Choosing technical components of the physical protection system of objects

S Yu Fedorov, V N Khalizev and E S Tarasov
Institute of Computer Systems and Information Security, Kuban State Technological University, Krasnodar, Russia
E-mail: fsu_50@mail.ru, ha53@mail.ru, helisar@mail.ru

Abstract. This article presents a method for solving the urgent problem of choosing a combination of technical systems of physical protection of objects of informatization of an organization, on the example of an integrated security system using methods of system analysis. The article proposes a new approach that combines the methods of the theory of antagonistic games and methods of fuzzy logic. On the basis of this mathematical model, a program and a database have been developed, including interconnected tables of physical protection systems, capabilities of protection systems, tables of threats and ways of implementing threats. As a result of the application of this method, with the help of the program, a specialist can quickly solve the complex problem of choosing the optimal combination of physical protection systems to counter probable threats for a specific object of the organization's informatization. Based on the results of the program's work, the developer receives a report with recommendations.

1. Introduction
The wide spread introduction of information systems and technologies provides new opportunities for solving social problems and opens up broad prospects for the development of the individual and society, but also aggravates old ones or generates new, previously unknown problems, becomes a source of new potential threats. At the moment, the acuteness of the problem of ensuring the information security of objects and protecting the information stored and processed in them from various threats is increasing. Without due attention to information security issues, the consequences of society's transition to new information technologies can be catastrophic. One of these problems is the provision of physical protection of information technologies and systems at the objects of informatization. Based on the analysis of international standards [1-4], it can be concluded that as one of the means of preventing information security incidents, it is necessary to use systems of physical protection of objects. Currently, there are a large number of such systems on the market, and the project developer has to make a personal decision to choose protection systems. The composition of physical protection systems can be varied depending on the threats, the purpose of the object, its significance and specific conditions. The problem is the lack of a unified regulatory framework and methods for choosing a means of physical protection of objects of the organization's informatization. The solution to this problem is a complex and urgent task due to the wide variety of such systems, the variety of protected objects, conditions and, accordingly, threats to them. The methodology proposed in this article allows to formally describing the process of choosing the means of physical protection systems for objects of informatization of an organization.
2. Materials and methods

Now almost every manufacturing enterprise, trade facility, government agency or office uses information technology and physical protection systems to ensure their safety. Traditionally, the set of physical protection systems included scattered components - video surveillance systems, security and fire alarms, and access control systems. Since about the mid-90s, consumer demands have become broader, and simple systems have ceased to solve more complex problems. Currently, in the Russian Federation, informatization objects are equipped with integrated security systems (ISS - hereinafter).

An integrated security system is a developed specialized complex technical system that combines, on the basis of a single software and hardware complex with a common information environment and a single database, target functional technical subsystems and technical means designed for comprehensive protection of an object from standardized threats of various origins and manifestations, according to GOST R 53704-2009 [5] contains a list of 17 technical subsystems that should be included in the ISS:

1. duty dispatching office; 2. production and technological control; 3. security and alarm systems; 4. fire alarm; 5. control and management of access; 6. CCTV / video surveillance and control; 7. search subsystems; 8. fire automatics (fire extinguishing, smoke protection), 9. warning, evacuation); 10. connection with the object; 11. information protection; 12. physical barriers; 13. engineering support of the facility: electric lighting and power supply; 14. gas supply; 15. water supply; 16. sewerage; 17. maintaining the microclimate (heat supply, ventilation, air conditioning).

The composition and number of these subsystems can vary. It depends on the purpose and importance of the protected object and the specific security conditions. The composition may include products from different manufacturers from different countries. One of the subsystems that can be included is the information security system. All system requirements must be taken into account by the developers when designing an integrated security system. The paper proposes to increase the selection accuracy to increase this number of subsystems to 22, by adding means to ensure the anti-terrorist security of an object, a mobile positioning subsystem (for mobile objects) and dividing the security alarm subsystem into a perimeter subsystem and a subsystem of object security equipment, as well as adding to the subsystems engineering support of the facility of backup power supply devices. Each subsystem has been assigned its own identifiers in the database table (figure 1). To solve the problem of choosing a set of subsystems, the ISS classification helps to a certain extent. ISS are subdivided depending on the...
required degree of automation of the facility and based on economic considerations. The first classification criterion is “the number of implemented basic protection functions. These ISS functions are exposed through its subsystems. So it can be: security alarm systems, fire alarm systems, alarm systems, fire extinguishing systems, access control and management, CCTV, etc. ISS must include at least two of the listed subsystems. The next criterion, the ISS classifications, are the principles of integration. The following types of subsystem integration are distinguished here: hardware, software and integration at the hardware-software level.

