

National Research Computer Network of Russia as an Infrastructure and Service Platform for a Common Digital Space of Scientific Knowledge

Alexey Abramov^{1[0000-0002-5186-957X]}, Anton Evseev^{2[0000-0002-2867-3034]},
Andrey Gonchar^{3[0000-0003-1184-7189]}, Boris Shabanov^{4[0000-0002-5238-366X]}

^{1,2} St. Petersburg Branch of Joint Supercomputer Center of the Russian Academy of Sciences,
Saint Petersburg 199034, Russia

^{3,4} Joint Supercomputer Center of the Russian Academy of Sciences, Moscow 119334, Russia

¹ abramov@niks.su, ² evseev@niks.su, ³ andrey.gonchar@jscc.ru,
⁴ shabanov@jscc.ru

Abstract. The contribution provides general information on the architecture of the National Research Computer Network (NIKS), operated and developed by JSCC RAS on the assignment of the Ministry of Science and Higher Education of the Russian Federation since 2019. The structure of the service platform of NIKS in the context of the current state and development prospects within the framework of the project of comprehensive network modernization for 2021–2024 is presented. The opportunities provided by NIKS for enhancement of a common digital space of scientific knowledge of the country, increasing the level of accessibility, information security and network protection of its resources and services are denoted. Individual scientific services, information technology services and services for collective use functioning on the basis of the NIKS infrastructure, built, including on massively exploited technologies of federated authentication and developed in cooperation with the global research and education community are introduced and discussed. Special attention is paid to the national identity federation of Russia in the field of science and education, implemented and promising projects and services under its umbrella.

Keywords¹: national research computer network, NIKS, infrastructure and service platform, common digital space of scientific knowledge, research infrastructure, scientific services, federated authentication.

¹ CDSSK–2020: International Conference “Common Digital Space of Scientific Knowledge”, November 10–12, 2020, Moscow, Russia

EMAIL: abramov@niks.su (Alexey Abramov); evseev@niks.su (Anton Evseev);

andrey.gonchar@jscc.ru (Andrey Gonchar); shabanov@jscc.ru (Boris Shabanov)

ORCID: 0000-0002-5186-957X (Alexey Abramov); 0000-0002-2867-3034 (Anton Evseev);

[0000-0003-1184-7189 (Andrey Gonchar); 0000-0002-5238-366X (Boris Shabanov)



© 2021 Copyright for this paper by its authors. Use permitted under Creative Commons License Attribution 4.0 International (CC BY 4.0)



CEUR Workshop Proceedings (CEUR-WS.org)

1 Introduction

The solution of the urgent task of forming a highly demanded and massively accessible Common Digital Space of Scientific Knowledge (CDSSK) based on advanced technologies [1–3] is largely linked to the advanced development of the global sectoral telecommunications network, which is operated and improved in the interests of the sphere of science and education, serving as a high-performance infrastructure and service platform for storing, analyzing and exchanging scientific and technical information in the implementation of research activities, the realization of joint projects with the provision of reliable ubiquitous access to digital research and educational (R&E) resources in a trusted and secure network perimeter.

The corresponding functions are traditionally assigned to the National Research and Education Networks (NREN) existing in most developed countries of the world, which are also responsible for ensuring high-speed network connectivity of R&E organizations in their countries, interconnection with foreign NRENs and network consortia with increased requirements for the quality of service, access of target users to the global ICT space, to public networks, the development and provision to users of specialized scientific services, information technology services and services for collective use [4–6]. In this regard, it is enough to mention the R&E network consortia GÉANT (Europe), NORDUnet (Nordic countries), individual NRENs – Internet2 (USA), DFN (Germany), SURFnet (the Netherlands), RENATER (France), GARR (Italy), which are well known in the professional environment.

It is worth noting that the users of the leading NRENs, in addition to R&E organizations of different levels and departmental affiliation, are also institutions of culture and art, medicine and health care, including libraries, museums, archives, medical scientific and research institutes and centers, hospitals, as well as publishing houses of R&E literature as significant sources of data for CDSSK. According to the established world practice of the functioning and development of NRENs, the demanded R&E resources and services are mainly located in the infrastructure of such sectoral networks and in some cases are available to users only when they are directly connected to them.

