“Social engineering in the international HR context: digital influence mechanisms, ethics, and intervention typology”

AUTHORS	Iryna Varis Oleksiy Subochev Oleh Voloboiev
ARTICLE INFO	Iryna Varis, Oleksiy Subochev and Oleh Voloboiev (2025). Social engineering in the international HR context: digital influence mechanisms, ethics, and intervention typology. *Social and labour relations: theory and practice*, *15*(1), 45-62. doi:10.21511/slrtp.15(1).2025.04
DOI	http://dx.doi.org/10.21511/slrtp.15(1).2025.04
RELEASED ON	Wednesday, 12 November 2025
RECEIVED ON	Wednesday, 16 July 2025
ACCEPTED ON	Wednesday, 15 October 2025
LICENSE	This work is licensed under a Creative Commons Attribution 4.0 International License
JOURNAL	"Social and labour relations: theory and practice"
ISSN PRINT	2410-4752
ISSN ONLINE	2415-3389
PUBLISHER	LLC “Consulting Publishing Company “Business Perspectives”
FOUNDER	State Higher Educational Establishment "Kyiv National Economic University named after Vadym Hetman", Social and Labour Relations Institute

NUMBER OF REFERENCES	NUMBER OF FIGURES	NUMBER OF TABLES
55	0	3

Iryna Varis (Ukraine), **Oleksiy Subochev** (Ukraine), **Oleh Voloboiev** (Ukraine)

SOCIAL ENGINEERING IN THE INTERNATIONAL HR CONTEXT: DIGITAL INFLUENCE MECHANISMS, ETHICS, AND INTERVENTION TYPOLOGY

Abstract

The digital transformation of human resource management has intensified interest in social engineering to influence employee behavior within HR practices. The relevance of this study arises from the need to systematize the forms of such influence, particularly in the context of the growing use of digital technologies that increasingly perform behavioral and regulatory functions. The article aims to develop a systematic approach to analyzing social engineering in HR management by proposing an original typology of targeted influence forms, exploring digital implementation mechanisms, and identifying ethical boundaries for such interventions. The object of the study is social engineering practices in human resource management systems. The methodological framework integrates an interdisciplinary approach, content analysis, theologization, and critical evaluation of ethical criteria for influence. As a result of the study, a five-component typology of social engineering in HR (cognitive-behavioral, emotional, normative-cultural, communicative, and organizational-structural vectors) is proposed, and digital influence tools are systematized. Four key ethical criteria were also identified for assessing the acceptability of such interventions. The practical value of the study lies in the potential to apply its results in developing ethical HR policies, implementing behavioral audit tools, and fostering a culture of digital security within organizations. HR professionals can use the proposed typology to design adaptive strategies that balance influence effectiveness with employee autonomy preservation.

Keywords social engineering, HR management, digital transformation, behavioral influence, ethical boundaries, organizational culture, cognitive mechanisms, digital HR technologies

JEL Classification M12, D91, O33

І. О. Варіс (Україна), **О. В. Субочев** (Україна), **О. А. Волобоєв** (Україна)

СОЦІАЛЬНИЙ ІНЖИНІРИНГ У МІЖНАРОДНОМУ HR КОНТЕКСТІ: ЦИФРОВІ МЕХАНІЗМИ ВПЛИВУ, ЕТИКА ТА ТИПОЛОГІЯ ІНТЕРВЕНЦІЙ

Анотація

Цифрова трансформація управління персоналом зумовила зростання інтересу до соціального інжинірингу як інструменту впливу на поведінку працівників у межах HR практик. Актуальність дослідження визначається потребою у систематизації форм такого впливу, зокрема в умовах поширення цифрових технологій, які дедалі частіше виконують поведінкову та регулятивну функцію. Метою статті є формування системного підходу до аналізу соціального інжинірингу в HR менеджменті шляхом розроблення авторської типології форм цілеспрямованого впливу, дослідження цифрових механізмів їх реалізації та визначення етичних меж допустимості таких інтервенцій. Об'єктом дослідження виступають соціоінженерні впливи в системі управління персоналом. Методологічну базу становлять міждисциплінарний підхід, контент-аналіз, метод типологізації та критичний аналіз етичних критеріїв впливу. В результаті проведеного дослідження автори запропонували п'ятикомпонентну типологію соціального інжинірингу в HR (когнітивно-поведінковий, емоційний, нормативно-культурний, комунікативний, організаційно-структурний вектори), систематизували цифрові інструменти впливу, а також виокремили чотири ключові етичні критерії для оцінювання допустимості таких втручань. Практична цінність дослідження полягає в можливості застосування результатів для розроблення політик етичного управління персоналом, впровадження інструментів поведінкового аудиту та формування культури цифрової безпеки в організаціях. Запропоновану типологію можна використати для побудови адаптивних HR стратегій з урахуванням балансу між ефективністю впливу й збереженням автономії працівника.

Ключові слова соціальний інжиніринг, HR менеджмент, цифрова трансформація, поведінковий вплив, етичні межі, організаційна культура, когнітивні механізми, цифрові HR технології

Класифікація JEL M12, D91, O33

BUSINESS PERSPECTIVES

Publisher

LLC "CPC "Business Perspectives"
Hryhorii Skovoroda lane, 10, Sumy,
40022, Ukraine

www.businessperspectives.org

V. HETMAN KNEU

Founder

State Higher Educational Establishment
"Kyiv National Economic University
named after Vadym Hetman",
Prospect Peremogy, 54/1, Kyiv,
03057, Ukraine

https://kneu.edu.ua/

Type of the article: Research Article

Received on: 16th of July, 2025
Accepted on: 15th of October, 2025
Published on: 12th of November, 2025

Iryna Varis, Ph.D. in Economics, Associate Professor, Kyiv National Economic University named after Vadym Hetman, Ukraine.

Oleksiy Subochev, Ph.D. in Economics, Associate Professor, Kyiv National Economic University named after Vadym Hetman, Ukraine.

Oleh Voloboiev, Applicant of the Educational Program «International Economics», Kyiv National Economic University named after Vadym Hetman, Ukraine.

Conflict of interest statement:
Author(s) reported no conflict of interest

http://dx.doi.org/10.21511/slrtp.15(1).2025.04

INTRODUCTION

The digital transformation of labor in the context of globalization fundamentally changes the nature of socio-labor relations. Automation of processes, the implementation of artificial intelligence, the spread of platform-based employment, and remote work formats transform not only the tools of personnel management but also the very nature of interaction between employee and employer. In this context, there is a growing tendency to use behavioral management strategies based on the analytics of digital footprints, employee experience management, and the application of soft influence mechanisms.

The phenomenon of social engineering – a systematic approach to designing and implementing mechanisms that influence employee behavior to achieve predictable outcomes in organizational activities - is becoming particularly relevant in this environment. In the modern HR context, social engineering goes beyond the narrow understanding of it as merely a tool for manipulation or informational intervention. Instead, social engineering increasingly manifests as an institutionally embedded practice through digital behavior assessment platforms, gamified motivation systems, algorithm-driven performance management, and behavioral indicators in HR analytics.

These processes emerge at the intersection of several scientific and practical fields - behavioral economics, social construction, digital management, and international economics. The concepts of choice and behavioral strategies, which are actively implemented in the personnel policies of multinational companies, aim to foster a culture of productivity, engagement, and loyalty with an emphasis on sustainable development, inclusivity, and digital flexibility.

On a global scale, social engineering is becoming not only a tool for influencing employees but also an element of economic competitiveness for countries and companies, as it enables effective management of human capital across transcultural teams, digital hubs, and virtual organizations. At the same time, there is a growing need for critical reflection on such strategies' potential social, ethical, and legal consequences.

Considering this, the study of social engineering as a contemporary tool of global HR management is highly relevant. It enables the analysis of recent transformations in personnel management approaches and the formulation of practical recommendations for balancing efficiency, ethics, and social responsibility in the context of the digital economy.

1. LITERATURE REVIEW

The study of social engineering in global HR management and behavioral economics is increasingly relevant in the context of digital transformation across all organizational processes. Ukrainian researchers have contributed significantly to its conceptual basis, emphasizing its role in cybersecurity, behavioral management, and the development of digital culture. Integrating behavioral economics, HR management, and information security, this interdisciplinary perspective highlights the need for a systematic review of recent Ukrainian research.

