Y. V. Baryshev, Cand. of Sc.; V. A. Kaplun; K. V. Neuimina

DISCRETIONAL MODEL AND METHOD OF DISTRIBUTED INFORMATION RESOURCES ACCESS CONTROL

The paper presents an analysis of access control models. The access control model, which, exploiting the hashing process peculiarities, allows to limit the number of workstations from which the user is allowed to get remote access to information resources, is proposed. The choice of authentication factors of a workstation and user has been substantiated, which allowed to develop the method that implements this access control model.

Key words: *authentication, hashing, authentication factors, access control model, workstation features.*

Introduction

Due to the presence of many security violation possible sources for information, which is processed by computational means such as personnel, intruders, failures, etc. [1], the task of this information security ensuring without significant loss of the performance rate of this information processing arises. One of the protection methods used for the task solution is computer system users control of the access to available information resources in the system [1, 2].

This approach is quite sufficient under conditions of information processing by workstations of an enterprise, where employees of the information security service have the opportunity to create secure conditions for this information processing. However, along with the development of mobile computing devices and the Internet of Things (IoT) legal users gained the ability to process data outside the enterprise, in conditions those do not bolster maintaining of the privacy of the information being processed. Therefore, the important task of such access control model and a method developing, which prevent the confidential data processing using unprotected computational means, arose.

The aim of this research is to improve information, which is provided to users by remote information resources, privacy protection.

The following tasks are to be solved to reach the aim:

– analysis of known access control models;

– development of the access control model, which provides the usage of secure computational means to access confidential information;

– substantiation of users authentication factors choice for this model implementation;

– development of rights granting method to access distributed information resources based on the developed model.

Analysis of known access control models

Access control systems perform management of information system subjects accessing objects of this system. At the heart of any such system lies the access control model. Known access control models are divided into discretionary, mandate and role-based models [1, 3, 4].

A discretionary access control model provides that subjects access rights for each certain object of the system may be limited on the basis of some external in relation to the system rule [1, 3, 5].

The principal element of the discretionary access control is the access matrix. The access matrix is the matrix D of the size $|S|\times|O|$ (where S – the set of information system subjects and O – the set of information system objects). The element of the access matrix $D[i, j]\subseteq R$ determines the access rules for the i^{th} subject for the j^{th} object (R – the set of possible access rights) [3-5].

Harrison-Ruzzo-Ullman model (HRU model) is the another instance of the discretionary access control model. The HRU model provides representing of the access control system by a finite automaton, which operates according to defined transition rules [3, 5].

The Take-Grant model is also a model of discretionary access control and provides an opportunity to analyze and verify the information system security state. The access graph and its transformations are used as principal elements in the Take-Grant model. The main task of the model is to determine the ability of the system subject to get accessing rights to the object in the state described by the access graph. Formally, the description of the Take-Grant model looks in the following way [3, 5, 6]:

– a set of objects – O, where $o_j \in O$, $O = \{o_1, o_2, ..., o_j\}$, $j \in N$;

– a set of subjects – S, where $s_i \in S$, $S = \{s_1, s_2, ..., s_i\}$, $i \in N$;

– a set of active subjects – $S \subseteq O$;

– a set of access rights R, where $r_n \in R$, $R = \{r_1, r_2, ..., r_n\} \cup \{t, g\}$, where $t(take)$ is the right to take access rights, $g(grant)$ is the right to grant access rights.

Using this model, it is possible to predict states of the information system depending on the access control [5].

The advantage of discretionary access control models is the demonstrativeness of access control system implementation, generality and high level of flexibility. Nevertheless, the principal disadvantage is the necessity of "manual" administration for these systems, and hence increasing of the human factor impact on the safety of the information protection system, which uses such access control model.

The mandate model combines the protection and limitation of the rights that are used toward computer processes, data and system devices, and is designed to prevent their unwanted usage [1-3, 5, 7].