There is a huge variety of means of protecting computer information on the market, however, with an increase in the level of security of the system, certain inconveniences in its use, limitations and difficulties for users arise. Therefore, it is often necessary to choose the optimal protection option, which would not create great difficulties in using the computer. Based on the analysis of documents, it can be concluded that the process of analysis and synthesis of integrated security systems, the choice of their subsystems is rather complicated and time-consuming, depending on a considerable number of various factors, the amount of knowledge and experience of designers. Therefore, errors may appear due to various reasons, which can lead to the choice of a deliberately expensive or not the best option, which can then affect the budget and safety of the entire facility. Therefore, the task of this formalized choice of the optimal composition of the set of integrated security systems (ISS) is relevant at this stage.

In this method, at the first stage, it is proposed to use the mathematical apparatus of the theory of matrix antagonistic games, which makes it possible to optimize the choice of means of physical protection of objects of informatization of an organization. System selection methods are divided into universal and special. As a rule, universal ones are less accurate, they do not reflect the specific features of the subject area, etc., therefore it is better to use special ones. It is proposed to use the methods of game theory, because in reality and in life there are two opposing sides - an attacker from whom threats emanate and an information security specialist who uses various means of protection to counter threats, an intruder. We used the example program described in the article [6]. The goal of the offender is to inflict maximum damage on the attacked computer system, and the goal of the information security specialist is to select a protection strategy in which the probable losses from information security incidents will be minimal. That is, the physical protection system must be ready to neutralize information security incidents that cause maximum damage on the part of the intruder. As a payment matrix, a game table was disassembled, in which the columns are the strategies of the information security specialist and are filled with the used physical protection means \( y_j \) (where \( j = 1, m \)), and the rows represent the strategies of the violator and the threats \( x_i \) are filled (where \( i = 1, n \)) of some matrix. As a strategy of the violator, various threats to physical protection objects presented in [5] were taken as a basis. The result of the game \( a_{ij} \) is the total damage that can be caused to the computer system when the violator implements his i-th strategy, as well as the damage inflicted to the IS specialist from the cost of the total cost of protective equipment from the j-th strategy. The desired value is the sum of the possible damage from the remaining attacks from the attacker's strategy and the cost of physical protection equipment. Given the available information on information security incidents, the result will be a strategy for physical protection systems that minimizes average losses, i.e. the minimum amount will be:

\[
a_{opt} = \min_{i} \max_{j} a_{ij}
\]  

All possible combinations of the following 21 threats were selected as possible strategies of the violator in this work. It was possible to obtain various strategies of the players by a simple enumeration of all possible information security incidents for an intruder and a similar enumeration of all physical protection software tools participating in the game for an information security specialist. To reduce the number of players' strategies, threats and physical protection were divided into groups. In this case, from each group of threats, one with the maximum damage is selected, and from each group of protection tools, one with the minimum cost is selected. From the resulting lists of incidents of information security and protection means, the strategies of the players are drawn up by enumerating all possible combinations. The total costs are obtained by summing the amount of damage that can be caused when
implementing the current strategy of the attacker, if the system was not protected from it by means of protection from the current strategy of the information security specialist, and the total cost of all means of protection from the current strategy of the security specialist. The calculation of damage from the implementation of threats is calculated in two stages. First, the attacker’s current strategy is matched against each of the physical defenses from the security specialist’s current strategy, and if the agent protects against any threats from the current set, then these threats are removed from the set. By comparing the current set of threats with all the means from the current strategy of the information security specialist, a certain number of threats are obtained, from which the system is not protected in this case. The received threats must be compared with all the existing threats and the damage values of those threats that are present in the received set must be summed up. Further, these two sums are added, and damage is obtained when the current pair of strategies of the violator and the information security specialist is applied [6]. The algorithm presented in [6] was refined using fuzzy logic and allows you to find the most dangerous ways to implement threats and select physical protection systems (PPS) based on a given list of intruder threats for a specific object and a specific situation. Rows have been added to the threat table in the database, containing the paths of the threat implementation. For example, an incident such as theft can be implemented in 2 ways:

Option 1 - by hacking (using special tools):
- through the balcony (id 10);
- through the basement (id 11);
- through the window (id 12);
- through the roof (id 13);
- through the door (id 14).

Option 2 - no hacking:
- through an unlocked front door (id 15);
- through an unlocked window id (16).

At the first stage, the maximum is determined. For each threat in the PPS combination, the value of non-avoidable damage is determined, which is initially assumed to be equal to the maximum possible damage caused without the use of PPS and decreases in the process of considering the capabilities of the PPS in combination to counteract their threats. To do this, first, the value of \( d \) is found - the unavoidable maximum damage caused by a specific way of implementing the threat according to the formula (2):

\[
d = U * k,
\]

where \( d \) is the unavoidable maximum damage caused by a specific way of implementing the threat;

\( U \) is the maximum damage to the threat realization; \( k \) is the coefficient of effectiveness of the implementation of this threat along the given path (where \( k = 0 \ldots 1 \)).

For each PPS in a possible combination

\[
NU = d - (d * kp),
\]

where \( NU \) is the non-preventable damage for this threat.

