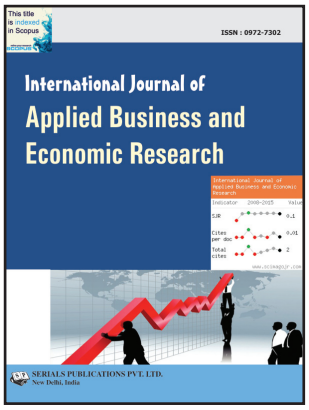

International Journal of Applied Business and Economic Research

ISSN: 0972-7302

available at http: www.serialsjournal.com

Volume 15 • Number 12 • 2017

Controlling Access to the Information and Software in a Commercial Bank

Viktor V. Erokhin[1], Galina A. Kulikova[2], Natalia V. Mudrova[3], Elena M. Shadoba[4], Viktor A. Romanov[5] and Natalia V. Podobai[6]

[1]*Bryansk State University Named after Academician I.G. Petrovsky, Bryansk, Russia. Email: erohinvv@mail.ru*

[2]*Financial University under the Government of the Russian Federation (Bryansk branch), Bryansk, Russia*

[3]*Moscow Psycho-social University in Bryansk, Bryansk, Russia*

[4]*Bryansk State Engineering-Technological University, Bryansk, Russia*

[5]*Bryansk State Agrarian University, Bryansk, Russia*

ABSTRACT

The paper sets out the main aspects and characteristics of the information protection technology in banking telecommunication systems, as well as approaches to the analysis of the information security of the banking systems. It presents a solution to the problem of reliability of banking software systems according to the criteria of the average time of the program, the availability, and reliability of computer systems. The model of access control without the restoration of the production server or a computer crash has been considered, and a model with their recovery has been presented. On the basis of the identified linkages, a structural model of the automated management of information flows of the bank has been developed, based on the principles of the protection of information and software of the bank. The main modules of the automated system of access distinction of information and software have been presented. Based on the analysis in the design process certain methods to improve existing solutions have been presented, taking into account the identified main advantages and disadvantages of similar modules of domestic and foreign manufacturers. The algorithm of controlling the bank's employees' access to the information structures of the bank has been created, including the identification process, the authentication, and authorization of employees. Also, we have found sufficient conditions under which the use of techniques of renovation increases the value of maximum accessibility of the computing system.

JEL Classification: C88, G21, L86, K22.

Keywords: Information security, access control, banking.

1. INTRODUCTION

Access control may be defined as request verification process to have access to the service in order to determine whether to allow or deny access. Most modern systems use access control model proposed by Lampson in 1974 (Figure 1).

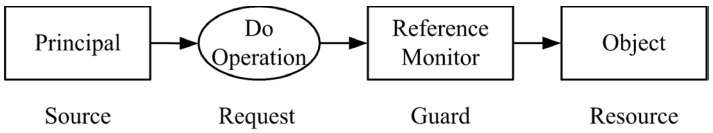

Figure 1: Access control model by Lampson, 1974

Lampson's model includes the following elements:

- the Principal that is the request's author (the principal is sometimes referred to as the subject);
- the Object that is informational, networking and computing resources;
- the Request that is a request to perform an operation with an object;
- the Reference Monitor that is access manager checking all requests to the object, and making decisions about allowing or banning the access.

Access manager holds three information protection procedures to take a decision. Determining the source of inquiry is called identification, confirmation of the authenticity of the source is called authentication, access control rules analysis is called the authorization (Bauer, 2007; Burnett, 2009; Erokhin, 2015; Erokhin, 2015). A complete interoperability of integrable systems is provided by semantic integration. Integration solutions using syntactic and structural approach are private, designed for specific systems. The widespread use of such solutions is problematic.

2. LITERATURE REVIEW

Information verification methods are aimed at confirming mathematical theories about the properties of software functioning or the results of the software's work. This method of software operation reliability control was first introduced in scientific publications of A.A. Lyapunov, T. Hoare, E. Dijkstra, Pratt, and Floyd.

