Stochastic Investigation of Secure Access to the Resources of a Corporative System

Radi Romansky, Irina Noninska

Abstract—The goal of this article is to introduce an idea for organization of security procedures in a corporative system for accessing and processing different information resources and personal data. Three types of resources could be organized in a business information environment – public (without access restriction or rules), private internal (stored in own memory environment) and private external (stored in a cloud data centre and used by cloud services). The paper presents an approach intended to investigate the procedures for secure access to these information resources, paying attention on personal data protection, as well. General structure of corporative management system for secure access to the information resources and an algorithmic scheme for procedures realization are proposed. Stochastic investigation of the procedures based on Markov chain is made. An analytical solution of the model is proposed and statistical assessments are calculated.

Index Terms—Cloud computing, Corporative information system, Information security and privacy, Markov's chain, Resources protection, Secure access, Statistical assessments, Stochastic modelling.

1 INTRODUCTION

THEcontemporary Information society rely on remote access to information resources located in different places of the global network. In many cases this access is not monitored or regulated which is risk for both – usersand resources. It is well known that many activities in the digital word require personal data uploading which could disturb the privacy [1]. In this reason different world institutions discuss development of new improved regulation in the cyber space, including procedures and tools for information security (IS) and for personal data protection (PDP) [2].

The publication [1] determines a Corporate Information System (CIS) as "*a fully integrated, company-wide system solution that aims to meet all organisational ICT (Information and Communication Technologies) requirements at all levels.*" European rule for all personal data is that "…data is held only once; it is "owned" by the organisation as a whole and used by different departments" [3].

The federal government's information systems security program [4] enables agencies' mission objectives through a comprehensive and consistently implemented set of risk-based, cost-effective controls and measures that adequately protects information contained in federal government information systems. The Information Systems Security Line of Business (ISSLoB) was created in 2005 to improve the level of information systems security across government by eliminating duplication of effort, increasing aggregate expertise, and enhancing the overall security posture of the federal government. This valuable proposition is supported through the use of Shared Service Centres (SSC's), consolidated acquisitions, agency standard practices, and lessons learned across agencies.

The business organizations and companies create, collect, process and support different types of information stored in their own memories or cloud data centres accessed via network. The cloud proposes services as IaaS, SaaS, PaaS and has many advantages regarding organization of business processes, requiring at the same time strong policy for IS and PDP which must be developed and used.

Protection of the sensitive business information is imperative and must be managed [5]. It should be based on the international standard ISO 27000 known as Information Security Management System (ISMS). This standard determines the measures for protection of confidentiality, integrity and availability of sensitive business information, including personal data.

The present article discusses organization of a system for business information protection in two cases: when it is stored as internal resources (in private memories) or stored as external resources (in a cloud data centre). An analytical model for secure procedures investigation by using Markov chain (MC) based on preliminary formalization of the processes is defined. Some assessments for the role of main procedures (registration, identification, authentication, authorization) are calculated by analytical solution of the model. Additional statistics are proposed by using Statistical Software Develve [6].

The article is organized as follows: section 2 is a survey of related works; section 3 deals with proposed general structure of corporative management system for secure access to the information resources and algorithmic scheme for procedures realization; sections 4 and 5 present an analytical model which is developed by using MC apparatus and the model solution; experiments planning and calculation of statistical assessments are presented in section 6, including assessments obtained by using specialized statistical software Develve; finally a conclusion is made in section 7.

- *Radi Romansky – full professor in Technical University of Sofia, Bulgaria; Ph.D. in Computer engineering and D.Sc. in Informatics and computer science. Area of interests: computer architectures, modelling, distributed systems, privacy and data protection, etc. E-mail: rrom@tu-sofia.bg*
- *Irina Noninska – associate professor in Technical University of Sofia, Bulgaria; Ph.D. in Information technology. Area of interests: information security and cryptography, e-business, data processing, etc. E-mail: irno@tu-sofia.bg*

2 Related Work

Development of business information environment must take into account necessity of secure access and information protection for personal profiles of users and staff, business information resources, corporative archives, etc. This requires implementation of contemporary means and tools for main processes as registration, verification, authentication and access rights management where specialised software, hardware and biometric technologies for user's identification could be applied.

Publication [7] determines each business system as "*an organized collection of parts (or subsystems) that are highly integrated to accomplish an overall goal. The system has various inputs, which go through certain processes to produce certain outputs, which together accomplish the overall desired goal for the system*". This publication outlines that the intentional information security culture has several important characteristics as follows: Alignment of information security and business objectives; A risk-based approach; Balance among organization, people, process and technology; Allowance for the convergence of security strategies.

