Information systems. Computer sciences. Issues of information security
Информационные системы. Информатика. Проблемы информационной безопасности

UDC 004.056.5
https://doi.org/10.32362/2500-316X-2024-12-6-39-47
EDN IYBIZH

RESEARCH ARTICLE

Modeling incident management processes in information security at an enterprise

Evgeny S. Mityakov [@],
Elena A. Maksimova,
Svetlana V. Artemova,
Anatoly A. Bakaev,
Zhanna G. Vegera

MIREA – Russian Technological University, Moscow, 119454 Russia
[@] Corresponding author, e-mail: mityakov@mirea.ru

Abstract

Objectives. The primary aim of the study is to develop a model for managing information security incidents within an enterprise that minimizes damage and costs associated with incident resolution under limited resources and time constraints.

Methods. The paper analyzes existing approaches to managing information security incidents, including mathematical and simulation models, stochastic differential equations, Markov chains, and other methods. The study is based on a systems approach, incorporating analysis of incident parameters, actions for their resolution, response times, damages due to incident occurrence, and the probability of incident elimination. To validate the developed model, synthetic data reflecting various types of incidents and possible actions were used.

Results. The proposed model optimizes incident management by minimizing damage and costs. It considers parameters such as incident criticality, available resources, response time, and the likelihood of successful incident resolution. Testing of the model on synthetic data showed that the proposed approach significantly improves the selection of optimal actions for responding to incidents in situations constrained by budget and time limitations, thereby enhancing the overall effectiveness of incident management.

Conclusions. Implementing the proposed model in enterprises will improve the overall level of information security, enhance incident response efficiency, and strengthen information protection processes. This will ensure the minimization of risks associated with data leaks and other incidents, thus helping enterprises to make informed and timely decisions under conditions of limited resources and time.

Keywords: incident management, information security, incident modeling, damage minimization, limited resources, mathematical modeling, optimization

• **Submitted:** 12.09.2024 • **Revised:** 30.09.2024 • **Accepted:** 14.10.2024

For citation: Mityakov E.S., Maksimova E.A., Artemova S.V., Bakaev A.A., Vegera Zh.G. Modeling incident management processes in information security at an enterprise. *Russ. Technol. J.* 2024;12(6):39–47. https://doi.org/10.32362/2500-316X-2024-12-6-39-47

Financial disclosure: The authors have no financial or proprietary interest in any material or method mentioned.

The authors declare no conflicts of interest.

НАУЧНАЯ СТАТЬЯ

Моделирование процессов управления инцидентами информационной безопасности на предприятии

Е.С. Митяков @,
Е.А. Максимова,
С.В. Артемова,
А.А. Бакаев,
Ж.Г. Вегера

МИРЭА – Российский технологический университет, Москва, 119454 Россия
@ *Автор для переписки, e-mail: mityakov@mirea.ru*

Резюме

Цели. Основной целью исследования является разработка модели управления инцидентами информационной безопасности на предприятии, минимизирующей ущерб и затраты на устранение инцидентов в условиях ограниченных ресурсов и времени.

Методы. В работе проведен анализ существующих подходов к управлению инцидентами информационной безопасности, включая математические и имитационные модели, стохастические дифференциальные уравнения, цепи Маркова и другие методы. Основанием для работы послужил системный подход, который включает в себя всесторонний анализ параметров инцидентов, действий по их устранению, времени реакции, а также ущерба от реализации инцидентов и вероятности успешного их устранения. Для проверки работоспособности разработанной модели использовались синтетические данные, которые отражают разнообразные типы инцидентов и возможные пути их ликвидации.

Результаты. Предложенная модель управления инцидентами позволяет оптимизировать управление инцидентами за счет минимизации ущерба и затрат. В рамках модели учитываются такие параметры, как критичность инцидентов, доступные ресурсы, время реакции и вероятность успешного устранения инцидентов. Апробация модели на синтетических данных показала, что предложенный подход существенно улучшает выбор оптимальных действий для реагирования на инциденты в ситуациях ограничений бюджета и времени, что в свою очередь повышает общую эффективность управления инцидентами.

Выводы. Внедрение предложенной модели на предприятиях позволит повысить общий уровень информационной безопасности, эффективность реагирования на инциденты и улучшить процессы защиты информации. Это обеспечит минимизацию рисков, связанных с утечками данных и другими инцидентами, и поможет предприятиям принимать обоснованные и оперативные решения в условиях ограниченных ресурсов и времени.

