Journal of Theoretical and Applied Information Technology
31st December 2015. Vol.82. No.3

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

RESEARCH OF PROCESSES OF IDENTIFICATION, AUTHENTICATION AND AUTHORIZATION

[1]AMANZHOLOVA S.T., [2]KALIZHANOVA A.U., [3]SHAIKULOVA A.A., [4]KOZBAKOVA A. KH.
[1,2,3,4]Kazakh National Research Technical University named after K.I. Satpayev
E-mail: [1]shokataeva@gmail.com, [2]kalizhanova_aliya@mail.ru, [3]shaikulova_ak_al@mail.ru, [4]ainur79@mail.ru.

ABSTRACT

The article herein considers the issues of users' identification. Aspects connected with identification, authentication and authorization are represented in the form of mathematical systems of queuing. The article uses single-channel two-phase and three-phase models. Simulation modeling is performed in the language GPSS World.

Keywords: *Mathematical Modeling, Two-Phase Modeling, Three-Phase Modeling, Simulation Modeling, Identification, Authentication, Authorization.*

1. INTRODUCTION

As it is known, mathematical modeling allows tracing the processes in any information processing systems. By means of analytical modeling we can obtain exact solutions, particularly it concerns the complex computer processes. Processes going on upon information security can as well be analyzed by means of mathematical modeling. Analytical modeling can be researched with following methods:

1) analytical, when it is necessary to obtain decisive constraints for system features in general;

2) numerical, when it is not probable to find equation solution in general and they are solved for definite initial data;

3) qualitative, when at the solution absence some of its properties can be found.

Analytical models can be obtained merely for comparatively simple systems. For complicated systems there often arise big mathematical problems. To apply analytical methods it is necessary to simplify initial model sufficiently. However, research on simplified model helps obtain only approximate results. Analytical models correctly reflect the link between input and output variables and parameters. However, their structure does not reflect the object's inner structure.

For instance, it is possible to apply common and widely known single- channel two-phase model for elaboration of users identification and authentication processes as well authorization one. Mathematical model for identification and authentication processes consideration can assume exponential nature of inquiries input into system, as commonly all computer systems have random nature of inquiry entry for identification. Mathematical model's first phase will represent users identification process, the second one is an authentication process. The sequential queue between the first and second phases will be bounded. Users' inquiries enter into the system with λ force. Prior to authentication phase there is assumed an endless inquiry queue. To calculate the model we shall define b_1 and b_2.

where b_1 is the service function in the first phase

where b_2 is the service function in the second phase.

In the model herein the first phase is the identification phase, the second phase is authentication phase (Figure 1.)

The scheme herein can be presented as a two-phase model:

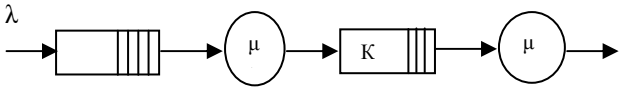


Figure 1 – A Single Channel Two- Phase Identification And Authentication Model

To avoid inquiries loss due to overflow of the buffer, there is introduced blocking state, which the system transfers to in non-availability of space in the second phase buffer. Exit from that state occurs in case of unbuffer in the second phase.

To exclude the input stream of inquiries from the analysis there is assumed availability of

Journal of Theoretical and Applied Information Technology
31st December 2015. Vol.82. No.3

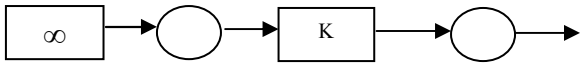
ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

infinite queue of requests in the input buffer (Figure 2.)

In that case, we assess two situations:

1) Serviced and blocked applications are in the devices of appropriate phases;

2) In the phases there do not exists posts for serving and blocked application.



μ_1 μ_2

Figure 2 – Identification And Authentication Model

where $\mu_1 = \frac{1}{b_1}$ (1)

$$\mu_2 = \frac{1}{b_2} \quad (2)$$

Let us introduce following designations for more detailed model description:

$P_{ij}(n)$ –system state probability where first phase state is characterized by index i, and second phase state is characterized by index j,

n – applications quantity in the second phase buffer is n=0÷k.

The first phase can accept the value i= {1,β}, the second phase can accept the value j={0,1}

If i=1, then it means that the phase is in the serving state, if i=β, then it is the blocked state.

If j=0, then the second phase is out of action in expectation of application from the first phase, if j=1, then the second phase is in service state.

Upon analytical modeling of the queuing, it is necessary to draw up a linear complex of such system's transfer states. (Figure 3).