A model for business information security is proposed in [7] and it is shown in Fig. 1. The main characteristics of this model are flexibility, three-dimensional, pyramid-shaped structure with four elements connected by six dynamic interconnections.

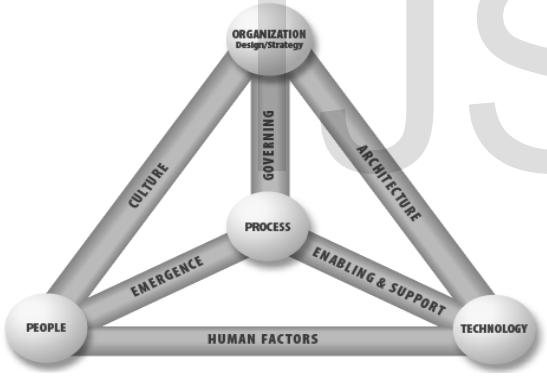


Fig. 1. Business Model for Information Security proposed in [7].

According to the definition in [8] "*an ISMS is a set of policies and procedures for systematically managing an organization's sensitive data*". In this reason the goal of ISMS is to protect personal data and business information resources in order to minimize risk of illegitimate access and using. This determines ISMS purpose as a collection of means and tools for preventive action. Article [5] extends the functions of ISMS with the goal to manage sensitive information for industrial control systems (ICSs), because the main priority of industrial control is safety of the system. In this respect, a new paradigm of ISMS for ICS based on confidentiality, integrity, and availability as well as system's safety is provided in [5].

The main aspects of reliable protection of information are discussed in [9]. This article regards each security system as a set of measures for reduction the risk of information abuses accomplished with reliable protection of all business information resources. The authors have made a brief description of the protection objects and the main threats, including those that are related to the processing of personal data. They have determined the important role of information security in all business processes. A formalization of access rights to information resources is presented and a block diagram for illustration the process of analysing the threats and vulnerabilities is given.

An overview of current risk management approaches that outlines their commonalities and differences is made in [10]. The evaluation of these approaches is made based on their capability of supporting cost-efficient decisions and proposing potential solutions. Existing approaches are compared in order to reveal the challenges which information security risk management could face. The authors declare that the analysed risk management approaches do not explicitly provide mechanisms to support decision makers in making an appropriate risk versus cost trade-offs, but it is possible to identify academic approaches which fulfil this need.

The risk for business information systems security grows when the corporative resources are stored in cloud data centres and are accessed via the global network. Cyber-physical security of Wide-Area Monitoring, Protection and Control (WAMPAC) from a coordinated cyber-attack perspective is discussed in [11]. This article describes briefly how cyber-physical test beds can be used to evaluate the security research and perform realistic attack-defence studies for smart grid type environments.

An investigation for business resources protection should precede the development of ISMS. In this reason the modelling as a suitable and efficient approach for determination of structural discrepancy could be used to revealspecial features determining processes realization. For example, [12] presents a scalable, stochastic model-driven approach for investigation of IaaS cloud and the migration of physical machines.

Ref. [13] proposes a stochastic model for investigation of cloud data centre management which is defined as a key factor due to the large number heterogeneous strategies that could be applied. The author discuses cloud computing infrastructure and evaluation of its performance. He stresses on the fact that as an important part of cloud strategy performance evaluation must correspond to the quality of service (QoS) demanded and experienced by users. An analytical model based on stochastic reward nets is presented in the paper and several performance metrics - utilization, availability, waiting time, responsiveness are defined and evaluated to analyse the behaviour of a cloud data centre.

3 General Structure of a Corporative System for Secure Access Management

Initial step of each investigation by using modelling should be formalization of the modelled object – a system or a process, and it is a compulsory stage which should precede model development. A formalization by using event-graph apparatus is proposed in [14] and it describes a corporative system for secure access to the information resources as a complex of the following two subsystems:

♦ Front office – this is an input point for remote user's access to the corporative system which is responsible for the

initial registration of a new user and preliminary identification of already registered users. The registration procedure creates a personal profile collecting a set of personal data. The identification procedure should guarantee legitimate access to the back office component. An audit file for registration of each access (time, IP address and relative attributes) and statistical data storing is included in this structure to enhance functionality of the front office.

♦ Back office – it deals with the basic administrative procedures that support processes of secure access. The functionality of this sub-system is directly connected whit the administrative database (Admin DB) which consists of different components. They are as follows: profiles created during the user's registration collecting personal data; system profiles for the staff; personal rights for the users' access which are defined according to the security rules of the corporative information system (CIS); components of Digital Rights Management System (DRMS), etc.