Today, the most common representative of mandate access control models is the Bell-LaPadula model [3, 5, 8]. This model ensures that a subject can only view information only in case of having sufficient authority and any subject other than the administrator cannot in any way transfer data from an object with a higher privacy level to an object with a lower privacy level. In the Bell-LaPadula model, the objects available in the information system are classified according to secrecy labels and subjects operating in this system are classified according to the classification levels (mandates). Furthermore, it is necessary to ensure the implementation of following rules [3, 5]:

– the subject of certain classification level is not allowed to perform the "read" operation for objects of a higher secrecy level (the "no read up" rule);

– the subject of certain classification level is not allowed to perform a "write" operation for objects of a lower secrecy level (the "no write down" rule).

If a user with a high-level mandate writes some data to an object with a lower secrecy level, they would become available to a subject with a lower classification level than it is allowed by the security policy.

The main disadvantage of this model is the high complexity of its implementation by programming means, which causes increased requirements to the resources of the computer system while being implemented.

Role-based access control (RBAC) provides access control both on the basis of access rights matrix for roles and through rules that regulates the roles assignment to users [3, 4, 8]. In this model, the computer system is represented by an array of following sets [3, 5, 7]: a set of users *U*; the set of roles *R*; a set of authority *P*; a set of sessions *C* of user interaction with the system.

The set of authority P in general is formed by special mechanisms that combine access operations and accessed objects, for instance, requests for data processing in database management systems.

The advantage of such model is that it requires less time for being administrated. Nevertheless, this advantage is obtained due to access control model flexibility reducing comparatively to the discretionary one. Nonetheless, the role-based model is more flexible than the mandate one, respectively it has a higher potential for adaptation to the needs of certain information system. Thus, the role-based model from the practical point of view is appropriate to be considered as a compromise one between mandate and discretionary. This leads to widespread usage of the role-based model, in particular, in operating systems and database management systems [3 – 5, 9].

Thus, from the analysis of the access control models, it follows that they have one common disadvantage: they do not provide a limitation of the workstations which could be utilized by the user in order to gain access. The latter disadvantage becomes significant in systems, which provides access to distributed information resources, in particular, file servers and cloud services. When managing access to distributed information resources to achieve the goal of this research, it is necessary that the enterprise access control system of the access should be as flexible as possible. That is why within the borders of this research it is required to improve the discretionary access control models.

Access control model with workstation binding

An approach to the user authentication that takes into account the workstations from which this user authentication is initiated are to be applied to the access control model development. Notably, the discretionary models, based on access matrix after implemention of proposed approach will change as follows: instead of a two-dimensional matrix in the original approach, a set of three-dimensional matrix is used $|S|\times|O|\times|PC|$, where PC – parameters of workstation (which is used by the subject for access obtaining). Such model of the access control requires a special method of users authentication, therefore it is proposed for its implementation to use the approach of organization of users secure access to network services, considered in the works [10 – 12]. In Fig. 1 authorization scheme of a user and a workstation is presented [10].