Ключевые слова: управление инцидентами, информационная безопасность, моделирование инцидентов, минимизация ущерба, ограниченные ресурсы, математическое моделирование, оптимизация

• **Поступила:** 12.09.2024 • **Доработана:** 30.09.2024 • **Принята к опубликованию:** 14.10.2024

Для цитирования: Митяков Е.С., Максимова Е.А., Артемова С.В., Бакаев А.А., Вегера Ж.Г. Моделирование процессов управления инцидентами информационной безопасности на предприятии. *Russ. Technol. J.* 2024;12(6):39–47. https://doi.org/10.32362/2500-316X-2024-12-6-39-47

Прозрачность финансовой деятельности: Авторы не имеют финансовой заинтересованности в представленных материалах или методах.

Авторы заявляют об отсутствии конфликта интересов.

INTRODUCTION

Information security incident management at enterprises involves processes of identifying, analyzing and responding to incidents involving information systems and data, which includes a set of measures for the prevention and minimization of damage, and restoration of the normal operation of systems following incidents.

In today's reality, such processes represent a key aspect of ensuring the information security of an organization. Contemporary enterprises face many threats involving cyberattacks and unauthorized access to data to information leaks. As well as entailing financial losses, such threats can undermine a company's reputation. Therefore, effective management of information security incidents at an enterprise becomes an integral part of its overall security strategy. Such management ensures a prompt response to current threats, as well as forming a proactive approach to predicting and preventing potential information security incidents in the future.

In the Russian Federation, information security incident management is regulated by a number of state standards. One of these, GOST R 59712-2022[1], is dedicated to computer security incident management, which represents a narrower area within information security. This standard describes a structured approach to the detection, registration, response and analysis of incidents within the framework of the state system GosSOPKA[2]. In turn, GOST R ISO/IEC TO 18044-2007[3] covers a wider range of information security incidents, setting out requirements for their documentation, legal examination, interaction with authorities, and adaptation to contemporary threats. However, the above standards do not take into account mechanisms for assessing damage from incidents and the costs of their elimination, thus limiting their application under conditions where time and resource constraints are critical.

The present work examines information security incident management processes in an enterprise, focusing on an analysis of existing approaches and models aimed at optimizing remediation costs, as well as increasing the responsiveness of incident response and minimizing damage. Here, the main aim is to develop a model that systematizes the incident management process to improve the efficiency of decision-making under resource and time constraints.

INCIDENT MANAGEMENT IN THE ENTERPRISE INFORMATION SECURITY SYSTEM

Information security incident management is critical to maintaining the integrity, confidentiality and availability of enterprise data. Effective incident management involves identifying, responding to and learning from security incidents to improve the overall security posture. An incident in the context of information security is any event or action that harms, or has the potential to harm, the confidentiality, integrity, or availability of information and information systems. The consequences of incidents, which can range from accidental errors to targeted attacks, can be quite serious for organizations.

Examples of incidents include virus attacks, data breaches, DDoS attacks, and unauthorized access. A distinction can be made between incidents and simple violations: an incident is an event that causes (or has the potential to cause) negative consequences to the secure operation of systems, while simple breaches typically do not cause significant consequences or damage and can be addressed without impacting the security of the system. Thus, incidents require more comprehensive analysis, rapid response, and potential application of appropriate remediation and protection measures.

Timely incident responses contribute to improving information security management processes. However, a link between incident response and security management functions is often absent. Therefore, enterprises need to establish integration between these two areas in order to develop a clear plan of action that can increase the trust and support of contractors [1].

[1] GOST R 59712-2022. National Standard of the Russian Federation. *Information protection. Computer incident management. Guide to responding to computer incident*. Moscow: Standartinform; 2023. 20 p. (in Russ.).

[2] https://gossopka.ru/ (in Russ.). Accessed July 15, 2024.

[3] GOST R ISO/IEC TO 18044-2007. National Standard of the Russian Federation. *Information technology. Security techniques. Information security incident management*. Moscow: Standartinform; 2008. 50 p. (in Russ.).

Real-time detection of security incidents is performed through specialized security management centers using information and information security event management systems. These centers, which collect, normalize, store, and correlate security events, are essential for rapid incident detection, loss minimization, vulnerability remediation, and IT service restoration [2].

