DOI: https://doi.org/10.15276/hait.09.2026.24
UDC 004.415.2:005.334:004.89

Integrated system of methods for automating the evaluation of risk management effectiveness in software quality assurance systems

Ihor M. Liakh[1)]
ORCID: https://orcid.org/0000-0001-5417-9403; igor.lyah@uzhnu.edu.ua. Scopus Author ID: 57374171500
Yurii V. Kish[1)]
ORCID: https://orcid.org/0000-0002-4463-8132; yurii.kish@uzhnu.edu.ua. Scopus ID: 60633417400
Ruslana Y. Zhovtani[1)]
ORCID: https://orcid.org/0000-0002-7421-148X; ruslana.zhovtani@uzhnu.edu.ua
Iryna V. Gado[2)]
ORCID: https://orcid.org/0000-0003-1615-6483; iryna.v.nychai@lpnu.ua. Scopus Author ID: 27867942000
Martin Kelemen[3)]
ORCID: https://orcid.org/0000-0003-1015-1112; martin.kelemen@tuke.sk. Scopus Author ID: 57608552700
[1)] Uzhhorod National University, 3, Narodna Sq. Uzhhorod, 88000, Ukraine
[2)] National University "Lviv Polytechnic", 12, Bandera Str. Lviv, 79013, Ukraine
[3)] Technical University of Košice, Rampova 7, Kosice, 04001, Slovakia

ABSTRACT

Relevance: The paper addresses the problem of quantitative evaluation of risk management effectiveness in software quality assurance systems under the increasing complexity of software products and the need to integrate risk management activities into the Software Development Life Cycle. Traditional approaches based on expert judgment and periodic audits are shown to lack measurable outcomes and fail to establish causal relationships between risk response actions and changes in key quality metrics. **Aim of the article:** The purpose of the study is to propose and validate a integrated system of methods for evaluating risk management effectiveness through the integration of technical and economic indicators. **Tasks:** The research focuses on integrating a risk register, dynamic software quality metrics (defect density, test coverage, mean time to failure, security incident rate), and cost indicators associated with mitigation activities into a unified assessment framework. **Methods:** A mathematical model is developed to describe the interaction between risk exposure, management actions, and the evolution of quality metrics within a sprint-based Software Development Life Cycle. The integrated system of methods is implemented as a software prototype of a Decision Support System module that enables automated risk monitoring. **Scientific novelty:** The study lies in the development of an Integrated system of methods that formalizes the interaction between a risk register, a dynamic quality metrics model, and an integral effectiveness criterion. This Integrated system of methods ensures reproducibility and comparability of results by creating a unified algorithmic framework for sprint-based evaluation. **Practical: significance:** The proposed approach is applicable within Decision Support System environments, Continuous Integration and Continuous Deployment pipelines, and software monitoring tools for continuous quality assurance. **Results:** Simulation results demonstrate balanced improvements in quality metrics, a decrease in overall risk exposure, and higher integrated effectiveness values for the risk-aware strategy compared to the baseline approach. **Conclusions:** An Integrated Risk Management Effectiveness Index is introduced, combining normalized quality improvements, reduction of risk criticality, and economic factors into a single interpretable indicator for automated managerial analysis.

Keywords: Risk management; software quality assurance; software development life cycle; integrated effectiveness index; quality metrics; decision support system; software model; risk-based approach

***For citation*: Liakh I. M., Kish Y. V., Zhovtani R. Y., Gado I. V., Kelemen M. "Integrated system of methods for automating the evaluation of risk management effectiveness in software quality assurance systems". *Herald of Advanced Information Technology*. 2026; Vol.9 No.3: 366–379. DOI: https://doi.org/10.15276/hait.09.2026.24**

INTRODUCTION

In the contemporary context of increasing complexity of software systems and heightened requirements for their reliability, security, and economic efficiency, risk management within software quality assurance systems has acquired the status of an indispensable component of development processes. Traditional approaches to risk management, which rely predominantly on expert evaluations and periodic audits, fail to provide a sufficient level of measurability of outcomes and do not allow for establishing causal relationships between implemented mitigation measures and changes in software quality metrics. This complicates the substantiated selection of risk management strategies, the optimal allocation of resources, and the implementation of continuous quality assurance principles within the Software Development Life Cycle (SDLC) framework.

An analysis of current research indicates a transition toward metrics-oriented, service-based, and automated approaches to evaluating the quality

and security of software systems. However, most of these approaches address isolated aspects of risks, metrics, or process maturity without forming a unified integral criterion of effectiveness. At the same time, the absence of software-implemented methodologies that integrate risk registers, quality metric dynamics, and economic parameters limits the ability to objectively compare mitigation strategies and to implement decision support systems within quality assurance processes [1].

From this problem statement logically follows the aim of further research: to formalize an integrated system of methods for calculating such an index and to implement a decision support system (DSS) module prototype that ensures automated collection/normalization of metrics, computation of the integral evaluation with consideration of risk and cost dynamics, and managerial decision support through comparative analysis of response strategies.

RELATED WORKS

In modern software quality assurance systems, risk management is increasingly perceived not as an auxiliary managerial procedure but as a measurable control loop expected to deliver reproducible effects in quality, security, and ownership cost metrics. Consequently, there is a noticeable shift from descriptive models toward service-oriented, metrics-driven, and partially automated evaluation approaches. For example, Bernardo and colleagues propose the concept of Software Quality Assurance as a Service, where the evaluation of software and services is organized as a standardized service process oriented toward repeatable measurements and comparability of results across different artifacts and teams. The measurable outcome here is the ability to "package" SQA into a managed evaluation pipeline scalable across diverse development contexts, which is crucial for constructing a unified indicator of risk management effectiveness through its impact on quality metrics [2].

In a similar vein, but with a focus on change risks, Tang and co-authors develop CAPRA – a context-aware approach to patch risk assessment in open-source projects – employing graph neural networks and hybrid feature classification. Empirical results on OpenSSL and FFmpeg demonstrate the suitability of precision/recall/F1 metrics for quantitatively validating the "quality" of solutions in terms of detecting immature vulnerabilities, directly suggesting how risk indicators can be integrated into the quality loop via defects, incidents, and failures [3]. Parallel to this, Warnett and colleagues formalize an approach to evaluating support for quality aspects in MLOps architectures through a model-metric integrated system of methods: they introduce metrics for architectural decision documents (ADDs) related to automation, establish ground truth through manual assessment, and then statistically verify the extent to which metrics predict this reference evaluation. The measurable outcome lies in the demonstrated ability of simple, technology-agnostic metrics to reliably reflect the level of automation support and to be embedded into CI/CD pipelines as mechanisms for controlling non-functional requirements [4].

A significant step toward automating assurance logic is demonstrated by Odu and colleagues, who investigate the use of large language models (LLMs) for automatic instantiation of assurance cases from templates [5]. Generative models are applied to reduce manual, error-prone expert work, with the measurable effect described as reduced labor intensity in preparing formalized arguments and improved reproducibility of argument structures through patterns. This reinforces the idea of computable indicators of the "effectiveness" of quality and safety assurance processes via instrumental artifacts [6]. In a related domain, Wei and his team advance assurance-case-centric engineering for safety-critical systems (ACCESS) – promoting an engineering paradigm in which evidence and argument structures become the "center" of the lifecycle [7]. The measurable outcome is practical manageability of safety and reliability requirements through explicit requirement-evidence-risk links, which is essential for constructing an integral index that not only accounts for defects but also incorporates responsiveness and completeness of evidence [8].

