# Evaluation of the Effectiveness of the Integrated Security System as an Information System

Tetiana Vakaliuk[a,b,c], Oleksandr Dubyna[a], Tetiana Nikitchuk[a], Oleksandr Andreiev[a]

[1] *Zhytomyr Polytechnic State University, 103 Chudnivsyka Str., Zhytomyr, 10005, Ukraine*
[2] *Institute for Digitalisation of Education of the NAES of Ukraine, 9 M. Berlynskoho Str., Kyiv, 04060, Ukraine*
[3] *Kryvyi Rih State Pedagogical University, 54 Gagarin Ave., Kryvyi Rih, 50086, Ukraine*

**Abstract**

Protection and health care, life, habitat, material, and intellectual property of a person is an essential task at the present stage of development of society. To solve this problem, integrated security systems consist of a video surveillance system, security and fire alarms, access control, and management systems. In the early stages of development, these components were mainly used as independent protection elements. To date, they are used in one complex to solve the problem of technical protection of the facility. One of the important hardware and software means of protection is the elements and devices of electronic technology, including touch devices. Their functioning is based on the achievements of solid-state physics, optics, electrooptics, electroacoustics, etc. Modern electronic technologies make it possible to create effective microelectronic sensor devices for security and protection systems, the operation of which consists of the use of optical, mechanical, magnetic, piezoelectric, tensometric, capacitive, and other types of signal converters. In the process of building modern security and protection systems, it is necessary, on the one hand, to have information about the capabilities and features of the functioning of individual constituent elements that ensure the fulfillment of tasks for the protection of an object. On the other hand, it is necessary to evaluate the effectiveness of the developed system, which should include both the reliability indicators of all elements and information transmission channels and the performance indicators of the functional task. The developed mathematical model of the effectiveness of the application of the security system will make it possible to make the right choice of the constituent elements of the system, the parameters of which most fully ensure the fulfillment of the security task. This approach ensures the organization of interaction between security alarm systems, fire alarms, access control systems, video surveillance systems, and centralized security consoles.

**Keywords**

a complex of technical means, a security system sensor, a centralized security control panel, the effectiveness of the security system

## 1. Introduction

At present, the object protection system is an integral part of any enterprise, private house, etc. [1], [2], [3]. In general, such a system is integrated or complex and includes a video surveillance system, a security and fire alarm system, and an access control and management system. By the tasks that are solved during the protection of both the object as a whole and the management of information protection, a complex integrated security system (ISS) must perform tasks related not only to detection (issuance of an "alarm" signal) or non-detection the fact of unauthorized access, but also the determination of belonging to a species, class, subclass or type depending on the problem being solved. Based on this, ISS should be considered an information system designed to obtain information about

ICST-2023: Information Control Systems & Technologies, September 21-23, 2023, Odesa, Ukraine.
EMAIL: tetianavakaliuk@gmail.com (T. Vakaliuk); Dubyna1357@gmail.com (O. Dubyna); tnikitchuk@ukr.net (T. Nikitchuk); Oleks.Andreyev@gmail.com (O. Andreiev).
ORCID: 0000-0001-6825-4697 (T. Vakaliuk); 0000-0003-3448-6072 (O. Dubyna); 0000-0002-9068-931X (T. Nikitchuk); 0000-0002-2601-1491 (O. Andreiev).

the state of the object and its further processing. This information can be sent both to the security control panel and the owner's computer or mobile phone, both via wired and wireless communication channels [1], [4]. This will allow the operational staff (OS) or the owner to take management actions aimed at taking appropriate measures related to the process of task forces and means of response.

Today, as primary sensors, devices that have a fairly powerful functionality with the formation of an extended format of data about the object can be used. The issue can be resolved not only by detection but also by its classification. This, firstly, affects the complication of the hardware implementation of the tools, secondly, it imposes restrictions related to the evaluation of the effectiveness of security systems taking into account their reliability.

This approach requires the use of private, generalized, and complex indicators when applying complex technical tools (CTT) in security systems by the assigned tasks. An analysis of the literature has shown that to date there is no mathematical model of CCT that would allow for an optimized choice of the structure and composition of the facility security system, taking into account the quality indicators of the system elements. Therefore, there is a problem in choosing a function model for evaluating the effectiveness of automated systems for the protection of objects of this type.

The **purpose** of the article is to build a mathematical model for evaluating the effectiveness of the security system, taking into account the reliability of its elements.

