засобів, ведення журналів симптомів і зв'язку з лікарями. Завдяки використанню Kotlin, Jetpack Compose, Room та інших технологій, розробники отримують змогу створювати надійні, безпечні та зручні додатки, що відповідають сучасним вимогам цифрової медицини й сприяють розвитку інтелектуальних сервісів підтримки здоров'я.

Подальший розвиток напрямку пов'язаний із інтеграцією хмарних технологій, елементів штучного інтелекту та автоматизованого тестування, що сприятиме підвищенню якості та інтелектуальності мобільних програмних систем.

Список використаних джерел

1. Android Developers. Build modern Android apps with Jetpack Compose. Android Official Documentation, 2025. URL: https://developer.android.com/jetpack/compose.
2. JetBrains. Kotlin Documentation: Asynchronous programming with coroutines. Kotlin Official Guide, 2025. URL: https://kotlinlang.org/docs/coroutines-overview.html.
3. Google Developers. Room Persistence Library. Android Jetpack Documentation, 2025. URL: https://developer.android.com/training/data-storage/room.

DOI 10.70286/ISU-12.11.2025.006

CHOOSING AN INFORMATION PROTECTION SYSTEM UNDER RISK CONDITIONS

Solodovnyk Ganna
Ph.D., Associate Professor
Chuieva Anzhelika
Student
Department of Cybersecurity and Information Technologies
Simon Kuznets Kharkiv National University of Economics, Ukraine

Relevance. The increasing informatization of society represents a response to a number of challenges posed by a turbulent external environment. The development of digital technologies provides access to an entire universe of possibilities. Simultaneously, the dependence of individuals and organizations on information resources is growing significantly, which makes the issue of information security for informatization objects especially critical. These objects can be understood as both socio-economic systems and individual entities. Information security ensures that informatization objects are protected from damage resulting from deficiencies in the quality of information and the state of the information infrastructure [1].

Information threats can be identified as those that distort or destroy data stored and processed by an automated system, thereby affecting its information resources, as

well as the means and services that implement information technologies. The sources of such threats may arise both from the external environment and from within the internal information domain of the automated object itself, due to imperfections in the information and analytical support of organizational and production processes [2].

Furthermore, information-related threats can be distinguished – those associated with the loss of operational efficiency of an automated system caused by the distortion, leakage, or destruction of information used for managerial and organizational decision-making [2]. In this context, the protection level of information can be evaluated according to criteria based on the quality requirements of information support and the overall performance of the information system [3]: confidentiality, as protection against unauthorized access; integrity, as the prevention of unauthorized modification or destruction of data and/or software-hardware environments; availability, as prevention of unauthorized information concealment; relevance, ensuring the accurate reflection of the state of domain objects in information resources at any given time; completeness, as the provision of the most comprehensive possible description of processes, events, and situations; authenticity, meaning the degree of correspondence between the information contained in the resources and the actual state of domain objects; timeliness, as the guarantee of data delivery and reception within required time frames to meet the informational needs of the system; and value, as the property of information resources determined by their suitability for practical use in various areas of the system's operation.

The factors outlined above determine the relevance of applying scientifically grounded decision-making methods for the selection of information protection systems and the safeguarding of information resources.

Literature Review. Modern challenges in the field of information protection have significantly increased the interest of both domestic and foreign researchers in the issues of information risk assessment and decision support for the development and selection of systems aimed at counteracting adverse events associated with damage to information resources. In [4], the authors conducted a systematic selection and review of published scientific works in the field of information security risk assessment, focusing on IT security risk evaluation and the selection of critical IT solutions using ISRA (Information Security Risk Assessment) elements as evaluation criteria. The study [5] proposes an integrated approach to cybersecurity risk assessment and management based on multi-criteria decision-making (MCDM). The authors developed a normative framework that combines traditional risk analysis techniques with mathematical decision-making methods such as the Analytic Hierarchy Process (AHP), the Technique for Order Preference by Similarity to Ideal Solution (TOPSIS), and other related approaches.

Studies [6, 7] examine methodological approaches to quantitative evaluation of the level of protection of information technologies in modern information systems. The research presented in [6] aims to create a unified system of indicators and criteria for assessing the effectiveness of protection measures at all levels – from technical to organizational. The work [7] relies on contemporary scientific approaches to information security management but is primarily educational and methodological in nature. A limitation of these studies is the absence of a clear definition of information risk as a probabilistic category, as well as the lack of mathematical models for

determining the optimal security system alternative from this probabilistic standpoint. In [8], a mathematical model for assessing information security risks was developed; however, it is limited to a specific application domain. The model presented in [8] is based on a scheme of independent trials using the Bernoulli formula and is rather complex for practical software implementation.

Based on the analysis of current research, the purpose of this study was formulated as follows: to develop and implement a software-based model for the rational selection of an information security system according to efficiency and risk criteria. The object of the research is the process of selecting and evaluating information security systems, while the subject is the model and methods for selecting an information security system based on efficiency indicators and risk levels, as well as their software implementation.