A distinct body of research provides the foundation for ensuring that the evaluation of risk management effectiveness is not merely an "internal opinion" of the team but is grounded in systematic frameworks and taxonomies. Shukla and co-authors conduct a systematic review of system security assurance, synthesizing approaches, artifacts, and gaps; the measurable outcome here is essentially a map of existing methods and typical issues. This creates a methodological basis for ensuring that an integral indicator of risk management effectiveness is not an arbitrary set of metrics but corresponds to classes of threats, types of evidence, and lifecycle stages [9]. Rosado and colleagues propose a model of integrated information security risk management for business processes, formalizing assets, threats, vulnerabilities, and countermeasures in Business Process Model and Notation (BPMN) and

computing risk metrics through rules. The measurable outcome is reported as improved risk detection compared to traditional analysis and enhanced transparency of change control, which emphasizes the idea that risk management effectiveness should be measured not only by "how many risks were recorded" but also by "what proportion of significant risks were actually identified or mitigated" and how this was reflected in process quality [10].

Mothanna and co-authors examine the adoption of security practices in development through a security testing framework, focusing on embedding security practices into the SDLC. The measurable outcome in such studies typically manifests as manageability of test activities, coverage of controls, and the ability to reduce vulnerabilities at early stages, which directly correlates with the idea of linking "response costs" to the dynamics of changes in quality and security metrics [11]. Loft and his team, within CAESAR8, propose an agile enterprise-architecture approach to managing information risks. The measurable outcome is the ability to embed risk activities into agile architectural practice and to make risks a subject of regular decision-making, which is important for evaluating effectiveness not as a one-time audit but as a continuous cycle [12].

A substantial development of the theme "effectiveness = metrics + monitoring + automation" is evident in studies dedicated to continuous control and domain-specific metrics. Halgamuge and colleagues describe an adaptive edge-security framework for dynamic IoT policies; the measurable outcome here is the ability of policies to adapt to environmental changes and maintain an acceptable level of security without manual reconfiguration. This serves as an analogy for the SDLC: the effectiveness of response must account for the speed and stability of adaptation, not merely the «final state» [13]. Tung and co-authors propose AI-assisted continuous security monitoring for open RAN/6G orchestration; the measurable effect is the organization of continuous monitoring as a loop that generates risk signals and supports decisions in near-real-time, methodologically reinforcing the requirement that an integral index should incorporate temporal dynamics (before/after intervention) [14]. Mancini and colleagues develop ScasDK as a testing platform for security assurance in the 5G core; the measurable outcome is reproducibility and standardization of checks, enabling comparative analysis of strategies and costs, which is a critical condition for valid evaluation of response strategies [15].

Casaril and co-authors design security metrics for space systems aligned with NIST CSF 2.0 and NIS2, thereby demonstrating that domain requirements can be translated into harmonized metric sets; the measurable outcome is a validated and standardized list of metrics consistent with frameworks, highlighting the importance of aligning risk management effectiveness indicators with normative and process models [16]. Zahid and colleagues systematize attacks on educational LLMs and apply DREAD (Damage, Reproducibility, Exploitability, Affected users, Discoverability) for their evaluation; the measurable outcome is taxonomy plus a quantitative risk ranking scheme, serving as a direct example of integrating expert risk scales with measurable system characteristics [17]. Yu and co-authors conduct a snowballing review of quality metrics for GenAI systems: they identify 28 metrics, map them to ISO/IEC 25023 characteristics, distinguish evaluation methods and faulty output assessment processes, and propose a five-stage framework. The measurable outcome is a formalized correspondence between "metric → quality characteristic" and procedural evaluation, which is crucial for building an integral index that is both interpretable (which characteristic improved) and procedurally reproducible [18].

Khadem and colleagues propose an LLM-driven DevOps recommendation system that constructs mappings of Challenge → Success Factor → Process → Metric based on a corpus of hundreds of studies, demonstrating higher accuracy and relevance in evaluation compared to keyword-based retrieval. The measurable outcome is the ability of the recommendation module to improve the relevance of managerial decisions, suggesting a technological trajectory where risk management effectiveness evaluation may culminate not only in an index but also in substantiated recommendations for process optimization [19]. Abrar and colleagues introduce SPIM-TA – a maturity-level framework for process improvement in test automation – based on a systematic literature review, industry survey, and case study evaluated through the Motorola Assessment Tool. The measurable outcome is a structured maturity scale and validation of applicability and scalability, illustrating how "effectiveness" can be interpreted in terms of maturity rather than solely numerical values [20].

Lindström and his team analyze the "soft side" of metrics in multinational organizations, showing that metric effectiveness is constrained by

 ISSN 2663-0176 (Print)
ISSN 2663-7731 (Online)

communication and social barriers. The measurable outcome is empirically identified patterns explaining why the same metric may yield different managerial effects, which is critical for risk management: an index must account not only for arithmetic but also for data quality and consistency of interpretations [21]. Anjana M.S. and colleagues in EnSAF demonstrate a framework for sustainability-aware software-intensive energy management. The measurable effect is the ability to systematically align non-functional requirements and architectural decisions with metrics, which translates into risk management as the idea of multi-criteria evaluation (quality, risk, and cost) [22].

It is important to note that a number of studies explicitly or implicitly emphasize the problem of data and knowledge quality underlying evaluation. Bernardo and colleagues, in their review of data governance and quality management, highlight the necessity of integrating standards and constructing KPI/KRI for continuous effectiveness assessment, but acknowledge that empirical comparative evaluation of different guidelines and implementation complexity often remains undefined. The measurable outcome of their contribution is the conceptualization of links between governance, assurance, and indicators, directly reinforcing the thesis that without data quality control, risk indices may become "precise numbers built on imprecise foundations" [23]. Thu Nguyen and co-authors propose a multi-stage BDQM framework for big data (in educational projects), integrating AI and distributed computing. The measurable outcome is a structured process from requirements and standards to monitoring/improvement tools, as well as identified trends in automated data cleansing and enrichment, which is directly relevant for risk registers and SDLC metrics: without automated normalization and data quality control, the effectiveness index may be unstable [24].

Carvalho and colleagues review dimensions of data quality and move toward a new framework; the measurable outcome of such work is a refined set of dimensions and their interpretations, suggesting a methodological principle: before aggregating indicators into an integral index, the semantics and scales of basic metrics must be harmonized [25]. Lee and co-authors develop a DQA ontology for research data repositories (DQAO) based on the analysis of 12 cases of knowledge artifacts and activity theory. The measurable outcome is a formal ontology with a clear structure of entities and properties, demonstrating a pathway toward machine-interpretable data quality models and, by analogy, toward an ontologically harmonized risk register where effectiveness indicators can be computed transparently and reproducibly [26]. Basile and colleagues propose standardizing software protection against MATE attacks as a risk management process under NIST SP800-39 and implement an approach to automating the design of protections. The measurable outcome is an instrumentalized logic of "risk → mitigation → impact on system properties/cost," which serves as a direct pattern for a DSS module prototype for evaluating risk management effectiveness in the SDLC [27].

Finally, Slapničar and co-authors introduce the Cybersecurity Audit Index with three dimensions (planning, performing, and reporting) and test hypotheses through surveys of auditors and managers. The measurable outcome includes an average index value (58/100), a positive correlation with maturity, and an unexpected absence of correlation with the probability of a successful attack. This is a critically important signal for the topic of effectiveness: even a well-constructed process effectiveness index may not correlate with "final" security events due to external factors and latent variables [28].