Works of following foreign scientists are dedicated to this subject: C. Baumgartner, R. Kienast, L. Qin, V. Atluri, E. Lupu, N. Yialelis, M. Sloman, D. Wijesekera, L. Wang, S. Jajodia, P.L. Kagal, A. Joshi, T. Finin, T. Bhavani, etc.

A great contribution to the development of methods to solve this problem was made by Russian scientists P.P.Parkhomenko, V.V. Lipaev, E.S. Soghomonyan, S.A. Mayorov, O.F. Nemolochnov, G.G. Ryabov, V.A. Seljutin, V.M.Kureichik and many others.

3. METHODS AND RESOURCES

Currently, the most popular technology of semantic integration is ontology defining a common vocabulary domain which can be shared by people or information systems. There is a wide set of tools to develop ontology: a language for describing ontologies OWL (The Web Ontology Language), which is a W3C

standard editing environment ontologies Protégé, Ontolingua, Chimaera, ready and available to use ontologies that describe various subject areas (Erokhin, 2015).

There are analogies of three types: centralized management, federated identity systems, integrated management systems. Centralized management systems include AAA systems (Authentication, Authorization, Accounting), LDAP (Lightweight Directory Access Protocol), KERBEROS (security protocol network authentication technology), A-Select (single sign-on system in the Web), SAML (Security Assertion Markup Language).

Systems (protocols) of federal identification are: Liberty, WS-Federation, OpenID, Windows Card Space.

The most commonly used integration management systems are IBM Tivoli Identity Manager, Sun Identity Manager, Oracle Identity Manager, Novell Identity Manager, Microsoft Identity Integration Server.

The main aspects of the protocol service integration with a unified directory access management in the banking systems are (Eliseeva & Zlobin, 2012; Erokhin, 2015):

1. Single directory infrastructure of users supports the use of the following methods of integration with information services for authentication and authorization of users:
   - Kerberos protocol.
   - NTLM Protocol.
   - Windows Integrated Authentication (SSPI).
   - LDAP protocol to verify the credentials (bind).
   - LDAP protocol to authenticate users. You can connect both on behalf of the user credentials and the name of the special service accounts.
   - TACACS + Protocol.
   - RADIUS protocol.
   - Integration of file services to DFS.
   - The use of the SSL-certificates (including smart cards) of the internal CA for the TLS-Active Directory authentication and authorization of users.
   - IPSec protocol (using the SSL/TLS protocols are internal, Kerberos, and NTLM).
   - Opportunities of IIS Web server for the Active Directory integration, authentication, authorization, and integration with federated authentication.
   - OAuth protocol (federated authentication).
   - Protocol WS-Federation/WS-Trust (federated authentication).
   - Protocol SAML 2.0 (federated authentication).
2. The infrastructure of a single directory of users supports the use of the following methods of user authorization and shared access (read and modify) to the information in Active Directory:

- LDAP protocol for data storage and configuration changes. The connection is made on behalf of the service accounts.
- API ADSI to connect to an LDAP domain controllers.
- Web service SOAP internal IT Directorate for simplified user data from Active Directory.
- Active Directory Web Services (including the possibility of using PowerShell).
- Integration with Exchange mail system with IMAP, SMTP or Exchange Web Services (EWS).
- Integration with other services that are integrated with Active Directory. This is possible only in agreement with the administrators and intermediate services administrators.

3. None of the methods and protocols of information services to integrate with Exchange mail system are supported, except for protocols (EWS, IMAP, SMTP).
4. Single directory infrastructure does not support the following Active Directory protocols for integration services:
   - SAMR (SAM Database Replication);
   - MAPI.
5. REPL Protocols (Replicate Directory Changes), Microsoft Windows NT 4.0 (NetAPI) and SAM are only supported for system tasks (such as replication, computer connect to the domain or SID resolution in the name), but are not supported in the integration of services with a single catalog.
6. In some cases, information service independently implements integration with Active Directory. However, in any case, it uses one of the methods listed above. Accordingly, levels of SSO and the requirements for integration methods as discussed below are applicable to such services.
7. In some cases, the methods of integration of services with a single directory may have additional regulations for use. When choosing a specific method of integration of information services with a single directory unit administrator should check with service administrator if there are additional regulations and instructions that may affect the integration of services.

