Optimization of the energy efficiency of an integrated security system based on modeling its optimal structure

Sergey Belokurov[1,*], *Alexei* Skrypnikov[1], *Oleg* Kondratov[1], *Dmitry* Levushkin[1] and *Oleg* Tveritnev[2]

[1] State University of Engineering Technologies, Faculty of Management and Informatics in Technological Systems, 19 Revolyutsii Avenue, Voronezh, Russia
[2] Mytishchi branch Bauman Moscow State Technical University, Faculty of Forestry, Mytishchi, ul. 1-ya Institutskaya, 1, Moscow Region, Russia

Abstract. As a result of system modeling we built a global model of the integrated security system as an information system. The proposed model allows us to differentiate one model into a set of private models, the elements of which one by one form the stages of its operation. The model of structural functioning proposed in the work, based on the analysis of the schedule of different states gave the key to understanding the permissible-possible stages of reducing the time of decision-making and thereby optimize its energy efficiency.

1 Introduction

Let us present a structural model of a typical integrated security system (ISB) in Figure 1 [1]:

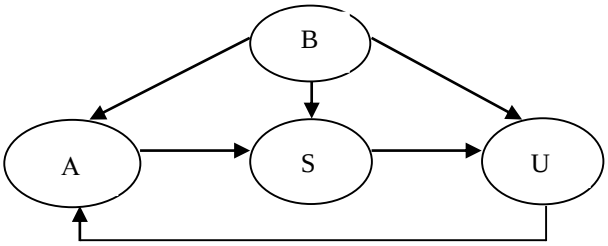

Fig. 1. Structural model of the ISB.

In Figure 1: *A* – intruder; *B* – external factors; *S* – ISB; *U* – decision maker (LPR), such as a centralized security post (CSP), which may include means of detection of the intruder, his detention, as well as means to neutralize the possible consequences.

*Corresponding author: bsvlabs@mail.ru

2 Materials and methods

As a rule, in the system *A*, the behavior of the intruder is described by a probabilistic model, by constructing a list of possible threats. The set of actions of the system *A*, as well as actions coming from the external environment, namely the system B (external factors) carry out all the impacts on the system *S* (ISB) [1-3].

Let us denote the system *S* as a complex structure, which includes a set of inputs, outputs, and a set of states passing from one to another:

$$S = (A, O, C, R) \tag{1}$$

where *A* is the input object; *O* is the output object; *C* is the changing states; *R* is the transition operator responsible for skipping objects and changing states.
System Structure *S*:

$$S = \{S_1, S_2, \dots, S_i\} \tag{2}$$

where $i = \overline{1, M}$ the number of subsystems in operation; *S1* – security subsystem (SS); *S2* – fire safety subsystem (FS); *S3* – alarm triggering subsystem; *S4* – access control system (ACS); *S5* – video surveillance subsystem;

System *S* sets its main task *W to* ensure the security of the object of protection (OOP) against threats [4].

All subsystems $_{Si}$ have their own objectives $_{Wi}$: *W1* – the ability to detect intrusion attempts in time: to eliminate the appearance of persons who do not have the necessary access to the territory important for the security of the OZ, the notification of the possible danger the decision maker (LPR): notification to the central surveillance desk (CCS), etc. *W2* – ability to detect encroachments on the fire safety of the object in time: consists of the same elements as W1, but with the addition of alerting the local fire department duty officer; *W3* – alerting the LPR of a possible encroachment directly; *W4* – creating a properly configured lawful access device with delimited rights, as well as denial of access in case of an unauthorized access (UAA) and alerting the LPR of an attempt to gain access by a person not having the necessary rights to obtain it; *W5* – creating full audio and video control of the OZ.

The internal state of the system *S* is evaluated by the quality of incoming and outgoing signals at its inputs and outputs $aj \in A$, at the information receiving devices, in which the initial processing of data on the state of the external environment, as well as on the behavior of the intruder takes place. An intruder, while attempting to gain access to the OZ, makes unauthorized input influences (UIIA) [5]:

$$A(t) = \{a_1(t), a_2(t), \dots, a_j(t), \dots, a_J(t)\} \tag{3}$$

where $j = \overline{1, J}$ – is the number of attempts by the intruder to commit a NEO at each time point t.

