computing@tanet.edu.te.ua
www.tanet.edu.te.ua/computing

ISSN 1727-6209
International Scientific
Journal of Computing

THE PROBLEMS OF INFORMATION DEFENCE IN DIAGNOSIS INTELLIGENT SYSTEMS OF MICROPROCESSOR DEVICES

Viktor Lokazyuk, **Oksana Pomorova**

Khmelnitsky National University, System Programming Department,
29016, Khmelnitsky, Kamenetski st., 112 (Ukraine), E-mail: kism@beta.tup.km.ua, haha@rp.km.ua

Abstract: *The method for protection of diagnosis intelligent system of microprocessor devices is represented in the paper. This method based on background authentication of the user in the process of keyboarding. The user's keystroke dynamics characteristics are the means of authentication. For realization of the user authentication method uses the artificial neural networks of ART2 architecture.*

Keywords: *microprocessor devices diagnosis system, authentication, artificial neural networks, keystroke dynamics*

1. INTRODUCTION

Microprocessor devices play the leading role in the modern technical systems. They are used in computer systems, household appliances, medical facilities, industrial and military control systems. The importance of solution of the microprocessor devices (MD) diagnosis task is permanently increasing. It creates a need to design the microprocessor devices diagnosis systems (MD DS) and regular escalates their possibilities.

Modern microprocessor devices diagnosis systems are intelligent. They are based on using of the artificial intelligence components and included in its structure a knowledge base, which accumulated the great volumes of the confidential information [1,2]. If we estimate the cost of obtaining such information for corporations, which are developing MD DS, we will see that only filling a knowledge base by the qualitative expert information costs tens, and even hundred thousand dollars. For example, the cost of one production rule is estimated about $100 [3], and the full-fledged expert system of microprocessor devices diagnosis contains a thousands rules.

And so, one of priority and important task at an operational phase of microprocessor devices diagnosis intelligent system (MD DIS) is securing of the expert information.

2. KNOWN SOLUTIONS REVIEW

Protection of modern software should meet the requirements, which are formulated for appropriate classes of safety in Trusted Computer System Evaluation Criteria, European ITSEC or Common Criteria for Information Technology Security Evaluation (CCITSE) [4, 5]. The basic components of the information protection models are protection means against unauthorized access to the information and resources that guarantee information integrity and provide access to the information.

Models of discretionary and mandatory access control are using widely in order to defend modern software products against unauthorized access. They provide to access division between subjects and data objects [6]. This models have a number of defects; and so, there is a possibility to have access to theirs protection systems. According to Hoffman's theorem, for arbitrary system of discretionary protection and a joint right of access to information resources, there is no possibility to prove whether assigned configuration of an information system is secure [7].

One of the modern effective means of the information protection is biometrics. Biometric authentication is a way of the person authentication by unique biometric characteristics, which are inherent to only this person. Biometric characteristics, such as genetic parameters of the subject: a fingerprints, hand geometry, voice, the iris of the eye or the retina and his individual behavioral features: handwriting, the signature, keystroke dynamics are of special interest for the use in the field of computer technologies [8].

One of main drawbacks of biometric systems that hindered with their wide implementation is the requirement for presence of special authentication hardware - scanners of the face and hand, fingerprint, etc. Special hardware is not necessary only for authentication of a person by keystroke dynamics.

Systems of authentication by keystroke dynamics are based on the procedure that while entering a key phrase computer enables to keep a record a user's parameters, such as the speed of entering of the information, the time of entering words and separate symbols, the time intervals between pressed and released of separate keys, etc. The user's authentication realized on the base of analyzes of these parameters. With this, the reliability index of this way of authentication is high enough – its level EER is 3-4 % [9].

The systems of authentication by keystroke dynamics are divided into two groups in accordance with their function: systems for authentication of the user, which wants to get access to software and monitoring systems user's software operations. Systems of the second group also make possibility to organize the hidden authentication.

Under increases the requirements to a class of software security, the models of access control, which are used in it simultaneously, also increases in number. Standard practice is integration of the models of discretionary and mandatory access control. Sometimes theirs are added biometrics authentication means. Result of integration of several base protection models is not only in integration of advantages of these models, but also in integration of their defects and weak points.