As a mathematical tool, the study employs the theory of probability. The software implementation was developed using the Python programming language, which belongs to the category of Free and Open Source Software and is distributed under the Python Software Foundation License, compatible with the GNU GPL. For obtaining graphical representations of the results, the Matplotlib library was used.

Main Part. The formulation of the problem regarding the selection of an information security system was defined as follows: given the predicted effect values e_{ij} resulting from the implementation of each i-th protection system under different estimates of the degree of impact on information resources, it is necessary to determine the optimal system. Each protection system was evaluated according to two criteria – efficiency *E* and risk *S*.

The theoretical foundation of the study is based on probability theory, according to which the expected efficiency E_i of implementing the i-th protection system is determined using the mathematical expectation of a random variable:

$$E_i = \sum_{j=1}^{m} e_{ij} p_j \, , i = \overline{1,n}, \quad (1)$$

where: e_{ij} – predicted effect of implementing the i-th protection system;

p_j – probability of occurrence of the j-th degree of impact on information resources;

m – number of identified degrees of impact on information resources;

n – number of alternative protection systems.

The a priori probabilities p_j of different degrees of impact can be determined using expert evaluation methods. In this work, the degrees of impact on information resources were defined on a qualitative scale with the values: low, moderate, and high. However, more detailed methods may be used – both qualitative (e.g., the scenario analysis method, the scoring method, or the Structured What-If Technique (SWIFT)) and quantitative (e.g., multi-criteria analysis or expected loss assessment) [6, 7].

The risk estimation in the process of selecting an information security system can be performed by evaluating both the probability of an adverse event and the magnitude of losses that the automation object would incur in such a case. The probability assessment consists of two components: the probability of an impact on the information system and the probability that this impact will exploit a vulnerability in the protection system. The loss magnitude may include the cost of restoring the information system

and its data, as well as the losses sustained by the organization in its core activities due to the system's failure, data damage, or unavailability. The risk level associated with the implementation of the i-th protection system, denoted as S_i, was determined using the standard deviation of a random variable, according to the formula:

$$S_i = \sum_{j=1}^{m} \left(e_{ij} - E_i\right)^2 p_j \, , i = \overline{1,n}. \quad (2)$$

Software testing of the developed model was carried out under various input data configurations, which provided different relationships between the mathematical expectation of the efficiency indicator of each protection system and its risk. These test cases included conditions where each system could be the optimal choice, as well as a situation in which the final decision remained at the discretion of the decision-maker.

During testing, the model parameters were set as follows: the number of alternative protection systems $n = 3$ and the number of degrees of impact $m = 3$. The input data consisted of the predicted effects of implementing each system. The results were presented in graphical form, where each system (A, B, and C) was represented as a point on a coordinate plane defined by the mathematical expectation and the standard deviation of the efficiency indicator. The graphical interface displaying the test results is shown in Figure 1.