Effective information security management requires a holistic approach, including the development and implementation of security policies, compliance training, and business-IT alignment[4]. For example, [3] notes that integrating digital forensics with incident handling can improve the effectiveness of incident response strategies.

Paper [4] shows that effective incident management requires a combination of technological solutions and management activities (development of security policies, training and information sharing between departments, etc.). Current incident management practices comply with ISO/IEC 27035 standards[5], but organizations often face certain challenges that are addressed through improved strategies.

Thus, effective enterprise information security incident management involves a combination of thorough incident analysis, strategic use of specialized information systems, and a holistic approach to security management, as well as the integration of technology and management solutions. By addressing communication gaps, using real-time monitoring tools, and implementing best practices, organizations can improve their incident response capabilities and overall security posture [5].

EXISTING INCIDENT MANAGEMENT MODELS

In order to improve the efficiency of incident management processes, various models have been proposed in the specialized scientific literature. For example, [6] considered cognitive modeling of destructive malicious attacks on critical information infrastructure objects and a model of states of critical information infrastructure subjects under destructive attacks in static mode.

Markovian chains and stochastic differential equations are used to describe the dynamics of security information and event management systems [7]. Supervised Markovian chains can be used to formalize and structure the decision support process for security event and incident management. This approach focuses on the dynamics of detecting and preventing cyber-attacks, as well as ensuring timeliness, validity, secrecy, and resource efficiency [8].

A number of studies have proposed simulation models for modeling incident management, which evaluate the effectiveness of incident management operations by analyzing real-world data and various strategies for deploying emergency response teams. Such models can predict the statistical patterns of cyberattacks and the effectiveness of incident response teams, enabling dynamic adjustments to maintain the required level of protection [9].

In [10], the implementation of a three-level incident management model using key metrics is shown to significantly improve the efficiency of incident handling. This model integrates process, technology and service metrics to improve the speed, user satisfaction and availability of incident handling channels.

In addition to the abovementioned models, various approaches based on formal languages and automata theory [11] (providing a structured approach to modeling and analyzing incident management processes to enable the identification and resolution of systemic problems), incident prioritization [12] (using feedback from analysts to correct errors in the assessment process to guarantee prompt resolution of the most critical incidents), etc., can be found in the scientific literature. By integrating feedback mechanisms and comprehensive security event management, organizations can maintain robust incident management processes that adapt to evolving threats and technological changes.

Thus, various models are used in information security incident management tasks, including mathematical, simulation, system dynamic and formal language approaches. These models aim to improve the identification and classification of incidents along with their appropriate responses to ensure effective and proactive security risk management [13]. Information security incident management acts as an important process that is directly related to ensuring three key elements: data integrity, authentication and availability [14]. The application of variation models can improve the processes of incident identification, classification and remediation. In order to achieve maximum efficiency, it is important to take into account the specifics of each organization, the degree of threats and the available resources to adapt the models to real conditions.

INFORMATION SECURITY INCIDENT MANAGEMENT MODEL AT THE ENTERPRISE

For describing information security incident management tasks, a model containing the following components can be used:

[4] Tran D.U. *Holistic Understanding of Information Security Posture*: Thesis Dr. Phil. University of Oslo, Department of Informatics, Series of Dissertations Submitted to the Faculty of Mathematics and Natural Sciences, no. 2696. 2023. https://www.duo.uio.no/bitstream/handle/10852/106520/PhD-Tran-2023.pdf?sequence=3&isAllowed=y. Accessed July 15, 2024.

[5] https://www.iso.org/standard/78973.html. Accessed July 15, 2024.

1. *Set of information security incidents* I = $\{I_1, I_2, \ldots, I_n\}$, where I_i is an information security incident recorded in the organization. Each incident is characterized by the parameters of detection time, degree of criticality, probability of threat realization, etc.
2. *Set of incident management actions* A = $\{A_1, A_2, \ldots, A_m\}$, where A_j is a certain action to eliminate the incident or minimize its consequences. Such actions can include blocking access, restoring data, implementing additional protective measures in the enterprise, etc.
3. *Incident response time* $T(I_i)$. This component of the model depends on the level of criticality of the incident and the resources available for response. Ideally, the higher the criticality of the incident, the shorter the response time should be.
4. *Incident damage function* $D(I_i)$ estimates the real or potential losses to the organization as a result of incident I_i (financial loss, reputational damage, data breach, etc.).
5. *Incident elimination probability function* $P(A_j, I_i)$ describes the probability of success of action A_j in relation to incident I_i. The probability depends on various factors (qualification of employees, execution time, type of incident, etc.).
6. *Incident elimination costs* $C(A_j, I_i)$ reflect how much resource (financial, time, and human) must be expended to implement action A_j in order to eliminate the incident I_i.