Bondarenko (2025) analyzes social engineering in modern scientific and media discourse, highlighting differences between academic and public interpretations. The author identifies key semantic markers – "manipulation," "cybercrime," and "information-psychological operation" and traces their relevance during the Russian-Ukrainian war, focusing on how cyber engineering and disinformation operate as parts of IPSO strategies. The study also emphasizes that social engineering historically evolved as an applied field for constructing technological social models.

Kudinova et al. (2023) view social engineering as a tool for shaping new social realities and managing societal processes. They outline its methodological principles and compare them with experimental economics, highlighting key conceptual differences in approaches to influencing the social environment.

http://dx.doi.org/10.21511/slrtp.15(1).2025.04

Yudin et al. (2021) examine social engineering as part of information warfare and influencing individual and collective consciousness. They substantiate their methods and use in digital environments for psychological impact, emphasizing the role of computer graphics, ICT, and international experience in applying these techniques and developing countermeasures.

Zhmurko (2024) sees social engineering as a key vector of modern cyberattacks that exploit the human factor to access information systems. The article systematizes phishing, vishing, and pretexting methods and analyzes their impact on business continuity and organizational security. The author stresses the need for a comprehensive response combining technical, managerial, and educational measures, including cybersecurity training and algorithms for detecting social attacks.

Maznyk and Drahan (2024) examine the role of cybersecurity specialists in developing HRM systems during digital transformation and rising cyber threats. The study highlights the need to integrate cybersecurity into personnel management, training, information protection, and compliance. The authors stress the importance of interdisciplinary training for security analysts, especially on social engineering, insider threats, digital ethics, and building a cybersecurity culture.

In examining the impact of digital transformation on global HR management and behavioral economics, Ohnivchuk (2024) highlights the human factor as a key vulnerability to social engineering. The author argues that purely technical measures are insufficient and supports practical training through realistic social engineering simulations. Similarly, Orel and Smahliuk (2023) stress the need for a comprehensive digital HR strategy. Ohnivchuk’s approach to training complements this by addressing human error and manipulation risks, making simulation programs essential for safeguarding HR processes, data security, and operational stability.

Petrova and Barash (2024) argue for rethinking HRM approaches in light of digital transformation, which changes employment structures, job nature, and behavioral models. They stress the growing need for ecosystem and human-centered strategies that address the socio-psychological impact of digital technologies and the risk of employees losing control over their professional future.

Chernyushkina et al. (2023) analyze principles for building strategic HR engineering amid digital transformation. They define the structure of HR strategy, its functional subsystems, and development stages, stressing the need for a Digital HR strategy that adapts to business changes. The authors also emphasize aligning HR strategy with digital challenges and anticipating internal and external shifts.

A review of foreign studies shows growing scientific interest in the ethical, behavioral, and security aspects of digital transformation, especially regarding AI, digital nudging, and social engineering. These works take an interdisciplinary approach, covering HR changes and cybersecurity, and offer conceptual models, frameworks, and practical solutions to strengthen ethics, transparency, and resilience in digital environments.

Dima et al. (2024) present a scoping review of 43 studies over 27 years on how AI affects HR activities and the roles of the HR triad (HR professionals, line managers, and employees). They summarize key areas of AI influence – from routine task automation to changes in the social aspects of work - and stress the need for all participants to adapt. The authors highlight research gaps, especially the lack of focus on interaction within the HR triad, and propose an integrative framework for future research.

Schmidt and Engelen (2020) present a systematic review of the ethical aspects of nudging - behavioral economics tools that influence choices without bans or coercion. They analyze arguments for and against nudging in terms of autonomy, transparency, well-being, and legitimacy, examining concepts like «manipulation», «paternalism», and «choice architecture». The authors stress that the ethical assessment of nudging depends largely on context, purpose, and implementation method.

Valta and Maier (2025) systematically reviewed 126 studies on digital nudging. They developed a taxonomy covering objectives, intervention types, digital environments, and user impact. They pay special attention to technical tools that shape online behavior, such as interface design, information structuring, and visual cues. The authors also highlight research gaps, including limited focus on ethics, long-term effects, and personalization, and suggest directions for future research.

Ruehle (2023) examines the moral permissibility of digital nudging in the workplace, distinguishing between justification and legitimization. The author emphasizes that even benevolent nudges must remain transparent, respect employee autonomy, and be accountable. This ethical framework helps prevent manipulation in digital HR practices.

Spiekermann and Winkler (2020) propose a value-oriented approach to developing digital technologies that embeds ethical principles into IT system design. Instead of merely following formal guidelines, they stress the need to consider values like dignity, autonomy, and justice at all stages of product creation.

Riso et al. (2022) investigate the ethical challenges of workplace digitalization, especially regarding artificial intelligence, employee monitoring, and algorithmic management. They emphasize the need for transparency, employee involvement in digital decision-making, and collective regulation to protect dignity and autonomy in the digital age.

Birthriya et al. (2024) comprehensively review social engineering attacks such as phishing, vishing, smishing, baiting, and pretexting. They classify these attacks by influence methods, distribution channels, and complexity, and analyze effective prevention strategies like user training, multi-factor authentication, and behavior monitoring. The authors emphasize that combining technical measures with greater user awareness is key to countering such threats.

Kolluri (2019) describes the concept of AI Sentry – a system that uses artificial intelligence to detect and neutralize social engineering attacks. Unlike static approaches, combining behavioral analysis, anomaly detection, and deception techniques creates a more adaptive and proactive cybersecurity model. The author emphasizes its potential to counter dynamic threats.

Hijji and Alam (2021) conducted a multivocal review on the rise of social engineering cyber threats during the COVID-19 pandemic. They analyzed 52 sources, including academic and grey literature, to identify main attack techniques – phishing, smishing, vishing, fraud, and spam – spread via email, fake websites, and mobile apps. The study discusses economic impacts and suggests solutions such as AI, blockchain, and big data analytics to strengthen cybersecurity.

Bhusal (2021) classifies social engineering attacks by interaction type and highlights the human factor's vulnerability. The author notes that traditional technical measures are often insufficient and recommends combining education with security policies. Salama et al. (2023) review attack types such as phishing, vishing, smishing, and pretexting, and analyze protection methods including user training, multi-factor authentication, and behavioral monitoring. They emphasize combining technical measures with user awareness to counter threats effectively. Kamruzzaman et al. (2023) examine main attack types – phishing, baiting, pretexting, quid pro quo, and tailgating – and analyze psychological principles like authority, urgency, scarcity, and familiarity. They suggest technical (antivirus, VPN) and behavioral (training, awareness) measures for prevention. Grbić and Dujlović (2023) show how ChatGPT can generate persuasive social engineering messages, lowering the barrier for attackers, and stress the need for updated cybersecurity strategies and user education.

Thus, the literature review shows that in the digital transformation era, social engineering is evolving from a narrow view as mere manipulation or cyber threat to a multidimensional socio-technological phenomenon within HR management. The analyzed sources demonstrate growing interdisciplinary interest in its mechanisms through the perspectives of behavioral economics, digital ethics, information security, and HR analytics.

Ukrainian researchers mainly focus on the security, psychological, and communication aspects of social engineering, highlighting its role in information warfare, cyber threats, stress resilience, and digital hygiene. In contrast, foreign authors view social engineering as part of behavioral management in digital HR, emphasizing ethical boundaries, transparency, nudge design, analytical decision-making, and the evolving role of HR in the AI era.

At the same time, both research traditions face the challenge of fragmented studies and the absence of a unified classification of social engineering forms in HR, complicating the integration of ethical, organizational, and technological approaches to shaping behavioral policy. Against this background, conceptualizing social engineering as a functional HR tool becomes essential. Therefore, this study aims to systematize existing methods and develop an original typology as a basis for a transparent, adaptive, and ethically grounded behavioral strategy in HR management.

