НАЦІОНАЛЬНА АКАДЕМІЯ НАУК УКРАЇНИ
ІНСТИТУТ ПРОБЛЕМ РЕЄСТРАЦІЇ ІНФОРМАЦІЇ НАН УКРАЇНИ

ІНФОРМАЦІЙНІ ТЕХНОЛОГІЇ ТА БЕЗПЕКА

МАТЕРІАЛИ XXIII МІЖНАРОДНОЇ НАУКОВО-ПРАКТИЧНОЇ КОНФЕРЕНЦІЇ

ВИПУСК 23

Київ – 2023

ІНФОРМАЦІЙНІ ТЕХНОЛОГІЇ
ТА БЕЗПЕКА

https://its.ipri.kiev.ua

ISBN 978-966-2344-96-7

НАЦІОНАЛЬНА АКАДЕМІЯ НАУК УКРАЇНИ
ІНСТИТУТ ПРОБЛЕМ РЕЄСТРАЦІЇ ІНФОРМАЦІЇ НАН УКРАЇНИ

ІНФОРМАЦІЙНІ ТЕХНОЛОГІЇ ТА БЕЗПЕКА

МАТЕРІАЛИ XXIII МІЖНАРОДНОЇ НАУКОВО-ПРАКТИЧНОЇ КОНФЕРЕНЦІЇ

ВИПУСК 23

Київ – 2023

Рекомендовано до друку Вченою радою
Інституту проблем реєстрації інформації НАН України
(протокол № 11 від 26 грудня 2023 р.)

Інформаційні технології та безпека. Матеріали XXIII Міжнародної науково-практичної конференції ІТБ-2023. – Київ: Інжиніринг. – 202 с. ISBN: 978-966-2344-96-7

До збірника увійшли матеріали доповідей, представлених на XXIII Міжнародній науково-практичній конференції «Інформаційні технології та безпека» (ІТБ-2023, 30 листопада 2023 року, м. Київ, Україна).

У збірнику представлені матеріали, присвячені питанням створення і впровадження інформаційних технологій, актуальним проблемам забезпечення інформаційної та кібербезпеки, протидії інформаційним операціям і кібертероризму, інтелектуальним технологіям підтримки прийняття рішень, проведенню аналітичних досліджень на основі сучасних методів інтелектуального аналізу даних.

Для фахівців в області інформаційних технологій, інформаційної і кібернетичної безпеки, а також для аспірантів і студентів старших курсів вищої школи відповідних спеціальностей.

ISBN 978-966-2344-96-7

–

MODEL-BASED INFORMATION SECURITY MANAGEMENT SYSTEMS ARCHITECTURE

V. Mokhor[1], O. Bakalynskyi[1], Ya. Dorohyi[2,3], V. Tsurkan[1,3]

[1]Pukhov Institute for Modeling in Energy Engineering of National Academy of Sciences of Ukraine, Kyiv, Ukraine
[2]Donetsk National Technical University, Lutsk, Ukraine
[3]National Technical University of Ukraine "Igor Sikorsky Kyiv Polytechnic Institute", Kyiv, Ukraine
v.mokhor@gmail.com, baov@meta.ua, argusyk@gmail.com, v.v.tsurkan@gmail.com

Investigated the representation of the information security management system architecture. The study elucidates the influences of the organizational environment on its fundamental

concepts and properties. This is manifested in the elements, relationships, principles, and evolution of the information security management system. The description of its architecture within a specific organization, considering the type, size, and nature, is condensed into constructing a model from the perspective of stakeholders. To achieve this, the proposed approach involves employing model-based systems engineering. This enables the attainment of a unified representation of the information security management system architecture primarily from the perspectives of various stakeholders. The formalization is based on the language of system modeling. According to its graphical notation, architecture elements are depicted as blocks, along with their properties and relationships.
Keywords: risk assessment, risk treatment, information security management system architecture, model-based systems engineering, model-based architecture, interested party.

Introduction

The embodiment of the fundamental concepts and properties of the information security management system in the surrounding environment is reflected in its elements, relationships, principles, and evolution [1]. Such representation is conventionally referred to as architecture. The description of its creation in a specific environment and/or community of stakeholders is determined by a model constructed from a particular perspective [2].

A distinctive feature of creating information security management systems is the orientation towards ensuring the integrity of essential information properties within an organization. This is achieved through risk assessment and, consequently, ensuring stakeholders of the proper handling of these risks. In this case, the organization is proposed to be interpreted as the surrounding environment defining parameters and conditions influencing the information security management system. Meanwhile, its fundamental concepts and properties are embodied in the architecture's elements and relationships [1, 3–5].

