ISSN 0147-6882, Scientific and Technical Information Processing, 2015, Vol. 42, No. 1, pp. 24–29. © Allerton Press, Inc., 2015.
Original Russian Text © O.V. Syuntyurenko, 2015, published in Nauchno-Technicheskaya Informatsiya, Seriya 1, 2015, No. 2, pp. 1–7.

The Digital Environment: The Trends and Risks of Development

O. V. Syuntyurenko

All-Russian Institute of Scientific and Technical Information, Russian Academy of Sciences, Moscow, Russia
e-mail: olegasu@mail.ru

Received November 25, 2014

Abstract—The structure and dynamics of the growth of the global digital environment, as well as trends in the development and use of information technologies, are discussed. Risks that are related to using certain new information technologies (for example, cloud computing, mobile applications, and big data) are analyzed. Problems are considered that are associated with the upcoming change of the dominant techno–economic paradigm and the beginning of the third industrial revolution, where information technologies play a key role. Certain conclusions, recommendations, and the most important problems that face the world information community are formulated.

Keywords: digital environment, information technologies, risks, automatic data generation, supercomputing, big data, server infrastructure, networks, web traffic, domain names, robotic systems, digital sovereignty, third industrial revolution

DOI: 10.3103/S0147688215010062

1. INTRODUCTION

In the 21st century information technologies became a true locomotive of economic and technological development. Today this is characterized by the changing views on the transformation of the industrial society into the postindustrial one, which is accompanied by new conceptual declarations concerning the construction of the information society. The world stands on the brink of a change in the dominant techno-economic paradigm. The new era of the third industrial revolution is beginning. It will be characterized by the large-scale industrial application of a number of new clusters of technologies, first and foremost, nanotechnologies, biotechnologies (including genetic engineering and regenerative medicine), robotics, new materials with predesigned properties, 3D printing, and new information technologies. The latter form the basis for the establishment and integration of separate technology clusters into the base industrial complex of the new techno–economic paradigm.

2. TRENDS IN THE DEVELOPMENT OF THE DIGITAL ENVIRONMENT

The modern digital environment is a part of the global information space.

Referring to the International Data Corporation (IDC), **the growth dynamics of the digital data volume** throughout the world is shown in Fig. 1 (where automatically generated data make up ~30%). We note that text information is only 0.3–0.4% of the total volume of digital data.

The digital environment comprises the entire continuum of computer and network technologies.

The base component of the macrostructure of the global digital environment is formed by telecommunication systems and networks, first and foremost, the Internet, which is the old and the largest segment of the net (web 1); the segment of social networks and platforms (web 2); the **segment of mobile applications** (smartphones, tablets, etc.), which has exhibited the fastest growth in the last 3 years (web 3); payment networks, for example, PayPal, SWIFT, and the Bitcoin; and the segment of dedicated embedded processors for various objects of the industrial, social, or civil infrastructures (the so-called **Internet of Things,** IoT), as well as embedded microchips for medical implants, toys, and clothing (the so-called **BodyNet**), which are connected to certain control centers via the Internet (as of 2014, about 18 billion devices are online).

According to the estimates of the IDC, the volume of information in the world doubles every 2 years. The Cisco corporation reports that at the beginning of 2013 mobile traffic alone reached ~900 petabytes per month (one petabyte equals to 10^{15} bytes); by 2016, the percentage of people who use devices to access the Internet will be ~48%. By 2016, the annual volume of the global IP traffic will reach 1.3 zettabytes (one zettabyte equals a billion gigabytes). One of the main factors that has encouraged such explosive growth is the **increase in the amount of automatically generated data:** from ~11% of the total data volume in 2005 to more than 40% in 2020. Figure 2 shows the growth dynamics of automatically generated data; its share in the total data volume (according to the IDC) is due to a

sharp increase in the production of sensors (from cardiological implants to control systems for power networks and pipelines). Even today, most IP addresses belong to the control systems of objects, as well as industrial, transportation, municipal, and infrastructure facilities. Cisco predicts that the number of such IP addresses will increase to ~50 billion in 2020 (as compared to 10 billion in 2013). According to the Neilsen Company, the IoT segment is now > 70% of the web traffic.

In addition, it should be noted that corporate digital information is increasing in volume by ~40% per year. Predictive estimates suggest that the number of corporate users of the Internet will increase to 2.3 billion in 2016 (as compared to 1.6 billion in 2011).

