Ivan TYSHYK[1], Antonina HOMONIUK[2], Natalia MAZUR[3]

Opiekun naukowy: Ivan TYSHYK[1]

EVALUATION OF THE EFFECTIVENESS OF THE PERIMETER PHYSICAL PROTECTION SYSTEM

Abstract. In the article the evaluation of the efficiency of the physical protection system of the perimeter for the given object of protection was conducted. One of the possible ways to improve the early detection of the fact of penetration of the object of protection and early warning of the security service is submitted for the adoption of adequate or preventive measures. The concept of timely detection of the offender in the controlled area of the space is formulated.

Keywords – object of the evaluation, systems of physical protection, critical point of detection, detection means, technical means of protection.

OCENA WYDAJNOŚCI SYSTEMU OCHRONY OBIEKTU

Streszczenie. W artykule przeprowadzono ocenę skuteczności (fizycznego) systemu ochrony obrzeża obszaru dla danego obiektu będącego pod ochroną. Jednym z możliwych sposobów poprawy wczesnego wykrywania faktu przeniknięcia intruza oraz wczesnego ostrzegania służb bezpieczeństwa - jest wprowadzenie odpowiednich środków zapobiegawczych. Opracowano koncepcję wykrywania sprawcy w kontrolowanym obszarze przestrzeni.

Słowa kluczowe: przedmiot oceny, systemy fizycznej ochrony, krytyczny punkt detekcji, środki wykrywania, techniczne środki ochrony.

1. Introduction

Today, the problem of information security for many businesses is more than ever relevant. The managers of the enterprises begin to take seriously the difficult task of choosing a security system in accordance with the specifics of its business. As a rule, at the initial stage before them there is a problem of the right choice of the perimeter security system (PSS), which would correspond to the optimal price / quality ratio present.

[1] PhD, Lviv Polytechnic National University, Associated Professor of Department of Information Security, ivan_tysh@i.ua
[2] Lviv Polytechnic National University, Department of Information Security, speciality: Cyber security, antonina.homoniuk@gmail.com
[3] PhD, Borys Grinchenko Kyiv University, Associated Professor of Department of Information and cyber security, v.buriachok@kubg.edu.ua

The main purpose of the perimeter security system is the early detection of the fact of penetration of the object of protection and early warning of the security service to take adequate or preventive measures. At the previous stage of choosing a security system for an object of a given type, it is necessary to analyze the possible variants of threats, to minimize the degree of damage from their implementation, to form a model of the offender. For a full and adequate assessment of threats, improvement of approaches to the use of existing methods is necessary, based on the experience of their implementation and traditional technologies for constructing private models of threats to information security. Usually, the imagination of the nature of the impact of the threat to security on information resources includes a certain list of constituents of the components, necessary and sufficient to create an adequate model [1, 2].

Taking into account the specifics of the objects of protection, it is quite obvious that there is no perfect perimeter security system; therefore, it is necessary to have a qualified approach as to the choice of the perimeter security system, and in its design. The issues of physical security of information objects are considered in particular by ISO / IEC 27002 "Information Technologies - Security Technologies - Practical Rules for Information Security Management". The standard describes the recommendations for comprehensive information security and provides best practices for information security management for those responsible for the creation, implementation and / or maintenance of information security management systems [3, 4].

The objects of influence in order to violate the confidentiality, integrity or availability of information may be not only elements of the information system, but also supporting infrastructure, which includes networks of engineering communications (systems of electricity, heat supply, air conditioning, etc.). In addition, attention should be paid to the territorial location of technical equipment that is to be protected. Wireless equipment is recommended to be installed so that the area of the wireless network does not go beyond the control zone.

In many information security standards, physical protection is considered in the context of the multi-level protection model as its foundation. From the point of information security, the multilevel security model defines a set of levels of information system security. The model is often used, in particular by Microsoft in its safety instructions. Correct organization of protection at each of the allocated levels, allows protecting the information security system from the implementation of threats [5, 6].

