
Nikolay A. Eroslaev
University of A.F. Mozhaisky
St.-Petersburg, Russia
e-mail: kvn@kvn.vika.pu.ru

Abstract
The main idea of this article is recombined protection systems in computing systems. The given data testify that the danger of the non-authorized actions above the information is not simply real, but has accepted already menacing character. By an inevitable consequence of this danger of steel the constantly increased charges and efforts to protection of the information.

1. Contents of the paper
Last years the plenty of the messages about the facts of the non-authorized influences on the equipment of processing, storage and transfer of the information with drawing of the large material damage has appeared. The given data testify that the danger of the non-authorized actions above the information is not simply real, but has accepted already menacing character. By an inevitable consequence of this danger of steel the constantly increased charges and efforts to protection of the information.

During functioning the computing system the structure of the computing system (CS), technology of data processing, data and their value (cost) can change. Therefore important the maintenance of efficiency of protection at a required level with current of time is at change of the above specified characteristics. Thus it is necessary to give the answers to two rather urgent questions:

1. How to get and to complete information system, that it could be made safe?

2. How practically to generate a mode of safety and to support it in conditions of a constantly varying environment and structure of the system?

For the decision of these questions in organization it is necessary to ensure management of risk, which includes all spectrum of measures resulting in the effective decisions in the field of safety.

Program of management of risk includes 4 basic elements [1]:

1. Definition of a degree of risk (analysis of risk).
2. Choice of security measures.
3. Their certification and accreditation.

One of steps at the analysis of risk is the definition of that property, which needs to be protected. General threat for the most part of organizations is the non-authorized access to the information. Therefore it is necessary to define the information, which needs to be protected. For this purpose it is necessary to be able to estimate its importance for efficiency of the appropriate activity. The parameters of two kinds are necessary for a rating of the information [2]:

1. Describing the information as a providing resource during the decision of various tasks.
2. Describing the information as object of work during information maintenance of soluble tasks.

The parameters of the first kind are defined by a role (importance) of the information during the decision of tasks, and also quantity, contents and sufficiency for information maintenance of soluble tasks.

As the information is represented as some sequence of symbols, i.e. is coded, as the basic characteristics of the second kind can act:

1. Way, encoder of the information.
2. Volume of the information or volume of a sequence of codes.

The importance of the information can be estimated on two groups of parameters:
1. On purpose of the information:
   a). Importance of tasks for provided activity;
   b). Degree of importance of the information for the effective decision of the appropriate task.

2. On conditions of its processing:
   a). Level of losses in case of undesirable changes of the information during processing under influence of threats;
   b). Level of expenses on restoration of the broken information.

Let's designate:

- \( K_{(i.i.)} \) - factor of importance of the information;
- \( K_{(i.t.)} \) - factor of importance of those tasks, for which maintenance is used the information;
- \( K_{(i.d.)} \) - factor of importance of the estimated information for the effective decision of tasks;
- \( K_{(i.l.)} \) - factor of importance of the estimated information from the point of view of losses at infringement of its quality;
- \( K_{(r.q.)} \) - factor of importance of the information from the point of view of restoration of its quality.

Then it is obvious:

\[
K_{(i.i.)} = f(K_{(i.t.)}, K_{(i.d.)}, K_{(i.l.)}, K_{(r.q.)}).
\]  

(1.1)

For today the listed above factors are not known. Quantitative value \( K_{(i.i.)} \) can be received at use of the approach based on informal - heuristic methods [2].

It is known, that in due course information loses the appeal and begins to become outdated, and on occasion its price can fall up to zero. It is necessary to examine adequacy to the information on duration of an interval of time between the moment of its reception and current moment. For a rating of adequacy on given parameter quite suitable is known in the theory of the information the so-called law of aging of the information. For reception of factor of aging of the information \( K_n \) (it can lay in an interval from zero up to unit and represents a curve falling from unit up to zero with current of time) probably use of expert systems.

By attribute of access the information can be classified according to [3]. Using the given classification it is possible to define the quantitative characteristics of the information to an attribute of access (factor of privacy - \( K_p \)). The storage of one information on different objects also influences value of the information (\( n - \) quantity of objects). Thus, the value of the information can be presented as function from 4 arguments:

\[
C(t) = f(K_{(i.i.)}, K_p, K_{p}, n).
\]  

(1.2)

All parameters of the information are divided into three categories: determining, essential, minor. The required level of security is determined on values of determining parameters, if necessary it can be corrected in view of values of essential parameters.

Sets of threats shall designate \( Q = \{q_i\}, i=1..n \). For definition of factor of realization of threat (the time, varying with current) can use exposition structures (means of grouping of problems of safety). Thus the ordering of threats can be carried spent by the commission of experts, formed in organization. The threats to the information are represented as a number, in which more dangerous threats (for the certain information) are located in a beginning of the list, and it appropriates numerical values \( \mu \) in an interval from 0 (if the threats at influence on the block of the information do not put organization of damage) up to 1 (at the maximal damage). At the discrete moments of time at change of conditions of functioning this procedure repeats. Hence, factor of realization of threat depends on time \( \mu(t) \). It is similarly possible to receive and factor of neutralization of threat by a means of protection \( \gamma(t) \). Set of means of protection we shall designate \( Y = \{\gamma_j\}, j=1..m \). Damage from realization i threat on block of the information at absence of a means of protection from it(her) shall express through:

\[
C_{ij}(t) = \mu_i(t) C(t).
\]  