One of the most promising directions in the development of the digital environment is **three-dimensional (3D) printing,** which is based on the additive manufacturing technology (manufacturing an object layer by layer using metallic powders, plastic materials, etc.). Today, 3D printing is being developed by Canon, Samsung, General Electric, and Siemens. This global market is estimated to be about $4 billion; it doubles every year and a half.

The segment of the so-called **cloud and distributed computing** is also growing markedly. The increasing popularity of cloud-computing technology is due to the availability (for individual and corporate users) of complex and expensive software and, often, information resources with high-quality service and low financial costs (for hardware, software, system administration, infrastructure, etc.). However, the use of cloud and distributed computing brings new potential risks that are related to information security.

The **growth of cyber crimes** is a steady negative trend. Experts suggest that the global damage caused by computer-related crimes, year by year, is about $600 billion (it increases by tens of percent per year).

We will take a closer look at the trends in the development of the technologies that are connected by the term **big data.** This field and the term itself appeared about 5 years ago as a result of digitization of the information society and the information explosion of the last decade (with marked exponential growth). Yet, there is still no common definition for big-data technologies. The key features of big data are the processing of heterogeneous unstructured and structured information (the percentage of structured information does not exceed ~40%), the high rate of data, and the high speed of processing large volumes of information in real time. The technological basis of big data is formed of high-speed telecommunications and supercomputing technologies. There is a common opinion that big data is a leading trend in economic and technological progress. In some sense, big data is an answer to new challenges in industry and science. The daily volume of information that is generated by the Large Hadron Collider (Switzerland) and processed in real time is comparable to the volume of information that circulates on the entire Internet. Big data technologies are based not only on the methods of mathematical statistics but also on relatively new mathematical

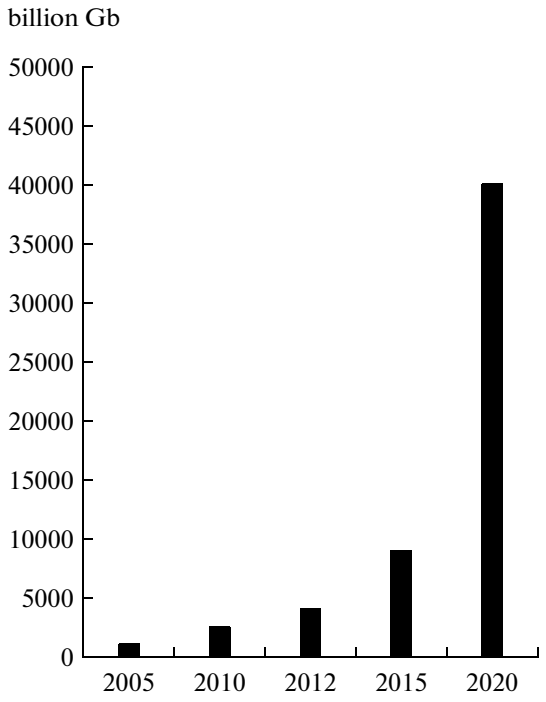


Fig. 1. The growth dynamics of the worldwide digital data volume.

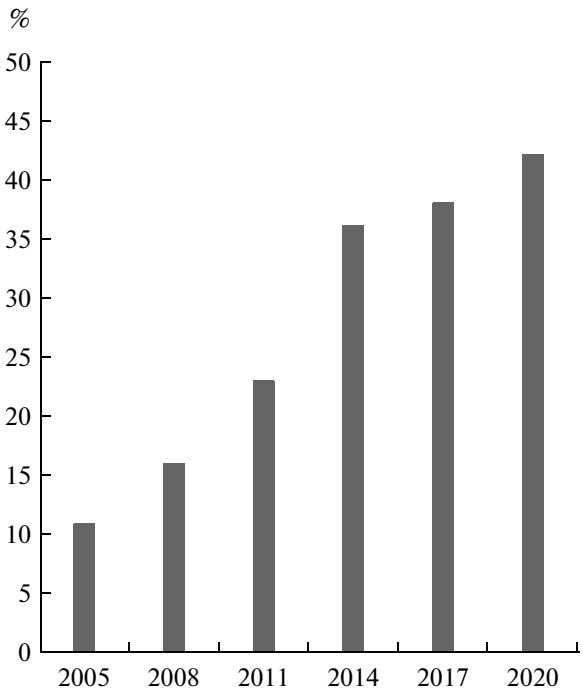


Fig. 2. The percentage of automatically generated data (yearly dynamics).

