https://doi.org/10.31891/2219-9365-2025-83-6
УДК 004.056.5:004.415

SAVCHUK Bohdan
Anbosoft LLC
https://orcid.org/0009-0009-8360-6385
e-mail: bogd.sav@gmail.com

DEVELOPMENT OF SOFTWARE QUALITY ASSURANCE PERFORMANCE INDICATORS FOR ASSESSING CYBER RESILIENCE OF SYSTEMS

Cyber resilience is becoming an essential property of modern information systems, particularly in critical infrastructure and enterprise environments where the ability to resist, absorb, and recover from cyberattacks is vital. While existing security frameworks emphasize threat detection, incident response, and risk management, the influence of software quality assurance (SQA) processes on cyber resilience remains insufficiently studied. This paper addresses this gap by proposing a structured methodology for evaluating the impact of SQA practices on the cyber resilience of software systems through a set of normalized and weighted quality indicators.

The proposed approach combines elements of established software quality models such as ISO/IEC 25010 and CMMI with cybersecurity standards and frameworks including NIST, MITRE ATT&CK, and CIS Controls. It introduces a unified system of metrics that includes test coverage, defect density, response time to vulnerabilities, mean time to recovery, code complexity, and review frequency. These metrics were empirically assessed in a controlled experimental environment using widely adopted DevSecOps tools such as Jenkins, SonarQube, and Allure Report.

The experiment involved two software development configurations: a basic setup with minimal quality assurance and an enhanced one featuring systematic testing, regular code reviews, and developer training. The findings show that improvements in SQA practices led to a significantly higher level of cyber resilience. The enhanced configuration demonstrated better performance in all key metrics, especially in reducing recovery time and increasing the percentage of test coverage.

The results confirm a strong correlation between effective software quality assurance and the system's capacity to withstand cyber threats. The proposed model can be used to support decision-making in secure software development, providing a foundation for automated monitoring of resilience based on existing quality assurance infrastructure. Future research will focus on expanding the metric set and applying the methodology to systems with diverse architectures and operational contexts.

Keywords: cyber resilience, software quality assurance, security metrics, DevSecOps, test coverage, recovery time.

САВЧУК Богдан
Anbosoft LLC

ФОРМУВАННЯ ПОКАЗНИКІВ ЕФЕКТИВНОСТІ SOFTWARE QUALITY ASSURANCE ДЛЯ ОЦІНЮВАННЯ КІБЕРСТІЙКОСТІ СИСТЕМ

Кіберстійкість є ключовим показником надійності сучасних інформаційних систем, однак вплив процесів забезпечення якості програмного забезпечення (SQA) на її рівень досі вивчено недостатньо. У статті запропоновано методику оцінювання кіберстійкості на основі сукупності нормалізованих і зважених метрик якості, що відображають глибину тестування, складність коду, щільність дефектів, час реагування на вразливості та частоту рев'ю. Підхід базується на поєднанні моделей якості ПЗ (ISO/IEC 25010, CMMI) та стандартів кібербезпеки (NIST, MITRE ATT&CK, CIS Controls), що дозволяє формалізувати взаємозв'язок між процесами розробки й рівнем стійкості до атак.

Метод реалізовано в експериментальному середовищі з використанням Jenkins, SonarQube та Allure Report. Проведене дослідження довело, що підвищення рівня SQA-практик суттєво покращує стійкість системи до кібератак. Запропонована модель може бути інтегрована у процеси безпечної розробки ПЗ для моніторингу показників стійкості на основі вже наявної QA-інфраструктури. Результати відкривають перспективу автоматизованого управління кіберстійкістю на основі даних із практик контролю якості.

