Decision Making Support Approach in Information Security Systems

I.V. Mashkina
Department of Computer Science and Robotics
Ufa State Aviation Technical University
Ufa, Russia
e-mail: mashkina@vtizi.ugatu.ac.ru

E.A. Rakhimov
Department of Computer Science and Robotics
Ufa State Aviation Technical University
Ufa, Russia
e-mail: gin2003@km.ru

Abstract[1]

The paper covers a new scientific approach to the problem of information security decision-making support system development.

The main advantages of this approach are:

1. It allows finding optimal information security compatible products composition on the basis of maximum value of "safety" to "expenses" ratio criterion function.

2. It allows using expert knowledge for probabilities estimation purpose.

3. It allows developing of real-time response measures to abnormal situations on the basis of gathering data about threats.

1. Introduction

It is a great problem to make information secure in wide-spread distributed networks with remote access service.

In this article term informatization object (IO) means local network as part of distributed network situated in one building.

In [1] it is marked, that the basic lacks of wide-spread information security system have been caused by system construction rigid principles. This systems can't solve successfully an information security level maintenance problem during all period of information system functioning. Information processing plans and corresponding security level requirements [2] change during information system functioning period. In other hand new malicious software and hardware threats widely grow. So, new approaches to information security should be developed. One of these approaches is intelligence information security system development. This system should acquire information security management principles. In other words, system reconfiguration and system resource redistribution and system reinforcement must be realized.

Basic requirements to this system consist of following:

- System should be able evaluate security level changes;
- System should have automated decision-making support subsystem for system resource redistribution;
- System should have automated decision-making support subsystem for intrusion avoiding;
- As system environment changes system parameters must be changed.

There are a lot of scientific researches in this field, but complex theoretic results are rare. So researches are still actual.

Intelligence information security system development is connected with models and methods synthesis of intelligence supplying theory.

Schedule information security management should be included in this system. One of this subsystem tasks is information security facilities selection on the basis of required security level. System should have response facilities for system state changing in real time.

So automated management decision-making support subsystem should be included in this system.

Approach to development of this subsystem has described in this article.

This subsystem should have two functional modules: Schedule information security management decision-making support subsystem and real –time management decision-making support subsystem.

Proceedings of the 8th International Workshop on Computer Science and Information Technologies CSIT'2006
Karlsruhe, Germany, 2006

Realization of these modules will be possible if intelligence information security system scientific approach will be developed.

Hearts of these modules are [3] scheduled solver and real-time solver. These solvers choose actions to information security system. This actions allows the system administrator to response on real-time system state changes or may be scheduled and depend on information plans changes.

2. Schedule Information Security Management Decision-making Support Subsystem

In this article authors introduce automated schedule information security management decision-making support subsystem (fig. 1).

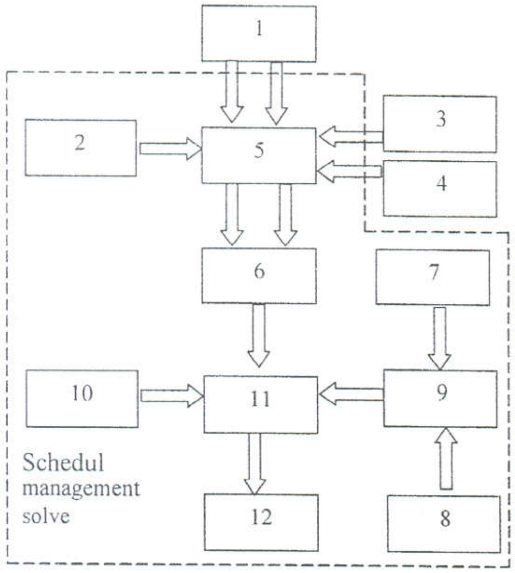

Figure 1. Architecture of Automated Schedule Information Security Management Decision-making Support Subsystem

In this figure:
1 – input data module;
2 – security profiles generating module;
3 – information security facilities database;
4 – information security products database;
5 – information security products combinatory morphological matrix;
6 – information security products compatibility test module;
7 – information security products "safety" criteria's hierarchy module
8 – information security products "expenses" criteria's hierarchy module
9 – "safety" and "expenses" analytic hierarchy process evaluation module;
10 – criterion function assigning module;
11 – complete enumeration of compatible products alternatives;
12 – optimal information security products complex.

Synthesis method of optimal complex of information security products is realized in schedule information security management decision-making support subsystem. This method based on analytic hierarchy process method for "safety" and "expenses" of products and information security products combinatory morphological matrix method.

Authors introduce model for ranging alternatives on the basis of multicriterion analysis and optimal information security products complex selection.

Combinatory morphological system synthesis method [4] is very useful for optimal information security products complex synthesis because it allows to make multicriterion and multi alternatives selection.

System synthesis variants are given as combinatory morphological matrix in module 5.

Compatible system variants are generated in module 6.

System variants with compatible software and hardware products from combinatory morphological matrix are formed as module 6 output.

Next selection is realized in module 11. This module produces complete enumeration of compatible products alternatives based on criterion function. Authors introduce

$$J = \max S / E = \max\left(\frac{\sum_{1} S_{l,m}}{\sum_{1} E_{l,m}}\right)$$

as criterion function for

$$S_r = \{A_{1i}, A_{2j}, \ldots, A_{1m} \ldots A_{ln}\},$$

where $\sum_{1} S_{l,m}$ - sum of system variant "safety" values,

$\sum_{1} E_{l,m}$ - sum of system variant "expenses" values.

