INTL JOURNAL OF ELECTRONICS AND TELECOMMUNICATIONS, 2023, VOL. 69, NO. 1, PP. 75-82
Manuscript received June 24, 2022; revised January, 2023. DOI: 10.24425/ijet.2023.144334

Adaptive Monitoring of Companies' Information Security

Valerii Lakhno, Saltanat Adilzhanova, Moldir Ydyryshbayeva, Aliza Turgynbayeva, Olena Kryvoruchko, Vitalyi Chubaievskyi, and Alona Desiatko

***Abstract*—Additions were proposed to the method of organizing the information security (IS) event management process of companies. Unlike existing solutions, the algorithm of the "Event handling" subprocess was detailed. This detailing is a complex, which includes the IS event processing substage. In addition, the proposed detailing of the "Event Handling" subprocess allows for covering the entire life cycle of an IS event. The performed research allows in practice to fill in potential gaps in information when creating a company's ISMS. An additional advantage of the proposed solution is the possibility of using this sub-process as an independent one. The proposed approach makes it possible to simplify the procedure for managing the information security of a company as a whole, as well as potentially reduce the costs of its construction for small companies and enterprises. Also, this sub-process can be considered as an independent information security management process, for example, for a company's CIS. The proposed solutions and additions, in contrast to similar studies, are characterized by invariance with respect to the methods of implementing the company's IS infrastructure solutions, and in particular its CIS. This ultimately allows, without changing the methodological tools, to scale this approach and adapt it to the ISMS of various companies.**

***Keywords*—information security; event processing; event management**

I. Introduction

SINCE the advent of first information systems (IS), and then corporate IS, the problem of information security (IS) in them has not lost its relevance. This is evidenced by the large-scale cyberattacks that swept across Ukraine and the world over the past year [1, 2]. The experience accumulated in the field of information security (IS), as well as new requirements for building an information security policy (ISP) of companies, made it possible to develop fairly effective recommendations for building an information security management system (ISMS). Moreover, today the ISMS integrates separate, often disparate measures aimed at ensuring the company's data protection and information security.

The central process in the ISMS of companies is the process of "Event Management" (or Event Management - EM). Only a competent organization of this process can ensure the proper level of the entire sequence of stages for the effective functioning of the company's ISMS. We are talking about the sequence of work: 1) Planning (Plan); 2) Implementation (Do); 3) Check (Check); Action (Act) [3, 4]. This chain of measures to ensure the company's IS has proven its effectiveness for preventive, reactive and/or retrospective measures in the framework of protecting corporate information of both small business entities and large companies.

Note that the solution of the problem related to the organization of the EM process within the framework of the company's ISMS is complex.

Depending on the scale of the company and the specifics of its business processes, various business entities use their own sets of ISMS processes and sub-processes. Also, as practice shows [5], approaches to the hierarchy and integration of ISMS processes and subprocesses also differ.

As Ukraine and its business entities integrate into the globalized international market, Ukrainian companies use ISO/IEC 2700x series standards as a methodological basis for building an ISMS [5,6].

However, it was noted that in some cases such formation of a company's ISMS based on ISO / IEC 2700x does not take into account the features of EM in domestic companies. This situation was a consequence of the fact that the international practice of building an ISMS of companies primarily relies on the Incident Management process. At the same time, many specialists in the field of IS of companies believe that EM is a less significant factor. Assuming that the priority in building an effective ISMS is given exclusively to Incident Management, one can lose sight of the following circumstance. The Incident Management process alone cannot embody an effective proactive approach within the delivery of IT services and the company's ISMS. And, therefore, does not provide the highest level of company's IS.

Limited attention to the implementation of the EM process in companies is often the result of the lack of a standardized and generally accepted methodology. Moreover, this methodology should be adapted to the PIB of companies. The complexity of solving this problem is primarily due to the volume and laboriousness of the preparatory work that must be carried out by the company's information security analysts. Moreover, the larger the scale of the company, the more parameters must be taken into account. The parameters taken into account may relate to both the organizational and technical levels of the IS or CIS of companies.

The foregoing determines the relevance of continuing research in the direction of further improvement within the ISMS of companies of ways to organize the EM process.

Valerii Lakhno is with National University of Life and Environmental Sciences of Ukraine, Kyiv, Ukraine (e-mail: lva964@nubip.edu.ua).

Saltanat Adilzhanova, Moldir Ydyryshbayeva and Aliza Turgynbayeva are with Al-Farabi Kazakh National University, Almaty, Kazakhstan (e-mail: asaltanat81@gmail.com, moldir_ydyryshbaieva@mail.ru, aliza1979@mail.ru).

Olena Kryvoruchko, Vitalyi Chubaievskyi and Alona Desiatko are with Kyiv National University of Trade and Economics, Kyiv, Ukraine (e-mail: {kryvoruchko_ev, chubaievsyi_vi, desyatko} @knute.edu.ua).