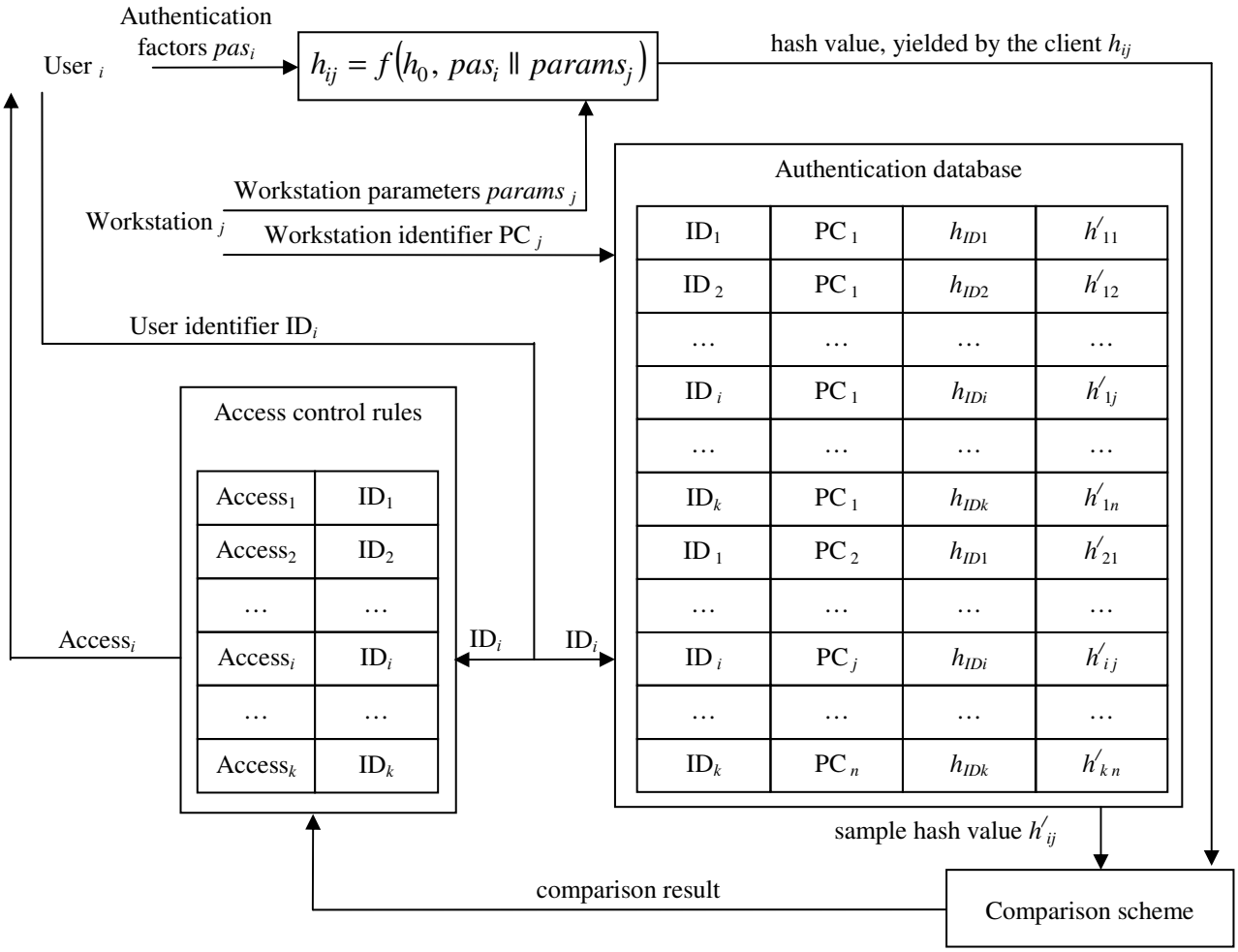

Fig. 1. User authentication scheme

The peculiarity of user authorization in case of such access control model usage is that the iterative hash function is to be used for authentication data protection. For instance, such designs include the Merkle-Damgaard constructions, HAIFA and $MPH_q(2;1;1;1;0)$ [13, 14]. Merkle-Damgaard construction is considered to be classicaal one and is formalized in the following way [13]:

$$h_i = f(m_i, h_{i-1}), \tag{1}$$

where h_i – the intermediate hash value, yielded at the i^{th} step; m_i – the i^{th} data block; $f(\cdot)$ – the reduction function, which provides fixed length of the output value.

HAIFA construction is an improved version of the Merkle-Damgaard construction, that allows to enhance cryptographic infeasibility against generic attacks by usage of computation number [13]:

$$h_i = f(m_i, h_{i-1}, \#bits_i, r), \tag{2}$$

where $\#bits_i$ – the number of already hashed message bits; r – the pseudorandom number (cryptographic salt).