## 2. Theoretical background

In [4], the importance and necessity of taking into account the success factors of information security management in the segment of small and medium-sized businesses is noted. 4 key success factors for information security management have been identified, including the fit of information security management with the company's business activities, top management support, tools of security controls, and organizational awareness. In [5], the considerable complexity of the construction of the perimeter security signaling system is shown. When choosing it, it is worth taking into account both the engineering means of strengthening the perimeter and the strategy of organizing security at the facility as a whole. In [2], an analysis of a significant number of factors affecting the qualitative and quantitative indicators of object protection systems is carried out. They include the composition of the object; its territorial location; configuration of the perimeter of fences; availability and location of means of access control and management; video surveillance; alarm systems, types of sensors, and types of communication channels. The complexity of building a facility's security system should correspond to the level of threats. In [6], the modern level of home automation to provide a security system, its capabilities, advantages, and disadvantages are noted. [7] shows the importance of providing home security to prevent intrusions into both private homes and business premises and offices. For this, a project built using a programmed microcontroller, motion sensors, and switches is proposed.

In [1], attention is paid to the deployment of home security/alarm systems using Global System Mobile (GSM) technology as a channel for transmitting alert signals to a smartphone. In [8] it is shown that access control mechanisms of corporate information security technology usually reduce the productivity of employees, forcing them to spend time on tasks related to security. The conducted analysis shows that today, both in the private sector and in production, considerable attention is paid to the safety of facilities. But organizations must invest heavily in security technologies and take steps to reduce their cost to maintain a balance between security costs, resource drain, and security technology effectiveness. In[9] , the general indicators of the evaluation of the effectiveness of complex protection systems and the methods of their calculation are given. At the same time, quite a few works are devoted to the effectiveness of technical protection of objects.

## 3. Results

### 3.1. A probabilistic approach to evaluating the effectiveness of an integrated security system

In the general case, indicators of efficiency with ISS, as an information system [2], can be represented by a group that includes, on the one hand, indicators characterizing the CTT of security

systems, on the other hand, indicators characterizing the human factor. Taking into account that the technical component of the CTT of protection systems is decisive in the reliability of their structures, in the future we will stop at the consideration of the first group of indicators.

To determine the effectiveness of the security system, we will use the approach in which the process of evaluating the effectiveness of the object's security systems as an information system consists of several stages, which include, first, the step-by-step transformation of the structures of the systems of private generalized indicators, and second, their presentation in an indicator containing models of the lower level of association, namely a complex (integral) indicator of efficiency. This makes it possible to visualize the indicators of complex-type protection systems in the form of a hierarchy of indicators of the efficiency and reliability of CTT [10].

When considering the "tree" of efficiency and reliability indicators (Fig. 1), it is assumed that the CTT consists (third level) of n sensors (primary elements) and m communication channels. Each of these elements is characterized by the efficiency index Kefs, Kefch (left branch) and reliability Krs, Krch (right branch). The second level is characterized, on the one hand, by efficiency indicators, namely Kefs, Kefch, which have the meaning of generalizing efficiency indicators both due to the use of security sensors and due to the use of communication lines (wired or radio communication), respectively, on the other hand on the other hand, efficiency indicators, namely Krs, Krch, which have the meaning of generalizing efficiency indicators that characterize the reliable characteristics of sensors and communication lines, respectively. The first level of the hierarchy of CTT efficiency and reliability indicators is characterized by higher-level indicators, which are presented in the form of Kectt, Krctt, which have the meaning of complex indicators of the effectiveness of the CTT structure and the reliability of the CTT structure, respectively. The higher level (zero) of the "tree" of indicators includes indicators of the lower level and is represented by a comprehensive indicator of the effectiveness and reliability of the CTT structure (Kef). At the same time, the analysis of the construction of object protection systems makes it possible to conclude that this structure is an information-automated system [5], which is identified by several subsystems. Therefore, during the analysis of CTT, it is possible to introduce information elements (IE) into consideration.

Next, IE will be understood as the simplest element of object protection, reflecting sources (channels) of information. Therefore, two classes of indicators that characterize, on the one hand, the detected and recognizable properties, and, on the other hand, the reliable capabilities of the security system, can act as indicators of the quality of the security system, in general, reflecting the efficiency and reliability of the third level of the hierarchy (Fig. 1).

The revealed and recognition properties of the CTT of the security system can be represented by the probabilities of correct detection of the signal by the sensors, erroneous or correct classification of objects, and timeliness of information processing in the path of signal recognition [9].