In our country, the functions of NREN are performed today by the National Research Computer Network (NIKS, <https://niks.su>), created in 2019 on the instructions of the Ministry of Science and Higher Education of the Russian Federation as a result of the integration of sectoral networks that were independently operated for 25 years – the federal university network RUNNet and the network of the Russian Academy of Sciences RASNet [6–10]. In accordance with the order of the Ministry, the functions of the administrator and operator of NIKS as NREN of Russia are performed by the Joint Supercomputer Center of the Russian Academy of Sciences (RAS) – Branch of Federal State Institution “Scientific Research Institute for System Analysis” of RAS (JSCC RAS).

2 NIKS: general information and features of the architecture

In terms of infrastructure, NIKS is a globally geographically distributed heterogeneous data transmission network of a federal scale with a presence as of 2021 in 38 regions of the country. NIKS directly provides telecommunication services to more than 150 state organizations of higher education and science, mostly subordinate to the Ministry of Science and Higher Education of the Russian Federation [8, 9]. According to rough estimates, more than 300 specialized Russian organizations participate in the exchange of data between themselves and with foreign organizations (connected to their local NRENs) using the infrastructure capabilities of NIKS.

12 leading Russian supercomputer centers of R&E (from the Top50 list, <http://top50.supercomputers.ru>), more than 150 centers for collective use of scientific equipment (CCU), more than 100 unique scientific facilities (USF) are connected to the network with the provision of barrier-free online access for users to such objects of research infrastructure for collective use (within the framework of connecting the operating organizations and if there is a principled opportunity).

On the basis of a global trusted data transmission medium, the network connectivity of participants in scientific, scientific and technical and innovative interaction is implemented, including federal authorities for R&E, research organizations and higher education institutions, world-class research/R&E centers, competence centers of the National Technology Initiative created within the framework of the National Project “Science and Universities”, engineering centers, technology transfer centers.

With regard to the current level of technological development, it can be noted that the backbone infrastructure of NIKS stretches from Amsterdam to Khabarovsk, while the typical bandwidth of communication channels within Russia is from 1 to 10 Gbps. The network has two independent connections to foreign NRENs through the infrastructure of the international consortia GÉANT and NORDUnet with a bandwidth of 10 Gbps [6–10].

Built on the basis of NIKS (and its predecessor networks), long-term sustainable interaction with European interstate consortia of R&E networks, historically perceiving it as a Russian NREN, provides domestic organizations with opportunities for full participation in international research projects, infrastructure support for joint research, access through the implemented connectivity to unique scientific facilities of the Megascience class, demanded resources and services of foreign NRENs, provides opportunities for the transfer of promising ICTs.

The NIKS ecosystem contains numerous sources of digital content for CDSSK, including Russian R&E web resources and services, relevant sectoral state information systems of the federal and regional levels, distance learning platforms, registries of online courses of educational organizations, problem-oriented portals, electronic libraries and archives, thematic and interdisciplinary digital collections of scientific data, etc.

One of the priority tasks of NIKS in the current realities is to provide ubiquitous secure access for students and teachers to the intensively developed and implanted in the education system of online learning platforms, including within the framework of the currently implemented global integrating project “Modern digital educational environment”. NIKS should be given a primary role in providing an infrastructure platform

for organizing access in a secure segment to such objects of critical information infrastructure in R&E, federal and state information systems based on certified solutions using VPN technologies and nowadays encryption protocols for network traffic. In this regard, it is impossible not to mention another complex digital project, which is currently being developed with the targeted support of the Ministry – “Digital platform of researcher”.

The architecture of the NIKS platform, which it is advisable to consider as an infrastructure and service basis for a unified digital environment in the sphere of R&E of the country (Fig. 1), can thus be presented in the context of its following key components and their corresponding tasks, focused primarily on to meet the constantly growing needs of target users and facilitate integration on the basis of the network of the potential of the Russian professional community [8, 9]:

- high-performance network connectivity of participants with special requirements, infrastructure-level services;
- trusted data transmission medium, barrier-free access to objects of research infrastructure for collective use, to digital R&E content;
- infrastructure for digital platforms of the line Ministry, industry applied ICT platforms, state information systems;
- promoting international cooperation in the field of education, science and technology;
- information security and federated authentication;
- wide range of specialized services for the R&E community.

