

TARAS SHEVCHENKO NATIONAL UNIVERSITY OF KYIV
(FACULTY OF INFORMATION TECHNOLOGY,
FACULTY OF COMPUTER SCIENCE AND CYBERNETICS)
NATIONAL TECHNICAL UNIVERSITY OF UKRAINE
“IGOR SIKORSKY KYIV POLYTECHNIC INSTITUTE”
VIKTOR GLUSHKOV INSTITUTE OF CYBERNETICS OF THE NAS OF UKRAINE
INSTITUTE FOR INFORMATION RECORDING OF THE NAS OF UKRAINE
INSTITUTE OF SOFTWARE SYSTEMS OF THE NAS OF UKRAINE
THE COUNCIL OF YOUNG SCIENTISTS OF THE FACULTY OF COMPUTER SCIENCE AND
CYBERNETICS AND THE FACULTY OF INFORMATION TECHNOLOGY OF
TARAS SHEVCHENKO NATIONAL UNIVERSITY OF KYIV
PUBLIC ASSOCIATION «COGNITIVE RESEARCH»

XI INTERNATIONAL CONFERENCE

Information Technology and Implementation (Satellite)

21 November, 2025

Conference Proceedings

Kyiv

2025

Vadym Ziuziun

PhD, Associate Professor of the Department of Technologies Management

Oleksii Korytnyi

Master's degree student of the Department of Technologies Management

Taras Shevchenko National University of Kyiv

RISK CONTROLLING AND MONITORING SOFTWARES THAT CONSIDER HUMAN BIAS AS A MAJOR RISK

Abstract. This research argues that a specialized IS offers a structured, quantitative, and proactive framework to not only identify and assess typical technical and financial risks but also to meticulously manage these complex human factors. The system must integrate advanced features like behavioral analytics and lessons-learned repositories to move beyond simple checklists. Furthermore, this paper provides a concise overview of existing risk management programs and platforms currently available in the market. By critically analyzing the capabilities and limitations of commercial-off-the-shelf (COTS) solutions – and noting their common deficiencies in handling the nuance of human risk – this work solidifies the requirement for a tailored IS that can effectively bridge the gap between technical risk assessment and human-centric project realities.

Keywords: information system, risk management, IT projects, human-induced risks, cognitive biases, risk management software.

Previous works have established the foundational importance of addressing human-induced risks in technology management, moving beyond generic risk models [2-3] and how can we assess them in IT projects [1]. This need for proactive management requires a critical comparison with existing solutions; thus, we must now analyse current commercial and proprietary software programs available for tracking IT project risks.

SHERPA human factor reliability [4] provides its software for pharmaceutical, oil & gas, defence and healthcare sectors. The SHERPA human factors software package integrates several different modules to help you stay on top of all the most critical tasks and improve human reliability:

- **Risk ranking:** generates risk matrices to indicate great concern areas and set priorities in risk management. The module allows to evaluate the most common zone for a human error, output risk index and likelihood and suggests tasks prioritization.
- **Hierarchical task analysis and human factors risk analysis:** conducts human factor risk assessments, including COMAH Safety Cases required by the Health and Safety Executive in the UK; Hierarchical Task Analysis (HTA) to systematically document tasks, PHEA etc.

Apart from this SHERPA also provides Failure Mode / Performance Influencing Factors (PIF) Analysis and Swimlane or Sequentially Timed Event Plot (STEP) Diagramming.

The NIST AI Risk Management Framework (AI RMF) [5] is a voluntary framework developed by the U.S. National Institute of Standards and Technology (NIST). Its primary purpose is to help organizations across both the public and private sectors manage the specific risks associated with designing, developing,

deploying, and using Artificial Intelligence (AI) products and systems. The AI RMF is distinct from traditional IT risk frameworks because it focuses on trustworthiness in addition to security. It aims to improve the ability to incorporate considerations such as:

- Fairness and Bias.
- Transparency and Explainability.
- Validity and Reliability.

Although the system does not directly specialise on human bias risks and their indication/evaluation, AI RMF outlines their 4 key pillars (Govern, Map, Measure, Manage) as to prevent extensive human risks with AI regulatory data governance. In order to start the “machine” the Institution suggests the next steps taken:

- 1) Establish a Strong Governance Structure.
- 2) Conduct a Comprehensive Risk Assessment.
- 3) Implement Risk Management Strategies.
- 4) Monitor and improve.
- 5) Knowledge sharing.