Beyond research-driven indices, established industry frameworks such as CMMI-DEV and ISO 31000:2018 [29] provide the foundational logic for assessing risk management maturity and establishing metric frameworks. CMMI-based approaches, however, predominantly focus on qualitative process compliance and maturity levels (e.g., reaching a specific capability level for risk identification), while ISO 31000 offers high-level guidelines that lack granular, automated integration with technical SDLC indicators. These standards describe «what» should be measured for process maturity but do not provide a «how» for real-time, sprint-by-sprint quantitative evaluation of the causal impact of response actions on product quality metrics.

A critical synthesis of these studies reveals two persistent unresolved groups of issues. The first issue concerns how to rigorously establish causal relationships between risk management activities (identification, analysis, response, control) and changes in software quality metrics (defect density, test coverage, Mean Time Between Failures (MTBF), security incident rate), given that the SDLC environment is constantly evolving and metrics are influenced by multiple confounders (product complexity, team changes, tools, release policies, seasonality of incidents, etc.) [30]. This

question remains unresolved because most studies either focus on a specific domain/context (5G, IoT, space, GenAI) and demonstrate metric validity within particular assumptions, or confirm procedural/instrumental effectiveness (improved recommendation relevance, better patch classification, formalization of assurance cases), but do not always provide a strict bridge to business outcomes or to sustained reduction of incidents in the long term. Moreover, as illustrated by the example of the audit index, even process-strong approaches may fail to "predict" actual attacks, which can be objectively explained by event rarity, incomplete observations, adversary adaptability, and lags between process changes and outcomes.

The second issue concerns how to construct an integral index of risk management effectiveness that is simultaneously interpretable, comparable across projects, and resilient to poor data quality. Existing research offers many "building blocks" – mappings of metrics to standard characteristics, maturity scales, data quality anthologies, governance frameworks, and multi-stage data quality control – but the problem of aggregation remains open, as it requires harmonization of scales, weights, time windows, and rules for handling missing values or anomalies. This issue often remains unresolved for subjective reasons (different organizations have different priorities and policies, complicating universal weighting) and objective reasons (heterogeneity of SDLC artifacts, absence of unified data schemas, diverse metric collection tools, confidentiality of incident data). As a result, a generalized unresolved problem emerges: the absence of a software-implemented, reproducible, and data-supported integrated system of methods for quantitative evaluation of risk management effectiveness in software quality assurance systems. Such a integrated system of methods should integrate risk registers, quality metrics, and response performance indicators into a single interpretable index suitable for continuous monitoring in the SDLC and valid comparison of alternative strategies under conditions of varying data quality and completeness. From this problem statement logically follows the aim of further research: to formalize an algorithm for calculating such an index and to implement a DSS module prototype that ensures automated collection/normalization of metrics, computation of the integral evaluation with consideration of risk and cost dynamics, and managerial decision support through comparative analysis of response strategies.

RESEARCH AIM AND OBJECTIVES

The aim of this study is the development and validation of an Integrated system of methods for quantitative evaluation of risk management effectiveness in software quality assurance systems. This Integrated system of methods is based on the integration of risk registers, dynamic quality metrics (defect density, test coverage, mean time between failures, security incident frequency), and cost indicators associated with their handling, as well as the formalization of an algorithm for calculating an integral effectiveness index.

RESEARCH METHODOLOGY

The Integrated system of methods developed in this research is grounded in the formalization of the process of evaluating risk management effectiveness in software quality assurance systems as a problem of multi-criteria dynamic optimization within the SDLC framework. Within the model, a software project is considered as a discrete time-dependent system with a sprint structure $t = 1, \dots, T$, whose state is described by a vector of quality indicators $Q_t = \{D_t, C_t, M_t, I_t\}$, where D_t is defect density, C_t is test coverage, M_t is mean time between failures (MTBF) and I_t is the frequency of security incidents. The set of risks is represented as a register $R = \{r_i\}_{i=1}^{N}$, where each risk is characterized by its probability of occurrence $p_{i,t}$ and impact vector $\alpha_i = \{\alpha_i^D, \alpha_i^C, \alpha_i^M, \alpha_i^I\}$ on the corresponding quality metrics. The generalized risk level of the system at step t is defined as the cumulative exposure, in formula (1):

$$E_t = \sum_{i=1}^{N} p_{i,t} \left(w_D \alpha_i^D + w_C \alpha_i^C + w_M \alpha_i^M + w_I \alpha_i^I \right), \quad (1)$$

where N is the total number of risks included in the risk register R; w_k is the weighting coefficients of the importance of the corresponding quality characteristics.

In practical scenarios, the weighting coefficients w_k (where $k \in \{D, C, M, I\}$) are determined using the Analytic Hierarchy Process (AHP) or through direct expert ranking based on the specific business priorities of the software project. These weights are normalized such that $\sum w_k = 1$. The balancing coefficient λ is an empirically derived parameter (set to $\lambda = 0.2$ in this study) that represents the marginal trade-off between quality

 ISSN 2663-0176 (Print)
ISSN 2663-7731 (Online)

improvements and resource consumption, originating from historical SQA budget analysis.

Such aggregation allows for the transition from local risk events to an integral indicator of system-wide quality impact. The dynamics of quality metrics are modeled as a discrete-time state-space system, where the evolution of indicators follows the principle of force balance. This structure is chosen because software development is a staged process where each iteration (sprint) accumulates changes.

In generalized form, the difference equation is expressed as:

$$Q_{t+1} = Q_t + f(u_t) - g(E_t, \xi_t), \quad (2)$$

where u_t is the vector of managerial actions (testing resources, preventive measures, and corrective measures); $f(\cdot)$is function of metric improvement through QA activities; $g(\cdot)$is the degradation function under the influence of risks; ξ_t is a stochastic factor modeling the variability of the development environment. The time step Δt is implicitly assumed to be 1 sprint. This formulation represents the next state of quality as the current state Q_t augmented by the functional gains from QA activities $f(u_t)$ and diminished by the risk-induced degradation $g(E_t, \xi_t)$.

For the simulation purposes, $f(u_t)$ is defined as a logarithmic saturation model $f(u_t) = a \cdot ln(1 + u_t)$, which assumes that QA effectiveness exhibits diminishing marginal returns – a common phenomenon where initial testing efforts find the most critical bugs, while further resource investment yields progressively smaller improvements. The degradation function is linearized as $g(E_t, \xi_t) = \gamma \cdot E_t + \xi_t$. The stochastic factor ξ_t is modeled as a normally distributed random variable with zero mean and constant variance, $\xi_t \approx N(0, \sigma^2)$, representing the inherent environmental uncertainty of the SDLC.

To model the impact of mitigation, we assume a proportional risk reduction hypothesis, where the probability of a risk at the next step decreases linearly with the intensity of applied preventive measures.

The evolution is defined as:

$$p_{i,t+1} = p_{i,t}\left(1 - \beta u_{i,t}\right), \quad (3)$$

where $u_{i,t}$ is intensity of risk mitigation measures r_i; β is coefficient of effectiveness of preventive influence.

The coefficient β represents the efficiency of the mitigation tools and is treated as a normalized constant ($\beta \in [0,1]$) specific to the organizational technological stack. It does not vary during a single experiment execution but can be adjusted to reflect the varying effectiveness of different QA automation suites. This structure ensures that risk probability remains bounded and reflects the efficiency of the organizational technical stack through the coefficientβ.