It is necessary to take into account that the formal models of protection operate only within the bounds of algorithms, incorporated in them and are not intelligent. They can inadequately react or not react in general to the changes characteristics of users interaction with software. Only a highly skilled software manager can compensate a lack of intelligence of this protection models. Only manufacturers can eliminate problems that arise in means of protection (presence of errors which appeared at a design stage) and can adapt them to new requirements by adding new functions and creating new versions of software products.

For the majority existing intelligent systems, for example, expert systems or decision support systems, methods of information protection are built on the formal models. Its methods built without taking into account the qualities of intelligent systems and it reduced the efficiency of protection [10].

3. MD DIS QUALITIES

In a number of cases the software intelligent systems of microprocessor devices diagnosis have the qualities that distinguish them from traditional software.

Such features are:

- possibility to obtain new knowledge on the basis of the information which contains in a knowledge base, for example creations "fast" production rules. Entering of the incorrect information in the knowledge base leads to creation of erroneous rules, and as consequence we make up the erroneous logical inference at problem solving;
- possibility to use the information from a knowledge base for training artificial neural networks which function in consisting of MD DIS. Using of the incorrect information leads to output neural nets the distorted or erroneous results;
- possibility to use the previous tasks solution results for generation of new rules of the inference and correction of problem solving algorithms in the further. Entering by the user of wittingly incorrect information about results of problem solving leads to creation of erroneous rules and algorithms;
- possibility to obtain the detailed information about the diagnosing object only by exhaustive search of a knowledge base during maintenance of system. Separately taken files of a knowledge base are low-comprehension.

Specified distinguishes make intelligent diagnosis systems more vulnerable, than usual DBMS or other software.

Modern literature does not attend enough attention to questions of intelligent systems protection by taking into account it's distinguishes. Specifically little attention pays to questions of systems protection from damage by introduce of the incorrect information in their knowledge bases. Besides, it is necessary to prevent of exhaustive search of knowledge bases during operation and others users incorrect actions that lead intelligent systems to the state when they will be unable to operate.

4. PROBLEM DEFINITION

The purpose of our research is improvements of characteristics of federated MD DIS protection systems at the expense of usage of the user biometric authentication resources. Authentication should be carried out not only at the moment of the user login in system, but also during all operate session with

system. For this purpose it is necessary to research characteristics of the user keystroke dynamics and to use them for carrying out of the hidden authentication. It is necessary to provide possibility of the adaptation of a protection system to changes of the user biometric characteristics. Process of the user authentication is necessary to make intelligent at the expense of usage of artificial neural networks.

5. CHARACTERISTICS OF KEYSTROKE DYNAMICS

There are following parameters using in the systems of user authentication by keystroke dynamics: the symbol input speed, the time between pressing the keys, the time dependence between pressing some of the keys, the characteristics using of "hot" and soft keys, and so on.

The MD DIS protection system used following characteristics of keystroke dynamics:

- time between pressing keys:

$$T_k^p = t_{i+1}^p - t_i^p, \qquad (1)$$

where $i = \overline{1, n-1}$, $k = \overline{1, n-1}$, n - quantity of presses keys;

- time between releasing keys:

$$T_k^r = t_{i+1}^r - t_i^r \qquad (2)$$

where $i = \overline{1, n-1}$, $k = \overline{1, n-1}$, n - quantity of releases keys;

- average rate of typing the text:

$$T^m = (\sum_{k=1}^{n-1} T_k^p + \sum_{k=1}^{n-1} T_k^r)/(2k) \qquad (3).$$

The special software for recording of users keystroke dynamics characteristics has been developed during our research.

In fig.1 are represented diagrams where were fixed periods between presses keys, between releases keys and an average rate of typing the text. In all figures on axis X indicated is values k, on an axis Y – the time (milliseconds).

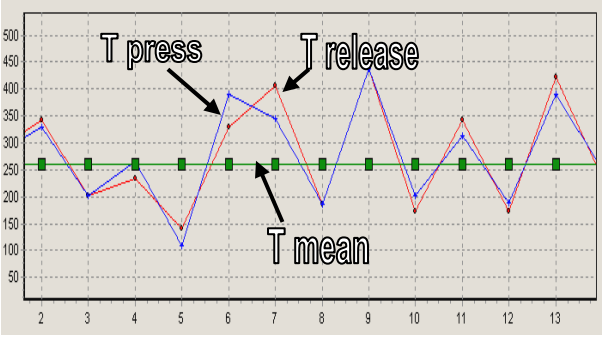


Fig1. Characteristics of the user keystroke dynamics.