The reliable capabilities of CTT are associated with sudden failures that occur during the operation of security systems and are characterized by a set of several indicators, among which can be highlighted, for example, the probability of error-free operation, the timely release of information through communication channels, the effectiveness of the task performed in communication channels.

## 3.2. Assessments of the effectiveness of the complex technical tools ISS

The above allows you to imagine the quality of the functioning of the security system of the object protection system based on the hierarchy of indicators (Fig. 1) and introduce a vector indicator that determines the effectiveness and reliability of CTT in the following form:

$$W_{ef} = \|W_1, W_2, W_3, W_4, W_5\| \quad (1)$$

In expression (1), components $W_1, W2, W3, W4, W_5$ are performance indicators characterizing the detection of an object by sensors, the correctness of object classification, timeliness and correctness of information processing in the processing unit, reliable characteristics of sensors and communication lines, and timeliness of information delivery through communication channels, respectively.

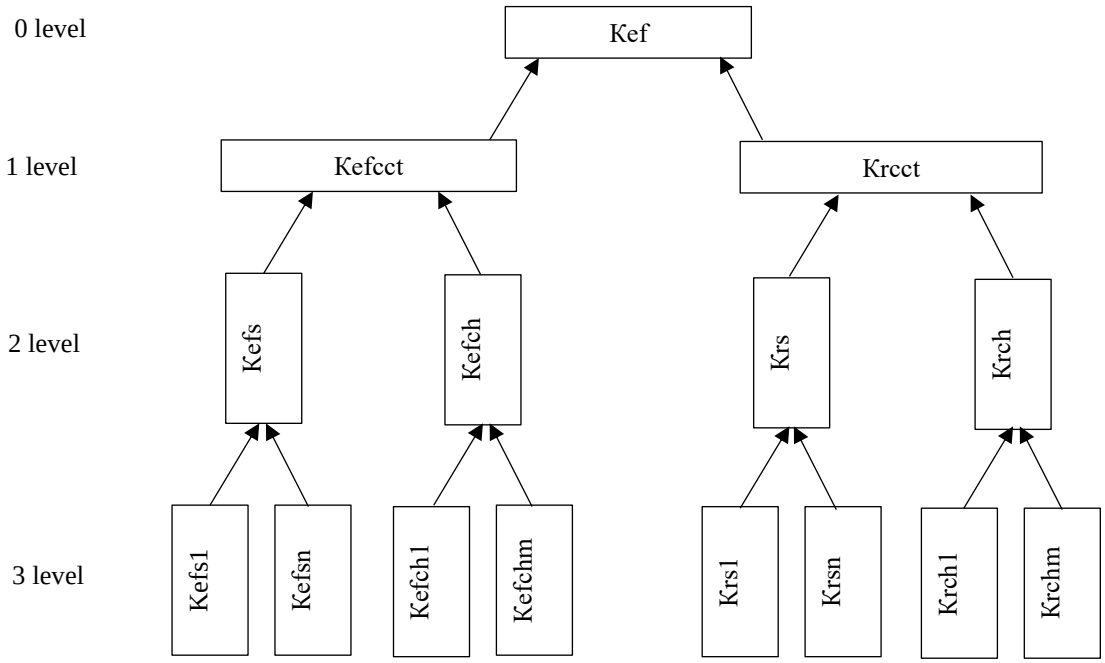


**Figure 1**: Hierarchy of indicators of efficiency and reliability of CTT

In general, the work of any security system consists in performing the following basic operations: detection of a conditional violator, his recognition or identification as a result of processing the primary information received from the sensor, making an appropriate decision based on the purpose of this system (formation of control signals) and data transmission by communication channels to the technical means of displaying information (computer, mobile phone, remote control) to the operator (owner).

It should be noted that a certain class of modern sensors (for example, video cameras) are capable of performing several of the main operations: detection, recognition, and identification, while for others only detection is performed, and the rest of the operations take place in the processing unit (video recorder, reception and control device, controller, etc.).

In the general case, when building protection systems taking into account the works to evaluate the constituent components $W_1$, $W_2$, and $W_3$ included in expression (1), probabilistic indicators can be considered:

$P_{os}$ – the probability of object detection by sensors;

$P_{kl}$ — the probability of correct classification of objects by sensors;

$P_{pr}$ is a probability that characterizes the timeliness of information processing in the signal recognition path.