On the base of these components we propose the General structure of a Corporative Information Security Management System (CISMS) which is shown in Fig. 2.

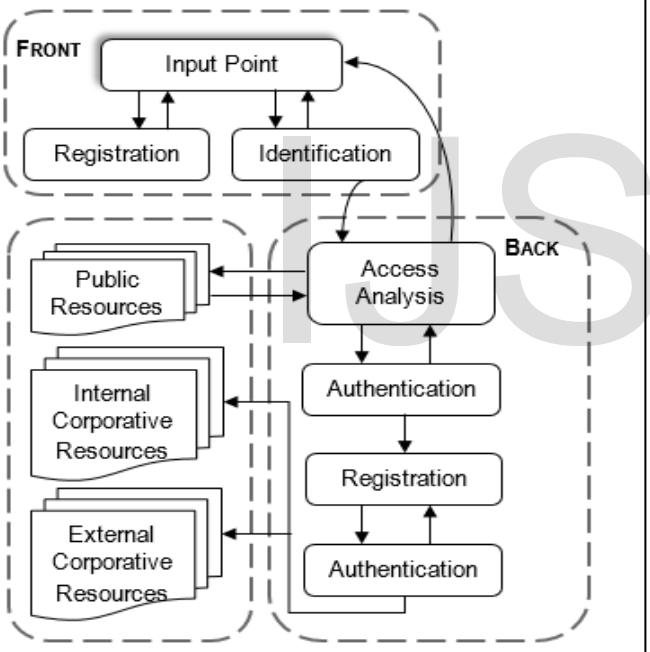


Fig. 2. General structure of CISMS – components: Front office; Back office; set of information resources

All measures for securing data protection and regulation of user's access to business information resources are realized as separate procedures in these sub-systems. The third component of corporative management system in Fig. 2 is the set of information resources determined as public, internal corporative resources and external corporative resources. The last two parts should be protected and access to these resources must be regulated. This is the goal of the proposed system for information security (SIS) which functionality is presented in Fig. 3 by an algorithmic scheme of security processes.

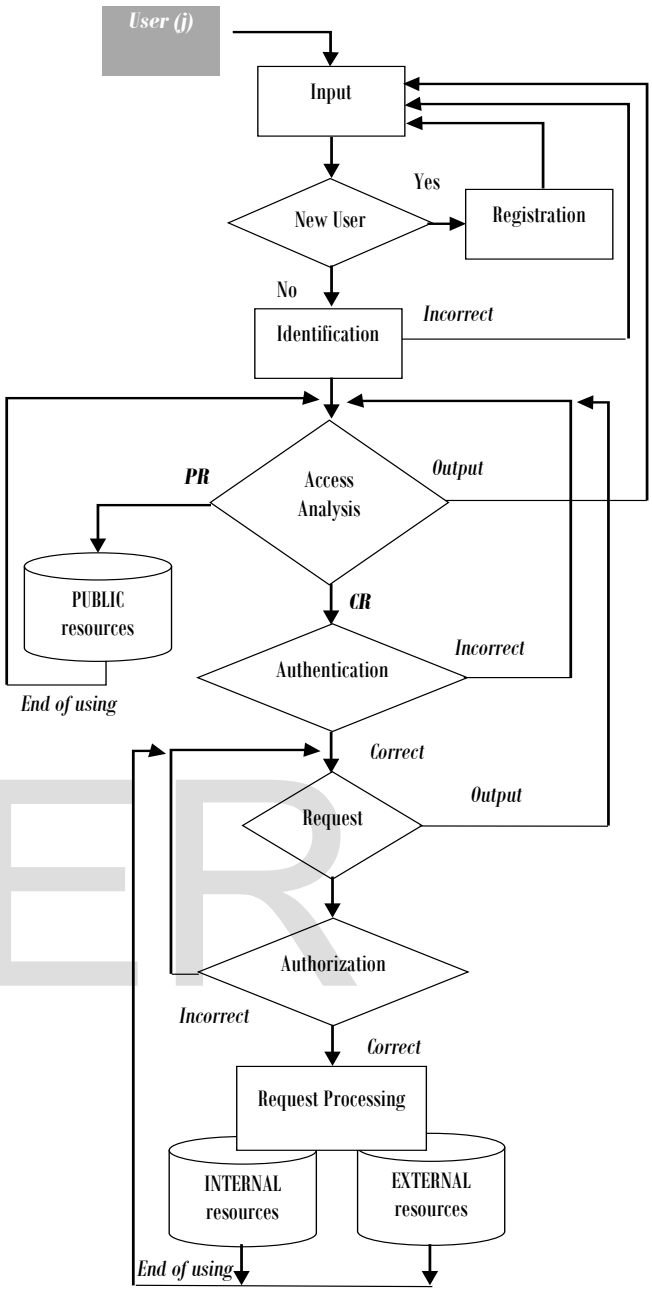


Fig. 3. Algorithmic scheme of processes supported by Security Information System (PR – access for using public information resource; CR – access for using corporative (private) information resource)