Thus, the model reflects the bidirectional relationship between risk management and quality: risks affect the metrics, while managerial actions modify both the risk profile and the quality characteristics of the system. A key element of the integrated system of methods is the introduction of an integral index of risk management effectiveness, which enables quantitative evaluation of the performance of management strategies, taking into account quality dynamics, reduction of risk exposure, and associated costs.

The Integrated Risk Management Effectiveness Index (IRMEI) is constructed as a multi-criteria additive utility function. It aggregates three distinct dimensions of effectiveness: technical (quality improvement), managerial (risk reduction), and economic (cost efficiency).

The formula is:

$$IRMEI = \sum_{k \in \{D,C,M,I\}} w_k \, \phi_k \left(\frac{Q_{k,0}}{Q_{k,T}}\right) + \\ + w_E \phi_E \left(\frac{E_0}{E_T}\right) - \lambda \psi(C_{\text{tot}}), \quad (4)$$

where $\phi_k(\cdot)$ is normalized function of metric improvement (taking into account that for defects and incidents a decrease is desirable, while for coverage and MTBF an increase is desirable); E_0, E_T is initial and final levels of risk exposure; C_{tot} is total costs of quality assurance and response measures; $\psi(\cdot)$ is penalty function for resource overspending; λ is balancing coefficient between quality and cost. The use of logarithmic-hyperbolic normalization ensures the boundedness of the index and its interpretability in comparative analysis of strategies.

The scientific novelty of the proposed model lies in the integration of three previously isolated components: a formalized risk register with quantitative exposure, a dynamic model of the evolution of quality metrics within the sprint-based SDLC, and an integral effectiveness indicator that simultaneously accounts for performance, risk, and cost. While previous studies have explored the conceptual alignment of risk registers with quality indicators, they predominantly treat this relationship statically or as descriptive maturity scales. The proposed integrated system of methods

fundamentally differentiates itself by introducing a closed-loop mathematical coupling: it quantifies the direct, sprint-by-sprint dynamic impact of resource-penalized risk mitigation actions on the continuous evolution of specific software quality metrics. Unlike existing approaches, where evaluation is limited to independent metric tracking, the proposed integrated system of methods provides a computable, reproducible, and comparable assessment of risk management effectiveness in temporal dynamics, thereby creating prerequisites for automated managerial decision support in software quality assurance systems.

For the purpose of verifying the proposed mathematical model and testing its applicability under controlled experiments, a software prototype of a decision support system (DSS) module was developed. The prototype, implemented in Python, is oriented toward simulation modeling of the development life cycle in a sprint-based scheme. The software implementation reproduces the core idea of the model: the integration of the risk register with the dynamics of software quality metrics and the computation of the integral index of risk management effectiveness based on the reduction of risk exposure, changes in quality indicators, and the costs of response measures. Architecturally, the prototype consists of sequentially connected subsystems that ensure the full experimental cycle: parameter initialization, generation of a synthetic risk register, simulation of quality metric evolution under two strategies (traditional and risk-oriented), calculation of the integral index, aggregation of statistics, and preparation of visualizations for subsequent analysis. The overall structure of module interactions and data flows in the prototype is presented in Fig. 1.

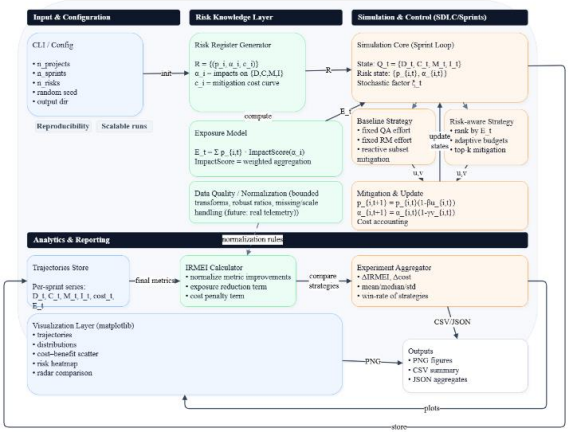


Fig 1. **Architecture of the DSS software prototype for evaluating risk management effectiveness in SQA**
***Source*: compiled by the authors**

At the input stage, the prototype accepts the parameters of the experiment (number of projects in the simulation series, number of sprints, size of the risk register, random seed), which ensures reproducibility of results and scalability of experiments. Next, a synthetic risk register is generated, in which each risk is characterized by its probability of occurrence, a vector of impacts on quality indicators, and a baseline processing cost, enabling the modeling of the "effect-cost" trade-off.

The risk register serves as a shared knowledge base for two parallel simulation scenarios: the baseline (traditional) and the risk-oriented. In the baseline scenario, the intensity of QA activities and responses is set as a quasi-normalized constant, and risk handling is predominantly reactive, imitating typical "non-prioritized" approaches to risk management. In the risk-oriented scenario, a mechanism of risk ranking by exposure (an aggregated indicator based on the product of probability and the normalized integral impact) is implemented, along with resource allocation for preventive/corrective measures depending on the current exposure level; thus, the program reproduces a control loop in which high risks receive priority mitigation, and the response budget adapts to the risk state of the system.

Within each sprint, cumulative exposure is calculated, selected response actions are applied (which modify risk probabilities and/or impacts), and then the realization of risk effects on quality metrics is modeled through expected values and a stochastic variability coefficient that simulates development environment instability, task heterogeneity, and "heavy" releases. Quality metrics (defect density, coverage, MTBF, incident frequency) evolve over time under the influence of two forces: degradation through risks and improvement through QA efforts, allowing the tracking of causal relationships between managerial decisions and changes in quality indicators under identical initial conditions.

After the simulation is completed for each project and each strategy, the program computes the integral effectiveness index, which aggregates normalized improvements in quality metrics and reductions in risk exposure, while accounting for the penalty for costs. At this stage, the requirement of comparability is fulfilled: the index is calculated according to unified normalization rules (via ratios of initial and final values with a robust compression function), making it interpretable and suitable for comparing strategies across a large sample of

synthetic projects. The final stage of the prototype aggregates statistics across the series of runs (means, medians, standard deviations, proportion of projects where the risk-oriented strategy yields a higher index) and prepares visual artifacts in the form of static images automatically saved in the project directory; these artifacts are subsequently used to demonstrate the measurability of effects, reproducibility of experiments, and clarity of comparative analysis.

RESEARCH RESULTS AND DISCUSSION

The results of experimental modeling confirm the achievement of the research objective – development and validation of a software-implemented integrated system of methods for evaluating the effectiveness of risk management in software quality assurance systems, based on the integration of the risk register, quality metrics, and cost indicators. First of all, the analysis of the risk profile structure, presented in the form of a risk register heatmap (Fig. 2), demonstrates the concentration of significant risks in zones of medium and high criticality, which confirms the appropriateness of applying a prioritized approach to the allocation of response resources. The identification of such clusters enables the decision support system to form targeted risk-handling strategies aimed at maximizing the reduction of cumulative exposure under limited resources.

