УДК 004.056

Vyacheslav Chaplyga[1], Elena Nyemkova[1], Serge Ivanishin[1], Zenon Shandra[2]
Lviv Institute of Banking the University of Banking of the NBU[1],
National university Lviv Polytechnic[2]

ADMINISTRATION OF ACCESS RIGHTS TO THE CORPORATE NETWORK WITH THE INTEGRATED AUTOMATION OF THE BANK

The article is devoted to the administration of access rights in Role-Based model Access Control to the corporate banking networks. Four main functional roles are offered in accordance with the international standard CobiT. The problem of remote connectivity to information resources of banks in terms of security is similar to the problem BYOD. There are proposed an algorithm of the automated control of remote access. The algorithm is based on the separation of the work area in the virtual space of the bank's server. The mathematical model of access for basic functional roles is presented.

Key words: integrated automation of the bank, functional roles: governance, management, audit, execution, hierarchy of roles, BYOD, Role-Based model Access Control.

АДМІНІСТРУВАННЯ ПРАВ ДОСТУПУ ДО КОРПОРАТИВНОЇ МЕРЕЖІ З КОМПЛЕКСНОЮ АВТОМАТИЗАЦІЄЮ БАНКУ

Запропоновано адміністрування множин прав доступу до корпоративної банківської мережі згідно з моделлю Рольового розподілу доступом. Розглянуто чотири основні функціональні ролі за міжнародним стандартом CobiT. Проблема безпеки віддаленого доступу до інформаційних ресурсів банку аналогічна проблемі BYOD. Запропоновано алгоритм автоматизованого контролю за віддаленого доступу. Алгоритм розроблено на підставі поділу робочої та віртуальної областей серверу банку. Запропоновано математичну модель доступу для чотирьох основних функціональних ролей.

Ключові слова: комплексна автоматизація банку, функціональні ролі: керівництво, менеджмент, аудит, виконання, ієрархія ролей, BYOD, модель Рольового розподілу доступом.

Introduction

Modern bank is characterized by a two-tier management structure. Thousands of users are working in the corporate banking network. Access rights of users of corporate of banking network on information resources are grouped based on their specific application. Role-Based model Access Control should be used for situations where the range of powers and responsibilities clearly defined. The role is a set of access rights to the objects of the computer system. The Rules of Role-Based model Access Control definite for granting access rights to users of corporate banking network, depending on the session and roles at any given time [1]. In reality, the corporate banking network structure of roles and rights is very complex. Therefore, the problem of administration is very important. Building an administration model of Rules of Role-Based model Access Control solves this problem.

Formalization of roles and rights in relation to the information bank business processes and information products is necessary to construct a model of administration of Role-Based model Access Control. In practice, there is a hierarchical structure of roles. Therefore, administration of role’s hierarchy is necessary. In accordance with the international standard CobiT there are dealing with four main functional roles: governance, management, audit, execution [2]. Example of a hierarchy of functional roles is shown in Figure 1.

These hierarchical structures are typical of advanced forms of business processes. They can be seen not only in the bank, but in any business structures. Each of the functional roles, in turn, is a hierarchical structure. For example, the Board of Commercial Bank (the functional role of management, M) consists of the Chief Accountant, the credit department, department of securities, management of work with individuals, management to work with legal entities, management automation, marketing management, security management and administrative management.

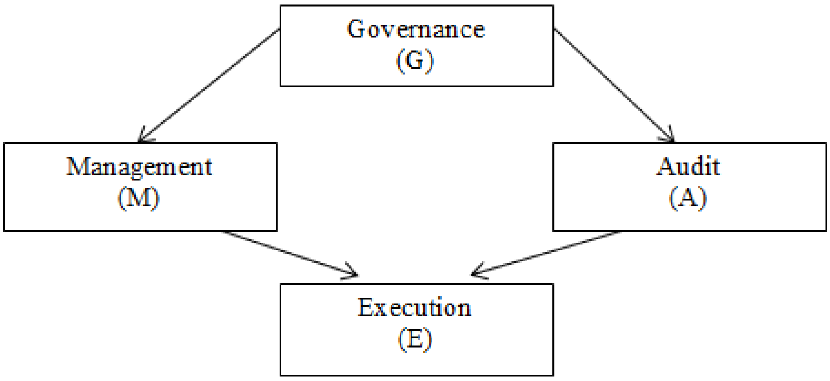

Fig. 1. Hierarchy of functional roles in bank

Each role has the right to selected area of an information resource and works with multiple software products. Below there are given peculiarities of work of the auditor.