II. LITERATURE REVIEW

Quite a lot of research has been devoted to the issues of building an effective ISMS of a company. Note that some authors [7-11] interpret such a term as "event" (Event) differently in the context of ISMS. Such a "discrepancy" in itself creates difficulties in the work of the company's information security analysts. First of all, at the level of terminology.

In the analyzed works [7-11], the authors do not take into account the fact that during the implementation of the processes associated with the EM, initially the analyst or the IS auditor is interested in the fact of recording an event. Such a record or records may need to be captured in the data collection system of the company's information security service. Additionally, related events and states of the CIS are recorded, for example, one can talk about increased load levels of processors (or cores) of servers, atypical established network connections [12], etc. The examples given are also events. However, most regulatory documents on information security management [12- 15] do not pay due attention to such events. According to the authors of [13, 14], it is not necessary to narrow the definition of "event" when it comes to ensuring the company's IS. According to some authors [17, 18, 19], the discrepancy between the concept of EM can lead to actual duplication of events and activities. And this, in turn, gives rise to inefficient use of the resources of the CIS defense side. And, more importantly, it can lead to a situation where important events in the context of information security can be overlooked by the company's IS analyst [20, 21].

Within the framework of this study, the two most effective options (the USA and Europe) for organizing the EM process were analyzed. Namely, a detailed comparison was made between the NIST SP 800-92 standard [22] and the ITIL methodology [23].

In [22], Log Management issues are regulated. In this document, the log (Log) is treated as a record corresponding to a specific event in the system. A system is understood, for example, as a CIS or a company network. For its purposes and taking into account the context of interpretation, one can talk about the description of the log as a description of the Event Control.

In turn, [23] considers a set of ISMS processes. Including touched upon issues of Event management.

Table 1 provides a detailed comparison of these documents and practices, highlighting their strengths and weaknesses.

TABLE I
World practices for organizing the EM process in ISMS

Regulatory document	**Scope**	**Advantages and Features**	**Disadvantages**
NIST SP 800-92 [22]	US federal agencies	Key benefits and features for: Allocation of priority logs; setting policies and procedures for Log Management; creating and maintaining secure log management infrastructures; carrying out activities related to staff training; monitoring the status of EM in relation to all event sources; event rotation monitoring; archiving; life cycle control (LC or (Event Life Cycle)) of the log accounting system; ensuring synchronization of events; flexible configuration of log fixing procedures; documentation and reporting.	Inconsistency in the presentation of process aspects
ITIL Methodology [23]	Any company or organization	Key benefits and features for: Definition of key activities of the EM process; event registration; event records.	The practical aspects of the implementation of modern IT infrastructures of companies are not taken into account. The features of the CIS and the context of event processing are not taken into account. Especially within the LC.

Thus, the analysis of literature sources, including leading world standards [22], methods [23], theoretical and practical studies [7, 11, 16, 19] allows us to draw the following conclusion.

These documents do not contain a structured description of the EM process, which a priori includes the principles of continuous improvement. Recall these principles are contained in the sequence: 1) Planning (Plan); 2) Implementation (Do); 3) Check (Check); Action (Act) [3, 4]. In addition, most of the considered theoretical works did not take into account the most important aspects of the implementation of modern IT infrastructures of companies, the features of modern business processes, the features of processing events that are implemented within their life cycle.

Thus, it can be stated. It is necessary to form an integrated approach to the organization of EM processes. This integrated approach should take into account the interconnectedness of

other management processes. In addition, it must be harmonized with the ISO/IEC 2700x standards.

III. The purpose and objectives of the study.

The purpose of this study is to formulate additions to the method of organizing the information security (IS) event management process and to comprehensively detail the algorithm of the "Event Handling" subprocess

Tasks:

1) simplify the procedure for managing the company information security as a whole and reduce the cost of building it for small companies
2) supplement the adaptive IS monitoring scheme, which includes procedures for processing and analyzing IS events within their life cycle
3) scale this approach and adapt it to the ISMS of various companies

IV. Methods and models

Improving information security management processes suggests the need to take into account the entire set of management principles. These principles take into account the features of the following objects [21, 22]:

1. "Information Security";
2. "the need to prevent incidents";
3. "the need to mitigate incidents".

The traditional approach involves solving the problem of increasing the company's IS level by increasing the cost of ISMS. In most cases, this helps to reduce the level of risks associated with the loss of information. This approach, from the point of view of mathematical modeling of the company's IS, is based on the search and justification of the optimal values of information loss risk indicators, as well as on the search for the corresponding values of the minimum costs for building an effective company information security system. If one proceed from the assumption that the approach to building an ISMS should be systematic, then in modern realities (changing the landscape of cyber threats, increasing the complexity of cyber-attack scenarios), the emphasis should be on the adaptability and invariance of the methods for implementing the company's infrastructure IS solutions. The introduction of IT into the IS management processes, and, in particular, into the organization of the IS Event Management processes of companies, helps to prevent potential losses. Taking into account the previous works [3, 4, 17, 18, 20, 24], within the framework of building the company's ISMS, additions to the method of organizing the EM process were proposed, see Fig. 1.