(1.3)

Considering, that factor of neutralization i of threat j by a means \( \gamma_j(t) \) is higher, if it to aspire to 0, damage at presence in system of protection of the information (PIS) of a means against i of threat we shall accept equal:

\[
C_{ij}(t) = \mu_i(t) C(t) \gamma_j(t).
\]  

(1.4)

The task of protection of the information (PI) can be formulated as follows: to support such quantity of means PI in PIS, at which parameter of security of the information \( P_i \) above required \( P_r \), and total cost of resources \( S_j \) thus aspires to the minimum: system of protection of the information

\[
P_s(t) \geq P_r(t) and \sum S_j \rightarrow \min \ \text{for } *j \in \{1,2...,m\}.
\]  

(1.5)

It is obvious, that for good safety information the process of protection should be continuous and controlled [4]. Therefore in system of protection there should be subsystems, with which help the direct and continuous protection of the information, and also component for management of these subsystems is carried out. Besides in system of complex protection of the information the bodies of its perfection should be stipulated. The management PI should have properties of detection and blocking of access to the protected information. Ability PIS to find out and block NAA it should to be taken into account at account of a parameter of security CS [5]. The principle of work of the automated protection is based that in it(her) the block of management makes the periodic control of gauges of detection of infringements. The
results of the control are observed by the man. The time for
development of a signal of the disturbing signal system is
necessary also. But as the physical access to object of pro-
tection is for the present open, the further actions are reduced
to definition of a place and organization of blocking of ac-
cess of the infringer, on what the time is required.
Thus, the condition of durability of protection with detection
and blocking NAA can be presented as a ratio [5]:

$$T_e + t_d + t_{dp} + t_b / t_p < 1,$$  \hspace{1cm}  (1.6)

where $T_e$ - period of interrogation of gauges,
t_d - time of operation of the disturbing signal system,
t_{dp} - time of definition of a place of access,
t_b - time of blocking of access,
t_p - expected time of overcoming of protection by the
infringer.

The initial basis for management of protection is served by
the plans of processing of the information in CS, and on the
basis of the analysis to subject processing of the information
the requirements to protection of the information are proved
which can be expressed by a required parameter of security
$P_r(t)$.

According to $P_r(t)$ the optimum sets of means of protection
(technical, program, organizational, legislative, moral - ethi-
cal), security, providing a required level, of the information
should be determined. The substantiation of such sets of
means of protection is a general task of mechanisms of man-
agement of means of protection. On the basis of the control
the parameter of the valid level of security $P_r(t)$ is defined. It
is compared to a required level $P_r(t)$ and if the mismatch
exceeds allowable value, the control system of protection
should react or change of a set of used means of protection or
change of a parameter of security $P_r(t)$.

The process $P_I$ is necessary for considering as a disputed
situation. For definition $P_r(t)$ most authentic and appropriate
to the validity represent game models of protection, i.e. the
models in which are available two parties. First builds pro-
tection, second overcomes it. The game $G$ is set [6]:

$$G = < X, Y, K >.$$

(1.7)

Where $X$ - set of measures, $Y$ - set of measures and means of
protection, $K$ - function of a prize of the first player.

For $m$ of measures and means of protection the amount of
possible variants of their use $u$ is calculated under the for-
mula:

$$u = 2^m - 1.$$  \hspace{1cm}  (1.8)

Set of variants of construction PIS $Z = \{Z_h\}, h=1,.., u.$

Cost PIS of object $S_h$ ($k$- quantity(amount) of objects of pro-
tection) is equal:

$$\Sigma^*_h, S^*_u = \sum_{j=1}^m w_{jh}^*_j,$$  \hspace{1cm}  (1.9)

where $S_{jh}$ - cost $j$-ãî of a means on $k$ object.

$w_{jh} = 0$, if the means $y_j$ is not used in variant PIS $Z_h$,

$w_{jh} = 1$, if the means $y_j$ is used in variant PIS $Z_h$.

The parameter of security can be expressed as function:

$$D_h = q (Z_h).$$  \hspace{1cm}  (1.10)

$V_{k}-$ a parameter of security reference PIS, which allows to
receive a situation of balance in game, where the functions of
a prize of the player are calculated on (1.4) at the certain
variant $u$. Then the generalized parameter of security $h$ of
variant PIS on object $S_h$ is calculated as follows:

$$D_h = V_{k}(G) / V_{k}(G).$$  \hspace{1cm}  (1.11)

The parameter of security should be recalculated at changes
of the listed above conditions and the control system of pro-
tection should react to all changes so that the conditions
(1.5), (1.6) were carried out.

The optimum decision of a complex problem of a safety of
the information now is possible only at the complex ap-
proach with use both organizational, and technical measures
of protection. The stated above material can be used at the
decision of a complex task of a choice of the appropriate
measures and means of protection at functioning CS.

References

1. Steng D., Mun S. Secrets of safety of networks. Kiev:
"Dialektika", 1996.

2. Gerasimenko V.A. Protection of the information in the

3. Nikolaev U. I. Designing of the protected information
technologies. S-Pb.: S-PbSTU publishing house, 1997.

4. Zima V.M., Moldovyan A.A., Multilevel protection of
the software of computing systems. S-Pb.: Academy of

5. Melnikov V.V. In. Protection of the information in