Puolustusvoimien tutkimuslaitos
Julkaisuja 15

Russia's ICT-infrastructure and its development prospects in the near future

Juho Niskanen

Finnish Defence Research Agency Publications 15
Puolustusvoimien tutkimuslaitoksen julkaisuja numero 15

RUSSIA'S ICT-INFRASTRUCTURE AND ITS DEVELOPMENT PROSPECTS IN THE NEAR FUTURE

Author
Juho Niskanen

PUOLUSTUSVOIMIEN TUTKIMUSLAITOS
FINNISH DEFENCE RESEARCH AGENCY

RIIHIMÄKI 2023

Cover design: Johanna Suominen

ISBN 978-951-25-3412-8 (printed)
ISBN 978-951-25-3413-5 (online publication)
ISSN 2342-3129 (printed)
ISSN 2342-3137 (online publication)

Puolustusvoimien tutkimuslaitos
Finnish Defence Research Agency

PunaMusta
Tampere 2023

Abstract

This publication describes the current state of Russia's ICT infrastructure, how the Russian import substitution program has progressed and what the future prospects are. The publication focuses on the most relevant aspects of the Russian ICT infrastructure, such as telecommunications networks, semiconductor products and software systems. Military technology is not covered in the publication. Much of the publication is based on original Russian sources.

The publication shows that Russia has a functioning ICT infrastructure, but it is largely based on foreign ICT technology. The Russian ICT technology import substitution program has not been successful, except for some software, and Russia is highly dependent on foreign ICT technology.

Russia’s ability to develop advanced ICT technologies in the future is limited due to various structural problems and Western sanctions. Russia will continue to source ICT products through grey imports. In the future, China’s production will play an increasingly important role in the production of Russian ICT components and products.

Russia continues to tighten control over the Russian Internet segment by introducing more effective Internet content control systems and improving existing ones. In the future, the content of the Russian Internet segment will increasingly consist of digital services and content provided by Russian state-controlled companies.

Key Words: ICT Infrastructure, Russian-made ICT Products, Import Substitution, Future Prospects of ICT Technology Development, Russia and China.

Introduction

This publication is based on research reports produced by the Information Technology Division of Finnish Defence Research Agency. This publication relates to the research project called *Changes in Russia's cyber warfare capability*, which was a part of a larger ongoing cyber study in the Information Technology Division.

The main goal of this publication is to depict and illustrate Russia's technical Information and Communication Technology (ICT) infrastructure based on mainly Russian open source publications. The second goal of this publication is to assess how Russia's ICT infrastructure is changing in the short and medium term as far as the beginning of the 2030s.

In this publication the emphasis is mainly laid on Russian ICT technology, software, and ICT systems. Therefore, over the Russian ICT practices and laws have been discussed only to the extent which has been necessary. Moreover, the emphasis is mainly on Russian civilian ICT technology and not on military ICT-technology. The reason for this is that the scope of the study did not allow to write in detail about both issues.

It should be noted that this publication is based on research reports written between 2021 and 2023, so not all the information presented has been updated to the latest data. This applies in particular to the legislation on ICT infrastructure. After the outbreak of the war in Ukraine, Russia has steadily tightened legislation on the control of telecommunications networks and devices used to monitor citizens in the Internet.

The structure of the publication is loosely based on OSI reference model[1], which means that first is analysed the Physical layer of the Russian ICT infrastructure and last the Application layer. Simultaneously it has been described what the presented devices and applications of the Russian ICT-systems are related to.

The publication offers plenty of references for further study and examination of the Russian technical ICT infrastructure. Therefore, the

[1] The Open Systems Interconnection model (OSI model).

publication is a springboard for detailed further research of the Russian technical ICT-infrastructure.

As the Federal Service for Technical and Export Control of Russia (FSTEC) puts it in their scenario papers: first one has to collect information about ICT systems and networks and only after that one can get inside into these systems and networks [1].

List of abbreviations

ARM	Advanced RISC Machine, ARM instruction set architecture. (Computer architecture).
AS	Autonomous System.
CDN	Content Delivery Network.
CERT	Computer Emergency Response Team.
CISC	Complex Instruction Set Computer. (Computer architecture).
CPU	Central processing unit.
CRM	Customer relationship management.
DDoS	Distributed denial-of-service attack, DDoS attack.
DPI	Deep packet inspection.
ERP	Enterprise Resource Planning
FSB	Russian Federal Security Service.
GPU	Graphics Processing Unit.
IaaS	Infrastructure as a service.
IMSI	International Mobile Subscriber Identity.
IMEI	International Mobile Equipment Identity.
IoT	Internet of Things.
IPSec	IP Security Architecture.
IXP	Internet eXchange Point.
LTE	Long Term Evolution.
MES	Manufacturing Execution System.
MIPS	Microprocessor without Interlocked Pipelined Stages. (Computer architecture).
PaaS	Platform as a service.
RISC	Reduced Instruction Set Computer. (Computer architecture).
SaaS	Software as a Service.
SCADA	Supervisory Control and Data Acquisition (system).
SDD	Solid-State Drive.
SOC	Security operations center.
TIER 1	Tier 1 is a network that can reach every other network on the Internet without purchasing IP transit or paying for peering.
VLIW	Very Long Instruction Word. A computer architecture.
VPN	Virtual Private Network.

Contents

1 Russian Telecommunications Networks and Surveillance

In this first chapter, before presenting the actual telecommunications networks, the definition of Russian telecommunications networks, the legislation and how Russian network surveillance is carried out in Russia are introduced.

1.1 Russian Definition for Telecommunications Networks

The Russian Federal Law on Communications[2] mentions Russia's main telecommunications networks [2]. The general concept of the networks is called Unified telecommunications network of the Russian Federation[3] This concept consists of four separate networks:

- Public telecommunications network[4]
- Dedicated communications networks[5]
- Technological communications networks[6]
- Special-purpose communications networks[7]

The Public telecommunications network consists of multiple networks and is connected to global Internet. In other words, these networks compose the Russian Internet segment. Owners of the Public telecommunications networks have to ensure information security and enable surveillance of the networks, which is a common procedure in Russian telecommunications networks.

The Dedicated communication networks are not by default connected to the Internet, but they might be connected to each other. Connecting to the Internet requires permission and if the connection is made, the same rules apply to these networks as Public telecommunications networks. Dedicated networks can be for example companies' own in-house networks.

The Technological communications networks are for Russian industry. Technological communications networks can be connected to the Internet under the same conditions as the Dedicated communication networks, but

[2] Russian: Федеральный закон "О связи".
[3] Russian: Единая сеть электросвязи Российской Федерации.
[4] Russian: Сеть связи общего пользования.
[5] Russian: Выделенные сети связи.
[6] Russian: Технологические сети связи.
[7] Russian: Сети связи специального назначения.

there are special conditions for foreign companies. Legislation on these networks is being tightened [3].

The Special-purpose communications networks are for the Russian government, special services and army. These networks are not a part of Internet, but there is a possibility to connect them into the Internet if needed.

Russian telecommunications networks are under the supervision of Russian authorities. Still, owners of the networks have many responsibilities in relation to telecommunications networks. Especially telecom operators are responsible for their networks and therefore all significant Russian telecommunications network owners are registered in the special register of Russian authorities [4].

Altogether, there are multiple different licences for telecom operators to offer telecommunications services in Russia [5]. In Russia there is no concept of Internet Service Provider (ISP), but instead telecom operator, which can acquire different kind of licences to produce telecom services, like the Internet services. Related to this, the number of licences issued in Russia has fallen significantly in recent years, as telecom operators find it difficult to meet licensing requirements due to the expensive network surveillance devices required by the authorities [6].

1.2 Internet Legislation and Control over the Internet in Russia

In Russia telecommunications networks, especially Internet is strictly controlled by authorities. The key laws in this regard are the Federal Law on Communications and the Federal Law on Information, Information Technologies and Information Protection, which were updated in 2019 [7]. These updates gave the name to the new law: The Law on the Sovereign Internet. The purpose of this law is to ensure the resilience, security and integrity of the Russian segment of the Internet. Moreover, the new legislation made it possible for authorities to monitor Russian networks, their users and operation of the networks centrally.

Altogether Russian Internet legislation tells owners of the Autonomous Systems (AS) and Internet eXchange Points (IXP), how to build their network infrastructure to enable the surveillance and how to act when authorities are conducting surveillance and control over the network. In 2020 Russian authorities even discussed prohibiting using DNS over TLS (DoT), TLS 1.3, DNS over HTTPS (DoH) protocols and Encrypted Server

Name Indication (ESNI), which are essential features for keeping user browsing data private [8].

Attempt to prohibit these protocols and safety mechanisms is related to a quest for better surveillance over the Russian networks and for using its own TLS certificates [9]. In connection with this, Russian authorities have actively tried to block the use of VPN Services in Russia [10]. To avoid harm for Russian business and companies, Russia has created own VPN service that complies with Russian legislation and is suitable for Russian organizations [11].

1.3 Russian Network Surveillance Systems

There are multiple network surveillance and monitoring systems in Russia. These systems are:

- SORM
- TSPU
- GosSOPKA
- TsMUSSOP

These systems consist of multiple subsystems and some of them are interconnected. There are also departments of authorities behind these technical systems for operating and maintenance. In addition, each system has its own area of responsibility related to surveillance.

1.3.1 SORM

The System for Operative Investigative Activities (SORM)[8] is intended for activities against crime and terrorism. Technically the SORM System is widely used in many countries all over the world [12] [13]. In Russia the SORM System is operated by the Federal Security Service of the Russian Federation (FSB) led by the Ministry of the Interior. The data gathered by the SORM System is available also for few other law enforcement agencies.

There have been three phases in the development of the SORM System and therefore there are three versions of the system [6]. The first SORM version was implemented in the 1980–1990s and it was mainly for wiretapping phone calls [12]. Instead SORM 2-3 are capable of monitoring modern ICT

[8] Russian: Система технических средств для обеспечения функций оперативно-розыскных мероприятий (СОРМ).

networks, collecting data and analysing the gathered data. In Russia, there are multiple SORM manufacturers and therefore SORM Systems are not technically unified, but each system works as required by the Russian law [14]. In addition, there is a special SORM ORI System for surveillance of Russian social media [15] and SORM Vitok[9] for Open Source Intelligence (OSINT) [16] [17].

Figure 1 shows Russian VAS Experts company's SORM 1–3 system solution [14]. As can be seen in the figure, there are the SORM 1 for phone calls, the SORM 2 for collecting data and the SORM 3 for analysing the customer data. The SORM 3 is the most advanced, it can analyse and send gathered data to FSB while monitoring the networks [18].