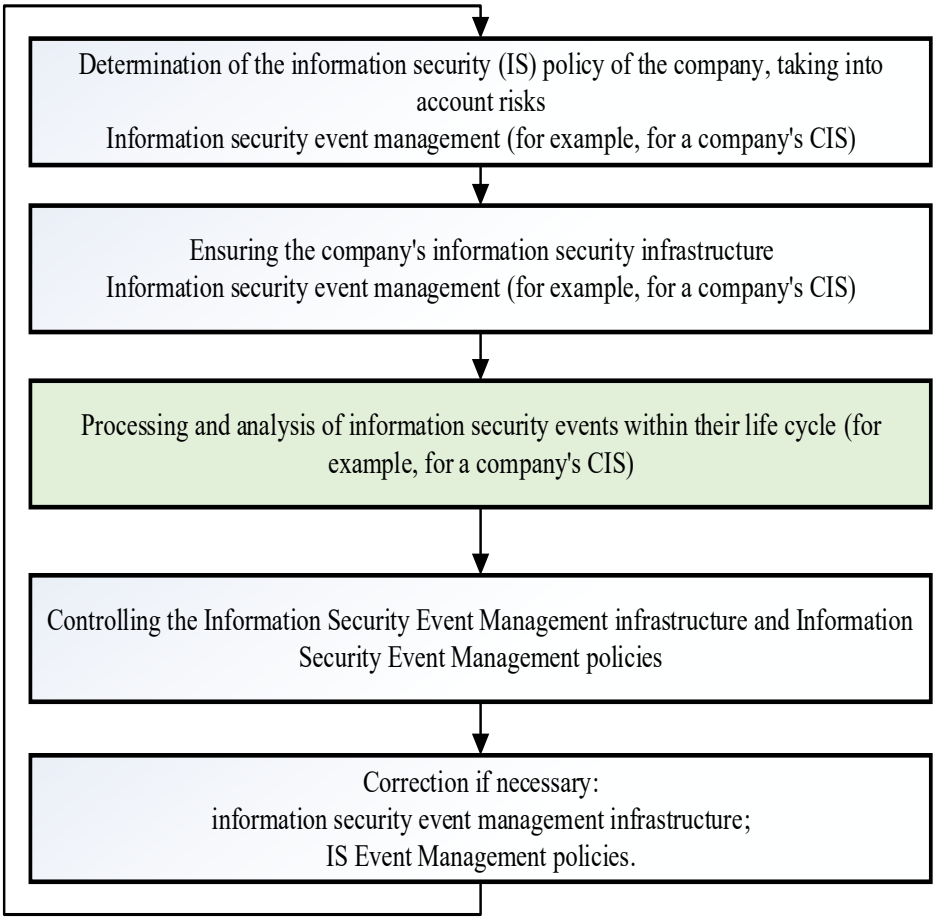

Fig. 1. Scheme of the adaptive process of managing IS events of the company

In contrast to existing practices, the proposed additions take into account the fact that:

- in practice, not all events are recorded;
- not all of the events that have been registered are sent for processing to SIEM (Security information and event management) [10] or SIP [25] class systems,
- event handling can fire new events.
- The scheme of the EM adaptive process proposed in Figure 1 allows, in our opinion, to take into account the features associated with:
- defining the EM policy for the company's CIS;
- providing infrastructure solutions for Event Management;
- event processing within their life cycle;
- control of infrastructure solutions for Event Management;
- EM policy control;
- if necessary, with the correction of infrastructure solutions for Event Management;
- if necessary, with EM policy adjustments.

Taking into account the fact that in the framework of this study, one is primarily interested in the economic aspects of organizing the management of the company's information security policy, one will dwell in more detail on such a sub-process of scheme 1 as "Processing and analysis of IS events within their life cycle (for example, for the company's CIS) ". In fig. 1 this sub-process is shown with light green shading.

Note that it is this sub-process, which is more detailed in Figure 2, which ultimately allows, based on the analysis of IS events, to minimize potential risks associated with possible losses of information resources (IR) of the company. And, consequently, it minimizes the potential economic damage caused by non-compliance with the company's IS policy.

The block diagram shown in Figure 2 includes the following main elements:

- The actual occurrence of the event. Based on changing or saving states that matter to IS. And besides, they can have or already have an impact on the performance of CIS infrastructure components (for example, networks). May have or already have an impact on the company's ISMS;
- Registration of events. At this stage, the corresponding entries in the logs (for example, in log files, database tables) are performed. At this stage, the registered events are ready to be sent;
- Sending an event message. At this stage, the event is transmitted to the "point", which acts as a centralized processing point. These can be hardware-software complexes of SIEM [10] or SIP [25] classes;
- Analysis of events. At this stage, metadata is extracted from the event;
- Event normalization. This stage corresponds to the procedure for converting the corresponding event fields into the most suitable representation for further processing.