As the additional arguments in the reduction function in the construction (2) causing of increased workload intensity for the server, which performs authentication, as compared with the construction (1), it is proposed to use hash functions, based on multipiped hash constructions $MPH_q(2;1;1;1;0)$ [14]:

$$\begin{cases} h_i^{(1)} = f^{(1)}\left(h_{i-1}^{(1)}, h_{i-1}^{(2)}, m_i, r_i^{(1)}, \#bits_i\right); \\ h_i^{(2)} = f^{(2)}\left(h_{i-1}^{(2)}, h_{i-1}^{(3)}, m_i, r_i^{(2)}, \#bits_i\right); \\ \ldots \\ h_i^{(q)} = f^{(q)}\left(h_{i-1}^{(q)}, h_{i-1}^{(1)}, m_i, r_i^{(q)}, \#bits_i\right). \end{cases} \quad (3)$$

The basic feature of the above-mentioned construction is that for the $(i+1)^{\text{th}}$ data block hashing it is sufficient to know intermediate hash value h_i regardless of the way by which it was yielded. The latter makes it possible to store on the server side the i^{th} user result of the authentication factors parameters hashing h_{IDi} and not the actual values of these parameters . This is provided by carrying out of the following equality:

$$f\left(h_0, pas_i \parallel params_j\right) = f\left(f\left(h_0, pas_i\right), params_j\right), \quad (4)$$

where $h_{IDi} = f\left(h_0, pas_i\right)$.

The features, analogues to the latter (4) will provide the abovementioned hash constructions in case of the message length further increasing if the increasing is multiple of data block m_i length.

In order to reduce the server workload, it is proposed to perform the workstation parameters hashing process of hedging immediately after adding the respective rule to the authentication database and storing this value h_{ij} at the database as it presented in Fig. 1. Due to the hashing feature, that is provided by using of the constructions (1) – (3), both the user and the workstation are authenticated before granting access to the information resource.

In this way, the properties of the subject are separated, by which it is authenticated by the factors that authenticate the user and the factors that authenticate its computing means. To develop the method, you need to identify potential authentication factors.

Therefore, the features of the subject by which it is authenticated into factors, that authenticate the user and the factors that authenticate its computing means are separated. To develop the method, it is needed to define potential authentication factors.

Substantiating of authentication factors choice

Authentication methods can be conventialy divided into single-factor and multi-factor ones [1, 2, 4, 15], where the factors are meant the subject property which is used for authentication performance. Therefore, single-factor factors are simpler to implement, nonetheless, they provide worse level of security, due to the less complexity of their forging.

Password authentication is the most wide-spread, simple and common method in which the user's knowledge of certain secret word – the password [1, 4, 5, 15] – is used as an authentication factor. Using of this authentication factor does not put forward additional requirements for hardware and software of information resources, but it often turns out to be instable due to the significant human factor impact.

There are known authentication methods that include using of unique devices that provide firmer protection than password authentication. Such factors are divided into two groups: passive ones, which only contain authentication information and transfer it to the information system on demand, and active ones which have certain computing resources and are involved in the implementation of cryptographic authentication protocols [1, 4, 15].

Authentication by means of unique devices has a number of drawbacks: the device may be stolen from the user, additional hardware/software is needed for workstations, emulation of factor's impact is possible.

Biometric authentication methods are based on the using of equipment for measuring and

comparing with the sample of certain individual features of the user [4, 15]. Such equipment allows to identify the owner using specific biometric feature with high accuracy and it is more difficult to forge such parameters than abovementioned ones [4, 15]. A significant drawback of biometric authentication is the need for additional equipment for each workstation for biometric characteristics retrieving.

Since the purpose of this research is to improve the information privacy protection, it is proposed to use multi-factor user authentication, based on his knowledge of the password and the possession of a passive unique device (flash drive). The first factor reduces the risk of unauthorized access to information as a result of stolen media, and the latter reduces the human factor impact.