Modern approach to the audit requires complex automation of all stages of the audit. The use of specialized audit software helps reduce the cost of the audit, improves the quality and efficiency of the audit. Nowadays there are dozens of software solutions of complex automation of auditing. The following programs are among the leaders in popularity. The program “IT Audit: Auditor 4.3” is integrated with 1C: Enterprise 7.7, 8.2. It provides auto-complete data of audit working papers with 1C: Enterprise. The program has the ability to create their own methods of audit term to 450 audit procedures [3]. The program “AuditModern” provides conceptually new approach to internal audit of various organizations, including banks. The program is autonomous and independent of the information systems of organization, restricts access of stakeholders to the results of audits, database audit evidence and findings, and provides control over the activities of internal auditors in the central and remote offices [4]. The program “AuditXP” allows you to plan and carry out audits in complex control quality assurance, change audit method [5].

The program of applications integrated automation of audit are provided by support of developer, of connection to the latest regulations and are of high cost - about $ 5,000. Placement of programs of this type on auditor’s laptop is the key to reliability and confidentiality of data and results of the audit. The auditor uses in his own practice specialized programs. Auditors require coordination questions mobility audits and information security business and corporate security software.

Important issues that arise in the course of complex automation audits are security auditor remote connect a laptop to the LAN of the organization to be audited. This imposes new requirements on safety management for the bank and for the mobile computer auditor and it known for our time as the problem of BYOD (Bring Your Own Device). Thus, convenience, high quality and reliability of remote audit department of the bank as well as any other organization require revision model of computer network security.

Administering of role of the auditor for remote access

The requirements of modern business processes in the bank significantly accelerate the pace of information management cycle in which bank’s corporate networks and personal devices (laptops, tablets) participate. For a complete solution to the problems have been proposed system BYOD class Mobile

Device Management (MDM). These systems have several disadvantages, do not provide a safe introduction of personal devices in business practice and practice remote audit. For example, MDM systems allow you to remotely manage mobile personal device if the device appears on the network. But these systems do not take into account the possibilities of insider threats. The most effective solution to data security is access to information assets through bank branch terminal session to Windows-virtual environments which are protected DLP (Data Leak Prevention) [6].

It is proposed all applications (in this case the program auditor), which work with corporate data, to run inside a virtual Windows session on a server of bank for all these requirements are provided after the rigorous mutual authentication of auditor and its device are made. The results of the program's calculation are transmitted to a computer auditor. After the session, all the results of the auditor's specialized program in a virtual environment are destroyed securely. In fact, in virtual server environment of the bank there should be organized workspace of auditor, where the agent of the program is runs with the laptop or tablet of auditor.

The agent has the right to read data located on a server bank, which he uses to further processing. The results of processing are transmitted to the device auditor through secure channel. DLP system that works within the perimeter of the corporate network bank is configured so that the data from the server does not have the right to leave the perimeter. But the results of the special program auditor represent entirely different data and DLP system does not prevent the transmission of data on the corporate network perimeter. A shredder runs in the workspace auditor virtual environment after the session.

The proposed strategy requires the agent in auditor's program that can be installed in a virtual environment and transmit the necessary information for further processing to a computer of auditor. There shredder is need. With server-side bank is important to apply the security model of the computer environment that allows you to perform secure changes in the level of confidentiality.

There are the basic concepts of the object and the subject of access to information in the theory of model of the computer system's security. Depending on the method by which access is provided, there are consider five basic types of security models of computer systems: Discretionary Access Control, Mandatory Access Control, Information Flow Security model, Role-Based model Access Control, Subject-Oriented Sandbox model [7].