2. AIMS

This study aims to develop a systematic approach to analyzing social engineering in HR management by creating an original typology of targeted influence forms on employee behavior, investigating digital tools for implementing such influence and identifying ethical criteria for the permissibility of social engineering interventions in the modern professional environment. The study develops recommendations for HR practitioners, researchers, and regulators on the safe, effective, and ethically justified use of behavioral technologies in personnel management.

3. METHODOLOGY

The study applies an interdisciplinary approach that integrates concepts from behavioral economics, social psychology, digital ethics, and personnel management. The researchers conducted a systems analysis method to identify patterns of social engineering manifestations in HR practices. Content analysis reviewed scientific sources and classified approaches to influencing employee behavior. The researchers utilized the typology method to develop an original model of social engineering types in the HR field. At the same time, structural-functional analysis helped determine the implementation of mechanisms in the digital environment. The researchers critically analyzed regulatory documents (GDPR, ISO/IEC 27001) and scientific literature on digital ethics to identify ethical boundaries of influence. The researchers applied a comparative approach to contrast Ukrainian and international contexts regarding the understanding and counteraction of social engineering in HR.

4. RESULTS

Despite growing interest in studying social engineering in related fields (cybersecurity, behavioral economics, organizational psychology), there is a lack of a systematized approach to examining its forms and manifestations in HR management. The literature review revealed several theoretical and empirical developments that are fragmentarily concerned with influencing personnel behavior but do not offer a unified concept of social engineering types within the HR function. This theoretical gap necessitated the formation of an author's typology.

Burda et al. (2024) analyzed 169 empirical studies on social engineering, covering 735 hypotheses, and noted that most experiments only partly simulate real attacks and rarely consider the cognitive characteristics of targets. They identify methodological gaps, such as underestimating context and variations in attack narratives, and call for a deeper interdisciplinary approach. Social-Engineer, LLC (2022) highlights the impact of cognitive biases like authority bias, confirmation bias, and herd mentality, which reduce critical information perception. They stress integrating psychological factors into cybersecurity strategies and raising employees' cognitive awareness as a key prevention. Bei (2017) argues for applying behavioral economics to shape HR managers' competencies, presenting a model that links managerial functions, professional skills, and behavioral aspects, including steps for developing competencies based on behavioral dynamics. Sazonova et al. (2022) identify core organizational behavior factors and propose a conceptual managerial model that aligns behavioral management with organizational and individual needs. They emphasize self-regulation, stress adaptation, and optimizing communication during military aggression.

Dâmbean and Gabor (2021) examined the correlation between emotional intelligence (EQ), stress, motivation, and job satisfaction at a machine-building enterprise. They empirically confirmed the key role of EQ in management, stress reduction, and productivity, establishing a positive link between high EQ, job satisfaction, and performance. Ahmed (2025) highlights the importance of EQ in HR, noting that the ability to identify, understand, and regulate emotions builds trust, improves communication, resolves conflicts, and boosts engagement. He also points out EQ's impact on recruitment, adaptation, motivation, and talent retention. Motorniuk and Krokhmalna (2022) also emphasize EQ as a crucial factor in personality assessment and HR management. They stress the value of developed EQ for leadership, success in global business, and mutual emotional understanding between employees and managers.

Tadesse Bogale and Debela (2024) systematically reviewed organizational culture as a tool for overcoming identification crises, analyzing 52 articles, classifying cultural orientations, and highlighting key dimensions and research gaps. They propose directions for future studies to enhance culture management. SHRM (2024) emphasizes organizational culture as a key factor for influencing employee behavior and achieving goals, stressing leaders' roles in shaping values and maintaining trust, engagement, and strategic effectiveness. Stambulska and Peredalo (2022) examine corporate culture's essence, components, typologies, and influence on managerial functions and target groups, identifying criteria such as culture type and organization size that determine this impact.

Kimani (2023) conducted a desktop study showing a positive link between effective internal communication – transparent, two-way, leadership-driven, and multi-channel – and higher employee engagement. Leadership communication is crucial for supporting interaction, with challenges including information overload and language barriers. The author recommends greater transparency, two-way processes, and stronger leadership skills. Fahmi (2024) also emphasizes the role of continuous communication for employee well-being, trust, and skill development, noting that adapting communication strategies is vital amid modern work trends. Zakharchyn (2023) explores communication culture in HRM, analyzing its functions, links to the social concept of HR, and the specifics of communication during wartime.

Zhanbo and Qiongyao (2021) emphasize studying the structure of HR knowledge to optimize selection, training, knowledge management, and competitiveness. They analyze its links to functional levels, business processes, and logic, proposing a four-dimensional HR Knowledge Framework and Development Model (HRKFDM) covering functional, environmental, process, and logical aspects. This model shows knowledge distribution across personnel levels and supports organizational learning and key competencies. The Factorial HR study (2021) highlights the role of HR functions in shaping and transforming organizational structure. It examines functional, matrix, and divisional structures, their impact on efficiency and strategic performance, and stresses HR specialists' role in ensuring flexibility, adaptability, and alignment with company goals. The study also outlines practical steps for structural change, including model audits, management involvement, and internal communication development.

Based on the analysis, several points stand out. Researchers view cognitive factors as crucial for understanding employee behavior, but most studies address them mainly in security or general behavioral management contexts (Burda et al., 2024; Social Engineer, 2022). Researchers recognize emotional intelligence as key for effective HR interaction (Ahmed, 2025; Motorniuk & Krochmalna, 2022) yet rarely position it as part of a broader influence system. Scholars mainly discuss organizational culture within management practice rather than as a distinct engineering type (SHRM, 2024; Stambulska & Peredalo, 2022). Communication processes support trust and engagement, but their role as a systematic social influence tool remains underexplored (Kimani, 2023; Fahmi, 2024). Organizational structure affects behavior design, yet classifications from a social engineering perspective are still lacking (Factorial, 2021; Zhanbo & Qiongyao, 2021).

Given the results of the systematic analysis of literature sources and the generalization of identified mechanisms of social influence on personnel, Table 1 presents the author's typology of social engineering in HR management. The proposed classification covers five basic types of social engineering, each reflecting a distinct vector of targeted influence on employee behavior through specific tools and management practices.

Table 1. Typology of Social Engineering in HR Management: Essence, Tools, and Practical Manifestations

Source: Developed by the authors based on the results of generalization of scientific research.

Type of Social Engineering	Essence	Key Tools	Main Manifestations in HR
Cognitive-Behavioral	Influence on thinking, perception, and behavioral patterns of personnel	Behavioral design, cognitive analytics, bias testing, nudging mechanisms	Candidate assessment by behavioral indicators, gamification of training, decision modeling
Emotional	Regulation of emotional state and emotional interaction among employees	EQ development, emotional leadership, wellbeing, stress management	Emotional support, trust microclimate, empathetic leadership, burnout prevention
Normative-Cultural	Shaping behavior through values, symbols, rituals, organizational norms	HR branding, codes of ethics, corporate rituals, onboarding symbols	Socialization, corporate identity formation, normative behavior regulation
Communicative	Managing the content and form of communication to shape behavioral expectations	Internal communication strategies, chatbots, multichannel communication, storytelling	Two-way feedback, transparency of decisions, unified information space
Organizational-Structural	Influence through building organizational architecture and management structure	Project offices, matrix teams, delegation, hierarchy changes, agile models	Creating flexible teams, role redistribution, increasing structural adaptability

The proposed typology of social engineering in HR, shown in Table 1, summarizes the author's generalization of current scientific approaches to mechanisms of social influence on personnel behavior. Its novelty is distinguishing five integrated vectors – cognitive-behavioral, emotional, normative-cultural, communicative, and organizational-structural – each with specific tools and channels within the HR function. This typology frames social engineering as a general socio-cybernetic phenomenon and an applied HR tool. It can serve as a foundation for further research, strategy development, and practical interventions to shape desired behavior, enhance communication, and transform organizational culture in a turbulent environment.

The proposed typology outlines key directions of organizational influence on employee behavior. The effectiveness of each type depends on applying specific psychological, informational, and managerial mechanisms that activate cognitive and emotional responses and shape predictable behavioral patterns within a given communication or cultural context. Therefore, examining the main social influence mechanisms through the lens of behavioral economics, cognitive psychology, and social engineering is relevant.