It should be noted that two factors must be taken into account when analyzing security systems, namely: firstly, the elemental base when creating sensors and communication channels is characterized by sudden failures, that is, the above-mentioned IE during operation has a finite failure time, and secondly, it is necessary to ensure the release of information within a time that does not exceed the established regulatory requirement. In this case, when evaluating the elements of the structures of the object protection system, it is advisable to present the components of the vector indicator with probabilistic indicators and supplement them with the following reliability characteristics: the probability of failure-free operation of the sensor $P_{rd}$, the probability of failure-free operation of the communication channel $P_{rch}$ and the probability of execution, which characterizes timeliness issuing information via the communication channel $P_{tch}$. Taking into account the above, the vector indicator represented by expression (1) is reduced to the form

$$W_{ef} = \|P_{os}, P_k, P_{pr}, P_{rd}, P_{rch}, P_{tch}\| \quad (2)$$

Taking into account the fact that currently the latest advances in microelectronics, namely integrated technologies, are used in the protection systems in the manufacture of IEs, the presented types of IEs are approximately equally reliable. In this case, from a practical point of view, in expression (2), along with the values $P_{rch}, P_{rd}$, it is possible to operate with the value of the average failure intensity $P_r$ [11].

Taking into account the multiplicative approach to combining generalizing indicators, the indicator of efficiency and reliability of the CTT of the security system can be written analytically as

$$W_{ef} = P_{os}, P_k, P_{pr}, P_r, P_{tch} \quad (3)$$

At the initial stage of the security system, the detection process takes place with $P_{os}$ - the probability of object detection by tools of detection (TD). This practically determines the next stages of processing and execution of the task by the security system as a whole [2]. A multifaceted protection system is formed, as a rule, based on the application of TD and classification, which work on different principles and refer to combined tools of detection (CTD) [12], [6].

The following schemes of logical processing of alarm signals from individual emergency shelters have become the most widespread for CTD: M with N, in particular: 1 with 2 (N=2, M=1); 1 of 3 (N = 3, M = 1); 2 of 3 (N=3, M=2). Processing of such signals, as a rule, is carried out based on AND and OR logic circuits.

According to the first scheme, all TDs must have the same probability of detection (when fixing the probability of false alarms). When processing signals according to the second scheme, it is advisable to equalize the values of the false alarm probabilities of all TDs, when fixing the probability of detection.

At present, the following algorithms for processing binary signals from TD are the most widely used:

- based on theoretically possible combinations of TD that worked;
- as a result of the assignment of weighting coefficients to TD.

We will give an example of the algorithm for processing binary signals from three TDs based on theoretically possible combinations of TDs. For each of the TD, let's take $P1, P_2, P_3$ - their detection probabilities and $\overline{P_1, P_2, P_3}$ - false alarm probabilities.

Table 1 gives for each of the combinations, the probabilities of their appearance when the violator $\Delta P_j$ passes and in the presence of interference $\overrightarrow{\Delta P_j}$ (j- number of the combination).

**Table 1**

Theoretically possible combinations of three TD

| j | Combination | $\Delta P_j$ | $\overrightarrow{\Delta P_j}$ |
|---|---|---|---|
| 1 | 111 | $P_1P_2P_3$ | $\overline{P_1P_2P_3}$ |
| 2 | 110 | $P_1P_2(1-P_3)$ | $\overline{P_1P_2}(1-\overline{P_3})$ |
| … | … | … | … |
| 8 | 000 | $(1-P_1)(1-P_2)(1-P_3)$ | $(1-\overline{P_1})(1-\overline{P_2})(1-\overline{P_3})$ |

To find the probability of detection for the logic processing scheme 2 out of 3, it is necessary to add up the probabilities of those combinations in which there are two or three units [11]:

$$P_{2/3} = \sum_{j=1}^{4} \Delta P_j \quad (4)$$

Probability of false alarm:

$$\overline{P_{2/3}} = \sum_{j=1}^{4} \overrightarrow{\Delta P_j} \quad (5)$$

With

$$\sum_{j=1}^{8} \Delta P_j = \sum_{j=1}^{8} \overrightarrow{\Delta P_j} = 1 \quad (6)$$

The optimal scheme for the logical processing of the CTD will be the one that, with the provision of a given probability of detection, has the lowest probability of a false alarm, and, accordingly, the synthesis of such an algorithm will be as follows: arrange the combinations in Table 1 in descending order of the ratio $\Delta P_j / \overrightarrow{\Delta P_j}$ and select from this table the number of first combinations that provide a given probability of detection.