The key objective of the model is to minimize the total damage from information security incidents and the cost of their elimination. In order to solve this problem, it is advisable to minimize the following target function:

$$Z = \sum_{i=1}^{n}\sum_{j=1}^{m}\Big[D(I_i)(1-P(A_j,I_i)) + C(A_j,I_i)\Big] \to \min,$$

where Z is the total damage and costs for all incidents. It is advisable to take into account the limitations on available resources, response time and risk level:

$$T(I_i) \le T_{\max},$$

$$\sum_{i=1}^{n}\sum_{j=1}^{m} C(A_j,I_i) \le R,$$

$$P(A_j,I_i) \ge P_{\min},$$

$$I_i \in \mathrm{I},\ A_j \in \mathrm{A},$$

where $T_{\max}$ is the maximum allowable incident response time (can be set by the enterprise security policy); R is the total available budget (number of resources) allocated to eliminate information security incident; $P_{\min}$ is the minimum allowable probability of successful incident elimination.

The use of the above model implies the following steps:

1. *Incident detection.*
2. *Incident data collection* (criticality, possible damage, remediation costs).
3. *Assessing the likelihood of a successful resolution of an incident,* taking into account time and cost constraints.
4. *Optimization of actions* (based on the presented model, the action A_j that minimizes damage and costs is obtained).
5. *Monitoring and adjustment* (once all necessary actions to address the incident have been completed, the model can be adjusted to further analyze and prevent future incidents).

The proposed model helps to systematize the process of information security incident management and make optimal decisions for their elimination. However, the model contains a number of limitations and assumptions. The limitations include the need for accurate and up-to-date data, difficulties in estimating damage and probability, and failing to account for the human factor. The assumptions entailed in the model include linearity of damage and cost functions, independence of incidents, unambiguous definition of criticality, and others. When adapting the model to their own information security conditions, enterprises should take these aspects into account.

In order to effectively test the model, a set of synthetic data simulating various types of incidents and possible means for their elimination was used. The choice of synthetic data over real data is due to the limited availability of the latter: enterprises are often unable or unwilling to share information about their incidents for security and confidentiality reasons. In addition, the use of synthetic data enables the construction of more complete and reliable models based on a variety of hypothetical scenarios. When combined with theoretical analysis and development, this approach provides a foundation for a better understanding of information security incident response and management mechanisms. Thus, the use of synthetic data represents a valid method in the face of a lack of real-world information and is aimed at ensuring high-quality and reliable model validation.

Let the analysis at the enterprise reveal a number of information security incidents, each of which requires different actions for elimination, which are limited in resources and time. Initial data for calculations are presented in the Table 1.

Table 1. Initial data

Incident	Potential damage (*D*), c.u.	Time of reaction (*T*), h	Criticality
Customer database data leakage	200000	2	High
Virus attack on servers	100000	5	Medium
Unauthorized access to the network	50000	1	Low

Table 2. Possible actions to address information security incidents

Incident	Action	Cost (*C*), c.u.	Probability of success (*P*)
Data leakage (I_1)	Disconnecting external connections (A_1)	15000	0.7
	Customer notification and vulnerability correction (A_2)	25000	0.9
Virus attack (I_2)	Reboot servers and start antivirus (A_3)	10000	0.8
	Hardware replacement and data recovery (A_4)	20000	0.95
Unauthorized access (I_3)	Disabling an intruder session (A_5)	5000	0.6
	Network audit and configuration remediation (A_6)	8000	0.85

Suppose the enterprise has limited resources for response: the budget for incident elimination is $R = 50000$ c.u. and the maximum response time for all incidents is 6 h. For each incident, let there be several possible actions with different costs, elimination probabilities and execution times (Table 2).