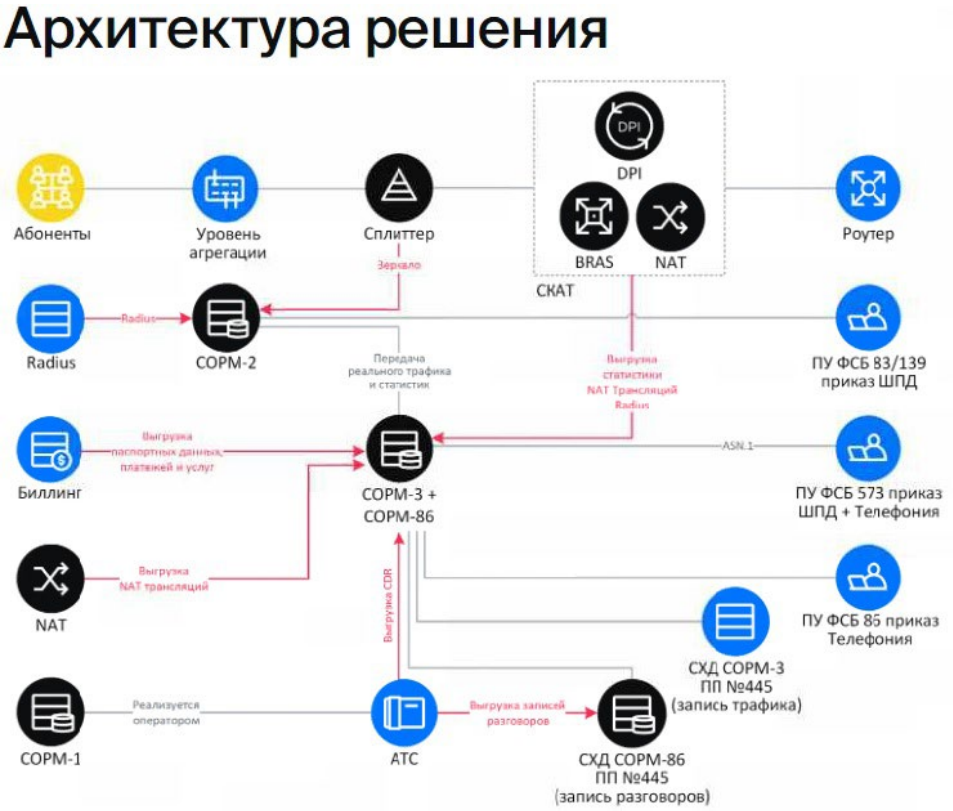

Figure 1. VAS Experts Company's SORM 1-3 system solution *[14]*.

[9] Russian: Комлект СОРМ Виток OSINT.

There is an ongoing connection from the SORM System to the office of the FSB. Connections of the SORM System have been implemented via specific encrypted IPsec VPN channels [19] [20]. Therefore, the FSB can target information requests in real time. The SORM System can gather various information and data. Here is listed the main features of the SORM System:

- Identifying the most common IP protocols
- Inspection of IP packets using DPI[10] technology
- Multiple different options and methods for gathering data
- Works on fixed and mobile networks
- Ability for long-term storage of collected data
- Federation wide system operated by local FSB offices
- A device for monitoring the performance of the surveillance[11]

The SORM system is generally functional, but there have also been a few problems. Firstly, digitalisation and the development of data encryption have made it more difficult to collect data. In the past, it was much easier to collect data from unencrypted analogue channels. As a result, the number of phone tapping licences has fallen significantly in Russia in the 2010s [21]. Despite encryption, there is a wealth of information available to the authorities, such as the time and location of phone calls. In addition, nowadays in Russia customers have to register when they buy a telephone or Internet subscription. Therefore, the customers' IMSI/IMEI[12] data of their telephone is available in the telecom operators' registers to which the SORM System has access.

Secondly, there have also been problems with the storage capacity of the devices and their high cost. Large-scale data gathering takes up a lot of space, as the law requires data to be stored for months ahead. For example, Russian Protej company's devices can record only one percent of all phone calls [22]. This means that the FSB operators have to choose which calls to listen to, as it is not possible to record all phone calls. In addition, the SORM devices are expensive, which has led some small telecom operators to neglect the purchase of devices [23].

---

[10] Deep Packet Inspection, DPI. Deep Packet Inspection means analysis of different IP-protocols such as BGP protocol.

[11] Russian: Ревизор. A device to be installed on the operator's network to monitor that the surveillance is carried out as desired.

[12] The international mobile subscriber identity (IMSI), International Mobile Equipment Identity (IMEI).

1.3.2 TSPU

The TSPU System (technical measures for threat protection)[13] is linked to the above-mentioned Law on the Sovereign Internet [24]. The system has two roles. Firstly, the system must block malicious content on the Russian Internet segment. Secondly, the system must prevent information security threats.

Reportedly, the TSPU system is based on devices that were selected by Roskomnadzor[14] at the turn of the 2020s [24] [25]. According to the findings, the supplier of the equipment is a Russian company called Research & Development Partners (RDP) [26] [27]. The RDP is indirectly owned by the state-owned company Rostelecom.

The TSPU System is linked to the Roskomnadzor's unified register, where the forbidden content is defined [28]. In practice, this means that the TSPU System checks whether the website requested by the Internet user is on the list of banned websites. If the website is on the list of banned websites, the Internet user will not be able to access the website in Russian territory. In addition, the TSPU system is able to slow down the use of foreign Internet services [29].

The second function of the TSPU System is to prevent external security threats, i.e. cyber threats[15] [29] [30]. The TSPU System is reportedly able to prevent cyber-attacks such as DDoS[16] attacks. [29]. Russia sees the evasion of the Internet surveillance as a cyber threat as well and, therefore, the TSPU System is also used, for example, to track down banned VPN services in Russia.

The TSPU and SORM Systems have many similarities, such as the underlying DPI technology of the systems and the connections from the telecom operators to the supervisory authorities. The SORM system is mainly intended for the fight against the traditional crime and terrorism, while the TSPU System is intended for the fight against threats in the information and cyberspace. Thus, the SORM system is operated by the

---

[13] Russian: технические средства противодействия угрозам (ТСПУ).
[14] The Federal Service for Supervision of Communications, Information Technology, and Mass Media.
[15] Russian: противодействия внешним угрозам.
[16] Distributed Denial-of-Service attack (DDoS attack).

FSB security service, while the TSPU system is operated mainly by the Roskomnadzor.

Unlike the SORM System, the TSPU System is paid and installed by the supervisory authorities. The TSPU System is installed on the networks of the Russian major telecom operators, with 60% coverage on fixed networks and 100% on mobile networks [29] [30]. It is impossible to say for sure how the SORM and TSPU Systems have been implemented in reality in the premises of the various Russian telecom operators. Figure 2 shows how the TSPU system is implemented together with the SORM System. In the figure 2 it is not the RDP company's DPI hardware, but the TSPU hardware introduced earlier in 2018. However, the picture shows the principle of how the systems are possibly implemented in the operators' equipment room.

Figure 2 shows that when a customer connects to the Internet, the traffic is first routed to the telecom operator's BRAS[17] router and to the TSPU device.

***Figure* 2.** VAS Experts Company's the TSPU and SORM system solution [31].

[17] Broadband Remote Access Server (BRAS).

If the website requested by the customer is legitimate, the request will be redirected to the Internet. If the website is not legitimate, the TSPU device blocks or slows down access to the website. At the same time, there is a splitter between the Internet and TSPU device, which collects data for the SORM System.

There are different ways to collect data from the network traffic, such as port mirroring, but the Russian TSPU System uses so called tapping by hardware method, where the data passes through the device. This is a method in which the inspection is done by a combination of a separate device and software and the data is collected for the further use. The TSPU System also includes a bypass switch to ensure that the network traffic is not interrupted if the device fails. [32] [33].

Likewise, the RDP company's TSPU System consists of hardware and software. The software is developed by the Russians, but it is not certain whether the hardware is Russian-made. At least the bypass switch associated with the TSPU System is foreign made [32].

As mentioned earlier, the role of the Deep Packet Inspection (DPI) has changed in recent years due to encryption. Therefore, the Russian supervisory authority will not be able to read the contents of IP packets, for example when using the HTTPS protocol. This leaves the option of either blocking the network traffic altogether or allowing it to pass. However, there are problems with the complete blocking of the network traffic as it can cause disruptions to other web services, as happened in 2018 and 2021 when the blocking of Twitter caused several other web services to shut down in Russia [34] [35].

According to the RDP's website, the company's TSPU system may possibly consist of the following devices [36]:

- EcoFilter
- EcoDPI
- EcoBRAS

The EcoFilter and the EcoDPI work together. The EcoFilter device is for URL-filtering and it sends all network traffic to the EcoDPI device for further analysis. If the data is in the HTTP format, the DPI device will compare the requested URL with the Roskomnadzor's blacklist and decide whether the requested website can be used. But if the data is in the HTTPS format, the DPI device tries to find the host certificate or the server name indication (SNI). If the SNI is encrypted, filtering is not possible. The

EcoDPI solution is designed to analyse IP packages up to the application layer (Layer 7) of the OSI model.

The EcoBRAS is a device that allows telecom operators to limit the speed of their customers' connections and control customer's access to the data services. Therefore, the EcoBRAS device is likely to be the device used to silence the Russian media.

In addition to the devices mentioned above, the TSPU System is also likely to include an encryption device. It has been suggested that the device could be a Russian made Kontinent device [37].

1.3.3 GosSOPKA

The Government System for Detecting, Preventing and Eliminating the Effects of Computer Attack (GosSOPKA)[18] system is based on fifth section of the law on Critical Information Infrastructure adopted in 2017 [38]. The GosSOPKA is a system that includes a network intruder detection, prevention, elimination and recovery from an intruder activity. The GosSOPKA system is similar to System of Incident and Event Management (SIEM), but it is nationwide and centralised. According to the law, all organizations belonging to Russia's Critical Information Infrastructure (CII) should be part of the system.

GosSOPKA has close ties with Russian Computer Security Incident Response Team (CSIRT) also known as CERT.GOV.RU (CERT-RU) [39] [40] and with FSCTEC[19]. The CERT-RU is responsible for the governmental networks of Russian Federation. The goal of the CERT-RU is to provide coordination for state authorities, local authorities and law enforcement units on identifying, preventing and removing consequences of computer incidents concerning state information-telecommunication networks. The authority responsible for operating the GosSOPKA System is the FSB, which leads the CERT-RU's activities [40].

[18] Russian: Государственная Система Обнаружения, Предупреждения и ликвидации последствий Компьютерных Атак на информационные ресурсы Российской Федерации (ГосСОПКА).
[19] The Federal Service for Technical and Export Control of Russia (FSTEC) (Russian: Федеральная служба по техническому и экспортному контролю, ФСТЭК (ФСТЭК России).

As a system, the GosSOPKA consists of a main centre and its subcentres. Therefore, the GosSOPKA has a multi-layered structure. The main centre is Security Operation Centre (SOC)[20]. GosSOPKA centres are divided into State and Corporate centres. Operators of the critical information infrastructure have different options for implementing GosSOPKA's requirements [40]. In practice, this means that governmental organizations must be connected to the State GosSOPKA centre, but private companies can form their own centre or join a commercial Corporate centre, which is connected to the main GosSOPKA centre [40].

