B. H. Ismailov, Cand. Sc. (Eng), Assist. Prof.

ANALYSIS OF MODELLING RESULTS OF INFORMATION PROTECTION SYSTEM IN DISTRIBUTIVE SERVICE NETWORKS

The paper contains comparative analysis of the results of mathematic and simulation methods aimed at solution of the problem dealing with determination of optimum software-hardware structure of information protection systems. The analysis of the results shows, that they differ within the limits of 2 -10%, and the degree of adequacy of analytical model to the object under investigation increases with the decrease of network load.

Key words: *information protection system, distributive networks, modelling.*

Introduction

Comparative analysis of the results of different approaches to the solution of the problem, dealing with determination of optimum software-hardware structure of information protection systems (IPS) is carried out [1]. Such systems are created between various types of distributive networks, on one hand, and global network – on the other hand. They control and filtrate information passing through them. It is a sort of a gateway, oriented on perfporming functions of information protection of the networks. Such structure of gateways allows to reduce the threat of non-authorized access to local and distributive networks as a result of using masquerading method, when the traffic from DN is sent on behalf of IPS, making DN practically "invisible". Methods of information transfer in such systems are considered in [2 – 4].

The analysis, carried out, shows that enumeration of possible threats cannot, practically, be realized due to their larger number. That is why, on the basis of certain characteristic features, such as programmed or non-programmed actions, blockage of post-box, finding illegal ways, loading of channel, computer failure, etc. in [1] the classification of possible threats is suggested. Clasification comprises such threats as: Troian horses, viruses, messages, littering mail box, attacks, aimed at failures of service and non correctly operating programs.

The problem of identification of IPS in DN characteristics is solved on the base of the given classification of possible threats. Proceeding from practical reasons, we can assume that the amount of ill-intentioned programs (messages) accounts one third of the total amount of messages.

Distribution networks, operating in conditions of great intensity at Poisson input with group arrival, are considered in [5]. Other models, connected with development of the methods of routing and flows control are analyzed in [6]. In order to provide information security of the networks it is necessary to organize protection system, comprising modern engineering facilities [7] for control of transferred information and their complex protection against various impacts. These systems contain complex of programs, requiring certain volume of memory:

- programs, performing cryptographic ciphering of mail messages, such as Pretty Good Privacy (PGP);
- utilities, enabling to detect and eliminate "spy" programs, for instance, Ad-aware X cleaner;
- firewalls, detecting and blocking non-authorized access to computer, not allowing entering "garbage", "spyware" and "troians" on hard disk;
- antivirus programs (Antivral Toolkit, Kaspresky antivirius, Dr. Web etc) and various utilities, aimed at fighting specific viruses.

Performing of periodic analysis of IPS efficiency is one of the main tasks in DN [7]. By means of improvement and optimization of protection systems characteristics we can provide their high efficiency, difficult – to overcome even for experienced malefactor. The solution of described problems requires elaboration of corresponding mathematical problems and methods of their analysis.

In available literature the attempts aimed at solution of the above-mentioned problems are described [2-4]. They mainly use methods of information protection on the level of user's name and password, but that is not sufficient to prevent penetration in the network unauthorized users. Besides, great amount of potential channels of penetration complicates information protection in the network. Unlike the above – mentioned works, the given paper suggests alternative approach to the solution of the problem, dealing with determination of optimum hardware-software structure of IPS. This approach is based on the principles of queueing system (QS) theory, taking into account the characteristics of various treats impects on network functioning.

Aim of research

The aim of the given research is comparative analysis of the results of mathematic and simulation models of information protection system in distributive queueing systems.

Problem set-up

The problem comprises the development of efficient approach to the solution of the problem of comparative analysis of the results of computation and optimization of information protection system functional structure in DN. The following multichannnel QS, consisting of N computers may serve as mathematic model of IPS.

Computers are mainly characterized by the intensitives of service, distributed in accordance with exponential law, Poisson input of messages enters the system, its intensity being λ_P, time of service is obeyed to exponential, constant and erlang distributive laws. The arriving information is filtrated and distributed in the networks.

Operation of the network can be distributed by the malefactors and recovered by means of a complex of programs both, when message transfer is suspanded. It is supposed that while information transfer (T_{ci}), time of correct operation of the network ($T_i = 1/d_i$), time of its recover (T_{ni}) and time of information aging ($T_D = 1/\nu$) in conditions of possible threats are distributed n accordance with exponential law with parameters μ_i, c_i, d_i, ν correspondingly.