approaches and algorithms, such as neural computing, pattern recognition, fuzzy mathematics, multivariate analysis, and the theories of categories and functors. The data-handling paradigm itself is changing considerably. The big-data technologies catalyze the rapid formation of a new science, viz., sociodynamics, that generalizes and analyzes empirical regularities that are found by processing vast arrays of information from social networks (Twitter, Google, Facebook, Odnoklasniki, etc.). The development of the methodology and methods of sociodynamics along with the use of big data will make it possible to trace the dynamics of social interactions (as well as their nature) and to effectively control social networks, communities, and target groups given the knowledge of the patterns of their formation and dynamics, as well as the characteristics of groups of any size and structure; this will inevitably give rise to new risks for society.

In the foreseeable future, we can expect automated decision-support systems based on big data to be created and used extensively; such systems will possess expanded multivariate statistical analysis capabilities to find the correlations between various characteristics, parameters, and events. Some experts suggest that the development of the big data technologies will soon result in the creation of distributed self-learning systems of cognitive computations, as well as new effective methods for predicting sci-tech, innovation, economic, and social processes.

In the United States, the development of supercomputing, as well as the construction of the broadband telecommunication network that connects supercomputers of various universities and agencies into a single distributed system is a steady trend. Information about this network is quite limited; however, based on indirect estimates, its power reaches ~50% of the total power of the Top500 (274 PFLOPS) (as of November 2014, first place is occupied by the Tianhe-2 (China) with 33.86 PFLOPS). In the same direction (in the United States), work is in progress on creating a prototype **quantum computer.** In 2013, Google in cooperation with NASA began experimental testing of the D-Wave Two quantum module. In the coming 3 years, according to the plan, several such modules will be networked to create a virtual analog of a fully functional quantum computer.

While analyzing the trends in development of supercomputing systems, we should point to the following two issues. First, concerning reliability and stability, the problems of the development and use of mathematical software differ fundamentally from most technical problems. The key **risk factor** is related to the fundamental reasons that highly complex software cannot be made so reliable that one can be certain that emergency situations will not occur (this is critically important for power engineering, transport, weapons systems, etc.). Second, there still is the fundamental mathematical problem of paralleling mathematical operations and algorithms (it is only 3–4% solved), which considerably reduces the real performance of supercomputing multiprocessor systems (the Tianhe-2 system that was mentioned above has 3 120 000 processors).

3. RISKS FROM THE DEVELOPMENT OF THE DIGITAL ENVIRONMENT

As the digital environment grows and new information technologies arise and spread, various risks and threats (for individuals and society) will increase (in the quantitative and qualitative senses). Many experts say that one of the cross-disciplinary super problems of the 21st century is threat protection and risk management in complex socio-technical systems. Partly because of this, computer modeling, prognostics, and supercomputing technologies became the main directions of research and development in the field of information technologies for the world's advanced countries.

The classification and systemization of IT risks is a complex methodological problem. When formulating risk-assessment problem, certain methods should be used to rank and cluster IT risks with respect to their range of impact (individual, corporation, state, or international community), potential negative effects, and domains (culture, education, industry, etc.). In this short paper it is impossible to give due consideration to the entire variety of IT risks. Let us consider only some of the new and not properly recognized (even by the professional community) risks and threats in the field of information technologies.

A. Risks that are related to the rapid expansion of internet-connected control microchips embedded into various objects (cars, domestic appliances, and medical implants) are increasing in significance. The level of protection against most of these risks is close to zero. In 2015, the sales volume of internet-connected individual medical devices is expected to reach ~15 million. The Internet of Things, as well as the BodyNet are extremely vulnerable to target impacts and cyberterrorism.

B. Substantial risks exist that are related to the use of foreign-made microchips in complex systems and critical applications. According to various estimates, on the global market, up to 75% of all software (primarily, operational systems and database management systems) and 85% of processors are produced by American companies. A number of large IT companies supplement their microchips with bugs in the interest of intelligence and special services. Only the manufacturing company knows the configuration and source codes of such "built-in" software. One of the latest examples is the failure of the Fobos-Grunt interplanetary station in 2011, which was probably due to the use of foreign-made microchips. Apple iPhones record the route of the user, log information about the

user's location, and copy the user's contacts and all mobile data (including photo and video data). These data are regularly sent to Apple servers. American corporations produce the lion's share of the commonly used multiplexers, routers, and server infrastructure. As a result, in most countries, even protected computer systems and networks are highly vulnerable to external unauthorized actions.