Implementing each type of social engineering in HR involves specific psychological and informational mechanisms that trigger employees' cognitive, emotional, and behavioral responses. These mechanisms help achieve management goals by shaping perceptions, attitudes, and behavior. Researchers justify their use through modern interdisciplinary approaches – behavioral economics, social psychology, and neuroscience – which show high applied effectiveness in HRM (Cantarelli, et al., 2018; Grensing-Pophal, 2020; Hull, 2024).

The most common mechanisms of social influence in HR practices are cognitive biases, emotional triggers, and informational scenarios.

Cognitive biases are systematic deviations in thinking that arise when people simplify decisions in complex or uncertain situations. In HR, such effects can be used deliberately – for example, the anchoring effect in pay negotiations or framing in motivational messages – but can also distort management decisions through biases like the halo effect or first impression bias. Cantarelli et al. (2018) show that cognitive biases significantly affect performance evaluation and that debiasing interventions can reduce their negative impact. Similar conclusions by Rastogi et al. (2022) highlight the anchoring effect's role and the importance of structured thinking in human-technology interactions.

Emotional triggers activate specific affective states that strongly influence trust, loyalty, and engagement. They shape behavioral responses and foster deeper connections in interpersonal and organizational settings. Understanding these mechanisms is key to building lasting relationships and improving engagement strategies. Typical

HR triggers include positive reinforcement (recognition, approval, symbolic rewards), messages that evoke belonging (empathy, care), and gamified or competitive elements to boost motivation. Grensing-Pophal (2020) highlights that managing emotional triggers is vital for employees' psychological safety, while Bentley (2025) emphasizes that conscious regulation of emotions supports stable interactions and reduces reactive decisions in teams.

Informational scenarios are structured ways of presenting messages that align with how people process information. In HR, they help format internal communication, neutrally or motivationally, manage expectations (via framing, repetition, social proof), and shape behavior through case studies and success stories. Hull (2024) notes that such scenarios ease new team adaptation and ensure message consistency. Modern HR platforms like ChangeEngine provide ready-made templates to reduce cognitive load and improve clarity (Rubin, 2025).

These mechanisms provide a practical foundation for applying different types of social engineering in HR, allowing for personalized behavior modeling, smooth adaptation, and stronger internal communication. Recent studies and cases confirm their scientific validity, supporting effective use without violating ethical standards, autonomy, or dignity. Their implementation increasingly relies on digital tools: automation, algorithms, and data analytics expand ways to influence behavior while maintaining efficiency and scalability. HRMS, e-learning platforms, recruitment chatbots, and behavior-tracking systems are the main digital vectors.

Implementing social engineering in modern HR increasingly depends on digital platforms and tools that go beyond technical or administrative functions. In behaviorally oriented HR, these tools serve as channels of social influence to shape behavior patterns, adaptation strategies, communication models, and employees' value orientations. Digitalized HR processes create the infrastructure for scaling, personalizing, and algorithmizing behavioral influence. These interventions integrate into daily activities through interfaces, scripts, decision scenarios, visual cues, and predictive HR analytics. Key digital vectors include:

- HRMS (Human Resource Management Systems) – provide centralized management of the employee lifecycle, recording behavioral metrics and supporting management decisions based on evaluation algorithms;

- e-learning platforms – enable the design of adaptation and learning trajectories embedded with targeted emotional-cognitive content, facilitating the assimilation of knowledge and organizational norms;

- recruiting chatbots – perform automated selection and initial interaction with candidates based on behavioral characteristics, influencing the formation of expectations and methods of self-presentation;

- employee behavior tracking systems – record digital activity, emotional states, and interaction frequency, creating a basis for managerial intervention and deviation forecasting;

- HR analytics (People Analytics) – allows for building individual and collective behavioral profiles, identifying demotivation, turnover, and conflict risks, and performing behavioral targeting;

- digital internal communication platforms (e.g., Slack, MS Teams, Workplace) – act as mechanisms for cultural integration, where standards of language, visual style, response speed, and engagement volume are systematically normalized;

- survey and feedback services – use to promptly assess moods, climate, and trust, with subsequent policies or interventions adjustment according to target responses;

- virtual assistants with artificial intelligence elements – model informational interaction scenarios, enhance cultural and normative socialization and ensure the constant presence of behavioral standards.

Digital HR solutions perform technical functions and act as tools of social engineering that influence employees' thinking, emotions, attitudes, and behavior. Their use creates new opportunities for behavioral management while improving efficiency, adaptability, and ethical control. Purposefully designed digital technologies extend beyond basic HR support and serve as instruments of social influence that shape desired behavior, build loyalty, support adaptation, and enable indirect control. From this perspective, social engineering in HR represents the construction of significant behavioral patterns through digitally managed communication and information environments.

Such environments include HRMS systems that record employee actions and set activity standards; e-learning platforms that educate through value-oriented cases; chatbots that standardize communication style; tracking systems that enable building individualized intervention trajectories; as well as internal corporate platforms that shape organizational culture through language, tone, and repeated signals.

Giermindl et al. (2021) note that these tools subtly shape behavior as "soft forms of control" through algorithms embedded in digital systems, warning about the risks of opaque standardization and emotional influence even without direct managerial action. HR analytics, in turn, predicts behavioral responses and helps organizations monitor and adapt management decisions (Saling & Do, 2020). Banerjee et al. (2025) add that digital HR data supports designing behavioral-level management interventions.

Thus, digital HR tools – from analytical platforms to communication environments – act as channels of social engineering. HR professionals use them to normalize, reinforce, and modify employee behavior, effectively creating a behavior-shaping infrastructure that integrates technology, management, and applied psychology.

By integrating digital tools into HR practices, organizations significantly expand their capacity to influence employee behavior – from designing programmed adaptation trajectories to managing algorithm-driven decisions and communication-based influence. Traditional and digital forms of social engineering – including behavioral design, communication scripts, cultural norms, and emotional triggers – directly affect employees' choices, evaluations, and motivation. These practices inevitably raise questions about the ethical legitimacy of such an influence.

As the arsenal of HR instruments expands, so does the risk of ethical imbalance, particularly when the boundary between promoting expected behavior and manipulating employees becomes blurred. As these tools of influence – digital or not – evolve into fully operational channels of social modeling, HR professionals must critically reflect on transparency, consent, awareness, and the acceptable limits of influence in the workplace.

That is why the next logical step involves addressing the ethical boundaries of influence in HR by answering key questions: What qualifies as ethical encouragement? What constitutes behavioral pressure? Moreover, when does influence cross the line into classical manipulation?

In the HR sphere, where traditional and digital social engineering tools are actively employed, the line between ethical behavioral stimulation and manipulative influence often remains blurred. The use of nudging, behavioral design, personalization algorithms, or tracking can generate positive effects on employee engagement and development but also risks concealed pressure, limited autonomy, or the substitution of conscious choice with predefined scenarios (Spiekermann & Winkler, 2020; Lembcke et al., 2019; Schmidt & Engelen, 2020).

Scientific approaches rely on several key criteria to define the boundaries of permissible influence:

- Awareness level. One of the key ethical indicators lies in whether the employee knows they are being influenced and whether they can recognize the mechanism of that influence. As Schmidt and Engelen (2020) point out, influence exerted through hidden cognitive triggers without informing the individual violates the principle of autonomy, even if the intention is favorable – a critical consideration in the HR context, where work-related decisions can have serious consequences.

- Voluntariness of Choice. The following criterion is whether the employee has a real choice: to accept or reject influence. Lembcke et al. (2019) emphasize that the existence of alternatives and the ability to refuse are crucial for distinguishing behavioral nudging from manipulation. In a corporate environment with hierarchical pressure, voluntariness is easily blurred, especially when implementing monitoring, rating, or gamification technologies.

- Transparency of purpose and means. Research by Bruns (2021) and Meske and Amojo (2020) shows that ethically acceptable nudging requires transparency – employees must know they are being influenced and understand the purpose behind it. In digitalization, where many influence mechanisms operate through interfaces or automatically, transparency becomes a key factor in establishing legitimacy.