For automated banking systems benefits are provided Role-Based model Access Control [8]. Nowadays, under Role-Based model Access Control there are developing actively a variety of options depending on the specific problems of safe access [9-11]. BYOD phenomenon needs its own development model of Role-Based model Access Control.

It is known that all security information described access of subjects to objects. In the case of the auditor's remote access to bank information objects will be called the following areas of space. Firstly, it's information area *(area(inf)),* which is required for all audit information - databases 1C: Enterprise and databases of other specialized banking software. Secondly, it is the working area *(area(work)),* virtual server bank area, where the agent program auditor operates.

The subject will be called an agent of specialized program of auditor which processes the data of object. Problem management consists of providing access rights as Role-auditor, depending on the object. There is need to extend the basic Role-Based model Access Control to solve this problem.

The user U_{aud} is added to the set of users U, the role R_{aud} is added to the set of roles R, the right P_{aud} is added to the set of rights P and the session S_{aud} is added to the set of sessions S.

The right P_{aud} is a function of the object to which role R_{aud} requesting access:

$$\mathrm{P_{aud}: P_{aud} \rightarrow P(area): P(area(inf))=\{read\};}$$

$$\mathrm{P(area(work))=\{read, write, create, delate, open, close, execute\}}$$

Function $PA: R \rightarrow 2^P$ determines for each role a set of access rights.

Function $UA: U \rightarrow 2^R$ determines for each user a set of roles to which he may be authorized. Sets of roles and sets of access rights for U_{aud} and for all other still divided into disjoint for object *area(work)*:

$\mathrm{R=R1 \cup \ldots \cup Raud \cup \ldots \cup Rn}$,

$\mathrm{Ri \cap Raud} = \varnothing$ for $\mathrm{i \neq aud}$;

|UA(Uaud)∩Ri |=0, Ri≠ Raud;

P=P1 ∪ … ∪ Paud ∪ … ∪ Pn,

Pi∩Paud=∅ for i≠aud;

$|PA(R_{aud})∩P_i|=0$, $P_i≠ P_{aud}$.

For the object *area(inf)* the role and user's access right of user U_{aud} may overlap with roles and access rights of other users, depending on the security policy of a particular banking institution:

R=R1 ∪ … ∪ Raud ∪ … ∪ Rn,

Ri∩Raud={A} for i≠aud;

|UA(Uaud)∩Ri |≤1m Ri≠ Raud;

P=P1 ∪ … ∪ Paud ∪ … ∪ Pn,

Pi∩Paud={B} for i≠aud;

|PA(Raud)∩Pi |≤1, Pi≠ Paud;

A and *B* are non-empty set.

Conditions on dynamic mutual exclusion roles are similar to the Role-Based model Access Control.

For the role of the auditor there should be limited to a maximum number of users that can be logged on it, similar to the access right of auditor there should be limited to a maximum number of roles:

$$|UA^{-1}(R_{aud})|=1,$$
$$|PA^{-1}(p)|=1.$$

Number of concurrent sessions *roles(r),* which can be simultaneously logged in to the role of the auditor is limited:

$$|roles^{-1}(R_{aud})|=1.$$

Also, for each role there is ensure that it could be an authorized user, it must be define the roles to which the user must be authorized also. For the role of the auditor such set is an empty set for the object *area(work),* and non-empty set for the field *area(inf)*. In the last case non-empty set is determined by the security policy of a particular bank. Similar requirements are imposed for access rights.

Administration model of the Role-Based model Access Control

There are selected the following elements to administer a set of authorized user roles:

AR – multitude of administrative roles $AR \cap R = \varnothing$;

AP – multitude of administrative rights of access $AP \cap P = \varnothing$;

APA: $AR \to 2^{AP}$ – function defines a set of administrative access rights for each administrative role;

AUA: $U \to 2^{AR}$ – function defines a set of administrative roles for each user, who can be authorized;

roles: $S \to 2^{R} \cup 2^{AR}$ – function defines a set of roles for user, who can be authorized on this session.