4 Model Definition by Using Markov Chain

An analytical model by using Markov Chain (MC) apparatus is defined. The main procedures of the security process organization are described as basic states and they determine the discrete set $S=\{s_j/j=1\div11\}$. The separate states are listed below.

s_1 – remote access to the input point;

s_2 – procedure for registration of a new user;

s_3 – procedure for identification of a user access to the corporative system;

s_4 – procedure for analysis the type of the required access to the corporative resources after input in the back office of the e-servicing corporative system;

s_5 – realization of a process for using a public resource which is unlimited without restriction;

s_6 – procedure for authentication of the user based on information from the personal profile created by the DRMS;

s_7 – procedure for analysing user's request for access to the private information and system resources;

s_8 – procedure of authorization based on information about user's rights defined by DRMS;

s_9 – process for realization of the user's request after successful authorization; the access could be performed into one of the following two directions;

s_{10} – access and using internal corporative information resources;

s_{11} – access and using external corporative information resources.

The last three states are connected with the transitions ($s_9 \rightarrow s_{10}$) and ($s_9 \rightarrow s_{11}$) with probabilities (p_{9_10}) + (p_{9_11}) = 1. This permits to unite these states and they could be regarded as a common state presented by s_9 only. Based on this acceptance the model shown in Fig. 4 is proposed as a graph of states and developed on the base of the definition:

- Set of discrete states $\boldsymbol{S} = \{s_j / j=1\div11\}$;
- Matrix of the transition probabilities $\mathbf{P}=\{p_{ij}\}$ – see table 1;
- Vector of initial probabilities $\mathbf{P}_0=<1, 0, 0, \ldots, 0>$.

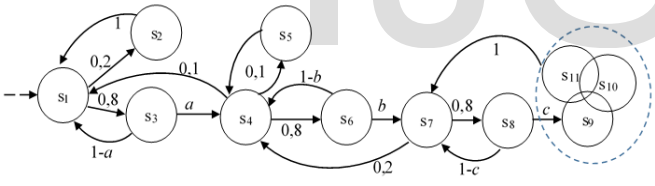


Fig.4.Graph of the states for the defined model as a Markov's chain

TABLE 1
MATRIX OF TRANSITION PROBABILITIES
(THE STATES '10' AND '11' ARE MARKED BY GREY COLOUR BECAUSE THEY ARE UNITED WITH THE STATE '9')

	1	2	3	4	5	6	7	8	9	10	11
1		0,2	0,8								
2	1										
3	1-*a*			*a*							
4	0,1				0,1	0,8					
5				1							
6				1-*b*			*b*				
7				0,2				0,8			
8							1-*c*		*c*		
9							1			0,6	0,4
10									1		
11							1				

Some additional hypotheses are accepted for development of the model:

(1) The probability for correct realization of security procedures (identification, authentication, authorization) at all levels is 0,8;
(2) The probability of access to public resources is very low and it is accepted that the value is $p(s_4 \rightarrow s_5)$=0,1; the same probability is accepted for the finalization of the work by using system components of back office sub-system $p(s_4 \rightarrow s_3)$;
(3) The important probabilities for main security procedures realization are defined as parameters: a – probability for correct realization of the identification procedure; b – probability for successful authentication of the user; c – probability for correct realization of the authorization procedure and permitted access to the corporative resources.
(4) After finishing the work with the selected corporative resource the system directs the access to the previously state for new analysis of the next request $p(s_{10}/s_{11} \rightarrow s_7)$ =1 with a possibility to finish the work (transition to the state s_4 and next transition to s_1).

Analytical definition of the model:

$$(1): p_1 = p_2 + (1-a).p_3 + 0{,}1.p_4$$
$$(2): p_2 = 0{,}2.p_1$$
$$(3): p_3 = 0{,}8.p_1$$
$$(4): p_4 = a.p_3 + p_5 + (1-b).p_6 + 0{,}2.p_7$$
$$(5): p_5 = 0{,}1.p_4$$
$$(6): p_6 = 0{,}8.p_4$$
$$(7): p_7 = b.p_6 + (1-c).p_8 + p_9$$
$$(8): p_8 = 0{,}8.p_7$$
$$(9): p_9 = c.p_8$$
$$(10): \sum_{j=1}^{9} p_j = 1$$

The equation (7) is defined based on uniting the states p_9, p_{10}, and p_{11} that permits to accept '$p_9=p_{10}+p_{11}$'.