This interpretation allows establishing credible influences on the information security management system from the organization's perspective in terms of its type, size, and nature [3, 4]. Furthermore, it considers the existence and interaction with other management systems, such as cybersecurity and privacy information security. This

is crucial for meeting the needs, expectations, and constraints of stakeholders within defined boundaries (organization, organizational unit). Therefore, a model-oriented representation of the architecture of information security management systems remains relevant.

Model-based information security management systems architecture

The prerequisite for defining the architecture of the information security management system is the analysis of the organization's activities as the surrounding environment. Based on established internal and external circumstances, requirements from stakeholders are formulated. Their implementation allows for the consideration and, consequently, satisfaction of defined needs, expectations, and constraints. As a result, the stakeholders' vision is transformed into a technical solution vision. This is essential for presenting characteristics, attributes, functional, and non-functional requirements for the information security management system within the organization [1–4].

Taking into account the interests of stakeholders and established functional and non-functional requirements is achieved by creating alternative variants of the architecture of information security management systems. Each variant defines elements and relationships between them, interfaces for interaction with other systems within the organization, as well as with other organizations (or structural components of the same organization). Additionally, it is crucial to consider the dependency on quality management systems, as they collectively form an integrated organizational management system [2–5]. Interfaces and interactions characterize the boundaries of its creation and implementation, while these aspects are addressed through the development of the information security management system architecture model. To accomplish this task, the use of model-based systems engineering is proposed [2, 6].

The adoption of the proposed methodology allows moving away from document-oriented model construction for the architecture of the information security management system. This achieves uniform representation, primarily from the perspectives of various stakeholders. This is important for clear understanding and meeting their needs, expectations, and constraints. The basis for such formalization is the Systems Modeling Language (SysML) [7, 8]. According to its graphical notation, the elements of the information security management system architecture are represented as blocks,

along with their properties and relationships. Simultaneously, the structure of each block can be further detailed through their ports and interfaces, which is useful for representing interactions within the elements of the information security management system architecture and with the surrounding environment.

Conclusion

Thus, the elements, relationships, principles, and evolution reflect the fundamental concepts and properties of the information security management system in the surrounding environment. By the surrounding environment, we mean the organization as a whole or a specific structural component. Considering this, its influence is determined based on the type, size, and nature. This representation in a specific environment is characterized by a model of the architecture of the information security management system constructed from the perspective of stakeholders.

The use of model-based systems engineering has allowed moving away from document-oriented model construction for the architecture of the information security management system. This has achieved uniformity in its representation, primarily from the perspectives of various stakeholders. The basis for such formalization is the Systems Modeling Language. According to its graphical notation, the elements of the information security management system architecture are represented as blocks, along with their properties and relationships.

References

1. ISO/IEC/IEEE 42010:2022. Software, systems and enterprise. Architecture description. [Valid from 2022-11-07]. URL: https://www.iso.org/standard/74393.html, last accessed 2023/11/22.
2. ISO/IEC/IEEE 15288:2023. Systems and software engineering. System life cycle processes. [Valid from 2023-05-16]. URL: https://www.iso.org/standard/81702.html, last accessed 2023/11/22.
3. ISO/IEC 27001:2022. Information security, cybersecurity and privacy protection. Information security management systems. Requirements. [Valid from 2022-10-25]. URL: https://www.iso.org/standard/27001, last accessed 2023/11/22.
4. ISO/IEC 27001:2022/Amd 1. Information security, cybersecurity and privacy protection. Information security management systems. Requirements. [Valid from 2023-09-19]. URL:

https://www.iso.org/standard/88435.html, last accessed 2023/11/22.
5. ISO/IEC 27002:2022. Information security, cybersecurity and privacy protection. Information security controls. [Valid from 2022-02-15]. URL: https://www.iso.org/standard/75652.html, last accessed 2023/11/22.
6. Shevchenko N. An Introduction to Model-Based Systems Engineering (MBSE). URL: https://insights.sei.cmu.edu/blog/introduction-model-basedsystems-engineering-mbse/, last accessed 2023/11/22.
7. OMG Systems Modeling Language (OMG SysML™). URL: https://sysml.org/.res/docs/specs/OMGSysML-v1.6-19-11-01.pdf, last accessed 2023/11/22.
8. Friedenthal S., Moore A., Steiner R. A Practical Guide to SysML. The Systems Modeling Language. Waltham : Elsevier, 2015. 599 p.