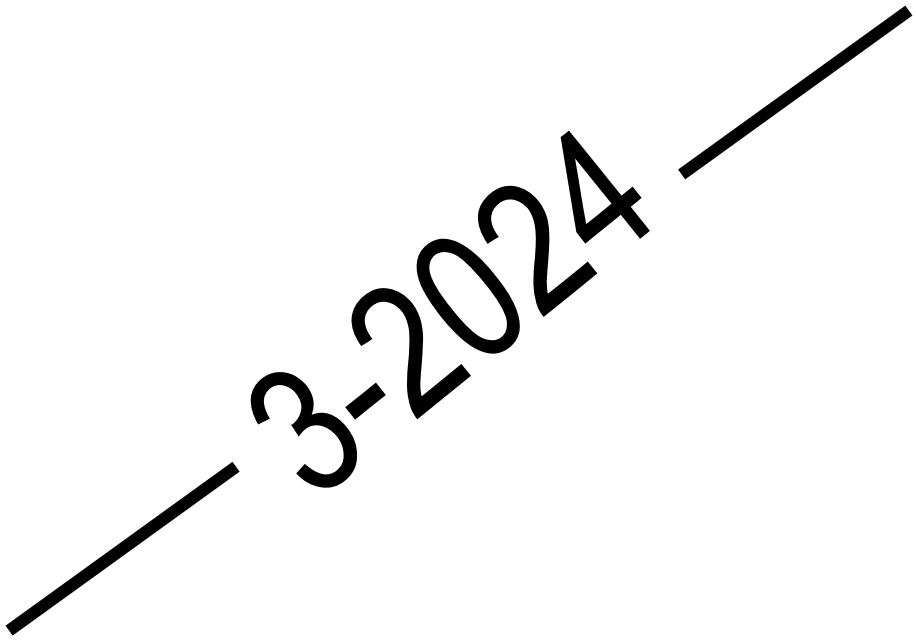
O‘ZBEKISTON RESPUBLIKASI

OLIY TA’LIM, FAN VA INNOVATSIYALAR VAZIRLIGI

FARG‘ONA DAVLAT UNIVERSITETI

FarDU. ILMIY XABARLAR

1995-yildan nashr etiladi
Yilda 6 marta chiqadi



НАУЧНЫЙ ВЕСТНИК. ФерГУ

Издаётся с 1995 года
Выходит 6 раз в год

Aniq va tabiiy fanlar

FIZIKA-TEXNIKA

KIMYO

FarDU. Ilmiy xabarlar – Scientific journal of the Fergana State University

Volume 30 Issue 3, 2024-yil **DOI: 10.56292/SJFSU/vol30_iss3/a125**

UO‘K: 004.056, 65.012.35

METHODS OF ANALYZING AND ASSESSING INFORMATION SECURITY RISKS

МЕТОДЫ АНАЛИЗА И ОЦЕНКИ РИСКОВ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

AXBOROT XAVFSIZLIGI XAVFLARINI TAHLIL QILISH VA BAHOLASH USULLARI

Tashatov Nurlan Narkenovich[1]
[1]Evrosiyo milliy universiteti. Qozog‘iston. Fizika-matematika fanlari nomzodi, professor

Onarkulov Maksadjon Karimberdiyvich[2]
[2]Farg‘ona davlat universiteti, fizika-matematika fanlari bo‘yicha falsafa doktori (PhD),

Askarbekkizi Akbota[3]
[3]Evrosiyo milliy universiteti, Qozog‘iston, magistrant

Annotatsiya

Ushbu maqolada axborot xavfsizligi xavfini boshqarish jarayonlarini va tashkiliy aktivlarni himoya qilishda xavflarni baholash masalalari qaralgan bo‘lib, xavflarni baholash bosqichlari identifikatsiya qilish, tahlil qilish, baholash va davolash batafsil bayon etilgan va CRAMM, FRAP, xavf soati, MSAT va CORAS kabi vositalarning turli xil tashkiliy sharoitlarda samaradorligi baholangan. Har bir vositaning afzalliklari va kamchiliklari tahlil etilgan, tashkilotlarga ISO 31000 standartlariga mos keladigan tegishli metodologiyalarni tanlash uchun ko‘rsatmalar berilgan. Ushbu ishda tashkilotlarga ortib borayotgan tahdidlarga moslashishga va xavflarni baholashning tegishli amaliyotlari orqali xavfsizlik tizimini takomillashtirish orqali muvofiqlikni saqlashga yordam berishga qaratilgan. Taqdim etilgan manba axborot xavfsizligini boshqarishni doimiy ravishda takomillashtirish uchun strategik manba bo‘lib xizmat qiladi.