5 ANALYTICAL SOLUTION OF THE MODEL

Two different solutions of the defined analytical model are made – solution based on probability p_1 and solution based on probability p_4. These two separate and independent solutions gave equivalent results. In this reason only first solution with analytical presentation of the probabilities by using p_1 is presented below.

The equations (2) & (3) presents the probabilities p_2 and p_3 as a function of p_1. Equation (4) permits to obtain the analytical presentation of p_4:

$$p_4 = a(0{,}8.p_1) + (0{,}1.p_4) + (1-b)(0{,}8.p_4) + 0{,}2.p_7$$

Equations (9) & (8) & (7) permit to make the presentation:

$$p_9 = c.p_8 = c.(0{,}8.p_7)$$
$$p_7 = b.(0{,}8.p_4) + (1-c)p_8 + c.p_8 =$$
$$= 0{,}8.b.p_4 + p_8 - c.p_8 + c.p_8 =$$
$$= 0{,}8.b.p_4 + 0{,}8.p_7 \Rightarrow p_7 = 4.b.p_4$$

After substitution in the equation for p_4:

$$p_4 = 0{,}8ap_1 + 0{,}1p_4 + (1-b).0{,}8p_4 + 0{,}2(4bp_4)$$
$$p_4 - 0{,}1p_4 - 0{,}8p_4 + 0{,}8bp_4 - 0{,}8bp_4 = 0{,}8ap_1$$
$$\Rightarrow p_4 = 8.a.p_1$$

Finally:

$$p_1; p_2 = 0{,}2.p_1; p_3 = 0{,}8.p_1; p_4 = 8.a.p_1;$$
$$p_5 = 0{,}8.a.p_1; p_6 = 0{,}8(8.a.p_1) = 6{,}4.a.p_1;$$
$$p_7 = 4.b.(8.a.p_1) = 32.a.b.p_1;$$
$$p_8 = 0{,}8.(32.a.b.p_1) = 25{,}6.a.b.p_1;$$
$$p_9 = 25{,}6.a.b.c.p_1$$

And after substitution in the equation (10):

$$p_1 = \frac{1}{(2 + 15{,}2a + 57{,}6ab + 25{,}6abc)} = \frac{1}{\pi}$$

and

$$p_2 = \frac{0{,}2}{\pi}; p_3 = \frac{0{,}8}{\pi}; p_4 = \frac{8a}{\pi}; p_5 = \frac{0{,}8a}{\pi};$$
$$p_6 = \frac{6{,}4a}{\pi}; p_7 = \frac{32ab}{\pi}; p_8 = \frac{25{,}6ab}{\pi}; p_9 = \frac{25{,}6abc}{\pi}$$

6 Experiments Planning and Statistical Assessments

Range [0,7 ÷ 1] is selected for the values of the parameters *a*, *b* and *c* based on assumption that the level of unregistered and illegitimate users us no more than 30%. Full experimental plan is selected. Set {0,7; 0,8; 0,9; 1,0} is determined for the three parameters to minimize number of experimental combinations of values for final probabilities calculation (Fig.5).