\( kp \) - coefficient of PPS counteraction to the given method of realization of the given threat.
Figure 2. Algorithm for finding the optimal combination of physical protection to counter possible threats.

Non-preventable damage for a given threat is determined by formula (3), as the difference between the maximum damage that cannot be prevented by a specific way of implementing the threat and the prevented damage, which is calculated as the product: \((d \times kp)\). For each threat, by comparing all values, the greatest value is found, this will be the most dangerous way of implementing the threat, that is, the way through which the greatest damage is possible. At the next stage, the minimum is found. By
enumerating and comparing all PPS values, we find the best PPS combination that provides the best security for a given threat in the current combination. Among all physical protection systems, there is the PPS that has the lowest value of the combination of non-avoidable damage covered by the implementation of a given threat and the maximum damage that can be caused by a threat to a given physical protection. Next, the sum of the minimum non-preventable damages for all threats is calculated. Then the total damage for the PPS combination is determined by summing up the non-preventable damage for all threats and the cost of all PPS included in this combination. To obtain the best combination of PPS, which ensures the greatest security of the informatization object, the combination with the lowest value of the total damage is selected by enumerating and comparing the current obtained combination of PPS with the total damage of the already existing best combination of PPS.

At the last step, the choice of physical protection subsystems to counter possible threats is carried out based on the application of the concept of building a protection system in the form of covering a set of functional requirements and developing a complex preference indicator according to a modified target method.

Table 1. Sample report. The optimal list of protection tools to prevent existing threats Results and discussion

| Means of protection | Tele / video surveillance and video monitoring subsystem | Alarm subsystem |
|---------------------|--------------------------------------------------------|-----------------|
| Cost                | 40 000.00                                              | 205 943.00      |
| Threat 1            |                                                        |                 |
| Path of threat realization | Through the roof                               | Theft           |
| Unavoidable damage  | 60 000.00                                              | Through an open window |
| Path of threat realization | Without violence against the person                  | Robbery         |
| Unavoidable damage  | 400 000.00                                              | With violence against the person, not dangerous to life and health |
| Threat 3            |                                                        | Sabotage        |
| Path of threat realization | economic                                               |                 |
| Unavoidable damage  | 270 000.00                                              | cyber diversion |
| Threat 4            |                                                        | Terrorism       |
| Path of threat realization | Organized, collective                          |                 |
| Unavoidable damage  | 1 350 000.00                                            | Organized, collective |

The total cost of protective equipment: 245 943.00. Total uncovered damage from threats: 780,000.00. The maximum costs will be no more than: 1,025,943.00.

A sample report is presented in table 1, which shows the optimal combination of physical protection means to counter potential threats for a specific object of the organization's informatization and the total costs of the selected systems. In addition, the report calculates the maximum costs for a complete set of all protection measures, which significantly exceed the costs of the combination selected by the program. The program also provides information on the most dangerous ways of implementing threats.

3. Results
Based on the described approach using the mathematical apparatus of antagonistic game theory and fuzzy logic, the following results were obtained:
1. An algorithm (figure 2), a database, a software application in the C++ programming language have been developed using a cross-platform integrated development environment IDE Qt Creator version 5.12.0.
2. Compiled a list of 17 threats and 21 physical protection subsystems.
3. The correctness of the developed mathematical model was checked.
4. The choice of the optimal combination of physical protection systems was made to ensure the security of a specific object of the organization's informatization and to counter potential threats in the event of information security incidents.
5. The most dangerous ways of implementing threats have been determined, based on the analysis of a potential list of threats for a given object.
6. Determined the maximum costs for a full set of physical protection of objects of informatization of the organization and the cost of an optimal set of physical protection. At the same time, significantly reducing the total costs.

4. Conclusions
Thus, the developed mathematical model and the program written on its basis allow solving the urgent problem of choosing the optimal set of physical protection means based on the analysis of a large amount of information (17 threats and 21 physical protection subsystems) to counter potential threats for a specific object of the organization's informatization.

References
[1] ISO / IEC TR 18044: 2004 Information technology - Security techniques - Information security incident management”.
[2] ISO / IEC 27035-1: 2016 - Information technology - Security techniques - Information security incident management - Part 1: Principles of incident management.
[3] ISO / IEC 27035-2: 2016 - Information technology - Security techniques - Information security incident management - Part 2: Guidelines to plan and prepare for incident response.
[4] ISO / IEC 27035-3: 2020 Information technology - Information security incident management – Part 3: Guidelines for ICT incident response operations.
[5] GOST R 53704-2009: Complex and integrated security systems. General technical requirements.
[6] Vakhniy T V and Guts A K, Novikov N Yu. 2016. Matrix-game program with the choice of criterion for determining the optimal set of security tools for a computer system. Omsk State University. Dostoevsky. Mathematical structures and modeling. 2 (38). 103-15
[7] Garcia M 2002. Design and assessment of physical protection systems. (M.: Mir: LLC "AST Publishing House").