Abstract

This article evaluates information security risk management processes, emphasizing the critical role of risk assessment in safeguarding organizational assets. It details the stages of risk assessment–identification, analysis, evaluation, and treatment–and scrutinizes tools such as CRAMM, FRAP, RiskWatch, MSAT, and CORAS for their effectiveness across various organizational settings. A comparative analysis assesses each tool’s strengths and limitations, providing guidance for organizations to select appropriate methodologies that align with ISO 31000 standards.

This study aims to help organizations adapt to evolving threats and maintain compliance by enhancing their security frameworks through suitable risk assessment practices. The insights offered serve as a strategic resource for continuous improvement in information security management.

Аннотация

В данной статье рассматриваются процессы управления рисками информационной безопасности, с акцентом на важности оценки рисков для защиты активов организации. Описываются этапы оценки рисков — идентификация, анализ, оценка и управление — и проводится анализ инструментов, таких как CRAMM, FRAP, RiskWatch, MSAT и CORAS, для оценки их эффективности в различных организационных средах. Проводится сравнительный анализ сильных и слабых сторон каждого инструмента, что помогает организациям выбирать подходящие методологии, соответствующие стандартам ISO 31000.

Цель данного исследования — помочь организациям адаптироваться к изменяющимся угрозам и поддерживать соответствие путем улучшения своих структур безопасности с помощью подходящих практик оценки рисков. Полученные результаты могут быть полезны для постоянного совершенствования управления информационной безопасностью и обеспечения ее соответствия международным стандартам.

Kalit so‘zlar: *xatarlarni boshqarish, tahdidlar, axborot xavfsizligi, xavflarni baholash, vosita*

Ключевые слова: *управление рисками, угрозы, информационная безопасность, оценка рисков, инструмент.*

Key words: *risk management, threats, information security, risk assessment, tool.*

INTRODUCTION

Information security risks represent potential threats that could lead to adverse events, causing various types of losses. Effective risk management processes involve coordinated actions to oversee and control such risks, ensuring the protection of information systems and assets.

The primary objective of risk assessment is to identify the characteristics of risks related to the information system and its assets. This includes determining the value of resources, evaluating the significance of threats and vulnerabilities, and assessing the effectiveness of existing and planned protective measures.

Different methodologies for risk analysis vary in complexity and scope:

– Baseline Security Analysis: Conducted according to minimum security requirements, often dictated by national standards. It generally lacks a detailed assessment of resource values and countermeasure effectiveness;

– Full Risk Analysis: This comprehensive analysis is essential for systems with heightened security demands. It involves a thorough evaluation of information resource values, threat and vulnerability assessments, and the selection and effectiveness evaluation of countermeasures.

Risk assessment can conventionally be divided into the following stages: risk identification; risk analysis; risk evaluation. Risk assessment is a systematic process of identifying, analyzing, and evaluating the potential risks that may be involved in a projected activity or undertaking. It involves determining the likelihood that a threat will exploit a vulnerability and the impact it would have, in order to establish appropriate measures to mitigate or manage the risk. In the context of information security, this process is crucial for protecting information assets against threats, ensuring confidentiality, integrity, and availability of data. [1]

THE MAIN PART

Several risk assessment tools analyzed, including CRAMM, FRAP, RiskWatch, and MSAT, highlighting their strengths and limitations. Each tool is evaluated based on its suitability for different organizational environments, the depth of risk analysis provided, and its alignment with strategic business needs.

The table below offers a scientific breakdown of each tool's approach to risk assessment, along with their respective advantages and challenges. This information can be crucial for organizations when choosing a risk assessment tool that best fits their operational environment and risk management needs.

Table 1. Comparative analysis of Risk Assessment Tools

Tool	Strengths	Limitations
CRAMM	The method uses an integrated approach to risk assessment, applies technologies for assessing threats and vulnerabilities based on indirect factors with the ability to verify results, has an extensive knowledge base on countermeasures and has versatility and adaptability to the profiles of different organizations [9]	Method requires special training and high qualification of the auditor. Auditing using this method is a rather laborious process and may require months of continuous work by the auditor. It does not allow you to create your own report templates or modify existing ones. The software exists only in English
FRAP	Streamlines risk management by focusing on critical risks, which is beneficial for resource-constrained environments. Effective for making quick decisions in dynamic business contexts. User-friendly for non-experts.	Might not be comprehensive enough for complex IT environments, potentially missing some less obvious risks. Lacks the depth required for detailed technical analysis and mitigation strategies
RiskWatch	The RiskWatch method uses the "prediction of annual losses" and the assessment of "return on investment" as criteria for assessing and managing risks.	The method is suitable if you need to conduct a risk analysis at the software and technical level of protection, without considering organizational and administrative factors. The risk estimates obtained