Let's dwell separately on event processing, which includes such sub-stages as:

- Filtration. At this sub-stage, some parameters are excluded from the events, for example, according to the criterion of the importance of the event source. This ultimately reduces the time and resources spent on event processing;
- Aggregation. This sub-step corresponds to the procedure for combining similar or virtually identical events. A merged event can contain several separate but similar events. This additionally helps to reduce the time and resources spent on event processing;
- Correlation. This sub-step corresponds to finding relationships between two or more events. Correlation is based on special patterns based on rules and/or statistical values, etc.
- Saving the archive;
- Deleting events.

At the event processing sub-stage (in Fig. 2, this block is shown with a blue fill), the IS analyst can use the appropriate software, analyze the parameters that characterize the stability of the CIS IS management. At the same time, one will assume that the CIS can act as an object of a cybernetic attack. Below is a fragment of the model that makes up the computational core of the software designed to process IS events.

One will assume that the result of processing IS events can be the determination (as a special case) of the indicator, which characterizes a possible decrease in the functional efficiency of the CIS as a result of the destructive actions of the attacking side.

The following relation is true

$$\left(\Delta EF, R_c\right) \to \min_{0<q<1}, \qquad (1)$$

where $\Delta EF -$ is a parameter that characterizes a possible decrease in the functional efficiency of the CIS as a result of the destructive actions of the attacking side;

$R_c -$ resource costs associated with building an effective ISMS of the company (in particular, its CIS);

$q -$ the probability of providing IS to the CIS (in particular, its CIS).

Researches devoted to the search for optimal solutions to this problem are the subject of many studies by various authors. At the same time, various methods and models can be used to find a solution, see Fig. 3. This issue is beyond the scope of this study, so one does not dwell on it in detail.