Ключові слова: кіберстійкість, забезпечення якості ПЗ, метрики безпеки, DevSecOps, тестове покриття, час відновлення

Стаття надійшла до редакції / Received 12.07.2025
Прийнята до друку / Accepted 16.08.2025

STATEMENT OF THE PROBLEM

In today's conditions of rapid development of digital technologies and the increase in the number of cyberattacks, ensuring the resilience of information systems to destructive influences is becoming particularly relevant [1]. The concept of cyber resilience encompasses the ability of a system to counteract cyberattacks, quickly recover from incidents, and ensure continuity of operation even in adverse conditions [2, 3]. One of the key factors that directly affects the level of cyber resilience is the quality of software, which determines reliability, security, and the ability to adapt to changes. In the practice of developing software systems, Software Quality Assurance (SQA) plays an important role – a set of measures and processes aimed at ensuring that software meets specified requirements and quality standards [4]. However, despite significant scientific and practical achievements in the field of software quality assurance, most models lack a focus on the relationship between quality characteristics and cyber resilience. Typically, the assessment of the effectiveness of SQA processes is carried out on the basis of internal technical or organizational

indicators that do not take into account the system's ability to counteract modern cyber threats [5]. At the same time, the development of a methodology for forming such indicators that would allow assessing how quality control measures affect the overall system's resistance to attacks remains a relevant research problem.

Growing requirements for cyber protection, the implementation of DevSecOps approaches, and the use of critical information systems in the infrastructure of the public and private sectors create the need to create a comprehensive model for assessing the effectiveness of SQA, focused on ensuring cyber resilience [6]. This requires the identification of relevant metrics, their quantitative expression, and practical implementation in the development and testing processes.

The purpose of the study is to form a system of indicators for the effectiveness of software quality assurance processes, focused on the quantitative assessment of the cyber resilience of information systems.

THEORETICAL BACKGROUND AND RELATED WORKS

SQA and cyber resilience of systems remain the subject of active scientific discussion. The authors of [7] investigated the role of software quality control processes in reducing vulnerabilities that can be exploited by attackers, emphasizing the need to integrate SQA measures into cyber defense strategies. In [8], they propose to consider cyber resilience as the result of the interaction of technical, process and organizational factors, in particular, focusing on the preventive value of testing and static code analysis. Existing standards, such as CMMI (Capability Maturity Model Integration), describe in detail the maturity levels of software development processes, but they lack direct guidelines for cyber threats. In [9], it is emphasized that even a high level of maturity according to CMMI does not guarantee resilience to modern attacks. At the same time, the ISO/IEC 25010 model [10] formalizes the concept of software quality through characteristics such as reliability, security, portability, etc., which partially overlap with aspects of cyber resilience. However, as researchers [11] point out, these characteristics do not form a complete picture of the relationship between code quality and the system’s ability to withstand complex cyber threats.

Approaches to assessing cyber resilience, proposed by organizations such as NIST [12], MITRE [13] and CIS Controls [14], focus mainly on threat detection, risk management and rapid system recovery. In [15], an attempt is made to combine these approaches with DevSecOps practices, but the authors acknowledge the difficulties of quantitatively measuring the effect of implementing software quality control mechanisms.

Modern metrics in SQA, in particular Defect Density, Test Coverage, Code Complexity, Mean Time To Recovery (MTTR), are of significant value for assessing the quality of development. In [16], an analysis of the effectiveness of these metrics in the context of incident resilience is presented, but it is found that only some of them have the potential to be extrapolated to cyber resilience indicators. The authors of [17] investigated an attempt to correlate the level of automated testing and the probability of exploiting vulnerabilities, but the results turned out to be dependent on the specifics of the project.

Thus, although there is a significant amount of research in the areas of software quality assurance and cyber resilience, a gap between these areas still remains. The lack of integrated models that take into account SQA metrics as a component of cyber resilience assessment complicates the implementation of unified approaches to building reliable and secure systems. This emphasizes the need to develop a methodology that combines quantitative SQA metrics with cyber resilience practices for their further practical application.

EXPERIMENTAL METHODOLOGY

To form a system of quantitative indicators of the effectiveness of software quality assurance processes, which allow indirectly assessing the level of cyber resilience of an information system, a methodological approach was proposed that combines the concepts of software quality models, modern SQA metrics and conceptual foundations of cyber resilience in accordance with the NIST SP 800-160 and MITRE ATT&CK standards.