The index of efficiency is mathematic expectation of loss probability as a result of untimely distribution of messages after filtration in the computers of the network, i.e., the following problem is to solve [1]:

$$M\left[\bar{P}\right] = \min \sum_{i=1}^{N} p_i q_i \tag{1}$$

at constrains

$$1 - \sum_{i=1}^{N} p_i = 0, \quad 0 \le P_i \le \mu_i k_i / \lambda, \quad i = \overline{1, N}, \tag{2}$$

$$\text{де } \mu_i = 1/T_{ci},\ h(p) = 1 - \sum_{i=1}^{N} p_i,\ q_i(p) = p_i,\ q_2(p) = p_i \le \frac{\mu_i k_i}{\lambda}, \tag{3}$$

$$q_i = \frac{(1 - p_i \lambda h_{1i})}{(1 - p_i \lambda h_{1i} + \nu_i h_{1i}}, \ h_{1i} = \frac{1}{\mu_i k_i}, \ \nu_i = \nu\left[k_i + \frac{(1-k_i)(\nu - p_i\lambda)}{\nu(1+\nu T_{ni}}\right], \ i = \overline{1, N}. \tag{4}$$

The following symbols are assumed here: $\bar{\bar{P}}$ – probability of the loss due to untimely distribution of messages computer-wise after filtration in DN, p_i – probability of loss due to non-arrival of messages for transfer to i-$^{\text{th}}$ computer, q_i – probability of loss in i-$^{\text{th}}$ computer, due to untimely delivery of messages k_i – coefficient of radiness, T_{ni} – average dawntime.

To solve problem (1) – (4) in [1] the method of generalized gradient [8] is suggested to use, on

the base of which algorithms of calculation and optimization of IPS characteristics by chosen quality criterion. This method enables to investigate IPS behavior at any ranges of measurement of structural and loading parameters of the model.

Analysis of the results of IPS mathematic model in DN

For calculation of IPS characteristics on the base of the developed algorithm numerous computational experiments in wide ranges of both structural and loading parameters of the model. For initial data $1/\mu_i = (0{,}042;0{,}042;0{,}063)$, $k_i = (0{,}97;0{,}79;0{,}81)$, $T_n = (0{,}6;0{,}9;1{,}0)$, $\nu = 0{,}5 (T_D = 2)$ dependences $p_i = f(\lambda), i = \overline{1,3}$ are investigated. Corresponding results are shown in Fig. 1.

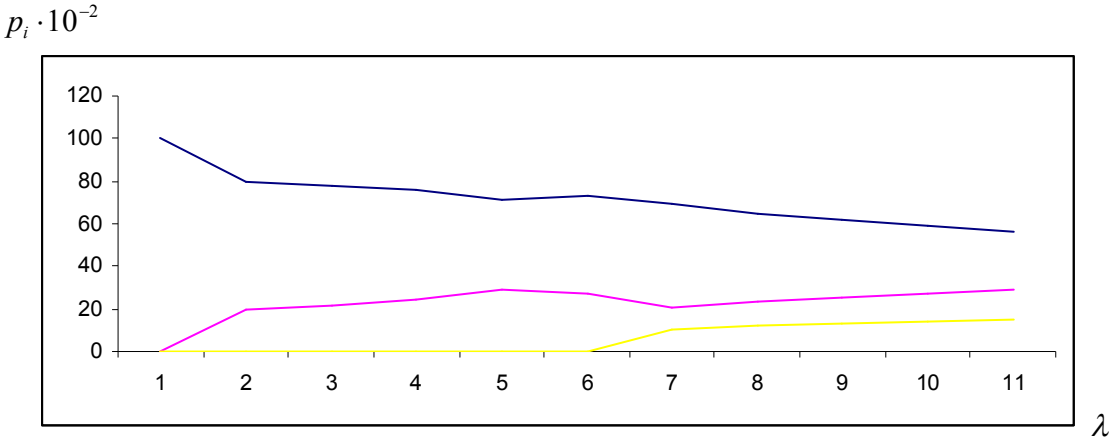


Fig. 1. Dependences $p_i = f(\lambda), i = \overline{1,3}$

Due to losses of information, shown in Fig. 1, basic characteristics of multichannel QS for exponential, constant and erlang service time. Here, main characteristics are

L_q – is queue length, L_s – is amount of messages in the system, τ_q – is waiting time of messages in the queue, τ_s – is time of messages stay in the system (Fig. 2 – 7, $a = (0{,}95;0{,}67;0{,}46)$, L_q, τ_q, – is upper line, L_s, τ_s – is lower line).