At present, approaches to evaluating the effectiveness of ISS practically do not take into account the fact that any object protection system operates under the conditions of significant uncertainty of both internal and external environments and is described by mathematical models based on information that is of an undefined or incomplete nature.

Existing approaches are based either on the exclusion of uncertainty from their mathematical models or on simplifications and formal descriptions. Therefore, the question arises in the development of new, additional analytical approaches to solving problems regarding the assessment of the effectiveness of ISS applications.

Based on the analysis of existing methods, it can be concluded that ISS should be considered a complex information system and its effectiveness should be characterized by several partial indicators and a general criterion should be formed based on them [9].

As the analysis [2] showed, the effectiveness of ISS functioning depends on a significant number of interrelated factors, which are assessed by a set of criteria that are in complex and quite often mutually exclusive relationships. The current lack of a general approach to solving tasks in this class causes a variety of different unrelated methods for assessing the level of security of objects. The process of determining the effectiveness of object protection systems begins with the selection and justification of indicators (criteria) for evaluating the effectiveness of the object protection system, followed by the selection or development of methods for calculating these indicators.

Table 2 shows the conventional names of the approaches that can be used to select criteria and evaluate the parameters of the effectiveness of object protection systems and their calculation methods [9].

**Table 2**

Conventional names of the approaches that can be used to select criteria and evaluate the parameters of the effectiveness of object protection systems and their calculation methods

| N | The ISS assessment approach | Indicator of performance assessment | Method of calculation |
|---|---|---|---|
| 1. | Optimizing | The task of discrete-form programming is solved: maximize $\sum_{j=1}^{n} c_i x_i$ If $\sum_{j=1}^{n} a_{ij} x_j \le b, i = \overline{1,m};$ $x_j \in \{0,1\}; j = \overline{1,n};$ | Balash's methods for integer variables, branches, and limits, exclusion of groups of unknowns, elements of duality theory, linear, convex, and parametric programming tools. |
| 2. | A multi-level approach | The ISS state is described by a set of privacy levels and a set of privacy categories. | Models of Bel La Padula, D. Denning. |
| 3. | Matrix | The ISS state is described by three parameters, for example: (S, O, AR) – set S – subjects, O – objects, AR – access rights. | 1. Finding parameters.<br>2. Formation of a three-dimensional matrix of relations and its transformation into a two-dimensional table.<br>3. Finding qualitative and quantitative values of indicators |
| 4. | Risk minimization method | The indicator of the economic effect of risk management is calculated according to the formula that takes | 1. To carry out risk fixing.<br>2. Determine the risk index. |

| | | | |
|---|---|---|---|
| | | into account $M_o$- total probable losses without treatment of identified risks; total probable losses after risk processing M; total actual losses from exposure to risks $I_f$; total actual costs for processing identified risks ($H = H_f$); total actual losses from exposure to risks $I_{fn}$; total actual costs for processing risks $H_{fn}$ $$E = \left(\sum_{i=1}^{N} M_{oi} - \sum_{i=1}^{N} M_i\right) - \left(\left(\sum_{i=1}^{N} I_{fi} + \sum_{i=1}^{N} H_{fi}\right) + \left(\sum_{i=1}^{N} I_{fni} + \sum_{i=1}^{N} H_{fni}\right)\right)$$ | 3. Classification of risks by level of action and degree of influence.<br>4. Determination of risk management methods.<br>5. Calculation of indicators characterizing risks.<br>6. Calculation of the indicator of the economic effect of risk management. |
| 5. | Neural network approach (multi-criteria evaluation) | Fuzzy indicators of protection of the object in the form of linguistic variables, such as: "completely unprotected", "insufficiently protected", "protected", "sufficiently protected", "fully protected" $$A = \sum_{i=1}^{n} \frac{\mu^A(x_i)}{x_i}$$ | Belonging to a certain level of security is determined on the interval [0, 1], reliability indicators are a function of membership $\mu^A(x_i)$, where $x_i$ is an element of the set X of security requirements, A is a set of values that determine the fulfillment of security requirements. Evaluation of efficiency is carried out according to clearly defined criteria. |
| 6. | Informational and entropic | Shannon's value of information entropy | An analytical calculation of the information entropy of the system is carried out using the concept of function convolution. With a linear dependence, the efficiency of the integration of subsystems in terms of information is considered satisfactory. Otherwise, it is ineffective. |
| 7. | Expert assessment | The SR security level of the S system $$SR_{(s,r)} = \frac{1}{n}\sum_{i=1}^{n} W_i G_i$$ | The number (n) and the list of parameters (i) that characterize ISO are determined. The values of the subjective coefficients of importance ($W_i$) are given to each of the characteristics $G_i$ assigned by an expert. SR parameter values are calculated. |