At the first stage, a decomposition of SQA processes into categories was carried out: process (development control, review, audit), technical (testing tools, automation, static analysis), organizational (development security policies, personnel training). For each category, a set of relevant metrics was determined that have the potential to influence cyber resilience (Table 1).

Table 1

Categorization of SQA metrics with potential impact on cyber resilience

Category	Metrics	Expected impact on cyber resilience
Process	Code review frequency, f_r (number/week)	Straight
Technical	Code coverage by tests, C_t (%)	Straight
Technical	Average complexity of functions, CC (Cyclomatic Complexity)	Reversed
Organizational	Number of trainings conducted, T_s (number/month)	Straight
Technical	Mean Time to Recovery, MTTR (hours)	Reversed

To construct a generalized assessment, a functional model is proposed that reflects the relationship between the set of SQA metrics and the level of cyber resilience of the system. The cyber resilience score in our model is

denoted as R_c and is determined through a normalized linear combination of weight metrics (1).

$$R_c = \sum_{i=1}^{n} w_i \cdot M_i \quad (1)$$

where M_i is the normalized value of the i-th metric, wi is the influence weight determined by expert analysis taking into account the analysis of OWASP Top-10 vulnerabilities and typical exploitation paths in MITRE ATT&CK.

The weight coefficients were determined using the analytical hierarchy process (AHP), which included a pairwise comparison of the importance of metrics by 12 experts in the field of cybersecurity and software development. The resulting pairwise comparison matrix was checked for consistency (consistency index $C_i = 0{,}083 < 0.1$), which indicates an acceptable level of reliability of the results.

Fig. 1 shows the logical sequence of stages in forming an assessment of the cyber resilience of the system based on software quality assurance indicators. The scheme reflects the process of transition from collecting the initial SQA metrics to calculating the aggregated integral indicator, including the stages of normalization, determination of weight coefficients and the final calculation of the level of system resilience to cyberattacks.

To ensure reproducibility of calculations, all metrics were reduced to the interval [0;1] using mini-max normalization (2).

$$M_i = \frac{X_i - X_i^{min}}{X_i^{max} - X_i^{min}} \quad (2)$$

where X_i is the actual value of the metric; X_i^{min}, X_i^{max} are the minimum and maximum values established empirically based on the results of monitoring real SQA processes.

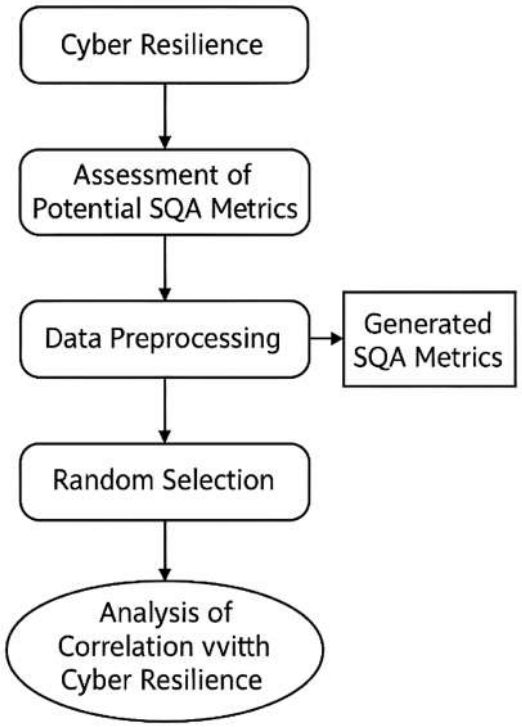

Fig. 1. Generalized scheme for forming a cyber resilience assessment based on SQA processes

The proposed model allows for quantitative comparison of systems with different levels of SQA practices implementation and to determine which of them make the greatest contribution to the system's resilience to cyberattacks.