All alternatives compare one to one for "safety" and "expenses" criteria's in module 9. All criteria's are ranging for relative importance.

The schedule information security management decision-making support subsystem model is realized as software [5,6].

3. Real-time Information Security Management Decision-making Support Subsystem

The most important problem is an optimal response generating to intrusions and abnormal occasions.

The real –time management decision-making support subsystem should make effective actions for decreasing of threats influence. In other hand, possible

disadvantages to system properties from these actions should be decreased too.

Real –time management decision-making support subsystem structure is showed in fig.2

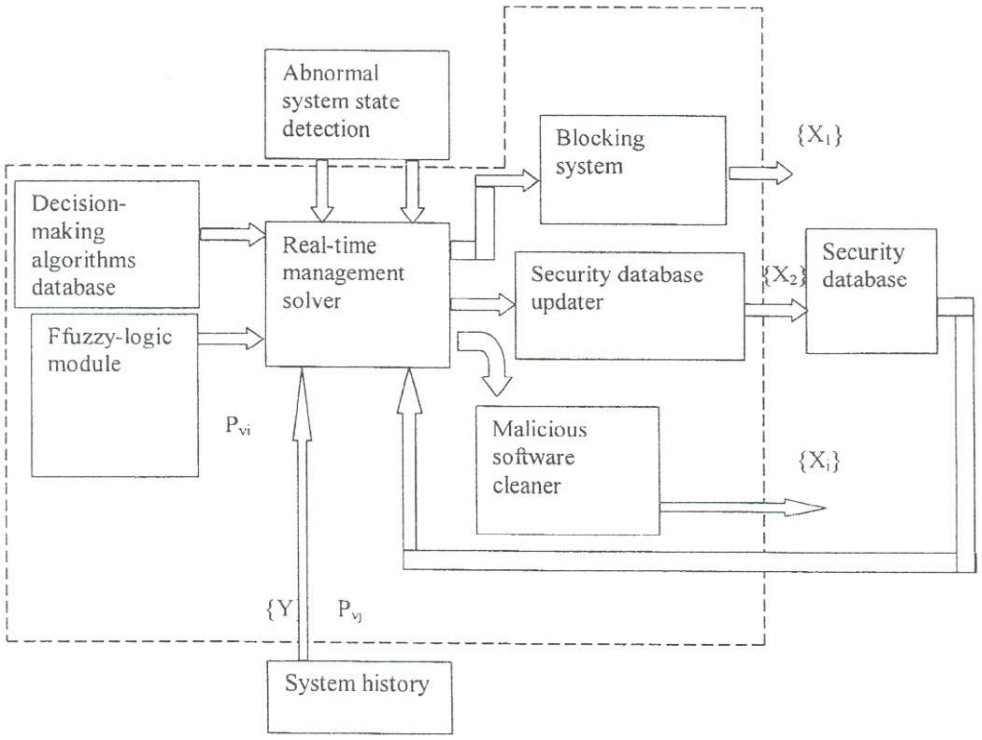

Figure 2. Architecture of Automated Real-time Information Security Management Decision-making Support Subsystem

Informatization object environment is fulfil of threats, so it is extremely important to monitor for information security system in order of gaining abnormal situation data. Monitoring results processing allows choosing responses for dangerous situations.

Informatization object state may be described by next parameters sets:

- controlled parameters {X};
- monitored parameters {Y};
- control actions {U}.

Controlled parameters are:

- user recourses state parameters, for example –user rights, user session time, user software sessions;
- system recourses state parameters, for example – CPU time usage, memory usage, virtual memory usage;
- network recourses state parameters, for example – connection time, connection type, numbers of connections;
- processes state parameters, for example – processes list, state of each process(run, hold, blocked, wait), process living time, CPU usage percent, child processes.

Control actions are: process blocking, process priority decreasing, port blocking, IP address blocking, user access restricting, user priority decreasing, recourse shutdown, full program removing.

Authors introduce decision-making method in abnormal situations. This method is based on risk condition decision-making method [7], but results probabilities are estimated by formula:

$$P_{\upsilon} = \arg\max\{P_{\upsilon i}, P_{\upsilon j}\},$$

where P_{vi} – calculated values of results probabilities on the basis of fuzzy logic;

P_{vj} – statistic values of probabilities.

If there is no statistic values of probabilities, calculated values of result probabilities are used for estimations.

Authors have developed software for this method [8].

References

1. Borodakiy Y.V. "Intelligence information security system". In: *Proc. of VII International scientific and practical conference "Information security"*. News of TRTU, 2005; 4: 65-69.
2. Malyuk A.A. "Information security and method basis of data protection". Hot line-telecom, Moscow, Russia, 2005.

3. Mashkina I.V., Rakhimov E.A. "Model of information security management system." In: *Proc. of VI international scientific and practical conference: "Information security"*. Taganrog, Russia, 2005, pp. 268-270.

4. Mashkina I.V. "Decision-making support system for information security purposes in organizations". Information technologies and hardware, USATU, Ufa, 2001, pp. 184-190.

5. Program registration paper №2004611453. Echoice V1.0 // Mashkina I.V., Zaripov A.T., Shaymardanov B.R.

6. Program registration paper №2006611352. Selection of information security system variants with compatible software and hardware products // Mashkina I.V., Rakhimov E.A., Divel' A.V.

7. Chernorutskiy I.G. "Optimization and decision-making methods". Lan', St.-Petersburg, Russia, 2001.

8. Program registration paper №2005611492. Decision making in risk state // Mashkina I.V., Vakaeva E.V., Verzakov A.V.