C. New risks are related to the convergence of information and biological technologies. The constant decrease in the cost of the equipment for carrying out complex biotechnological process and products (including genetic engineering) makes them available for small firms, which not only expands the application area of biotechnologies but also gives rise to risks of the creation of biological weapons by various terrorist groups.

D. The use of cloud and distributed computing by corporations creates risks of two kinds: first, the company increases its dependence on the reliability of the telecommunication system; second, the distribution of responsibility concerning information security between the user companies, the owner of the cloud platform, and the internet provider effectively leads to the dilution of responsibility and to a decrease in the level of security control.

E. The steady trend towards network space extension and an increase in the number of Internet users (according to various estimates, in 2015, it will be up to ~70% of the people in all countries) gives rise to related risks for most countries. The weak elements of the Internet are the system of domain name assignment and the system of web-traffic transfer. Domain names are assigned by the nonprofit organization ICANN (Internet Corporation for Assigned Names and Numbers, USA). This organization also registers top-level domains, for example, .net, .com, .info, and .org, as well as national domains, including the .ru domain zone. Theoretically, from these facts it follows that ICANN can close a domain zone in the same way as it can open it. In this case, all web sites and all email services in this domain will be unavailable (for an indefinite period). A similar problem arises with web traffic. The transfer of web traffic from the side of a certain national zone can be suspended at any critical moment. Since American internet providers have full access to web traffic, they, just as the largest email service providers such as Gmail, Postfix, or Hotmail, can make it available to the American government.

In the case of purposeful unfriendly actions, we should acknowledge the possibility that the operation of the Internet in the territory of the Russian Federation can be destabilized. Key elements of the Internet are located outside Russia. Access (to a website) can be blocked at any stage: root servers can mistranslate the website address into the machine form, not respond to requests, or physically disconnect the network segment from the Internet. Thus, RuNet can be entirely blocked. A precedent occurred in the disconnection of the Syrian Arab Republic from the Internet in 2012. Some countries, for example, China have recognized these risks and have embarked on creating national segments of the Internet. China also implements additional measures to protect itself against destructive intrusions and unattended access to information resources. By raising the question of the complete refusal to use Microsoft products, China managed to obtain the source code of the Windows operating system, as well as the source codes of the software for the Cisco routers that are used in most networks and servers throughout the world (and, by the way, are produced in China). It should be noted that almost all leading companies that are specialized in the development of software solutions for Internet information security are registered in the United States, as are all the major service providers (Twitter, Google, Amazon, eBay, Facebook, etc.).

F. In recent years, the risks increased that are related to the growing confrontation in the field of acting on one's social conscience and carrying out destructive social transformations (so-called conscience warfare and/or network-centric warfare). This is due to the rapid development of big-data technologies, the growth of the network space, and the success that has been achieved in the cognitive and behavioral sciences. Effective projects have been developed that are focused on implicit data collection and implicit control of the behavior of large groups. Supercomputing enables the automatic segmentation and processing of massive amounts of information. By summarizing the gathered data and selecting key sense groups in them, one can obtain information (in various aspects) about the interests and sentiments of all the subjects that are represented in a segment under study. The analysis of a critical amount of data will allow one to determine the sentiments and value systems that dominate in the segment under study and, as a result, to infiltrate information into this community (which includes the use of mass media) as well as to form, based on certain ideological and worldview concepts, the desired context in a certain country. The behavior of society (or large social groups) inside the country becomes an instrumental factor that can be exposed to external influence to govern the behavior of the country in the international arena. Network-centric warfare is an effective instrument for implementing social transformations and, sometimes, real geopolitical change.