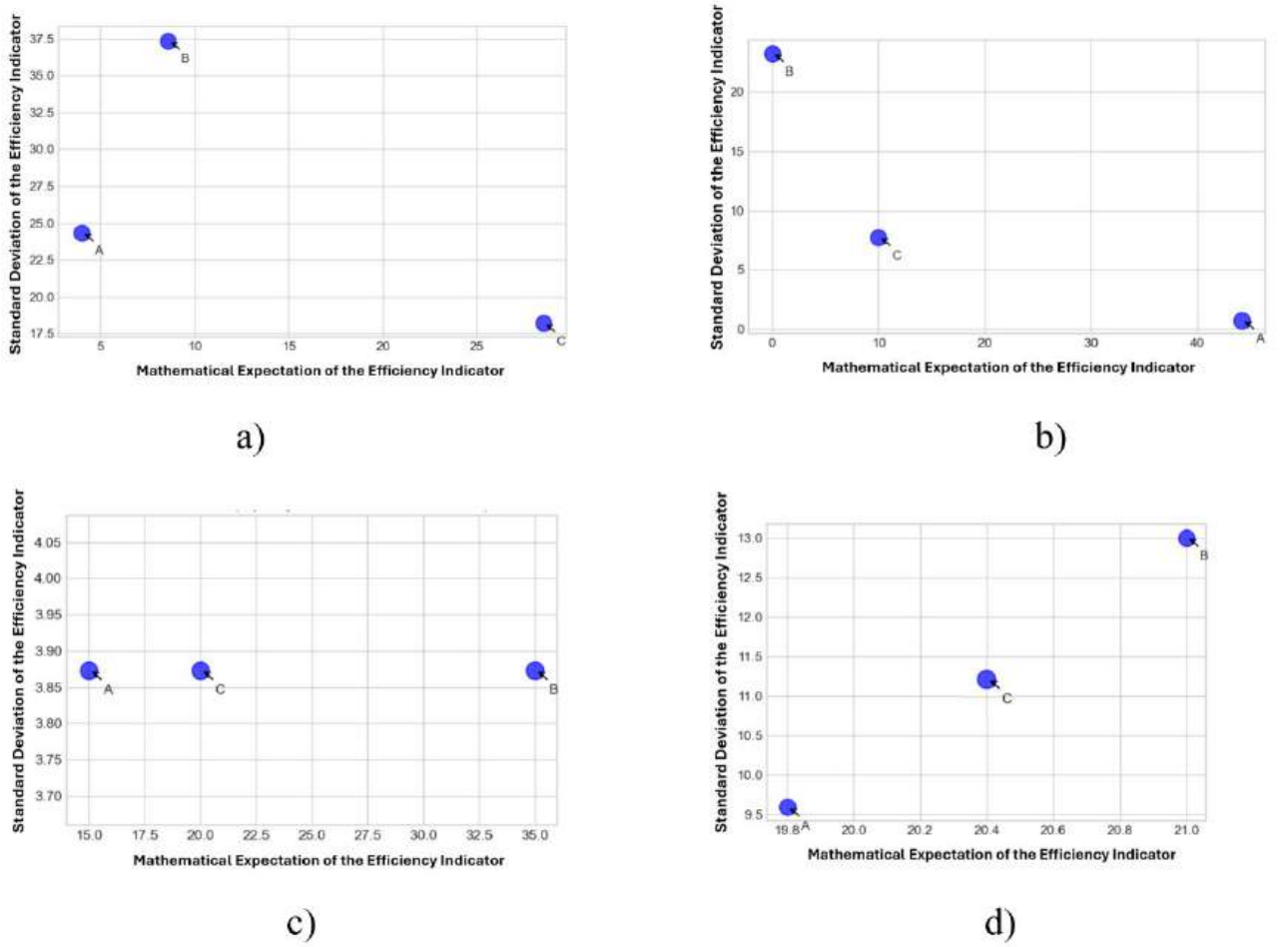

Figure 1. Results of the Analysis of Information Protection System Projects

According to the proposed model, the rational choice corresponds to the system whose representative point is located closer to the lower right corner of the graph. The system that satisfies this condition will have the highest expected effect from

implementation and the lowest expected risk of impact on information resources. Figure 1(d) illustrates a case in which the final choice of the protection system depends on the decision-maker, specifically on their attitude toward risk.

Conclusion. The model presented in this study is universal with respect to the application domain and can be employed for the rational selection of projects under risk conditions across various fields of activity. Further development of the mathematical model involves the application of quantitative assessment methods to determine the degrees of impact on information resources. The improvement of the software implementation is planned through the development of an intuitive user interface that will enhance the model's usability and practical applicability.

References

1. Verkhovna Rada of Ukraine. (2025). Zakon Ukrainy "Pro osnovni zasady zabezpechennia kiberbezpeky Ukrainy" [Law of Ukraine "On the Basic Principles of Ensuring Cybersecurity of Ukraine"]. Retrieved November 5, 2025, from https://zakon.rada.gov.ua/laws/show/2163-19#Text
2. IT Governance. (2025). Understanding the CIA Triad in 2025: A cornerstone of cyber security. Retrieved November 5, 2025, from https://www.itgovernance.co.uk/blog/what-is-the-cia-triad-and-why-is-it-important
3. Security Scorecard. (2020). What is the difference between information security vs cybersecurity? Retrieved November 5, 2025, from https://securityscorecard.com/blog/information-security-versus-cybersecurity
4. Macek, D., Kadlec, I., & Kolar, J. (2020). A systematic literature review on the application of multicriteria decision-making methods for information security risk assessment. International Journal of Safety and Security Engineering, 10(6), 757–767. https://doi.org/10.18280/ijsse.100605
5. Ganin, A. A., Quach, P., Panwar, M., Collier, Z. A., Keisler, J. M., Marchese, D., & Linkov, I. (2020). Multicriteria decision framework for cybersecurity risk assessment and management. Risk Analysis, 40(1), 183–199. https://doi.org/10.1111/risa.12891
6. Batechko, S. V. (2021). Metodyka otsinky zakhyshchenosti informatsiinykh tekhnolohii [Methodology for assessing the security of information technologies]. Informatsiini systemy [Information Systems], 3(11).
7. Yatskiv, V. V., Davletova, A. Ya., & Drapak, V. I. (2023). Oporni konspekt lektsii z dystsypliny "Upravlinnia informatsiinoiu bezpekoiu" [Lecture notes on the discipline "Information Security Management"] (49 p.). Ternopil: TNTU.
8. Berko, A. Yu., Vysotska, V. A., & Rishnyak, I. V. (2008). Metody ta zasoby otsiniuvannia ryzykiv bezpeky informatsii v systemakh elektronnoi komertsii [Methods and tools for assessing information security risks in e-commerce systems]. Visnyk Natsionalnoho universytetu "Lvivska politekhnika". Informatsiini systemy ta merezhi, (610), 20–33. Retrieved from https://science.lpnu.ua/sites/default/files/journal-paper/2019/apr/16336/vis610inform-syst-20-33.pdf