COMPUTER SCENARIOS OF BUSINESS GAMES FOR PERSONNEL TRAINING AT INDUSTRIAL ENTERPRISES

Ostroukh A.V., Barinov K.A., Surkova N.E.

Moscow Automobile and Road construction State Technical University, Moscow, e-mail: ostroukh@mail.ru, barinov@asu.madi.ru, sneee@mail.ru

Introduction. The organizational and technological level of modern industrial enterprises is largely determined by the creation and application of effective mechanisms for the formation and implementation of strategic plans for the development and effectiveness of the operational management of all production, logistics and organizational processes that aim to achieve high profitability, development and improvement of production. Therefore, the construction of the organizational structure of enterprise management is a complex multi-level problem [1–15]. Principles and methods of the construction of organizational management structure are directly dependent on many factors. The most significant of these are the specifics of the particular production process the set of technological processes used, production volume, productive capacities used, tactical, technical and quality parameters of the products, the issues of standardization and certification, the qualification level of technical, administrative and management personnel, the management system utilized, the regulatory and legal framework of the enterprise and the organization of internal and external documents. The task of building the organizational structure in an industrial environment is a high-priority task in relation to other problems of industrial process control. Formulation and solution of this problem at a high scientificand technical level is a prerequisite for the effective organization of production, the output of highly competitive products ,the growth of financial and economic indicators, dynamic development and continuous improvement of production.

The relevance of the topic is determined by the need to optimize the organizational structure of the enterprise management as the problem of the «upperlevel» to be the priority decisions as a basic component of a successful and efficient operationofany industrial enterprise, regardless of the type of products and production capacity.

Formation mechanisms of the business game scenarios

Let's consider the mechanisms of the formation of scenarios that have software support in the workbench «SOTA». The general case of organizational and structural medium of multirole BSG is shown in Fig. 1, where

G – multirole business game (MBG);

R_j – roles in G; $1 \le j \le N_R$, where N_R – number of roles in G;

g_i – samples of G; $1 \le i \le N_g$, где N_g – number of samples of G;

r_{ijk} – samples of roles in the samples of G; $1 \le i \le N_{Rj}$, where N_{Rj} – number of samples of the role R_j.

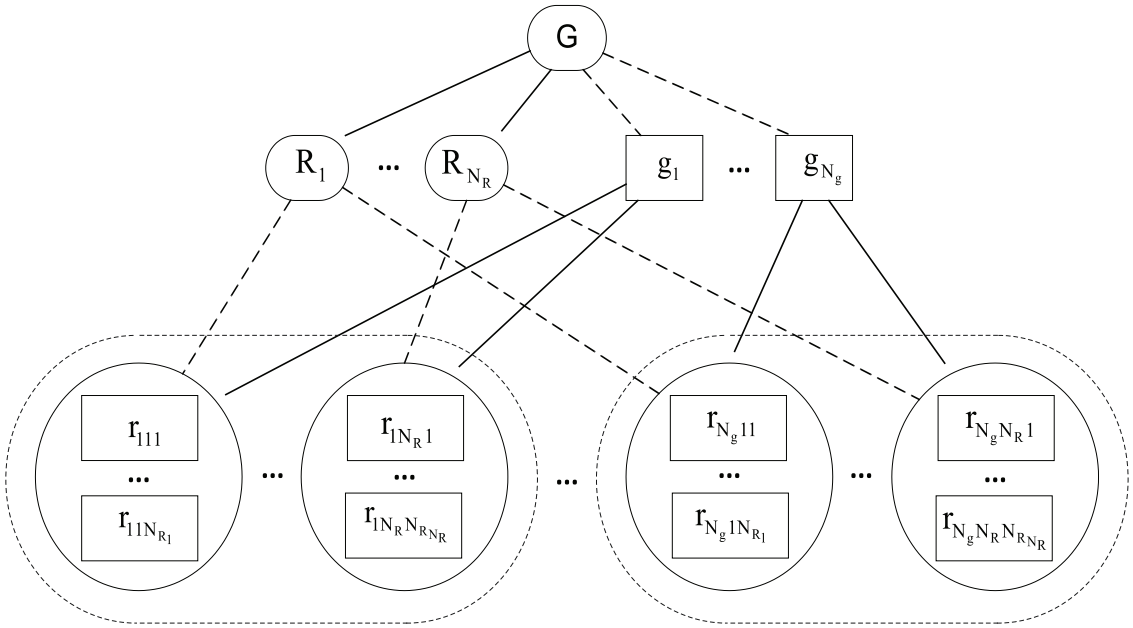

Fig. 1. General case of the organizational structure of the multipart BSG environment

