Enterprise functioning quality management under conditions of destructive program actions

Malika Davliatova 1*, Alexandr Brechko 2, Natalia Lvova 2, Mikhail Sorokin 2

1 Peter the Great St. Petersburg Polytechnic University, Polytechnicheskaya st., 29, Saint Petersburg, 195251, Russia
2 S. M. Budjonny Military Academy of the Signal Corps, Tichorezki ave., 3, Saint Petersburg, 194064, Russia

* E-mail: malika.davliatova@gmail.com

Abstract. The trends of development of modern enterprises lead to building network-connected territorially dispersed structures, which determine the enhanced requirements to control systems. Therefore, the control systems are compelled to use general technological resource — cyber-domain, which is the reason for transition of competitive confrontation to technological sphere and leads to the emergence of premeditated direct or indirect destructive program actions as one of the most efficient facilities for getting competitive advantage. The enterprise functioning quality control under new conditions requires provision of a subsystem of taking decisions with timely, authentic and complete information on the state of cyber-domain. The task of getting such information can be realized using modeling methods. The analysis of the existing modeling methods of communication networks has demonstrated availability of an essential deficiency — absence of keeping record of destructive program actions with simultaneous functioning of two conflicting enterprise control systems at the unified technological resource. The article describes a new method of simulating communication networks rectifying the revealed deficiency. The presented method can make a basis of the model, which is capable to enhance information awareness of the subsystem of taking decisions on the state of a simulated network, enhancing by the same the quality of enterprise control and, accordingly, the quality of functioning of the enterprise proper. The article is the development of the method of simulating of premeditated damages of elements of communication network patented by the authors.

1. Introduction
The modern enterprises are characterized by complex and inhomogeneous structure, a great number of components and wide territorial (up to global) dispersion thereof. The management of such enterprises requires complex and hi-tech, and most importantly, distributed management system. The functioning of enterprises’ distributed management systems require high quality of functioning of management technical subsystem — communication systems.

Building of the inherent communication system isolated and functioning for the benefit of only one user is a complex and utterly resource-consuming task. Whereby, practically all network enterprises management systems, including small ones, utilize the resources of global communication network — cyber-domain.
2. Methods

According to [1] the cyber-domain is characterized by network-centricity, dissimilarity of composition and structure, and most importantly, by functioning for the benefit of many parties, including heterogeneous and antagonistic users. The use of common technological resource by the competing management systems transfers competitive confrontation to a new technological sphere. The analysis of sources [2–4] has shown a permanent growth of the number of destructive program impacts of different types being implemented both in the territory of Russia and all over the world. Such dynamics is explained by the efficiency, anonymity and low sensitivity thereof to mutual separation of subject and object of impact [5]. The management of network enterprise functioning quality under new conditions — under conditions of using destructive program impacts by the competitive management systems demands up-to-date, authentic and complete data about general functioning environment — cyber-domain.

Direct investigation of the cyber-domain is an unconventional task due to intricacy and dynamic change of structure and links between elements, ambiguity of behavior algorithms under different conditions, a great number of parameters and variables, incompleteness and non-determination of the initial information, versatility and probabilistic nature of external environment impacts and other factors. Solution to a problem of up-to-date, authentic and complete data about a state of cyber-domain fragment, localized by the area of functioning of competing management systems is a possibility by application of modeling methods. The modelling methods make a theoretical basis of any models. The analysis of the existing methods of simulating communication networks [6–8] has shown an availability of a general essential drawback — absence of a possibility of simulating a process of emergence of premeditated damages to the elements of communication network featuring different structural significance in the network.

The presented modeling method eliminates the above deficiency and figure 1 [9] explains this method.

3. Innovative modeling method

The following initial data is designated in block 1 (figure 1):

- Modeling interval $T_m$ — time span, when modeling process takes place.
- Modeling time period $\Delta t$ — a period, with which iterations take place during model functioning.
- Control systems of competition enterprises services by communication network — a multiplicity of elements of investigated control system $K = \{ k_1, k_2, \ldots, k_n \}$ and $R$ of information directions between its elements as well as a multiplicity of elements of an enterprise competition control system $L = \{ l_1, l_2, \ldots, l_m \}$ and $P$ of information directions between its elements.
- Routing protocol — a protocol, according to which the routes following designated information directions will be built. The routing protocols are known and described, e.g., in [10, 11].
- Mean time for restoration of every element of communication network and its root-mean-square deviation. The mean time of element restoration and root-mean-square deviation shall be in multiples of modeling time period duration $\Delta t$.
- Threshold value of damage probability for referring the communication network elements to a multiplicity of disabled ones.
To define the beginning of the next statistical realization

To define an indicator of the relative structural importance of each element CN

To number elements of a communication network (CN)

To generate time of emergence of damages of elements CN

To place elements of the control systems (CS) on communication network elements

To build routes for service of information directions of CS

To define the elements CN used as investigated, and competing CS

To remember the elements CN used for ensuring communication on each information direction (ID) investigated by CS

To redefine the structural importance of the elements CN which are stored in memory taking into account their use both CS

To put the structural importance of elements CN and probability of their deliberate damage in compliance