Presence of essential distinctions in keystroke dynamics of different users was observed in the process of experiments.

In fig.2 is represented the example of fixing of the user keystroke dynamics, where he typed the same text 4 times.

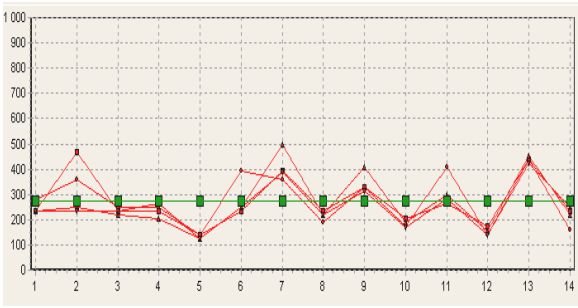
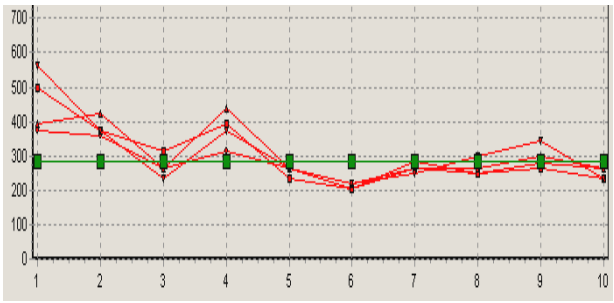


Fig.2. Diagram of times between pressing keys, where user typed the same text 4 times.

Examples of keystroke dynamics diagrams of two different users are represented in the fig.3a and 3b. As we see, the keystroke dynamics of different users have essential distinctions.



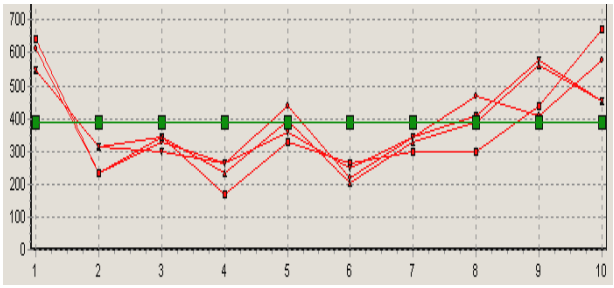


Fig 3a, 3b. The keystroke dynamics diagrams of two different users

Fixing of periods between releases keys has given similar results. The average rate of typing for different users also essentially differed even after reusable trainings (200-400 milliseconds).

Cases of perfect coincidence between diagrams of three characteristics for different users it has not been detected. Consequently, each user has his keyboard handwriting. At attempt of keyboard handwriting falsification of the most essential distinctions were observed in a graphics of time between releases of keys and a graphics of typing average rate.

At a reusable typing of the same text (20-50 times) small size (5-20 characters) characteristics of the user keystroke dynamics in the beginning slowly vary, and farther become more stable. That is, the user studies, he adapts to type fragments of the text in the way most convenient for him. In fig. 4a, 4b we presented user keystroke dynamics when he typed the text 4 times before and after learning.

The most essential deviations in samples of the user keystroke dynamics were observed in cases when the user distracted from type, hastened or was nervous. For revealing of the user's keystroke dynamics features the minimum length of the typed text should not be smaller 6-7 characters. At typing the big fragments of the text (it is more than 15 characters) the user can distract, that leads to deviation his keystroke dynamics characteristics.