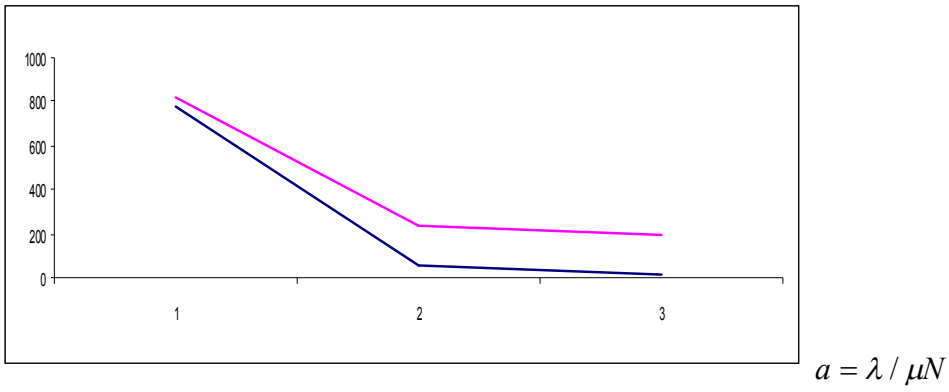
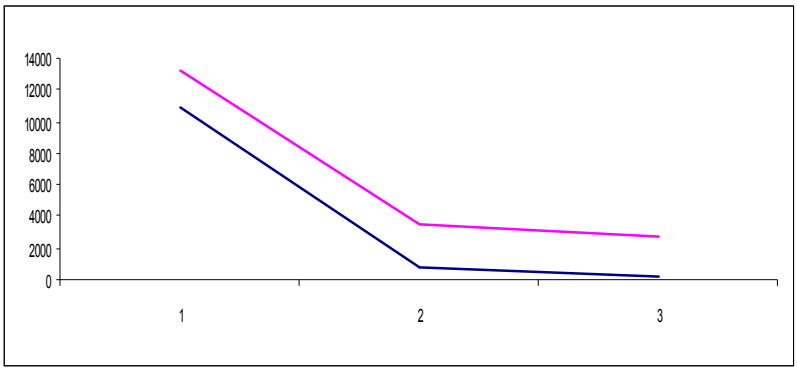


Fig. 2. Dependences $L_q = f(a)$, $L_s = f(a)$ for exponential service time

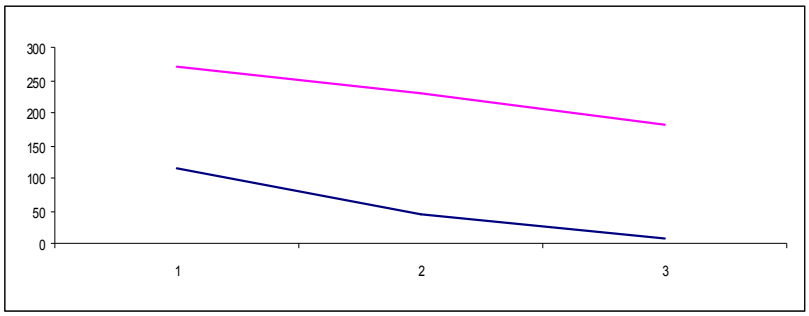
τ_q, τ_s



$a = \lambda / \mu N$

Fig. 3. Dependences $\tau_q = f(a)$, $\tau_s = f(a)$ for exponential service time