a	b	c	p_1	p_2	p_3	p_4	p_5	p_6	p_7	p_8	p_9	total	p_{10}	p_{11}
0,85	0,85	0,85	0,0138	0,0028	0,0111	0,0941	0,0094	0,0753	0,3200	0,2560	0,2176	1,0000	0,1305	0,0870
1,0	1,0	1,0	0,0100	0,0020	0,0080	0,0797	0,0080	0,0637	0,3187	0,2550	0,2550	1,0000	0,1530	0,1020
0,9	1,0	1,0	0,0110	0,0022	0,0088	0,0795	0,0080	0,0636	0,3180	0,2544	0,2544	1,0000	0,1527	0,1018
0,8	1,0	1,0	0,0124	0,0025	0,0099	0,0793	0,0079	0,0634	0,3171	0,2537	0,2537	1,0000	0,1522	0,1015
0,7	1,0	1,0	0,0141	0,0028	0,0113	0,0790	0,0079	0,0632	0,3160	0,2528	0,2528	1,0000	0,1517	0,1011
1,0	0,9	1,0	0,0109	0,0022	0,0087	0,0869	0,0087	0,0695	0,3128	0,2502	0,2502	1,0000	0,1501	0,1001
0,9	0,9	1,0	0,0120	0,0024	0,0096	0,0867	0,0087	0,0693	0,3120	0,2496	0,2496	1,0000	0,1498	0,0998
0,8	0,9	1,0	0,0135	0,0027	0,0108	0,0864	0,0086	0,0691	0,3111	0,2489	0,2489	1,0000	0,1493	0,0995
0,7	0,9	1,0	0,0154	0,0031	0,0123	0,0861	0,0086	0,0689	0,3099	0,2479	0,2479	1,0000	0,1487	0,0992
.....														
1,0	0,8	0,7	0,0129	0,0026	0,0103	0,1031	0,0103	0,0825	0,3298	0,2639	0,1847	1,0000	0,1108	0,0739
0,9	0,8	0,7	0,0143	0,0029	0,0114	0,1028	0,0103	0,0822	0,3289	0,2631	0,1842	1,0000	0,1105	0,0737
0,8	0,8	0,7	0,0160	0,0032	0,0128	0,1024	0,0102	0,0819	0,3277	0,2622	0,1835	1,0000	0,1101	0,0734
0,7	0,8	0,7	0,0182	0,0036	0,0146	0,1019	0,0102	0,0816	0,3262	0,2610	0,1827	1,0000	0,1096	0,0731
1,0	0,7	0,7	0,0143	0,0029	0,0114	0,1142	0,0114	0,0913	0,3197	0,2558	0,1790	1,0000	0,1074	0,0716
0,9	0,7	0,7	0,0158	0,0032	0,0126	0,1138	0,0114	0,0911	0,3187	0,2550	0,1785	1,0000	0,1071	0,0714
0,8	0,7	0,7	0,0177	0,0035	0,0142	0,1134	0,0113	0,0907	0,3174	0,2540	0,1778	1,0000	0,1067	0,0711
0,7	0,7	0,7	0,0201	0,0040	0,0161	0,1128	0,0113	0,0902	0,3158	0,2527	0,1769	1,0000	0,1061	0,0707

Fig. 5. Experimental data (full factor experiment for selected values)

The last two columns consist of the values calculated for the probabilities p_{10} and p_{11} based on the assumption in section 4 for their uniting with p_9. For the case study in fig. 4 it is accepted that $p(s_9 \rightarrow s_{10})$=0,6 and $p(s_9 \rightarrow s_{11})$=0,4, but their values could vary during extended experimentation.

The first row in fig. 5 presents average state of the controlled parameters *a*=*b*=*c*=0,85 and the calculated assessments for the final probabilities are presented in fig. 6.

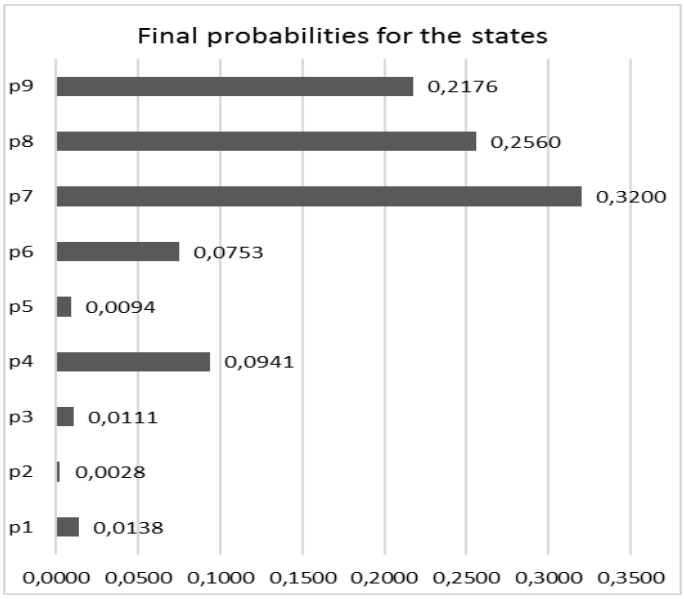
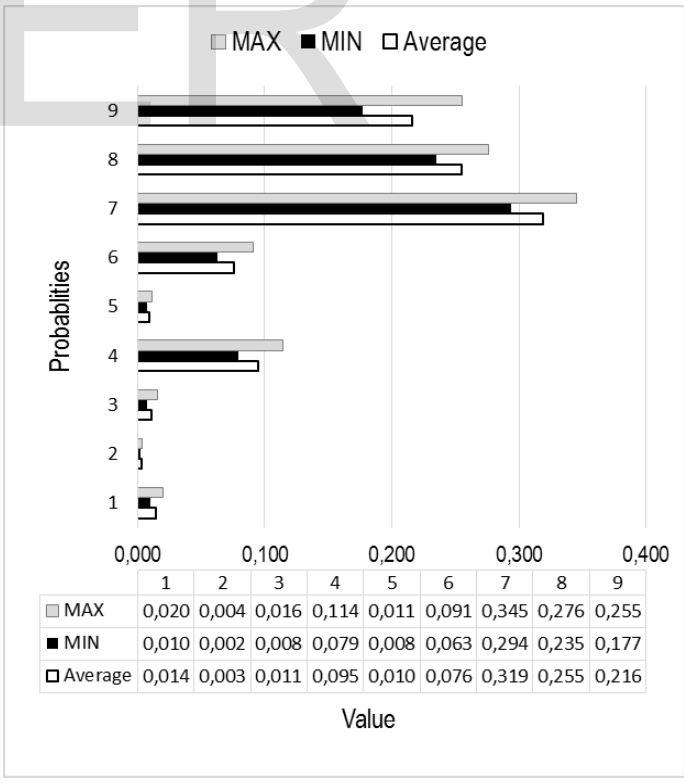