In order to integrate control access to different types of services, there is used a technique based on the semantic approach. The method consists of the following steps (Erokhin, 2015):

1. Set a number of services S which are subject to integration.
2. Set a number of models M, used to control access to the services of the set S.
3. Set a number of repositories of access control rules R which are subject to integration.
4. Set a number of access control protocols P that is used by the services of the S set.
5. Develop a unified access control model M_0. The model includes a semantic description of the basic concepts and Access control systems operations (represented as an ontology), and syntax rules of access control using this semantics.

6. Define the mapping of access control models $m_i \in M$ into a unified model M_0: $F : m_i \rightarrow M_0 \mid m_i \in M$.
7. Create a consolidated repository R_0 of access control rules, using the unified model M_0.
8. Develop *AR* adapters, providing data transfer from the repositories $r_i \in R$, into consolidated repository R_0.
9. Create a software access control, implementing information security procedures using access control rules in the consolidated repository R_0.
10. Develop *AS* adapters of access control protocols $p_i \in P$, providing interaction of $s_i \in S$ services with software access control to perform information security procedures using $p_i \in P$ protocol.
11. Configure $s_i \in S$ services to interact with access control via $a_i \in AS$ adapters for protocols $p_i \in P$.
12. Develop a policy management console access control in the consolidated repository R_0.

4. RESULTS AND DISCUSSION

For authentication in the operating systems with SSO level above the unit for common applications and Web applications without a federated authentication will require the integration of client computers with Active Directory users (inclusion of client computers into the domain). For web applications with an integrated federated authentication, integration of users' computers with Active Directory will be needed to achieve the fifth level of the SSO.

In order to ensure SSO level is higher than one for routine applications and Web applications without a federated authentication will also require the integration of servers with Active Directory. For Web applications with integrated federated authentication server is enough to integrate with federated authentication to provide any level of SSO (Erokhin, 2015).

Authentication in the Windows operating system:

1. The best method of integration with Windows OS is to form OS account in Active Directory and connect the computer to an Active Directory domain.
2. When you connect to a Windows domain it is allowed to use all standard formats of usernames.
3. If it is impossible to connect the computer to Active Directory domain, then it is necessary to integrate the OS with Active Directory using the Kerberos protocol. You can use the MIT Kerberos software tool (krb5), or a standard utility ksetup.exe (for the convenience in addition to it you can optionally use the program "runas" or "klogon.exe" link "http://fy.chalmers.se/~appro/nt/klogon/"). The account in the Active Directory is also necessary. Nevertheless, in this case, OS will lose the following opportunities: access to the LDAP, group policies, Secure Channel (automatic time synchronization, the SID resolution of names, etc.), synchronization, and other certificates.
4. If you cannot use the Kerberos protocol, then it is possible to integrate with the application "pGina" program, but for most of the services SSO level will not be greater than one.

5. Authentication in Windows OS is available in the DMZ (DemilitarizedZone) and inside, i.e. outside the corporate network.
6. Only administrators can connect computers to Active Directory domain divisions. Users cannot do that.

Authentication in * nix-systems:

1. The following types of * nix-systems' integration with Active Directory domain are not prohibited:

   Beyond Trust Powerbrokeropen/Likewiseopen application software for authorization and authentication of users;

   Centrify Express application software for authorization and authentication of users;

   The use of LDAP for authentication and authorization;

   The use of the Kerberos protocol to perform authentication and authorization;

   The use of winbind.
2. The use of winbind allows the following variations:

   It can be integrated with winbind krb5 kerberos support for an optional protocol. With Kerberos it is possible to perform authentication and authorization;

   Winbind can be integrated with Active Directory domain via LDAP to perform authorization;

   The full version of winbind has krb5 and LDAP in its composition.
3. Authorization and Authentication in * nix-systems is available within the corporate network (intranet).