There are different estimates of how many organizations are covered by the GosSOPKA System, because the system is multi-layered. In 2022, the number of organizations directly connected to the GosSOPKA system was estimated at 670 and 2 500 to the subsystems [41]. The GosSOPKA is not the only SIEM/SOC system in Russia, as there are similar systems in the banking sector, for example [42].

***Figure* 3.** Organizational structure of the GosSOPKA system [43].

[20] Russian: Центр мониторинга информационной безопасности, Главный центр.

Technically, the GosSOPKA System consists of the following parts and features:

- Originally based on the Max Patrol SIEM system from the Russian company Positive Technologies [44] [45].
- Several service providers whose systems meet the regulatory requirements
- Linked to the FSTEC's Data Security Threats Database[21] [46]
- Centralised control over the critical information infrastructure by government administrations.

1.3.4 TsMUSSOP

The TsMUSSOP[22] System is the Centre of Monitoring and Managing of the Public Communications Networks. The task of the TsMUSSOP System is to control and manage the activities of the Russian Internet segment centrally.

Like the TSPU System, the TsMUSSOP System is based on the law of Sovereign Internet mentioned earlier. The law sets out how the centralised control of the Russian Internet segment should be carried out [7]. The TsMUSSOP is basically an administrative organization whose task is to control and manage the Russian Internet by using various information systems and databases. The possible organizational structure of the system is shown in Figure 4. As can be seen in Figure 4, the system has several departments for different tasks. The TsMUSSOP System operates under the supervision of the Roskomnadzor and the Radio Frequency Service[23].

[21] Russian: Банк данных угроз безопасности информации.
[22] Russian: Центр Мониторинга и Управления Сетью Связи Общего Пользования (ЦМУ ССОП).
[23] Russian: Главный Радиочастотный Центр (ГРЧЦ).

***Figure* 4.** The possible organizational structure of the TsMUSSOP System [47].

In practice, the TsMUSSOP implements centralised management of the Russian Internet segment using the systems described earlier. In addition, the TsMUSSOP System has access to all the databases of the systems related to the critical information infrastructure.

The role of the TsMUSSOP System is particularly important when the resilience, security and integrity of the Russian segment of the Internet are at risk. The Roskomnadzor has practised the use of the TsMUSSOP System regularly in annual exercises [48]. Moreover, there have been occasions when the TsMUSSOP System has been used to slow down social media platforms like Twitter [49].

Technologically, the TsMUSSOP System consists of Chinese and Western ICT hardware and software [50]:

- Server computers and database systems implemented mainly on Lenovo hardware and Windows servers
- Network devices implemented on Lenovo, Juniper and Silicom hardware
- Virtualisation implemented on VMware vSphere platform
- Encryption implemented by products of Russian companies Security Code, Infotecs and CryptoPro
- SIEM system implemented on Russian Max Patrol SIEM system.

The main task of the TsMUSSOP System is to monitor the operation of Russian telecommunications networks, which is why Roskomnadzor needs all vital information of all Russian networks and their owners. So, for this

purpose a separate RANR[24] register has been set up to store the data of the Russian AS systems and IXP points. Russian authorities fine the network owners if they fail to provide the requested information.

In addition, Roskomnadzor has published instructions on how telecom operators should transmit all detailed information about their networks to the TsMUSSOP System and how to connect to the Russian DNS system [51]. In practice, this means that Roskomnadzor has full control over the Russian networks and Roskomnadzor will block all networks, which are not registered to the TsMUSSOP System.

There are indications, that the TsMUSSOP System with the TSPU System will be used more and more for cyber threat detection in the future [52] [30]. The reason for this might be a significant increase in DDoS attacks in Russia during the war in Ukraine.

1.3.5 The Overall Picture of the Surveillance

Russia tries to collect information on citizens through the SORM System and to restrict citizens' access to information through the TSPU System. But there are few ways to try to circumvent the surveillance of the networks in Russia [13] [53] [33].

It goes without saying that one should not use traditional phone calls and text messages in Russia, as their data is easily readable by the authorities. One can also try to avoid surveillance by not using web services whose servers are located in Russia. For example, Russian email services and social media platforms such as Mail.ru and Vkontakte are heavily monitored by the authorities and they can read users' data [13]. Therefore, it would be advisable to use foreign encrypted messaging services to circumvent network surveillance in Russia.

However, the problem is that the Russian authorities are doing their best to prevent or restrict use of all significant foreign web services in Russia. This has included restricting foreign encryption protocols and VPN services [33]. In the last two years, foreign VPN services have been in particular at the center of the chase in Russia [53].

[24] Russian: Реестр адресно-номерных ресурсов (РАНР) Рунета.

The use of VPN services to circumvent surveillance depends on the implementation of the VPN solutions. The more IP addresses and servers a VPN service provider has, the harder it is to block the VPN service, because blocking the VPN service is done by blocking the IP address of the VPN server [53]. The TSPU System identifies whether network traffic is coming from inside or outside Russia. However not all of the VPN network traffic coming from abroad is blocked in Russia, as this could jeopardise the VPN connections of Russian companies and thus their business [53].

In the long run, Russia's actions on the country's Internet segment could accelerate the balkanization of the Internet [54]. Russia, China and many others authoritarian countries are examples of regionally segmented networks with limited access to and from the global Internet. So far, Russia does not have the technological capacity to build a system similar to the China's Great Firewall. Currently, Russia's Internet restriction is based on blocking IP addresses and domain names, while China is already using artificial intelligence to find protocols in network traffic [53].

However, there are indications that Russia is also increasingly using advanced technology for surveillance [55]. For example, so called Okulus[25], Vepr[26] and Ohotnik[27] Systems are state-of-the-art Internet content monitoring systems in Russia at the moment [56] [57] [58]. In addition, Russia has advanced technology for facial recognition [59] [60].

[25] Russian: Окулус.
[26] Russian: Вепрь.
[27] Russian: Охотник.

2 Fixed and Mobile Networks

This chapter presents the main physical fixed backbone and mobile networks in Russia. The main emphasis is laid on Russian commercial networks.

2.1 Rostelecom's Backbone Networks on the Map

Rostelecom upgraded its backbone network significantly at the turn of the 2000s by building a renewed optical fiber network extending from Moscow to Khabarovsk in the east, and to Novorossiysk in the south [61]. Today, Rostelecom's backbone network covers almost the entire inhabited area of Russia, but has required upgrading. The main problems with Rostelecom's networks have included [62]:

- non-uniformity of network devices
- network overlap and routing architecture
- difficulties in repairing defects

According to J'son & Partners Consulting, between 2020 and 2030, the Russian backbone network will require 400 000 km of fiber to be replaced [63]. The total length of the fiber-optic networks in Russia is estimated to be around one million kilometers. The need to renew optical fibers will become more important as modern information systems require more and more data transmission capacity.

In early 2021, Rostelecom built a submarine fiber-optic cable link to Kaliningrad, a separate part of Russia's land territory [64]. Before that, a submarine fiber-optic cable had been built in the Kuril Islands, the Kamchatka peninsula, Sakhalin, Magadan and Tsukotsk. Russia's aim has also been to develop backbone network connections from the west of Russia to the east. Related to this, Russia is building a high-speed fiber-optic backbone cable to Asia [65]. In addition, a submarine fiber-optic cable to Asia via the Arctic Northeast Passage is under construction [66]. The construction of this Artic fiber-optic line is a part of the development program for the Arctic region. The fiber-optic line is planned to be completed in 2026.

All Russian backbone networks are illustrated in Figure 5 [67]. As can be seen in the figure, there are a lot of backbone fiber-optic cable lines across the whole country excluding unpopulated areas. The figure also shows that Russia has a large number of cross-border foreign backbone connections, which is a significant difference compared to, for example, China or Iran with significantly fewer cross-border IXP points [68].

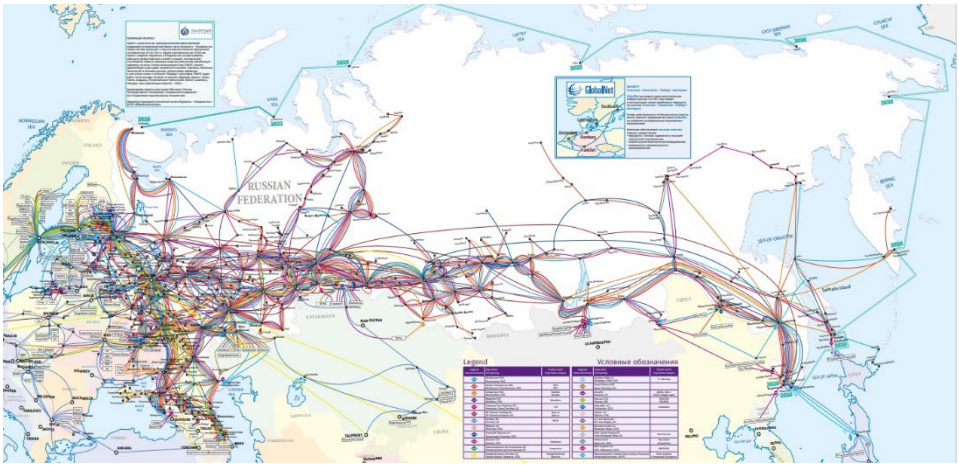

***Figure* 5.** Russian backbone networks and the planned Arctic fibre-optic cable line to Asia [67].

2.2 Fixed WAN and MAN Networks

The requirements for Rostelecom's Wide Area Network (WAN), Metropolitan Area Network (MAN) and access network devices and network connections are described in the company's supplier portal [69]. In addition, Russia has a register called TORP[28], which lists network devices approved for use in Russia [70] [71].

In the 2020s, Rostelecom's WAN networks use equipment from seven different network device suppliers[29], only one of which is Russian [72]. The Russian WAN network supplier is a company called T8 [73]. T8's share of the Russian backbone network market has been limited, only around 10 percent [74]. For this reason, Russia is dependent on foreign suppliers of network devices, in particular the Chinese company Huawei. T8's Volga network platform [75] has been implemented using Dense wavelength-division multiplexing (DWDM) technology, which has also been used for Rostelecom's backbone networks [76].

[28] Russian: Реестр телекоммуникационного оборудования российского происхождения (ТОРП).
[29] Alcatel-Lucent, Huawei, NEC, Infinera, Coriant, ECI and OOO «T8».

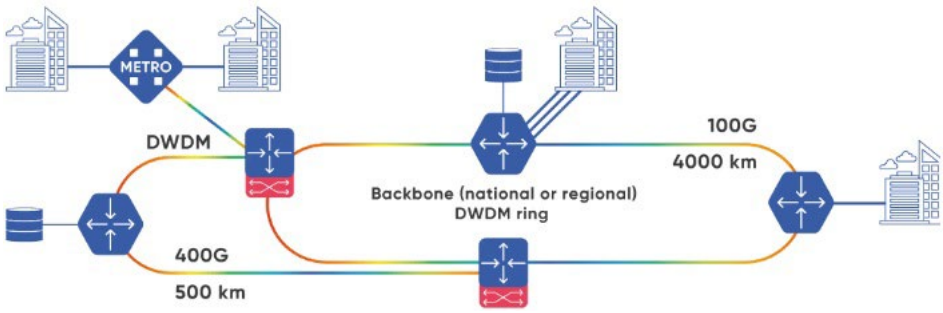

***Figure* 6.** T8's Backbone DWDM networks' topology [75].

Rostelecom's MAN network exists alongside with the WAN backbone network. The MAN network is a high-speed IP trunk line and it is based on the resources of Rostelecom's own primary network, which uses Multi-protocol Label Switching (MPLS) technology to integrate video, speech and data transmission services to customers. The MPLS network uses mainly Juniper, Cisco and Huawei network devices and includes a data center network [77].