Tool	Strengths	Limitations
		(mathematical expectation of losses) far from exhausts the understanding of risk from a systemic perspective – the method does not consider an integrated approach to information security
MSAT	Developed by Microsoft; good for IT infrastructure. Integrates easily with other Microsoft security tools, providing a cohesive security environment. Offers actionable insights and benchmarks against best practices.	The MSAT assessment is designed to cover broad areas of potential risk in an environment, rather than providing in-depth analysis of specific technologies or processes. As a result, the tool cannot evaluate the effectiveness of the applied safety measures
CORAS	The positive side of the CORAS method is that the software product implementing this methodology is distributed free of charge and does not require significant resources for installation and application	Method does not provide for the frequency of risk assessment and updating of their values. CORAS does not allow you to evaluate the effectiveness of investments made in the implementation of security measures. It also does not make it possible to find the necessary balance between measures aimed at preventing, identifying, correcting, or restoring information assets.
OCTAVE	The method provides for regular risk assessment and updating of their values as part of the risk assessment process. It does not use such a risk management method as circumvention (exclusion).	The OCTAVE method does not provide a quantitative assessment of risks, but a qualitative assessment can be used to determine the quantitative scale of their ranking
ГРИФ	The method does not require special knowledge in the field of information security, providing a detailed document that gives a complete picture of possible damage from incidents, ready for presentation to the company's management, forms a complete model of the information system from the point of view of information security, considering the actual fulfillment of the requirements of a comprehensive security policy.	The method does not link to business processes, the ability to compare reports at different stages of the implementation of a set of security measures and add company-specific security policy requirements [8]

CRAMM (CCTA Risk Analysis and Management Method) is a government-standardized tool used primarily in the UK. It provides a comprehensive framework for risk assessment and management by combining asset, threat, and vulnerability evaluations to propose risk mitigation measures. CRAMM emphasizes the qualitative analysis of risks and offers detailed guidance on security controls and procedures. However, its complexity and the need for detailed input can make it cumbersome for smaller organizations or those requiring quick assessments [2].

The main objectives of the CRAMM methodology are:

- Formalization and automation of risk analysis and management procedures;
- Optimization of control and protection costs;

– Comprehensive risk planning and management at all stages of the information systems lifecycle;
– Reduction of time for the development and maintenance of a corporate information security system;
– Justification of the effectiveness of the proposed protection measures and controls;
– Change and Incident management;
– Business continuity support;
– Prompt decision-making on security management issues, etc.

Risk management in the CRAMM methodology is carried out in several stages [2] (Fig. 1).

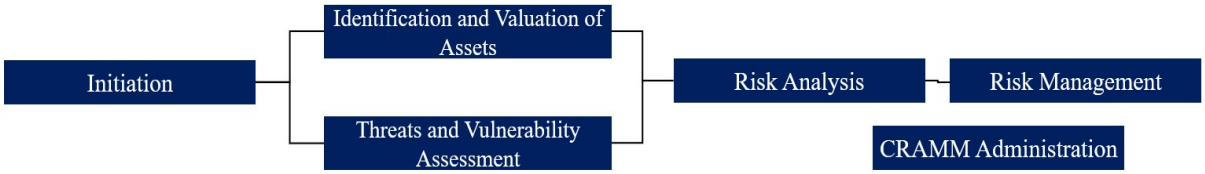


Figure 2. CRAMM stages

The Facilitated Risk Analysis Process (FRAP) methodology is proposed by the Peltier Associates consulting company, specializing in assessing losses from the presence of vulnerabilities in the security system and developing recommendations for their prevention. The technique was developed by Thomas Peltier. In the methodology, the provision of information security is proposed to be considered as part of the risk management process [3].

IMPACT

PROBABILITY

	High	Medium	Low
High	A	B	C
Medium	B	B	C
Low	B	C	D

A - Corrective action must be implemented
B - Corrective action should be implemented
C - Requires monitor
D - No action required at this time

Figure 2. Risk matrix FRAP

RiskWatch offers a balanced approach between qualitative and quantitative analyses, making it versatile for various industries. RiskWatch allows organizations to perform detailed security assessments that calculate potential financial impacts of risks, aiding in cost-benefit analysis of security investments. It is particularly noted for its user-friendly interface and flexibility in customizing assessments to fit specific organizational policies and goals [5].