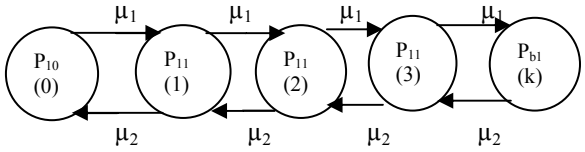


Figure 3.-Linear Complex Of Double-Phase Model Transfer States

Where $P_{10}(0)$ is system's zero state

$P_{11}(n)$ is system states at k-applications

$P_{b1}(k)$ is the last probable state of the system.

For model thereof, a balance equation is correct

$$\mu_1 P_{10}(0) = \mu_2 P_{11}(1)$$
$$(\mu_1 + \mu_2) P_{11}(1) = \mu_1 P_{10}(0) + \mu_2 P_{11}(2)$$
$$(\mu_1 + \mu_2) P_{11}(n) = \mu_1 P_{11}(n-1) + P_{11}(n+1), n = \overline{1,k}$$
$$\ldots$$
$$\mu_2 P_{B1}(K) = \mu_1 P_{11}(K-1)$$

With normalization requirement

$$P_{10}(0) + P_{B1}(K) + \sum_{n=1}^{K-1} P_{11}(K) = 1 \quad (4)$$

From that condition of normalization requirement we can find the probability $P_{10}(0)$

$$P_{10}(0) = \left[\sum_{r=0}^{k} \rho^r \right]^{-1} \quad (5)$$

and remained probabilities from recurrence formula

$$P_{11}(n) = \rho^n \cdot P_{10}(0) \quad (6)$$

$$P_{11}(n) = \rho^k \cdot P_{10}(0) \quad (7)$$

Two-phase model characteristic

Use factor of the first and second phases:

$$\eta_1 = 1 - P_{\beta 1}$$
$$\eta_2 = 1 - P_{10} \quad (8)$$

Where $P_{\beta 1}$ – first phase blocking probability.

System capacity equals to $\varpi = \mu_1 \eta_1 = \mu_2 \eta_2$

Average delay in queue in the second phase buffer is calculated from the formula

$$m = \sum_{r=2}^{k-1} (r-1) \cdot P_{11}(r) + P_{\beta 1}(K-1) \cdot P_{\beta 1}(K) \quad (9)$$

Average delay in queue

$$q = \sum_{r=1}^{k-1} r \cdot \nu_2 P_{11}(r) + k \cdot \nu_2 P_{\beta 1}(k). \quad (10)$$

Average time in system:

$$U = \frac{1}{\varpi} + q + \nu_2 \quad (11)$$

where $\nu_2 = \frac{1}{\mu_2}$ - application average maintenance time in the first phase,

$\frac{1}{\varpi}$ - application average stay duration in the first phase.

That, in its turn, is combined from average maintenance time

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

$\nu_1 = \frac{1}{\mu_1}$ and blocking $\tau_{\beta 1}$ applications in the first phase, i.e. $\frac{1}{\omega} = \nu_1 + \tau_{\beta 1}$.

Based on calculated features we can assess the system behavior in actual conditions.

Analyzing information security tasks properties and requirements to its model, it can be concluded that considered general case information security model shall possess following properties: on a scale of simulated processes to be in accord within formation security maintenance on the state, region, district or separate generalized protection object scale. i.e. shall be universal; according to simulated process interpretation it shall be scholastic [6]; according to simulation method — in the form of analytical and logical correspondences; according to the current task — optimizing; as intended — research, staff and training. Denoted properties can be possessed by general mathematical model, instantiated, according to the investigation method, as imitative-heuristic and according to the solution method, as functional-logistic.

The model is used upon developing information security concept at decision making, in planning process, information security threat prevention and neutralization.

Model serves for analysis and assessment of the state's (society) information media threats sources, calculation and selection of the best information security strategy per quality target value and its performance evaluation. Information security strategy is regarded as methods of the state's (society) information media threats sources assessment, security objects selection, rational application of information security forces and means (repellents), order and methods of their usage, forecasting potential move and information security problem solution outcome, performance assessment.

Upon testing the model herein, the program in simulating modeling GPSS World language can be written.

Figure –4.Program Code In GPSS World

After program start-up there is obtained a standard report presented on Figure 5.