In order to minimize damage subject to constraints, it is necessary to select actions for each incident. Consider the alternatives.

For I_1. Action A_1 is cheaper, but has a probability of success of 0.7, while action A_2 is more expensive, but has a higher probability of success (0.9). Given the criticality of the incident, it is appropriate to choose action A_2, since data leakage is highly damaging.

For I_2. Action A_3 is cheaper and has a sufficiently high probability of success (0.8). Given the budget constraints, we choose action A_3.

For I_3. Action A_5 is the cheapest, but its probability of success is only 0.6. In this case, it is more appropriate to choose action A_6, since its probability of success is much higher (0.85) and it can be fitted within the budget.

Let us build a model using the initial data. The target function and model constraints will have the following form:

$$Z = \sum_{i=1}^{3}\sum_{j=1}^{2}\left[D(I_i)(1-P(A_j,I_i)) + C(A_j,I_i)\right],$$

$$C(A_1,I_1) + C(A_3,I_2) + C(A_5,I_3) \leq 50000 \text{ c.u.},$$

$$T(I_1) + T(I_1) + T(I_1) \leq 6 \text{ h}.$$

The final model solution will be as follows:

- A_2 for incident 1 (cost is 25000 c.u.; probability of success is 0.9).
- A_3 for incident 2 (cost is 10000 c.u.; probability of success is 0.8).
- A_6 for incident 3 (cost is 8000 c.u.; probability of success is 0.85).

Having calculated the total costs and damage, we get $Z = 90500$ c.u. Thus, application of the model enabled the optimal actions to be selected in order to eliminate incidents with minimal costs and damage within the available budget and reaction time.

CONCLUSIONS

The incident management model proposed in this article can be used to minimize damage and costs through the optimal selection of actions under conditions of limited resources. Although the model has its limitations, its use in practice can significantly increase the level of information security of the enterprise.

The article proposes a model of information security incident management aimed at minimizing damage and costs. However, its practical use raises a number of issues related to simplifications: linearity of damage and cost functions, independence of incidents and unambiguous definition of their criticality. Such assumptions do not always reflect the complexity of real-life situations, where incidents are interrelated, and their consequences may be nonlinear. In addition, the model does not account for human error or the difficulty of obtaining accurate data during the response phases. Real-world conditions imply resource constraints, stressful situations, and the need for prioritization.

Despite these limitations, the proposed model significantly advances existing information security incident management standards and models. The model includes incident prioritization, criticality assessment, and resource allocation, to enable more informed and timely decision-making under time and resource constraints.

Thus, the model can complement existing approaches by offering tools for more accurate analysis and effective incident management focused on mitigating incidents and improving the overall resilience of the enterprise to information security threats.

In further research, it is planned to conduct testing on real data, which will enable a more accurate assessment of the effectiveness of the developed model. In addition, further research may involve integrating incident management models with other information security management processes. It will also be crucial to assess the impact of the human factor on incidents and develop effective mechanisms for employee training.

Authors' contributions

E.S. Mityakov—conducted the majority of the research, including the development of the concept of the incident management model, the definition of the model's key elements, the analysis of existing approaches, and the formulation of practical recommendations.

E.A. Maksimova—contributed to the literature review, formalization of the model, and the definition of incident management stages.

S.V. Artemova—participated in the analysis of existing incident management models, collecting and systematizing information about the practice of applying models in various organizations.

A.A. Bakaev—supervised the research process, provided guidance on problem formulation and model development, and conducted an expert evaluation of the obtained results.

Zh.G. Vegera—conducted numerical calculations based on the model, contributed to the interpretation of the modeling results, and participated in preparing the article for publication.