The list of selected levels is somewhat different in varied documents. A variant is presented in Fig. 1 [7].

Information security policy should describe all aspects of the system in terms of providing information security. Therefore, the level of security policy can be considered as a basic one. This level also implies the availability of documented organizational security measures (procedures) and event notification, user education in the field of information security and other similar measures as recommended by ISO / IEC 27002.

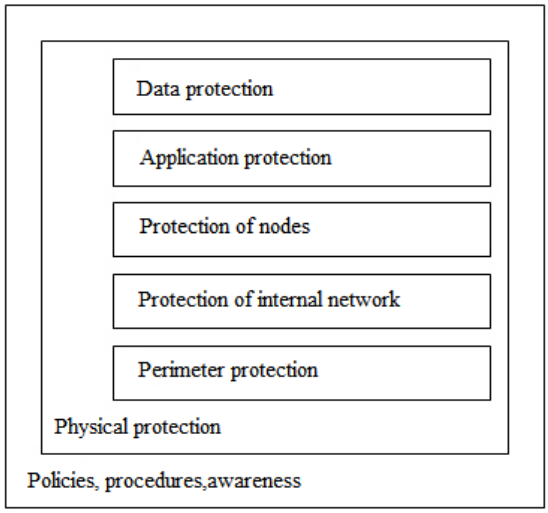

Figure 1. Multi-level protection model

The level of physical protection includes measures to restrict physical access to system resources - security of premises, access control, video surveillance, etc. Hither the means of protecting mobile devices used by employees for official purposes are included.

Level of perimeter protection IS defines security measures at "entry points" in a network that is protected from external, potentially dangerous networks. A classic IS firewall is a firewall that, based on the rules, determines whether arrived network packet can be skipped into a secure network. Other examples of perimeter protection means of information system include intrusion detection systems, antivirus protection for security locks, and so on.

The internal network security level is "responsible" for ensuring the security of traffic that is transmitted internally and in network infrastructure. Examples of means and mechanisms of protection at this level are the creation of virtual local area networks with the help of managed switches, protection of transmitted data using the protocol IPSec, etc. Often, within the network, too, are means that are specific to perimeter protection, such as firewalls, including personal (installed on a computer that is protected). This is due to the fact that the use of wireless network technologies and virtual private networks results in "blurring" of the perimeter of the network. For example, if an attacker was able to connect to a wireless access point inside a secure network, then its actions would no longer be controlled by the firewall set at the "border" of the network, although formally the attack would be carried out from the outside with respect to the computer network. Therefore, sometimes during the analysis considers "network security" level, which includes both perimeter protection and internal network protection.

The next is the level of nodes protection. Here are considered attacks on a separate node of the network and, corresponding, protection measures against them. The functionality of the node can be appreciated, and the protection of servers and workstations is considered separately. First of all, need to pay attention to security at the operating system level - settings that enhance the security of the configuration

(including the disconnection of services that are not used or potentially dangerous services), the organization of fixes and updates, reliable authentication of users. Antivirus protection plays an extremely important role.

The level of application protection (application software) is responsible for protecting against attacks directed at specific applications - mail servers, web servers, database servers. As an example, SQL injection can be considered as attacks on the database server, which consists in the fact that the input text string contains SQL statements that can break the logic of data processing and lead to receiving confidential information offender. This also includes the modification of applications by computer viruses. To protect against such attacks, the security settings of the applications themselves, installation of updates, antivirus protection means are used.

The level of data protection determines the order of protection of processed and stored data in the system from unauthorized access and other threats. Examples of countermeasures include the delineation of access to data by means of the operating system, the encryption of data in storage and transmission.

In the process of identifying risks, the purpose of the offender is determined, and at what level or levels of protection it can be resisted. Accordingly, countermeasures are also selected. Protection from threats at several levels reduces the likelihood of its implementation, and hence the level of risk.

