2023 IEEE Ural-Siberian Conference on Biomedical Engineering, Radioelectronics and Information Technology (USBEREIT) | 979-8-3503-3605-4/23/$31.00 ©2023 IEEE | DOI: 10.1109/USBEREIT58508.2023.10158871

Selection of Criteria for the Problem of Optimizing Resource Allocation when Implementing an Information Leakage Prevention System at an Enterprise

Sinadskaia Olga
U*ral Federal University*
Yekaterinburg, Russia
o.iu.sinadskaia@urfu.ru

Sinadskiy Mikhail
U*ral Federal University*
Yekaterinburg, Russia
mishasinad@yandex.ru

***Abstract*—The article considers the problem of choosing criteria for the task of optimizing resource allocation when implementing an information leakage prevention system in an enterprise. An information leakage prevention system is a software and hardware system designed to detect unauthorized transmission of information. The choice and implementation of an information leakage prevention system in an organization is a time-consuming task that requires an integrated approach and optimal allocation of resources. To obtain the best option for implementing an information leakage prevention system in a particular organization, it is necessary to solve the problem of optimizing the distribution of resources of this organization. The article considers the characteristics of the information leakage prevention system that affect its effectiveness. The boundaries of the optimization problem are determined, the restrictions on the controlled variables are described. As controlled variables for optimization, an economic indicator, human resource, implementation time, structure and technical equipment of the organization were chosen.**

Keywords—information leakage prevention system, DLP system, resource optimization problem, optimization problem criteria, choice of optimization criteria

I. INTRODUCTION

At the present stage of development of information technologies, their extremely high integration into many areas of activity is noted. Information flows act as a link between the object and the subject of management. Even for the simplest systems, the essential components are the connections between the elements of the system. With the complication of the system, with an increase in the level of its hierarchical organization, the connecting information flows are growing rapidly, which makes it difficult to control and protect the information circulating in them.

Nowadays, accidental or intentional data leakage is the most common problem faced by organizations. If earlier the emphasis was shifted to protection from an external intruder, then recently, as a priority direction for the development of information security, enterprises choose protection against internal threats and information leaks, especially information of limited distribution, by implementing information leak prevention systems [1].

A Data Leak Prevention or DLP system is a software and hardware system designed, as the name suggests, to detect unauthorized transmission of information. DLP systems can control both all information crossing the perimeter of an informatization object and circulating inside the object. DLP systems consist of three main components: an information interceptor, an analyzer that determines the legitimacy or illegitimacy of information transfer, and a response tool. Depending on the settings, DLP systems can operate either in the mode of registering events that lead to information leakage, or in the mode of blocking information transfer.

The implementation of a DLP system in an enterprise is a time-consuming task that requires an integrated approach based on optimizing the distribution of resources [2]. To find the best option, it is necessary to determine the criteria by which a decision will be made on the implementation of a DLP system in a particular enterprise.

An analysis of the scientific literature has shown that optimization problems are widely used in economics, engineering, computer science, but the scientific problem of optimizing the distribution of resources for the implementation of a DLP system has not yet been solved. Therefore, it can be assumed that the results of this work will be in demand by managers and information security specialists of organizations of various sizes and forms of ownership when implementing DLP systems.

II. GENERAL INFORMATION ABOUT DLP SYSTEMS

The emergence of information leakage prevention systems or DLP systems in the early 2000s is associated with the awareness of internal threats to the information security of objects. According to the report of the InfoWatch analytical center on a practical study of the level of protection of corporate information, 77% of managers and 85% of IT and information security employees believe that the danger to their employers' business is not associated with external, but with internal threats [3]. The focus of attention has shifted to the illegal actions of persons who have access to the controlled area to standard computer equipment. The infrastructure of the employer, personal means of communication of employees can become a weapon of crime. It should be noted that information security incidents do not always have a criminal connotation, which can include theft of information or material assets of an organization, sabotage, collision with competitors, etc., often an accidental unintentional leak can cause irreparable harm.