The IAVs are possible threats to the OZ, in addition, they can be committed either separately or in parallel with each other in multiple ways:

$$a_j(t) = f(H(t)) \tag{4}$$

$$H(t) = \{h_1(t), h_2(t), \dots, h_n(t), \dots, h_N(t)\} \tag{5}$$

where $n = \overline{1, N}$ – is the total number of possible threats.

The inverse signal *oj* (output action) of the system *S*, namely, the response to the NSVS *aj*(*t*) at a certain time t will be a function:

$$o_j(t) = R[C(t), a_j(t)] \quad (6)$$

where $R = F(Rm)$ *is the* total response *of S* to the return signal *aj*(*t*) (input action)*;* Rm is the single response of one *m-th* subsystem $_{Sm}$ to the return signal *aj*(*t*) (input action)*;* $C(t) = \{Cm(t)\}$ *is* the total internal state of *S* at a certain time *t*; *Cm*(*t*) is the internal state of one m-th subsystem $_{Sm\ at\ a}$ certain time *t*.

$$O(t) = \{o_1(t), o_2(t), \dots, o_j(t), \dots, o_J(t)\}. \quad (7)$$

In general, the utility of the system $_{Si}$, if the evaluation criterion is a goal $_{Wi}$, can be represented as a function:

$$q(t) = f[a(t), o(t)]. \quad (8)$$

For all possible perfect NSVS, the utility of each of the subsystems $_{Sm}$ if the evaluation criterion is the goal *Wm* at a certain time *t*, can be represented as a function:

$$q_m(t) = f[A(t), O(t)] = f[A(t), R_m(C_m(t), A(t))]. \quad (9)$$

If we set the probabilistic nature of all possible outputs *O*(*t*), in this case we can get the total probability of obtaining information about the state of OZ for the LPR, respectively, the probability is estimated on a scale from 0 to 1 and the closer to 1 the system value *O*(*t*), then the higher the efficiency of this system. Using this approach, we can build a safety matrix (Table 1).

Table 1.

	***a1*(*t*)**	***a2*(*t*)**	- • • •	***aj*(*t*)**	- • • •	***aJ*(*t*)**
S1	*q11*(*t*)	*q12*(*t*)	- • • •	*q1j*(*t*)	- • • •	*q1J*(*t*)
S2	*q21*(*t*)	*q22*(*t*)	- • • •	*q2j*(*t*)	- • • •	*q2J*(*t*)
- • • •	- • • •	- • • •	- • • •	- • • •	- • • •	- • • •
Sm	*qm1*(*t*)	*qm2*(*t*)	- • • •	*qmj*(*t*)	- • • •	*qmJ*(*t*)
- • • •	- • • •	- • • •	- • • •	- • • •	- • • •	- • • •
SM	*qM1*(*t*)	*qM2*(*t*)	- • • •	*qMj*(*t*)	- • • •	*qMJ*(*t*)
S	*qi*(*t*)	*q2*(*t*)	- • • •	*qk*(*t*)	- • • •	*qJ*(*t*)

3 Results and discussion

At the beginning of the paper we presented a generalized representation of the SOFI, on the basis of which we will consider a way to optimize the structure of the SOFI. It is worth paying attention to the extensive number of assorted states of the system *S* at period *t*:

$$C(t) = \{Cz(t)\}. \quad (10)$$

From where it will be equal to $z = \underline{1, Z}$ – is a measure of the number of all different states *S* is in.

Let us turn to the set *C* and delineate from it 3 states *SR, CO, CA*, which will adhere to the conditions [6, 7]:

$$CP \cup CA = C,\ CP \cap SA = \emptyset\,. \tag{11}$$

Wherefore, *SR* is a simple-level system operating without any action from outside. And *CA* will be an ensemble of system states. Each such state will deal with unauthorized influence.

Let us list these states of the system *S* (Figure 2).

