ISSN 0147-6882, Scientific and Technical Information Processing, 2021, Vol. 48, No. 2, pp. 97–106. © Allerton Press, Inc., 2021.
Russian Text © The Author(s), 2021, published in Nauchno-Tekhnicheskaya Informatsiya, Seriya 1: Organizatsiya i Metodika Informatsionnoi Raboty, 2021, No. 5, pp. 1–11.

Trends and Risks of Network Technologies

O. V. Syuntyurenko[a, *] and R. S. Gilyarevskii[a, b, **]

[a] *All-Russian Institute for Scientific and Technical Information, Russian Academy of Sciences, Moscow, 125190 Russia*
[b] *Faculty of Journalism, Lomonosov Moscow State University, Moscow, 125009 Russia*
**e-mail: olegasu@mail.ru*
***e-mail: giliarevski@viniti.ru*
Received February 4, 2021

Abstract—Several new directions and trends in the development of network technologies are analyzed by a system approach using scientometric methods and comparative analysis. The spectrum of potential negative consequences of applying new information and network technologies in social, economic, and scientific and engineering activities is considered. Topical problems of developing the national information infrastructure are discussed, as well as information and digital inequality issues. Proposals and recommendations are formulated. The most significant tasks of elaborating on the topic of risks in and threats to the development of network and information technologies are highlighted.

Keywords: network technologies, risks, information infrastructure, Internet of Things (IoT), information security, digital inequality, cloud technologies, e-learning, social programming, technology convergence

DOI: 10.3103/S0147688221020088

INTRODUCTION

The modern digital environment is part of the global media landscape. The dominant trend in the new information environment is the rapid growth of digital data, Internet resources, and a permanent expansion of the global telecommunications network. The digital environment includes the entire continuum of computer and network technologies. The basic macrostructural component of the global digital environment is telecommunication networks and systems, first of all, the Internet, including its largest and long-established web 1 segment; web 2 segment with its social networks and platforms; mobile app web 3 segment (on smartphones, tablets, and other such devices), which has exhibited the highest growth rates for the past 3 years; payment processing networks like Paypal, SWIFT, Bitcoin, and others; and dedicated onboard processors for various production and amenity infrastructure facilities. According to the estimates from International Data Corporation (IDC), the global volume of information doubles every 2 years. According to Cisco, in 2021 the global IP-traffic volume will exceed 3.3 zettabytes (a zettabyte is a billion gygabytes) [1]. The development of network technologies and the Internet entails the change from the hierarchical to the network functional paradigm of the content management system for research and development. The most vibrant direction in the electronic communication development of the research and production sector is the creation of distributed network information assets (IA). It is possible to acknowledge that digital network technologies are deeply *interwined* with the texture of educational, production, and magament processes. The World Wide Web is used as the basis for creating a common digital environment (infrastructure) for connecting machines, equipment, infrastructural facilities, transport, logistical chains, organizations, and intended users. It should be noted that there is still no clear definition of the term *network technologies*. The term that is sometimes used as an alternative is *core technologies*. Generally, network technologies are a coherent set of standard protocols, hardware, and software used in the network environment to implement the entire body of methods, procedures, services, and technologies that shape and sustain the business and digital information environment for acquiring, producing, and processing data in various fields, such as industry, science, and education.

The expansion of the digital environment and the advent and spread of new network and information technologies will result in the numerical and quality growth of various risks and threats to people and societies; this will objectively lead to the growth of various kinds of information integrity threats. It can be predicted with a high degree of probability that such factors as the adoption of new network technologies, the expansion of the global telecommunications network, and the development of semantic Internet and mass media will make the formation of various kinds of risks and growth of information security threats an increasingly pressing issue. According to many experts, one of the interdisciplinary supertasks for this century is to

counter threats and manage risks in complex socioengineering systems [2]. Thus, the development of digital economy makes it an interdisciplinary and, to some extent, transdisciplinary issue of utmost importance and relevance to identify, assess, and mitigate threats and risks for the development and application of new, first of all, network technologies. This article considers the most significant trends in network technologies and a content-limited continuum of frequently indirect risks and threats to using new network and information technologies. These risks and threats are relevant in terms of negative effects of the scientific engineering and postindustrial development of the digital economy.

TRENDS IN NETWORK TECHNOLOGIES

The most significant trends that can be distinguished in the development of network technologies from the standpoint of the system approach, scientometric methods, and comparative analysis are described below.

A. Convergence of Information, Network, and Telecommunication Technologies

Convergence is one of the key trends and a megatrend in the IT sector and provides an essentially new level of technological integration, draws systems of various classes closer to each other in terms of performance properties, and significantly expands the range of IT infrastructure. Convergence means not only mutual influence but also transfusion of technologies when the boundaries between individual technologies are blurred and many important effects occur precisely during the interdisciplinary work across different fields. Convergence results in cutting-edge solutions, networks, technologies, and services with new capabilities. This definition is based on an increasingly intensive application of the IP protocol stack in all aspects of telecommunications and information and media technologies. The use of IP protocols with fixed broadband access and cutting-edge wireless technologies has created a common base for ensuring seamless access to any information from any device anytime in any place. Modern data-processing trends with expanded capabilities of multidimensional statistical analysis show that in the near future information resources will be concentrated in next-gen large-scale supercomputer systems (Big Data systems). In this context, such tasks are mainstreamed to create high-speed telecommunications and design and develop parallel programming tools, including communication interfaces, parallel languages, and language extensions [3]. In the long run it is necessary to develop integrated hyperconvergent systems designed to provide computational capacities, network support, and data storage systems as whole products.