The international standard ISO 15408 has been developed on the basis of the "General criteria of safety of information technologies"."General criteria" presuppose the existence of two types of security requirements - functional and trust. Functional requirements relate to security services, such as identification, authentication, access control, audit, etc. The requirements of security confidence relate to the technology of development, testing, analysis of vulnerabilities, supply, maintenance, maintenance documentation, etc.

The main structures of the "General Criteria" are the profile of protection and security tasks. A security profile is defined as "independent of the implementation of a set of security requirements for a certain category of an object of evaluation (OE) that meets the specific requirements of the consumer. Under the object of evaluation (OE) is understood as "the product of information technology (IT)". These objects include, for example, operating systems, applications, IS, etc.

The security profile defines the "model" of the security system or its individual module. The number of profiles is potentially unlimited; they are designed for different applications (for example, the profile "Specialized Protection against Unauthorized Access to Confidential Information" profile).

A security profile serves as the basis for creating a security task that can be considered as a technical project for the development of OE. Security tasks may include requirements for one or more security profiles. It also describes the level of functional capabilities of the means and mechanisms of protection implemented in the OE, and justify the degree of their adequacy. According to the results of the evaluations, catalogs of certified security profiles and products (operating systems, information security devices, etc.) are created.

From the study of information security standards, it is clear that the physical security of any enterprise includes a set of engineering and technical measures that can effectively protect the business from possible attacks from competing organizations, insider attacks, and possible natural disasters.

In order to increase the effectiveness of the physical protection of the perimeter of the given object, the task is analyzing the typical time characteristics of the physical protection system, which in their aggregate must guarantee the achievement of the forces responding the given area and occupying their position after receiving an alarm for a specified time period, seeking ways to improve early detection the fact of penetration into the object of protection and early warning of the security service to take adequate or preventive measures. The proposed concept of timely detection will provide an impetus for the development of further methods for evaluating the functional efficiency of the perimeter security alarm system.

2. Evaluation of the efficiency of the physical protection system

An important characteristic of the physical protection system (PPS) of an object is the time period that is required by the response forces to reach a designated site and occupy a position after receiving an alarm signal.

The response time includes the sum of all the average time periods required to implement the following actions [8]:

1. Transmission of an alarm signal caused by detecting the offender in a given area of the space, on the guard post. 2. Evaluation of the alarm signal (reliable / false). 3. Challenge of the response forces (guards, Special Forces, police, etc.). 4. Preparation of response forces for action. 5. Arrival of the response force to the moment of action. 6. Occupation of positions necessary for successful detention / prevention of offender actions.

The listed detection points must be identified along the trajectory of violator, where the sum of the next time delays (T) must exceed the response time of the response forces (T_{CP}). The detection point associated with the smallest total delay time (T_{min}) will be a critical detection point *(CDP)*; it means the system must identify the offender even before it reaches this point so that it can successfully prevent its further actions. Thus, the perimeter physical protection system will be effective in fulfilling the key condition $T_{min} > T_{CP}$.

Each of the time delays, which characterize the stages passed by the offender on the path, cannot be reliably determined. Accordingly, the aforementioned comparison is estimated with some uncertainty. If adhere to the principle of conservatism, then can use the following deterministic approach: for the values of average time periods (T_i, $T_{CP\ cep}$) set the interval of uncertainty in the size of 30% (as supposed at the international level for human actions). Then, T_{min} and T_{CP} are calculated as [8]:

$$\mathrm{T}_{\min} = 0{,}7 \cdot \sum_i T_i \ , \tag{1}$$

$$\mathrm{T}_{CP} = 1{,}3 \cdot T_{CP\,cep} \tag{2}$$

The averaged time delays of all components that affect the overall delay time depend too much on the training and technical equipment of the offender, as well as on the quality knowledge of the designers of the security system for the installation alarm systems by them. Therefore, the development of further methods for evaluating the functional efficiency of the perimeter security alarm system for any objects is relevant.