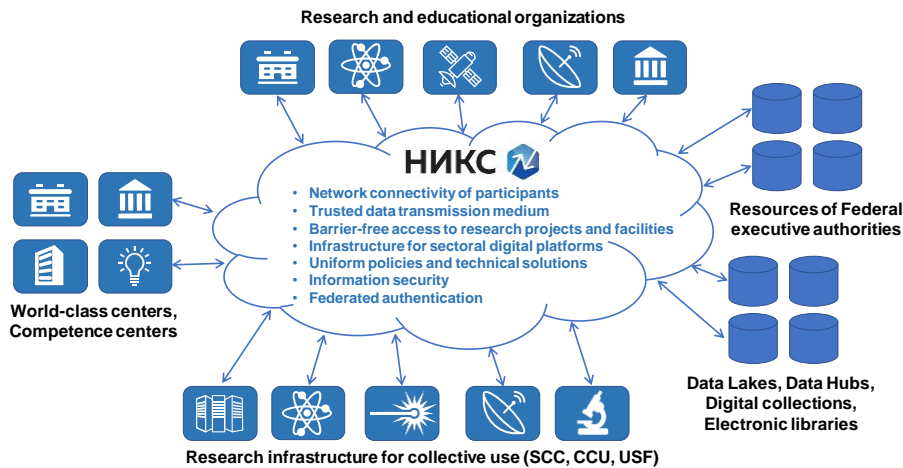


Fig. 1. NIKS as an infrastructure and service basis for a unified digital environment in the sphere of R&E

NIKS, within the framework of the comprehensive modernization of infrastructure and global geographic expansion [8, 9], planned as part of the work on the National Project “Science and Universities” for 2021–2024, is aimed at connecting most of the

leading R&E organizations of the country [11], the main participants of scientific, scientific and technical and innovative interaction, placement in its trusted and protected environment of the demanded objects of research infrastructure for collective use primarily industry-specific supercomputer centers, large digital collections, digital platforms developed under the auspices of the Ministry.

3 Service platform of NIKS

NIKS uses to solve problems on the current operation of the network, provides to users, takes part in the implementation and development of both “traditional” network and specialized “niche” services for R&E, for which the following classification has been developed and adopted with an emphasis, including on the experience of leading foreign NRENs [12]:

- infrastructure services;
- basic network services and telematics services;
- infrastructure monitoring and management services;
- information technology services;
- specialized services for R&E;
- professional services.

In the context of the construction of CDSSK that meets up-to-date requirements, combining heterogeneous R&E resources located in a distributed network environment, a special role, it seems, should be assigned to information and network security services, collection and analysis of statistics on resource use, as well as federated authentication, authorization and access control.

Federated authentication technologies are widely integrated into the public Internet space and are used to seamlessly transition between massively demanded shared resources of general use. With regard to the field of R&E, these technologies solve the problem of creating and ensuring the functioning of a barrier-free trusted environment to provide students, teachers, researchers with opportunities for ubiquitous access to professional information (including with different rights and in the absence of a rigid “binding” to organization-specific IP-addresses) [13–17].

Appropriate access control techniques and technologies have been developed and successfully operated within the framework of identity federations, which are associations of service providers and identity providers that have joined the general regulation in order to securely exchange information about users (when interacting with an account management system) and resources, and grant access to the latter in accordance with the Single Sign On (SSO) conception [13, 14]. In this case, a single user credential is used with the possibility of end-to-end authentication on different resources included in the identity federation, which is performed once at the identification node of the “home” organization (with which the user is affiliated).

Examples of resources proposed by large service providers with federated access capabilities are Scopus and Web of Science citation databases, full-text databases of scientific literature and periodicals such as Elsevier, Springer, EBSCO, Cambridge

University Press, Wiley & Sons, IEEE, and individual digital collections with the results of unique case studies.

NIKS specialists have created a national identity federation called RUNNetAAI (<https://runnetaai.ru>) [16, 17], which since 2018 has been participating in the international project eduGAIN (<https://edugain.org>) – an interfederation that unites today 73 national federations around the world with more than 4300 nodes of identity providers and more than 3200 nodes of service providers [5]. Within the framework of RUNNetAAI, federated access to Scopus and Web of Science, to the domestic Antiplagiat system (<https://antiplagiat.ru>) and a number of other resources has been implemented and functioning in the interests of Russian participating organizations.

It should be noted that federated authentication technologies allow, when establishing the exchange of necessary meta-information between the providers included in the identity federation, to generate objective, reliable and highly demanded statistics on the use of various electronic resources, for example, within the framework of a centrally funded national subscription to scientific information resources.