B. Increase in Data Transmission Speed and Communication Channel Capacity

The development of network technologies is based on creating new, more advanced information interchange and network management protocols and developing physical and logical network topology to provide the simultaneous processing of requests from a large number of subscriber systems and make the delivering of data packages to adressees more rapid and reliable by creating alternative routes. According to the forecast by the National Science Foundation (NSF) of the United States, in 2021 the number of Internet users will reach five billion. According to Internet Live Stats, the daily web traffic consumption exceeds three zettabytes. The predicted increase in online activities will affect the rapid transition of telecommunication entities from the available network infrastructure to the concept of multiservice network. A multiservice network is a network environment that is able to transfer audio- and videostreams and data in unified (digital) format along a common protocol (at network level IPv6). Packet switching when used instead of channel switching makes this network always ready for use. Bandwidth, transmission priority control, and quality-of-service (QoS) redundancy protocols allow differentiating services provided for various types of traffic. This guarantees a transparent and consistent network connection and access to network resources and services for both existing client devices and those that will appear in the near future. The past decade has witnessed an active development of global broadband Internet access services (at ≥10 Gb/s). These services are considered the basic elements of the information infrastructure. However, it should be noted that wireless networks currently cover approximately 50% of global web traffic. The next 5 years are expected to bring new types of wireless communications that will be the basis for developing cutting-edge technologies, for example, robotics, autonomous land and aerial vehicles, and healthcare devices. Wi-Fi networks are the basis for high-capacity wireless networks (first of all, Wi-Fi 6, which supports the 2.4 and 5 GHz ranges) and will remain so in the next few years [4]. The first ever fifth-generation (5G) cellular networks were launched in 2018; however, according to the analysts from Gartner, it will take 5 to 8 years to deploy these networks around the world [5].

Some of the research and developments conducted under the auspices of the International Telecommunication Union (ITU) within the framework of megaproject Network 2030 [6], innovative developments included, are described below.

Holographic type communications (*HTC*) will involve creating 3D images either without glasses at all or with AR devices and provide a throughput in gigabits per second.

Tactile Internet for remote operations (*TIRO*) will involve remote work with robots intended for various

purposes, such as computer-aided manufacturing and surgery.

Human System Interface (*HSI*) will allow making 360-degree videos (broad channel) with delays corresponding to the capabilities of eyes and other organs of senses.

C. Snowballing Growth of the Internet of Things (IoT)

Essentially, the IoT is a network of physical items (things) equipped with a built-in technology of interaction and an external telecommunication environment. IoT provides accelerating growth of the share of automatically generated data in the global digital environment. Most IP addresses belong to control systems of things, as well as to industrial, transport, public utility, and infrastructural objects. According to Cisco, in 2021 the number of these IP adresses will exceed 50 billion against 10 billion IP adresses in 2013. According to the estimates by Nielsen Analytics, the IoT currently produces more than 70% of Internet traffic. According to *Business Insider Intelligence*, there will 41 billion IoT devices installed by 2027. The creation and development of these networks is considered to be a technology to reform socioeconomic process by excluding the need for human participation from some part of actions and operations. The dominant IoT solution is remote monitoring [6]. Industrial companies use IoT solutions mainly for optimizing and automating production processes [7]. The most promising technologies are edge computing, 5G, and artificial intelligence. In particular, the formation of the Internet of Things will be greatly affected by the adoption of 5G. The development of IoT technologies will allow making new objects suitable for transmission on the Internet, for example, odors. A machine will analyze the molecular composition of the air in one point and transmit these data along the network. Then this composition, that is, odor, will be synthesized at another point of the network. The prototype of this device (web generator) called Olly has already been made by US-based company Mint Foundry [8, 9].

D. Software Defined Networks (SDN)

The growth of numerical load indicators has made network control more complicated; in the context of tougher reliability and security requirements, networks have become more numerous, significant, and critical. The main transformative trends for network architectures are the accelerating growth and spreading of cellular devices and respective kinds of contents, the virtualization of servers, and the birth of cloud services. The advent of SDN as an essentially new approach to building computer networks has become a promising direction in their development [10–13]. In SDN the levels of network control and data transfer are separated from one another by delegating the functions of control (over routers, switches, and other devices) to apps run on a separate server (with a network operation system). Actually, the physical resources of the network are virtualized. SDN-based technologies allow improving the efficiency of network equipment by 25–30%, cutting the network operation costs by 30%, and improving network security; they also allow the user to create new services in software and promptly upload them to the network equipment. In Russia SDNs are studied at the Applied Research Center for Computer Networks, a resident of Skolkovo Foundation (IT cluster).