| | | | |
|---|---|---|---|
| 8. | Frequency | The expected loss from the i-th threat is calculated: $R_i = F(S, V)$ where $S$ - is the parameter of the frequency of the appearance of the threat; V is a conditional indicator of loss. | Based on the analysis of statistical material, the value of S is set, the value of V is chosen to be equal from 1 to the maximum possible amount of damage, and the value of the indicator $R_i$ is calculated as a function of the parameters V and S. |
| 9. | Probable | Total average losses $R = \sum_{i=1}^{2^n} \sum_{j=1}^{2^n} P(\vec{\gamma}/\vec{x}) P(\vec{s}) V(\vec{\gamma}/\vec{s}) + m$, $P(\vec{\gamma}/\vec{x})$ – the probability of elimination; $P(\vec{s})$ – a priori probability of the state of the object of control; $V(\vec{\gamma}/\vec{s})$ – loss of decision-makings at the state of the object s m is the number of recognized threats. | The probability of non-fulfillment of tasks as intended by the object as a result of the implementation of threats is determined. |
| 10. | Statistical | The threat of the i-th type occurs on average during the time $T_i$ | Statistical processing of potential threats and their consequences. |

One of the ways to evaluate the effectiveness of ISS is an approach called optimization or combinatorial. It solves the task of optimizing a species: maximizing a certain function under given constraints. The type of objective function and the system of restrictions are built depending on the nuances of the task [6]. Let:

$U = \{u_j\}$ – a plural of security threats, $j = 1, \dots m$;

$A = \{a_i\}$ – a plural of TD, $i = 1, \dots n$;

$C = \{c_i\}$ – allowable defense costs, moreover $c_i$ – this is the cost of receiving $i$-th TD;

$W(i, j)$ – the effectiveness of the application of the i-th threat to neutralize the j-th threat.

To build a mathematical model, we enter the variable p(i,j) equal to 1 if the jth threat is detected by the ith - TD and 0 otherwise.

We believe that informational threats are not related to each other. The task is to find the maximum effect from the detection of threats U with the help of the declared in the system of TD A, subject to restrictions on the total amount of expenses C.

Taking into account the obtained analytical expressions, the optimization problem of determining the best structure of the integrated security system is presented in the form of the following ratio:

$$\sum_{j=1}^{m} \sum_{i=1}^{n} W_{ef}(i,j)\ p(i,j) \to max \tag{7}$$

with restrictions

$$\sum_{i=1}^{n} c_i * sign \sum_{j \in U}^{n} p(i,j) \le C \tag{8}$$

$$p(i,j) \in (1,0)$$

Modern object protection systems can use several information transmission channels to increase reliability. It can be a wired or Wi-Fi channel, or one or more mobile communication channels using

different operators [12]. In addition, in the case of using wireless communication, the main and additional data transmission channels on different frequency bands can be provided.

To investigate the effectiveness of the proposed approach and mathematical model, we will use the modern equipment of the Ajax security system. It represents the basic security alarm kits on the market, which are necessary for the technical protection of the object. The main components of the kit are a control panel, wireless motion, and opening detectors, and a key fob. Based on this set, by adding the necessary elements, depending on the complexity of the object, you can form the required integrated security system. These sets differ in various parameters and characteristics of the devices included in the composition. In addition, video cameras from most modern manufacturers can be added to the system. Thus, we get a modern integrated security system (ISS).

By the proposed mathematical model, the probability of detecting an object $P_{os}$ is determined by motion sensors and partially by video cameras, the probability of correct classification $P_k$ is determined by video cameras, the operator, and the capabilities of special software, the probability characterizing the timeliness of information processing in the signal recognition path $P_{pr}$ is determined by the operator and the capabilities of special software, the probability of execution characterizing the timeliness of information output via the communication channel $P_{tch}$ is determined by the state and number of channels In addition, each element is characterized by a failure probability, which is approximately equal to $P_r$.

Table 1 shows the main characteristics of the elements of the basic set of the integrated security system (ISS). By the proposed mathematical model, the probability of detecting an object $P_{os}$ is determined by motion sensors and partially by video cameras, the probability of correct classification $P_k$ is determined by video cameras, the operator, and the capabilities of special software, the probability characterizing the timeliness of information processing in the signal recognition path $P_{pr}$ is determined by the operator and the capabilities of special software, the probability of execution characterizing the timeliness of information output via the communication channel $P_{tch}$ is determined by the state and number of channels In addition, each element is characterized by a failure probability, which is approximately equal to $P_r$.