REFERENCES

1. Żywiolek J., di Taranto A. Creating value added for an enterprise by managing information security incidents. *System Safety: Human – Technical Facility – Environment.* 2019;1(1):156–162. https://doi.org/10.2478/CZOTO-2019-0020
2. Zidan K., Alam A., Allison J., Al-sherbaz A. Assessing the challenges faced by Security Operations Centers (SOC). In: Arai K. (Ed.). *Advances in Information and Communication. FICC 2024. Lecture Notes in Networks and Systems*. Springer; 2024. V. 920. P. 256–271. https://doi.org/10.1007/978-3-031-53963-3_18
3. Sackey A. Information Security Incident Handling in the Cloud. In: *Book Chapter Series on Research Nexus in IT, Law, Cyber Security & Forensics*. 2022. P. 103–108. https://doi.org/10.22624/AIMS/CRP-BK3-P17
4. Demina A.K. Information security incident management. *Mezhdunarodnyi zhurnal gumanitarnykh i estestvennykh nauk = International Journal of Humanities and Natural Sciences*. 2024;5–1(92):227–231 (in Russ.). https://doi.org/10.24412/2500-1000-2024-5-1-227-231, available from URL: https://elibrary.ru/aizkwa
5. Khorev P.B., Karpeeva V.A. Software tools for analyzing information security incidents based on monitoring of information resources. In: *2022 6th International Conference on Information Technologies in Engineering Education* (*Inforino*). IEEE; 2022. https://doi.org/10.1109/Inforino53888.2022.9782979, available from URL: https://elibrary.ru/qjfmzi
6. Maksimova E.A. Cognitive modeling of destructive malicious impacts on critical information infrastructure objects. *Trudy uchebnykh zavedenii svyazi = Proceedings of Telecommunication Universities*. 2020;6(4):91–103 (in Russ). https://doi.org/10.31854/1813-324X-2020-6-4-91-103, available from URL: https://elibrary.ru/lirtxz
7. Kotenko I.V., Parashchuk I.B. Model of security information and event management system. *Vestnik Astrakhanskogo gosudarstvennogo tekhnicheskogo universiteta. Seriya: Upravlenie, vychislitel'naya tekhnika i informatika = Vestnik of Astrakhan State Technical University. Series: Management, Computer Science and Informatics*. 2020;2:84–94 (in Russ). https://doi.org/10.24143/2072-9502-2020-2-84-94, available from URL: https://elibrary.ru/owaldx
8. Kotenko I., Parashchuk I. An approach to modeling the decision support process of the security event and incident management based on Markov chains. *IFAC-PapersOnLine.* 2019;52(13):934–939. https://doi.org/10.1016/j.ifacol.2019.11.314, available from URL: https://elibrary.ru/eqccxc
9. Dohtieva I., Shyian A. Simulation of the work of the information security incident response team during cyberattacks. *Herald of Khmelnytskyi National University.* 2021;303(6):115–123.
10. Mikryukov A.A., Kuular A.V. Development of an incident management model in an enterprise information system based on a three-tier architecture using key (relevant) metrics. *Otkrytoe obrazovanie = Open Education*. 2020;24(3):78–86 (in Russ.). https://doi.org/10.21686/1818-4243-2020-3-78-86, available from URL: https://elibrary.ru/fcqjjr
11. Mouratidis H., Islam S., Santos-Olmo A., Sanchez L.E., Ismail U.M. Modelling language for cyber security incident handling for critical infrastructures. *Comput. Secur.* 2023;128(8):103139. https://doi.org/10.1016/j.cose.2023.103139

12. Renners L., Heine F., Kleiner C., Rodosek G. Design and evaluation of an approach for feedback-based adaptation of incident prioritization. In: *2019 2nd International Conference on Data Intelligence and Security* (*ICDIS*). IEEE: 2019. P. 28–35. https://doi.org/10.1109/ICDIS.2019.00012
13. Maksimova E., Sadovnikova N. Proactive modeling in the assessment of the structural functionality of the subject of critical information infrastructure. In: Kravets A.G., Shcherbakov M., Parygin D., Groumpos P.P. (Eds.). *Creativity in Intelligent Technologies and Data Science* (*CIT&DS 2021*). *Communications in Computer and Information Science*. Springer; 2021. V. 1448. P. 436–448. https://doi.org/10.1007/978-3-030-87034-8_31
14. Alin Z., Sharma R. Cybersecurity management for incident response. *Romanian Cyber Security Journal.* 2022;4(1):69–75. Available from URL: https://elibrary.ru/ihxntg