The structure of the individual single-sample BSG which has the possibility to create several interconnected samples of its single role is analogous to the individual BSG with the only sample of this role but supporting several interacting samples of the game [1, 2, 6, 8]. Broken lines indicate the class-sample relationships. Arrows indicate relationships of belonging. Various versions of the organization of the management flow are possible when developing the body of BSG (Fig. 2). Octagons denote syncing fragments.

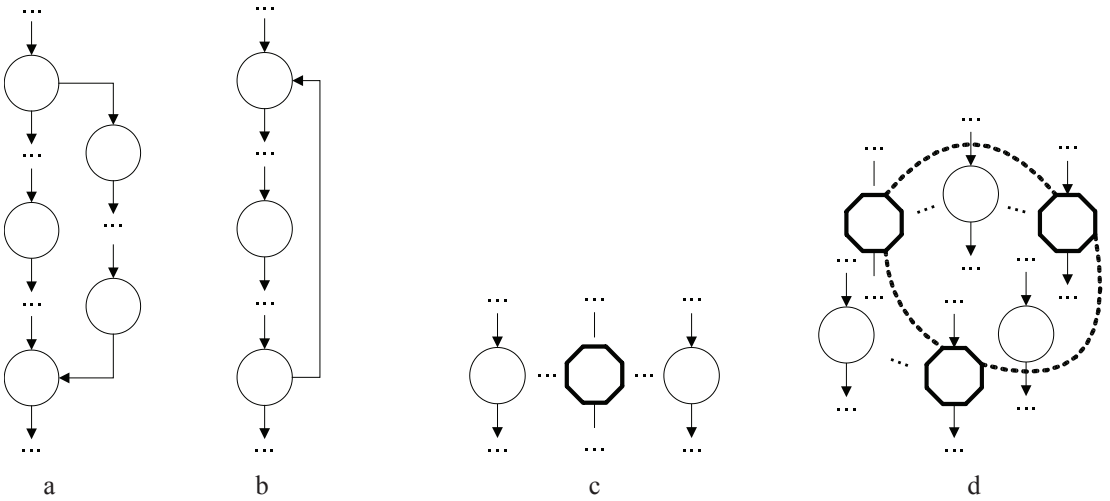

Fig. 2. Options of the flow control

Performance of the BSG frame is defined by the following parameters (their values are set during the developmental stage of the game): whether it is single or multipart; there is limitation in the choice of roles.

Schematically, the process of creating a new multirole BSG on the basis of the framework and using the developed tools can be represented by the diagram on Fig. 3. Typically, the BSG scenario then consists of the main part and auxiliary part.