- Consequences for dignity and autonomy. The final ethical criterion of influence involves assessing its impact on an employee's independence and dignity. In a review by Meske, and Amojo (2020), the authors emphasize that specific digital nudges – particularly opaque, interactive, and behavior-dependent – can undermine user autonomy. They classify these interventions as potentially intrusive or manipulative because they alter behavior without allowing room for conscious, voluntary choice. In the HR context, this may result in employees losing subjective control over their career paths, professional conduct, or decisions that traditionally fall within personal discretion.

Our analysis shows that ethicality cannot be defined solely by good intentions or organizational effectiveness in HR, especially with social engineering and digitalization. Instead, clear ethical boundaries must be set using a comprehensive approach. Key criteria include employees' awareness of the influence and its mechanisms, the availability of real alternatives, transparency of goals and interfaces, and respect for individual dignity and autonomy.

These criteria help distinguish ethical encouragement from manipulative practices that managers or technology designers might disguise as innovation. This issue is especially relevant in digital HR, where algorithmic decisions, automated prompts, behavioral interfaces, and nudging tools increasingly shape daily employee interactions. Such influence shifts the balance between freedom of choice and predetermined behavior, making it harder to maintain ethical standards.

In summary, ethical and social engineering in HR is only possible if we adhere to voluntariness, transparency, predictability of influence, and respect for each employee's autonomous choice. Failing to uphold these principles erodes trust in HR practices and can lead to formalized manipulation disguised as organizational development.

5. DISCUSSION

The study's findings systematize the forms of social engineering in HR and conceptualize it as a multidimensional socio-technological process that varies by cultural, legal, and economic context. In the digital era, where organizations increasingly shape behavior through algorithmic, emotional, and communicative interventions, social engineering becomes systemically significant, especially in HR at the intersection of national security and global corporate challenges. For example, in Ukraine, it is linked to hybrid aggression against state institutions, while internationally, the focus is on ethical data use, behavioral interventions, and organizational accountability. This asymmetry highlights the need for comparative analysis of ethical frameworks and countermeasures in HR.

In Ukraine, experts often view social engineering as part of cyber threats linked to hybrid warfare. CERT-UA reports phishing campaigns that use HR-themed emails to spread malware like WRECKSTEEL, targeting government institutions and critical infrastructure (Stahie, 2025). Russian hackers also launch phishing attacks to compromise Signal messenger accounts of Ukrainian users, creating significant risks for HR departments that handle sensitive information (Asokan, 2025).

Internationally, social engineering seriously threatens corporate security, especially in HR. HR departments are prime targets for phishing, vishing, smishing, and pretexting because they handle employee data. Attackers exploit human vulnerabilities – trust, fear, or helpfulness – to access confidential information or systems, making these techniques highly effective (Perception Point, n.d.).

To gain a comprehensive understanding of the specific characteristics of social engineering in the HR domain, it is essential to compare Ukrainian

http://dx.doi.org/10.21511/slrtp.15(1).2025.04

Table 2. Comparison of Ukrainian and International Approaches to Social Engineering in the HR Sphere

Source: Summarized and systematized by the authors based on Stahie (2025), Asokan (2025), Perception Point (n.d.).

Aspect	Ukraine	International Context
Main Focus	Protection against state cyber threats and hybrid warfare	Protection against cybercrime and insider threats
Typical Attacks	Phishing via HR documents, messenger compromise	Phishing, vishing, smishing, pretexting
Role of HR	Target of attacks due to access to sensitive information	Key player in preventing social engineering through training and security policies
Key Security Measures	Raising awareness, implementing security policies, cooperation with government bodies	Regular training, phishing simulations, implementation of multi-factor authentication
Regulatory Environment	Active involvement of government agencies such as CERT-UA	Compliance with international standards such as GDPR, ISO/IEC 27001

and international approaches, which differ significantly in focus, threat types, the role of HR departments, and response strategies, as illustrated in Table 2.

Approaches to social engineering in HR differ between Ukraine and the global context but share similarities. In Ukraine, organizations focus on defending against state-sponsored cyber threats, while international companies prioritize protection from cybercrime and insider risks. Despite these differences, HR plays a crucial role in cybersecurity everywhere, underscoring the need to train HR professionals and enforce strong security policies.

Thus, regardless of the regional context, social engineering challenges in HR require a systematic response – both at the level of security strategies and through daily management practices. These issues become especially urgent in the context of digitalization, which not only transforms HR management tools but creates new vectors of potential influence on employee behavior.

The digital transformation of HR processes has fundamentally altered the technical architecture of workforce management and introduced new points of entry for social engineering influence. The most vulnerable areas to digital risks and behavioral interventions include recruitment, onboarding, learning and development, performance evaluation, personal data protection, and the organizational culture of trust (see Table 3).

As the table shows, the digital transformation of HRM offers vast opportunities but creates new risks for transparency, security, and trust. Digital tools now shape not only administrative workflows but also the behavioral architecture of employees, influencing their decisions and interactions. These developments raise critical ethical questions: Where is the line between acceptable motivation and manipulation? Which digital HR practices respect autonomy, voluntariness, and human dignity, and which violate these principles? Answering such questions requires referring to current ethical and legal standards.

Table 3. Vulnerable Areas of HR in the Context of Digital Transformation and Social Engineering

Source: Compiled and systematized by the authors based on the conducted analysis.

HR Area	Digital Tools	Socio-Engineering Mechanisms	Potential Risks
Recruiting	AI recruiters, chatbots, online questionnaires	Job framing, adaptive self-presentation, behavioral filters	Information manipulation, choice substitution, phishing
Onboarding	E-learning, onboarding modules, gamification	Standardized norm transfer, role framing, nudge scenarios	Unconscious adoption of cultural codes, passive loyalty
Performance Evaluation	HR analytics, digital dashboards, OKR systems	Activity monitoring, algorithm-based evaluation	Behavioral normalization, emotional exhaustion, self-censorship
Learning and Development	LXP platforms, adaptive learning, digital courses	Nudge design, automated promotion scenarios	Restriction of individual development freedom, cognitive standardization
Data Protection	HRMS, account systems, questionnaires, tracking	Behavioral targeting, non-transparent profile building	Privacy violation, risk of discriminatory decisions
Trust Culture	Slack, MS Teams, social reactions, surveys	Normative activity signals, reaction algorithms	Loss of authenticity, communication formalization, covert control

The digitalization of HR processes has opened new horizons for influencing employee behavior. However, these advancements also heighten the risk of losing ethical balance. Today, social engineering in HR goes far beyond predictive analytics – it actively shapes behavioral trajectories. Organizations must establish clear boundaries between legitimate motivational influence and manipulative interventions.

The General Data Protection Regulation (GDPR) is a key document defining legal limitations on digital interventions. Article 22 states that individuals have the right not to be subject to a decision based solely on automated processing, including profiling if such a decision produces legal effects or similarly significant consequences for them (European Parliament, 2016). In the HR domain, this directly concerns using algorithms for employee evaluation, selection, or ranking without adequate explanation or the opportunity for appeal. The ISO/IEC 27001 standard also emphasizes the need to ensure information security, including the protection of data confidentiality, integrity, and availability. This standard requires organizations to establish precise access controls for personal information and conduct risk monitoring, which becomes particularly relevant when using digital HR platforms (ISO/IEC, 2022).

In this context, researchers can apply four core criteria of ethical behavioral influence - awareness, voluntariness, transparency, and preservation of autonomy. These criteria serve as a cross-cutting analytical tool throughout the study: initially, researchers examine them within the academic discourse on the ethics of digital influence and subsequently interpret them within the legal framework (GDPR, ISO/IEC 27001) as normative guidelines that define the permissible boundaries of behavioral interventions in the HR domain.

- Awareness Level. Schmidt and Engelen (2020) emphasize that influencing individuals through hidden cognitive triggers without informing them directly violates the principle of autonomy. In HR, this issue becomes particularly critical when decisions have long-term consequences for employees.

- Voluntariness of Choice. Winkler and Spiekermann (2019) argue that the availability of a genuine alternative serves as a key criterion for distinguishing ethical nudging from manipulation. In HR environments, hierarchical dependencies can distort the voluntariness of employees' decisions.