2.3 Mobile Networks

In Russia, development of mobile networks has been based on similar factors and needs as in the West. This means that the mobile networks must be able to transmit with a short delay multiple data formats for different purposes. In 2021, there were approximately 300 Long Term Evolution (LTE) mobile networks in 83 different Russian regions [78]. In practice, 4G/LTE networks are available in all major population centres in Russia. Russia has made efforts to extend mobile networks to remote areas.

Russia has had a goal to build mobile networks with Russian base stations [79]. However, Russia has no mobile base station manufacturing of its own and therefore it is almost fully depended on foreign manufacturers. At the beginning of the 2020s, Russia had a total of around 300,000 4G mobile base stations [80]. Sanctions resulting from the war in Ukraine have forced Russia to abandon the deployment of 5G networks.

Russian mobile telecom operators are characterised by a concentration of business in a few large operators, some of which are state-controlled through Rostelecom or by the company owners. The four biggest Russian mobile telephone operators are MTS, Megafon, Bilain, and Tele2 [81].

2.4 Commercial Satellite Communications Operators

Russia has two commercial satellite communications operators in geostationary orbit (GEO), the Russian Satellite Communication Company (RSCC)[30] and the Gazprom Space Systems (GSS)[31] and one operator in low Earth orbit (LEO), the Satellite system Gonets (SSG)[32] [82] The satellites are operated by following:

- Express satellites (RSCC)
- Yamal satellites (GSS)
- Gonets satellites (SSG).

The RSCC company provides a full range of communications and broadcasting services via its own Express satellite fleet of 12 satellites and terrestrial infrastructure. The RSCC possesses the largest GEO satellite constellation in Russia and the company have five ground teleport satellite communications centers in Dubna, Bear Lakes, Skolkovo, Zheleznogorsk, and Khabarovsk [83]. The RSCC has also its own high-speed fiber-optic network.

The Express satellites are manufactured by Franco-Italian Thales Alenia Space aerospace manufacturer on the Russian H1000 platform [84]. The expected lifetime of the Express satellites is 15 years. Most of the Express satellites have launched in the mid-2010s and the latest satellite launch was in 2021.

The GSS company operates and develops Yamal satellite communication system and provides telecommunication and GEO-information services. The GSS has five Yamal 200–600 series satellites and over 400 ground terminals for the use of Gazprom [85]. The expected lifetime of the Yamal satellites is between 10–15 years and the latest satellite launch was in 2019. The manufacturer of the latest Yamal satellites is the above-mentioned Thales Alenia Space [86].

The SSG company provides mobile satellite communications services in low Earth orbit [87] via Gonets satellites. The main purpose of multifunctional system for personal satellite communications Gonets-D1M, is the transmission of data and the provision of mobile satellite

[30] Russian: Федеральное государственное унитарное предприятие "Космическая связь".
[31] Russian: Акционерное общество «Газпром космические системы»
[32] Russian: АО Спутниковая система Гонец.

communications to subscribers. The system is designed especially for transportation and industrial use. This satellite system is possibly built at least partially with Russian components.

In general, it is widely known that Russia has problems with their military satellites [88]. Problems include the adequacy of satellites and their lifetime. This is partly due to Western sanctions which make it difficult to manufacture advanced satellites with long lifespan. [88]. Therefore, it is difficult to say for sure, what the real performance of Russian made satellites and satellite communications is. All in all, in 2022 Russia had approximately 170 satellites including military satellites [89].

2.5 The Coverage of the Networks

The coverage of the Rostelecom's fixed networks can be found on the company's website [90]. Modern high-speed FTTx/xPON[33] Internet connections are available to customers in the biggest cities and slower ADSL[34] connections in the most remote areas.

In general, the use of mobile Internet subscriptions in Russia is significantly higher than that of fixed Internet subscriptions [91]. The most common fixed connection type is the FTTx. Overall, Russia has fairly functioning Internet connections in the populated area [92]. In 2020, the most common average speed for fixed Internet connections was 10 Mbps.

2.6 Russian IXPs, ASs, Tier Operators and DNS

As mentioned earlier, all Russian Internet exchange points (IXP) and autonomous systems (AS) are registered in the Roskomnadzor register [93]. Russia has a total of 35 IXPs all over the Russian territory and the most important IXP is the Moscow MSK IXP [68] [94]. There are about 4,500 active AS systems on a daily basis in Russia compared to 15,000 in the United States [95]. The biggest Russian AS system is the Rostelecom AS [96].

In Russia, the system based on Tier 1 telecommunications operators is slightly different from that in the Western countries and Russia does not

[33] Fiber to the x (FTTx), Passive Optical Networking (PON).
[34] Asymmetric Digital Subscriber Line (ADSL).

officially have any global Tier 1 telecommunications operator[35]. In Russia, the equivalent of Tier 1 telecommunications operators are the country's largest telecoms operators, through which Internet traffic is routed to the global Internet [97].

Below these large telecommunications operators, there are a large number of networks (ASs) of smaller operators, which are peering between each other. Thus, Russia is densely routed inside the country, but has lesser abroad peering than many western countries [98]. For example, in France, there are around 2,500 connections (AS links) with foreign countries and within the country only around 1,500 connections. In Russia, there are around 10,000 connections within the country and around 2,500 connections with foreign countries [98]. However, Russia is important in the sense that approximately 20 percent of Europe's Internet traffic to Asia passes through the Russian Internet segment [99] [67].

Russia has developed its own national Domain Name System (DNS)[36]. The main goal of the Russian DNS system is to preserve access to the Internet for Russians in any case. There have been discussions that Russia should be disconnected from the global DNS system [100].

There are 13 DNS root servers in the world, none of which are located in Russia. However, Russia has anycast DNS root servers, which are copies of the global DNS root servers. Even shutting these anycast DNS servers down would not hinder access to a root server, but would only add delay for some queries of the root zone from some Russian networks [100]. Therefore, one purpose of the Russian DNS system is to copy DNS root server's data to the Russian DNS system and use their own DNS system if needed.

Another purpose of the Russian DNS system is to gather information about the networks of the owners of the AS systems, because they have to share all information with Roskomnadzor. Therefore, that is one reason why Roskomnadzor wants the Russian DNS system working all the time and not only when the global DNS system is not accessible [101].

---

[35] Tier 1 is a network that can reach every other network on the Internet without purchasing IP transit or paying for peering.
[36] Russian: Национальная система доменных имён (НСДИ).

3 ICT Systems on the Russian Networks

In this chapter is described the most significant Russian governmental ICT-networks and systems. The chapter also describes how Russia uses its own backbone networks in the Russian ICT-infrastructure. Russia has hierarchically different levels of administrative authorities within their own information systems, which is why Russia has made efforts to harmonize its governmental ICT networks and systems. Russian e-government systems have been under development since the early 2000s and have still not been finalized. However, progress has been made, but it is still not certain what the complete system will be.

3.1 RSNet and ESPD Networks

Russian State Network (RSNet)[37] is, according to the document of the Russian Federal Protective Service (FSO)[38], a network consisting of ICT systems and ICT networks, which are under the control of the FSO [102]. The main purpose of the RSNet is to connect governmental ICT systems securely to the Internet. In practice, RSNet offers secure IPSec VPN connections to the Russian authorities. As such, there is nothing unusual about the RSNet, rather it is a common organizational intranet with a state-level information security.

The network on which RSNet operates in parallel is called Unified Data Network (ESPD)[39] [103] [104] [105]. The ESPD network allows the creation of virtual networks for government agencies and is maintained by Rostelecom [106].

Both, the RSNet and the ESPD networks, are connected to several Rostelecom's communications nodes and data centers. Altogether, the RSNet network has been developed from the 2020s on, for example by increasing capacity and improving the cyber security [107].

3.2 State IS and GIS Systems

Russian state ICT systems consists of IS[40] and GIS[41] systems. IS systems are top category of the Russian ICT systems [108]. The most salient of

[37] Russian: российский сегмент сети интернета.
[38] Russian: Федеральная служба охраны Российской Федерации (ФСО).
[39] Russian: Единая Сеть Передачи Данных для госорганов (ЕСПД).
[40] Russian: Информационная система (ИС).
[41] Russian: Государственная информационная система (ГИС).

these IS systems are the NSUD[42] and SMEV[43] systems [109] [110] . These systems are federal electronic service platforms for governmental information sharing and integrating registers and ICT systems in one place [111] [112]. For example, Russian state electronic service platform Gosuslugi[44] belongs to the IS systems category. These service platforms are connected to state sub ICT systems.

Russia has hundreds of state and municipal GIS sub ICT-systems [113]. The number of the GIS systems has increased throughout the 2010s and in 2018 there were already 300 systems [114]. An example of a GIS system is the national property maintenance service system, which operates on the Gosuslugi platform [115]. Logging into the GIS systems is done through the central Gosuslugi ESIA[45] portal [116] and the data authentication and secure sessions are implemented with the Russian CryptoPro CSP products [117] [118].

3.3 Gosteh and GEOP Platforms

Gosteh platform[46] is a digital ecosystem for development and use of the state ICT systems [119] [120]. The platform hosts government information systems and promotes the adoption of Russian software. The state GEOP cloud platform is also built on the Gosteh platform.

GEOP[47] also known as GosOblako[48], is a cloud platform that centralises the hardware and software resources for the production of the government e-services [121].

[42] Russian: Национальная система управления данными (НСУД).
[43] Russian: Система межведомственного электронного взаимодействия (СМЭВ).
[44] Russian: Госуслуги, Единый портал государственных услуг Российской Федерации (ЕПГУ).
[45] Russian: Единая система идентификации и аутентификации (ЕСИА).
[46] Russian: Платформа ГосТех.
[47] Russian: Государственная единая облачная платформа (ГЕОП).
[48] Russian: Государственное облако (ГосОблако).