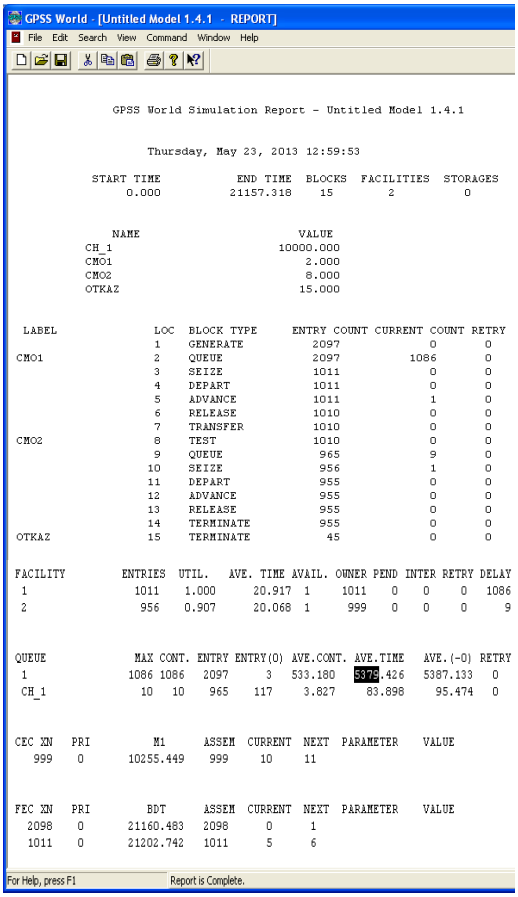


Figure – 5.Outcome Of The Program In GPSS World (Tracking)

Tracking contains following key information.

Column ENTRY_COUNT (inputs meter) shows amount of transacts during simulating every

Journal of Theoretical and Applied Information Technology
31st December 2015. Vol.82. No.3

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

model block [7]. Thus GENERATE module outputs is 2097 transacts, it is the number of terminal users, having come to identification and authentication. 45 transacts have been destroyed on module FAULT. It is the number of terminal users, not having come to identification and authentication. From here, we can find the assessment of failure chances:

Pfault. = 45/2097 = 0,022.

From mathematical point of view subscribers appearance process represents the events recurrent flow [8]. Applying appropriate mathematical knowledge we can see overall amount of incoming subscribers, i.e., number 2097 is random. In the same way faults number 45 represents only one of potential random implementations, i.e., quite inaccurate value. As well applying the analysis of stationery probabilistic characteristics convergence evaluations we can conclude that cumulative failure frequency obtained above and equal to 0,022 is of quite high precision. At least, it can be predicated, that all three figures, subsequent to the comma, are proximate.

In column CURRENT_COUNT (currents meter) there is shown amount of transacts delayed in each module upon models shutdown.

Queues statistics contains a table with main data on every queue in the model.

Column QUEUE contains queue number or name.

Column MAX (maximum) contains queue maximum length achieved within overall modeling process. Naturally, that in our model the queue length could not exceed 1086.

Column CONT (content) shows queue current length at model shutdown.

Column ENTRIES contains transacts amount entered the queue.

In column AVE.CONT (average content) there is obtained the average queue length. The column with a title AVE.TIME contains transact passing average time through a queue. Nearest-neighbor column AVE.(-0) shows the same average time, but rated only for transacts, having passed the queue for non-zero time, i.e. actually delayed in the queue.

At set-up parameters the average length of users' queue to identification and authentication processes comprises 533,18 users per first phase and 3,827 in the second phase, expected waiting time of serving commencement equals to 5379,426 minutes in the first phase and 83,898 minutes in the second phase.

Only title UTIL shall be clarified separately. Under the title, herewith there is defined storage-utilization factor. Contrary to the device, capacity factor it represents, not the share of the time, within which memory has been occupied, but an average memory of memory content divided by capacity. That coefficient is also rated, i.e. being always within limits from 0 to 1.

Use factor appeared equal to 1 per the first phase and 0,907 per the second phase. It means, that the first phase in average 100% of time is occupied and therefore, shall be unloaded. And the second phase for 90, 7% time is occupied with direct serving the users.Maybe such mode intensively loads a processor.

Consequently, having simulated the model herein and obtained modeling outcomes, it can be said with certainty, that the system herein is optimal for simultaneous inquiring of 1000 users to the system to get an access to resources.

Provided authorization processes shall be accounted apart from identification and authentication, there can be applied a single-channel, three-phase model. Let us consider a simple three-phase model. First phase is identification, second phase is authentication and third one is authorization. This model is with continued buffer prior to the first phase, the input of which receives the simplest force flow λ, and service time in every separate phase out of three, has exponential with parameter μ. It is supposed that simultaneously the system can serve only one inquiry. Merely upon completion of the inquiry passing along overall chain of devices, the next inquiry can be selected for service.