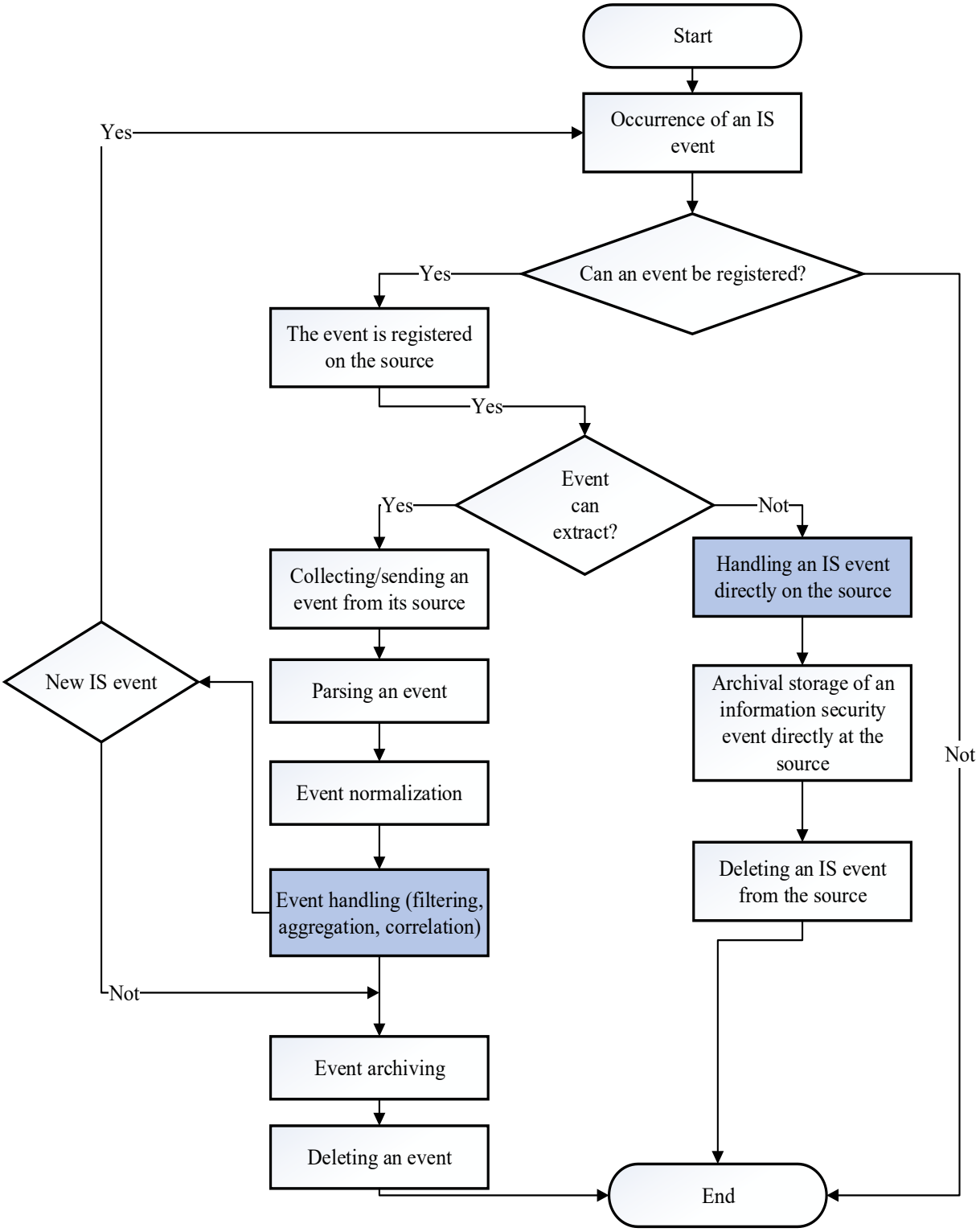

Fig. 2. Processing and analysis of IS events within their life cycle

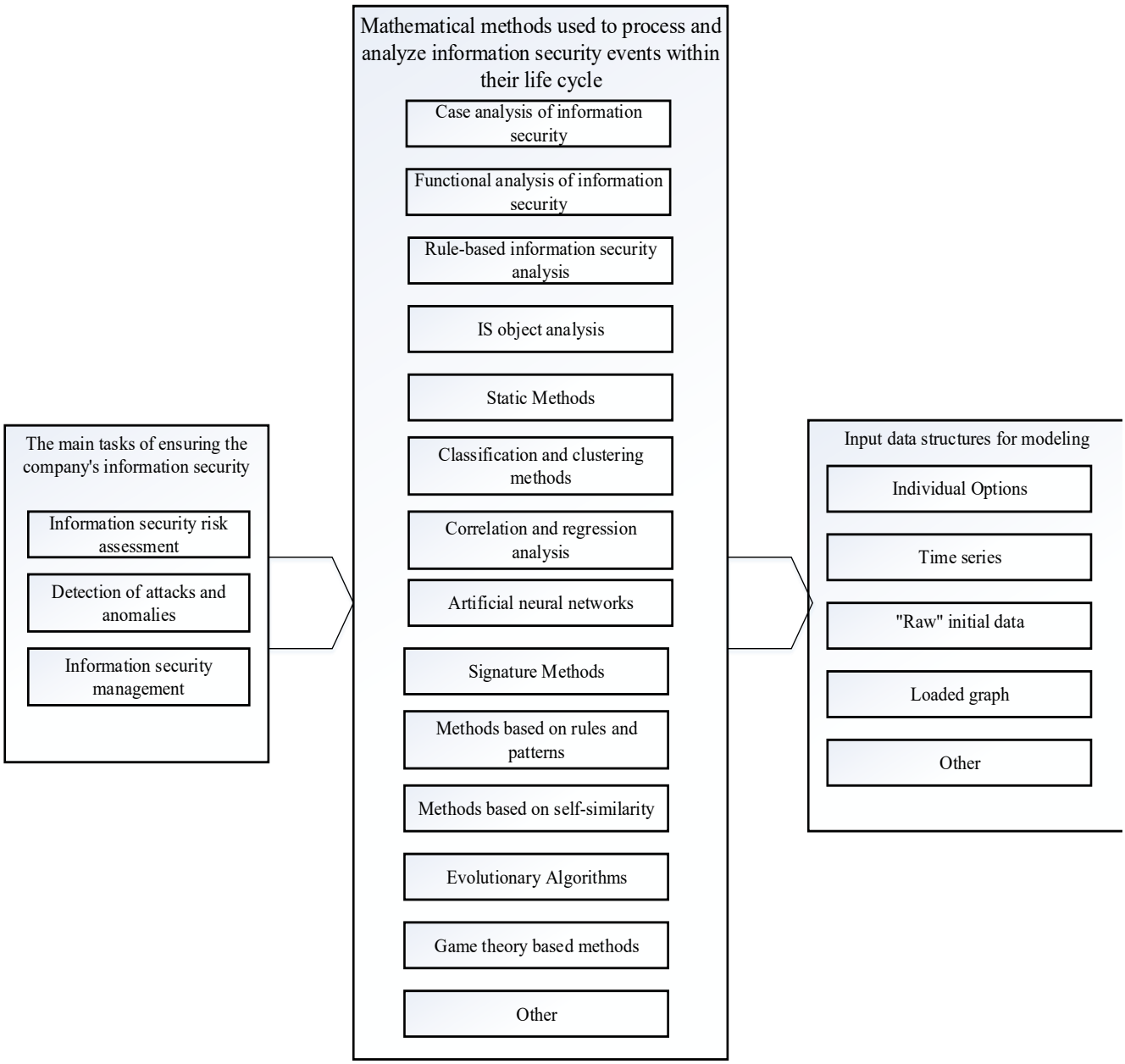

Fig. 3. Scheme of correspondence between the tasks of ensuring the company's IS, and mathematical methods for their solution

Researches devoted to the search for optimal solutions to this problem are the subject of many studies by various authors. At the same time, various methods and models can be used to find a solution, see fig. 3. This issue is beyond the scope of this study, so one does not dwell on it in detail.

The solutions and additions proposed in our study, in contrast to similar studies by others by the author, for example, in [17, 18, 24, 26, 27, 28], are characterized by invariance with respect to the methods of implementing the company's infrastructure IS solutions. This statement is also true about the IS of CIS companies. The proposed additions ultimately allow, without changing the methodological tools, to scale this approach and adapt it to the ISMS of various companies.