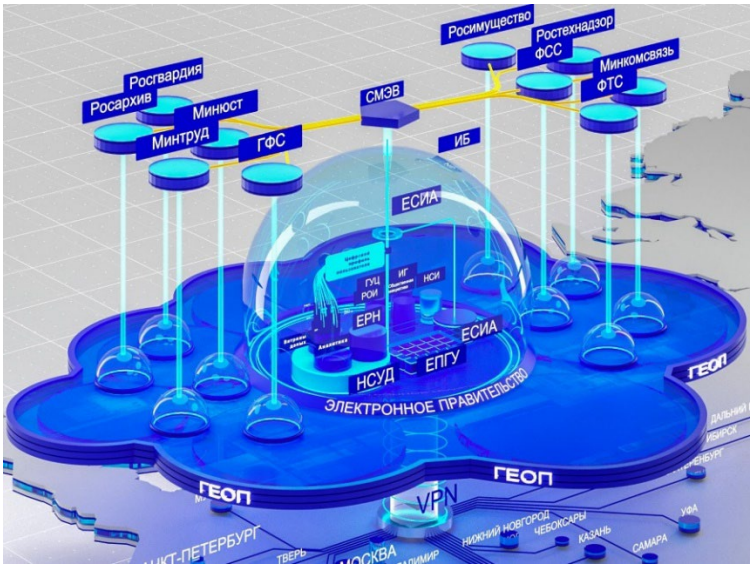

***Figure* 7.** An illustrative figure of the planned GEOP GosOblako [122].

Figure 7 shows the previously mentioned IS systems on an integrated cloud platform. The GEOP GosOblako provides SaaS, PaaS and IaaS cloud services for government agencies. The GEOP system has already been implemented in several government agencies and ministries [120]. The system has been implemented by Russian companies Rostelecom and Voshod. However, there have been problems in completing the GEOP system due to difficulties in obtaining the ICT hardware and software needed for the system [123].

3.4 ZSPD and MTSS Military Networks

ZSPD[49] and MTSS[50] are military networks belonging to the Russian Ministry of Defence [124]. ZSPD network is a kind of a closed military Internet and it operates at least in part on Rostelecom's backbone network.

The MTSS is a newer military network that has presumably its own backbone network and therefore it is not connected to the civilian backbone networks [124] [125]. It is unclear at what stage the development of this new military network is at. By some accounts, Russian military networks are still fragmented [126].

---

[49] Russian: Закрытый сегмент передачи данных (ЗСПД).
[50] Russian: Мультисервисная транспортная сеть связи (МТСС).

3.5 Other ICT Systems at the Federal Level

The Russian security authorities reportedly have a number of their own dedicated federal-level ICT networks and systems. For example, the President has his own federation-wide Situation Center[51] and governmental e-platform[52] [127]. The Presidential Situation Center is linked to the other Russian situation centers, from which the situation picture is compiled. The governmental e-platform is reportedly for the president and prime minister [128]. In 2021, the governmental e-platform was still in development [107].

Related to the ICT infrastructure security, Russia has its own federal-level cyber training range environment [129] [130] [131]. The cyber training environment is provided by Rostelecom and its subsidiary Rostelecom-Solar. The purpose of the cyber training environment is to improve the cyber resilience of the Russian Internet segment. The cyber training environment is nationwide and in 2023 it was possible to connect to it remotely from eight different locations [131].

[51] Russian: Ситуационный центр президента.
[52] Единая цифровая платформа органов власти (ЕЦП ОГВ), Сегмент ЕЦП ОГВ.

4 Data Centers

In Russia, there are state and commercial data centers which are governed by laws and licenses. However, there are many problems with data center management and administration in Russia, for a number of reasons [132].

Russia has an intention to use only Russian-made data centers, especially in government administration. This is linked on the one hand to Russia's import substitution[53] program and on the other hand to Russia's desire to improve information security by using only domestic data centers for storing confidential and classified information [133]. A key obstacle to this goal is Russia's dependence on global data center operators and suppliers, which operate on the basis of Western legislation and certification.

Russian law requires that data containing information on Russian citizens must be located within the borders of Russia [132]. Therefore, there have been problems in coordinating the use of foreign data centers in Russia to comply with the requirements of the legislation. For example, in 2015 Google relocated its servers containing data on Russian citizens to Russia [134].

Problems have also been caused by Russian requirements for companies to disclose information to the Russian authorities as was the case in 2019 when the FSB requested Yandex to provide them with the encryption keys in order to monitor users [135]. In addition, Russian data center operators will have to hand over data of their ICT system architecture to the Roskomnadzor and TsMUSSOP [136].

4.1 Legislation and Standardization

Russia is reforming its legislation on data centers [137]. Previously data centers were not defined in Russian Law on communications. The new legislation on data centers aims to clarify the granting of licenses, the registration of data center operators and access to the state subsidies [138].

Russia has its own standards for data centers, but despite this, the majority of Russian data centers are based on Western standards and certifications. For example, the Rostelecom and its subsidiaries use the TIER data center

[53] Russian: импортозамещение.

standard, certified by the US company Uptime, as the standard[54] for data centers [139] [140] [141].

4.2 Data Center Markets

The use of cloud services in Russia in the 2020s has been significantly lower than in the West [142]. The Russian cloud computing market accounts for around six percent of the total IT market and only three percent of Russian companies use the IaaS[55] cloud computing technologies in their ICT infrastructure [143], while around 27 percent of companies use external cloud services [91]. The number of data centers in Russia has grown steadily in the 2020s and the largest data center operator in Russia is Rostelecom [144].

Currently, the sanctions imposed because of the war in Ukraine are hampering the construction and development of data centers in Russia. In 2022, Russian companies were only be able to manufacture the server racks and cables needed for data centers [145]. The departure of foreign data center suppliers from Russia has meant that the turnkey solutions are no longer available and equipment has to be purchased in a roundabout way. As a result, Russian data center projects are being delayed while Russian suppliers wait for equipment to become available from countries such as India etc. [145].

4.3 Rostelecom's Data Centers

In Russia, the distribution of commercial data centers is such that the majority of all data centers are located in Moscow (76%) and St Petersburg (14%), only a small number of data centers are located in other regions (10%) [144]. Rostelecom has the widest distributed data center network in Russia [139].

[54] TIA/EIA-942 standard.
[55] Infrastructure as a service (IaaS).

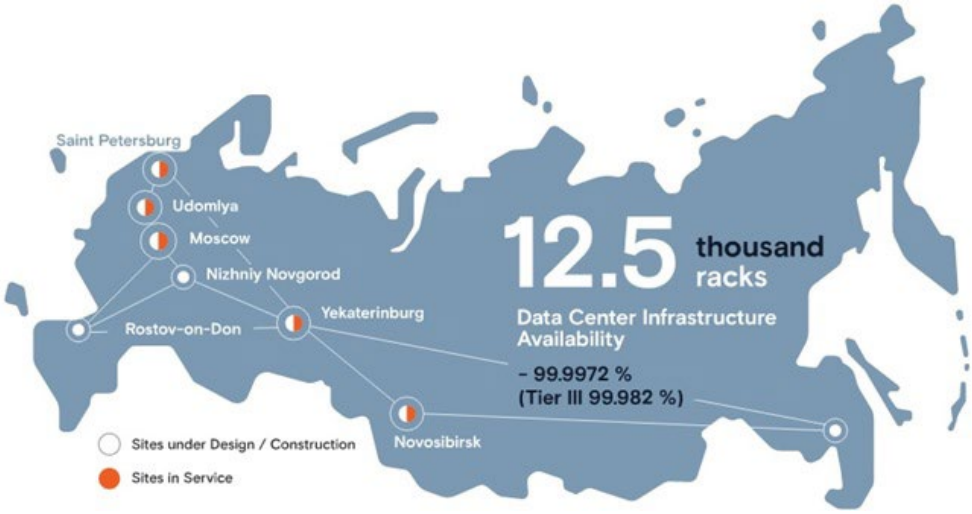

***Figure* 8.** Rostelecom's data centers in 2021 [146].

Rostelecom is an important data center operator as it provides the data center services required by the Russian state. This is one reason why some of Rostelecom's data centers are located close to science centers and key communication hubs, such as the MMTS9 (MSK-IX) data center in Moscow [139]. In addition, Rostelecom's data centers are used for the state IS and GIS ICT systems.

4.4 State Data Centers

The Russian administration has sought to ensure that state agencies do not have to build all the data center capacity themselves but to use so called hybrid cloud solutions where some of data center services are purchased from commercial data center operators when possible [147].

Despite this, Russian ministries continue to use and construct own data centers because they cannot store all data on commercial servers. For example, the Ministry of the Interior is building a large data center in Moscow [133]. The plan is to use processors from the Russian company MCST (Elbrus) for the servers in the data center. Elbrus 4S processors have already been used in the Russian ICT systems, such as the passport system [148]. The problem, however, is that there are not enough microchips available in Russia for Elbrus processors to build large data centers.

Overall, it is unclear how Russia will be able to implement large-scale state data center and cloud service projects in the future, such as the aforementioned GosOblako the state cloud service platform. It is possible

that the existing data centers will become more important in the future. For example, the Russian company Yandex has extensive data center resources including cloud and content delivery network (CDN) services in Russia [149] [150] and there have been speculations about a takeover of the company by the Russian state [151].

5 Semiconductor Production and Hardware

Semiconductor production, or rather the lack thereof, is Russia's Achilles heel. This chapter presents the Russian semiconductor industry and some ICT hardware manufactured in Russia. The chapter also looks at microchip manufacturing from a global perspective. As a rule, military technology is not included, although some of the companies presented are related to military technology (see [152]).

5.1 Terminology and the Global Importance of Semiconductors

5.1.1 Terminology

There are only a few companies in the world capable of producing the advanced microchips used in modern computers and smartphones. Semiconductor products exist for many different purposes such as microcontrollers for embedded systems in home appliances and cars, and systems-on-chips (SoC) in smartphones, for example.

In the public debate, the development state of microchips is often described using the marketing term nanometer (nm), where the number of nanometers reflects the level of development of the microchip. Currently, the world's highest quality microchips are around three nanometers (3 nm). The nanometer range of microchips in ordinary domestic appliances and cars is usually between 45 and 200 nm.

In addition, there are fabless semiconductor companies and companies with their own factories producing microchips. This is something to be aware of when discussing microchip and processor manufacturers. For example, Baikal Electronics and MCST, designers of Russian Baikal and Elbrus processors, are fabless semiconductor companies. The microchips used by these companies are manufactured (fabbed) by the Taiwanese company TSMC [153]. It should also be noted that the companies that manufacture the devices used to make microchips do not usually manufacture the microchips themselves, an example of this is ASML company.

The fabless semiconductor companies mentioned above are designing microchips based on a specific computer architecture or instruction set. The most common computer architectures are CISC (x86) and RISC which

includes ARM, RISC-V and MIPS architectures[56]. A lesser-known computer architecture is VLIW[57], which is used in the Russian Elbrus processors.

5.1.2 The Global Importance of Semiconductors

At the moment, there is global short supply of microchips. This is due to several reasons. Firstly, microchips are very difficult to manufacture and the manufacturing process is difficult to replicate. Therefore, it takes a lot of time and financial resources to manufacture microchips and it is difficult for a single country to build a functioning production system for microchips.

As a result, the manufacture of microchips in the 2000s has been concentrated in just a few large global manufacturers, such as TSMC, Intel and Samsung Electronics. This has been very problematic for Russia, as all major microchip manufacturers except the Chinese have refused to supply Russia with microchips. Microchip manufacturing increases global tensions also in the sense that the world's largest manufacturer, TSMC, is located in Taiwan, which China considers to be part of China. This is underlined by the fact that both China and the United States are also dependent on TSMC's microchips [154].