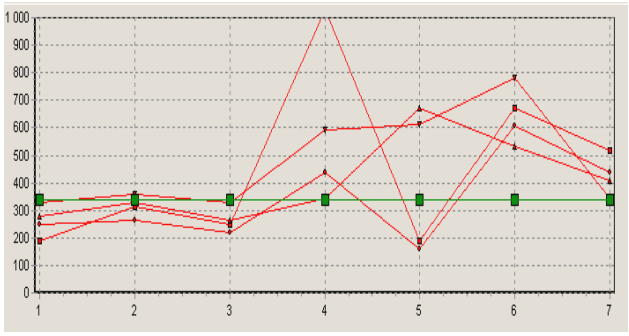


Fig. 4a. The user keystroke dynamics before learning

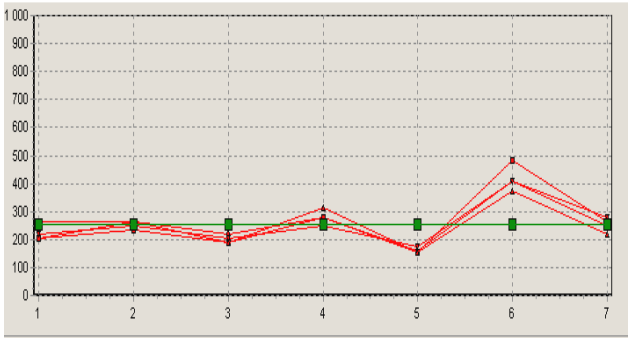


Fig. 4b. The user keystroke dynamics after learning

In the authors opinion, for the authentication of the user on the basis of keystroke dynamics is necessary to use fragments of the text with length of 6-15 characters. Thus, for improvement of the reliability characteristics of the authentication - FRR and FAR (False Rejection Rate and False Acceptance Rate), the same fragments, which the user "has learned" to type, are necessary to use.

The user authentication by keystroke dynamics has a number of advantages comparing to another biometric methods:

- does not require special hardware;
- to make a minimum of requirements for the user;
- it is used in the background, it is imperceptible for the user;
- it can be used with other protection methods.

There are also a number of problems if to use this method of authentication, in particular:

- keystroke dynamics varies from time to time (the user learning);
- reliability of authentication depends on the size of the printed text;
- keystroke dynamics of the user frequently depends on his psychological state;
- majority of existing systems require presence of a standard sample of the key phrase and the sample that is researched for revealing specific features of keystroke dynamics. The presence of standard samples of keystroke dynamics in computer enables to receive them and to use for violation of the security of the system.

Researches of the selected keystroke dynamics characteristics are showing that they complex using would be quite enough for user authentication if will be solved noted above problem.

6. INTELLECTUALIZATION OF THE USER AUTHENTICATION PROCES

Taking into account the features of modern MD DIS and the problems of the keystroke dynamics authentication the task of improvement of the characteristics of integral protection resources by means of using of the artificial intelligence components is very important. For implementation of the user authentication has been elected the artificial neural network of ART2 architecture (fig.5). ART2 is designed to process real-valued patterns [11].

The ART2 architecture is composed of two groups of neurons referred to as the F1 layer and F2 layer. The F1 layer is further divided into input and interface neurons. The F1(a) input neurons process inputs from the environment. The F1(b) interface neurons combine inputs from the F1 input neurons and the F2 layer neurons. The F2 layer is a competitive layer where the neurons serve as cluster prototypes. There are “bottom-up” connections between nodes in F1(b) and F2. There are also “top-down” connections from F2 to F1(b). A reset mechanism along with a vigilance parameter determines whether a F2 node learns a pattern. The F1 units do not change during the resonance phase so the equilibrium weights can be determined exactly so the iterative solution to the differential equations is not required.

Network ART2 realize the clusterization algorithm, that similar to algorithm of "the sequential leader". According to this algorithm, the

first input vector is considered as a sample of the first cluster. The following input vector is compared to a sample of the first cluster. The input vector will belong to the first cluster if the distance between it and a sample of the first cluster will be smaller than threshold that was indicated by the developer.

