Assessment of the Protection and Efficiency of Work of Information Systems Used in the Mining Industry

Gulzira Mukasheva[1], *Natalya* Stenina[2], and *Kakim* Sagindykov[3]

[1]Kazakh Humanitarian-Law Innovative University, Semey, Kazakhstan
[2]Kuzbass State Technical University named after T.F. Gorbachev, Kemerovo, Russia
[3]L.N. Gumilyov Eurasian University, Nur-Sultan, Kazakhstan

Abstract. The issues of digitalization of the mining industry, including open-pit mining, are considered. The issues of the use of semantic systems as an element of information flows, allowing to determine and select the right decisions in the process of mining management, in particular, in the mining of minerals by open mining, are covered. The article formulates requirements for semantic networks for the description of material in computer-aided learning tools and analyzes the most well-known models of semantic networks.

1 Introduction

Digitization of all spheres of activity and sectors of the national economy is an inevitable process that has fully affected the mining industry. This process is associated with a huge flow of digital information, the creation of databases, the automation of technological processes of production and mining. Information stored and transmitted in digital form, especially representing a certain level of secrecy, needs protection, for which all sorts of protection systems are developed. Information Security System (GIS) is a complex set of software, hardware, cryptographic means of organization, methods and measures designed to protect information.

The level of information security of mining enterprises, including enterprises and organizations that extract minerals in the open way, has a high need. In addition, the need and objectives of data protection can be completely different and different tasks. Their definition and solution can be complex organizational and specialized tasks that require an integrated approach. The organization of each transfer of support may have several mechanisms with particular efficiency, complexity, and the ability to perform and maintain. In this regard, it is important to assess the effectiveness of the decisions made and taken to ensure the safety of information on the organization of technological processes in the mining industry.

The method of successive assignments is an iterative man-machine procedure in which the developer analyzes the change in others using acceptable increments of one parameter (in particular, by specifying a decrease in the safety factor), making a decision on the admissibility of assignments [1].

Currently, there are many works on computer security in the preparation of data and information protection systems [2].

However, many methodological and methodological aspects of data protection are questionable. This is due to the limited study of certain aspects of protection, due to the complexity of these systems, as well as the constant change in the list of risks and the lack of a unified approach to the creation, evaluation and analysis of protection systems.

For example, despite the work of many companies engaged in the development of antivirus software, various specialized conferences and regular classes in computer virology, there is still no uniform approved and standardized virus classification table. Also, the information security assessment system and security security criteria are insufficient, which makes the task necessary and relevant.

2 Discussion

In practice, information security at mining enterprises is carried out under the conditions of random exposure to various factors. Some of them are systematized in standards, some of which are unknown in advance and may reduce effectiveness or even violate the measures envisaged. In evaluating the effectiveness of information security, both objective and subjective factors must be taken into account.

The project is designed to create a web version of the archive, consisting of various paper documents. The functionals implemented in the system provide archivist operators with easy-to-use tools for inserting and updating information, as well as provide convenient and transparent interfaces that allow end users to visualize and search for information stored in the archive [3].

Models that evaluate the effectiveness of information security systems do not provide quantitative methods for determining the value of security against unauthorized access to an information system (IS). Analysis and evaluation of such indicators, as a rule, are provided by specialists in the field of information technology.

Risk management mainly takes into account the increased likelihood of information systems functioning. Such threats are usually insignificant or preventable, but in reality a lot of attention needs to be paid to a lot of damage and a lower probability. This can lead to unreasonably high costs for creating and maintaining an information security system.

Based on the construction of a threat model, the most optimal way to create GIS has been developed, which is presented in the form of threats and measures to protect information.

In information security models (K), the event's hazard coefficient (K) from damage (Yi) caused by unauthorized actions (Hi). In the case of unauthorized actions, damage occurs regardless of the cost of creating an automated system. Thus, the task of creating a data protection system to neutralize or reduce the damage from unauthorized actions.

The task of information security is to provide a system of measures in the development of a model that solves the problems of creating, using and evaluating the effectiveness of GIS. The GIS model is shown in Figure 1.