СПИСОК ЛИТЕРАТУРЫ

1. Żywiolek J., di Taranto A. Creating value added for an enterprise by managing information security incidents. *System Safety: Human – Technical Facility – Environment.* 2019;1(1):156–162. https://doi.org/10.2478/CZOTO-2019-0020
2. Zidan K., Alam A., Allison J., Al-sherbaz A. Assessing the challenges faced by Security Operations Centers (SOC). In: Arai K. (Ed.). *Advances in Information and Communication. FICC 2024. Lecture Notes in Networks and Systems*. Springer; 2024. V. 920. P. 256–271. https://doi.org/10.1007/978-3-031-53963-3_18
3. Sackey A. Information Security Incident Handling in the Cloud. In: *Book Chapter Series on Research Nexus in IT, Law, Cyber Security & Forensics*. 2022. P. 103–108. https://doi.org/10.22624/AIMS/CRP-BK3-P17
4. Дёмина А.К. Управление инцидентами информационной безопасности. *Международный журнал гуманитарных и естественных наук.* 2024;5–1(92):227–231. https://doi.org/10.24412/2500-1000-2024-5-1-227-231, URL: https://elibrary.ru/aizkwa
5. Khorev P.B., Karpeeva V.A. Software tools for analyzing information security incidents based on monitoring of information resources. In: *2022 6th International Conference on Information Technologies in Engineering Education* (*Inforino*). IEEE; 2022. https://doi.org/10.1109/Inforino53888.2022.9782979, URL: https://elibrary.ru/qjfmzi
6. Максимова Е.А. Когнитивное моделирование деструктивных злоумышленных воздействий на объектах критической информационной инфраструктуры. *Труды учебных заведений связи*. 2020;6(4):91–103. https://doi.org/10.31854/1813-324X-2020-6-4-91-103, URL: https://elibrary.ru/lirtxz
7. Котенко И.В., Паращук И.Б. Модель системы управления информацией и событиями безопасности. *Вестник Астраханского государственного технического университета. Серия: Управление, вычислительная техника и информатика*. 2020;2:84–94. https://doi.org/10.24143/2072-9502-2020-2-84-94, URL: https://elibrary.ru/owaldx
8. Kotenko I., Parashchuk I. An approach to modeling the decision support process of the security event and incident management based on Markov chains. *IFAC-PapersOnLine.* 2019;52(13):934–939. https://doi.org/10.1016/j.ifacol.2019.11.314, URL: https://elibrary.ru/eqccxc
9. Dohtieva I., Shyian A. Simulation of the work of the information security incident response team during cyberattacks. *Herald of Khmelnytskyi National University.* 2021;303(6):115–123.
10. Микрюков А.А., Куулар А.В. Разработка модели управления инцидентами в информационной системе предприятия на основе трехуровневой архитектуры с использованием ключевых (релевантных) метрик. *Открытое образование.* 2020;24(3):78–86. https://doi.org/10.21686/1818-4243-2020-3-78-86, URL: https://elibrary.ru/fcqjjr
11. Mouratidis H., Islam S., Santos-Olmo A., Sanchez L.E., Ismail U.M. Modelling language for cyber security incident handling for critical infrastructures. *Comput. Secur.* 2023;128(8):103139. https://doi.org/10.1016/j.cose.2023.103139
12. Renners L., Heine F., Kleiner C., Rodosek G. Design and evaluation of an approach for feedback-based adaptation of incident prioritization. In: *2019 2nd International Conference on Data Intelligence and Security* (*ICDIS*). IEEE: 2019. P. 28–35. https://doi.org/10.1109/ICDIS.2019.00012
13. Maksimova E., Sadovnikova N. Proactive modeling in the assessment of the structural functionality of the subject of critical information infrastructure. In: Kravets A.G., Shcherbakov M., Parygin D., Groumpos P.P. (Eds.). *Creativity in Intelligent Technologies and Data Science* (*CIT&DS 2021*). *Communications in Computer and Information Science*. Springer; 2021. V. 1448. P. 436–448. https://doi.org/10.1007/978-3-030-87034-8_31
14. Alin Z., Sharma R. Cybersecurity management for incident response. *Romanian Cyber Security Journal.* 2022;4(1):69–75. URL: https://elibrary.ru/ihxntg

About the authors

Evgeny S. Mityakov, Dr. Sci. (Econ.), Professor, Acting Head of the “Subject-Oriented Information Systems” Department, Institute of Cybersecurity and Digital Technologies, MIREA – Russian Technological University (78, Vernadskogo pr., Moscow, 119454 Russia). E-mail: mityakov@mirea.ru. Scopus Author ID 55960540500, RSCI SPIN-code 5691-8947, https://orcid.org/0000-0001-6579-0988