- Transparency of Goals and Means. In their systematic review, Valta and Maier (2025) emphasize that only those digital interventions that remain transparent to users – clearly articulating their purpose and expected outcomes and making the influence recognizable – can be considered ethically acceptable. Using opaque or behavior-dependent mechanisms that lack explanation or intuitive understanding may significantly restrict individual autonomy, especially in HR, where digital tools affect employee evaluation, communication, and career trajectories.

- Consequences for Dignity and Autonomy. Valta and Maier (2025) also stress that certain forms of digital nudging - exceptionally personalized, opaque, and behavior-dependent techniques - can undermine user autonomy, particularly when implemented without clear communication of purpose and genuine choice. The authors emphasize that such interventions can modify a person's behavior without their full awareness, raising ethical concerns about the loss of decision-making control in the digital HR environment.

The examples above demonstrate that the boundary between acceptable and risky behavioral HR engineering remains fluid. It demands continuous reevaluation of ethical criteria in light of the digital environment, legal frameworks, and employee expectations. HR professionals must act as administrators of digital tools and as ethical facilitators capable of maintaining a balance between effectiveness and human dignity.

In this regard, an essential next dimension of analysis involves examining the influence of the global context on standards of digital personnel management. Globalization expands the potential applications of social engineering while simultaneously complicating the observance of ethical norms in multicultural and multilayered environments. This dynamic calls for evaluating internal organizational aspects of digital HR interventions and the challenges of applying universal technologies across diverse international settings.

Globalization has significantly reshaped human resource management practices, accelerating the adoption of digital HR tools, such as HRMS platforms, e-learning systems, algorithmic recruitment solutions, and behavioral analytics. Transnational corporations often design and promote these technologies as universal solutions for the global labor market. However, such universality does not always ensure effectiveness or ethical neutrality in local contexts.

Firstly, local companies in countries with lower levels of digital maturity often lack the infrastructure and the qualified personnel necessary to implement complex digital interventions, exacerbating digital inequality in HR management. Riso et al. (2022) notes that digitalization can create structural asymmetries between large corporations and small enterprises, deepening disparities in access to personalized HR solutions and protecting workers' rights.

Secondly, implementing "universal" HR technologies does not always align with local cultural, legal, and labor traditions. For example, acceptable behavioral interventions in the United States may conflict with privacy norms and labor autonomy in Europe or post-Soviet countries. A study published in Frontiers in Psychology emphasizes that integrating artificial intelligence into HR practices requires cultural sensitivity and adaptation to the organizational context; otherwise, there is a risk of ethical conflicts and a loss of employee trust (Dima et al., 2024).

Thirdly, as Deodhar et al. (2024) point out, global companies are increasingly developing their ethical frameworks for digital technologies, including social engineering in HR. In contrast, local organizations often rely on external regulations or lack any ethical policy altogether, which creates asymmetry in governance and reduces the transparency of HR practices.

Although digital HR tools offer significant potential to enhance management practices globally, implementing them without considering the local context can reduce effectiveness and deepen inequalities between global and regional labor market players.

Given the rise of ethical challenges and digital asymmetries, HR departments must go beyond simply adhering to integrity standards when applying social engineering methods - they also need to build an enabling organizational environment. Such a shift in HR responsibilities requires expanding traditional roles to include proactive information security measures and increasing employee digital awareness in today's digital economy. Accordingly, one of the key transformational roles of HR professionals involves fostering a cybersecurity culture as an integrated element of organizational culture and human resource management strategy.

As digital risks and cyber threats grow, building a cybersecurity culture has become an IT function and a new area of responsibility for HR. Organizations increasingly recognize employees as active agents of information security, not just passive objects. This recognition calls for integrating cybersecurity principles into training programs, onboarding processes, and behavioral management policies.

According to Dima et al. (2024), HR professionals increasingly shape responsible digital behavior, organize cybersecurity awareness training, and help enforce access policies for corporate systems. Their role goes beyond introducing technical restrictions - they also develop behavioral norms that reduce the risk of human error in security incidents.

Moreover, Riso et al. (2022) emphasizes that the key elements of cybersecurity culture include transparent data handling procedures, regular communication about digital threats, and fostering trust in digital systems. In this approach, the HR department acts as a facilitator between strategic leadership, IT teams, and employees, maintaining a balance between efficiency, control, and digital human rights.

The modern HR function must not only respond to cybersecurity challenges but also proactively shape a digital culture in which employee behavior becomes the first line of defense.

The formulated recommendations build logically on the analytical findings of the study and aim to expand the managerial, academic, and regulatory toolkit for addressing social engineering in HR practices. These proposals take into account the complex nature of the phenomenon, which involves both the risks of digital interaction and the potential for constructive influence on employee behavior within ethically regulated processes.

The recommendations target key stakeholders – HR professionals, management structures, researchers, and policymakers – considering the context of digital transformation, security challenges, and the growing importance of behavioral architecture in human resource management.

For HR professionals and management teams:

- Design and implement digital awareness programs to educate employees about social engineering methods, including phishing simulations, cybersecurity hygiene practices, and cognitive resilience against manipulative influence.
- Institutionalize ethical standards for behavioral influence in HR practices, emphasizing goal transparency, voluntary participation, and protection of employee autonomy in algorithm-driven management environments.
- Integrate information security functions into HR processes through ongoing collaboration with cybersecurity specialists, particularly when developing access policies, processing personal data, and assessing digital risks.

For business and corporate governance:

- Promote the development of Digital HR strategies that treat the human factor as a key point of digital vulnerability and a source of organizational resilience to socio-technological threats.
- Use algorithmic and AI-driven HR solutions within ethical and legal responsibility boundaries, ensuring decision-making model transparency, the right to appeal, and privacy protection.
- Conduct ethical audits of behavioral HR interventions, especially in recruitment, performance evaluation, and corporate training, to prevent covert forms of digital coercion or discrimination.

For the academic community:

- Deepen interdisciplinary research on social engineering in HR by integrating perspectives from human resource management, behavioral economics, cognitive psychology, information security, and digital ethics.
- Develop typologies of socioengineering influence in organizational settings by distinguishing between constructive, motivation-oriented practices and destructive, manipulative strategies.
- Analyze the cultural and legal diversity in how behavioral interventions in HR are perceived across different countries to design universal yet adaptable approaches to digital regulation.

For government bodies and regulators:

- Create legal and regulatory frameworks that define the acceptable use and boundaries of socio-technological tools in personnel management while respecting autonomy, transparency, and digital integrity standards.
- Establish precise accountability mechanisms that hold organizations responsible for the consequences of socioengineering attacks – particularly regarding data breaches, information security violations, or covert employee profiling.
- Promote the development of national ethical codes for the HR sector that regulate behavioral digital practices in an era of increasing algorithmic management.

CONCLUSION

This article demonstrates that social engineering in the HR domain represents a multidimensional phenomenon that includes cognitive, emotional, communicative, cultural, and structural mechanisms for influencing employee behavior. The literature review reveals a lack of a unified approach to classifying socioengineering practices within human resource management, which prompted the development of an original typology of social engineering in HR functions.

The proposed typology identifies five fundamental vectors – cognitive-behavioral, emotional, normative-cultural, communicative, and organizational-structural – each associated with relevant managerial influence tools. The study also systematizes key psychological and informational mechanisms of influence, including cognitive biases, emotional triggers, and informational scripts.

The study pays particular attention to the role of digital HR technologies as infrastructural carriers of social engineering. HRMS systems, e-learning platforms, chatbots, tracking, and analytics services increasingly shape the behavioral architecture of employees. This transformation opens new opportunities for personalized management but raises ethical concerns regarding the boundaries of acceptable influence, algorithms' transparency, and personal autonomy preservation.

The analysis identifies the key ethical criteria for socioengineering practices in HR: the degree of awareness of the influence, the voluntariness of choice, the transparency of objectives, and the preservation of employee dignity. The study also outlines the differences between Ukrainian and international approaches to social engineering in HR, considering the contexts of security, legal regulation, and digital maturity.

