cultural and psychological dynamics that influence digital risk response.

A total of 35 staff members (primarily methodists and administrative support staff) were selected to participate without prior notice. The phishing email was crafted to look like an official internal message requesting recipients to review "urgent updated guidelines" from university leadership. It included a link to a spoofed login page, hosted using the open-source platform GoPhish.

The results of the simulation were concerning but illuminating:

- 80% of recipients opened the email, indicating low initial suspicion.
- 40% clicked the phishing link, demonstrating significant vulnerability to deception.

Only 3 out of 35 participants completed a follow-up survey voluntarily. These findings echo those of Doe et al. [4], who observed similarly high engagement with phishing content in academic institutions and emphasized the persistent lack of training despite frequent digital communication. Parsons et al. [5] also note that users often default to trusting internal-looking emails, especially when they carry a sense of urgency or come from perceived authority figures.

Following the campaign, several staff members were approached individually for informal debriefings. Surprisingly, many displayed discomfort, anxiety, and even defensiveness upon learning the email had been a test. A few outright denied receiving the email or claimed they hadn't interacted with it—despite the logged data showing otherwise. Some expressed fear that the results might affect their job security or reputation.

This emotional response reveals more than a lack of technical awareness—it reflects organizational culture. Burda et al. [9] found that in environments where authority is strict and transparency is low, users are more likely to hide mistakes or avoid participation in security-related activities. Similarly, Pfleeger and Caputo [6] emphasize that employees will not engage openly with cybersecurity programs if they feel they are being judged or punished.

Fear-based responses severely limit the effectiveness of phishing awareness campaigns. Instead of opening a dialogue or learning opportunity, the simulation risked reinforcing silence and shame.

 doi:10.20944/preprints202511.1827.v1

Carroll et al. [18] highlight that simulations should be used to educate without blame, or they risk losing the trust of participants.

The outcome also reflects broader cultural and institutional norms in educational environments within Central Asia. Jumalieva [20] points out that digital transformation in public and educational institutions in Kyrgyzstan often faces resistance due to generational divides, low digital literacy, and unclear data privacy norms. In such environments, users may be reluctant to question emails or speak up—even when something feels suspicious.

Moreover, Eshetu et al. [17] found in a similar university setting that fear of being wrong is a bigger obstacle than lack of knowledge. This implies that even basic training programs may fail if they do not address trust, transparency, and emotional safety.

The AIU simulation provided critical insight into both the technical vulnerability and the human factors involved in social engineering risks. Based on the results and observed behavior, the following recommendations were made:

- Offer short, repeatable training sessions (15–20 minutes) focused on specific types of attacks and how to respond without judgment.
- Create a clearly communicated non-punitive policy for reporting suspicious emails or falling victim to phishing—this is key to building trust [6,9].
- Use visual awareness tools like posters, infographics, and checklists (e.g., "Think Before You Click") displayed in staff rooms and offices.
- Introduce monthly micro-quizzes or simulated challenges to build habit strength and reinforce learning over time [3,10,18].
- Establish leadership participation in awareness efforts to demonstrate top-down support, as recommended by Chatchalermpun et al. [3].

By grounding future phishing training in empathy, behavioral science, and consistent reinforcement, the university can shift from a reactive to a proactive posture. The key takeaway from this case is that human trust is as critical as technical defense, and security programs must prioritize culture as much as code.

5. Comparative Review of Open-Source Phishing Simulation Tools

To assist with practical deployment, a comparative review of widely used open-source phishing tools was conducted. The tools were evaluated based on usability, features, and educational value.

GoPhish was found to be the most practical tool for education and awareness due to its intuitive interface and rich documentation. Phishery provides a fast way to create phishing documents, though it lacks automation or email sending capabilities. Evilginx2 offers powerful MITM-based capabilities but is challenging for novice users. King Phisher supports full tracking and credential capture but has high installation requirements.

6. Conclusions

Phishing remains a persistent and evolving threat in cybersecurity, not because of technical complexity, but due to its psychological and social nature. This study, grounded in both field experimentation and literature review, demonstrates that defending against phishing attacks requires more than filters, firewalls, or sophisticated software—it requires understanding human behavior, institutional culture, and the emotional context of digital decision-making.