$N = 1$

$1$ $2$ $3$

Figure 1. Block diagram of modeling method.
The communication network elements are numbered in block 2 (figure 1).
The beginning of the next statistical implementation is determined in block 3 (figure 1).
The indicator of the relative structural significance of every communication network element is
determined in block 4 (figure 1) [12]:

\[ Z_i = 1 - \frac{G_i^{\text{damage}}}{G_i^{\text{function}}} \]  

(1)

where \( G_i^{\text{damage}} \) — indicator of communication network survivability with damaged i-n communication network element,
\( G_i^{\text{function}} \) — indicator of communication network survivability with functioning i-n communication network element.
A cumulative volume of transmitted traffic with functioning i-n element and volume of traffic with
damaged i-n element can be selected as indicator of communication network survivability.

Time of occurrence of damages to communication network elements is generated in block 5
(figure 1).
The moments of time deliberate damages occurrence are generated, the generation time is in
multiples of duration of modeling time period \( \Delta t \). The generated time moments get saved.
The elements of competition control systems are hosted by communication network elements in
block 6 (figure 1). Every element of every control system is hosted by one of communication network
elements.
The routes for servicing information directions of control systems are built in block 7 (figure 1).
The routes are being built with respect to every specified information direction in accordance with the
assigned routing protocol.
The communication network elements used by the investigated control system and competition
control system are determined in block 8 (figure 1).

Since the control systems utilize a unified telecommunications resource, some communication
network elements may participate in servicing both control systems after building routes according to
assigned information directions [13, 14].
The communication network elements used for providing communication via every information
direction of the investigated control system are saved in block 9 (figure 1).
The structural significance of communication network elements used by both control systems is set
to zero [23].
The structural significance of communication network elements is put in correspondence with
probability of deliberate damage thereof in block 11 (figure 1). At that, the probability of deliberate
damage of communication network elements used by the competition control system will equal zero.
Value 1 is assigned to variable \( N \), \( N \) — a service counter required for functioning algorithm in
block 12 (figure 1).
The elements for N-n information direction stored in memory are selected in block 13 (figure 1).
A searching of all \( R \) information directions takes place in a cycle by increasing variable \( N \) by a unit
in block 22 (figure 1).
The current time of modeling \( t_m \) and time of serviceable condition \( t_p \) of N-n information direction
are reset to zero in block 14 (figure 1).
The deliberate damages implemented by the competition control system are generated in block 15
(figure 1).
If the moment of time of emergence of deliberate damage generated earlier occurs, the deliberate
damage will be generated for the selected elements, where the probability of a deliberate damage
exceeds the design threshold value.
The beginning of process of restoration of unserviceable communication network elements is initiated in block 16 (figure 1).

The restoration of every unserviceable element over the specified mean time begins taking into account the root-mean-square deviation.

They check the fact, whether all the selected elements are serviceable in block 17 (figure 1). If all the elements are serviceable, they increase the time of serviceable state of \( N-n \) information direction by the value of modeling time period in block 18 (figure 1).

The information direction consists of the successively connected elements of communication network [15, 19], therefore, it is deemed serviceable in that case only, when all the elements are fit [16, 22].

The current modeling time \( t_m \) gets increased by the duration of modeling time period \( \Delta t \) in block 19 (figure 1).

They check, whether the modeling interval has expired in block 20 (figure 1). If not, they will repeat the actions described in blocks 15–20 (figure 1). If the modeling interval has expired, they calculate an availability factor for \( N-n \) information direction in block 21 (figure 1).

The availability factor is a probability of the fact that an object will appear to be serviceable in any arbitrary instant of time and is to be calculated according to the equation:

\[
K_r = \frac{\sum_{i=1}^{M} t_i}{\sum_{i=1}^{M} t_i + \sum_{i=1}^{M} \tau_i}
\]

(2)

where, \( t_i \) — accumulated operating time of \( i-n \) object within a specified interval of operation, \( \tau_i \) — accumulated restoration time of \( i-n \) object over the same period of operation, \( M \) — number of apparent objects within a specified interval of operation [17, 18].

Since one object — one information direction is under observation, then \( N = 1 \) and, hence, the expression will be as follows:

\[
K_r = \frac{t_i}{t_i + \tau_i}
\]

(3)

The accumulated operating time is a duration or volume of object operation.

The duration of operation of information direction is equivalent to the time of serviceable condition \( t_p \) being determined in block 18, which means: \( t_i = t_p \).

The interval of operation is equivalent to modeling interval \( T_m \), and since the information direction was in serviceable and unserviceable condition only, then:

\[
t_i + \tau_i = T_m
\]

(4)

Subsequently, considering expressions 1, 2, 3 the availability factor of information direction [19–21]:

\[
K_r = \frac{t_p}{T_m}
\]

(5)

where, \( t_p \) — total time of serviceable condition of \( N-n \) information direction, \( T_m \) — modeling interval equal to total functioning (observation) time of information direction.

After calculating availability factor a list of unserviceable elements of communication network at every period of modeling time is depicted.