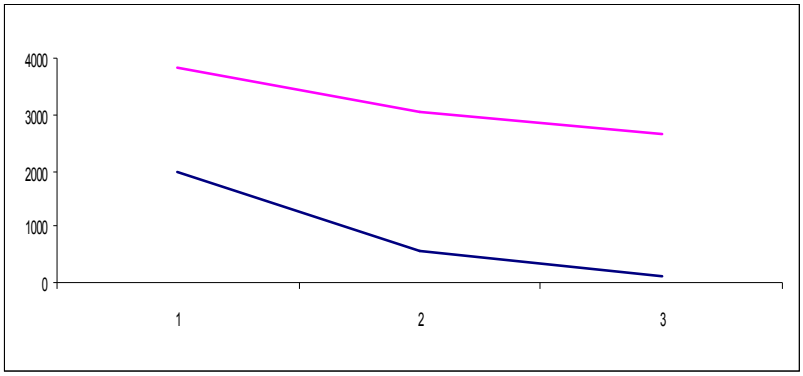
$L_q 10^{-2}$, $L_s 10^{-2}$



$a = \lambda / \mu N$

Fig. 4. Dependences $L_q = f(a)$, $L_s = f(a)$ for constant service time

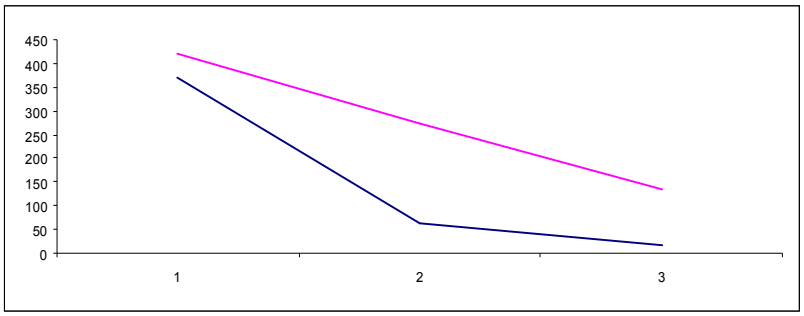
τ_q, τ_s



$a = \lambda / \mu N$

Fig. 5. Dependences $\tau_q = f(a)$, $\tau_s = f(a)$ for constant service time

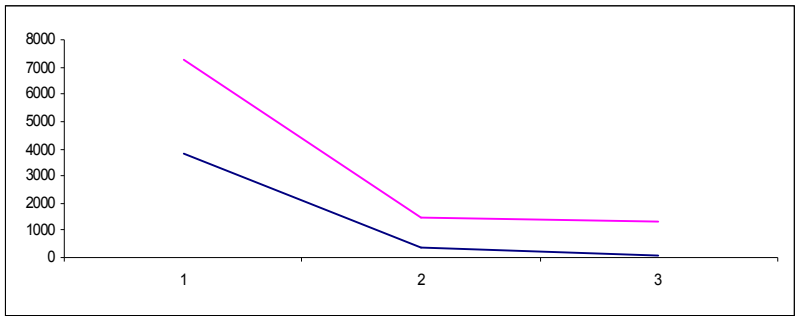
$L_q 10^{-2},\ L_s 10^{-2}$



$a = \lambda / \mu N$

Fig. 6. Dependences $L_q = f(a)$, $L_s = f(a)$ for erlang service time

$\tau_q,\ \tau_s$



$a = \lambda / \mu N$

Fig 7. Dependences $\tau_q = f(a)$, $\tau_s = f(a)$ for erlang service time

The results obtained proved theoretical expectations regarding behavior of losses function as a result of untimely distribution of messages among the computers after filtration in DN with certain scheme of messages distribution route in the network in conditions of possible threats by malefactors.

While construction of IPS in DN along with analytical methods of modelling method of simulation modelling is often used [9]. This methods enables the developers to investigate objects of practically any complexity. Simulation modeling is used as a part of the system of computer-aimed-design at the stages of sketch and engineering design. One of the most widely used tools of decision-making support is General Purpose simulation System (GPSS) [9].

Analysis of IPS simulation model results in DN

Variants of IPS simulation models in DN, having the following routing schemes of two types are considered.

The route of messages processing for the first type is performed by functions (operations for information protection) [1 – 3], and for the messages of the second type the route is performed by functions (operation for information protection) [4 – 6]. Distribution of information protection functions by computers $k_i, i = \overline{1,3}$, time intervals between arriving messages and time of their completion are preset.

It is necessary to determine average load of each computer, average time of each type of message processing, length of queues for processing by the computers, volume of the memory, necessary for the given flow of messages. In the model the time is adjusted for execution of modeling during preset model time. If necessary, the time must be adjusted. After simulation model of IPS in DN the results are obtained. On the basis of these results dependences, shown in Fig. 8 – 10, are constructed and investigated.