EXPERIMENT RESULTS

To verify the effectiveness of the proposed model for assessing cyber resilience, an experiment was implemented in a test environment built on the basis of an open-source incident management and logging system, Fig. 2. The test system was deployed in a Docker virtual environment with the connection of CI/CD modules, static code analysis (SonarQube), task tracking (Jira-like interface) and an automated testing system with HTML report generation. Based on two different configurations of SQA processes – basic (traditional) and improved (with active implementation of DevSecOps practices) – the necessary metrics were collected and the generalized cyber resilience index R_c was calculated according to (1).

Fig. 2. Test environment interface when collecting SQA metrics

Figure 2 shows a fragment of the environment in which software quality control was carried out: a panel for automatically launching unit tests, indicators of code coverage by tests, a report on the number of defects detected by the static analysis tool, and an event log with response times to detected vulnerabilities.

During the five-week development cycle, the values of key metrics were collected: the average number of detected defects per 1000 lines of code, response time to a simulated vulnerability, the percentage of test coverage, and the average recovery time after errors. The data for both configurations were normalized and analyzed according to the proposed model, with the calculation of the integral cyber resilience indicator R_c.

The collected data were normalized to the interval [0;1] and analyzed using the weighted aggregation method. In the configuration without automation (baseline practice), the R_c value was 0.41, which reflected a low level of coverage (32%), complexity of functions (Cyclomatic Complexity >13), as well as a long incident response time (average 48 hours). In the improved configuration with the introduction of unit testing, regular code reviews and team training, the R_c level increased to 0.76 with 81% coverage and an average recovery time of 11 hours. The results demonstrate a nonlinear relationship between testing depth and the increase in the cyber resilience index. The effect of a sharp increase in R_c after reaching coverage above 60%, which corresponds to the critical threshold of test saturation, is particularly pronounced. The results from Table 2 confirm that the metrics related to the speed of response to defects and the level of automated quality control have the greatest impact on the increase in cyber resilience.

Table 2

Comparing performance in two environment configurations

Indicator	Basic configuration	Improved configuration
Code Coverage (%)	32 %	81 %
Defect Density (per 1 KLOC)	4.1	1.2
Mean Time to Recovery (h)	48	11
Cyclomatic Complexity	13.5	7.2
Code review frequency (times/week)	0	2
Final R_c	0.41	0.76

The results show a significant increase in the integrated cyber resilience index R_c under the conditions of implementing systematic software quality control practices. The improved configuration allowed to reduce the number of defects, shorten the average response time to vulnerabilities and achieve a high level of test coverage. This confirms the hypothesis that effective SQA processes can directly affect the ability of a system to withstand cyberattacks.

CONCLUSION

The article proposes a methodological approach to quantitative assessment of cyber resilience of information systems based on Software Quality Assurance metrics. A theoretical review of existing software quality assessment models (CMMI, ISO/IEC 25010) and cyber resilience frameworks (NIST CSF, MITRE, CIS Controls) revealed a lack of integration between these domains, which creates a gap in the tools for security management at the development process level.

The proposed model uses normalized indicators of software development and maintenance quality, aggregated by weight coefficients, to calculate the integral cyber resilience indicator R_c. An experiment in a test environment showed that an increase in such indicators as the level of test coverage, the frequency of code reviews, and the reduction of recovery time after incidents significantly increases the value of R_c, and therefore the system's resilience to cyber attacks.

The results confirm the presence of a direct correlation between qualitatively implemented SQA processes and the ability of IT systems to withstand external and internal threats. Thus, ensuring a high level of software quality is considered not only as a reliability factor, but also as a component of cybersecurity. In further research, it is planned to expand the set of metrics and verify the model in environments with different architectures and levels of automation. The proposed approach can become the basis for creating practical tools for automated monitoring of cyber resilience based on the existing QA infrastructure of enterprises.