As other examples of information technology services and specialized application services, including those with federated access, which are currently being operated and developed or are planned for implementation on the basis of NIKS in the near future, one can point to [8, 12]:

- international roaming service in Wi-Fi networks for the R&E community with single credentials and authentication on the side of the “home” organization within the framework of the international project eduroam (<https://eduroam.ru>) [15, 16, 18];
- service for secure access to NIKS and local networks of users from public Internet networks (taking into account the experience of the international project eduVPN, <https://eduvpn.org>);
- cloud services for collective use and collaboration (eduTEAMS, NextCloud, etc.);
- cloud services for distributed work with scientific data (archival and temporary storage, virtualization, data exchange, processing and analysis, reuse);
- communication services in real time for conferences, seminars, personal professional communication (webinars, video conferencing, streaming broadcasts, replicating the eduMEET solution, etc.);
- support services for actual methods and technologies of distance learning (digital learning environments, online or blended education, access to E-content, videoconferencing for education, student management systems, etc.);
- services for numerical computations, visualization and descriptive presentation of results – integrated high-level environments in the form of sought-after “science notebooks” (Science Notebook as a Service, SNaaS).

The emphasis here is primarily on service solutions based on free and open source software developed to a large degree by the community of NRENs representatives.

Among the planned for the creation and development of network and information security services in accordance with the topic under discussion, one should mention the comprehensive protection of the network infrastructure of NIKS, data centers, information systems and services located in the contour of the network, the provision of information security services in the interests of users and their digital resources, technologies and tools for effective protection against DDoS attacks.

The above list of service solutions does not claim to be complete – for example, promising (taking into account the profile activities and competencies of the staff of JSCC RAS) applied services of high-performance computing and artificial intelligence [19–21], development and testing on the basis of the NIKS infrastructure of new ICT, services in the context of the increasingly popular blockchain technology in relation to the optimization of the publishing process, reviewing scientific papers, grant projects, applied Scientometrics, etc.

4 Conclusion

The National Research Computer Network of Russia, officially functioning as the country's NREN, is currently on the eve of a sharp leap in the development in accordance with the federal-approved plan to modernize the main components of the infrastructure and service platform.

NIKS should be considered today as a reliable and secure infrastructure basis and a source of contemporary service solutions for the emerging common digital space of scientific knowledge. Modernization of the NIKS telecommunications infrastructure and significant expanding territorial accessibility will help to smooth the existing digital divide between regions; will allow all scientists and researchers to get access to scientific data of various nature and services to work with them, regardless of their place of residence.

The enhanced service platform of NIKS, the emphasis on the use of federated authentication technologies, time-appropriate information security tools, cloud computing technologies of various delivery models, scientific services and services for collective use forms a saturated trusted service environment of high availability, ensures the satisfaction of the constantly growing digital requirements of target users both for their own needs and during the implementation of joint scientific activities.

The publication was carried out within the framework of the state assignment of the SRISA RAS “Conducting fundamental scientific research (47 GP)” on topic No. FNEF-2021-0014. 0580-2021-0014” (Reg. No. 121031300097-1).

References

1. Antopolskii, A.B., Kalenov, N.E., Serebriakov, V.A., Sotnikov, A.N.: Common digital space of scientific knowledge. *Bulletin of the Russian Academy of Sciences* 89(7), P. 728–735 (2019). <https://doi.org/10.31857/S0869-5873897728-735>
2. Savin, G.I.: Common digital space of scientific knowledge: goals and tasks. *Information Resources of Russia* 5(177), P. 3–5 (2020).
3. Kalenov, N.E., Savin, G.I., Sotnikov, A.N.: The architecture of a common digital space of scientific knowledge. In: *Common digital space of scientific knowledge: problems and solutions: Collection of scientific papers*, P. 7–16. Moscow, Berlin (2021). <https://doi.org/10.51218/978-5-4499-1905-2-2021-7-16>. doi:10.51218/978-5-4499-1905-2-2021-320-333
4. Allocchio, C., Balint, L., Berkhout, V., Bersee, J., Izhevskiy, Y. et al.: *A History of international research networking: the people who made it happen*. Wiley-VCH, N.Y. (2010).