E. Development of the Concept of Semantic Internet

The recent decade has clearly outlined the prospects of the Internet's transition to an essentially new level of operation, from handling webpages to the interaction of network hosts through structured data. For this purpose, the Semantic Web standards set has been elaborated, standardized technologies of interaction through web services are used, and data exchange formats and other approaches unified. Frameworks for describing information sources with RDF (resource description framework) standards and semantic domain-specific ontologies in OWL (Ontology Web Language) have become not only a universal adopted approach to data structuring on the Internet but also found use in process standards, for example, ISO 15926. The broad use of semantic topologies is considered one of the main constituents of the evolutionary phase of development of Internet 3.0. That said, respective tools and systems have been designed that allow storing data and interacting with a standard query language and interchange formats. This allows creating integrative Internet solutions connected in a network of linked data (LD). However, this direction has not currently been developed in practice due to the limited availability and complexity of tools for solving these tasks. Nevertheless, some initiatives have been proposed to create tools and services for the transition of the Internet to phase Web 4.0. This phase implies a more active and deeper information interaction among net members and the development of a network of integrated intelligent agents (tools and services) [8, 14].

F. Development of a System of Navigation and Knowledge Searching in a Heterogeneous Network Environment on the Basis of a Universal Intelligent Metadata Converter

In this day and age characterized by an accelerating growth in the amounts of scientific data and the diversity of its kinds and representation formats, information searching has become a critically complex issue. The theory of scientific and technical information has no method of industrial integration of knowledge represented in various sources. The main type of scientific information searching in the global media landscape is

lexical search; this kind of searching is at the core of popular search engines, such as Yandex and Google. However, it is characterized by low search completeness and precision, in particular, because it ignores semantic connections of concepts. The All-Russian Institute for Scientific and Technical Information, Russian Academy of Sciences, has created a methodology and is developing a system of efficiently searching for information in diverse resources containing data indexed according to various classifications, key words, and full-text search capabilities. Supported by grants nos. 17-07-00153 and 20-07-00103 from the Russian Foundation for Basic Research, this project includes the development and adoption of algorithms of automatically converting search queries received in a natural language to a form that provides information searching with various classificatory and descriptor languages. The spatial ontology of scientific knowledge can be represented as a network of semantic links among concepts rendered in key words and classification entries. The specialized database supporting the developed ontology will be the basis for the conceptual navigation across sources structured by various indexing systems [15, 16]. This will provide an efficient search for scientific and technical information in the context of the diversity of information resources on the Web.

G. Trends of Network Management Technologies

The modern digital economy is impossible to imagine without using network technologies in management: this offers both new prospects and challenges and speeds up to the maximum management processes and aquisition of necessary information.

According to [17], the prospective trends of network management technologies are robotic processes automation (RPA), intelligent automation and artificial intelligence (AI), deep learning and Big Data, as well as new modern business modeling tools such as simulation modeling.

Artificial intelligence technologies allow collecting statistical data on the performance of industrial-scale plants, analyzing trends and identifying abnormalities for preventing accidents and predicting the need for maintenance. Using these technologies together with conventional automation methods will make industrial facilities more energy efficient. The prospective solutions for the field of science and technology also include the convergence of network technologies, scientometric methods, and comparative analysis for managing research and development [18]. Network management technologies will use supercomputing, cloud storages, and cloud-based data processing, software-defined networks, and cellular devices (Android, iOS) for visualization, and wireless technologies with low energy consumption (LoRa, ZigBee, BLE). In particular, the latter will be used in autonomous sensors. Summarizing the above, it can be assumed that there is a macrotrend to the active penetration of network management technologies in various social and economic areas.

H. Development of Webometric Network Technologies

Considering the trend for the digitalization of information resources and the swift expansion of digital information landscape, network webometric technologies are steadily growing in relevance and significance. Convergent as they are, these technologies are a relatively new scientific trend and an efficient means of upgrading methods and techniques of using digital IR. Analytical data postprocessing based on scientometric methods and multidimensional statistical analysis of digital IR indicators allows identifying the strengths and weaknesses of electronic libraries, DB generators, and websites of scientific bodies. Webometry allows conducting analytical user research in various sections and forming contrastrive ranking scores of websites. Network webometric technologies and derived systems must be developed by an integrated interdisciplinary approach, including the methodology of computer system design, computational mathematics, and computer linguistics methods, modern network services, and visualization methods. A webometric system must provide nonexpert automatic (automated) generation of contrastive, rating, and integrated scores, identify empirical regularities, and obtain integral characteristics of websites in near-real time mode (the structural analysis of scientific websites must be made using the graph theory and principal component analysis) [19, 20]. Maintaining the open status of a webometric system allows implementing the multiplicity of using an electronic information analytical resource in formation, converting on comprehensive opportunities for the system's prospective re-engineering, and ensuring an essentially higher performance level of structures in the network environment.

Network webometric technologies provide opportunities for undertaking new kinds of scientific and information activities embodied in the virtual environment of the digital information landscape. It should be highlighted that these technologies are relatively cheap, available, objective, and follow the main trends of modern computer science.

I. Development of Network Technologies for Remote Work and E-Learning

The current economic crisis is not quite typical of modern history, which forces businesses and organizations drastically rebuild themselves and search for solutions to efficiently transform their activities. The general trend is to switch to the modern network model of remote work that is easy to deploy, upscale, and control from any point. This model is also easily protected against purposeful attacks that have become

more frequent with the mass-scale transition to remote work mode.