G. Risks are growing that are related to the increasing use of information technologies in the military field, in particular, in military space programs. The main risks are due to the fundamental reasons that software cannot be made so reliable as to avoid emergency situations and unauthorized use of nuclear missiles. Moreover, the level of risks rises as the scale and complexity of military systems increase. This problem is complicated by the intensive development and wide

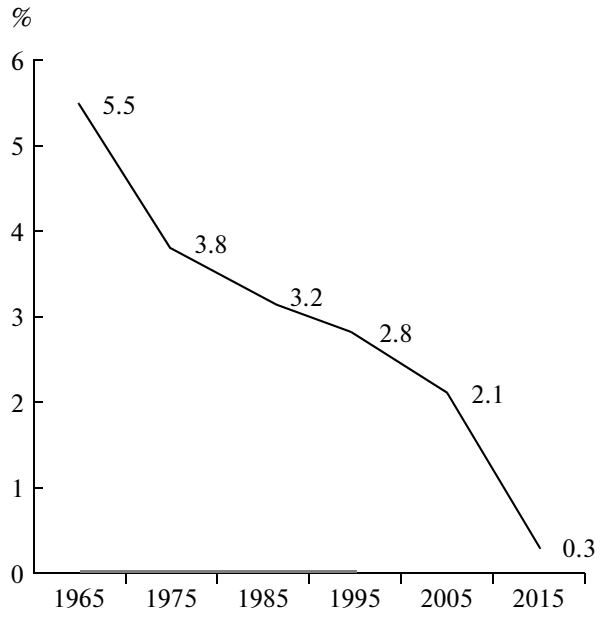


Fig. 3. The decline in the global GDP of developed economies.

use of supercomputing technologies, robot systems, and artificial intelligence systems in various military complexes.

Let us make a summary and formulate the most important problems for the development of the Russian digital environment, information technologies, and risk minimization.

Summary

1. The ongoing processes of economy globalization, the wide use of information technologies, and the explosive expansion of the digital environment are smoothly transforming the world community, thus preparing the initial stage of the third industrial revolution and digital production. Even today, it is obvious that the establishment of a new techno–economic paradigm will result in massive changes in the field of production and the social sphere. We can expect with high probability that competition will increase, confrontations will intensify, and social, as well as international, tensions will rise. The problem of information security will increasingly rise in importance for individuals and society.

2. The enlargement of the telecommunication infrastructure along with the progress in cognitive computations, expert systems, and big-data technologies will allow one to model economic and social processes, as well as to influence them directly. Obviously, multidimensional investigation of the effects of the new global-information environment on the material and spiritual lives of individuals and the entire society is of central importance.

3. The extension of the information space, the emergence of new technologies that enable domination in various areas of activity, the progress in network technologies for implicit control of group (and mass) behavior, and the programming of destructive actions via social networks all bring a qualitatively new level, viz., the problem of digital inequality and information sovereignty, into focus.

Topical Problems

1. The general methodology, as well as methods for classification, systemization, and multivariate estimation of the risks that are related to the use of information technologies should be developed based on system analysis and methods of socio–technical engineering.

2. To prevent the intensification of digital (conscience and network-centric) warfare, coordinated efforts of the world community, as well as close cooperation in the field of information technologies and information security, are required. An immediate measure that should be taken is the internationalization of the control over the Internet (for example, under the aegis of the United Nations) to ensure, on a state-by-state basis, the digital sovereignty of the members of the international community.

3. The Russian Federation should intensify its participation in the development of international legislation and regulatory support related to the use of global open networks. In the area of the national legislation that concerns information security, a cadastre should be developed to increase the quality of legislative acts and to ensure their consistency.

4. The protection of the Russian information space is one of the priority issues of national security. It is essential to create a national segment of the Internet, which is reasonable from both economic and strategic points of view. For the Russian Federation, it is necessary (a) to create the domestic key infrastructure of the Internet, including national root servers and a national system of route-address information, and (b) to organize the production of domestic electronic components, equipment, and system software. As an example, we can point to the Russian analog of Oracle: the 8.1 Platform that has been developed by the 1C Company.

4. CONCLUSIONS

We would like to make a remark of a more general nature that is somewhat beyond the scope of the problem under consideration. The most important characteristic of today's global economy is the long-term decline in the multifactor effectiveness of production. Figure 3 shows the dynamics of the decline in the global GDP of developed economies for the last 50 years.

It can be concluded that the prerequisites of the forthcoming third industrial revolution are not only technological factors but also economic factors (which are probably even more important). According to the experts from the European Technology Assessment Group (Karlsruhe, Germany), the core of the third industrial revolution will be formed by 21 technology clusters in several key industries. In turn, information technologies are a crucial component of all the technology clusters that transforms them into a new single industrial complex; this will inevitably result in priority development of information technologies, as well as increased competition and an international race in this field. The risks (as well as the cost) will increase considerably.