Further development of research in this direction can be work related to the organization of IS event management processes. These works precede the formation of a logical and integrated ISMS of the company.

Synthesis of adaptive monitoring procedures, see fig. 4 [28] and Management of company IS events in modern conditions is a non-trivial task. This is not least dictated by the variety of IS tasks and the dynamic features of protected objects. The implementation of the systems theory methodology made it possible to formulate the general principles of such adaptive monitoring and IS event management:

- Hierarchical connectivity of IS events;
- Integrity;
- The similarity of IS events.

On fig. Figure 4 conceptually shows an extended scheme of adaptive IS monitoring, including procedures for processing and analyzing IS events within their life cycle.

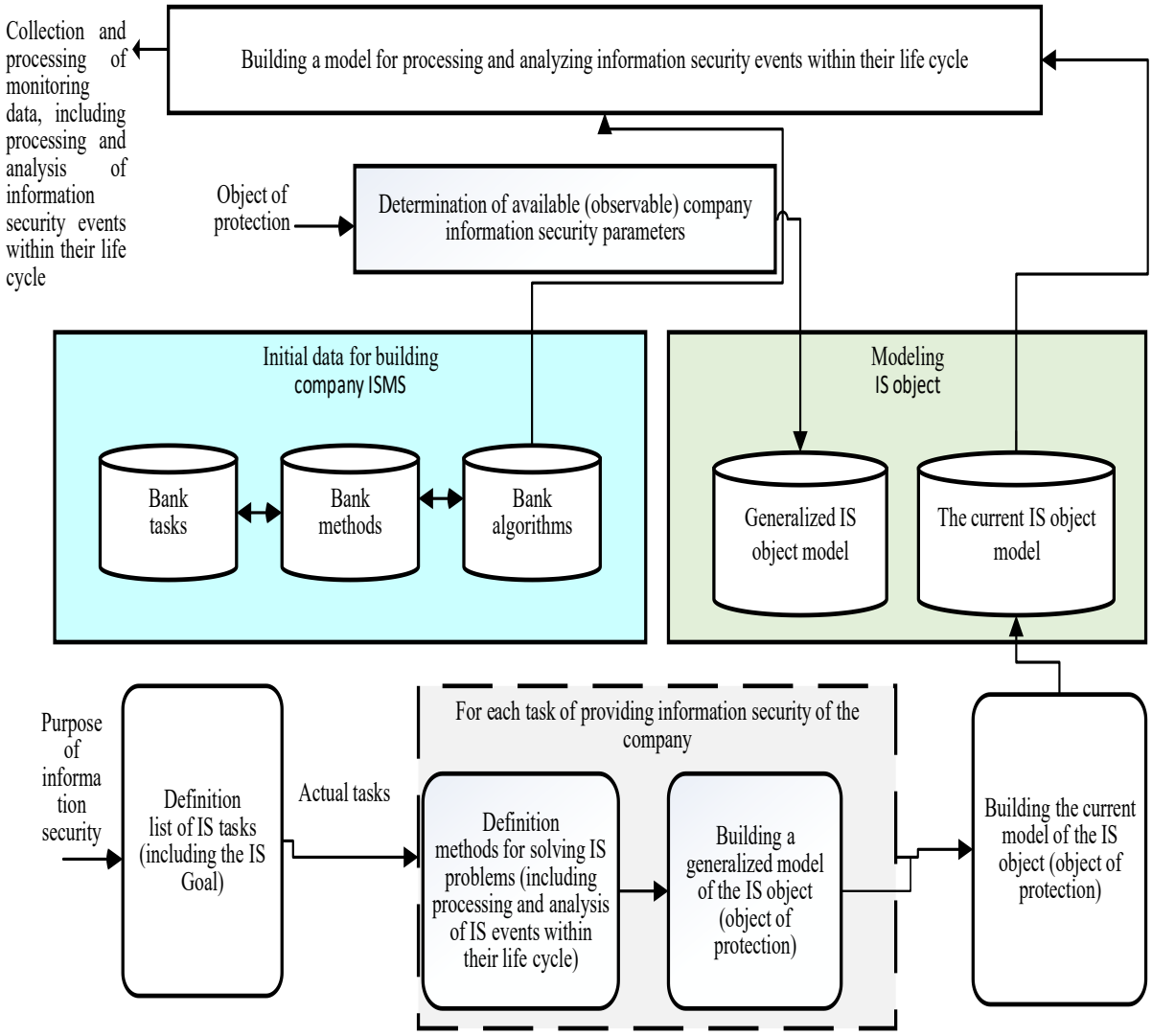

Fig. 4. Extended scheme of adaptive IS monitoring, including procedures for processing and analyzing IS events within their life cycle