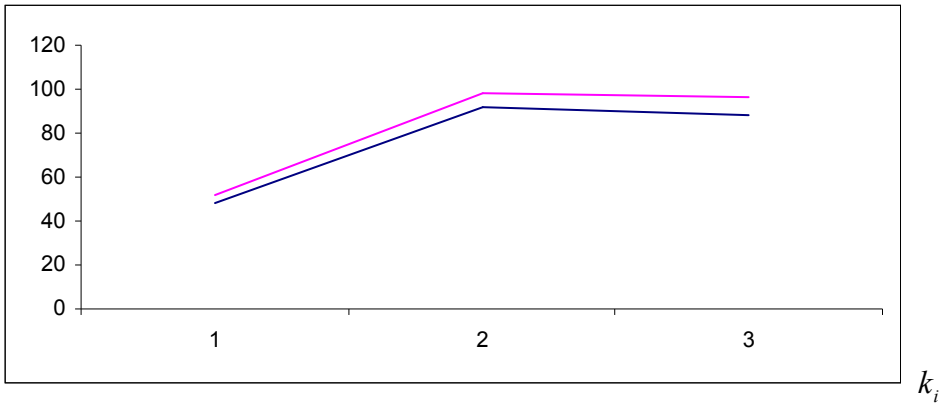


Fig. 8. Average load of computers (in %) k_i, during 8 hours. (upper line), during a week (lower time)

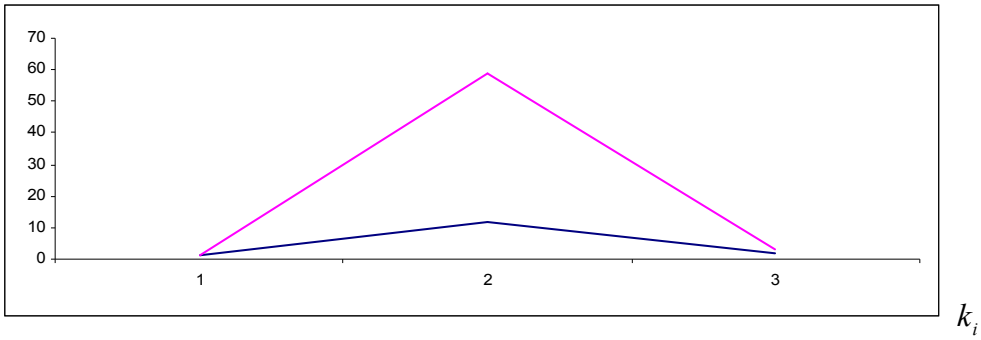


Fig. 9. Maximum length of queues to computers k_i, during 8 hours. (upper line), during a week (lower line)

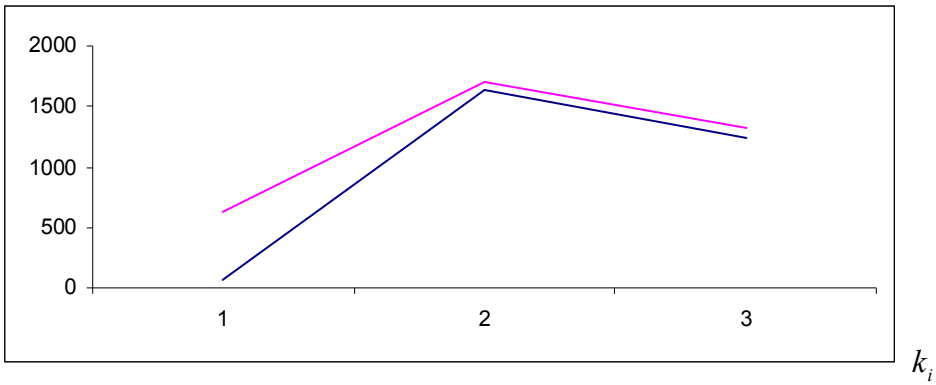


Fig. 10. Average time of messages processing by the computers (in min) k_i, during 8 hours. (upper line), during a week (lower line)

By the results of modeling, we can make a conclusion, that the total number of the processed messages during 8 hours is 40, during a week – 142. The data allow to calculate the necessary volume of memory for IPS in DN. The first computer k_1 is loaded by 50%, and a computer k_2 is overloaded (average percentage of usage 98% ad length of queue 59 messages prove this conclusion). Computer k_3 has optimum loading. It should be noted that to improve the efficiency of IPS operation in DN at the given messages flow – two computers can be used.