The main directions and tasks of adopting remote work and e-learning technologies are:

• creating the conditions for cooperation in a virtual environment (paperwork, customer and employee communications, conferences, meetings, safe access to network resources, and general staff performance);

• transition to hyperconverged infrastructure (HCI); in this case, however, data storage devices, servers, and networks are additionally connected with software tools;

• organization and supervision of remote employee work (data management, protection and recovery, and workflow control);

• provision of information security (safe access to corporate network, protection of workstations and cellular devices and uninterrupted protections of apps and corporate network against purposeful attacks).

The WebQuest technology enjoys a rising demand with the development of e-learning formats. The peculiarity of the WebQuest is that some or all the information presented on a website for self-guided or group work of students is scattered across various websites. However, valid hyperlinks make this fact unnoticeable to the students and allow them to work in a common information space. The WebQuest technology allows making academic activities a fully vivid, multimedia, and interactive process [21, 22].

The comprehensive adoption of remote work and e-learning solutions is made possible using a broad range of hardware and apps to provide the organization of conferences, meeting, presentations, and webinars, provide safe remote access, form an infrastructure of virtual desktops, manage and administer computer and server equipment, organize remote cooperation in online mode, etc. [23].

J. Network Technologies and Social Networks

A social network is an automated social environment that makes the communication among groups of users who share common interests possible. This communication is arranged on interactive multiuser websites. Social networks are one of the basic communication channels on the Internet. The major strengths of social networks are mass-scale user involvement, mobility, and agility in use, user openness to generating news pegs and dialog [24, 25]. Social networks are classified by type, information accessibility, geographical coverage, and development level (Web 2.0, 3.0, and 4.0 are modern social networks, problem-oriented networks, and prospective semantic webs, respectively). Job-related social networks offer unique opportunities to their target audiences for rapid and high-quality information interchange while managing issues that emerge during research, development, and technology transfer.

The main global trends of social networks are:

• socialization of all socioeconomic segments and, therefore, rapid development of niched and private social networks;

• development of mobile technologies and tools of interaction with social networks as well as mobile social networks using Wi-Fi and Bluetooth;

• broad use of cloud technologies

• using means and models of artificial intelligence;

• formation of new Internet services (cultural, educational, economic, and others) in the structure of social networks.

RISKS OF NETWORK TECHNOLOGY DEVELOPMENT

The spread of information and communication technologies, the expansion of the network information environment, the original interactive essence of the Internet, and the advent of social networks result in new risks and threats to information security and, indirectly, social stability. Network technologies are largely the basis for the development of modern digital economy. It can already be acknowledged that these technologies have become widespread as basic components of manufacturing, production, educational, and management processes, which is attended by the expansion of the range of risk factors. The absence of geographical boundaries, the hard-to-define nationality of objects on the Worldwide Web, and the possibility of anonymous access to its resources all result in greater vulnerability of information, personal, and social security. Since it is not possible to pay enough attention to the whole multitude of IT risks in this short article, let us discuss only some relatively new and incompletely perceived (even by the community of professionals) risks and threats of network technologies.

Rapid Growth of Conventional Risks and Threats in Digital Network Environment

The broad use of modern network technologies creates potential prerequisites for such threats, as information leaks, thieveries, distortions, copying, spoofing, and blocking and, therefore, economic, environmental, social, and other kinds of damage.

With their unauthorised intrusions in computer networks, adversaries can not only copy the information stored there but also contaminate them with viruses destroying applied or system programs that respond after some time (or with the occurrence of certain conditions), which makes the detection of adversaries much more complicated. These actions can result in functional disorders in information systems, protection of critical infrastructure, and controlled objects, and also cause social tensions, for example, in case of leaks and unauthorized use of per-

sonal data, false mine laying at aircraft and railroad facilities, etc. According to *Positive Technologies*, in 2018 the statistics on cyberthreats were as follows: the shares of purposeful attacks, attacks intended to steal personal, accounting, and payment card data were 62, 30, 24, and 14%, respectively; malware was used in 56% of the cyberattacks [26]. It can be predicted with a high degree of probability that such factors as the adoption of new network and information technologies (supercomputing and AI systems included), the expansion of the global telecommunications network, and the development of semantic Internet and mass media will make the growth of conventional risks and threats in the digital network environment an increasingly relevant issue.

Risks of Developing the Internet of Things

It has already been noted above (see subsection C in the Trends section) that IoT is precisely the technology that encourages accelerating growth in the amount of data automatically generated in the global digital environment. According to a predictive study by Amazon, by 2025 the number of these devices (connected power plants, civic buildings, levees, dams, robots, medical implants, and urban and transport infrastructure) will increase to 50 million items, and they will be engaged in at least 2500 to 3025 billion daily sessions. According to expert estimates, by 2022 the IoT will help to create telecommunication networks so complex and convoluted that they will be not only uncontrollable but a priori unreliable. The problem is complicated by the fact that the recent decade has witnessed an active development of broadband Internet that is currently considered a prospective basic part of information infrastructure. The global web including a diversity of segments, such as hierarchical and peer-to-peer networks, optic fiber networks, and repeater station and satellite connections is very vulnerable [27, 28]. Even minor faults, breakdowns, and off-nominal conditions of various instruments, sensors, and software can cause a whole cascade of unpredictable negative effects. According to studies conducted by the Massachussets Institute of Technology, rolling outages and failures due to software errors and imperfections will become part of our daily routine and reach dozens and hundreds of cases every year.