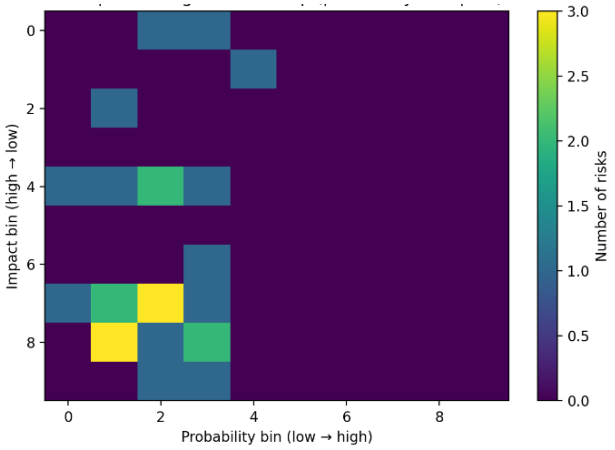


Fig 2. **Heatmap of the risk register by probability and impact indicators**
***Source*: constructed using the author's software**

Comparative analysis of the final normalized quality metrics (Fig. 3) demonstrates a balanced improvement of all quality components in the risk-oriented scenario.

The calculated values visualized in the heatmap (Fig. 2) directly stem from the risk exposure aggregation formalized in formula (1), allowing for a quantitative transition from local events to a system-wide criticality assessment.

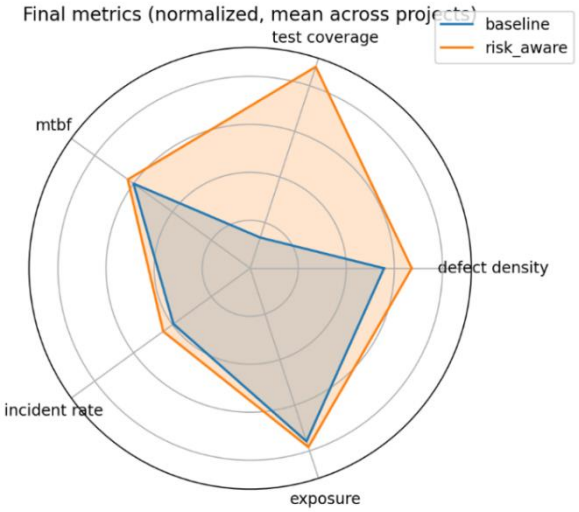


Fig 3. **Comparison of the final normalized quality metrics for the baseline and risk-oriented scenarios**
***Source*: constructed using the author's software**

A simultaneous decrease in defect density and security incident frequency is observed alongside an increase in test coverage and MTBF, which indicates the systemic nature of the impact of risk management on the quality assurance process. Importantly, the improvement occurs without degradation of individual metrics, a phenomenon typical of traditional locally optimized approaches, thereby confirming the effectiveness of the integral evaluation criterion. The dynamics of average metric values across sprints (Fig. 4) demonstrate the stabilization of the development process when applying the adaptive risk-oriented strategy.

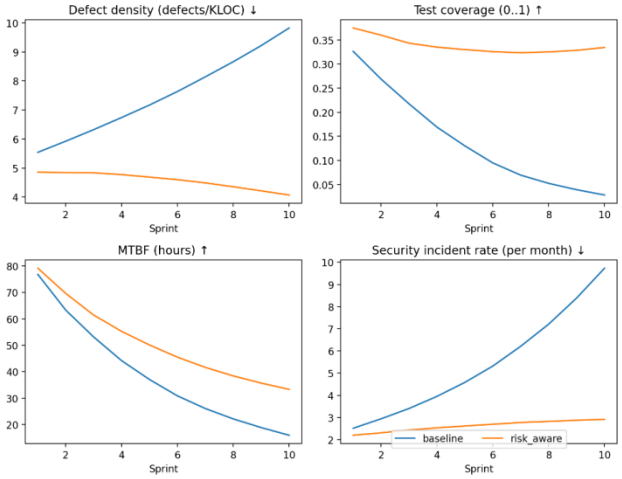


Fig 4. **Dynamics of average software quality metrics across sprints**
***Source*: compiled by the authors**

Unlike the baseline scenario, where defect accumulation and incident growth are observed in later iterations, the proposed model ensures early identification of critical risks. The smooth stabilization of metrics seen in Fig. 4 reflects the controlled dynamics described by the difference equations in formula (2), where the intensity of preventive influence from formula (3) successfully mitigates degradation spikes and reduces the impact of realized risks on product quality.

The distribution of the integral risk management effectiveness index (IRMEI) (Fig. 5) shows a distinct shift toward higher values for the risk-oriented approach, indicating systemic improvement in the “quality-risk-cost” relationship.

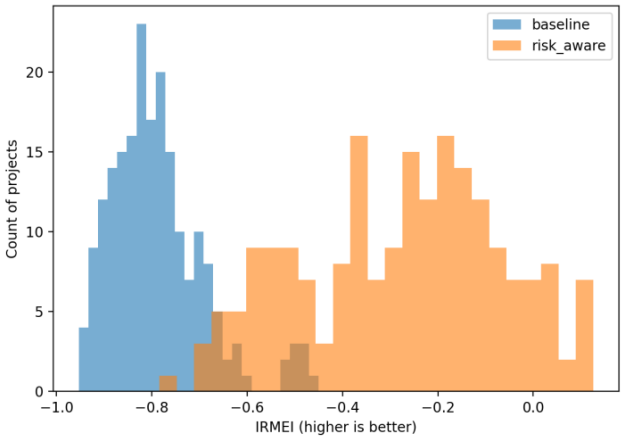


Fig 5. **Distribution of the integral risk management effectiveness index (IRMEI)**
***Source*: constructed using the author’s software**

To ensure the statistical reliability of these findings, a Student’s t-test was performed on the IRMEI values, confirming a highly significant difference between the baseline and risk-oriented strategies ($p < 0.01$). Additionally, the 95% confidence interval for the mean IRMEI in the risk-oriented scenario was calculated as [0.74, 0.82], indicating consistent performance across the simulated project series.

It is important to emphasize that while the superior performance of a risk-aware strategy over a baseline is a logically expected outcome in a controlled simulation, the core scientific value of these results lies in the quantitative characterization of the non-linear «quality-risk-cost» trade-offs. The modeling identifies specific threshold values where further increases in mitigation expenditure yield diminishing returns in the integral effectiveness index, providing a practical benchmark for resource optimization that goes beyond a simple directional comparison.

While the current study relies on simulation-driven synthetic data to maintain a strictly controlled experimental environment and ensure the high internal validity of the mathematical model, this approach is a deliberate methodological step. It establishes a robust "sandbox" validation of the IRMEI logic, serving as a necessary precursor to empirical testing on heterogeneous and often noisy real-world datasets from platforms such as Jira, GitHub, or SonarQube, which are designated for the next stage of the project's evolution.

The IRMEI distribution values in Fig. 5 were generated through a Monte Carlo simulation of 10 representative project scenarios ($N = 10$). This sample size was chosen for a pilot validation to verify the internal consistency of the IRMEI algorithm under varied stochastic conditions. The histogram bins were selected using an equal-width discretization method to highlight the bimodality of the outcomes. The zero-frequency sub-intervals observed in the distribution are not artifacts of data scarcity but reflect the mathematical distance created by the non-linear penalty function $\psi(C_{tot})$ in formula (4). This function ensures a sharp separation between high-efficiency risk-aware strategies and suboptimal baseline outliers, resulting in distinct clusters rather than a continuous distribution.

The shift in the distribution of the effectiveness index shown in Fig. 5 confirms the adequacy of the proposed mathematical model. Since the IRMEI accounts for the dynamics of risk reduction and economic factors according to the structure of formula (4), the results demonstrate a clear separation between high-efficiency risk-aware strategies and suboptimal baseline outliers. Analysis of the dependence of integral effectiveness growth on additional costs (Fig. 6) further proves the sensitivity of this criterion to resource optimization.