The variable \( N \) (service counter) per unit is increased in block 22 (figure 1).
They check, whether the availability factor is calculated for all information directions and a list of unserviceable elements is depicted in block 23 (figure 1). If not, they will repeat the actions described in blocks 13–23 (figure 1).

If the availability factor is calculated for all information directions of the management system under investigation and a list of unserviceable elements of communication network in every period of modeling time is depicted, the modeling process will be finished and the acquired data will be depicted in block 24 (figure 1).

4. Conclusions
It is possible to calculate $K_r$ of every information direction of management system under investigation and get a complete list of unserviceable elements of communication network at any moment of time of observation taking into account occurrence of damages to the elements of communication network featuring different structural significance as a result of fulfilling actions according to the presented method.

The presented method forms a theoretical basis of communication network model. The use of such model will help increase quality of management of network enterprise under conditions of destructive program impacts due to improvement of subsystem of taking decisions in the way of providing it with more up-to-date, authentic and complete information on the state of the used network. The model can be used also for the improvement of other systems of control of complex objects under conditions of destructive program impacts.

References
[1] Starodubtsev Yu I 2017 Information Services Quality Control (Saint Petersburg: Publishing House of Polytechnic University)
[2] An annual report by Kaspersky Lab, https://securelist.ru/statistics/
[3] Report of the Financial Sector Computer Emergency Response Team (FinCERT) of the Directorate General for Security and Information Protection of the Bank of Russia, http://www.cbr.ru/statichtml/file/14435/fincert_survey.pdf
[4] Cybersecurity threatscape Q4 2017, https://www.ptsecurity.com/upload/corporate/ru-analytics/Cybersecurity-threatscape-2017-rus.pdf
[5] Grechishnikov E V, Lyubimov V A, Pominchuk O V and Chemeris G V 2005 Device for Modeling Failures and Damages in Sophisticated Systems, patent № 2292583
[6] Grechishnikov E V, Pominchuk O V, Ivanov V A., Shashkina N E and Belov A S 2007 Method of Modeling Failures and Damages in Communication Networks, patent № 2351012
[7] Voitsekhovskiy A I, Belov A S, Kiselev A A, Ivanov V A., Kriventsov O B and Melnov A I 2011 Method of Modeling Deliberate Damages of Elements of Communication Networks, patent № 2449366
[8] Brechko A A, Vershinnik E V, Latushko N A, Lvova N V and Starodubtsev Yu I 2017 Method of Dynamic Modeling of Communication Networks Taking Into Account Interdependece of Elements Thereof, patent № 2665506
[9] Brechko A A, Bukharin V V, Vershennik A V, Vershennik E V, Lvova N V and Starodubtsev Yu I 2017 Method of Modeling Deliberate Damages of Elements of Communication Networks Functioning for the Benefit of Heterogeneous, Including Antagonistic Control Systems, patent № 2655466
[10] Olifer V and Olifer N 2016 Computer Networks. Principles, Technologies, Protocols (Saint Petersburg: Piter)
[11] Stekolnikov Yu I 2002 Systems Survivability (Saint Petersburg: Politechnika)
[12] Fedotov A V 2010 Fundamentals of Theory of Reliability and Technical Diagnostics (Omsk: Publishing House of OmSTU)
[13] Brechko A A and Starodubtsev Yu I 2017 Week of Science at SPPU. Proc. of Sci. Conf. with International Participation 421–23
[14] Brechko A A, Starodubtsev Yu I and Davliatova M A 2018 Proc. of XXI Int. Conf. on Soft Computing and Measurements (SCM-2018) 380–383
[15] Brechko A A, Beskov A V and Kovaikin Yu V 2018 Proc. of IV All-Russian Research and Practical Conf. “Up-to-Date Information Technologies. Theory and Practice” 142–146
[16] Brechko A A, Lvova N V, Martynyuk I A and Pervov M S 2018 Proc. of III Interuniversity Research and Practical Conf. “Problems of Technical Support of Troops Under Modern Conditions” 165–67
[17] Starodubtsev Yu I and Brechko A A 2018 Neural Computers and Application Thereof. XVI All-Russian Scientific Conference: Scientific Conference Abstracts 109–A
[18] Davliatova M A and Starodubtsev Yu I 2018 XXI International Conference on Soft Computing and Measurements (SCM-2018) 417–420
[19] Davliatova M A and Starodubtsev Yu I 2017 Higher Educational Institutions Functioning Assessment and Quality Management Under the Conditions of Globalization. Strategic Partnership of Universities and Enterprises of Hi-Tech Branches (Science. Education. Innovations) (SPUE) 2017 IEEE VI Forum 215–217
[20] Davliatova M A and Starodubtsev Yu I 2018 Scientific and Technical Bulletin of SPSPU. Economical Sciences 11 (4) 251–262
[21] Davliatova M A, Kurochkina A A and Starodubtseva V V 2016 Components of Scientific and Technological Progress 4 (30) 10–13
[22] Davliatova M A, Starodubtsev G Yu and Khnykina T S 2017 International Technical and Economic Journal 2 82–85
[23] Starodubtsev Yu I and Davliatova M A 2018 Proc. of III Interuniversity Research and Practical Conf. “Problems of Technical Support of Troops Under Modern Conditions” 316–321