In order to authenticate a workstation, it is proposed to use a combination of several unique features of this station. Workstation's authentication factors use the following features of the computer system [15]: the properties of the software (system files, operating system version, creation date and checksum of BIOS, features of the file system), hardware properties (performance, serial numbers of key hardware components, additional peripheral equipment availability). For this research, the serial number of the hard drive, the date of creation and the checksum of the BIOS are chosen. The choice of these properties is due to their relative stability and the complexity of their values prediction by an intruder.

In certain cases, to give uniqueness to each of authentication sessions, it is proposed to add cryptographic salt to the authentication factors – pseudorandom numbers [4, 13, 14]. This measure will prevent the attack of hashed authentication factors retransmitting and hide from intruders who have the ability to analyze traffic, both the user's authentication data and the workstation which he operates.

Method of access rights differentiation to distributed information resources

To implement the method, the software structure of the client-server architecture is proposed. In Fig. 2 the structure of the client application for the method implementation is presented.

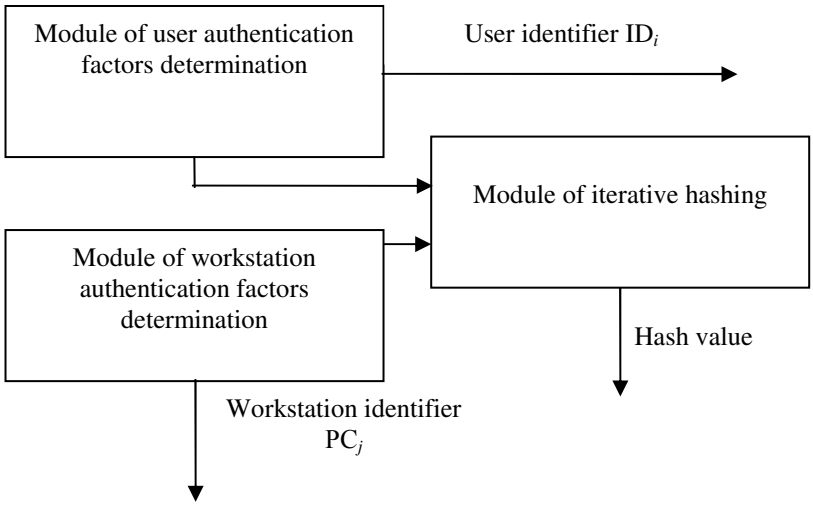

Fig. 2. The structure of client's application for the method implementation

According to the access rights differentiation method on the client side the following actions are to be performed:

– using the module of user authentication factors determining he inputs his credentials and determines the parameters of the authorization factors (for instance, the password and the parameters of the flash drive);

– concurrently, defining of the workstation authentication factors parameters are implemented (for the purposes of this research – the serial number of the hard drive, the date of creation and the

checksum of BIOS);

– using the module of iterative hashing on the client side, hash value of the concatenation result of the authentication factors parameters of user and workstation, as well as cryptographic salt, is yielded:

$$h_{ij} = f\left(h_0,\ pas_i \parallel params_j \parallel r\right); \tag{5}$$

– the obtained hashing result, workstation identifier and user identifier are sent to the server side.

Fig. 3 shows the structure of server's application that interacts with the client, which is shown in fig. 2

As is can be seen from Fig. 3 the following steps are to be implemented on the server side:

– according to user and workstation identifiers values received from client the hash values of user authentication factors h_i and workstation parameters are determined;