Thus, the main potential economic and social risks of IoT consist not so much in its purposeful use by intruders but in its very existence and further development.

Nontechnical (Social and Personality) Risks and Threats of the Internet

Content risks are found on websites, social networks, forums, blogs, videohostings with ethically negative information encouraging racial hate, pornography, violence, aggression, propaganda of anorexy, phagomania, suicides, narcotics, and other destructive behaviors. Content risks can be linked with other types of network risks; for example, watching certain videos can contaminate the computer with viruses and cause the loss of important data.

Social communication risks have to do with interpersonal relations of Internet users and involve the risk of being verbally abused and attacked by others. Examples of these risks are illegal contacts, for example, grooming, cyber stalking, cyber bullying, and others. The tools used for these purposes are various chats, online messengers, such as ICQ, Googletalk, Skype, social networks, dating sites, forums, blogs, and others.

Internet addiction risks are defined as a compulsive wish to go online and the impossibility to go offline, an irresistible urge to use the Internet with perilous effects on household, educational, social, working, family, financial, and phychological activities [29].

The Growth of Risks of Negative Effects of Modern Digital Network Environment Technologies on Human Behavior and Cognitive Capabilities

A new kind of threat perceived with an increasing degree of awareness during the evolution of network and information technologies is the destruction of forms and methods of personal identification as a result of long-term information and psychological impacts (IPI). Thus, certain types of consciousness can be modified, erased, cease to exist, and displaced from socially acceptable and permissible [30]. There are several main social programming technologies aimed at destroying or transforming consciousness. Their first type is the disintegration and simplification of the information and communicative environment, where a specific consciousness lives and develops; as a result, this environment is made structurally simpler. Secondly, is the dissemination of texts and images that destroy the activity of consciousness by special methods and psychotechnologies along communication channels. A steady trend currently observed among many users is the replacement of logical discursive thinking with its visual associative (mosaic) counterpart. Mosaic thinking makes people much more susceptible to suggestion and prone to noncritical information perception. Thirdly, there is the destruction of forms and methods of personal identification in relation to stable communities, which results in depersonalization and changes forms of self-determination. The main vector is the purposeful change of the public mind and behavioral preferences of large groups by active methods, psychometric algorithms included.

Destructive social networks, new multimedia, and virtual reality technologies engage people in new forms of existence and can affect the construction of identity to some extent. As a result, there is a growing level of

social and personal alienation, destruction of human psyche, and perversion of public morals [31, 32].

Information and Digital Inequality Threats

Information and digital inequality is made a dynamic and pressing issue by the rapid development of network and information technologies. The development of information and communication technologies gives an impetus to integrative socioeconomic processes; at the same time, however, there is a growing polarization among various groups of people, regions, and countries. The danger that emerges is the formation of a new information elite and the expansion of a certain stratum of people made marginal in relation to information and computer technologies. The main factors that encourage the development of information digital inequality are underdeveloped information and communication infrastructure, the high cost of Internet services, a low level of education and digital literacy, absence of social assistance in mastering information technologies, and weak motivation and readiness of various population groups to using information and computer technologies [33]. In terms of geopolitics IT penetration develops very unevenly and sharply intensifies the technological stratification among different countries. As a powerful catalyst of scientific and engineering progress, IT penetration significantly boosts the development of advanced countries and thus foredooms the others to an increasing underdevelopment. This is the reason that it is already necessary to take steps for mitigating the negative consequences of the development of global information inequality, because this issue aggravates the stratification of the society and constitutes a threat to its stability. It should be acknowledged that the development of the digital economy will inevitably aggravate information and digital inequality and, therefore, economic inequality, which will mean threats conditioned by growing sociopolitical tensions.

The Risks of Using Network and Information Technologies in Space and Defence Industries

The development of network and information technologies will inevitably be attended by a growing number of risks conditioned by the broadening use of these technologies in the field of armaments, first of all, in the military space sector (the International Space Station is connected to the Internet, which makes its operation and interaction with the Earth much swifter [9]). The main risks are caused by the existence of fundamental reasons that software cannot be made so reliable as to have no doubt about the impossibility of emergencies that can cause an unauthorized use of nuclear weapons. The existing software verification methods are imperfect. The use of popular object-oriented programming (OOP) and the use of high-level programming languages, such as C++, Java, C# increases the probability of risks of off-nominal software statuses and, therefore, unpredicted situations. OOP code is indetermined. Unlike functional programming, OOP provides no guarantee of having equal output data at equal input data. "In the long run OOP is a ticking bomb that can explode when the code base becomes large enough. OOP provides the developers with too many tools and options without imposing appropriate restrictions. The OOP code encourages the use of shared alterable states that can be nonsecure from time to time" [38].