Fig. 6. Final probabilities assessments for an average case (a=b=c=0,85)

Some basic descriptive statistics are calculated and they are shown in Fig. 7 both - as a column diagram and as a table of values.



	1	2	3	4	5	6	7	8	9
MAX	0,020	0,004	0,016	0,114	0,011	0,091	0,345	0,276	0,255
MIN	0,010	0,002	0,008	0,079	0,008	0,063	0,294	0,235	0,177
Average	0,014	0,003	0,011	0,095	0,010	0,076	0,319	0,255	0,216

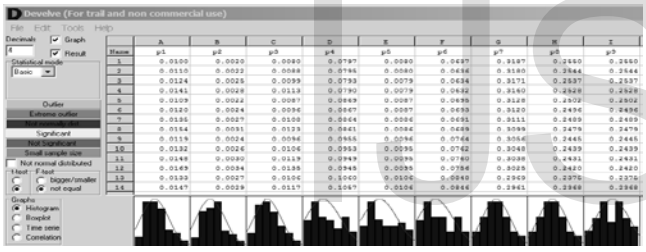
Fig. 7. Basic statistic assessments based on the experimental data

An additional statistical analysis is carried out by using Sta-

TABLE 2
STATISTICAL ASSESSMENTS FOR THE FINAL PROBABILITIES CALCULATED ON THE BASE OF OBTAINED EXPERIMENTAL DATA

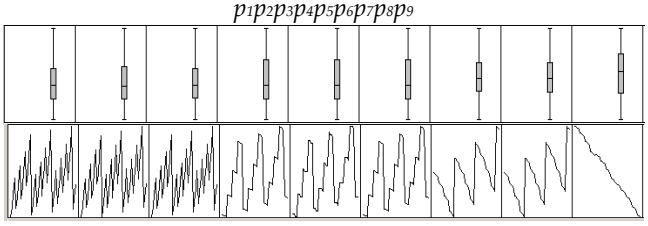
$p_1p_2p_3p_4p_5p_6p_7p_8p_9$									
Max	0.0196	0.0039	0.0157	0.1113	0.0111	0.0891	0.3461	0.2761	0.2560
Min	0.0100	0.0020	0.0080	0.0790	0.0079	0.0632	0.2986	0.2349	0.1922
Mean	0.0139	0.0028	0.0111	0.0935	0.0094	0.0748	0.3167	0.2534	0.2244
Median	0.0136	0.0027	0.0109	0.0912	0.0091	0.0730	0.3171	0.2537	0.2250
STDEV	0.0024	0.0005	0.0019	0.0101	0.0010	0.0081	0.0127	0.0102	0.0186
Kurtois	-0.456	-0.539	-0.441	-1.174	-1.170	-1.172	-0.402	-0.404	-1.124
Skewness	0.463	0.434	0.469	0.315	0.318	0.314	0.319	0.317	-0.034
Normality A^2	0.358	0.462	0.362	1.034	1.062	1.028	0.266	0.263	0.507
Normality p	0.44	0.25	0.43	0.00	0.00	0.00	0.68	0.69	0.19

tistical software *Develve* [6] giving results which are presented and discussed below. The main screen which imported all calculated values for the final probabilities is shown in Fig. 8. This set of probabilities is processed by Develve and graphical interpretation of histograms, boxplots and time series are shown in Fig.8. Additional statistics are calculated and presented in Table 2.