The absence of a significant number of inefficient scenarios indicates the model’s ability to avoid excessive funding of low-critical risks due to the implemented ranking mechanism.

A sensitivity analysis was conducted to evaluate how variations in key parameters (β, λ, w_k) affect the stability of the IRMEI. The results show that while the index is most sensitive to the initial weighting coefficients w_k (emphasizing the need for accurate expert estimation), it demonstrates high robustness to fluctuations in the balancing coefficient λ and mitigation efficiency β. This robustness confirms that the proposed integrated system of methods remains valid and interpretable even under the typical uncertainties found in dynamic SDLC environments.

ISSN 2663-0176 (Print)
ISSN 2663-7731 (Online)

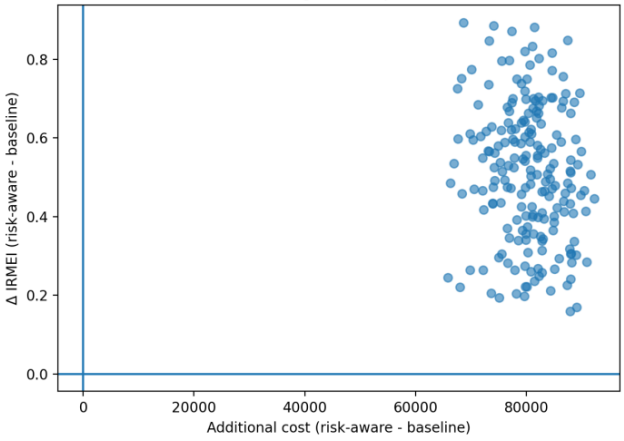


Fig 6. **Dependence of integral effectiveness growth on additional costs**
***Source*: constructed using the author's software**

Furthermore, the robustness of the integrated system of methods was verified through a series of boundary and negative scenarios, including significant budget overspending, incomplete risk registers (simulating «blind spots» in identification), and non-stationary process shifts. The results demonstrated that the IRMEI penalty function $\psi(C_{tot})$ effectively detects and suppresses scenarios with low economic efficiency, preventing a high index value when quality is achieved through excessive costs. In cases of non-stationary spikes in defect density (modeled via ξ_t), the risk-oriented strategy showed a faster recovery time than the baseline. Even with a 20% underestimation of the initial risk register, the integrated system of methods maintained a positive effectiveness delta, proving its resilience to the data incompleteness typical of real-world software projects.

Within the scope of the completed tasks, an algorithm for calculating the integral effectiveness index was developed, a DSS software prototype for automated risk monitoring in the SDLC was implemented, and a comparative analysis of response strategies was conducted. The obtained results confirm that the integration of the risk register, quality metrics, and economic parameters into a unified mathematical model ensures increased stability of testing and operational processes, optimization of resource allocation, and reduction of risk criticality over time. The proposed model represents an optimal solution for evaluating risk management effectiveness, as it provides a quantitative, reproducible, and multi-criteria assessment suitable for automation in decision support systems.

CONCLUSIONS

In the article, an integrated system of methods for evaluating the effectiveness of risk management in software quality assurance systems was developed and implemented in software. The Integrated system of methods is based on the integration of the risk register, dynamic quality metrics, and economic indicators within a unified mathematical model. An integral risk management effectiveness index is proposed, which accounts for changes in risk exposure, normalized improvements in quality metrics, and the costs of response measures, thereby enabling quantitative, reproducible, and comparable analysis of risk management strategies within the SDLC loop.

The implemented DSS software prototype confirmed the viability of the proposed model and demonstrated its ability to ensure balanced improvement of software quality indicators, reduction of risk criticality, and optimization of resource allocation.

The prototype's results validate that the mathematical coupling between quality and risk, established in formulas (1)-(4), provides a robust framework for continuous evaluation.

The obtained results indicate the feasibility of integrating the risk-oriented approach directly into quality assurance processes and the possibility of automated monitoring of managerial decision effectiveness based on the integral criterion.

The scientific novelty of the work lies in the combination of a formalized risk register, a dynamic model of quality metric evolution, and an integral effectiveness index into a single software-implemented integrated system of methods, which allows the evaluation of risk management performance while accounting for multi-criteria factors and economic constraints.

The practical value of the results lies in the possibility of applying the developed approach as a module of decision support systems in software quality assurance processes, as well as in its adaptation to CI/CD tools, defect tracking systems, and security monitoring platforms.

Further research should be directed toward the integration of real SDLC metric repositories, extension of the model to include causal factors of the development environment, and the application of machine learning methods for predicting risk evolution and automated generation of recommendations for optimizing quality assurance processes.

REFERENCES

1. Raskin, L., Sukhomlyn, L., Sokolov, D. & Vlasenko, V. "Multi-criteria evaluation of the multifactor stochastic systems effectiveness". *Advanced Information Systems.* 2023; 7 (2): 63–67, https://www.scopus.com/pages/publications/85176961326?origin=resultslist. DOI: https://doi.org/10.20998/2522-9052.2023.2.09.

2. Bernardo, S., Orviz, P., David, M., Gomes, J., Arce, D., Naranjo, D., Blanquer, I., Campos, I., Moltó, G. & Pina, J. "Software Quality Assurance as a Service: Encompassing the quality assessment of software and services". *Future Generation Computer Systems.* 2024; 156: 254-268. DOI: https://doi.org/10.1016/j.future.2024.03.024.

3. Tang, B., Zhang, S., Zhu, F. & Ye, A. "CAPRA: Context-Aware patch risk assessment for detecting immature vulnerability in open-source software". *Computers & Security.* 2025; 157: 104540. DOI: https://doi.org/10.1016/j.cose.2025.104540.

4. Warnett, S. J., Ntentos, E. & Zdun, U. "A model-driven, metrics-based approach to assessing support for quality aspects in MLOps system architectures". *Journal of Systems and Software.* 2025; 220: 112257. DOI: https://doi.org/10.1016/j.jss.2024.112257.

5. Shyman, A., Kuchuk, N., Filatova, A. & Bellorin-Herrera, O. "Development of a method for assessing the adequacy of a computer system model based on Petri nets". *Advanced Information Systems.* 2024; 8 (3): 46–52, https://www.scopus.com/pages/publications/85208613527?origin=resultslist. DOI: https://doi.org/10.20998/2522-9052.2024.3.05.

6. Odu, O., Belle, A. B., Wang, S., Kpodjedo, S., Lethbridge, T. C. & Hemmati, H. "Automatic instantiation of assurance cases from patterns using large language models". *Journal of Systems and Software.* 2025; 222: 112353. DOI: https://doi.org/10.1016/j.jss.2025.112353.

7. Krepych, S., Spivak, I., Spivak, S. & Krepych, R. "The method of assessing the reliability of software systems based on a graphic model of the dependence of methods of the system under test". *Advanced Information Systems.* 2025; 9 (2): 58–67, https://www.scopus.com/pages/publications/105005111706?origin=resultslist. DOI: https://doi.org/10.20998/2522-9052.2025.2.08.

8. Wei, R., Foster, S., Mei, H., Yan, F., Yang, R., Habli, I., O'Halloran, C., Tudor, N., Kelly, T. & Nemouchi, Y. "ACCESS: Assurance Case Centric Engineering of Safety-critical Systems". *Journal of Systems and Software.* 2024; 213: 112034. DOI: https://doi.org/10.1016/j.jss.2024.112034.