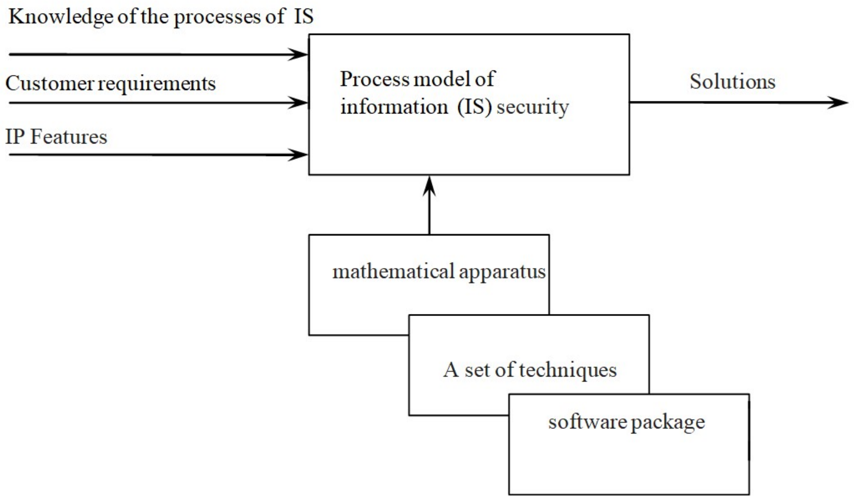

Fig. 1. Model GIS.

The main goal of the model is to ensure the process of creating an information security system, correctly assessing the effectiveness of solutions and selecting the optimal technical implementation of the information security system.

Features of solving the problem of creating a security system:
- uncertainty of the initial information on the composition of IP and threats;
- multi-element tasks associated with the need to account for a large number of individual indicators of GIS;
- availability of quantitative, qualitative indicators that must be considered when solving problems of development and implementation of GIS.

Such a model must meet several requirements.
1. General provisions for use as:
- guidelines for creating GIS;
- methods of forming indicators and requirements of SZI;
- devices for assessing GIS.
2. Accessibility properties:
- universality;
- complexity;
- visibility.
3. Allow:
- setting various levels of protection;
- obtaining a digital assessment;
- GIS assessment.

The effectiveness and security of GIS is expressed in relation to the beneficial results of its operation in relation to the creation of resources expended. The main indicator of the effectiveness of SZI is the coefficient of efficiency K_{eff}, the indicator of marginal costs of SZI:

$$K_{eff} = \frac{C_{SZI}}{M_{SZI}} \quad (1)$$

Where C_{SZI} – is the cost of creating a GIS;
M_{SZI} – marginal costs of GIS.

To assess the criterion of "cost-effectiveness" coefficient is applied K_{eff} . The effectiveness of information security systems depends on the “damage-cost” indicator, since using GIS it increases its costs and risks of information violation. Thus, the effectiveness of the protection system, at the lowest cost to create it, requires the maximum cost of breaking it.

General approaches to quantifying the effectiveness of GIS correspond with the modern theory of evaluating the effectiveness of the system, the quality of any object, including GIS, only in the process of its intended use, therefore, the assessment of the effectiveness of the application is the most objective.

The organization and application of GIS in open pit mining is really associated with unknown events and therefore always include elements of uncertainty. In particular, there are other similar reasons, such as complete information and factors for making management decisions. Thus, for example, considerable uncertainty is suitable for phase design. The level of project implementation decreases, but the effectiveness of GISis not reflected and is not described adequately by deterministic indicators.

Testing, certification or authorization strategies do not pass without the complete vulnerability of the properties of a GIS or its individual elements and do not take into account the intermittent nature of attacks. Therefore, only the probability characterizing the degree of capabilities of a real GIS under a given set of conditions with the level of its adaptation to the required level of security can serve as a characteristic of the quality of SZI. In the general theory of the system, this characteristic is called the probability of achieving the goal of the operation and the probability of completing the information security system task. This probability should be based on criteria for evaluating the effectiveness of GIS and a set of indicators. Evaluation criteria are the concepts of suitability and optimality.

The development of data protection systems can be a comprehensive step-by-step preparation, starting with identifying the causes of GIS and aimed at maintaining the effectiveness of the updated GIS adaptation. The main stage of creating data protection should have an understanding and requirements for their protection.

To improve the performance of automated information systems, an urgent task is the algorithm, since exponential dependence on the purpose of the study and execution of tasks. And the size of the task, in turn, depends on the complexity of the GIS, increasing with the advent of new security threats, and the complexity of GIS, complicated by the development of the information system itself, in which the protection system is created.

The criteria for evaluating the work of GIS can be categories of suitability and optimality. This system is evaluated according to the requirements set forth in this system, optimality is achieved by adopting one of the characteristics of the extreme value [4]. With several characteristics, and for each, the situation in which it is necessary to achieve extreme values is difficult. Then you need to turn to complex methods that get integrated aggregates.

Suitability includes the fulfillment of all established requirements for GIS, and optimality is the achievement of one of the characteristics of an extreme value while observing restrictions and conditions on other properties of the system. When choosing a specific criterion, it is necessary to coordinate it with the goal that is downloaded to the GIS. In the synthesis system, the problem of solving a problem with a multi-criteria indicator arises. Some authors consider performance indicators for solving problems of various GIS structures. It is also recommended to use performance indicators of a potentially temporary nature in accordance with the value of the distribution function [5].