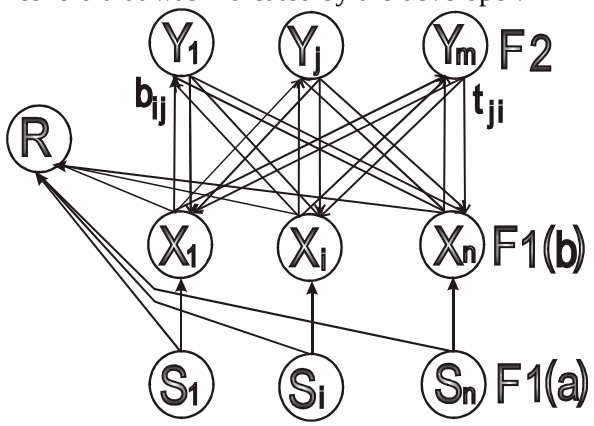


Fig. 5. The ART2 architecture

Otherwise, for the second input vector the separate cluster will be created. This process repeats for all following input vectors. Thus, the number of clusters grows eventually and depends from value of a threshold and from distance that using for comparison entry signals and samples of classes. Limitations of the neurons quantity in an output layer are defined only by possibilities of the computer system and the wishes suggested by developers. The special parameter of the control (vigilance) allows regulate accuracy of images coincidence.

In our case the vectors, composed from characteristics of the user keystroke dynamics, are giving to the network as an input layer: $S_i = (T_k{}^p, T_k{}^r, T^m)$, where $k = \overline{1, n-1}$, n - the greatest possible quantity of pressing or releasing keys (maximum length of an input fragment of the text), i - number of a fragment, $i = \overline{1, p}$, p - quantity of fragments. If the fragment of the text has length smaller n, then empty positions of an input vector will initialize by zero values. The fragment of the text which is typed by the user at first, is a sample for creation of an appropriate output cluster.

On an output the network forms a vector $Y = (y_1, y_2, ..., y_p)$, which have only one neuron with maximum value. This neuron is signaling about reference of an input vector of the keystroke dynamics characteristics to one of clusters. That is authentication of the user by this fragment has passed successfully. The quantity of output vector elements should not exceed quantity of used fragments of the text. If during recognition of the input fragment there is a need to create additional element of the output vector, than authentication will be unsuccessful. Quantity of the text fragments which will be used for authentication and accuracy of coincidence of keystroke dynamics samples are defined by the MD DIS developer.

Usage of ART2 neural nets helps to organize process of authentication more effectively and has a number of advantages than usage of neural networks of other architectures [12, 13]:

- ART2 network studies "without the teacher", the sample of an educational vector is inputing by the user of appropriate fragment of the text at first;
- the developer can be in control of the accuracy of the input vectors coincidence with samples which already are in the network;
- if presence a changes in the user keystroke dynamics characteristics (the user learning by experience of type) the network will adapt to them;
- the quantity of outputs ART2 network can be increased, that permit of necessity to increase quantity of the text samples for authentication;
- using of a ART2 network does not need storage in a knowledge base of standard samples of the user keystroke dynamics that prevents their abducting;
- the ART2 network admits using for authentification of several separate fragments of the text, that in the complex enables to raise efficiency of process of authentication and to reduce requirements to the user;
- for each user there is the separate copy of the ART2 network. If the user is deleted from system, that only his variant of the network will be deleted, retraining of other users networks is not necessary.

7. METHOD OF MD DIS PROTECTION

The user's interface of diagnosis intelligent systems is organized in the dialog mode, as well as in all modern software products. The user enters the information in appropriate fields of screen forms and receives the necessary information in other fields on the screen. The user have to ask question to MD DIS for getting the information from the knowledge base, that is he have to type. From this it follows that we can to organize monitoring of keystroke dynamics in a background, that is imperceptible for the user. The protection system ensure the authentication of the user at logon and the control of his keystroke dynamics over all operating time according to the algorithm presents in fig. 6.