The general principle of operation of a DLP system is to analyze information flows moving both inside and through the protected perimeter. Not only information flows within the network infrastructure of an object are analyzed, but also the transfer of documents to printers, mobile media, etc., which determines the presence of components in DLP systems both

at the network level and at the workstation level. Network components are typically installed on servers to control traffic that crosses information system boundaries. To control the transmission of information via local communication channels, components of the node level are installed on personal computers.

Information categorization technologies form the core of DLP systems. The first DLP systems that appeared used a content-context mechanism for filtering traffic for the presence of confidential information: regular expression search, digital fingerprints, partial comparison of documents, linguistic analysis. In improved systems, in addition to filtering by content, file metadata began to be used, machine learning and artificial intelligence technologies were used. The next generation of DLP systems will probably move from registering incidents to assessing risks in relation to information resources, channels, employees and other entities [4]. Analysis of information flows and applied analysis of the behavior of people who have access to the information assets of an enterprise or organization can predict the probability of risks and find ways to improve the efficiency of information security systems.

Depending on the settings, DLP systems can operate either in the mode of registering events that lead to information leakage, or in the mode of blocking information transfer. The so-called DLP systems with active control of user actions are considered primary. These systems block the channel of information leakage in accordance with the specified security rules, but streaming blocking is justified to prevent unintentional leaks, in the case of an attacker, blocking will signal to the intruder that this channel is being controlled, that is, the system itself teaches the intruder how to bypass it. The vast majority of DLP systems used are passive in nature, designed to register and notify information security officers about incidents or suspicious events, which allows you to track user behavior, expose planned criminal events, and see insider loopholes.

III. The Problem of Optimizing the Distribution of Resources for the Introduction of the Information Leakage Prevention System

The implementation of a DLP system in an enterprise is a rather complex technical and organizational task. First, it is necessary to resolve the issue of the functional content of the system: what the system will control, at what level monitoring is planned, what should be the analytical capabilities of the system, whether the DLP system will need certificates. At the preparatory stage, it is required to compile a list of the organization's confidential data, a list of technical devices and communication networks in which confidential information circulates, lists of users with established access rights to information, lists of employees who will be informed or investigate incidents. Then it is necessary to draw up a work plan for deploying the test part of the system, deploying the DLP system in full and configuring its components, conducting trial operation and acceptance tests. After launching into commercial operation, you should regularly review and update the security policies in the settings of the DLP system. Solving the problem of optimizing the distribution of resources of an organization implementing a DLP system will help you choose the best option among other rational options under given conditions.

In general, mathematical optimization problems are described by the following formula:

$$f(x) \rightarrow \min (\max), x \in U, \qquad (1)$$

where $f(x)$ is the objective function, x are the controlled variables, U is an admissible set specified by constraints on the controlled variables

Determining the values of intrasystem variables that correspond to the best situation is an optimization problem. To solve it, it is necessary to establish the boundaries of the system to be optimized, select a characteristic criterion, determine the intrasystem variables that most affect the characteristic criterion, and build a model.

IV. Borders of the Optimization Problem

In order to use mathematical methods in practice, it is necessary to formulate the problem to be solved in mathematical language or build a mathematical model. In most real situations, it is impossible to take into account all the interconnections of the internal parts of the system and the connection with the outside world, since the model is an object that replaces the original, retaining the most important characteristics for solving the problem, no model can describe the process under study completely and comprehensively,

Consider the assumptions that are assumed to determine the boundary of the optimization problem. We assume that an organization planning to install a DLP system:

- this is an isolated system, that is, we neglect the influence of other organizations;
- this is an organization, the individual components of which work in close relationship with each other, there are no divisions that can work separately;
- at the stage of implementation of the DLP system, the structure of the organization and its technical devices and communication channels will not change;
- at the stage of implementation of the DLP system, the list of protected information in the organization is defined and will not change.