The phishing simulation conducted at Ala-Too International University revealed a high level of vulnerability among non-technical staff: 80% of recipients opened the phishing email and 40% clicked on the malicious link. These results are consistent with prior findings that even well-educated professionals are susceptible to phishing when messages appear urgent or authoritative [5,18]. More critically, participants' emotional reactions—including fear, avoidance, and denial—highlight deeper institutional challenges. As Burda et al. [9] and Pfleeger and Caputo [6] argue, training alone is ineffective if it is delivered in environments where users feel judged or unsafe.

 doi:10.20944/preprints202511.1827.v1

From a tool implementation perspective, the comparative review of open-source phishing platforms such as GoPhish, King Phisher, Phishery, and Evilginx2 reinforces that usability and accessibility are just as important as feature richness. While tools like Evilginx2 offer advanced capabilities for credential harvesting and reverse proxy attacks, they are not practical for educational institutions without strong technical support. On the other hand, tools like GoPhish offer an ideal balance of functionality and simplicity, especially for repeated awareness simulations [7,11,13].

This paper also emphasizes the need for a multi-layered approach to phishing defense. Based on the literature reviewed, effective mitigation combines technical tools, behavioral training, policy support, and a shift in organizational culture [1,3,4,9,17]. For instance, Chatchalermpun et al. [3] and Jackson [8] both recommend regular, scenario-based simulations, but they caution that engagement levels will remain low unless users feel emotionally safe and culturally supported.

Furthermore, emerging threats from AI-generated phishing attacks are poised to increase the complexity of detection. Studies by Eze and Shamir [13] and Schmitt and Flechais [15] suggest that phishing emails can now be personalized using AI to bypass both user awareness and technical filters. This growing sophistication means that future defense strategies must go beyond education and embrace adaptive, AI-aware defense mechanisms, potentially combining deception technologies and real-time behavioral analytics [12,16]. The findings of this study call for immediate and long-term action at multiple levels:

- Educational institutions should implement non-punitive, role-specific training supported by leadership.
- Organizations should integrate open-source tools that balance functionality with ease of use.
- Policy makers should promote digital literacy and develop supportive cybersecurity frameworks like those found in the Kyrgyz Republic's national strategy [19,20].

In conclusion, phishing resilience is not achieved solely through technology or policy, but through empathy, education, and empowerment. Cultivating a security-aware culture—where users are confident, informed, and unafraid to ask questions—is one of the most powerful defenses against social engineering in the digital age.

References

1. K. Hong, "Understanding phishing attacks and their countermeasures," Journal of Network and Computer Applications, vol. 107, pp. 146-157, 2018.
2. P. Bhavsar and A. Shah, "Phishing attack detection using machine learning techniques," International Journal of Computer Applications, vol. 182, no. 46, pp. 25-30, 2018.
3. T. Chatchalermpun et al., "Phishing awareness and educational interventions," IOP Conference Series: Materials Science and Engineering, vol. 1088, no. 1, 2021.
4. J. Doe et al., "Phishing simulation experiments and user behavior analysis," Cybersecurity Research Journal, vol. 15, no. 3, pp. 223-239, 2022.
5. K. Parsons, A. McCormac, M. Pattinson, M. Butavicius, and C. Jerram, "Phishing for the truth: A scenario-based experiment of users' behavioural response to emails," 28th IFIP International Conference on Information Security and Privacy Protection (IFIP SEC), vol. 405, pp. 366–378, 2013.
6. S. L. Pfleeger and D. D. Caputo, "Leveraging behavioral science to mitigate cyber security risk," Computers & Security, vol. 31, no. 4, pp. 597–611, 2012.
7. B. Gokkaya, L. Aniello, and B. Halak, "Software supply chain: review of attacks, risk assessment strategies and security controls," CoRR, vol. abs/2305.14157, 2023.
8. K. A. Jackson, "A systematic review of machine learning enabled phishing," Master's thesis, Heinz College of Information Systems and Public Policy, Carnegie Mellon University, 2022.
9. P. Burda, L. Allodi, and N. Zannone, "Cognition in social engineering empirical research: A systematic literature review," ACM Transactions on Computer-Human Interaction, vol. 31, no. 2, Article 19, pp. 1–55, 2024.
10. R. Montañez Rodriguez and S. Xu, "Cyber social engineering kill chain," Lecture Notes in Computer Science: Proceedings of the 4th International Conference on Science of Cyber Security (SciSec 2022), vol. 13551, pp. 487–504, 2022