Table 3 shows the main characteristics of the elements of the basic set of the integrated security system (ISS).

**Table 3**

Main characteristics of the elements of the basic set of the integrated security system (ISS)

| The composition of the security system | Central | Motion detector | Price |
|---|---|---|---|
| Ajax StarterKit | Supports up to 100 devices.<br>1 SIM card, Ethernet.<br>(2 independent communication channels) | Detection range - 12 meters.<br>The viewing angle is 88.5.<br>There is no photo verification function. | 230 |
| Ajax StarterKit Cam | Supports up to 100 devices.<br>2 SIM cards, Ethernet.<br>(3 independent communication channels) | Detection range - 12 meters.<br>The viewing angle is 88.5.<br>There is a photo verification function. | 334 |
| Ajax StarterKit Cam Plus | Supports up to 200 devices.<br>2 SIM cards, Wi-Fi, Ethernet.<br>(4 independent communication channels) | Detection range - 12 meters.<br>The viewing angle is 88.5.<br>There is a photo verification function. | 442 |

Approximate probability values of the relevant parameters are presented in Table 4.

To obtain realistic values, it is necessary to conduct a study of each specific device (which is partially done in production) and use expert groups. The price of each set is presented in conventional units.

A graph of the dependence of the allowable costs of protection C on the efficiency of a given ISS is shown in Fig. 2.

**Table 4**
Theoretically possible combinations of three TD

| ISS equipment option | Composition of the security system | $P_{os}$ | $P_k$ | $P_{pr}$ | $P_r$ | $P_{tch}$ | $W_{ef}$ | C |
|---|---|---|---|---|---|---|---|---|
| 1 | Ajax StarterKit Video camera (2 MP) | 0.8 | 0.7 | 0.9 | 0.9 | 0.7 | 0.32 | 282 |
| 2 | Ajax StarterKit Cam Video camera (2 MP) | 0.9 | 0.8 | 0.9 | 0.9 | 0.8 | 0.47 | 386 |
| 3 | Ajax StarterKit Cam Plus Video camera (2 MP) | 0.9 | 0.8 | 0.9 | 0.9 | 0.99 | 0.58 | 494 |
| 4 | Ajax StarterKit Cam Plus Video camera (4 MP) | 0.99 | 0.99 | 0.9 | 0.9 | 0.99 | 0.79 | 520 |
| 5 | Ajax StarterKit Cam Plus Video camera (8 MP) | 0.99 | 0.999 | 0.9 | 0.9 | 0.99 | 0.793 | 545 |

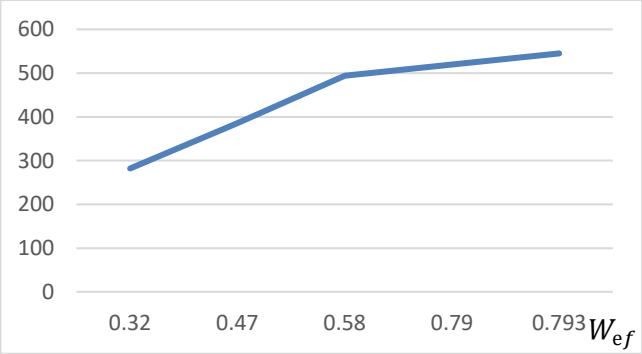


**Figure 2**: Graph of the dependence of the allowable cost of protection C on the performance indicator of a given ISS

The analysis of the data in Table 4 and the graph in Fig. 2 shows the value and nature of changes in the components of the security system depending on the probability indicators and, accordingly, the costs. Thus, when using a motion detector without photo verification, the values of $P_{os}, P_k$ will be the lowest, and with only two communication channels in the central unit, the value of $P_{tch}$ will also be minimal, which determines the lowest efficiency indicator and, accordingly, the lowest costs. The use of security system elements with better performance leads to an increase in costs, but also an improvement in efficiency. At the same time, the proposed mathematical model makes it possible to determine the weight of the improvement of the efficiency indicator when selecting the necessary elements. For example, increasing the resolution of the video camera to 4 and 8MP in variants 4 and 5 (Table 4) leads to a slower improvement in the efficiency indicator than in the first three variants.

Paper [13] proposes an algorithm for finding the optimal combination of physical protection means and the mathematical model is supposed to minimize the cost of organizing a security system.