References

1. Rozlomii, I., Faure, E., & Naumenko, S. (2025). Authentication methods in embedded systems with limited computing resources. Measuring and computing devices in technological processes, (1), 29-35. https://doi.org/10.31891/2219-9365-2025-81-4
2. Verma, P., Newe, T., O'Mahony, G. D., Brennan, D., & O'Shea, D. (2025). Towards a Unified Understanding of Cyber Resilience: A Comprehensive Review of Concepts, Strategies, and Future Directions. IEEE Access.
3. Nakonechna, Y., Savchuk, B., & Kovalova, A. (2024). Fuzzy logic in risk assessment of multi-stage cyber attacks on critical infrastructure networks. Theoretical and Applied Cybersecurity, 6(2), 52-65. https://doi.org/10.20535/tacs.2664-29132024.2.318023
4. Alam, M. M., Priti, S. I., Fatema, K., Hasan, M., & Alam, S. (2024). Ensuring excellence: A review of software quality assurance and continuous improvement in software product development. Achieving sustainable business through AI, technology education and computer science, 331-346.
5. Altrichter, H., Ettl, K., Grinner, K., Kolleritsch, K., Kopp-Sixt, S., Leeb-Brandstetter, R. & Postlbauer, A. (2024). Revisions of evidence-based governance: The case of the Austrian quality management system SQA. Policy Futures in Education, 22(2), 207-227.
6. Hamretskyi, R., & Gnatyuk, V. (2024, October). Methods and Models for Software Quality Assessment in Information and Communication Systems. In 2024 IEEE 7th International Conference on Actual Problems of Unmanned Aerial Vehicles Development (APUAVD) (pp. 62-67). IEEE.
7. Ali, M., Ullah, A., Islam, M. R., & Hossain, R. (2025). Assessing of software security reliability: Dimensional security assurance techniques. Computers & Security, 150, 104230.
8. Gadhi, A., Gondu, R. M., Chaudhary, H., & Abiona, O. (2024). Cyber Resilience through Real-Time Threat Analysis in Information Security. International Journal of Communications, Network and System Sciences, 17(4), 51-67.
9. Rocha, A., Alaba, F. A., Musa, H., Sousa, M. J., de Vasconcelos, J. B., & Pereira, R. (2024, October). Cybersecurity Maturity Models: A Systematic Literature Review. In The International Conference on Strategic Innovative Marketing and Tourism (pp. 179-206). Dordrecht: Springer Netherlands.
10. Jereb, B., & Kajba, M. (2023). Logistics Systems Digitalisation And Software Quality: Why It'S Important And How It'S Related To Iso/Iec 25010. Business Logistics in Modern Management, 23, 413-430.
11. Klima, M., Bures, M., Frajtak, K., Rechtberger, V., Trnka, M., Bellekens, X. & Ahmed, B. S. (2022). Selected code-quality characteristics and metrics for internet of things systems. IEEE Access, 10, 46144-46161.
12. Annarelli, A., Clemente, S., Nonino, F., & Palombi, G. (2021, July). Effectiveness and adoption of NIST managerial practices for cyber resilience in Italy. In Intelligent Computing: Proceedings of the 2021 Computing Conference, Volume 3 (pp. 818-832). Cham: Springer International Publishing.
13. Ahn, G., Jang, J., Choi, S., & Shin, D. (2024). Research on Improving Cyber Resilience by Integrating the Zero Trust security model with the MITRE ATT&CK matrix. IEEE Access, 12, 89291-89309.
14. Pemmasani, P. K. (2023). National Cybersecurity Frameworks for Critical Infrastructure: Lessons from Governmental Cyber Resilience Initiatives. International Journal of Acta Informatica, 2(1), 209-218.
15. Sinan, M., Shahin, M., & Gondal, I. (2025). Integrating Security Controls in DevSecOps: Challenges, Solutions, and Future Research Directions. Journal of Software: Evolution and Process, 37(6), e70029.
16. Cheng, Y., Elsayed, E. A., & Huang, Z. (2022). Systems resilience assessments: a review, framework and metrics. International Journal of Production Research, 60(2), 595-622.
17. Komaragiri, V. B., & Edward, A. (2022). AI-Driven Vulnerability Management and Automated Threat Mitigation. International Journal of Scientific Research and Management (IJSRM), 10(10), 981-998.