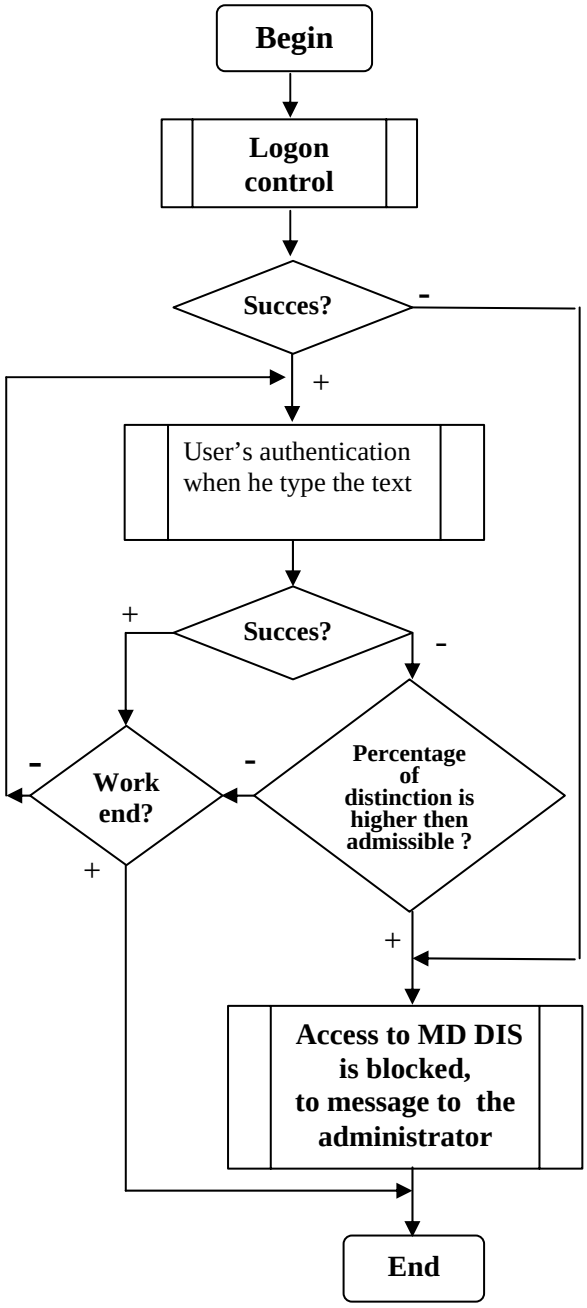


Fig. 6. The algorithm of operation of the MD DIS protection system

Authentication of the user at logon is based on the login and the password. The user keystroke dynamics are also inspected during authentication. User is admitted to operation with system in a case of coincidence all his data and characteristics. Monitoring of the user keystroke dynamics on the separate fragments of the text is carried out during of all session. If presence essential differences in the user keystroke dynamics then protection system will be locked and the alarm will be transferred to manager or safety expert.

Generally process of the user authentication consist of two stages. A preliminary stage:

- it is necessary during MD DIS engineering to provide even one field on each screen form for typing information by user. The typed in this field text will be used for authentication. The text should not vary. First of all there are login, password and also the information about types of devices, tags of faults, etc.;
- the user should typed some times keywords and phrases before beginning operation with MD DIS. In further they will be entered into the fields of forms and used for authentication. System will receive the typical samples of the user keystroke dynamics at the first filling fields of dialogue forms.

Main part:

- the protection system generates for the user new copy of ART2 network at the first registration in MD DIS;
- the monitoring program in the typing proces registers values of time between pressing the keys, time between release the keys and the average rate of typing the text, forms a vector of parameters of keystroke dynamics and submits theirs on an input of the network;
- the vector of keystroke dynamics parameters, which received at the first filling of the form fields, is using for learning;
- on the output the neural net forms vector, where only one neuron by maximum value gives the signal about successful user authentication, thus, each screen form receives the number of a neuron of the output vector;
- form that already was filled earlier, has number of the neuron that received maximum value. If the form after felling do not receive the response from respective neuron, then this form will be noticed by a special marker of "infringer";
- after each filling of the form fields, the protection system mades a calculation of the percentage relation between quantity of the forms with a marker of "infringer" and total quantity of the filled forms. If percent of differences exceeds the admitted percent then will be sent message to the administrator and MD DIS access will be blocked;
- the control of keystroke dynamics is more hard at introduction of the password and less hard at filling forms during operation.

Usage of the offered method of MD DIS protection does not demand the big expenses of

computing resources, provides possibility to adapt the protection system to changes of the user keystroke dynamics, does not demand saving in a knowledge base of the user keystroke dynamics samples, that prevent their theft. Simultaneously there is a possibility to installate the requirements level for protection and a possibility to obtain keystroke dynamics of the infringer and to use their for his identification in the further. In aggregate with other protection models the proposed method enables to raise reliability and efficiency of the information protection in the MD DIS knowledge base.

8. CONCLUSIONS

The analysis of MD DIS characteristics show as that it have a number of features which do it more vulnerable, than usual software products. For this reason formal models of access control cannot provide effective protection of MD DIS.