It should be noted that, according to many experts, the use of OOP in modern aircraft electronics has been the cause of some of the well-known aircraft accidents in recent years (with Boeing 747, SSJ-100, and others). An especially worrysome growth of threats with the evolution of network and information technologies is observed in the increasing scale and complexity of system engineering defence suites. This issue is currently aggravated by the active development and large-scale adoption of supercomputing technologies, robotic and artificial intelligence systems in various defence engineering suites [39].

The Risks of Using Imported Microminiature Circuitry in Telecommunication Systems and Critical Apps

By various estimates, the fraction of processor units and network equipment made by American-based companies is 85%. Several major IT companies integrate target backdoors in their chips to the benefit of security services. The circuits and source codes of wired-in software are known only to the developer. American companies produce an overwhelming amount of industry-standard routers and multiplexing and server infrastructure equipment. As a result of this, even trusted computer systems of most countries are highly vulnerable to external unauthorized actions. According to certain estimates, about 90% of Russia's power grids face high potential risks of malfunction (irreparable outage, hostile takeover, and others) due to both attacks by computer viruses, such as Duqu or Stuxnet, and external unauthorized actions effected beyond their possible detection and identification limits [40]. The leading producers of network software and hardware are US-based companies. Some countries, for example, China are aware of Internet traffic security vulnerability risks and have, therefore, begun to develop national Internet segments. Having raised the possibility of fully giving up on using Microsoft systems, China has succeeded in getting the source program code of the Windows OS as well as the source texts of the software for Cisco routers that maintain the operation of most of the world's networks and servers and are made in China [28]. It should also be noted that almost all of the leading developers that focus on designing software solutions for Internet security, as well as major Internet giants (Twitter,

Google, Amazon, eBay, Facebook and others) are subject to the jurisdiction of the United States.

Cloud Technology Risks

The occurrence of two groups of risks entails the use of cloud and grid computing, first of all, at the corporate level. First of all, companies become more dependent on the reliability of telecommunication systems. Secondly, the sharing of responsibilities in the domain of information security among user companies, owners of cloud platforms, and Internet access providers results in the diffusion of responsibility and degrades the level of controlling and managing security protections.

The main reason that many companies do not dare to adopt cloud computing is security issues. The large-scale adoption of cloud technologies is still impeded mainly by the fears about the integrity of confidential data, including both commercially sensitive information and personal customer data. The main security threats of cloud-based work are data thievery, data loss, account cracking, loopholes in interfaces, and application programming interface (API), distributed denial-of-service (DDoS) attacks, insider activities, hacker intrusion risks, and downtime by the fault of providers [41]. It should be noted that files can be encrypted before being directed to storage, which will provide that the access to sensitive information will be provided only to authorized users (some vendors allow their corporate clients to use proprietary encyption keys).

Negative Aspects of E-Learning and Remote Work

The relevance of developing e-learning and remote employment has been made a pressing issue by the COVID-19 pandemic. For all the obvious positive effects of adopting e-learning technologies in the educational process, these solutions also have their dark side, which includes:

• the need for high-quality technical equipment and access to the Internet. Technical issues are often the sticking point of e-learning. There can be issues with the compatibility of e-learning platforms and operation systems, browsers, or smartphones, whereas low Internet speeds can cause skipping of online classes or difficulties with downloading videorecorded lessons;

• the existence of such factors, as low digital literacy, difficulties with adapting to e-learning formats, and various technical defects. In addition, students do not always have the necessary equipment, that is, a computer and a stable access to Internet;

• methodological discrepancy of network interaction approaches and principles;

• imperfections of and the need for upgrading online education programs, which includes reconsidering the course of classes, providing more detailed and simpler explanations and an increased number of academic hours for studying each topic, expanding the range of learning tools, and other steps, as well as highly skilled specialists able to compose such study guides.

As well, since e-learning has no such section as practice, it is often not possible to use this mode of learning for training practical skills, especially in engineering, healthcare, and pedagogical specialties.

On the whole, the development of remote employment is a major positive step towards a greater flexibility of the labor market and an objective trend, irrespectively of pandemic and other limitations. According to experts, as time goes on, more employees in Russia and abroad will be transferred to teleworking. Whatever the location of each employee, the use of information technologies in this approach to workflow allows the entire company to work in a swift and well-coordinated manner. The negative determinative factors of this approach are a growing number of problems and increased costs of ensuring the information security of private companies or state-run organizations and underdevelopment of information and communication infrastructure in Russia (topology, high-speed Internet, network services, and other components).

CONCLUSIONS

(1) The upgrading of the national information infrastructure, including network topologies, and the creation of new enhanced data interchange and network management protocols, information and telecommunication technologies, as well as software for networks and improvements in their reliablity are extremely relevant for implementing formidable tasks of digital economic development. Such promising directions have been made priorities as Big Data tech and broadband Internet access, whose development in Russia is far behind international levels.

(2) It should be acknowledged that the expansion of the digital media landscape, the advent of new technologies that make it possible to provide dominance in various walks of life, the upgrade of network technologies of hidden group (mass) conduct control, and the programming of destructive actions via social networks raise the issue of digital inequality and information sovereignty to an essentially new level of relevance.