3. Determination of the integral probability of detection of the offender.

The basis of the new technique may be not to compare the characteristic time of the offender and the security forces, but the assessment of the aggregate importance of the interim and final objectives of the offender - zones of penetration or possible intrusion, which must be blocked by appropriate (suitable) means of detection (MD) or alarm signaling detectors. The total number of them, as a rule, is limited to reduce the possible excess flow of false positives. As a rule, a real object uses a limited number of MD of different types (j = 1 ... M), and, for blocking any i-*th* zone, their number typically does not exceed $M(i) \leq 4$. From the correct choice of the nomenclature $j = 1 \ldots M(i)$ MD with a limited number of them, to block all $i = 1 \ldots N$ protection zones, the effectiveness of the operation of the object depends primarily on the PPS object.

The total probability of detecting an offender in the i -*th* area of space (P_{ei}) M by means that completely overlap it and under the condition of independence of the action of the MD is calculated as:

$$P_{ei} = 1 - \prod_{j}^{M(i)} \left(1 - P_{ej}\right) \tag{3}$$

where P_{ej} – probability of detecting the offender by j-*th* means.

Consequently, the aggregate probability of detection (P_{ei}) characterizes the probability of an offender detecting system before the total time delay provides the required response time. Such a characteristic of the system of physical protection is called the concept of timely detection. From this it follows that any time-delay manipulation to the first positively evaluated detection has no real effect, since the reaction's anxiety begins only after the first detection. The path of the offender, in which P_{ei} is the least, is a critical path.

The above approach is described in Fig. 2 [8], where the offender must complete 8 successful actions (for example, jump over the fence, approach the next barrier, penetrate past him, run into the building, penetrate it, etc.).

In fig. 2 is shown that the detection point that relates to Stage 5 is a critical detection point (CDP) along this particular path, since after this point, the total delay time of systems still exceeds the response time of the response forces.

However, the formula (3) does not take into account the correct application of the type of MD in a specific i-zone of protection. For example, an alarm signaling device intended for indoor use may be ineffective in protecting the perimeter area. Therefore, an estimation of the correctness of the use of j-*th* type of MD in the i-*th* area of protection can be accomplished by multiplying the parameter P_{ej} by a certain coefficient of correction K_{ij}, and K_{ij}=1, if the application of MD fully meets the perimeter protection requirements, K_{ij}=1/2, if the application of the MD is partially in line with the terms of protection and K_{ij}=0, if the application of the MD does not fully comply with these conditions.

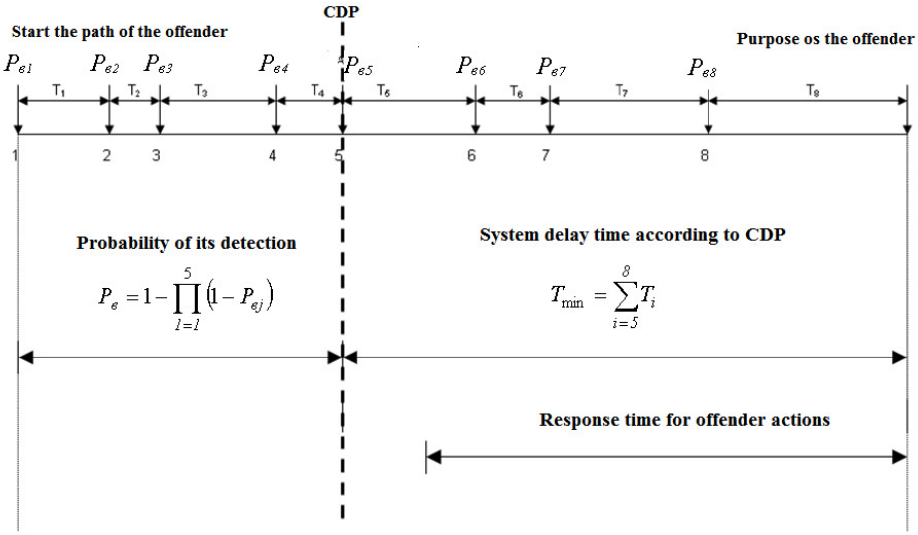

Figure 2. Schematic diagram of the trajectory of the offender movement

In view of the above, the expression (3) for the complex indicator of the ability of the security alarm to detect the offender in the i-*th* zone will look like:

$$P_{ei} = 1 - \prod_{j}^{M(i)} \left(1 - K_{ij} \cdot P_{ej}\right) \tag{4}$$

The required K_{ij} coefficient of i-zone protection can be determined using expert judgment, for example, in the range 0 ÷ 10 for all N targets (then averaged over each group). The smaller coefficient corresponds to the lower significance of the target, and, therefore, there is a lower need for protection in the limitation of composition of technical means of protection (TMP).

For the target parameter of the efficiency of the PPS of an object, the functional E_0 is taken as the sum of the multiplicative components $K_{ie} \times P_{ei}$ for all local zones of protection $i = 1 \ldots N$, while the efficiency criterion has the form:

$$E_o = \sum_{i=1}^{N} K_{ie} \cdot P_{ei} \tag{5}$$

where K_{ie} – expert coefficient of importance or necessary protection of the zone; P_{ei} – aggregate indicator of the ability to detect an offender in the i-*th* area.

The maximum value of E_o can be obtained by simulation, for example, using the genetic algorithm method [9]. In practice, it can be calculated in close proximity to the optimal layout of the MD, proposed by an experienced TMP designer to protect the perimeter.

The concept of timely detection of the offender in the controlled area of the space is formulated. It has been established that the efficiency of the physical protection

system of the perimeter is characterized by the probability of detecting the violator system before the total time delay provides the necessary response time of response forces. Such a characteristic of the system of physical protection is called the concept of timely detection. From this it follows that any time-delay manipulation to the first positively evaluated detection has no real effect, since the alarm begins only after the first detection.

REFERENCES:

1. GONCHAR S.: Analysis of probability of realization of threats of information protection in automated control systems of technological process, Information protection, V.16(2014)1, 40-46.
2. CHUNYAN QIU, WEI ZHAO, JIANHUA JIANG,J IALING HAN. (2013), A Teaching Model Application in the Course of Information Security, Education and Management Engineering, (2013)1, 14-20.
3. ISO/IEC 27002:2013 Information technology -- Security techniques -- Code of practice for information security controls
   URL: https://www.iso.org/standard/54533.html
4. WENJUN FAN, KEVIN LWAKATARE, RONG RONG: I-E based Model of Human Weakness for Attack and Defense Investigations. Computer Network and Information Security, 1-11, Pub. Date: 2017-01-08.
5. Federal Criteria for Information Technology Security, Draft Version 1.0 (Volumes I and II), jointly published by the National Institute of Standards and Technology and the National Security Agency, US Government, January 1993.
6. SHABNAM MOHAMMAD HASANI,NASSER MODIRI: Criteria Specifications for the Comparison and Evaluation of Access Control Models, Computer Network and Information Security, 19-29, Pub. Date: 2013-04-16.
7. The Security Risk Management Guide, URL: *http: // trygstad.rice.iit.edu:8000 / Books / TheSecurityRiskManagementGuide-Microsoft.pdf.*
8. Evaluation of the effectiveness of the physical protection system of nuclear facilities (with the exemption of those operating reactor having less than 1 MW thermal power), and radioactive waste temporary storage and final disposal facilities. Published by: Dr. József Rónaky, director-general of HAEA Budapest, 2011 October.
9. ZVEZHINSKY S.S.: Evaluation of the functional effectiveness of burglar alarm of small objects. Zvezhinsky S.S., Golubkov G.V., Ivanov V.A., Sizov S.M. - Special equipment and communication. 2013.