5.2 Electronics Industry in Russia

Western sanctions on Russia's electronics industry have had an impact since 2014 [155]. Russia has been trying to develop its own electronics industry since the early 2000s without success [156]. In practice, Russia has to source almost all its advanced semiconductor products from abroad and its basic electronics products are of lower quality than Western ones [157]. The Russian microelectronics industry has problems at several levels, including design, manufacturing technology and hardware programming [158].

According to Russia's electronics strategy (2020), the development of telecommunications equipment, computing technology and management systems are particularly important for import substitution and critical ICT

[56] Complex instruction set computer (CISC), Reduced instruction set computer (RISC), Advanced RISC Machine, (ARM), RISC-Five, (RISC-V) and Microprocessor without Interlocked Pipelined Stages, (MIPS).
[57] Very-Long Instruction Word, (VLIW).

infrastructure [159]. However, there have been serious problems with the implementation of the Russian import substitution program for electronics. The main reason for this is that it is difficult for Russia to develop its own electronics market that can compete with international electronics markets in terms of product quality, price and supply chain performance [160]. Other problems include the availability of the technology needed to manufacture electronics and a shortage of skilled labor.

In 2020, Russia had around 1,600–1,700 organizations involved in the development of electronics [159]. The main Russian electronics industry organization is the state-owned Rostec group, which includes the holding company Ruselectronics with over 140 subsidiary companies. Ruselectronics produces approximately 50 percent of Russian electronic components [161]. Russia also has a large number of private companies that supply electronics to state companies and the military-industrial complex. The structure of the Russian electronics industry in 2020 was as follows [159]:

- 420 state-owned organizations (share 55%)
- 1,200 private SMEs with Russian capital (share 23%)
- 30 organizations with foreign capital (share 22 %)

Of the 420 state-funded organizations mentioned above, 370 belong to the Russian military-industrial complex. As mentioned earlier, a significant number of the Russian SMEs are also involved in government contracts, but some of these private companies do not publicly reveal that they produce electronics for the Russian armed forces for fear of western sanctions.

Products from the Russian electronics industry can be viewed on the Ministry of Industry's GISP[58] online platform [162]. The platform's products are classified according to the Russian OKPD-2[59] classification, according to which ICT products fall into category number 26 [163].

It is worth noting that the products on the GISP platform are not 100 percent Russian-made. This is because Russia has a scoring system that allows a product to qualify as a Russian product even if it is not made entirely from Russian components [164]. For example, according to the GISP platform,

[58] Russian: Государственная информационная система промышленности (ГИСП).
[59] Russian: Общероссийский классификатор продукции по видам экономической деятельности (ОКПД).

the Sobol security appliance of the Russian cyber security company SeucrityCode is Russian-made, although the product image of the device indicates that it is equipped with a microchip made by AMD Xilinx [165].

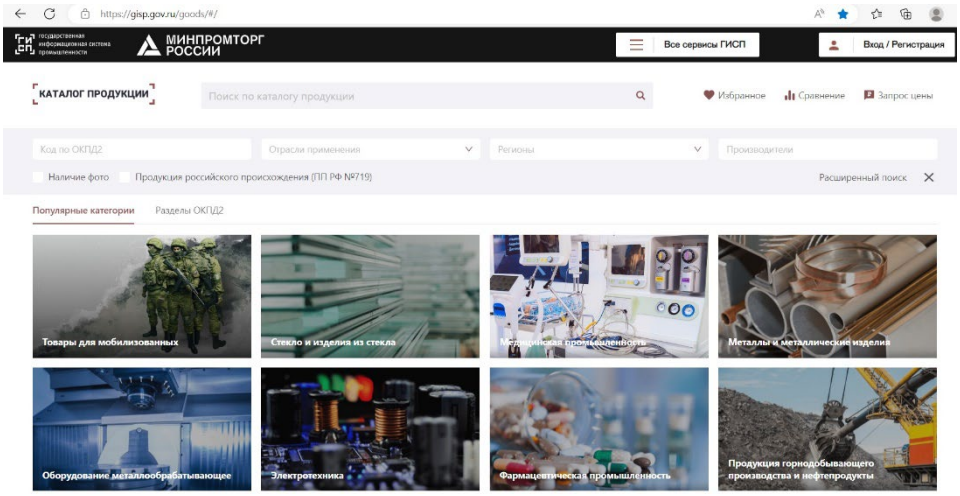

***Figure* 9.** The GISP online platform [162].

5.3 Organizations Designing Microchips

There are several organizations in Russia that design microprocessors and use them in the devices they manufacture. It is worth noting that in 2022, Russia did not have the capability to manufacture microchips smaller than 90 nanometers. As a result, all advanced ICT equipment in Russia has foreign sourced microchips. In other words, Russia's problem is that it doesn't have lithographic machines of sufficient quality to make the microchips on which microprocessors operate.

The following is an overview of the most important electronics companies in Russia and their links to equipment used by Russians, including some military equipment. As a limitation, the presented organizations mainly manufacture microcontrollers or larger semiconductor products.

5.3.1 Microelectronic Conglomerates

To mention just a few, the four significant Russian conglomerates for commercial ICT technology are Rostec, Ruselectronics, Angestrem and GK Element. These organizations are mainly state-owned and include hundreds of Russian technology companies, which is why most Russian electronics companies are at least indirectly state-controlled. This will benefit Russia in the sense that it will allow ownership to be blurred and thus make it easier to circumvent western sanctions.

ICT companies presented in the following subchapters are all on the OFAC[60] sanctions list [166]. The companies have been selected on the basis of their potential importance to Russia's critical ICT infrastructure.

5.3.2 Mikron

Mikron is one of Russia's leading developers of microchips. Mikron is reportedly the only company in Russia that manufactures 90 nm microchips [167]. The company's product range includes smart cards and microchips for cars and IoT among others. The company's problem has been insufficient capacity on the production lines. The company is able to produce about three thousand 90–200 nanometer microchips per month, while the Russia's demand would be 30,000 pieces per month [168] [169]. Mikron is developing also a new MIK32AMUR microcontroller based on the RISC-V architecture with company JSC NIIMA Progress [170] [171] [172]. Mikron is a part of the Russian RTI Systems[61] military technology group [173].

5.3.3 NM-Tech

NM-tech is known to manufacture 200 nm microchips and collaborates with the company Mikron [174] [175] [176]. The production capacity of the company is estimated at a couple of thousand microchips per month. According to the company's website, the company produces microelectronic components on 200 mm silicon wafers [176].

5.3.4 STC Module

STC Module[62] company produces components for navigation equipment and unmanned aerial vehicles (UAV). [177]. There is also information that components developed by the company are used in the Russian Kalibr missile [152].

The company develops special NeuroMatrix digital signal processors (DSP). For example, the NeuroMatrix 1879VM5YA processor model [178] used in the Kalibr missile is used in the missile's navigation system[63].

---

[60] The Office of Foreign Assets Control (OFAC).
[61] Russian: Радиотехнический институт имени академика А. Л. Минца (РТИ) / Концерн РТИ Системы.
[62] Russian: АО НТЦ «Модуль». English: STC Module / RC Module / NTC Module.
[63] Slyusar, Vadym 2022. Ukraine: Lessons learned in the context of SBAMD, JCG SBAMD, 12 Oct. 2022.

The microchip of the processor in question is produced by Fujitsu [179]. This microchip, manufactured by Fujitsu, was launched in 2013 and has a topology of 90 nm. The NeuroMatrix processor dates back to 2012. The STC Module company cooperates with JSC NIIMA Progress [172], which also manufactures components for GLONASS navigation systems.

***Figure* 10.** The NeuroMatrix 1879VM5YA processor [178][64].

5.3.5 NIISI RAN

The NIISI RAN design centre develops Russian Komdiv processors, Baget microcontrollers and firmware [180] [181] [152]. Komdiv and Baget microchips, which have a topology of less than 250 nanometers, are manufactured by TSMC [182]. In the latest Komdiv 64-bit processors, the topology of the microchips is reportedly 28 nanometers [182] [183]. Komdiv processors are based on the MIPS computer architecture and are used, for example, in Russian Su-34 and Su-35 military aircrafts [181] [182]. NIISI RAN has also been linked to the Russian company Korund, which manufactures military computers with Elbrus 8S processors [184].

Other major fabless microchip companies in Russia include Elvees and Yadro. Elvees[65] is one of the few Russian companies designing SoC microchips [185]. Both are dependent on TSMC's microchips. The following is a brief introduction to Russia's most famous processors, Baikal and Elbrus [186].

[64] Photo from right: Slyusar, Vadym 2022. Ukraine: Lessons learned in the context of SBAMD, JCG SBAMD, 12 Oct. 2022.
[65] Russian: АО НПЦ ЭЛВИС.

5.3.6 Baikal Electronics

Baikal Electronics is a fabless SoC microchip maker. Baikal processors are used by several Russian computer companies and computers with Baikal processors are used by the Russian state administration and companies. For example, the Russian company Graviton sells server machines that run on two Baikal-8C processors and use Russian operating systems [187]. There are also two workstation versions of the Baikal processor, Baikal-T and Baikal-M (BE-M1000). The Baikal-M processor has also been developed into a laptop computer primarily for government agencies [188]. Baikal-M and C processors are based on ARM architecture with 28 nm topology and Baikal-T on MIPS architecture.

It is not certain how much TSMC company was able to supply Baikal Electronics with microchips before it stopped supplying in 2022. There are estimated to be many thousands of computers running on the Baikal processors in Russia, especially in state organizations. Overall, Baikal-M processors are outdated [189] and more expensive than similar computers on the global market.

5.3.7 MCST Elbrus

MCST Elbrus company[66] designs processors on VLIW architecture. Like Baikal Electronics, MCST is a fabless microchip company. Elbrus processors are widely used by the Russian authorities. This is partly because the Elbrus processor is well suited for server and database use. In contrast, little consumer software has been designed to fit the Elbrus architecture.

Elbrus processor-based servers are suitable for government database systems but not for the Russian banking sector. In 2021, Elbrus-8C processor failed Russian Sberbank's tests due to lack of performance [190]. MCST has four different versions of Elbrus, the most used being 8C and the latest 16C [191]. The development and deployment of Elbrus processors has been hampered since TSMC stopped supplying microchips.

5.4 Commercial Super Computers

Supercomputers are important for the high-performance computing that is essential for the development of new technologies. According to the

[66] Russian: АО МЦСТ Эльбрус.

TOP500 supercomputer list, the highest-ranked Russian supercomputer in November 2022 was Yandex's Chervonenkis at number 25 [192].

Russia has seven supercomputers in the TOP500 list, five of which are in the top 100. Overall, Russia ranks 12th in supercomputers, accounting for 1.4 percent of all supercomputers. Russian commercial supercomputers are based entirely on Western technology, mainly Nvidia CPU/GPUs.