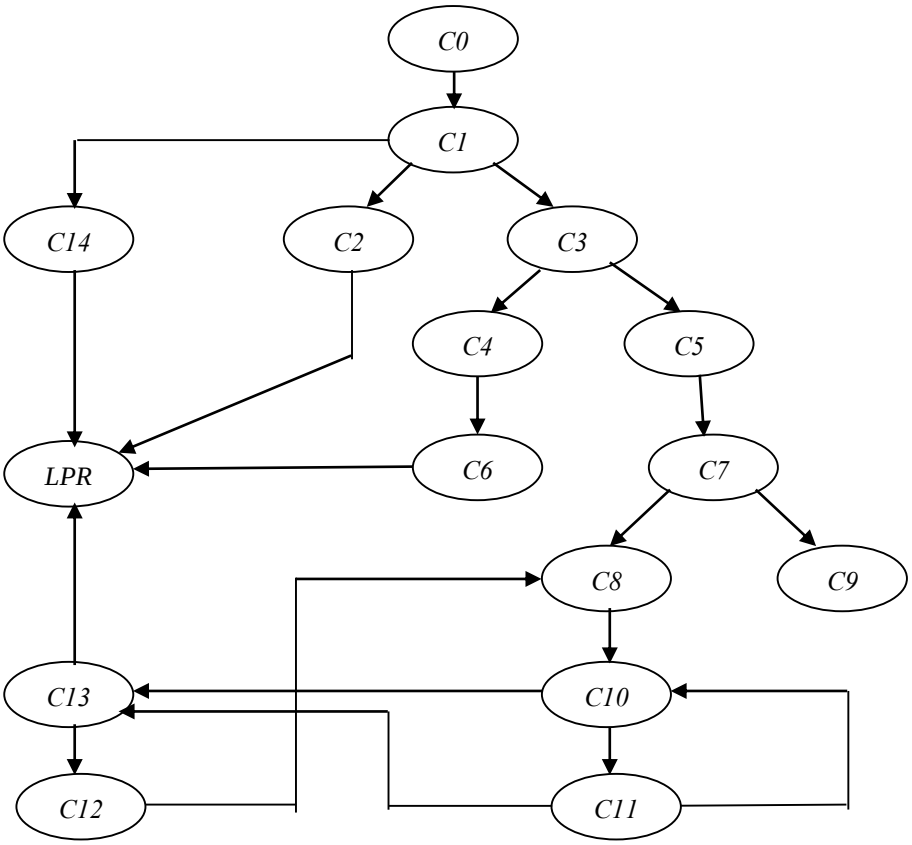

Fig. 2. Graph of security system states.

On Figure 2: *CO* – incomprehensible actions from outside and deviant; *C1* – the system works in statute mode; *C2* – the system stops working in statute mode and there is a threat of a complete shutdown of its own or its components, which forces the responsible person to intervene; *C3* – when an alarm occurs, the system is checked for the source of unauthorized impact; *C4* – the alarm is established and a decision is made about the absence of unauthorized impact; *C6* – "missed target", during the check there is no NSVV; *C5* – checking the alarm leads to a conclusion about the unauthorized impact; *C7* – "false target", the lack of impact of the deviant of the violation causes the system to signal the NCVS; *C3* – a report of threats of unauthorized impact, the system alerts about the attack and blocks access to the deviant of the violation; *C8* – the system transmits information to the LPR after all the threats are fully identified; *C10* – the LPR is aware and all the NSVS are

detected; *C11* – not all NSVS are detected, the LPR is notified; *C13* – the system goes to the stable mode of operation after the LPR has made a decision and eliminated the outcome; *C12* – the LPR was unable to apply methods to eliminate the NSVS; *C14* – the system sends notification to the LPR as a result of power failure.

One of the main flaws of such systems of integrated security system is the process of inevitable intercession of the person – the decision maker in this area and is directly responsible for the implementation of his decisions (LPR).

Such is human nature that even the most "savvy mind" can make mistakes, not to mention the average employee, this is the flaw of the ISB system, because of which in some extreme states there is a possibility of both a complete failure of the system, and its looping.

At the present stage of scientific and technological development of society there is no possibility to automate this process of decision-making, excluding the factor of intercession of LDP, however, in the future such work will be done by artificial intelligence based on a neural network, but the same network must be trained based on human experience, i.e. should take a while before such system will work and function flawlessly.

The Markov chain probability matrix will serve as the basis for obtaining complete information about the variants of probability states (stages) of the system itself:

$$P = \left|P_{ij}\right| = \left|P_{00}\, P_{10} \cdots P_{n0} \;\; P_{01}\, P_{11} \cdots P_{n1} \;\; \cdots \cdots P_{ij} \cdots \;\; P_{0n}\, P_{1n} \cdots P_{nn} \right|. \quad (12)$$

It is true for the transition probability matrix:

$$\sum_{j=1}^{n} P_{ij} = 1 \qquad (i = \underline{0,n}), \quad (13)$$

And

$$0 \le P_{ij} \le 1. \quad (14)$$

The chance of transition of a stage in period t and state i to some other allowed in time period $t+\Delta t$ other than this one is unity, which is proved by conditions (13) and (14).