(3) Russian IT companies are not found among the leaders in the domain of information technologies. Considering the growing trend for the incorporation of information and digital resources of many countries into global networks, one should keep in mind the possible transformation of IT risk issues (first of all, in computer systems with critical applications) to the issue of minimizing risks of computer-aided force

pressure [39]. It is obvious that the postindustrial context of information society development makes it impossible to give up on the integration and opportunities of using the global media landscape. At the same time, the uncontrolled integration in the global telecommunication (information, computational) infrastructure without any complex management of computer risks can have far-reaching consequences related to the loss of national information independence. This is the reason that Russia's national strategy of developing information infrastructure and information technologies must combine the maximal use of capabilities for information search, interchange, and processing in network environments with the minimal risks of negative influence on the domestic scientific and engineering information resources, large-scale programs and projects, first of all, in the field of cutting-edge technologies.

(4) The tasks the solution of which is needed for curbing the risks of and potential threats to information and economic security are

(a) developing taxonomic methods of risk classification and collation;

(b) provide early prevention of risks of new technologies and their convergent variants;

(c) developing the methodology of assessing these risks against a multitude of criteria;

(d) developing the methodology, recommendations, and comprehensive measures for minimizing the risks of adopting new (and adapted) network technologies in the national information infrastructure.

FUNDING

The work is supported by the Russian Foundation for Basic Research, project no. 20-07-00014.

REFERENCES

1. According to Cisco Forecasts, the Global Volume of IP-Traffic in 2021 Will Exceed Three Zettabytes. https://mobile-review.com/news/po-prognozam-cisco-mirovoj-obem-ip-trafika-k-2021-g-prevysit-tri-zetta-bajta. Cited January 21, 2021.
2. Malinetskii, G.G., Scenarios, strategic risks, and information technologies, *Inf. Tekhnol. Vychisl. Sist.,* 2002, no. 4, pp. 83–108.
3. Modern Supercomputers: Computing Technologies for Progress. https://integral-russia.ru/2019/09/10/sovremennye-superkompyutery-tehnologii-vychislenij-na-sluzhbe-progressa/. Cited January 21, 2021.
4. Top-5 Trends in the Development of Network Technologies According to Cisco. https://netstore.su/articles/top-trends-2020-po-versii-cisco. Cited January 21, 2021.
5. Ten Most Promising Wireless Technologies of the Future. https://zen.yandex.ru/media/mcs/desiat-samyh-perspektivnyh-besprovodnyh-tehnologii-buduscego-5d4d754f0ef8e700ad7730a9. Cited January 27, 2021.
6. Concept of Network 2030: How the Internet Will Change in 10 Years. https://habr.com/ru/company/ncloudtech/blog/511242/. Cited January 25, 2021.
7. The Future of the Internet of Things—Business Insider Intelligence Report. https://techrocks.ru/2020/08/05/future-internet-of-things/9. Cited January 26, 2021.
8. Prerequisites for Creating a Platform for the Internet of Objects. https://zen.yandex.ru/media/id/5c8ac05452e1b000b34779d8/predposylki-sozdaniia-platformy-interneta-obektov-5d246ad4998ed600aee65306. Cited January 29, 2021.
9. Trends in the Development of Computer Networks and the Internet. https://idaten.ru/technology/tendencii-razvitia-komputernih-setei-i-interneta. Cited January 29, 2021.
10. MintFoundry Found a Way to Communicate Smells on the Internet. https://vk.com/wall-35198041_7. Cited January 22, 2021.
11. Research of Development Trends of Modern Network Technologies on the Example of Software-Defined Networks. https://cyberleninka.ru/article/n/issledovanie-tendentsiy-razvitiya-sovremennyh-setevyh-tehnologiy-na-primere-programmno-konfiguriruemyh-setey. Cited December 29, 2020).
12. Prospects for the Development of Network Technologies. https://compress.ru/article.aspx?id=12094. Cited January 27, 2021.
13. Krasotin, A.A. and Alekseev, I.V., Software-defined networks as a stage in the evolution of network technologies, *Model. Anal. Inf. Sist.,* 2013, vol. 20, no. 4, pp. 110–124.
14. Intelligent Information Networks and the Semantic Web. https://habr.com/ru/post/116574/. Cited January 29, 2021.
15. Syuntyurenko, O.V., Beloozerov, V.N., Dmitrieva, E.Yu., et al., *Set' klassifikatsii po nauke i tekhnike kak mekhanizm smyslovoi navigatsii i poiska informatsii v prostranstve znanii* (The Network of Classifications in Science and Technology as a Mechanism for Semantic Navigation and Information Retrieval in the Space of Knowledge), Available from VINITI, 2019, no. 120-V2019.
16. Shapkin, A.V., Beloozerov, V.N., and Dmitrieva, E.Yu., Integration of linguistic tools for document search in the information space, *Inf. Resur. Ross.,* 2020, no. 5, pp. 34–38.
17. Business 2020: Digital Development Trends. https://zen.yandex.ru/media/id/5b518f187438af00a99201df/biznes2020-tendencii-cifrovogo-razvitiia-5ce256d8b3217a00b388769c. Cited December 31, 2020.
18. Syuntyurenko, O.V. and Gilyarevskii, R.S., The use of scientometric methods and comparative data analysis for the management of scientific research in thematic areas, *Nauchno-Tekh. Inf., Ser. 2,* 2016, no. 12, pp. 1–12.
19. Galloway, L.M. and Pease, J.L., Altmetrics for the Information Professional: A Primer, Special Libraries Association, Biomedical and Life Sciences Contributed Paper, 2013. http://works.bepress.com/linda_galloway/3/. Cited January 21, 2021.
20. Bulycheva, O.S. and Syuntyurenko, O.V., Conceptual provisions and prerequisites for the creation of a webometric system of the digital space of libraries, *Sb. Prez.*