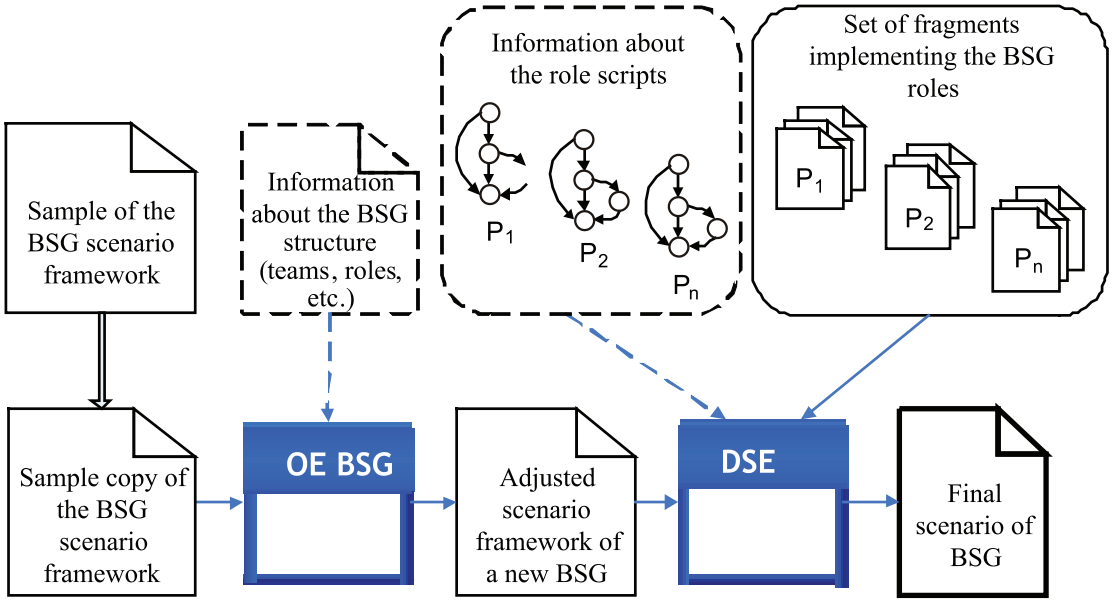

Fig. 3. New BSG creation process

The auxiliary part represents a universal frame work that implements initialization and de-initialization functions common to a large class of BSGs. These functions are preparatory for the formation of the organizational structure of the BSG in accordance with limitations introduced

at the developmental stage and are responsible for the dissolution of the BSG. The organizational and structural environment created during the BSG forms as a result of registration of participants of the game.

The BSG framework consists of the following four elements:

● *Initialization part:*

1) F_1 – creation of the new BSG sample (new gaming group) or choosing the existing one (choosing the group);

2) F_2 – choosing a role from the list of roles provided in the BSG, creation of the sample (joining the group in the quality defined by the chosen role);

3) F_3 – waiting for the selection of the other compulsory available roles (the number for each role has a predefined number of samples) by the remaining participants of the game. Any participant registered in the given sample of the game can initiate the game if the conditions below are satisfied:

a) There are BSG roles assuming an arbitrary number of samples;

b) All the compulsory roles with the predefined number of samples are occupied in all the current BSG samples.

If a new participant of the game started registering in at least one of the samples of the BSG and has not finished the registration yet, the initiation of the game can temporarily be blocked even if all the above-mentioned conditions are met. Once all the participants are registered the game can be initiated by any of the participants. This fragment of the game is syncs the game.

● *De-initialization part:*

1) F_4 – completion of the role sample. If this was the last incomplete sample of the role among all the samples of roles connected to the given sample of BSG then the completion of this BSG sample takes place. This fragment of the game is non-visual.

Formal approach to the automation of the business game development process

The proposed principles of BSG can partially automate the process of developing new games. This can be done through the usage of a quick scenario assembling designers, parameter adjustment of the template frame of the BSG, storing of the most commonly executed fragment sand their re-use, the availability of means to integrate with mathematical packages – the latter can be used to realize particular aspects of a scenario.

It is possible to estimate the qualifications of the personnel based on the results of the game on the basis of the proposed interactive gaming model. It allows the calculation of the time required to make decisions regarding the management of the production processes.

This work solves the distribution of the personnel and assignment of a particular task problem directed at improving the time parameters of the technological process through variation of the number and time characteristics of human resources in the simulation model associated with each operation in the technological process.

Thus, the random elements a_{ij} of the matrix of responses A are indicative of the successful execution of the task at thejth level of BSG by the ith participant, that is

$$a_{ij} = \begin{cases} 1, & \text{if the solution is correct} \\ 0, & \text{if it is not} \end{cases}. \quad (1)$$

Probabilities of possible values of a_{ij} in the main logistical Rasch model are described by the success function

$$p_{ij} = p\left\{a_{ij} \middle| (\Theta_i, \delta_j)\right\} = \exp\left[a_{ij}(\Theta_i - \delta_j)\right] \cdot \left[1 + \exp(\Theta_i - \delta_j)\right]^{-1}, \quad (2)$$

where the level of readiness Θ_i of the i the participant and the complexity level δ_j of the task j are parameters which can be evaluated; $i = 1, 2, ...n$; $j = 1, 2, ...k$.