3 Results

In the study of GIS, it is advisable to use a systematic approach, involving the adoption of an object as a system operating in a specific area. The system approach examines the integrity of the object, its internal structure, the relationship with external factors. This involves the analysis of common elements, the transition to individual elements. Evaluation components are developed in three vectors: "fundamentals", "directions", "stages".

Each vector consists of four, five, and seven elements. The effectiveness of GIS can be assessed according to the specified requirements on the basis of finished software products that optimize the system. Such an approach strengthens the connection between security elements, but it does not take into account the stochastic nature of events and phenomena arising in the process of protecting information.

Since information security tools are associated only with the cost of allocating funds, costs can be reduced and funds can be released. But in the future, this will allow mining companies to solve strategic tasks related to improving market adaptation and ensuring competitiveness, since information security affects these processes.

Therefore, many companies that specialize in open pit mining are investments in information security and digitalization of production. In this regard, we can expect specific results of creating GIS, the ability to assess the return on investment and their effectiveness. The main economic efficiency, calculated by the company when creating GIS, is to reduce damage in the implementation of information security risk. To assess the effectiveness of GIS, you can calculate the effectiveness of investments in information security. There are ways to calculate return on investment capital (Returnof Investments - ROI). ROI is the ratio of the economic effect derived from the project to the cost of implementing this project as a percentage. The obtained value should be compared with the reference project, that is, with the average for all indicators in this segment [6-7].

In order to evaluate the guarantee of protection, it is necessary to formulate it in digital form. Information security regulations use a classification approach. The most constructive are the most common probabilistic methods in the practice of ensuring safety in other areas. In accordance with these methods, the levels of security of GIS are changed to the corresponding prices of indicators. To solve the problem, one can present a theory of statistical solutions that allows one to find the optimal level of security guarantees.

The assessment of the optimal level of security depends on the damage associated with an error in the choice of a specific value of the information protection performance indicator. To obtain a quantitative risk assessment, it is necessary to know the number of distribution of random variables. This often limits the quantitative study of the level of security guarantees provided by an IMS, but in many practical situations an assessment can be made. [8-10]

Table 1. Indicators of the effectiveness of GIS.

GIS requirements	Types of GIS effectiveness indicator
Offensive event	Event probability
Achievement of characteristics	The probability of reaching no less than the required level
Deviation from the specified characteristics	Standard deviation from the desired result

Table 2. Criteria for the effectiveness of GIS.

concept of the effectiveness of GIS	Performance criteria
Suitability	Satisfactory result
	Valid warranty
Optimality	Good result
	Average result
	Guaranteed result

Most methods for evaluating the effectiveness and protection of GIS have certain disadvantages. To solve this problem, you can use several criteria, and then average the quantitative indicators with confidence coefficients for different methods. Another solution is to use the methods of clear logic, as for averaging various methods of evaluation and translation of a fuzzy linguistic expert opinion on a quantitative value.

4 Conclusion

1. A general analysis of the work of GIS at mining enterprises shows that there is currently no assessment of the security of information systems.
2. Fuzzy logic methods are a promising way to assess the state and effectiveness of information systems protection.

References

1. A.B. Diallo, D.T. Dim, S.R. Bakasov, V.N. Bogatikov, Eurasian Scientific Journal, **1:10** (2018)
2. M. Johanson, *Dzhesper Security. Resources Windows Server* (Russian Edition Pub., Moscow, 2009)
3. A. Marchuk, A. Nemov, K. Fedorov, S. Antyoufeev, ADVIS, **2,** 20 (2002)
4. R.Vacul´ın, K.Wiesner, K.Sycara, IEEE Computer Society, **12,** 87 (2008)
5. V. I. Esin, S. G. Rassomakhin, V. M. Grachev, N. G.Polukhina, Bulletin of the Lebedev Physics Institute, **41:5**, 123 (2014)
6. A. Fedorchenko, A. Chechulin, I. Kotenko, Proceedings – 23rd Euromicro International Conference on Parallel, Distributed, **2,** 559 (2015)
7. A. I. H. Suhaimi, Y. Goto, J. Cheng, Transactions on Information and Systems. **E97:6**, 1516 (2014)
8. H.Y. Zhao, X.Y. Liu, Z. Jing, Applied Mechanics and Materials, **397:400**, 2536 (2013)
9. N.V. Mostovaya, E.V. Lebedenko, Proceedings of the XXIV-th International Open Science Conference, **1,** 97 (2019)
10. Fuzzy, II Articlein Cybernetics and Systems Analysis, **52:1**, 38·(2016)