Histograms

$p_1p_2p_3p_4p_5p_6p_7p_8p_9$



Boxplots and time series for the final probabilities

Fig. 8. Graphical interpretation of statistical assessments obtained by using statistical software DEVELVE

7 CONCLUSION AND FUTURE WORK

This article presents an investigation focused on efficiency of procedures supported by the main modules in a corporative system for secure access where different information resources are used. It is well known that all public resources usually allow free access and using, but private (corporative) resources need strong technical and organizational measures, including means and tools for information security management. In this reason we propose two separate sub-systems. The first one (Front office) deals with preliminary registration and identification of the users. The second sub-system (Back office) which is supported by DRMS is responsible for the rest administrative procedures – personal data protection, authorization and authentication.

The apparatus of Markov chains permits to realize an investigation based on stochastic approach. In this reason an analytical model is defined and used to collect and analyse experimental data for different situations by varying three controlled parameters on the base of controlling the experimental plan as a whole. Additional assessments and statistics are calculated by using Excel and the statistical software Develve. The final probabilities p_3, p_6 and p_8 are connected with the procedures of identification, authentication and authorization. The experimental results permit to analyse means, medians, standard deviation and other assessments that allow to make conclusion about efficiency level of secure access to the corporative resources.

This investigation could be enhanced by extending the stochastic modelling by using Markov chain or by additional simulation which will be the future work of the authors

ACKNOWLEDGMENT

The research is with the support of project DH-07/10 funded by Bulgarian Ministry of Education and Science.

REFERENCES

[1] R. Romansky, "Digital Privacy in the Network World", *Proc. of the 28th International Conference on Information Technologies*, *St. St. Constantine and Elena, Bulgaria*, 2014, pp.273-284.

[2] A.E. Fischer, "Improving User Protection and Security in Cyber-Space", *Report of Committee on Culture, Science, Education and Media, Council of Europe*, http://www.statewatch.org/news/2014/mar/coe-parl-ass-cyberspace-security.pdf, 12.03.2014.

[3] Teacher Resource Bank. *GCE Information and Communication Technology. INFO3. Definition of a Corporative Information System*, 2010.http://filestore.aqa.org.uk/subjects/AQA-2520-W-TRB-U03DFINFO3.PDF

[4] "*Information Systems Security Line of Business*", The Federal Government's Information Systems Security Program, Homeland Security,USA, 14.10.2015, https://www.dhs.gov/information-systems-security-line-business

[5] S. Park and K. Lee,"Advanced Approach to Information Security Management System Model for Industrial Control System". *The Scientific World Journal*, July 2014, Article ID 348305, 13 p.

[6] Develve Statistical Software for Quality Improvement, Design of Experiments (DOE), http://develve.net

[7] ISACA. *An Introduction to the Business Model for Information Security*, USA, 2009, 28 p. https://www.isaca.org/knowledge-center/bmis/documents/introtobmis.pdf

[8] Whatis.com, *Information Security Management System (ISMS)*, 2011http://whatis.techtarget.com/definition/information-security-management-system-ISMS

[9] Z. V. Rodionova and L. K. Bobrov. "Protection of the information resources of a library based on analysis of business processes". *Scientific and Technical Information Processing*, vol. 43, no.1, 2016, pp.20-27. http://link.springer.com/article/10.3103%2FS0147688216010032

[10] St. Fenz, J. Heurix, T. Neubauer, and F. Pechstein. "Current chal-

lenges in information security risk management", *Information Management & Computer Security*, vol. 22, no. 5, 2014, pp.410-430. Available at: http://www.emeraldinsight.com/doi/abs/10.1108/IMCS-07-2013

[11] A. Ashok, A. Hahn, M. Govindarasu. Cyber-physical security of wide-area monitoring, protection and control in a smart grid environment. *Journal of Advances Research*, vol. 2, no.5, 2014, pp.481-489.

[12] R. Ghosh, "Scalable analytics for IaaS cloud availability", *IEEE Transactions on Cloud Computing*, vol. 2, no. 1, 2014, pp.57-70.

[13] D. Bruneo,"A Stochastic Model to Investigate Data CentrePerformance and QoS in IaaS Cloud Computing Systems", *IEEE Transactions on Parallel and Distributed Systems*, vol. 25, no.3, 2014, pp.560-569.

[14] R. Romansky and I. Noninska, "Discrete Formalization and Investigation of Secure Access to Corporative Resources",*International Journal of Engineering Research and Management*, vol. 3, no.5, 2016, pp.97-101, Available: http://www.ijera.com/