In contrast, the proposed mathematical model makes it possible to find the best set of components of an integrated security system at limited costs based on quantitative indicators characterizing the quality of the main functions of the devices. This, in turn, more accurately takes into account the specifics of each device and its contribution to the overall optimization process.

## 4. Conclusions

Thus, the considered approach to assessing the quality of the functioning of the technical component in automated security systems, based on the use of the proposed probabilistic indicators, allows for the analysis of devices of CTT from the position of an element of an automated information system. The proposed analytical expressions make it possible to evaluate the effectiveness of the work of the CTT

within the framework of the implementation of the assigned tasks, taking into account the reliability of their structures and probability indicators of information elements.

As an efficiency indicator, it is proposed to use a complex parameter determined by the probabilities of correct detection and classification of the object, timeliness of information processing, and fault-free operation of both primary sensors and information transmission channels.

To evaluate the effectiveness of the security system, it is suggested to use an optimization approach. It allows you to determine the optimal ISS structure with the necessary restrictions that are characteristic of this enterprise (cost, reliability, number of security lines, etc.). The optimization problem can be solved by the methods of Balash or parametric programming.

It is known that the probability of correct detection and classification is affected by a large number of factors (time of day, weather conditions, distance to the object, etc.). One of the solutions to this issue can be the application of the theory of fuzzy sets.

## 5. References


[1] I.K. Olarewaju, O.E. Ayodele, F.O. Michael, E.S. Alaba, R.O. Abiodun, Design and Construction of an Automatic Home Security System Based on GSM Technology and Embedded Microcontroller Unit, American Journal of Electrical and Computer Engineering, 1 1 (2017) 25-32. doi: 10.11648/j.ajece.20170101.14

[2] I.I. Yenina. Processing of signals in case of unauthorized intrusions into the protected object, Scientific notes: a collection of scientific works, 19 (2016) 158-162.

[3] N.M.Lobanchykova, I.A. Pilkevych, O.Korchenko, Analysis and protection of IoT systems: Edge computing and decentralized decision-making, Journal of Edge Computing, 1 1 (2022) 55–67. doi: 10.55056/jec.573

[4] A. Ključnikov, L. Mura, D. Sklenár, Information security management in SMEs: factors of success, Entrepreneurship and Sustainability Issues, 6 4 (2019) 2081-2094. doi: 10.9770/jesi.2019.6.4(37).

[5] I. I. Yenina, S. P. Pleshkov, Integration of technical means in perimeter security alarm systems, Scientific notes: a collection of scientific works, 19 (2016)176-180.

[6] S. Kaur, R. Singh, N. Khairwal, P. Jain, Home automation and security system, Advanced Computational Intelligence: An International Journal (ASCII), 3 3 (2016) 17-23.

[7] G.C Nwalozie, A.N Aniedu, C.S. Nwokoye, I.E,Abazuonu, Enhancing Home Security Using SMS-based Intruder Detection System, International Journal of Computer Science and Mobile Computing. 4 6 (2015) 1177- 1184.

[8] W. Zeng, M. Koutny, Modelling and analysis of corporate efficiency and productivity loss associated with enterprise information security technologies, Journal of Information Security and Applications, 49 (2019). doi:10.1016/j.jisa.2019.102385.

[9] S. V. Toliupa, Y. Ya. Samokhvalov, N. V.Tsiopa, Complex information protection systems of special objects and their assessment methodology, Modern Information Security, 1 (2014) 81-88.

[10] H.M. Rozorinov, I.A. Sirchenko, An expert estimation of efficiency of the information defense systems application in the networks of audiovisual content distribution, Scientific notes of Taurida National V.I. Vernadsky University. Series: Technical Sciences 6 (2022) 48-52. doi: 10.32782/2663-5941/2022.6/09

[11] N. R. Hansen, Probability Theory and Statistics, Department of Mathematical Sciences University of Copenhagen, November 2010.

[12] D. S. Bhadane, M. D. Wani, S. A. Shukla, A. R. Yeole, A Review on Home Control Automation Using GSM and Bluetooth, International Journal of Advanced Research in Computer Science and Software Engineering. 5 2 (2015).

[13] S. Yu. Fedorov, V. N. Khalizev, E.S. Tarasov, Choosing technical components of the physical protection system of objects, IOP Conference Series: Materials Science and Engineering. IOP Publishing, 1227 1 (2022). doi: 10.1088/1757-899X/1227/1/012008