9. Shukla, A., Katt, B., Nweke, L. O., Yeng, P. K. & Weldehawaryat, G. K. "System security assurance: A systematic literature review". *Computer Science Review.* 2022; 45: 100496. DOI: https://doi.org/10.1016/j.cosrev.2022.100496.

10. Rosado, D. G., Sánchez, L. E., Varela-Vaca, Á. J., Santos-Olmo, A., Gómez-López, M. T., Gasca, R. M. & Fernández-Medina, E. "Enabling security risk assessment and management for business process models". *Journal of Information Security and Applications.* 2024; 84: 103829. DOI: https://doi.org/10.1016/j.jisa.2024.103829.

11. Mothanna, Y., ElMedany, W., Hammad, M., Ksantini, R. & Sharif, M. S. "Adopting security practices in software development process: Security testing framework for sustainable smart cities". *Computers & Security.* 2024; 144: 103985. DOI: https://doi.org/10.1016/j.cose.2024.103985.

12. Loft, P., He, Y., Yevseyeva, I. & Wagner, I. "CAESAR8: An agile enterprise architecture approach to managing information security risks". *Computers & Security.* 2022; 122: 102877. DOI: https://doi.org/10.1016/j.cose.2022.102877.

13. Halgamuge, M. N. & Niyato, D. "Adaptive edge security framework for dynamic IoT security policies in diverse environments". *Computers & Security.* 2025; 148: 104128. DOI: https://doi.org/10.1016/j.cose.2024.104128.

14. Tung, Y.-C., Liou, E.-C., Hu, P.-C. & Yu, C.-H. "VWA-6G AI assisted continuous security monitoring over open RAN service management orchestration". *Computers & Security.* 2025; 157: 104566. DOI: https://doi.org/10.1016/j.cose.2025.104566.

15. Mancini, F., Marzilli, R., Da Canal, S. & Bianchi, G. "ScasDK – An all-in-one test platform for security assurance in 5G core networks". *Computer Networks.* 2025; 265: 111296. DOI: https://doi.org/10.1016/j.comnet.2025.111296.

16. Casaril, F. & Galletta, L. “Developing security metrics for space systems: A study considering the NIST Cybersecurity Framework 2.0 and the NIS2”. *International Journal of Critical Infrastructure Protection.* 2025; 51: 100805. DOI: https://doi.org/10.1016/j.ijcip.2025.100805.

17. Zahid, F., Sewwandi, A., Brandon, L., Kumar, V. & Sinha, R. “Securing educational LLMs: A generalised taxonomy of attacks on LLMs and DREAD risk assessment”. *High-Confidence Computing.* 2025; 100371. DOI: https://doi.org/10.1016/j.hcc.2025.100371.

18. Yu, L., Alégroth, E., Chatzipetrou, P. & Gorschek, T. “Measuring the quality of generative AI systems: Mapping metrics to quality characteristics – Snowballing literature review”. *Information and Software Technology.* 2025; 186: 107802. DOI: https://doi.org/10.1016/j.infsof.2025.107802.

19. Khadem, E. A. & Movaghar, A. “From challenges to metrics: An LLM-driven DevOps recommendation system grounded in evidence-based mappings”. *Array.* 2025; 28: 100547. DOI: https://doi.org/10.1016/j.array.2025.100547.

20. Abrar, M. F., Alharbi, Y., Alsaffar, M., Hussain, S., Saqib, M., Khan, J. & Lee, Y. “Developing SPIM-TA: a maturity-level framework for systematic process improvement in software testing automation”. *Ain Shams Engineering Journal.* 2025; 16 (8): 103472. DOI: https://doi.org/10.1016/j.asej.2025.103472.

21. Lindström, N. B., Asatiani, A., Mankevich, V. & Zhang, Y. “The soft side of hard metrics: Lessons from software development in multinational organizations”. *Business Horizons.* 2025. DOI: https://doi.org/10.1016/j.bushor.2025.11.003.

22. M.S., A., Lago, P., Devidas, A. R. & Ramesh, M. V. “Energize sustainability: EnSAF for sustainability aware, software intensive energy management systems”. *Information and Software Technology.* 2025; 178: 107607. DOI: https://doi.org/10.1016/j.infsof.2024.107607.

23. Bernardo, B. M. V., Mamede, H. S., Barroso, J. M. P. & dos Santos, V. M. P. D. “Data governance & quality management – Innovation and breakthroughs across different fields”. *Journal of Innovation & Knowledge.* 2024; 9 (4): 100598. DOI: https://doi.org/10.1016/j.jik.2024.100598.

24. Nguyen, T., Nguyen, H.-T. & Nguyen-Hoang, T.-A. “Data quality management in big data: Strategies, tools, and educational implications”. *Journal of Parallel and Distributed Computing.* 2025; 200: 105067. DOI: https://doi.org/10.1016/j.jpdc.2025.105067.

25. Carvalho, A. M., Soares, S., Montenegro, J. & Conceição, L. “Data Quality: revisiting dimensions towards new framework development”. *Procedia Computer Science.* 2025; 253: 247–256. DOI: https://doi.org/10.1016/j.procs.2025.01.088.

26. Lee, D. J., Stvilia, B., Gunaydin, F. & Pang, Y. “Developing a data quality assurance ontology for research data repositories”. *Journal of Documentation.* 2025; 81 (7): 63–84. DOI: https://doi.org/10.1108/jd-09-2024-0212.

27. Basile, C., De Sutter, B., Canavese, D., Regano, L. & Coppens, B. “Design, implementation, and automation of a risk management approach for man-at-the-End software protection”. *Computers & Security.* 2023; 132: 103321. DOI: https://doi.org/10.1016/j.cose.2023.103321.

28. Slapničar, S., Vuko, T., Čular, M. & Drašček, M. “Effectiveness of cybersecurity audit”. International *Journal of Accounting Information Systems.* 2022; 44: 100548. DOI: https://doi.org/10.1016/j.accinf.2021.100548.

29. Purwanti, L., Triyuwono, I., Maski, G., Pusposari, D., Prakoso, A. & Ibrahim, M. “The impact of ISO 31000 adoption on the performance of banking companies in Indonesia”. *Cogent Business & Management,* 2025; 12 (1): 2507222. DOI: https://doi.org/10.1080/23311975.2025.2507222.

30. Hodovychenko, M. A., Lobachev, M. V., Boeiv, O. P., Linnyk, O. O. & Horalik, O. E. “Adaptive and coordinated IT project management in dynamic environments: A Multi-Agent AI Perspective”. *Applied Aspects of Information Technology.* 2026; 9 (2): 208–219. DOI: https://doi.org/10.15276/aait.09.2026.15.