Use factor in such model is defined per formula:

$$\rho = \frac{3\lambda}{\mu} \quad (12)$$

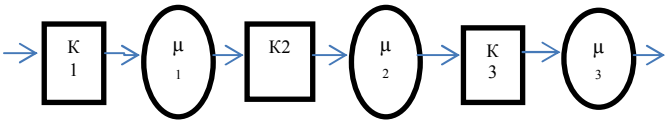


Figure 6- Single-Channel, Three-Phase Model Of Identification, Authentication And Authorization

μ_1 – inquiries processing force in the first phase (identification), μ_2 – inquiries processing force in the second phase (authentication), μ_3 – inquiries processing force in the third phase (authorization).

In order to reveal features of the model herein we shall, as well as for the two-phase model, draw up transfer state graph. Upon drawing up the network, let orientate at transfers with help of $\mu_{i\_}x$, see figure 7.

Journal of Theoretical and Applied Information Technology
31st December 2015. Vol.82. No.3

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

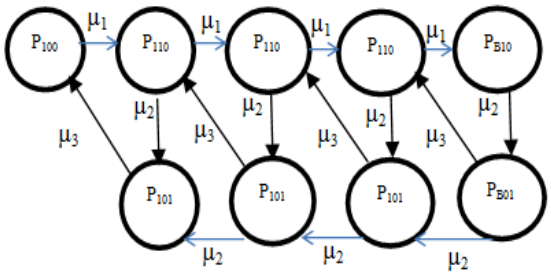


Figure 7 – Network Of Three-Phase Single-Channel Model Transfer States.

Where P_{100} – system's initial state, inquiry entered the first phase, other phases are in waiting mode, P_{110} – inquiry entered the second phase, at that, there are no inquiries in the third phase yet, P_{B01}- first phase blocking, as the queue to it is restricted, P_{101}- inquiry moved from the second phase to the third one, P_{B01} – inquiry is in the third phase, at that the third phase is blocked, as the queue is limited.

In this case, we can use previous two-phase model uniting either «identification» and «authentication» processes or «authentication» and «authorization» ones to obtain features, usual for us. Generally upon the processes of entering the system, users pass faster «identification» и «authentication» processes, as for «authorization» process it takes longer time (it might be digital code generation time or respond to secret question known to the user. Therefore, we can replace three-phase model by two-phase model and unite «identification» and «authentication» processes, see figure 8.

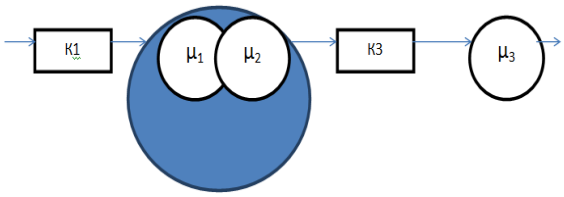


Figure 8 – Two-Phase Single-Channel Model.

Where μ_{12}- pooled force of first phase service (identification + authentication).

$$\mu 12 = \frac{1}{\nu 12} \quad (12)$$

$$\nu 12 = \frac{\mu 1 + \mu 2}{\mu 1 * \mu 2} \quad (13)$$

$$\rho = \frac{\mu 12}{\mu 3} \quad (14)$$

ρ – use factor of the model herein.

Remained model features will be the same as in the previous two-phase model.

μ1 μ2 Having tested three-phase model herein by means of simulation modelling in language GPSS World we obtain following outcomes.