Future research may focus on empirically validating the typology of social engineering, developing methods for evaluating its effectiveness, and designing tools for ethical auditing of behavioral HR interventions.

AUTHORS CONTRIBUTIONS

Conceptualization: Iryna Varis.
Data Curation: Iryna Varis, Oleksiy Subochev.
Formal Analysis: Iryna Varis.
Funding Acquisition: Iryna Varis.
Investigation: Iryna Varis, Oleksiy Subochev, Oleh Voloboiev.
Methodology: Iryna Varis.
Project Administration: Iryna Varis.
Resources: Iryna Varis, Oleksiy Subochev.
Software: Iryna Varis, Oleh Voloboiev.
Supervision: Iryna Varis.
Validation: Oleksiy Subochev.
Visualization: Iryna Varis, Oleh Voloboiev.
Writing - Original Draft: Iryna Varis.
Writing - Review & Editing: Iryna Varis, Oleksiy Subochev, Oleh Voloboiev.

REFERENCES

1. Ahmed, Z. (2025). *The Role of Emotional Intelligence in HR*. FlowHCM. Retrieved from https://flowhcm.com/emotional-intelligence-in-hr/
2. Asokan, A. (2025). *Ukrainian Signal Users Fall to Russian Social Engineering*. CIO.inc. Retrieved from https://www.cio.inc/ukrainian-signal-users-fall-to-russian-social-engineering-a-27550
3. Banerjee, P., Pandey, J., & Gupta, M. (2025). *People Analytics: Theory, Tools and Techniques* (1st ed.). Routledge India. https://doi.org/10.4324/9781032624013
4. Bei, H. (2017). Kompetentnisni skladovi HR-menedzhmentu v konteksti formuvannia i rozvytku povedinkovoi ekonomiky [Competence components of HR management in the context of the formation and development of behavioral economics]. *Ekonomika i orhanizatsiia upravlinnia – Economics and Organization of Management, 4*(28), 47-55. (In Ukrainian). Retrieved from https://jeou.donnu.edu.ua/article/view/5989
5. Bentley, J. (2025). *Emotional triggers aren't scary … ignoring them is*. Retrieved from https://www.linkedin.com/pulse/emotional-triggers-arent-scaryignoring-them-john-bentley-moroe
6. Bhusal, C. (2021). Systematic review on social engineering: Hacking by manipulating humans.

Journal of Information Security, 12(1), 104-114. http://dx.doi.org/10.4236/jis.2021.121005

7. Birthriya, S., Ahlawat, P., & Jain, A. (2024). A comprehensive survey of social engineering attacks: Taxonomy of attacks, prevention, and mitigation strategies. *Journal of Applied Security Research, 20*(2), 244-292. https://doi.org/10.1080/19361610.2024.2372986
8. Bondarenko, I. (2025). The Controversy of the Concept of Social Engineering in the Conditions of Socio-Political Changes. *Scientific Notes of V. I. Vernadsky Taurida National University. Series: Philology. Journalism – Vcheni zapysky TNU imeni V. I. Vernadskoho. Seriia: Filolohiia. Zhurnalistyka, 36*(75), 293-299. (In Ukrainian). https://doi.org/10.32782/2710-4656/2025.1.2/47
9. Bruns, H. (2021). Nudges can be transparent and yet effective. *Publications Office of the European Union*. Retrieved from https://publications.jrc.ec.europa.eu/repository/handle/JRC125313
10. Burda, P., Allodi, L., & Zannone, N. (2024). Cognition in Social Engineering Empirical Research: a Systematic Literature Review. *ACM Transactions on Computer-Human Interaction, 31*(2), 19. https://doi.org/10.1145/3635149
11. Cantarelli, P., Belle, N., & Belardinelli, P. (2018). Behavioral Public HR: Experimental Evidence on Cognitive Biases and Debiasing Interventions. *Review of Public Personnel Administration, 40*(1), 56-81. https://doi.org/10.1177/0734371x18778090
12. Dâmbean, C., & Gabor, M. (2021). Implications of Emotional Intelligence in Human Resource Management. *Economics, 9*(2), 73-90. https://doi.org/10.2478/eoik-2021-0016
13. Deodhar, S., Borokini, F., & Waber, B. (2024). *How companies can take a global approach to AI ethics*. Harvard Business Review. Retrieved from https://hbr.org/2024/08/how-companies-can-take-a-global-approach-to-ai-ethics
14. Dima, J., Gilbert, M.-H., Dextras-Gauthier, J., & Giraud, L. (2024). The effects of artificial intelligence on human resource activities and the roles of the human resource triad: Opportunities and challenges. *Frontiers in Psychology, 15*. https://doi.org/10.3389/fpsyg.2024.1360401
15. European Parliament. (2016). *General Data Protection Regulation (EU) 2016/679*. Retrieved from https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32016R0679
16. Factorial. (2021). *How HR can reimagine organizational structure*. Retrieved from https://factorialhr.com/blog/organizational-structure/
17. Fahmi, L. (2024). Internal Communication and Well-being: Organizational Challenge. *International Journal of Humanities, Social Sciences and Education, 11*(2), 64-68. https://doi.org/10.20431/2349-0381.1102007
18. Giermindl, L. M., Strich, F., Christ, O., Leicht-Deobald, U., & Redzepi, A. (2021). The dark sides of people analytics: reviewing the perils for organisations and employees. *European Journal of Information Systems, 30*(2), 153-172. https://doi.org/10.1080/0960085X.2021.1927213
19. Grbić, D., & Dujlović, I. (2023). Social engineering with ChatGPT. *Proceedings of the 22nd International Symposium INFOTEH-JAHORINA (INFOTEH)* (pp. 1-5). https://doi.org/10.1109/INFOTEH57020.2023.10094141
20. Grensing-Pophal, L. (2020). *The benefits of workplace scripts*. HR Daily Advisor. Retrieved from https://hrdailyadvisor.com/2020/06/01/the-benefits-of-workplace-scripts/
21. Hijji, M., & Alam, G. (2021). A multivocal literature review on growing social engineering based cyber-attacks/threats during the COVID-19 pandemic: Challenges and prospective solutions. *IEEE Access,* 9, 7152-7166. https://doi.org/10.1109/ACCESS.2020.3048839
22. Hull, L. (2024). *How to deal with emotional triggers at work: 4 effective strategies*. Retrieved from https://brainleadership.com/how-to-deal-with-emotional-triggers-at-work/
23. ISO. (2022). *Information technology - Security techniques - Information security management systems - Requirements (ISO/IEC 27001:2022)*. International Organization for Standardization. Retrieved from https://www.iso.org/standard/27001
24. Kamruzzaman, A., Thakur, K., Ismat, S., Ali, M. L., Huang, K., & Thakur, H. (2023). Social engineering incidents and preventions. *Proceedings of the 2023 IEEE 13th Annual Computing and Communication Workshop and Conference (CCWC)* (pp. 494-498). https://doi.org/10.1109/CCWC57344.2023.10099202
25. Kimani, B. (2023). Internal Communication Strategies and Employee Engagement. *Journal of Public Relations, 2*(1), 13-24. https://doi.org/10.47941/jpr.1695
26. Kolluri, V. (2019). Revolutionary research on the AI Sentry: An approach to overcome social engineering attacks using machine intelligence. *International Journal of Creative Research Thoughts (IJCRT), 7*(3), 590-593. Retrieved from https://ijcrt.org/papers/IJCRT1135522.pdf
27. Kudinova, A., Kyryanova, O., & Dvornik, I. (2023). Experimentalna ekonomika ta sotsialnyi inzhynirynh: spilne ta vidminne [Experimental economics and social engineering: Similarities and differences]. *Rynkova ekonomika: suchasna teoriia i praktyka upravlinnia - Market Economy: Modern Theory and Management Practice, 21*(2(51)), 42-55. (In Ukrainian). https://doi.org/10.18524/2413-9998.2022.2(51).274365
28. Lembcke, T.-B., Engelbrecht, N., Brendel, A. B., & Kolbe, L. (2019). To Nudge or Not To Nudge: Ethical Considerations of Digital Nudging Based on Its Behavioral Economics Roots. *In Proceedings of the 27th European Conference on Information Systems (ECIS).*