Let there be given hierarchy of roles, see Figure 2. Minimum role in the hierarchy is the technician (*Tec*); the maximum role is the Head of the Department of Automation Control (*HDAC*). The department has four sectors. Maximum the role of each sector is Head of Sector (*HSsw*, *HSacn*, *HSe, HSts*). Minimal role of each sector is a specialist (*Ssw*, *Sacn, Se, Sts*). Roles of the proficient and role of the control are in sectors of S.W.I.F.T. and ACN (*Psw, Pacn, Cswift, Cacn*).

Hierarchy of administrative roles consists of six roles with a maximum role - a senior security officer (*SSO*), the role of a security officer (*SO*) and four roles of security officers of sectors (*SOsw, SOacn, SOe, SOts*).

To administer a set of authorized users there are given functions:

can-assign: $AR \to CR \times 2^{R}$ – function defines set of roles that can be included in the authorized user's role using the administrative role;

can-revoke: $AR \to 2^{R}$ – function defines set of roles that can be excluded in the authorized user's role using the administrative role.

Values of the functions *can-assign()* and *can-revoke()* defined in Table 1 and Table 2.

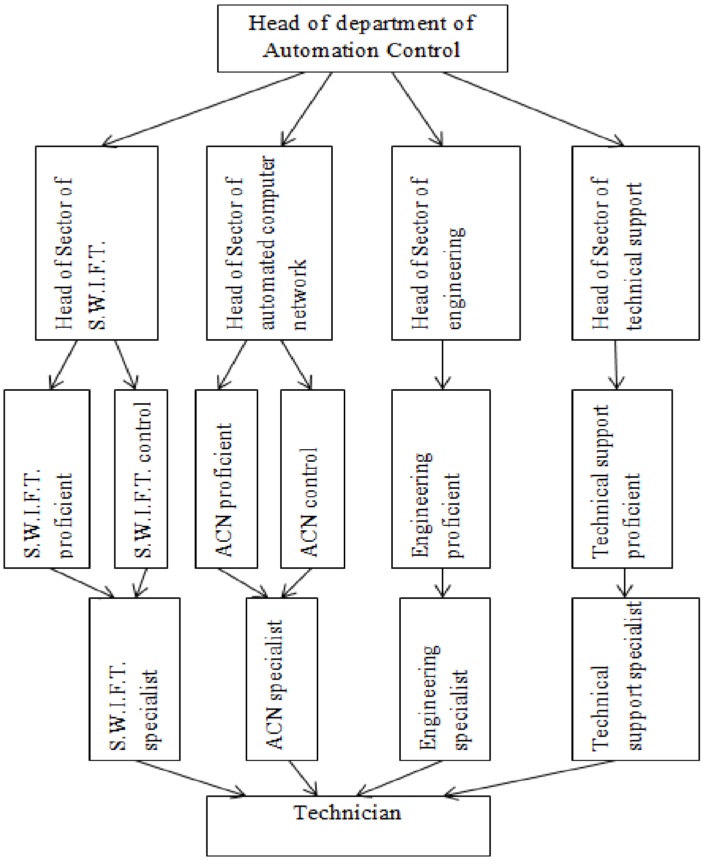
Head of department of Automation Control
Head of Sector of S.W.I.F.T.
Head of Sector of automated computer network
Head of Sector of engineering
Head of Sector of technical support
S.W.I.F.T. proficient
S.W.I.F.T. control
ACN proficient
ACN control
Engineering proficient
Technical support proficient
S.W.I.F.T. specialist
ACN specialist
Engineering specialist
Technical support specialist
Technician

Fig. 2. Hierarchy of roles of department of Automation Control

Table 1

Value of the function *can-assign()*

Administrative role	Precondition	Multiple roles
SO	*Tec and (not HSacn) and (not HSe) and (not HSts)*	*[HSsw, HSsw]*
SO	*Tec and (not HSsw) and (not HSe) and (not HSts)*	*[HSacn, HSacn]*
SO	*Tec and (not HSsw) and (not HSacn) and (not HSts)*	*[HSe, HSe]*
SO	*Tec and (not HSsw) and (not HSacn) and (not HSe)*	*[HSts, HSts]*
SOsw	*Tec*	*[Ssw, HSsw)*
SOacn	*Tec*	*[Sacn, HSacn)*
SOe	*Tec*	*[Se, HSe)*
SOts	*Tec*	*[Sts, HSts)*

Administrative role *SOsw* allows to include roles *Ssw*, *Psw* and *Cswift* for user who already has role *Tec*. There are analogous to roles *SOacn*, *SOe*, *Sots*. Administrative role SO allows to include role *HSsw* for user who already has role *Tec*; and the user should not have a roles *HSacn*, *HSe*, *HSts*. There are analogous to roles *HSacn*, *HSe*, *HSts*.