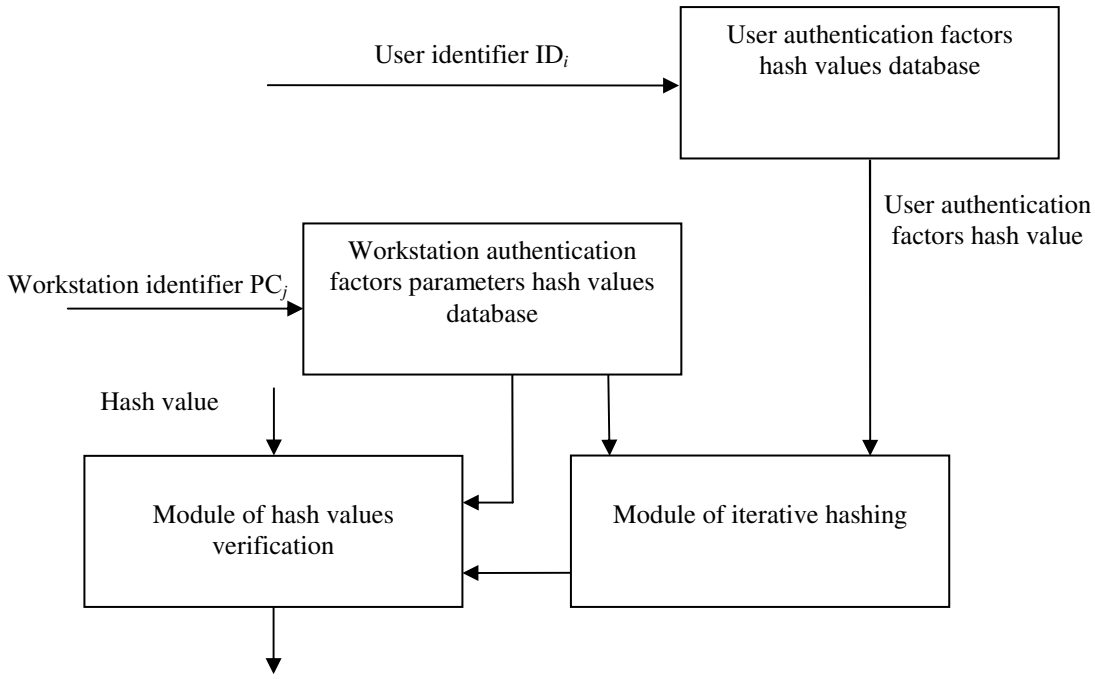

Fig. 3. The structure of server's application for the method implementation

– hashing of workstation parameters and cryptographic salt are performed:

$$h'_{ij} = f\left(h_i,\ params_j \parallel r\right); \tag{6}$$

– by comparing the computed and received hash values the decision concerning user access allowance or denial is drawn.

The proposed method may be modified by pre-computing hash values for all combinations {user; workstation}. This will reduce the server's workload, but it makes using of cryptographic salt inapt, which will reduce the infeasibility of the method for breaking.

Conclusions

The performed analysis of access rights differentiation models revealed their aiming at user authentication. Nonetheless, these models do not take into account the workstation from which the authorized user tries to access. With the development of mobile computing and IoT, this drawback causes the vulnerability of the processed information, because the guarantees that the workstation on the client side has an adequate information security system disappear. To overcome this drawback, the access rights differentiation model is proposed that provides both user limitations and

restrictions on workstations from which the user can gain information. Thus, it is proposed to limit the list of workstations for each user separately. Such model not only allows to provide the appropriate level of information protection during its processing by the users, but also reduces the vulnerability of the system to insider attacks, since each employee is bound to his workplace, that reduces his ability of invisible attack implementation.

The factors of users and workstation authorization for this model implementation are proposed. The structure of access control means has been developed, that enables to propose a method that implements the access rights differentiation according to the model. The peculiarity of the method is using of iterative hashing, which allows, without hash keys and user authentication factors on the server side storing, perform simultaneous verification of both users and workstations authentication.

REFERENCES

1. Luzhetskiy V. A. Fundamentals of information security : manual / V. A. Luzhetskiy, A. D. Kozhukhivskiy, O. P. Voitovych. – Vinnytsia: VNTU, 2013. – 221 p. (Ukr).