The likelihood function L of a discrete random variable a_{ij} is a function of the arguments Θ_i, δ_j as the product of the probabilities (2) for all possible values of i and j:

$$L(a_{ij}; \Theta_i, \delta_j) = \prod_{i=1}^{n}\prod_{j=1}^{k} p\left\{a_{ij} \middle| \Theta_i, \delta_j\right\} =$$

$$= \exp\left[\sum_{i=1}^{n}\sum_{j=1}^{k} a_{ij}(\Theta_i - \delta_j)\right]\left[\prod_{i=1}^{n}\prod_{j=1}^{k}\left(1 + \exp(\Theta_i - \delta_j)\right)\right]^{-1}. \quad (3)$$

The values of latent parameters $\hat{\Theta}_i$, $\hat{\delta}_j$ at which the likelihood function (3) reaches the maximum (we are talking about the global maximum and not the local one here) are taken as the point estimate of the latent parameters. These estimates of $\hat{\Theta}_i$ and $\hat{\delta}_j$ are called the highest likelihood estimates.

Since the functions L and $\ln L$ reach a maximum at the same values of their arguments, instead of looking for the maximum of L, one can look for the maximum of the log-likelihood function $\ln L$

$$\ln L = \sum_{i=1}^{n} b_i \Theta_i - \sum_{j=1}^{k} c_j \delta_j - \sum_{i=1}^{n}\sum_{j=1}^{k} \ln\left[1 + \exp(\Theta_i - \delta_j)\right], \quad (4)$$

where $\sum_{i=1}^{n} a_{ij} = c_j$;

$$\sum_{j=1}^{k} a_{ij} = b_i \qquad (5)$$

are initial scores of the participants and levels of BSG respectively.

It has been shown that the log-likelihood function depends on the primary scores b_i and c_j only, which are sufficient statistics (5) of the initial observations (1).

Extremum of the functionis achieved only at the critical points, so we can look at the partialderivatives of the function (8) for each of its arguments

$$\begin{aligned} \frac{\partial \ln L}{\partial \Theta_i} &\equiv b_i - \sum_{j=1}^{k} \frac{\exp(\Theta_i - \delta_j)}{1+\exp(\Theta_i - \delta_j)} \equiv b_i - \sum_{j=1}^{k} p_{ij} = 0; \qquad i = 1,2,...,n; \\ \frac{\partial \ln L}{\partial \delta_j} &\equiv -c_j + \sum_{i=1}^{n} \frac{txp(\Theta_i - \delta_j)}{1+\exp(\Theta_{ij}\delta)} \equiv c_j + \sum_{i=1}^{n} p_{ij} = 0; \qquad j = 1,2,...,k. \end{aligned} \qquad (6)$$

The system of equations (6) represents a system of equations of likelihood. It is nonlinear and contains $n + k$ equations with $n + k$ unknown latent parameters Θ_i, ...,Θ_n, δ_1,...,δ_k.

This work demonstrates that the system (6) has only one solution which corresponds to the maximum of log-likelihood function.

Conclusion

In conclusion, the principles of the scenario construction and instruments of the BSG were developed. We proposed network models of the technological processes that form the basis of the description of the interactive simulation scenario and allow us to check the correctness of the scenario, to see the presence of dead-ends and blocks in its description. Also they allow us to identify possible options of the development of the simulated technological process at the early stages of the game.

It was shown that it is possible to transform formal description schemes of the technological processes into a multipart BSG scenario automatically similar to the usage of the critical sections based on the blocking variables during the syncing of the flows of a single process.

References

1. Barinov K.A. Implementing the innovative multimedia methodological complexes in the learning process. Opytvned renijainno vacionnyhmul' time dijnyhuchebno-metodicheskih kompleksov v uchebnyj process / K.A. Barinov, A.V. Ostrouh, M.N. Krasnyanski, P.S. Rozhin, N.E. Surkova // Vestnik MADI (GTU), issue 1 (8) / MADI (GTU). – M., 2007. – P. 89–94.

2. Barinov K.A. Implementation of the business games in computer-based learning systems / K.A. Barinov, A.V. Ostrouh, N.E. Surkova // Open and distance learning, № 3 (27), Tomsk state university 2007. – P. 28–33.