MD DIS protection was improved by means of the biometric methods, namely authentication based on characteristics of users keystroke dynamics. During learning characteristics of keystroke dynamics has been detected, that even small samples of typed text (6-15 characters) allow to distinguish the keystroke dynamics. Based on it the method of MD DIS protection has been developed.

The process of authentication has been realized on base of the artificial neural network ART2 architecture, it allowed improve upon effectiveness of the process.

The using of the protection method, suggested by authors, in the complex with methods of discretionary and mandatory access control enables to improve the protection of MD DIS.

9. REFERENCES

[1] V.Lokazyuk. The problem of control and diagnosis contemporary microprocessor devices and systems. Measuring and computing devices in technological processes. 2 (2000). p.10-17

[2] V.Lokazyuk, O.Pomorova, A.Dominov. Intellectual diagnosis of microprocessor devices and systems."Taki spravi". Kyiv, 2001. p.286.

[3] E. Popov. Expert systems: Solution of unformalized tasks on dialogue from the computer. Science. Moscow, 1992. p.288.

[4] Trusted Computer System Evaluation Criteria (TCSEC), US Do 5200.28-STD, 1983.

[5] Information Technology Securite Evaluation Criteria. Harmonised Criteria of Franse – Germany – the Netherlands – the United Kindom. Department of Trade and Industry, London, 1991.

[6] A.Grusho, E. Timonina. Theoretical bases of the information protection. Publishing house of agency " Yahtsmen". Moscow, 1996. p. 192.

[7] Scherbakov. Learning in the theory and practice of computer safety. Publishing Molgacheva, 2001. p. 352.

[8] F.Monrose, Aviel D. Rubin. Keystroke Dynamics as a Biometric for Authentication. Future Generation Computer Systems. (March, 2000) p. 15.

[9] A.Gince. Biometric technology in monitoring systems of access control. Systems of safety 46 (2002). P. 46-49.

[10] V. Tarasenko, A. Mykhailyk, D.Vorobei. Problem of expert systems information safety. Materials of Anniversary scientific and technical conference " Legal, normative and metrological supports of a protection system of the information in Ukraine", Kyiv, 1998. - pp. 62-64

[11] G.Carpenter, S.Grossberg. ART2: Seif-organization of stable category recognition codes for analog input patterns. Applied Optics 26 (23): P.4919-4930, 1987.

[12] M.S.Obaidat, D.T. Macchairolo. A Multilayer Neural Network System for Computer Access Security. IEEE Transactions on Systems, Man and Cybernetics, Vol.24, No.5, P.806-813, 1994.

[13] R.Joyce, G.Gupta. Identity Authentication Based on Keystroke Latencies. Communications of ACM. Vol. 33, No. 2, P.168-176, 1990.

Victor Lokazyuk *was born in 1944 in Ukraine.*
He graduated the physics faculty of Kamenez-Podolsk Pedagogical Institute in 1970.
From 1981 he worked as the engineer at an instrument-making factory and engaged the scientific researches.
In 1990 he received PhD degree on a speciality "The elements and devices of computer engineering and control systems" in the Kiev Institute of Automatics.
In 1995 he received doctor science degree on a speciality "The computing engine, systems and networks" in the Vinnitsa National Polytechnical University.
At present he work as head of System Programming Department of the Khmelnitsky National University.
He is a member of the Iinternational Academy of Computer Sciences and Systems and the member of International Academy of Information.

The area of the scientific interests: an artificial intellect, computer networks, microprocessor diagnosis systems, artificial neural networks, systems simulation.
He has published more than 150 scientific works, including 6 books.

***Oksana Pomorova** was born in 1969 in Ukraine.*
In 1992 she graduated faculty of cybernetics of the T.Shevchenko National University in Kiev on a speciality applied mathematics.
She received PhD degree in 2002 in the Kiev Institute of Automatics on a speciality "Control-automation system and progressive information technologies".
She work at the reader on Department of System Programming of Khmelnitsky National University.
The area of the scientific interests: an artificial intellect, digital devices diagnosis systems , artificial neural networks, expert systems, multiagent systems.
She is published more than 30 scientific papers, including 2 chapters of book. She Is IEEE member.