 doi:10.20944/preprints202511.1827.v1

11. A. Rahman, S. I. Shamim, D. B. Bose, and R. Pandita, "Security misconfigurations in open source Kubernetes manifests: An empirical study," ACM Transactions on Software Engineering and Methodology, vol. 32, no. 4, Article 99, pp. 1–36, 2023
12. S. Seo and D. Kim, "SOD2G: A study on a social-engineering organizational defensive deception game framework through optimization of spatiotemporal MTD and decoy conflict," Electronics, vol. 10, no. 23, article 3012, pp. 1–23, 2021.
13. C. S. Eze and L. Shamir, "Analysis and prevention of AI-based phishing email attacks," Electronics, vol. 13, no. 10, article 1839, pp. 1–19, 2024.
14. Y. Zhang, S. Egelman, L. Cranor, and J. Hong, "Phinding Phish: Evaluating anti-phishing tools," Proceedings of the 14th Annual Network and Distributed System Security Symposium (NDSS 2007), 2007.
15. M. Schmitt and I. Flechais, "Digital deception: generative artificial intelligence in social engineering and phishing," Artificial Intelligence Review, vol. 57, article 324, 2024.
16. T. Riebe, J. Bäumler, M.-A. Kaufhold, and C. Reuter, "Values and value conflicts in the context of OSINT technologies for cybersecurity incident response: A value sensitive design perspective," Computer Supported Cooperative Work (CSCW), vol. 33, pp. 205–251, 2024.
17. A. Y. Eshetu, E. A. Mohammed, and A. O. Salau, "Cybersecurity vulnerabilities and solutions in Ethiopian university websites," Journal of Big Data, vol. 11, article 118, 2024.
18. F. Carroll, J. A. Adejobi, and R. Montasari, "How good are we at detecting a phishing attack? Investigating the evolving phishing attack email and why it continues to successfully deceive society," SN Computer Science, vol. 3, article 170, 2022.
19. Ministry of Justice of Kyrgyz Republic, "Kyrgyz Republic Cybersecurity Strategy," https://cbd.minjust.gov.kg/15479/edition/962966/ru.
20. Cholpon Jumalieva, "Improving the Digital Transformation in the Sphere of Public Administration and Ensuring Information Security," Alatoo Academic Studies., vol. 23, 2023.
21. Alrantisi, K. M., "Social Engineering in Cybersecurity: Attack Modes, Mathematical Foundations, and Algorithmic Defenses," 2025.
22. Gulbarga, M. I., "Digital security threats and vulnerabilities," *Alatoo Academic Studies*, no. 4, pp. 344–354, 2021, doi: 10.17015/aas.2021.214.40.
23. Gulbarga, M. I. and Alrantisi, K. M., "Machine Learning Techniques for Urban Resilience: A Systematic Review and Future Directions," 2025.
24. Gulzada, E., Younes, E. D. A. F., and Khan, M. T., "Detecting Malware Applications through a Hybrid Approach: Permission Profiling and User Experience Analysis," 2025.
25. Esenalieva, G. A., "Cyber security in the education system,"*Alatoo Academic Studies*, no. 1, pp. 167–171, 2022, doi: 10.17015/aas.2022.221.21.
26. Amanov, R. K., Isaev, R. R., Ermakov, A. V., Esenalieva, G. A., and Davletshin, A. D., "Organization and analysis of a cybersecurity olympiad in CTF format for schoolchildren of Kyrgyzstan," in *Avtomatizatsiya, telekommunikatsii, informatsionnye tekhnologii i programmnoye obespecheniye 2024 (ATITS 2024): Materialy mezhdunarodnoy nauchno-prakticheskoy konferentsii* [Automation, telecommunications, information technologies and software 2024 (ATITS 2024): Proceedings of the international scientific-practical conference], Yalta, 24–27 September 2024, Simferopol: V. I. Vernadsky Crimean Federal University, p. 65, 2024.– EDN KAGNAA.