In order to define optimum IPS structure in DN at a preset message flow the run of the model may be continued. Besides, if the structure of the network cannot be changed, then using the possibilities of modeling language GPSS, such message flow can be selected, that would allow to load the network optimally.

Development of algorithm of analysis and comparison of the results of mathematical and simulation methods

For comparative analysis of the results of mathematic and simulation methods the following

algorithm was developed.

Step1. Construction of simulation model for various cases.

Step 2. Realization of simulation process at normal conditions, obtaining different variants and substantiation of the model.

Step 3. Comparison of the results of mathematic and simulation models.

Step 4. If the results of mathematic and simulation models converge, simulation for peak loads are performed. Otherwise, the system expands its possibilities (i.e. value of structural parameters increases).

Step 5. Testing process is performed (construction and processing of DN and verification of all functions).

Step 6. Realization of simulation at normal conditions and construction for obtaining different variants.

Step 7. Verification of results convergence. If they converge, the network is additionally tested in conditions of peak loadings. Otherwise, the network expands its abilities and transition to the fourth step is performed.

Comparison of the results of mathematic and simulation models is performed in the following way:

$$\Delta P = \left[\frac{(P^{\bullet} - P)}{P} \right] \cdot 100\,\%, \qquad (5)$$

where, $P^{\bullet}$, $P-$ are values of characteristics of mathematic and simulation models, correspondingly. On the base of the developed algorithm, the analysis of the results, obtained after the run of both models, shows that they differ within the limits of 2 – 10%, and the degree of mathematic model adequacy to the investigated object, increase with the decrease of load value $a = \lambda / \mu N$.

Conclusions

Comparative analysis of the results of mathematic and simulation models of information protection in distributive networks is carried out. Computational experiments, based on the developed algorithms are carried out, numerical results are obtained. The analysis of the results of both models shows, that they differ within the limits of 2 – 10%, and the degree of mathematic model adequacy to investigated object increase with the decrease of load $a = \lambda / \mu N$.

REFERENCES

1. Исмайлов Б. Г. Исследование характеристик систем защиты информации распределенной сети / Б. Г. Исмайлов // Автоматика и вычислительная техника. – Рига: – 2006. – №3. – С. 51 – 59.

2. Герасименко В. А. Основы защиты информации / В. А. Герасименко, А. А. Малюк. – М.: ППО «Известия» УДПРФ. – 1997. – 372 с.

3. Герасименко В. А. Защита информации в автоматизированных системах обработки данных. Развитие, итоги, перспективы / В. А. Герасименко // Зарубежная радиоэлектроника. – 1993. – № 3. – С. 3 – 21.

4. Грушо А. А. Теоретические основы защиты информации / А. А. Грушо, Е. Е. Тимонина. – М.: Издательство Агентства «Яхтсмен». – 1996. – 130 с.

5. Алиев А. А. Анализ характеристик многопотоковых сетей обслуживания / А. А. Алиев, Б. Г. Исмайлов // Радиоэлектроника, информатика и управление. – Запорожье: 2001. – № 2. с. 66 – 69.

6. Maxchemchuk N. F. Routing and flow control in high–speed wide area networks / N. F. Maxchemchuk, M. Ei. Zarki // Proc. of the IEEE. – 1990. – Vol. 78. – N1. – P. 204 – 221.

7. Алябев С. В. Проблемы защиты информации в сети промышленного предприятия / С. В. Алябев // Сб. трудов ПУКИ. – 2003. – Выпуск 8. Воронеж: Центральное Черноземное книжное издательство. – С. 69 – 70.

8. Химмелблау Д. Прикладное нелинейное программирование / Д. Химмелблау. – М.: Мир, 1975. – 540 с.

9. Шрайбер Т. Дж. Моделирование на GPSS / Т. Дж. Шрайбер – М.: Машиностроение, 1980. – 592 с.

Ismailov Balamy Gasym ogly – Cand. Sc. (Eng)., Assistant professor, Department of Information, E-mail: Balemi@rambler.ru

Sumgait State University, Azerbaijan.