V. Criteria for the Optimization Problem

The choice and implementation of a DLP system in an enterprise is a decision that has a serious long-term impact that requires careful analysis, including mathematical modeling and the development of a decision support system. As a rule, such decisions are made by the head of the organization alone or by a collegial governing body, that is, an essential element is the presence of a person in the decision-making process. Thus, when setting the task of optimizing the distribution of resources for the implementation of a DLP system, it is necessary to consider both the time requirements and the economic component, as well as the features of human decision making.

When implementing DLP systems, as a rule, the main goal is to minimize the likelihood of information security threats. Although there may be additional goals, for example, suppression of the use of company resources for personal purposes, analysis of the effectiveness of the use of working time by employees, automation of the document flow in the investigation of incidents, and others. After the goal of introducing DLP systems is determined, you can proceed to the description of the optimization criterion or the objective function. This may be an economic criterion, for example, loss

of profit due to the theft of the company's information assets, the cost of implementing DLP systems, an increase in profits due to more rational use of working time by employees, etc. These may be technological criteria, for example, an increase in productivity due to a decrease in the time of inefficient use of computer technology. Often the choice of an optimization criterion (characteristic criterion) is not obvious and unambiguous, the reason for this may be the complexity of the objective function that describes a large set of heterogeneous goals, the uncertainty in the formulation of some goals, the impossibility of describing some parameters by quantitative characteristics, the dependence of goals and their importance on the point of view of the researcher and etc.

The totality of all restrictions on the controlled variables determines the so-called admissible set of the optimization problem. In real conditions, the choice of values of controlled variables and their number, as a rule, are subject to restrictions associated with the limited availability of resources, capacities, and other capabilities.

As a rule, when describing controlled variables, first, they consider an economic indicator - the cost of implementing DLP systems. This indicator is the sum of the costs of acquiring DLP systems, the salaries of employees who install this system, the costs of staff training, and the costs of other stages of the life cycle of DLP systems. In general, the costs of implementing a DLP system should not exceed the potential profit from its operation. When choosing DLP systems, the following parameters are considered:

– target tasks (identifying and blocking illegitimate transmission of information outside the controlled perimeter, preventing information leakage based on the analysis of information flows and behavioral analytics, predicting the likelihood of risks and finding effective means of ensuring information security);
– mode of operation (monitoring, events leading to information leakage are registered, blocking dangerous actions in accordance with predetermined instructions);
– monitoring level (at the workstation (client) level, at the gateway (network) level);
– information transmission channels (wire and wireless networks);
– analyzed data formats and types of analyzed file content (text, graphic information, sound and video recording);
– control regime (solid or selective control);
– volume and methods of data collection for incident investigation (complete data collection for a predetermined period or selective data collection according to predetermined rules);
– the mode of storage of accumulated information (within the organization or on media controlled by the organization or outside the controlled area of the organization; a single or distributed archive of accumulated data for investigating information security incidents);
– possibility of analytical processing of accumulated information;
– possibility of integration with information systems existing in the organization;
– possibility of customization.

Since DLP systems are human-dependent systems that are configured by people and control the actions of people, it is necessary to consider the most significant indicator - the human resource involved in setting up and operating the system. The most vulnerable link in the enterprise security system is uninformed or poorly trained employees, both users and administrators. The data of an analytical study [3] indicate that almost half of the leaks are accidental, occurring precisely because of the negligence or incompetence of employees. Therefore, the introduction of a DLP system cannot replace personnel training organized at a permanent and systemic level. The second half of the leaks are related to the actions of attackers who deliberately use their knowledge to harm the organization. DLP systems cannot prevent all information leaks, so the choice of a protection strategy should be based on an analysis of the factors that influence the formation of risks.

Installing a DLP system is undoubtedly a complex and time-consuming task, but much more important and resource-intensive work is carried out during the implementation process - determining the information that needs to be protected, creating rules, procedures, policies, setting up the implemented system for the tasks of a particular enterprise, taking into account its organizational structure and geographical location, all this requires broad competencies in a variety of information security issues. The development of documentation support for the implementation of a DLP system in an organization begins at the stage of pre-project survey. The presence of documents fixing the ranking of information by various categories, rules and procedures for the movement of information inside and outside the organization, regulations on the procedure and conditions for access of subjects to information system objects, descriptions of business processes will significantly reduce the time to install a DLP system. In addition, human and time resources will be required to document the planned work on the deployment of the DLP system, its trial operation and acceptance tests. But even after the introduction of a DLP system, it is necessary to regularly analyze information security incidents and improve the system for preventing information leaks.