Elena A. Maksimova, Dr. Sci. (Eng.), Associate Professor, Head of the “Intelligent Information Security Systems” Department, Institute of Cybersecurity and Digital Technologies, MIREA – Russian Technological University (78, Vernadskogo pr., Moscow, 119454 Russia). E-mail: maksimova@mirea.ru. Scopus Author ID 57219701980, RSCI SPIN-code 6876-5558, https://orcid.org/0000-0001-8788-4256

Svetlana V. Artemova, Dr. Sci. (Eng.), Associate Professor, Head of the “Information Protection” Department, Institute of Cybersecurity and Digital Technologies, MIREA – Russian Technological University (78, Vernadskogo pr., Moscow, 119454 Russia). E-mail: artemova_s@mirea.ru. Scopus Author ID 6508256085, RSCI SPIN-code 3775-6241, https://orcid.org/0009-0006-8374-8197

Anatoly A. Bakaev, Dr. Sci. (Hist.), Cand. Sci. (Juri.), Associate Professor, Director of the Institute of Cybersecurity and Digital Technologies, MIREA – Russian Technological University (78, Vernadskogo pr., Moscow, 119454 Russia). E-mail: bakaev@mirea.ru. Scopus Author ID 57297341000, RSCI SPIN-code 5283-9148, https://orcid.org/0000-0002-9526-0117

Zhanna G. Vegera, Cand. Sci. (Phys.-Math.), Associate Professor, Head of the Department of Higher Mathematics, Institute of Cybersecurity and Digital Technologies, MIREA – Russian Technological University (78, Vernadskogo pr., Moscow, 119454 Russia). E-mail: vegera@mirea.ru. Scopus Author ID 57212931836, RSCI SPIN-code 9076-5678, https://orcid.org/0000-0001-7312-3341

Об авторах

Митяков Евгений Сергеевич, д.э.н., профессор, и.о. заведующего кафедрой КБ-9 «Предметно-ориентированные информационные системы», Институт кибербезопасности и цифровых технологий, ФГБОУ ВО «МИРЭА – Российский технологический университет» (119454, Россия, Москва, пр-т Вернадского, д. 78). E-mail: mityakov@mirea.ru. Scopus Author ID 55960540500, SPIN-код РИНЦ 5691-8947, https://orcid.org/0000-0001-6579-0988

Максимова Елена Александровна, д.т.н., доцент, заведующий кафедрой КБ-4 «Интеллектуальные системы информационной безопасности», Институт кибербезопасности и цифровых технологий, ФГБОУ ВО «МИРЭА – Российский технологический университет» (119454, Россия, Москва, пр-т Вернадского, д. 78). E-mail: maksimova@mirea.ru. Scopus Author ID 57219701980, SPIN-код РИНЦ 6876-5558, https://orcid.org/0000-0001-8788-4256

Артемова Светлана Валерьевна, д.т.н., доцент, заведующий кафедрой КБ-1 «Защита информации», Институт кибербезопасности и цифровых технологий, ФГБОУ ВО «МИРЭА – Российский технологический университет» (119454, Россия, Москва, пр-т Вернадского, д. 78). E-mail: artemova_s@mirea.ru. Scopus Author ID 6508256085, SPIN-код РИНЦ 3775-6241, https://orcid.org/0009-0006-8374-8197

Бакаев Анатолий Александрович, д.и.н., к.ю.н., доцент, директор Института кибербезопасности и цифровых технологий, ФГБОУ ВО «МИРЭА – Российский технологический университет» (119454, Россия, Москва, пр-т Вернадского, д. 78). E-mail: bakaev@mirea.ru. Scopus Author ID 57297341000, SPIN-код РИНЦ 5283-9148, https://orcid.org/0000-0002-9526-0117

Вегера Жанна Геннадьевна, к.ф.-м.н., доцент, заведующий кафедрой высшей математики, Институт кибербезопасности и цифровых технологий, ФГБОУ ВО «МИРЭА – Российский технологический университет» (119454, Россия, Москва, пр-т Вернадского, д. 78). E-mail: vegera@mirea.ru. Scopus Author ID 57212931836, SPIN-код РИНЦ 9076-5678, https://orcid.org/0000-0001-7312-3341

Translated from Russian into English by Lyudmila O. Bychkova
Edited for English language and spelling by Thomas A. Beavitt