   Apple MAC OS supports integration with Active Directory domain.

Authentication in Web services:

1. The following authentication methods for Web applications are used:

   Authentication using standard protocols previously described (e.g., requesting a username and password via Forms method);

   Authentication using federated authentication technologies;

   Authentication using the IIS web server capability (without Forms method).
2. If one of the standard protocols described above is implemented, then it is necessary when integrating the service with a single directory, to ensure:
   - what method is needed to get an account or to change the password (for example, showing the users' contacts or a unit administrator or to activate a link to the appropriate service in self-service applications "https://*.*/Access Management");
   - processing of messages that the user is required to change the password before entering, and point out how it is necessary to carry out (for example, carrying out the functional

themselves or activating the link to the appropriate service in self-service applications "https://*.*/ProfileManagement").

3. Integration of web-based applications with a unified directory is feasible on the basis of federated authentication technologies (based on the use of Active Directory Federation Services) by the following methods:

   The use of protocol WS-Trust/WS-Federation - Passive by the web application;

   The use of protocol WS-Trust/WS-Federation - Active by the web application. This protocol can also be used for conventional applications in which the client sends its credentials to the server;

   The use of SAML 2.0 protocol by the web application;

   The use of web application OAuth protocol (supported only Authorization Code Flow) by the web application;

   Services that use integrated authentication IIS can be configured to use of federated authentication with AD FS provider via C2WTS (Claimsto Windows Token Service). This setting can be done automatically via FedUtil utility;

   The use of Shibboleth SP application with Apache web server or IIS Web server. This Web application requires ShibbolethSP support.

4. In order to execute integrated web service with a single directory service integration, it is necessary to apply the rules to federated authentication, described in a separate document.

5. With the integration of web services using ADFS, services automatically receive the possibility of using single sign-on Web applications. At the same time users on the computers, but not in the domain, need to carry out the activation of the login and password only once to access all the web services (SSO fourth level). The users on the computers in the domain do not need to activate the login and password to access the web services (SSO fifth level).

6. In the application of federated authentication infrastructure, web service users have the opportunity (if required) to change the password before entering the system, and the ability to reset their password or get a new account.

7. Integrated with ADFS Web services automatically receive the support of all standard formats of usernames.

8. Integration of conventional (non-web) services with Active Directory Federation Services is possible with the use of WS-Federation protocol - Active.

9. Services for integration with federated authentication can authenticate and authorize users from other external systems (social networks - vk/facebook etc.) and catalogs of other companies.

10. To apply the authentication and authorization of users from other external systems and directories, as well as other companies, use the appropriate connector. If the connector required to the system has not yet been designed, then it is necessary to design, test, and connect it to the ADFS.

11. In the application of federated authentication, multi-factor authentication can be performed. To increase security, the service may require re-authentication of the user each time you access the service.
12. Federated authentication of access inside and outside of an intranet, as well as in the DMZ.

Log in services:

1. Integration of service with the domain (common catalog) Active Directory is used for user authentication and authorization, using the following tools:
   - predefined security groups (for example, Domain Computers, Domain Users, All Tutors, All Services, IMKN Computers, etc.);
   - security groups, formed by the administrator of a bank branch. Unit administrators and other authorized users (managers/owners of service) can manage users in these groups, which will provide access to administrators division. Users in these groups can be managed using tools MMC, and also with the help of users of the Web management interface to an intranet, as well as with your own/other software tools for LDAP/ADSI protocol (Averchenkov, 2005; Averchenkov, 2006);
   - User attributes (attributes used are to be agreed with the Active Directory service administrators, because part of the attributes can be modified by the user on their own, and some may not contain values that are required for authentication).
2. To authorize it is prohibited to have a user account in a directory (organizational unit), as the user account can be transformed into a different organizational unit at any time in accordance with the logic of the functioning of the single directory and synchronize processes with the Bank's HR systems.
3. The service can carry out its own authentication mechanisms without authorization through Active Directory. The service can combine their own authentication methods with Active Directory authentication methods (for example, the attribute of Active Directory user to receive data from another database and make a decision on authorization on the basis thereof).
4. The service can perform authentication and obtain data from Active Directory, without fulfilling authorization.
5. When using authorization using Active Directory groups the service is required to support global, local and universal groups, and nested groups, and if necessary, deploy the group. For NTLM protocol, Kerberos, RADIUS, SSPI it is usually maintained automatically. When using the LDAP protocol to support groups of recursive filters, you must either use the operator "LDAP_MATCHING_RULE_IN_CHAIN" (OID ": 1.2.840.113556.1.4.1941:") for LDAP-attribute "membefOf" and "member", or the code to deploy group recursively by reading LDAP-attribute "membefOf" and "member".
6. To increase the safety of the banking system the service could complement authorization and authentication via Active Directory own implementation of multi-factor authentication (for example, via an email, phone, optional password, re-enter a password, a certificate, a fingerprint reader, smart card, token, etc.) to perform additional authorization.

Let us define the reliability of access control to information and software in a commercial bank.

Reliability refers to the probability of the event consisting in the fact that the information system fulfills the task computed in the time interval $[0, t]$. Availability is the probability of the event, consisting in the fact that the information system fulfills the task computed at a given time. Let us consider the model without the restoration of a workstation after a crash and recovery model.

Consider the original case without recovery workstation. Let (i, j) is the state of the system. The index i denotes the number of functioning workstation (takes values 0, 1, 2), the $j = 1$, if the server is running, $j = 0$- the server is in an error state. We assume that the information system is in working condition, i.e. at least server and one functional workstation are in operation. The set of potential states of the system is denoted as $A = \{(0, 1), (1, 1), (1, 0), (2, 0), (2, 1)\}$. Let $X_t(w)$, $t \in R_+$ is a random process describing the state of the information system, taking values from the set A. Let $\pi_i(t) = P(w: X_t(w) = i)$, $i \in \{(2, 1), (1, 1), (0, 1), (2, 0), (1, 0)\}$. Suppose that a random $X_t(w)$ process is a Markov chain with the following diagram shown in Figure 2.

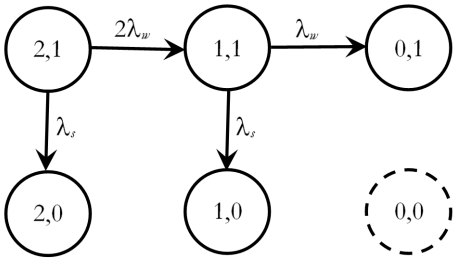

Figure 2: Markov chain diagram

The value of reliability $R(t)$ for the information system is calculated by the following formula:

$$R(t) = \pi_{(2,1)}(t) + \pi_{(1,1)}(t) = 2\exp(-(\lambda_w + \lambda_s)t) - \exp(-(2\lambda_w + \lambda_s)t).$$

Markov chain diagram for an information system with the recovery will be shown in Figure 3.

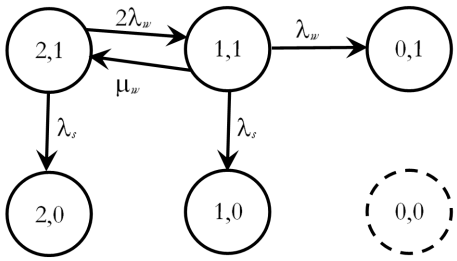

Figure 3: Markov chain diagram for an information system with the recovery

$$R(t) = \left(\frac{\mu_w}{k_1 + 2\lambda_w + \lambda_s} + 1\right)C_1 \exp(k_1 t) - \left(\frac{\mu_w}{k_2 + 2\lambda_w + \lambda_s} + 1\right)C_1 \exp(k_2 t);$$