V. Discussion of the Results of the Study.

In the course of the process of algorithmization of procedures related to the processing and analysis of IS events within their life cycle, and following the principle of integrity, protected objects (for example, corporate information systems) should be analyzed from different angles. Such an analysis begins with individual components of the object of protection and ends with its analysis as a whole, including the analysis of the external environment. The implementation of the principles of integrity and similarity of IS events in the course of managing the adaptive parameters of monitoring procedures and processing of IS events within their life cycle consists in building mutual mappings between IS tasks and the corresponding methods for their solution. At the same time, the fundamental role is played by the available data necessary to use the potential of a particular method or model in the processes of processing and analyzing IS events within their life cycle. Based on such mappings, monitoring schemes can be optimized. With this optimization, it is important to focus the attention of the IS analyst on the hierarchical connectivity of IS events. Such hierarchical connectivity makes it possible to obtain a bijective display of the IS of the protected object, having the necessary data for monitoring IS events. The proposed scheme for adaptive IS monitoring, including the procedures for processing and analyzing IS events within their life cycle, complies with the principles of hierarchical connectivity, integrity, and similarity of IS events

Conclusion

Additions to the method of organizing the IS event management process for the company are proposed. Unlike

existing solutions, the algorithm of the "Event processing" sub-process is detailed. This detailing is complex. In addition, it covers the life cycle of an IS event. The studies were performed to make it possible in practice to fill in potential information gaps when creating a company's IS management system. An additional advantage of the proposed solution is the possibility of using this sub-process as an independent one. This makes it possible to simplify the procedure for managing the IS of a company as a whole and reduce the costs of its construction for small companies. Also, this sub-process can be considered as an independent process of IS management, for example, for a company's CIS.

The scheme of adaptive IS monitoring has been supplemented, which includes procedures for processing and analyzing IS events within their life cycle. The proposed scheme complies with the principles of hierarchical connectivity, integrity and similarity of IS events.

The proposed solutions and additions, in contrast to similar studies, are characterized by invariance with respect to the methods of implementing the company's IS infrastructure solutions, and in particular its CIS. This ultimately allows, without changing the methodological tools, to scale this approach and adapt it to the ISMS of various companies.

REFERENCES

[1] R Akhmetov, B., Lakhno, V., Malyukov, V., Akhmetov, B., Yagaliyeva, B., Lakhno, M., Gulmira, Y. A Model for Managing the Procedure of Continuous Mutual Financial Investment in Cybersecurity for the Case with Fuzzy Information, (2022) *Lecture Notes on Data Engineering and Communications Technologies, 93,* pp. 539-553. https://doi.org/10.1007/978-981-16-6605-6_40

[2] Begun AV, Osipova OI, Urdenko OG Pro odnu z sytuatsiynykh modeley upravlinnya informatsiynoyu bezpekoyu pidpryyemstva [About one of the situational models of information security management of the enterprise]. *Modeling and information systems in economics: collection. Science. pr. / Ministry of Education and Science of Ukraine, SHEI "Kyiv. nat. econ. Univ. Vadim Hetman "; [editor: OE Kaminsky (ed.), etc.]. - Kyiv: KNEU, 2020. - Issue. 100.* - P. 39–50. https://doi.org/10.33111/mise.100.13

[3] Bhatt, S., Manadhata, P. K., & Zomlot, L. (2014). The operational role of security information and event management systems. *IEEE security & Privacy, 12(5),* 35-41. https://doi.org/10.1109/MSP.2014.103

[4] Culot, G., Nassimbeni, G., Podrecca, M., & Sartor, M. (2021). The ISO/IEC 27001 information security management standard: literature review and theory-based research agenda. *The TQM Journal*. https://doi.org/10.1108/TQM-09-2020-0202

[5] Fonseca-Herrera, O. A., Rojas, A. E., & Florez, H. (2021). A model of an information security management system based on NTC-ISO/IEC 27001 standard. *IAENG Int. J. Comput. Sci*, *48*(2), 213-222.

[6] Gabriel, R., Hoppe, T., Pastwa, A., & Sowa, S. (2009, March). Analyzing malware log data to support security information and event management: Some research results. *In 2009 First International Confernce on Advances in Databases, Knowledge, and Data Applications (pp. 108-113). IEEE.* https://doi.org/10.1109/DBKDA.2009.26

[7] ITIL Service Operation Second edition. 2011. C. 58-72.

[8] Kang, K., & Kim, J. (2015). A case study on converged security with event correlation of physical and information security. *International Journal of Security and Its Applications, 9(9),* 77-94. https://doi.org/10.14257/ijsia.2015.9.9.08

[9] Khokh, V. D., Meleshko, E. V., & Smirnov, O. A. (2017). Doslidzhennya metodiv audytu system upravlinnya informatsiynoyu bezpekoyu. [Follow-up methods for auditing information security management systems]. *Management systems, navigation and communication. Collection of scientific works, 1(41),* 38-42.