2. Maliuk A. A. Information security:conceptual and metrological fundamentals of information security : manual / A. A. Maliuk. – M. : Hot line-Telecom, 2004. – 280 p. (Rus).

3. Devianin P. N. Models of computer systems security / P. N. Devianin. – M. : Publishing centre "Academy", 2005. – 144 p. (Rus).

4. Authentification. Theory and practice of safe access provision to information resources. Manual for graduate students / [A. A. Afanasiev, L. T. Vedeniev, A. A. Vorontsov et al.] ;Under the editorship of A. A. Shelupanov, S. L. Gruzdev, Yu. S. Nakhaev. – M. : Hot line-Telecom, 2009. – 552 p. (Rus).

5. Tsirlov V. L. Fundamentals of information security of automated control systems. Concise course / V. L. Tsirlov. – M. : Phoenix Publishing House, 2008. – 174 p. (Rus).

6. Mironova V. G. Take-Grant model realization as the presentation of access rights differentiation systems in the premises / V. G. Mironova, A. A. Shelupanov, N. T. Yugov // Reports of ТУСУР. – 2011. – № 2 (24). – P. 206 – 210. (Rus).

7. Theory and practice of information security provision / [Under the editorship of P. D. Zegzhdy]. – M : Yachtsman, 1996. – 302 p. (Rus).

8. Zhora V. V. Approach to modeling of role-based security policy / V. V. Zhora // Legal, normative and metrological provision of information security systems in Ukraine : internet journal. – 2003. – № 7. – P. 45 – 49. (Ukr).

9. Panasenko S. Methods of authentification / S. Panasenko // Banks and technologies. – 2002 – № 3. – P. 56 – 60. (Rus).

10. Baryshev Yu. V. Methods of authentification of remote users for networking services / Yu. V. Baryshev, V. A. Kaplun // Information technologies and computer engineering. – 2014. – № 2. – P. 13 – 17. (Ukr).

11. Baryshev Yu. V. Method of remote users authorization / Yu. V. Baryshev, K. V. Neuimina // Abstracts of the Fifth International Scientific Practical Conference "Methods and means of coding, protection and compression of information" Vinnytsia, 19-21 april 2016. – Vinnytsia : VNTU, 2016. – P. 65 – 67. (Ukr).

12. Baryshev Yu. V. Method and means of file server users authentification / Yu. V. Baryshev, K. I. Kryveshko // Proceedings of IV International Scientific Practical Conference "Processing of signals and non-Gaussion processes", dedicated to the memory of Professor Yu. P. Kunchenko : Abstracts. – Cherkasy : CSTU, 2013. – P. 109 – 111. (Ukr).

13. Biham E. A Framework for Iterative Hash Functions: HAIFA [Electronic resource] / Eli Biham, Orr Dunkelman // Second cryptographic hash workshop. – 2006. – 9 c. – Access mode to the resource : http://csrc.nist.gov/groups/ST/hash/documents/DUNKELMAN_NIST3.pdf.

14. Baryshev Yu. V. Methods and means of rapid multichannel data hashing in computer systems. Author's abstract of Candidate of Science (Engineering) Dissertation on specialty 05.13.05 «Computer systems and components» / Yu. V. Baryshev. – Vinnytsia : VNTU, 2012. – 20 p. (Ukr).

15. Dudatiev A. V. Software security. Part 1. Manual / A. V. Dudatiev, V. A. Kaplun, S. P. Semerenko. – Vinnytsia : VNTU, 2005. – 140 p. (Ukr).

Baryshev Yurii – Cand. Sc. (Eng.), Assist. Prof. with the Depatment of Informatin Protection , e-mail: yuriy.baryshev@gmail.com.

Kaplun Valentyna – Senior Lecturer with the Department of Information Protection.

Neiyumina Krystyna – Student with the Department of Information Protection.

Vinnytsia National Technical University.