Summarizing, various worldwide practices incorporate standard time-checked risk management models and approaches to define and manage risks in projects. However, with AI slightly taking over the edge of new insights, people also adopt the machine learning to optimise and control the common project management to a new level, which predicts the outcome. Thus, it supports our previous statements [2-3] about the necessity to create an information system for risk management of it projects and make an artificial intelligence its core module of analysis and prediction

References:

1. Ziuziun V. Analysis of possible risks in human resources management in IT companies. 5th International Scientific and Practical Internet Conference «Integration of Education, Science and Business in Modern Environment: Summer Debates», August 3-4, 2023. P.79-81. URL: <http://www.wayscience.com/konferentsiya-5-3-4-serpnya-2023/>. Access date: 23.10.2024
2. Korytnyi O., Ziuziun V. Digital Ways of Controlling Risk Management and Assessment in Projects. 2st International scientific and practical conference «Information Systems and Technology: Results and Prospects» (IST 2025), Kyiv, Ukraine, 2025, p. 167-171.
3. Korytnyi O., Ziuziun V. Justification of the need to create an information system for risk management of IT projects. Information Technology and Implementation (Satellite): Conference Proceedings, November 21, 2024, Kyiv, Ukraine / Taras Shevchenko National University of Kyiv and [etc]; Vitaliy Snytyuk (Editor). – Kyiv: Publishing House «Caravela» – P. 236-237.
4. SHERPA Human Reliability 2025. Official website. <https://www.humanreliability.com/human-factors-software/#demo>.
5. Leia Manchanda, CISO Perspectives: A Practical Guide to Implementing the NIST AI Risk Management Framework (AI RMF). September 30, 2025. Field CISO.

<i>Danylo Rybachok, Andrii Yarmilko. ARCHITECTURAL PARADIGMS FOR CONTESTED ENVIRONMENTS: A COMPARATIVE ANALYSIS OF MONOLITHIC AND MICROSERVICE DESIGNS FOR MODERN MILITARY LOGISTICS</i>	296
<i>Bohdan Semonov, Sergiy Pogorilyy. SEMANTIC ENRICHMENT OF SOURCE CODE IDENTIFIERS THROUGH AUTOMATIC ABBREVIATION EXPANSION FOR COMMIT MESSAGE GENERATION</i>	299
<i>Oleksandr Timinskyi, Denys Liashenko. ANALYSIS OF THE DEVELOPMENT DIRECTIONS OF COMPUTER SCIENCE MODELS IN THE FIELD OF IT PROJECT MANAGEMENT</i>	303
<i>Oleksandr Timinskyi, Artem Yurechko. COMPARATIVE ANALYSIS OF IT PROJECT MANAGEMENT METHODOLOGIES IN THE DEVELOPMENT OF WEB- AND CONTENT-ORIENTED SYSTEMS</i>	307
<i>Diana Vashchilina, Olena Vashchilina, Anastasiia Nikolaienko. STRUCTURING EDUCATIONAL IT PROJECTS WITH NPM WORKSPACES</i>	311
<i>Oleksii Vedmiediev. ASPECTS OF PROACTIVE ORGANIZATIONAL DEVELOPMENT OF CONSTRUCTION PROJECT TEAMS WHEN IMPLEMENTING VALUE HARMONIZATION WITH THE IT CONTEXT</i>	314
<i>Oleksandr Voitenko, Valerii Hudov. DAMPEN-TURBULENCE MODELS OF PROJECT PORTFOLIO MANAGEMENT TEAM OF A GENERAL CONTRACTING ORGANIZATION AND THEIR IT SUPPORT</i>	318
<i>Oleg Zhulkovskyi, Inna Zhulkovska, Anastasiia Shevchenko. OPTIMIZING NUMERICAL THERMAL SIMULATIONS THROUGH DATA-LEVEL PARALLELISM</i>	322
<i>Vadym Ziuziun, Tetiana Danilina. FEATURES OF DATABASE STRUCTURE DEVELOPMENT FOR THE "PETHEALTH" MOBILE APPLICATION</i>	324
<i>Vadym Ziuziun, Oleksii Korytnyi. RISK CONTROLING AND MONITORING SOFTWARES THAT CONSIDER HUMAN BIAS AS A MAJOR RISK</i>	326
<i>Vadym Ziuziun, Yuliia Koziuk. KEY CHALLENGES AND RISK MITIGATION STRATEGIES FOR UKRAINIAN IT STARTUPS DURING THE WAR</i>	328
<i>Vadym Ziuziun, Daria Shcherbak. MANAGEMENT OF QUALITY IN AN IT PROJECT DURING THE DEVELOPMENT OF THE ECOLOGICAL WEB APPLICATION "СМАЧХОГО"</i>	330