[10] Ključnikov, A., Mura, L., & Sklenár, D. (2019). Information security management in SMEs: factors of success. *Entrepreneurship and Sustainability Issues, 6(4),* 2081. . https://doi.org/10.9770/jesi.2019.6.4(37)

[11] Ko, K., Kim, H. K., Kim, J., Lee, C. Y., Cha, S. G., & Jeong, H. C. (2009, August). Design and Implementation of SIP-aware Security Management System. *In International Workshop on Information Security Applications* (pp. 10-19). Springer, Berlin, Heidelberg. https://doi.org/10.1007/978-3-642-10838-9_2

[12] Kuznetsov, A. V. (2015). A method of organizing the event management process in terms of their processing within the enterprise information security management system. *Information security issues,* (2), 57-62.

[13] Lakhno, V., Plyska, L. Analysis of Models for Selection of Investment Strategies, (2021) 2020 *IEEE International Conference on Problems of Infocommunications Science and Technology, PIC S and T 2020 - Proceedings, № 9468024,* pp. 43-46. https://doi.org/10.1109/PICST51311.2020.9468024

[14] Lallie, H. S., Shepherd, L. A., Nurse, J. R., Erola, A., Epiphaniou, G., Maple, C., & Bellekens, X. (2021). Cyber security in the age of covid-19: A timeline and analysis of cyber-crime and cyber-attacks during the pandemic. *Computers & Security*, *105*, 102248. https://doi.org/10.1016/j.cose.2021.102248

[15] Lopez, M. A., Silva, R. S., Alvarenga, I. D., Rebello, G. A., Sanz, I. J., Lobato, A. G., & Pujolle, G. (2017, October). Collecting and characterizing a real broadband access network traffic dataset. *In 2017 1st Cyber Security in Networking Conference (CSNet) (pp. 1-8). IEEE.*

[16] Miller D. et al. *Security information and event management (SIEM) implementation.* – McGraw-Hill, 2011.

[17] Nadezhdin, E. N., & Belyanskaya, O. V. (2019). K voprosu analiza ustoychivosti sistemy upravleniya riskami informatsionnoy bezopasnosti. In Sovremennyye instrumental'nyye sistemy, informatsionnyye tekhnologii i innovatsii. [On the issue of stability analysis of the information security risk management system]. *In Modern tool systems, information technology and innovation* (pp. 144-148).

[18] National Institute of standards and technology. Special Publication 800-92. Guide to Computer Security Log Management. 2006. - 61 p

[19] Ovcharenko M. Yu. Analysis of correlation rules in information security and security management systems / M. Yu. , *8–9 April 2021 - VA ZS AR; NTU "KhPI"; NAU, SE "PDPRONDIAVIAPROM"; UmZh, 2021. - Vol. 2, sections 3-5.*– pp. 46. https://doi.org/10.30837/IVcsitic2020201358

[20] Poltavtseva, M. A., & Zegzhda, D. P. (2020). Adaptive monitoring of CFS information security from the point of view of a systematic approach. *Methods and technical means of ensuring information security, (29), 88*. pp. 1661-1669. https://doi.org/10.3390/sym13122425

[21] Renners, L., Heine, F., & Rodosek, G. D. (2017, September). Modeling and learning incident prioritization. *In 2017 9th IEEE International Conference on Intelligent Data Acquisition and Advanced Computing Systems: Technology and Applications (IDAACS) (Vol. 1, pp. 398-403). IEEE.* https://doi.org/10.1109/IDAACS.2017.8095112

[22] Shatnawi, M. M. (2019). Applying Information Security Risk Management Standards Process for Automated Vehicles. *Bánki Közlemények (Bánki Reports), 2(1),* 70-74.

[23] Sievierinov O.V., Ovcharenko M.Y. Analysis of correlation rules in Security information and event management systems. *Computer and information systems and technologies.* 2020. P. 24-25. https://doi.org/10.30837/IVcsitic2020201358

[24] Siponen, M., & Willison, R. (2009). Information security management standards: Problems and solutions. *Information & management, 46(5),* 267-270. https://doi.org/10.1016/j.im.2008.12.007

[25] Tanadi, Y., Soeprajitno, R. R. W. N., Firmansah, G. L., & El Karima, T. (2021). ISO 27001 Information Security Management System: Effect of Firm Audits in Emerging Blockchain Technology. *Riset Akuntansi dan Keuangan Indonesia*, *6*(2), 198-204. https://doi.org/10.23917/reaksi.v6i2.15146

[26] Ushatov V., Severinov O.V. Problems of operational detection and response to information security incidents. – Kharkiv: KNURE, 2019. - pp. 104–105. (2019).

[27] White, G. (2021). Generation Z: Cyber-Attack Awareness Training Effectiveness. *Journal of Computer Information Systems*, 1-12. https://doi.org/10.1080/08874417.2020.1864680

[28] Wu, W., Shi, K., Wu, C. H., & Liu, J. (2021). Research on the Impact of Information Security Certification and Concealment on Financial Performance: Impact of ISO 27001 and Concealment on Performance. *Journal of Global Information Management (JGIM)*, *30*(3), 1-16. https://doi.org/10.4018/JGIM.20220701.oa2