The next value, the value of which can be changed to achieve the best result, is the time required to implement a DLP system. The minimum period declared by the manufacturers is two days - but this is only the time that will be spent on the direct installation of the software product. At least another week will be required to configure information security policies and debug the solution. The implementation period of a DLP system depends on the scale of the organization, the complexity of its structure, the number of employees, the types and number of information transmission channels. The time for setting up a DLP system is significantly reduced if the customer has a pre-prepared package of documents describing business processes and working with information. It is important to consider that the more time it takes to implement a DLP system, the higher the economic costs.

The main parameters of the architecture of technical channels and information processes can be either controlled variables or not. If the management of the organization is not ready to change the structure of the organization and modernize the technical means, then this parameter will be considered fixed, otherwise it is adjustable, that is, a controlled variable. In some cases, the analysis of the accumulated data on information flows allows you to optimize business processes, restructure the organization or change the functional responsibilities of employees.

So, the economic indicator, human resource, implementation time, structure and technical equipment of the organization are selected as controlled variables for optimization. There is no simple relationship between the four variables considered. It is impossible to reduce the time of implementing a DLP system in an organization by simply increasing the number of employees involved in setting up the system, on the other hand, it is possible to complete the implementation of the system faster by easing quality-related restrictions. If top management deliberately sacrifices quality, then the human factor may come into play, for example, employees will have a feeling that they are using a defective product. An increase in monetary costs will not entail a proportional increase in the speed of implementation of the DLP system in the organization, on the other hand, by increasing the amount of investment, you can expand the functionality of DLP systems. In turn, the implementation of additional protection measures complicates communication and leads to additional costs.

As a rule, it is impossible to find a solution for which the best values are achieved by several criteria at once. Therefore, in the practical sphere, two options are possible. First, choose one main criterion, and consider the remaining criteria as secondary, they can be considered with the help of additional restrictions on controlled variables or not considered when solving the problem. Second, adding weight coefficients to various objective functions and combining them into a complex criterion.

VI. Conclusion

The task of effective implementation of DLP-systems in a particular organization requires an integrated approach and optimal allocation of resources, its solution is possible using popular optimization procedures. In practice, it is difficult to single out a single optimization criterion, so two options are possible. First, choose one criterion and consider it the main one, and the remaining criteria - secondary, which may not be considered when solving the problem, or secondary criteria are considered with the help of additional restrictions on the controlled variables. Second, adding weights to various objective functions and combining them into a complex criterion.

In the considered problem of optimizing the distribution of resources for the implementation of an information leakage prevention system, it is assumed that the controlled variables can change on a certain set. The economic indicator, human resource, implementation time, structure and technical equipment of the organization were chosen as controlled variables.

References

[1] I.O. Shabanov. “Analysis of the information security market in Russia. Part 1.”, Anti-Malware.ru. Available at: https://www.anti-malware.ru/analytics/Market_Analysis/ analysis-information-security-market-russia-part-1 (Accessed: January 24, 2023) (in Russ.).

[2] O.L. Tsvetkova and A.R. Aydinyan, “Intellectual system for assessing the security of enterprises from an external threat,” in *Bulletin of computer and information technologies*, vol. 8 no. 122, pp. 48–53, 2014 (in Russ.).

[3] InfoWatch.ru. “Information security in corporate information systems. Internal threats.”, Available at: https://www.infowatch.ru/sites/default/files/report/analytics/russ/InfoWatch_Report_2013_ugroz.pdf (Accessed: January 24, 2023) (in Russ.).

[4] M.V. Razumovskaya, “DLP next generation for protection against internal threats,” in *Data protection. Inside*, vol. 5 no. 101, pp. 26–29, 2021 (in Russ.).