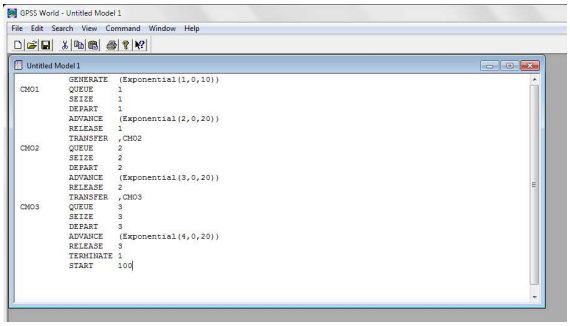


Figure – 9. Outcome Of Program In GPSS World For 100 Inquiries

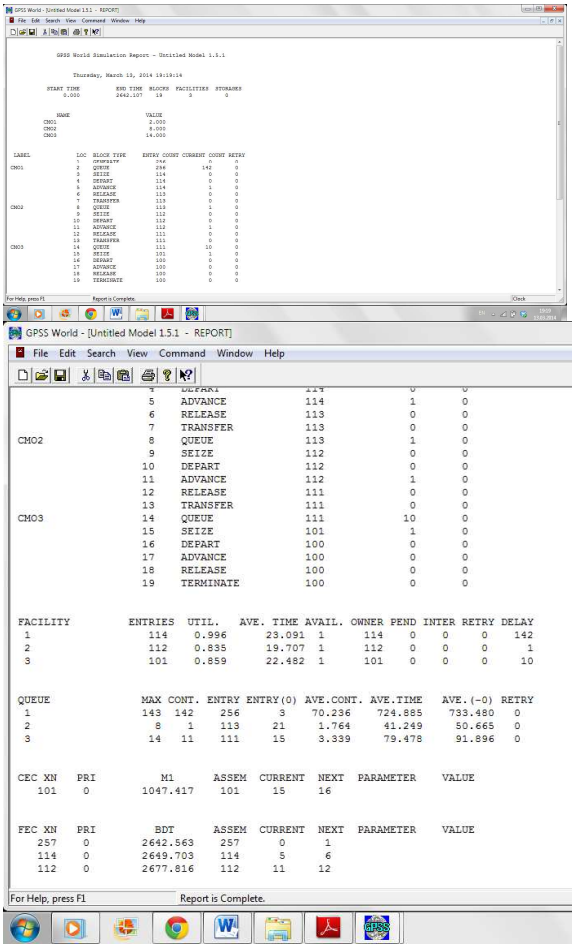


Figure – 10. Outcome Of Program In GPSS World (Tracking) 1000inquiries

Journal of Theoretical and Applied Information Technology
31st December 2015. Vol.82. No.3

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

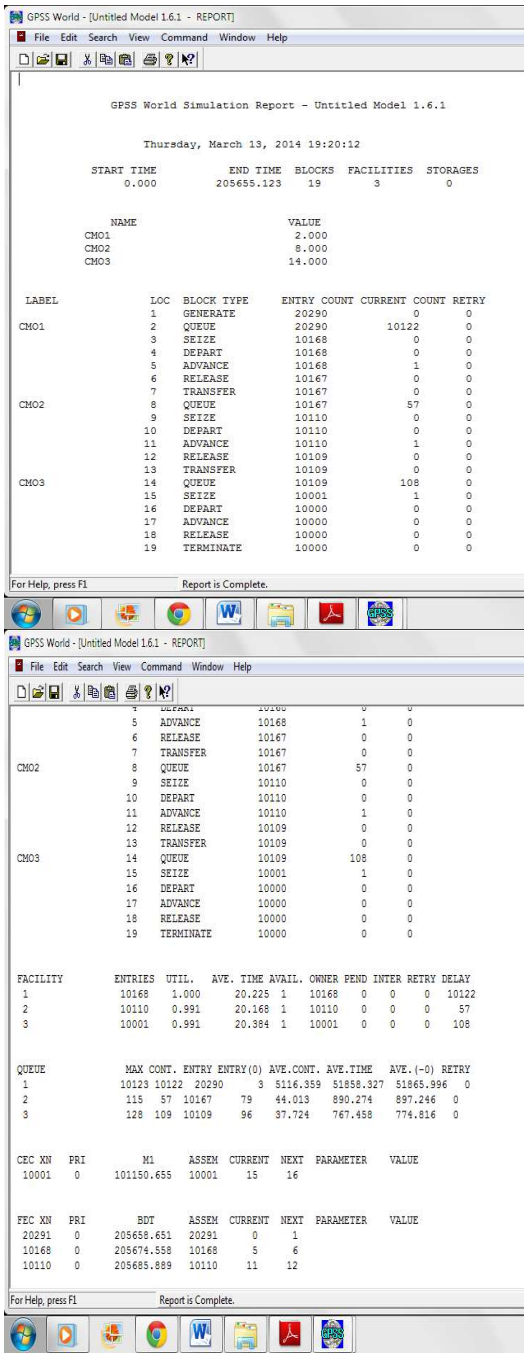


Figure – 11.Outcome Of Program In GPSS World (Tracking) 10000 Inquiries

Upon researching 1000000 inquiries, modeling time has increased, see figure 12.