Bibl., im. B.N. El'tsina, Ser. Elektron. Bibl., 2018, no. 8, pp. 19–31.

21. Archilaeva, S.G., Application of Web-Quest Technology in Modern Education. https://urok.1sept.ru/articles/671383. Cited February 2, 2021.
22. Zubekhina, T.V., Kolesnik, A.V., and Markievskaya, L.L., Web-quest technology in electronic education, *Nauchno-Tekh. Inf., Ser. 1,* 2019, no. 3, pp. 20–25.
23. Software and Hardware for Remote Work. https://store.softline.ru/specials/detail/programmnoe-obespechenie-i-oborudovanie-dlya-udalennoj-raboty/. Cited January 29, 2021.
24. How Social Networks Will Change by 2025. https://otzyvmarketing.ru/articles/kak-socialnye-seti-izmenyatsya-do-2025-goda-5-osnovnyh-tendencij/. Cited January 28, 2021.
25. Manaeva, E.V., New communication technologies of social networks in Russian business. https://cyberleninka.ru/article/n/novye-kommunikatsionnye-tehnologii-sotsialnyh-setey-v-rossiyskom-biznese. Cited January 28, 2021.
26. Relevant Cyber Threats—2018. Trends and Forecasts. https://www.ptsecurity.com/ru-ru/research/analytics/cybersecurity-threatscape-2018/. Cited January 29, 2021.
27. Petrov, V.Yu. and Rudashevskaya, E.A., The "Internet of Things" technology as a promising modern information technology, *Fundam. Issled.,* 2017, no. 9–2, pp. 471–476. http://fundamental-research.ru/ru/article/view?id=41775. Cited January 19, 2021.
28. Syuntyurenko, O.V., The risks of the digital economy: Information aspects, *Sci. Tech. Inf. Process.,* 2020, vol. 47, no. 2, pp. 104–112.
29. Kalinina, N.V., Risks and threats of the modern Internet environment and their prevention among minors. https://mou11.edusite.ru/infosec/files/5705e756-f4f3-47cd-a9b4-e13e6b705aa7.pdf. Cited January 21, 2021.
30. Gromyko, Yu., Weapon that targets consciousness: What is it?, in *Al'manakh "Rossiya-210"* (Almanac Russia-210), Moscow, 1997. http://www.pereplet.ru/text/grom0.html. Cited January 21, 2021.
31. Smirnov, I., Beznosyuk, E., and Zhuravlev, A., *Psikhotekhnologii* (Psychotechnologies), Moscow, 1996. https://gigabaza.ru/doc/87209.html. Cited January 21, 2021.
32. Syuntyurenko, O.V., Network technologies of information confrontation and manipulation of public consciousness, *Nauchno-Tekh. Inf., Ser. 1,* 2015, no. 10, pp. 1–7.
33. Syuntyurenko, O.V., Social and economic risks of information technology development, *Nauchno-Tekh. Inf., Ser. 1,* 2012, no. 6, pp. 1–5.
34. Object Oriented Programming: The Biggest Mistake in Computer Science. https://proglib.io/p/obektno-orientirovannoe-programmirovanie-samaya-bolshaya-oshibka-kompyuternyh-nauk-2021–01–23?utm_referrer=https%3A%2. Cited January 22, 2021.
35. Why OOP Is Bad. https://yandex.ru/turbo/ru.hexlet.io/s/blog/posts/pochemu-oop-eto-ploho. Accessed April 2, 2021.
36. Goodbye, Object-Oriented Programming. https://webdevblog.ru/proshhaj-obektno-orientirovannoe-programmirovanie/. Cited February 4, 2020.
37. Why Has Object-Oriented Programming Failed? http://citforum.ru/gazeta/165/. Cited February 4, 2020.
38. Opinion: Object Oriented Programming Is a Trillion-Dollar Disaster. https://tproger.ru/translations/oop-the-trillion-dollar-disaster/. Cited February 4, 2020.
39. Syuntyurenko, O.V., Digital environment: Trends and development risks, *Nauchno-Tekh. Inf., Ser. 1,* 2015, no. 2, pp. 1–7.
40. How Internet in Syria Was Turned off. https://d-russia.ru/otklyuchenie-strany-ot-internetaprecedent-byl.html. Cited January 22, 2021.
41. Security Threats in the Cloud. https://www.tadviser.ru/index.php/Статья:Главные_угрозы_безопасности_в_облаке. Cited January 21, 2021.

Translated by S. Kuznetsov