Russian commercial supercomputers are mainly owned by large companies and universities such as Yandex, Sberbank, MTS and MGU[67] [193]. Among Russian ICT companies, T-Platformy has been developing the Lomonosov 2 supercomputer together with MGU and the supercomputer is ranked 290 on the TOP500 list. However, the T-Platformy company went bankrupt in 2022 and the company has possibly been taken over by the Russian state [194].

5.5 Smartphones

Since the early 2010s, Russia has been developing its own smartphones based on foreign microchips and components [195]. By 2023, Russia had not been able to develop a single smartphone with a Russian microchip (SoC) while the above-mentioned Elvees company has designed a microchip suitable for smartphones [196].

Russian state companies, such as the postal service and state railways, have ordered a large number of ostensibly Russian-made smartphones, such as the INOI-R7 and Qtech-QMP-M1 [195]. These smartphones are ostensibly Russian because, for example, Qtech's QMP-M1 smartphone is actually Chinese Phonemax M1 smartphone [197]. What these "Russian" smartphones have in common is that they use the Aurora[68] (Sailfish OS Jolla) operating system (OS).

[67] The Moscow State University. Russian: Московский государственный университет (МГУ).
[68] Also known as: Sailfish Mobile OS RUS. Russian: ОС Аврора.

***Figure* 11.** QTECH QMP-M1-N IP68 smartphone [198].

Russian smartphones are not popular with ordinary consumers due to their poor performance and range of applications. For example, the "Russian" AYYA T1 smartphone, launched in 2021, has not sold despite the fact that many foreign suppliers have stopped supplying smartphones to Russia [199]. The AYYA T1 smartphone was marketed as data-protected because of its features, which is why the thousands of smartphones ordered are likely to be used mainly by public authorities. The AYYA T1 smartphone is made by a subsidiary of Rostec, but the smartphone uses Taiwanese MediaTek Helio P70 SoC. In 2022 AYYA T1 smartphone development ran into difficulties [200]. In the first half of 2023, the largest supplier of smartphones to Russia was the Chinese company Xiaomi [201].

5.6 Use of Russian-made ICT Hardware

Russia has tried to use Russian semiconductor products in the critical ICT infrastructure. Below are presented a few devices or systems where (ostensibly) Russian microchips are known to have been used.

As mentioned earlier, Russian processors are mainly used by government organizations. There are also indications that some companies in the energy industry may be using Elbrus processors for their ERP systems [202].

One major Russian server supplier is the Jahont company which supplies Jahont database servers powered by Elbrus 8S processors [203]. Jahont company also manufactures SORM equipment and is a part of the Norsi Trans Russian ICT company [204] which manufactures Tiara server platform with Baikal-M processors [205]. Jahont server systems are used, for example, in document management systems for public authorities (Jahont-YVM E12) and in the healthcare sector (Jahont-EMK)[69] [203]. Reportedly Jahont servers are running on Astra and ALT SP Linux operating systems [206].

In Russia, there is limited production of peripherals related to microchips, such as motherboards and solid-state drive (SSD) devices. For example, the Russian company Edelweiss has manufactured motherboards for Baikal microchips [207] and GS Nanotech manufactures SSD flash memories [208]. However, it is unclear what the grade of SSDs is and to what extent they are Russian-made.

In computer networking, Russian processors are used in routers manufactured by Istok company. Istok belongs to the Ruslectronics group and manufactures routers using Baikal BE-T1000 processors [209]. By the end of 2022, 5,000 routers were reported to be produced but the problem in the future is likely to be the limited number of the Baikal processors.

In terms of information security, there are at least three companies in Russia that manufacture data diodes[70], Ancud, CBI and AMT Infodiode. Of these companies, AMT Infodiode in particular specialises in the security of Russia's critical ICT infrastructure [210]. However, it is uncertain whether these devices are Russian-made either.

***Figure* 12.** Ancud company's DIOD 1000-SX data diode adapter [211].

[69] Russian: Яхонт-УВМ Э12, ЯХОНТ-ЭМК.
[70] Data diode technology lets information flow safely in only one direction.

6 Operating Systems and Software

In March 2022, the Russian President issued an order that no more foreign software may be purchased for Russia's critical ICT infrastructure and that the use of existing foreign software must cease from the beginning of 2025 [212]. This in itself is nothing new as Russia has been striving for independence from foreign software for years without success.

Russia has had to compromise on its ICT import substitution targets several times and it is unlikely that Russia will be able to fully implement the switch to Russian software. The previous target was to have a 50–70 percent share of Russian software by the end of 2021, but only a 30–35 percent share was achieved [213].

However, Russia has prepared a software replacement in which a substitute for the main Western software has been developed [214]. Currently, the Russian Software Register contains about 14,000 pieces of software classified as Russian software [215] [216].

In recent years the Russian software market has been growing [217] and the Ukrainian war has led to a significant increase in demand for Russian software as foreign software companies have withdrawn from the Russian market. [218].

According to a survey published in 2022, about a half of Russians who had used Russian software were satisfied with quality of the software [219]. 60 percent of the survey participants had used Russian software and 67 percent of them would be willing to use Russian software if the quality of software improved and the range of products expanded. 29 percent of respondents had Russian Internet browser and anti-virus software on their work computers. Russian office and email software were used by 18 percent of respondents. Only 4–9 percent of Russian employees had a Russian operating system, CRM system or video conferencing system in place. Respondents' use of Russian operating systems and office software on their home computers was even lower [219].

6.1 BIOS and Operating Systems

6.1.1 BIOS

Basic Input/Output System (BIOS) and Unified Extensible Firmware Interface (UEFI) are firmware used to provide runtime services for operating systems and programs and to perform hardware initialization

during the booting process. According to the Russian Software Register, there are companies in Russia that produce BIOS and UEFI software. For example, the Russian IT company Kraftway produces BIOS software [220]. Another BIOS/UEFI software manufacturer is Numa, which has the approval of the Russian FSTEC authority and the company's BIOS/UEFI software is intended to replace the BIOS/UEFI software of AMD and Intel companies [221].

6.1.2 Operating Systems

All operating systems developed in Russia are Linux-based. Operating systems developed in Russia cannot be called fully Russian, because they are based on Linux versions developed in the West, which have been modified in Russia and further localised for their own specific needs. Russian operating systems are certified by the FSTEC.

The following is an overview of the operating systems used in Russia's critical infrastructure:

- Astra Linux
- MSVS Linux
- OSNova Linux
- ALT SP Linux
- RED OS Linux
- ROSA Linux

6.1.2.1 Astra Linux

There are two versions of the Russian company RusBITech-Astra LLC's Astra Linux operating system. Astra Linux Special Edition and Astra Linux Common Edition [222]. Astra Linux distributions are available for the four instruction sets: x86 (AMD/Intel), ARM (Baikal), VLIW (Elbrus) and MIPS (Komdiv). The Astra Linux distribution versions differ in the level of security in that the general-purpose Orjol version (Common Edition) has the lowest level of security, the second highest level of security for the Voronezh version and the highest for the Smolensk version (Special Edition). A mobile version of Astra Linux has also been developed [223].

In Russia, Astra Linux Special Edition is used by public authorities, some energy companies and nuclear power plants [224]. Western sanctions have accelerated the Russian authorities' move to Astra Linux [225]. In addition, Astra Linux Special Edition was also certified for use by the Belarussian authorities in 2021 [226].

6.1.2.2 MSVS Linux

MSVS[71] Linux is a military operating system that was introduced in Russia back in 2002 [227]. The MSVS operating system has been developed by the Russian VNIINS Research Center[72] according to the requirements of the Russian Ministry of Defense. There are 32-bit and 64-bit versions of the operating system and it runs on x86, SPARC and MIPS processor architectures.

The MSVS operating system is functionally obsolete, with issues such as difficult to install modern advanced software [228], which may be one of the reasons why the Russian Armed Forces started to switch to Astra Linux Special Edition from 2018 onwards [229]. The MSVS operating system is likely to remain at least partly in use in the Russian armed forces, as the transition period for the change of operating system is several years [230].

6.1.2.3 OSNova Linux

The OSNova[73] Linux operating system is developed by the Russian company NPPKT and is intended for processing classified data [231] [232]. OSnova operating system is based on Linux Debian 10th version and according to the product description it is recommended for use where confidential information is handled [233]. The operating system is approved by the FSTEC authority.

6.1.2.4 ALT SP Linux

ALT SP Linux is an operating system developed by the Russian company Bazalt SPO and is certified by the FSTEC authority [234]. ALT SP Linux is a general-purpose operating system and can be used on standard desktop computers, but also on servers. ALT SP Linux is available for the three instruction sets: x86, ARM (Baikal) and LVIW (Elbrus).

ALT SP Linux is used, among others, by the Russian MFTs platform, which is developed to replace Western platforms [235]. The operating system is also used in educational and healthcare organizations [235].

---

[71] Russian: Мобильная Система Вооружённых Сил (МСВС).
[72] Russian: Всероссийский научно-исследовательский институт автоматизации управления в непромышленной сфере имени В. В. Соломатина, ВНИИНС.
[73] Russian: Операционная система общего назначения (ОСОН) "ОСнова"

6.1.2.5 RED OS Linux

The RED OS Linux operating system from the Russian company RedSoft is available for workstations and server versions [236]. RED OS Linux is available for x86, ARM and LVIW instruction sets.

RED OS Linux distribution is widely used in Russia. The RED OS operating system is used on server machines at Rostelecom and by some Russian authorities such as the Russian judiciary [237].

6.2 Mobile OS Aurora

The Aurora OS[74] operating system is originally the Finnish Jolla company's Sailfish operating system [238]. The Aurora OS is further developed by the Russians and it is certified by FSB and FSTEC [239].

The Aurora operating system is available for sale in Russia only for mobile devices of corporate and government organizations, according to the Aurora company's webpage [240]. The Aurora operating system is marketed as secure and is used by some Russian state-owned companies, such as Russian Post [241].

6.3 Other Mobile Operating Systems

There are three mobile operating systems in Russia, the aforementioned Aurora, Astra Linux and Rosa Linux [242]. There is also one operating system for embedded systems. The OS ROSA mobile OS is based on the ROSA Linux desktop operating system [243] and is still under development [242].

The only manufacturer of operating systems for embedded systems in Russia is reportedly Navitel. Navitel develops Navitel Embedded Linux operating systems mainly for navigation devices [244] [245].

6.4 Russian Distribution Services

In Russia, three new distribution services were launched in early 2022 [246]. Distribution services are designed to replace the popular Google Play distribution service for Android Apps [247] [248]. The Russian distribution services are called NashStore, RuStore and RuMarket. The

[74] Russian: ОС Аврора.

reason for the development of the platforms were Western sanctions; Russian consumers have not been able to use Google Play normally.

According to the NashStore's website, there are about three thousand applications on NashStore [249]. Hundreds of Russian software companies have been involved in the development of NashStore, because these companies want to have their own applications on the platform. However, the rapidly deployed distribution service has had problems with the quality of the platform and the range of applications [250].

The RuStore distribution service is supported by the Russian Ministry of Digital Development [251]. In practice, the RuStore is a distribution service provided by Russian state-owned companies, including applications from major Russian banks [248] [246].