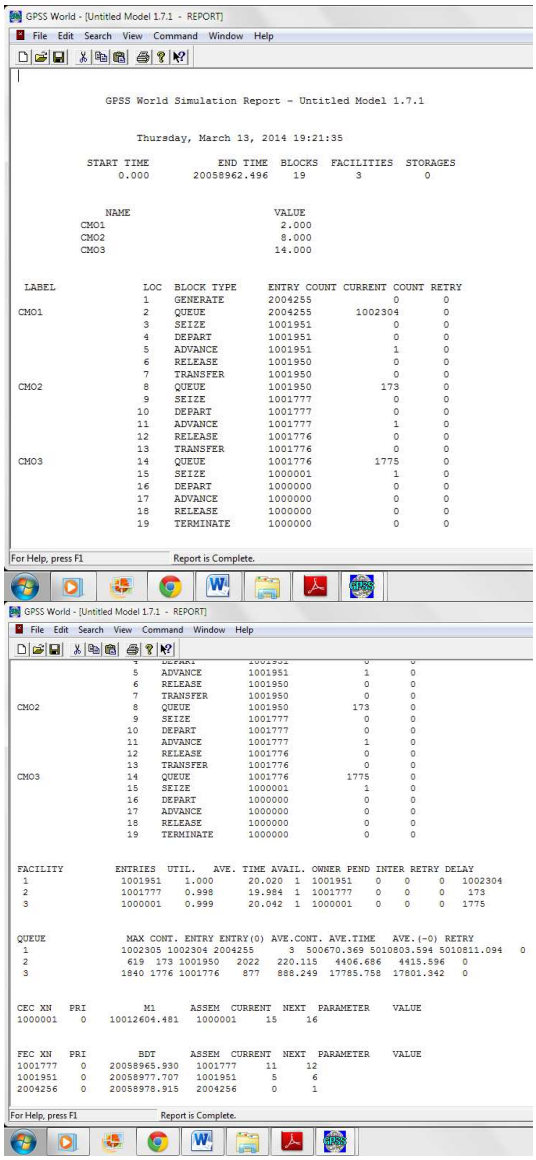


Figure – 12.Outcome Of Program In GPSS World (Tracking) 1000000 Inquiries

Thus, having tested three-phase model we can say that identification, authentication and authorization processes are impossible upon over 1000000 simultaneous users' inquiries, therefore, there shall always be considered the opportunity to address different computer resources, operating in parallel mode.

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

REFRENCES:

[1] Common Concepts Underlying Safety, Security, and Survivability Engineering. Donald G. Firesmith, December 2003.

[2] AliyevT.I. Fundamentals of sampling simulation. – Collected works: SPGUITMO, 2009. – 363 p.

[3] Amanzholova S.T., Uskenbayeva R.K. «Complex metric approach to DCS information security system arrangement», Works ofII INTERNATIONAL SCIENTIFIC-PRACTICALCONFERENCE «Information–innovation technologies :integration of science, education and business» dedicated to 20th Anniversary of RK Independence, Almaty, Kazakhstan, December1-2, 2011

[4] Security Requirements Reusability and the SQUARE Methodology. Travis Christian, Faculty Advisor.Nancy Mead September 2010 TECHNICAL NOTE CMU/SEI-2010-TN-027 CERT® Program.Unlimited distribution subject to the copyright. http://www.sei.cmu.edu

[5] YermakovA.S AmanzholovaS.T.Assessing means of keys parallel generation on «user – server» technology // International symposium «Information and system technologies in industry, education and science». – Karaganda, 2006. – p.p. 95-97.

[6] Amanzholova S.T. Comparing the means of keys parallel generation on SIMD and MIMD servers arrangements // «Information and system technologies in industry, education and science»: works of international scientific-practical conference dedicated to 75th anniversary of KazNTU named after Satpayev K.I.– 2008, November 27–28. – p.p. 307–309.

[7] YermakovA.S Amanzholova S.T. Priority service model atmagnet disc «Container cryptooperation» // KazNTU Herald. – 2009. – # 2(72). – p. 92–101.

[8] YermakovA.S Amanzholova S.T. Authentication and identification models of distributed information computer systemby the example of distance education system // NTO «KAKHAK». – 2009. – # 1 (23). – p. 11–17.

[9] Collins, A.J.; S.R. Shefrey, J. Sokolowski, C.D. Turnitsa, E. Weisel (January 2011). "Modeling and Simulation Standards Study: Healthcare Workshop report". VMASC Report, Suffolk VA.