Applying the probability theory itself, we just find those probability states of the system itself. Paying attention to the event *L*, which is the stay of the system at the stage *Cz*, for example, *C2* – the event *L2*. The finding of the system at stage *C2* is itself a non-uniformly complex incident at time $t+\Delta t$. The occurrence of such an incident, and actually its probabilistic value, is possible only when reproduced simultaneously with one of the following non-complex events, such as the event *L0* at stage *C0 at* time *t*, or *L1* at stage *C1* or *L2* at stage *C2*.

On this basis, it is possible to make such a note that

$$L2 = L0L2 + L1L12 + L2L22, \quad (15)$$

The system will make the transition from stage to stage in the time period Δt, which are assigned ordinal numbering indices: L02, L12, L22.

We take the sum and product of probability theorems as the basis, then:

$$P(L2) = P(L0)P(L2/L0) + P(L1)P(L2/L1) + P(L2)P(L2/L), \quad (16)$$

or

$$P2(t+\Delta t) = P0(t)P02(\Delta t) + P1(t)P12(\Delta t) + P2(t)P22(\Delta t). \quad (17)$$

The index $R_u(t)$ will be an indication that the channel occupancy $y = \underline{0,n}$ at time period *t*, and then calculate the absolute probability of the outcome in which the system will be free of *K* channels at time period $t+\Delta t$;

$$Pk(t+\Delta t) = \sum_{y=0}^{n} \quad P_y(t)P_{yk}(\Delta t). \tag{18}$$

Based on the small increase in the rate of increase in the value of Δt, the index $_{Ruk}(\Delta t)$ will mean the conditional transition probability, because the chance of occurrence of at least one incident, leading the system to the state *K* from the state *y*:

$$R_{uk}(\Delta t) = 1 - e^{-\lambda y k \Delta t} \cong \lambda\, y\, k\Delta t + 0(\Delta t). \tag{19}$$

$R_{uu}(\Delta t)$ is a measure of the probability that no incident was reproduced that could determine the transition of the system from one state to any other at stage *Cz*:

$$P_{yy}(\Delta t) = 1 - \sum_{k=1}^{n-y} \quad P_{y,y+k}(\Delta t). \tag{20}$$

Given (20), we obtain

$$P_{yy}(\Delta t) = 1 - \sum_{k=1}^{n-y} \quad \lambda_{yk}(\Delta t) + 0(\Delta t). \tag{21}$$

4 Conclusions

As a result of system modeling of the interaction of the elements of the external environment with the ISB, a global model of the ISB functioning from the perspective of the information system was built. The proposed model allows the differentiation of one model in the form of a set of private models, the elements of which one by one form the stages of its operation.

The model of the structural functioning of the ISB based on the analysis of the graph of different states gave the key to understanding the permissible-possible stages of the system itself under study, and the Markov chain graph makes it possible to obtain a detection function of the probability chance of moving this system from one stage to any other.

The model of structural functioning proposed in the work, based on the analysis of the schedule of different states gave the key to understanding the permissible-possible steps to reduce the decision time and thereby optimize its energy efficiency.

References

1. S.V. Belokurov, J.E. Lvovich, Noev A.N. et al. *Mathematical modeling of mechanisms for detecting threats of information leakage through parametric channels*, International Conference "Applied Mathematics, Computational Science and Mechanics: Current Problems", J. Phys.: Conf. Ser., **1202**. 012012 (2019)
2. S.V. Zapechnikov, N.G. Miloslavskaya, A.I. Tolstoy [et al] Information security of open systems: a textbook for universities. In 2 volumes. Volume 1. - Threats, vulnerabilities, attacks and approaches to protection. Moscow (2006)
3. Lamonov A.V. Safety of information technologies, **1** (2007)
4. Anthimos Alexandros Tsirigotis. Cybernetics, Warfare and Discourse: The Cybernetisation of Warfare in Britain. Palgrave Macmillan (2017)
5. Michael E. Whitman and Herbert J. Mattord. Principles of Information Security. Cengage Learning (2014)
6. Novikov D. New Frontiers in Information and Production Systems Modelling and Analysis: Incentive Mechanisms, Competence Management, Knowledge-based Production. Springer (2017)
7. Raymond Pompon. IT Security Risk Control Management. Apress (2016)