The third industrial revolution will inevitably change the basic structures of the economy, as well as the composition and structure of society. Taking the economic lag of the last 25 years for the Russian Federation into account, the third industrial revolution is a necessity and a historic opportunity to be seized in a systemic way and in a very short time that is guided only by economic and technological advisability. All the required prerequisites exist to do this: adequate scientific, technological, and human (especially in the field of program systems) resources, as well as the reserve for the future in a number of development directions. The only factor that is needed is a complex state program and its accurate and consistent implementation.

ACKNOWLEDGMENTS

This work was supported by the Russian Foundation for Basic Research, project no 12-06-00092 (Social-philosophical and methodological problems of the technological risks in modern society).

REFERENCES

1. Malinetskii, G.G., Scenarios, strategic risks, and information technologies, *Inf. Tekhnol. Vychisl. Sist.*, 2002, no 4, pp. 83–108.
2. Syuntyurenko, O.V., Infrastructure problems of development and use of high-performance computing, *Inf. Tekhnol. Vychisl. Sist.,* 2003, no. 1, pp. 21–29.
3. Chumakov, A.N., *Globalizatsiya. Kontury tselostnogo mira* (Globalization: Contours of the holistic world), Moscow: TK Velbi, 2005.
4. Gromyko, Yu.V., Lecture on consciental weapon and consciental warfare. http://gtmarket.ru/laboratory/publicdoc/2007/782.
5. Siountiourenko, O., The problems of providing information security: the case of information infrastructure, in *Studies in Eastern Europe: Technological and Environmental Policy*, Banse, G., Ed., Berlin, 2007, pp. 161–179.
6. Liddell Hart, B.H., *The Strategy Of Indirect Approach*, London: Faber and Faber, 1954.
7. Dugin, A.G., Network-centric warfare: New war theory, in *Setevye voiny. Ugrozy novogo pokoleniya* (Network Warfare: Threats of a New Generation), Moscow: Izd. Evraziiskoe Dvizhenie, 2009.
8. Dement'ev, I.O., Intellectualization of global telecommunication systems using semantic networks, in *Materialy Vserossiiskoi konferentsii studentov, aspirantov i molodykh uchenykh MIREA: Iskusstvennyi intellekt: filosofiya, metodologiya, innovatsii* (Proc. All-Russian Conference of Students, Post-Graduate Students, and Young Researchers of the MIREA: Artificial Intelligence: Philosophy, Methodology, and Innovations), Moscow, 2009.
9. Reese, G., Cloud Application Architectures. http://www.msit2005.mut.ac.th/msit_media/1_2557/NETE4640/Materials/20130713172714AN.pdf.
10. Badalyan, L.G. and Krivorotov, V.F., *Istoriya. Krizisy. Perspektivy: Novyi vzglyad na proshloe i budushchee* (History, Crises, and Perspectives: A New Look at the Past and Future), Moscow: Izd. Librokom, 2012.
11. Syuntyurenko, O.V., The social and economic risks of the development of information technologies, *Sci. Tech. Inf. Process.*, 2012, vol. 39, no. 2, pp. 113–116.
12. Gorokhov, V.G. and Syuntyurenko, O.V., Technological risks: Informational aspects of security of the society, *Programmnye sistemy i vychislitel'nye metody*, 2013, vol. 5, no. 4, pp. 344–353.
13. Dbar, S.A., Lacis, A.O., and Hramtsov, M.Y., MVS-express computational system and shmem-express base communication library: Programmer guide. http://www.kiam.ru/MVS/documents/k100/shmem-progman.html.
14. Larina, E.S. and Ovchinskii, V.S., *Kibervoiny XXI veka. O chem umolchal Edvard Snouden* (Cyber Warfare of the XXI century: What Edward Snowden passed over in silence), Moscow: Knizhnyi mir, 2014.
15. Bychkov, I.V., Oparin, G.A., Feoktistov, A.G., et al., Service-oriented approach to organization of distributed computing using the DISCENT instrumental complex, *Inf. Tekhnol. Vychisl. Sist.*, 2014, no. 2, pp. 7–15.
16. Korovin, V.M., *Tret'ya mirovaya setevaya voina* (Third World Network War), St. Petersburg: Piter, 2014.
17. Mayer-Schonberger, V. and Cukier, K., *Big Data: A Revolution that Will Transform How We Live, Work, and Think*, Boston: Houghton Mifflin Harcourt, 2013.

Translated by Yu. Kornienko