Stockholm & Uppsala, Sweden, Retrieved from https://aisel.aisnet.org/ecis2019_rp/95/

29. Maznyk, L., & Drahan, O. (2024). Rol fakhivtsiv z kiberbezpeky v rozvytku HRM-systemy [The role of cybersecurity specialists in the development of the HRM system]. In N. S. Skopenko (Ed.), *Problemy i perspektyvy vidnovlennia ta rozvytku pidpryiemstv kharchovoi promyslovosti v suchasnykh umovakh* [Problems and prospects of restoration and development of food industry enterprises in modern conditions] (pp. 285-301). Kyiv: TsP Komprynt. (In Ukrainian). Retrieved from https://dspace.nuft.edu.ua/server/api/core/bitstreams/73292a2f-9d13-4eb7-bfc2-957e923ed0c2/content#page=285

30. Meske, C., & Amojo, I. (2020). Ethical guidelines for the construction of digital nudges. *Proceedings of the 53rd Hawaii International Conference on System Sciences* (pp. 3928-3937). Retrieved from http://hdl.handle.net/10125/64222

31. Motorniuk, U., & Krokhmalna, Ya. O. (2022). Emotional Intelligence in the Staff Management System: Structure and Problems of Assessment. *Menedzhment ta pidpryiemnytstvo v Ukraini: etapy stanovlennia ta problemy rozvytku - Management and Entrepreneurship in Ukraine: Stages of Formation and Problems of Development*], *2*(8), 56-64. (In Ukrainian). Retrieved from https://science.lpnu.ua/sites/default/files/journal-paper/2022/dec/29504/220972maket-56-64.pdf

32. Ohnivchuk, M. (2024). *Zlamayte svoyi mirky persh, nizh tse zrobyt khaker [Hack your brains before a hacker does it]*. H-X Technologies. (In Ukrainian). Retrieved from https://www.h-x.technology/ua/blog-ua/hack-your-brains-before-hacker-does-ua

33. Orel, Yu., & Smahliuk, A. (2023). HR-menedzhment v ukrainskomu biznesi: vyklyky tsyfrovizatsii [HR-management in Ukrainian business: Challenges of digitalization]. *Akademichni vizii - Academic Visions, 19*. (In Ukrainian). https://doi.org/10.5281/zenodo.7954499

34. Perception Point. (n.d.). *7 Social Engineering Prevention Methods and Why Your Organization Needs Them*. Retrieved from https://perception-point.io/guides/bec/social-engineering-prevention-methods-why-your-organization-needs-them/

35. Petrova, I., & Barash, A. (2024). The Impact of Digital Economy on the Transformation of Employment and Strategeis of Human Resource Management. *Aktualni problemy ekonomiky - Actual Problems of Economics*, *1*(279), 78-86. (In Ukrainian). https://doi.org/10.32752/1993-6788-2024-1-279-78-86

36. Rastogi, C., Zhang, Y., Wei, D., Varshney, K., Dhurandhar, A., & Tomsett, R. (2022). *Deciding fast and slow: The role of cognitive biases in AI-assisted decision-making*. https://doi.org/10.48550/arXiv.2010.07938

37. Riso, S., Adascalitei, D., Forés, L., & Lechardoy, L. (2022). Ethics in the digital workplace. *European Foundation for the Improvement of Living and Working Conditions*. Retrieved from https://ddd.uab.cat/pub/estudis/2022/259406/ef22038en.pdf

38. Rubin, J. (2025). 326 free HR communication templates for seamless workplace messaging. *ChangeEngine*. Retrieved from https://www.changeengine.com/articles/326-communication-templates-to-streamline-hr-announcements

39. Ruehle, R. (2023). The moral permissibility of digital nudging in the workplace: Reconciling justification and legitimation. *Business Ethics Quarterly, 33*(3), 502-531. https://doi.org/10.1017/beq.2023.4

40. Salama, R., Al-Turjman, F., Bhatla, S., & Yadav, S. (2023). Social engineering attack types and prevention techniques: A survey. *Proceedings of the 2023 International Conference on Computational Intelligence, Communication Technology and Networking* (pp. 817-820). https://doi.org/10.1109/CICTN57981.2023.10140957

41. Saling, K., & Do, M. (2020). Leveraging People Analytics for an Adaptive Complex Talent Management System. *Procedia Computer Science, 168,* 105-111. https://doi.org/10.1016/j.procs.2020.02.269

42. Sazonova, T., Kurchenko, A., & Zalipa, T. (2022). Features of Personnel Behavior Management in Modern Conditions. *Naukovyi visnyk Uzhhorodskoho natsionalnoho universytetu. Seriia: Mizhnarodni ekonomichni vidnosyny ta svitove hospodarstvo - Scientific Bulletin of Uzhhorod National University. Series: International Economic Relations and World Economy, 42,* 125-129. (In Ukrainian). Retrieved from http://www.visnyk-econom.uzhnu.uz.ua/archive/42_2022ua/24.pdf

43. Schmidt, A., & Engelen, B. (2020). The ethics of nudging: An overview. *Philosophy Compass, 15*(4), e12658. https://doi.org/10.1111/phc3.12658

44. SHRM. (2024). *How to build a strong organizational culture*. Retrieved from https://www.shrm.org/topics-tools/tools/toolkits/understanding-developing-organizational-culture

45. Social Engineer. (2022). *Cybersecurity and cognitive bias*. Retrieved from https://www.social-engineer.com/cybersecurity-and-cognitive-bias/

46. Spiekermann, S., & Winkler, T. (2020). *Value-based engineering for ethics by design*. https://doi.org/10.2139/ssrn.3598911

47. Stahie, S. (2025). *WRECKSTEEL campaign uses fake HR emails to spy on Ukrainian government systems*. Hot for Security. Retrieved from https://www.bitdefender.com/en-us/blog/hotforsecurity/wrecksteel-fake-emails-spy-ukrainian

48. Stambulska, K., & Peredalo, K. (2022). Corporate Culture, its Essence, Types and Role in the Development of the Organization. *Efektyvna ekonomika - Effective Economy*, 1. (In Ukrainian). https://doi.org/10.32702/2307-2105-2022.1.204

49. Tadesse Bogale, A., & Debela, K. (2024). Organizational culture: a

systematic review. *Cogent Business & Management*, *11*(1). https://doi.org/10.1080/23311975.2024.2340129

50. Valta, M., & Maier, C. (2025). Digital nudging: A systematic literature review, taxonomy, and future research directions. *ACM SIGMIS Database for Advances in Information Systems, 56*(1), 101-125. https://doi.org/10.1145/3715966.3715973

51. Winkler, T., & Spiekermann, S. (2019). Twenty years of value sensitive design: A review of methodological practices. *Ethics and Information Technology, 23,* 17-21. https://doi.org/10.1007/s10676-018-9476-2

52. Yudin, O., Matviichuk-Yudina, O., & Suprun, O. (2021). Information-Psychological War and Technologies of Social Engineering. *Naukoyemni tekhnolohii – Science-intensive Technologies, 50*(2), 130-139. (In Ukrainian). https://doi.org/10.18372/2310-5461.50.15684

53. Zakharchyn, H. (2023). Rol komunikatsiinoi kultury v upravlinni personalom [The role of communication culture in personnel management]. *Ekonomika ta suspilstvo – Economics and Society*, 56. (In Ukrainian). https://doi.org/10.32782/2524-0072/2023-56-125

54. Zhanbo, L., & Qiongyao, L. (2021). Research on Organizational Human Resources Knowledge Structure Model Based on the Perspective of System Engineering Methodology. *Social Sciences, 10*(2), 48. https://doi.org/10.11648/j.ss.20211002.12

55. Zhmurko, A. (2024). Sotsialna inzheneriia yak zahroza kiberbezpetsi: metody zapobihannia ta zakhystu [Social engineering as a threat to cybersecurity: Prevention and protection methods]. *Pedahohika okhorony zdorovia ta bezpeky – Pedagogy of Health Protection and Safety, 9*(1), 37-42. (In Ukrainian). https://doi.org/10.31649/2524-1079-2024-9-1-037-042