3. Barinov K.A. Development and testing of electronic educational resources of new generation distance learning / K.A. Barinov, D.A. Burov, M.N. Krasnyanski, A.V. Ostrouh // Nauchnyjvestnik MGTU-GA, issue № 141 / MGTU GA. – M., 2009. – P. 181–188.

4. Barinov K.A. Development of role playing games for training and re-training of the production plant and transportation of industry personnel /K.A. BarinovA.V. Bugaev, D.A. Burov, A.V. Ostrouh // Nauchnyjvestnik MGTU GA, issue № 141 / MGTU GA. – M., 2009. – P. 189–197.

5. Barinov K.A. Virtual training complexes for the training of the chemical and Virtual'nye trenazhernye kompleksy dlja obuchenija i treninga personalahim icheskihi mechanical engeneeringindustries / K.A. BarinovD.L. Dedov, M.N. Krasnyanski, A.V. Ostrouh, A.A. Rudnev // Vestnik TGTU. Volume 17. № 2. – Tambov, 2010. – P. 497–-501.

6. Barinov K.A. Formation of the organizational management structure of the production plant using multipart business games. / K.A. BarinovA.B. Vlasov, V.Yu. Stroganov, G.G. Yagudaev // Science and Education. Moscow State Technical University named after N.E. Bauman. Electronic magazine 2011. № 8. Online access: http://technomag.edu.ru/doc/206805.html (connection date 27.09.2013).

7. Barinov K.A. Application of business game tools to the problems of the management of production in the highly competitive environment / K.A. Barinov ,A.A. Solncev, P.A. Timofeev, V.M. Rachkovskaya // Science and Education. Moscow State Technical University named after N.E. Bauman. Electronic magazine 2011. № 9. Online access: http://technomag.edu.ru/doc/207618.html (connection date 27.09.2013).

8. Barinov K.A. Formal models of representation and organization of business games / K.A. Barinov B.S. Goryachkin, L.V. Ivanova, A.B. Nikolaev // Moscow State Technical University named after N.E. Bauman. Electronic magazine 2011. № 9. Online access: http://technomag.edu.ru/doc/207391.html (connection date 27.09.2013).

9. Barinov K.A. Correlation between the educational plan modules. / K.A. Barinov O.B. Rogova, D.V. Stroganov // The world of Scientific discoveries, issue № 9 (21) / Scientific Research Center – Krasnoyarsk, 2011. – P. 28–34.

10. Barinov K.A. Intellectualization of the test controls in the open education / K.A. Barinov L.V. Ivanova, E.Yu. Tolkaev, G.G. Yagudaev // The world of Scientific discoveries, issue № 9 (21) / Scientific Research Center – Krasnoyarsk, 2011. – P. 86–92.

11. Barinov K.A. Methods and algorithms of adaptive computer-based testing / K.A. Barinov Kartashev M.I. // The world of Scientific discoveries, issue № 9 (21) / Scientific Research Center – Krasnoyarsk, 2011. – P. 93–106.

12. Barinov K.A. Quality evaluation of the heterogeneous testing / K.A. Barinov, L.V. Ivanova, K.A. Nikolaeva // The world of Scientific discoveries, issue № 9 (21) / Scientific Research Center – Krasnoyarsk, 2011. – P. 126–130.

13. Barinov K.A. Algorithm of the virtual training complex for re-training of petrochemical company personnel / K.A. Barinov, M.N. Krasnyanski, A.Yu. Malamut, A.V. Ostrouh, G.G. Yagudaev // The world of Scientific discoveries, issue № 2.6 (26) / Scientific Research Center – Krasnoyarsk, 2012. – P. 168–174.

14. Barinov K.A. Application of the module-competentive approach in development of electronic educational resources for an e-learning system of professional education institution / K.A. Barinov A.V. Ostroukh // Engineering Competencies – Traditions and Innovations. Proceedings, 37-th International IGIP Symposium 2008. – Moscow, Russia, 7–10 September, 2008. – C. 253–254.

15. Barinov K.A. Algorithm of the Virtual Training Complex Designing for Personnel Retraining on Petrochemical Enterprise / K.A. Barinov M.N. Krasnyanskiy, A.J. Malamut,

A.V. Ostroukh // International Journal of Advanced Studies 2, № 3 (2012). Online access: http://journal-s.org/index.php/ijas/article/view/201236/pdf_13 (connection date 27.09.2013).