5. GÉANT Compendium of National Research and Education Networks in Europe – 2020 Edition, <https://compendium.geant.org>, last accessed 2021/07/10.
6. Abramov, A.G., Evseev, A.V.: RUNNet: infrastructural and service basis of the national research and education network of the Russian Federation. In: Proc. VIII Int. Conf. “Distributed Computing and Grid-technologies in Science and Education”, GRID 2018, vol. 2267. P. 52–57. CEUR Workshop Proceedings, Aachen (2018). URL: <http://ceur-ws.org/Vol-2267/52-57-paper-8.pdf>
7. Abramov, A.G., Evseev, A.V.: Conceptual aspects of creating a new generation national research computer network in the Russian Federation. *Information Technologies* 25(2), P. 724–733 (2019). <https://doi.org/10.17587/it.25.724-733>.
8. The concept of the functioning and development of the new generation National Research Computer Network for 2021–2024. Minobrnauki of Russia, Moscow (2021).
9. Abramov, A.G., Gonchar, A.A., Evseev, A.V., Shabanov, B.M.: The new generation National research computer network: current state and concept of development. *Information Technologies* 27(3), P. 115–124 (2021). <https://doi.org/10.17587/it.27.115-124>
10. Abramov, A.G., Evseev, A.V., Gonchar, A.A., Telegin, P.N., Shabanov, B.M.: National Research Computer Network of Russia: regulatory status and plans for the development of regional telecommunications infrastructure in 2021–2024. CEUR Workshop Proceedings 2930, P. 29–37 (2021). URL: <http://ceur-ws.org/Vol-2930/paper3.pdf>
11. Abramov, A.G., Gonchar, A.A., Evseev, A.V., Shabanov, B.M.: To the development of criteria for the connection of research and educational organizations to the new generation National Research Computer Network. *Journal of Information Technologies and Computing Systems* 2, P. 22–33 (2021). <https://doi.org/10.14357/20718632210203>
12. Abramov, A.G.: Service platform of the new generation National Research Computer Network in the context of development prospects. *Informatization of Education and Science* 48(4), P. 47–65 (2020).
13. Chadwick, D.W.: Federated Identity Management. In: Foundations of security analysis and design. P. 96–120. Springer Berlin Heidelberg, Berlin (2009).
14. Bertino, E., Takahashi, K.: Identity Management: Concepts, Technologies, and Systems. Artech House, Norwood (2011).
15. Ovsyannikov, A.P., Savin, G.I., Shabanov, B.M.: Identity federation of the research and educational networks. *Software & Systems* 4. P. 3–7 (2012).
16. Abramov, A.G., Vasilyev, I.V., Porhachev, V.A.: Development of the authentication and authorization infrastructure for the identity federation within the eduGAIN and eduroam projects based on the RUNNet network. *ITNOU: Information Technologies in Science, Education and Management* 4. P. 56–64 (2017).
17. Abramov, A.G., Vasilyev, I.V., Porhachev, V.A.: Principles of functioning and management of the identity federation RUNNetAAI in the framework of interfederal interaction with the eduGAIN project. *Informatization of Education and Science* 47(2). P. 40–47 (2019).
18. Abramov A.G., Vasilyev, I.V., Morin, Yu.N., Ovsyannikov, A.P., Porhachev, V.A.: Issues of enhancement the Russian segment of roaming service in wireless networks eduroam in the context of the integration of research and education networks RUNNet and RASNet. The Proceeding of the Scientific Research Institute for System Analysis of the Russian Academy of Sciences 9(6). P. 67–76 (2019). <https://doi.org/10.25682/NIISI.2019.6.0009>
19. Savin, G.I., Shabanov, B.M., Baranov, A.V., Ovsyannikov, A.P., Gonchar, A.A.: On the use of federal research telecommunication infrastructure for high performance computing. *Bulletin of the South Ural State University. Series: Computational Mathematics and Software Engineering* 9(1). P. 20–35 (2020). <https://doi.org/10.14529/cmse200102>

20. Shabanov, B., Ovsyannikov, A., Baranov, A., Leshchev, S., Dolgov, B., Derbyshev, D.: The distributed network of the supercomputer centers for collaborative research. *Program Systems: Theory and Applications* 8:4(35). P. 245–262 (2017).
21. Baranov, A.V., Shabanov, B.M., Ovsyannikov, A.P.: Federative identity for the distributed infrastructure of the supercomputer centers. *The Proceeding of the Scientific Research Institute for System Analysis of the Russian Academy of Sciences* 8(6). P. 79–83 (2018). <https://doi.org/10.25682/NIISI.2018.6.0011>