$$C_1 = (k_1 + 2\lambda_w + \lambda_s)(k_2 + 2\lambda_w + \lambda_s)[\mu_w(k_2 - k_1)]^{-1};$$

$$k_1 = -0,5(3\lambda_w + 2\lambda_s + \mu_w) + 0,5(\lambda_w^2 + \mu_w^2 + 6\lambda_w\mu_w)^{0,5};$$

$$k_2 = -0,5(3\lambda_w + 2\lambda_s + \mu_w) - 0,5(\lambda_w^2 + \mu_w^2 + 6\lambda_w\mu_w)^{0,5};$$

$$\lim_{\mu_w \to \infty} R(t) = \exp(-\lambda_s t).$$

Condition $\mu_w \Rightarrow +\infty$ shows that in the case of a workstation failure an immediate transition to the "ideal" state is implemented (2, 1). At this point, the value of reliability R(*t*) takes the maximum value and the limit value R(*t*) depends only on the value of λ_s – the average time of a server failure.

Next, we examine the method of updating of the program operation. We assume that at the outset of the computer system, which runs the program, is in a perfect condition. The probability of failure in this state is close to zero. The ideal state is denoted by "0". We assume that the presence of an information system in a state of "0" is not infinite, and after some time the information system goes into the "P" condition where the probability of failure is no longer zero. This shift is due to the fact that the operation process for the system eventually degrades, and a gradual reduction in the resources of the computer system begins. After some time, from the "P" condition the information system goes into the "F", which corresponds to the malfunction of the system. Such a process can be formalized by the following mathematical model. Let $X_t(w)$, $t < \in R_+$ is a random process with values in the set {0, P, F}. We believe that $X_t(w)$,$t < \in R_+$ is a Markov chain, the diagram of which will be shown in Figure 4.

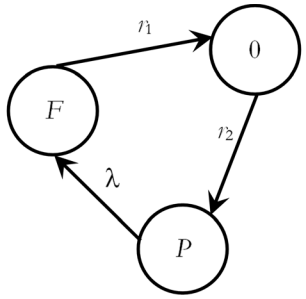

Figure 4: Markov chain diagram $X_t(w)$, $t < \in R_+$

Suppose also that the process $X_t(w)$ is homogeneous in time and has the Markov property. Denote $\pi_i(t) = P(X_t(w) = i)$, $i \in \{0, P, F\}$.

In this case, the Kolmogorov system of differential equations is applicable:

$$\begin{cases} \pi_0'(t) = -r_2\pi_0(t) + r_1\pi_F(t) \\ \pi_P'(t) = -\lambda\pi_P(t) + r_2\pi_0(t) \\ \pi_F'(t) = -r_1\pi_F(t) + \lambda\pi_P(t) \end{cases}$$

Using the ergodic theorem, we obtain $\exists\pi_i = \lim_{t\to\infty} \pi_i(t), i \in \{0, P, F\}$.

Finally we get equation system for the limiting probabilities:

$$\begin{cases} -r_2\pi_0 + r_1\pi_F = 0 \\ -\lambda\pi_P + r_2\pi_0 = 0 \\ -r_1\pi_F + \lambda\pi_P = 0 \\ \pi_0 + \pi_P + \pi_F = 1 \end{cases}$$

Hence, $\pi_F = r_2\lambda(r_2\lambda + r_1r_2 + r_1\lambda)^{-1}$.

The value π_F is limiting the probability of finding the information system in a failed state. With its help it is possible to assess the reliability of the computer system. If π_F value is close to one, it means that

the information system is less reliable. The value of the availability of information systems is defined as $\pi_A = 1 - \pi_F$.

Consider a model in which the information system of the state "P" may also go into a state "R", which marks the renewal of the system. Let the diagram of the information system transitions has the form shown in Figure 5.