The work is submitted to the International Scientific Conference «New technologies in education», Indonesia (Bali), February, 17-25, 2014, came to the editorial office on 12.12.2013.

SECURITY SCANNERS

Shaikhanova A.K., Zhangisina G.D., Zholymbet B., Katasheva Z.C., Bolathan L.

Kazakh National Technical University named after K.I. Satpayev, Almaty, e-mail: igul7@mail.ru, gul_zhd@mail.ru

The directions in the field of information security, as an adaptive network security were considered. This directions are composed of two major technologies – security analysis (security assessment) and the detection of attacks (intrusion detection). And the subject of the paper will be the first technology aforesaid.

Introduction. The network consists of channels, nodes, servers, workstations, application and system software, databases, etc. All of these components need to be evaluated for their protection effectiveness. Means tested network security analysis and look for «weak» place in it, analyze the results and based on them create various reports. In some systems, instead of «manual» intervention by the administrator, some vulnerability that found will be eliminated automatically (for example, in the System Scanner). Here are some of the problems identified by the analysis of security systems:

✓ «hatches» in the programs (back door) and programs such as «Trojan horse»;

✓ weak passwords;

✓ susceptibility to penetration of unprotected systems;

✓ improperly configured firewalls, Web – servers and databases;

✓ etc.

Technology of security analysis is an effective method of implementing network security policies before implementing its attempt to breach the inside or outside of the organization.

The modalities of the work

There are two basic mechanisms by which the scanner checks for vulnerabilities – Scan (scan) and probing (probe) [1].

Scanning – the mechanism of passive analysis, in which the scanner is trying to determine the presence of vulnerabilities without actual confirmation of its presence – on circumstantial evidence. This method is fast and simple to implement. In terms of ISS, this method is called «inference» (inference). According to Cisco this process identifies open ports found on every network device and collects associated with ports headers (banner), found by scanning each port. Each received header is compared with table rules of network devices, operating systems and potential vulnerabilities. On the basis of this comparison are made the conclusion about the presence or absence of vulnerabilities.

Probing – active mechanism analysis, which ensures presence or absence vulnerability on the analyzed node. Probing performed by simulating the attack, using the validated vulnerability. This method is slower than the «scan», but almost always much more accurate. In terms of ISS, this method is called «confirmation» (verification). According to Cisco's process uses information obtained during the scanning process («inference»), for a detailed analysis of each network device. This process also uses well-known methods of the attacks in order to fully confirm the alleged vulnerability and discover other vulnerabilities that cannot be detected by passive methods, such as susceptibility to attacks such as «denial of service».

In practice, these mechanisms are implemented by several following methods.

«Checking the headlines» (banner check).

This mechanism is a series of tests such as «Scan» and allows you to make a conclusion about the vulnerability of relying on the information in the request header scanner. A typical example of such a test – analysis of program headers Sendmail or FTP-server that allows you to find out their version and use that information to draw a conclusion about the presence of these vulnerabilities.

«Active probing test» (active probing check).

Also related to the mechanism of «scanning». However, they are not based on checking the software version in the headlines and on the comparison of the «digital snapshot» (fingerprint) piece of software with a cast of well-known vulnerabilities. Likewise as antiviral system, comparing the scanned fragments software virus signatures that are stored in a dedicated database. A variation of this method are the check sums or the date of scanning software, which are implemented in scanners running on the operating system level.

«Imitation of attacks» (exploit check).

These checks include the mechanism of «probing» and is based on the exploitation of various defects in the software.

Some vulnerabilities do not reveal themselves until you «push» them. For that purpose against a suspect or service node they run a real attack. Header checks carried out initial inspection of the network, and the method of «exploit check», rejecting the information in the headers to simulate a real attack, thereby more effectively (but less speedy) detecting vulnerability scanning nodes. Imitation of attacks is a more reliable method of analysis of security than the header checks, and usually more reliable than active probing test [2].

However, there are cases where the simulated attack cannot always be realized. Such cases can be divided into two categories: a situation in which the test results in a «denial of service» of the analyzed