MSAT (Microsoft Security Assessment Tool) is designed to provide a quick and easy way to assess the security posture of an organization relative to established best practices. It uses a series of questions to gauge the maturity of an organization's information security management. MSAT's main advantage is its simplicity and speed, making it suitable for preliminary assessments to identify major vulnerabilities and areas for improvement [7].

The OCTAVE method is a method for rapid assessment of critical threats, assets, and vulnerabilities [6].

CORAS is a model-based risk assessment tool that provides a graphical interface for threat and risk modeling. CORAS offers a detailed methodological framework for conducting thorough risk analyses, supported by a set of templates and predefined scenarios. It excels in environments where detailed, visual documentation of threats and vulnerabilities is necessary, such as complex IT projects or systems with intricate security requirements [4].

CONCLUSION

The effectiveness of an organization's information security risk management hinges crucially on the appropriate selection and application of risk assessment methodologies. As demonstrated in this analysis, each tool – CRAMM, FRAP, RiskWatch, MSAT, and CORAS – brings unique strengths and addresses different needs depending on the organizational context.

CRAMM's comprehensive approach is well-suited for organizations that require detailed risk analysis and can dedicate the resources to thorough assessments. FRAP, with its focus on critical risks, offers a streamlined alternative beneficial for smaller or resource-constrained environments. RiskWatch provides a balanced mix of qualitative and quantitative analysis, making it versatile across various industries. MSAT, developed by Microsoft, is particularly advantageous for quick assessments within IT infrastructures, aligning well with other Microsoft security tools. Lastly, CORAS stands out for its graphical representation of risk assessments, which is essential for complex IT projects requiring detailed, visual documentation.

Organizations must carefully evaluate these tools against their specific requirements and constraints to choose the most appropriate method. Aligning the choice of a risk assessment tool with the organizational risk profile and the standards such as ISO 31000 ensures not only compliance but also enhances the efficacy of risk management practices. The ongoing evolution of threats necessitates continuous improvement in risk assessment methodologies to protect information assets effectively and ensure resilience against emerging threats. This study underscores the importance of adapting to changing threat landscapes by selecting and tailoring risk assessment practices that best fit an organization's specific needs.

REFERENCES

1. International Organization for Standardization. (2018). ISO/IEC 31000: Risk management – Guidelines (ISO/IEC 31000:2018). https://www.iso.org/standard/65694.html

2. Волкова, Л. В., Макарова, Д. В., & Докучаев, В. А. (2021). Использование метода CRAMM для оценки информационных рисков. Телекоммуникации и информационные технологии, 8(1), 103-109.

3. Putra, S. J., Gunawan, M. N., Sobri, A. F., Muslimin, J. M., & Saepudin, D. (2020, October). Information Security Risk Management Analysis Using ISO 27005: 2011 For The Telecommunication Company. In 2020 8th International Conference on Cyber and IT Service Management (CITSM) (pp. 1-5). IEEE.

4. Wirtz, R., & Heisel, M. (2020). Model-based risk analysis and evaluation using CORAS and CVSS. In Evaluation of Novel Approaches to Software Engineering: 14th International Conference, ENASE 2019, Heraklion, Crete, Greece, May 4–5, 2019, Revised Selected Papers 14 (pp. 108-134). Springer International Publishing.

5. Kuzminykh, I., Ghita, B., Sokolov, V., & Bakhshi, T. (2021). Information security risk assessment. Encyclopedia, 1(3), 602-617.

6. Alimzhanova, Z., Tleubergen, A., Zhunusbayeva, S., & Nazarbayev, D. (2022, April). Comparative analysis of risk assessment during an enterprise information security audit. In 2022 International Conference on Smart Information Systems and Technologies (SIST) (pp. 1-6). IEEE.

7. Chandrinos, T. A. (2023). Analysis of frameworks/methods for information security risk management (Master's thesis, Πανεπιστήμιο Πειραιώς).

8. Исатайұлы, С. Қ., & Алимжанова, Ж. М. Аудит информационной безопасности методами оценочного динамического моделирования. In The XIII International Science Conference «Perspective of science and practice», December 13–15, Amsterdam, Netherlands. 322 p. (p. 305).

9. Сидоркін, П., Горліченко, С., Некоз, В., & Шилан, М. (2023). Методи управління ризиками інформаційної безпеки CRAMM та COBIT 5 for Risk. Сучасні інформаційні технології у сфері безпеки та оборони, 47(2), 41-47.