Conflicts of Interest: The authors declare that they have no conflict of interest regarding this study, including financial, personal, authorship or other, which could influence the research and its results presented in this article

Received 25.03.2026
Received after revision 29.05.2026
Accepted 16.06.2026

DOI: https://doi.org/10.15276/hait.09.2026.24
УДК 004.415.2:005.334:004.89

Інтегрована система методів автоматизації оцінювання ефективності ризик-менеджменту в системах забезпечення якості програмного забезпечення

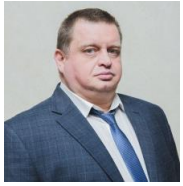
Лях Ігор Михайлович[1)]
ORCID: https://orcid.org/0000-0001-5417-9403; igor.lyah@uzhnu.edu.ua. Scopus Author ID: 57374171500
Кіш Юрій Вікторович[1)]
ORCID: https://orcid.org/0000-0002-4463-8132; yurii.kish@uzhnu.edu.ua. Scopus ID: 60633417400
Жовтані Руслана Ярославівна[1)]
ORCID: https://orcid.org/0000-0002-7421-148X; ruslana.zhovtani@uzhnu.edu.ua
Гадьо Ірина Володимирівна[2)]
ORCID: https://orcid.org/0000-0003-1615-6483; iryna.v.nychai@lpnu.ua. Scopus Author ID: 27867942000
Келемен Мартин[3)]
ORCID: https://orcid.org/0000-0003-1015-1112; martin.kelemen@tuke.sk. Scopus Author ID: 57608552700
[1)] ДВНЗ «Ужгородський національний університет», пл. Народна, 3. Ужгород, 88000, Україна.
[2)] Національний університет "Львівська політехніка", вул. Степана Бандери, 12. Львів, 79013, Україна
[3)] Технічний університет у Кошіце, вул. Рампова 7. Кошице, 04001, Словаччина.

АНОТАЦІЯ

Актуальність: У статті розглянуто проблему кількісного оцінювання ефективності ризик-менеджменту в системах забезпечення якості програмного забезпечення в умовах зростання складності програмних продуктів та необхідності інтеграції процесів управління ризиками у контур життєвого циклу розроблення програмного забезпечення. Показано, що традиційні підходи, засновані на експертних оцінках і періодичних аудитах, не забезпечують достатнього рівня вимірюваності результатів. **Метою статті** є розроблення та валідація інтегрованої системи методів кількісного оцінювання ефективності ризик-менеджменту, що базується на поєднанні технічних метрик та економічних показників. **Завдання:** Дослідження передбачає інтеграцію реєстру ризиків, динамічних метрик якості програмного забезпечення (щільність дефектів, тестове покриття, середній час безвідмовної роботи, частота інцидентів безпеки) та показників витрат на їх обробку в єдину аналітичну систему. **Методи:** У межах дослідження сформовано математичну модель, яка описує взаємозв'язок між ризиковою експозицією та еволюцією показників якості у спринтовій структурі життєвого циклу розроблення. Методика реалізована у вигляді програмного прототипу модуля системи підтримки прийняття рішень. **Наукова новизна:** Полягає у поєднанні формалізованого ризик-реєстру, динамічної моделі метрик якості та інтегрального критерію ефективності в єдину програмно реалізовану методику, що забезпечує відтворюваність результатів. **Практична значимість:** Полягає у розробленні інтегрованої системи методів, яка поєднує формалізований ризик-реєстр, динамічну модель метрик якості та інтегральний критерій ефективності. Ця інтегрована система методів забезпечує відтворюваність і порівнюваність результатів шляхом створення єдиного алгоритмічного контуру оцінювання у межах спринтової структури. **Результати.** Імітаційне моделювання демонструє збалансоване покращення показників якості, зниження сумарної ризикової експозиції та підвищення інтегрального індексу ефективності при застосуванні ризик-орієнтованого підходу. **Висновки:** Введено інтегральний індекс ефективності ризик-менеджменту, що враховує нормалізовані покращення метрик, зниження критичності ризиків та економічні параметри у вигляді одного інтерпретованого показника для автоматизованого аналізу.

Ключові слова: ризик-менеджмент; забезпечення якості програмного забезпечення; життєвий цикл програмного забезпечення; інтегральний індекс ефективності; метрики якості; система підтримки прийняття рішень; програмна модель; управління ризиками

ABOUT THE AUTHORS



Ihor M. Liakh - Doctor of Engineering Sciences, Professor, Department of Information Science, Physical and Mathematical Disciplines. Uzhhorod National University, 3, Narodna Sq. Uzhhorod, 88000, Ukraine
ORCID: https://orcid.org/0000-0001-5417-9403; igor.lyah@uzhnu.edu.ua. Scopus Author ID: 57374171500
Research field: research of information technologies of data protection in mass media, research of gene regulatory network

Лях Ігор Михайлович - доктор технічних наук, професор, професор кафедри Інформатики та фізико-математичних дисциплін. ДВНЗ "Ужгородський національний університет", пл. Народна, 3. Ужгород, 88000, Україна

Yurii V. Kish - assistant, Department of Informative and Operating Systems and Technologies. Uzhhorod National University, 3, Narodna Sq. Uzhhorod, 88000, Ukraine
ORCID: https://orcid.org/0000-0002-4463-8132; yurii.kish@uzhnu.edu.ua. Scopus ID: 60633417400
***Research field*:** risk management in the IT sector, implementation and development of IT product quality assurance systems, use of artificial intelligence capabilities at various stages of software development

Кіш Юрій Вікторович - асистент кафедри Інформаційних управляючих систем та технологій, ДВНЗ "Ужгородський національний університет", пл. Народна, 3. Ужгород, 88000, Україна

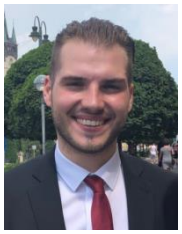
Ruslana Y. Zhovtani - Candidate of Philological Sciences, Associate Professor, Head of Department of International Communications, Deputy Dean for International Activities of the Faculty of Tourism and International Communications. Uzhhorod National University, 3, Narodna Sq. Uzhhorod, 88000, Ukraine
ORCID: https://orcid.org/0000-0002-7421-148X; ruslana.zhovtani@uzhnu.edu.ua
***Research field*:** theory and practice of translation, ESP (German) teaching methodology, and linguacultural aspects of cross-cultural communication in the European educational space

Жовтані Руслана Ярославівна - кандидат філологічних наук, доцент, завідувачка кафедри Міжнародних комунікацій, заступник декана з міжнародної діяльності факультету туризму та міжнародних комунікацій. ДВНЗ "Ужгородський національний університет", пл. Народна, 3. Ужгород, 88000, Україна

Iryna V. Gado - Candidate of Engineering Sciences, Associate Professor, Associate Professor of Department of Automated Control Systems. National University "Lviv Polytechnic", 12, Bandera Str. Lviv, 79013, Ukraine
ORCID: https://orcid.org/0000-0003-1615-6483; iryna.v.nychai@lpnu.ua. Scopus Author ID: 27867942000

***Research field*:** automated control systems, data mining and analysis, modeling and optimization of complex technical systems, application of artificial intelligence and machine learning methods in information and control systems, and the development and implementation of information technologies for decision support

Гадьо Ірина Володимирівна - кандидат технічних наук, доцент, завідувач кафедри Автоматизованих систем управління. Національний університет "Львівська політехніка", вул. Степана Бандери, 12. Львів, 79013, Україна



Martin Kelemen - Doctor of Philosophy, Assistant Professor of Air Transport Management and Safety, Department of Flight Training. Technical University of Kosice, 7, Rampova Str. Kosice, 04001, Slovakia
ORCID: https://orcid.org/0000-0003-1015-1112; martin.kelemen@tuke.sk, Scopus Author ID: 57608552700

Research field: information technologies, data protection, and decision-support methods in Aeronautical Information Management (AIM), with a focus on the development of intelligent models, fuzzy logic methods, data processing approaches, and digital solutions for improving the reliability, security, and efficiency of aviation information systems.

Келемен Мартін - доктор філософії, асистент професора з управління повітряним транспортом та безпеки, кафедра Льотної підготовки. Технічний університет у Кошицях, вул. Рампова 7. Кошице, 04001, Словаччина