Table 2

Value of the function *can-revoke()*

Administrative role	Multiple roles
SO	*(Tec, HDAC)*
SOsw	*[Ssw, HSsw)*
SOacn	*[Sacn, HSacn)*
SOe	*[Se, HSe)*
SOts	*[Sts, HSts)*

Values of functions *can-assign()* and *can-revoke()* are determined independently from each other. The role can be removed from the set of authorized user roles regardless of how this role has been included in this set.

Conclusions

The complexity of software, security and business continuity as well as secrecy of audit require of remote audit from laptop of auditor. Automation of internal audits requires remote access to the corporate banking network. This is due to the requirements of the mysteries of the audit, the complexity of the software and developed a two-tier system of banking institutions. The problem of remote connectivity to information resources of banks in terms of security is similar to the problem BYOD.

There are proposed an algorithm of the automated control of remote access. The algorithm is based on the separation of the work area in the virtual space of the bank's server. Agent of program of auditor has all the powers of access to databases. Necessary calculations are carried out in virtual space within the perimeter of the corporate network. The results of the audit are transmitted over a secure channel on the laptop of the auditor. Workspace safely cleared the shredder at the end of the session. There are proposed a model of remote access control based on the Role-Based model Access Control for the algorithm. This requires changes to the Role-Based model Access Control. The character of the changes is determined by different access right of auditor for the individual workspace server of bank and depends on the security policy of a particular bank.

1. Девянин П. Н. Модели безопасности компьютерных систем / П. Н. Девянин. – М. Издательский центр "Академия", 2005. – 144 с. 2. Cobit 4.1 IT Governance Institute; http://ua.bookfi.org/g/ Cobit%204.1 3. Автоматизация аудита в IT Аудит: Аудитор; http://www.audit-soft.ru/. 4. IT Аудит: Аудитор 4.0; http://www.audit-it.ru/software/auditing/71677.html. 5. Audit XP "Комплекс аудит"; http://www.auditxp.ru/products/reportaudit/editions/complex/. 6. А. Астахов. Модель информационной безопасности BYOD, 17-07-2014; http://iso27000.ru/blogi/aleksandr-astahov/model-informacionnoi-bezopasnosti-byod. 7. Зегжда Д. П., Івашко А. М. Основы безопасности информационных систем. – М.: Горячая линия – Телеком, 2000. 8. Обеспечение информационной безопасности на стадиях жизненного цикла автоматизированных банковских систем, Дата введения: 2014-09-01; http://iso27000.ru/zakonodatelstvo/normativnye-dokumenty-banka-rossii/rs-br-ibbs-2. 6-2014-obespechenie-informacionnoi-bezopasnosti-na-stadiyah-zhiznennogo-cikla-avtomatizirovannyh -bankovskih-sistem. 9. D.R. Kuhn, E.J. Coyne, and T.R. Weil, "Adding Attributes to Role Based Access Control," Computer, vol. 43, no. 6, 2010; http://csrc.nist.gov/groups/SNS/rbac/ documents/kuhn-coyne-weil-10.pdf. 10. E.J. Coyne, T.R. Weil, ABAC and RBAC:Scalable, Flexible, and Auditable Access Management, IEEE IT Professional, May/June 2013; http://csrc.nist.gov/groups/SNS/rbac/documents/ coyne-weil-13.pdf. 11. Щеглов К. А., Щеглов А. Ю. Новый подход к реализации контроля и разграничения прав доступа к данным в информационных системах; август 2014; http://www.securitylab.ru/blog/personal/Information-security/79419.php.