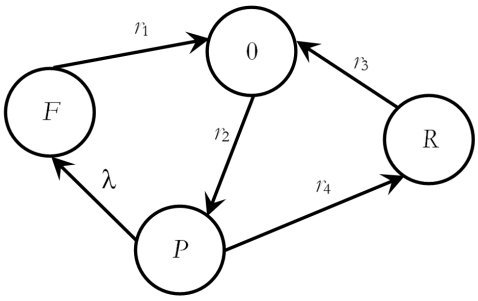

Figure 5: The diagram of the information system transitions

We believe that while in a state "R" the information system is not workable. Then the formula for the calculation of the marginal probability of system failure is of the form

$$\pi_F^{rejuv} = r_2(r_3\lambda + r_1r_4)[r_2(r_3\lambda + r_1r_4) + r_1r_3(\lambda + r_2 + r_4)]^{-1}.$$

The value of the availability of information systems is calculated as $\pi_A^{rejuv} = 1 - \pi_F^{rejuv}$.

1. If $r_3 > r_1(1 + r_2/\lambda)$, then π_F^{rejuv} decreases by r_4 parameter.
2. If $r_3 < r_1(1 + r_2/\lambda)$, then π_F^{rejuv} increases by r_4 parameter.

These expressions indicate a sufficient condition under which the update method increases the size limit availability.

5. CONFIRMATION

Consolidated repository access control rules are based on the LDAP-directory Sun Java System Directory Server. Identification protocol adapters are implemented using software Free RADIUS, OpenSSO, Samba. The control system is based on the Sun Java System Delegated Administrator, which has extended functionality for access control to services of various types. The control system provides two types of interfaces: the command line and the Web. The distribution of powers between administrators is carried out using a delegate at two levels: the administrator of the organization and an administrator with full access. The complex is run by the Solaris OS. Reliability of the complex is provided with structural redundancy.

The ease of services application is enhanced by a single password and ID. The amount of identifiers required for the operation decreased from 10 (corresponding to the number of services that are connected to the access control system) to one. Reducing the number of identifiers thus reduced the number of requests in the helpdesk for password recovery and consultation in order to access services by 60%.

Thus, a comparative analysis of the timing control access to services with the use of an integrated management system process and without it has been implemented (Table 1).

Table 1
Comparative analysis of the time spent in the process of access control to services in the bank information system

Process	*Traditional access control systems, min.*	*Integrated access control, min.*
Account setting	10…25	2…6
Account changing	4…12	1…3
Account delete	10…20	4…7
Access rights transfer	12…16	5…8
Access rights change	6…12	2…4

The time saved with access control using integrated control system, can be up to 90% of the time with the use of traditional access control systems due to reducing the number of manual operations.

Integration of access control services of various types reduces demands to system administrators by providing a single Web-based user-friendly control system.

The practical significance of the work consists in the development of methodical maintenance of hardware and software to protect the bank's automated systems, based on the results of the analysis of the merits and shortcomings of existing technology solutions. The work is of a theoretical nature, but the results can be applied in the design information banking systems as well as in the study of their reliability.

References

Averchenkov, V. (2005). *Security System of Russian Federation* (1st ed.). Bryansk: Bryansk State Technical University.

Averchenkov, V. (2006). *Organizational management systems* (1st ed.). Bryansk: Bryansk State Technical University.

Bauer, F. (2007). *Decrypted secrets. Methods and Maxims of Cryptology* (1st ed.). Moscow: Mir.

Burnett, S. (2009). *RSA Security's Official guide to Cryptography* (1st ed.). Moscow: Binom-Press.

Eliseeva, E., & Zlobin S. (2012). Innovative approaches to the use of Internet technology for training in the field of IT technology. *Innovation based on information and communication technologies, 1,* 39-41.

Eliseeva, E., Zlobin, S., & Kashlikova, T. (2010). *Information technology in socio-economic sphere* (1st ed.). Bryansk: "Ladomir", LLC.

Erokhin, V. (2015). *Safety of information systems* (1st ed.). Moscow: FLINTA.

Erokhin, V. (2015). *Software protection and information verification in the bank's information and telecommunication systems* (1st ed.). Moscow: MSU Publishing.