The RuMarket is reportedly the smallest of the distribution platforms in terms of number of applications [252] [246]. What these Russian distribution services have in common, is that they are downloadable via an APK file, unlike Google Play. Moreover, Russian delivery services reportedly allow to pay using the Russian MIR payment system.

In addition to these distribution services, Russia has an electronic RusSoft platform for Russian software, supported by The Ministry of Digital Development, which aims to support Russian software development [253].

Although Russian software and distribution services are not of the same quality and scope as Western ones, but they allow Russia to use its own distribution services if it is completely blocked from using Western distribution services and software.

6.5 Digital Service Platforms

Russia has digital services built at least partly on Russian hardware and software. An example is the use of Russian ICT hardware and software in the so-called MFTs[75] municipal services, which are part of the Gosuslugi system [254] [255].

MFTs services use workstations with Elbrus 8C and Baikal-M (BE-M1000) processors, Russian ALT SP Linux operating systems, Postgres

[75] Russian: многофункциональный центр оказания государственных и муниципальных услуг (МФЦ).

database systems and office software. The server platform used in the system is the aforementioned Russian Jahont server platform [254] [255].

The above mentioned GosOblako cloud service platform has also used Russian ICT hardware and software, but it is uncertain to what extent the Russian processors will be used, as Russia will find it difficult to get microchips for processors. Instead, the move to Russian software is likely to increase in the future.

6.6 Examples of Russian Software

6.6.1 Office Software

Some office software similar to Microsoft Office has been developed in Russia. The best-known and most widely used office software is called My Office[76] [256]. My Office works on PCs, mobile devices and in the cloud on a web browser. My Office is used by Russian authorities such as FSO, which acquired 10,000 licences in 2021 [257].

Other Russian office software include R7 Office [258], Tsirkon Office [259] and Alter Office. Of these office software, R7 Office and possibly the Tsirkon Office are used by public authorities, but the Alter Office is less popular in Russia.

6.6.2 Database Software

The most common Russian database software is Postgres Pro [260]. Postgres Pro database software is used by some public authorities and state-owned companies. Other Russian database software are SUBD Linter and NitrosBase SQL [261].

Russia has a large number of Western software applications using Microsoft and Oracle SQL databases, which has made the migration to the open source Postgres SQL database not without problems. [262].

6.6.3 ERP Software

Due to the war in Ukraine, many Western Enterprise Resource Planning (ERP) suppliers have reduced their operations in Russia, which has accelerated the transition to Russian ERP systems [263]. The most potential

[76] Russian: МойОфис.

replacement for Western ERP software is the Russian 1Ci ERP software [264].

Russian 1Ci is an international company and its ERP software is also used outside Russia. In Russia, the 1Ci ERP system is used by some defence companies, including Sukhoi, an aircraft manufacturer, for example [265]. Other Russian ERP vendors include Galaktika, Parus and Compas but their market share is significantly smaller than that of 1Ci [263].

6.6.4 MES and SCADA Software

There are a few companies producing modern manufacturing execution system (MES) software in Russia, such as RTSoft [266], Galaktika [267] and Konsom Grupp [268]. Of these companies, RTSoft in particular has had extensive projects with Russian industrial companies [266].

There are at least five supervisory control and data acquisition (SCADA) system software suppliers in Russia. Examples of SCADA systems used in Russian industry include SCADA-KRUG, which runs on the Windows operating system and not on Linux [269]. According to the company's website, its SCADA system is used by major Russian energy companies [270]. It is therefore possible that some Russian energy companies will be forced to use both Windows and Linux operating systems in parallel, instead of replacing Windows operating systems entirely with Russian ones.

However, there are SCADA system manufacturers in Russia whose software runs on Linux. For example, the Russian MasterSCADA, IntraSCADA and RapidSCADA software run on Linux [271].

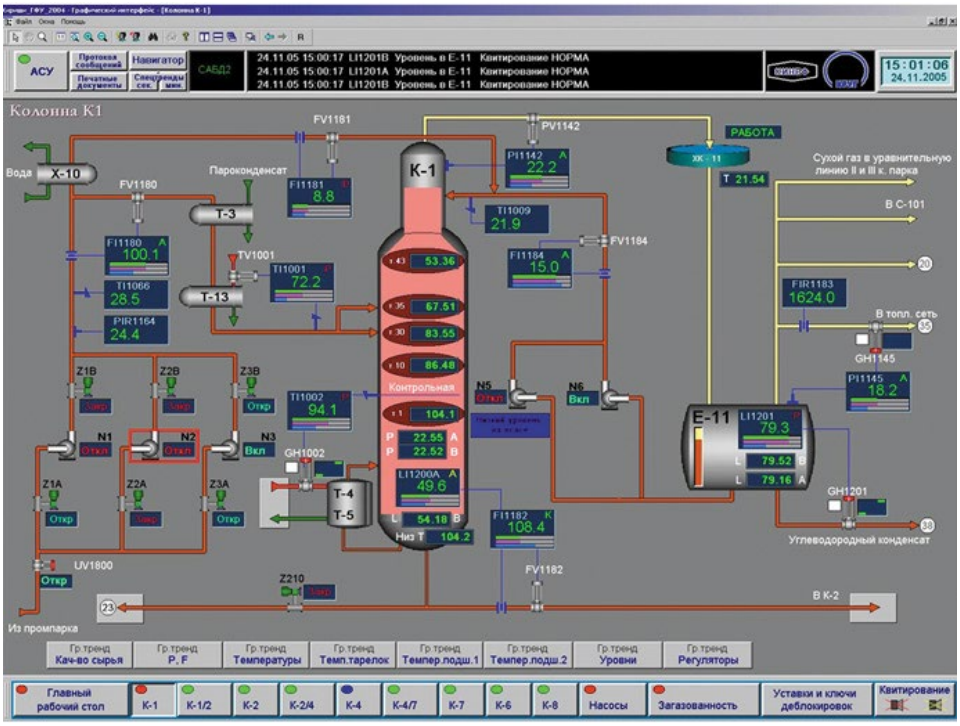

***Figure* 13.** SCADA-KRUG graphic interface [270].

6.6.5 SIEM Software

The are several SIEM system suppliers in Russia. The three most commonly used SIEM systems are MaxPatrol-SIEM, RuSIEM and Kaspersky SIEM. The extent to which Russian SIEM systems are used in Russia is largely influenced by the fact that organizations belonging to the critical ICT infrastructure should use SIEM systems approved by the Russian authority (FSTEC).

In 2022, half of Russian commercial organizations had only a few Russian security solutions in place [272]. Even state-owned companies in critical infrastructure did not all have Russian security solutions, but most plan to switch to Russian products in 2023.

7 ICT-infrastructure's Development Prospects Until 2030

This last chapter describes the prospects for the development of Russia's ICT infrastructure up to 2030. The focus is on ICT hardware, which will play the biggest role in the future operation of the Russian ICT infrastructure.

7.1 A Few Words about R&D in Russia

From the early 2000s until 2022, Russia had good opportunities to develop its own ICT production together with Western companies. However, Russia missed this opportunity and is increasingly struggling with structural problems in research and development (R&D). These structural problems in R&D include [273] [274] [275] [276] [277] [278] [279]:

- Lack of investments
- Misuse of investments and corruption
- Lack of ICT markets and inefficiencies
- Low number of patents
- Low prestige and low pay for research work
- Lack of ICT experts and specialist
- ICT workers leaving the country

In addition to these factors, Russia's ICT technology development is particularly affected by the reduced availability of high technology from the West. The lack of Western research cooperation and the departure of large western ICT companies from Russia will inevitably affect Russia's future R&D potential and thus the possibility of developing its own high-tech ICT products in the near future [279] [280].

7.2 Future Prospects for Microelectronics and Devices

According to Russian government's own estimate in 2022, Russia's microchip industry was 10 to 15 years behind the rest of the world [280]. For example, Russia is currently struggling to produce microchips below 180 nm. Russia does not have sufficient production capacity to produce the required 30,000 200 nm microchips per month[174]. Currently, Russia is estimated to have the capacity to produce 8,000 pieces of approximately 200 nm microchips.

This problem is compounded by the fact that the need for microchips is expected to grow in the future. Thus, it would be very important for Russia

to have equipment to manufacture general-purpose microchips. This can be very difficult in the context of the sanctions because of the war in Ukraine. For this reason, it is estimated that Russia will not be able to launch large-scale independent production of microchips in the next ten years [174] [169].

There are number of factors that will affect the development of Russian own microchips or their future supply from abroad. First of all, the equipment to make the microchips is hard to buy at the moment, which is why the equipment have to be sourced through Russia's allies or through other illegal channels. Secondly, setting up own microchip production cost at least more than ten billion dollars [169].

Russia is more likely to acquire microchip technology from abroad than to manufacture it itself. There are indications that China and Turkey are supplying Russia with the microchip technology it needs, and the level of microelectronics supplies to Russia is already at pre-war levels [281] [282]. Therefore, Russia is likely to continue to receive enough microchips in the years to come, at least for the most important uses, such as the armed forces.

In terms of computer architectures, Russia is possibly trying to move an open RISC-V architecture that is immune to western sanctions [280]. This is also in line with China's efforts to shift to the use of RISC-V architecture [283]. This may be of interest to the Russians as the Chinese company SMIC manufactures modern microchips.

7.3 Future Prospects for Networks

As mentioned earlier, Russia has started to produce network devices, but it is unlikely that Russia will be able to use domestic network devices to any significant extent in the coming years. It is possible that these Russian network devices are used in the networks where Chinese or US network devices are not wanted for security reasons.

In this context, Russia will have to think about how to replace the US Cisco and Uniper network devices which are widely used in Russian networks. Russia has justified the switch to Russian network devices on the grounds of information security, but from this point of view switching to Chinese network devices will not improve the situation at all, because Russia also suspects China of cyber espionage. However, it may be that in the future Russia will have no choice but to use more and more Chinese ICT

technology, as Western technology is not sufficiently available, despite parallel imports[77].

As regards telecommunications network cables, the situation in Russia is that most of the fiber-optic cables are supplied by foreign companies [284]. Currently, there is only one fiber-optic cable company in Russia [285]. In 2021, the Russian Deputy Prime Minister said that the production of optical fibers in Russia is crucial for the functioning of the Internet and that the materials used in optical fibers are important for the ICT sector [286]. It is unlikely that Russia would be able to become fully self-sufficient in fiber optic cables in the near future.

Similarly, in mobile networks in Russia, the lack of base stations could be a problem in the near future, as Russia does not have its own base station production. In 2022, it was estimated that the first Russian base stations could be available in 2–3 years [287]. Russian telecom operators have a total of around 800,000 base stations [288].

According to some estimates, Russia may need 100,000 base stations in the future to support high-speed mobile Internet [289]. Achieving this in the future with Russian base stations will not be possible and Russia will probably have to use Chinese base stations. 3G networks in Russia are planned to be maintained alongside 4G/LTE networks until 2027. It is possible that Russia will not be able to significantly expand its mobile networks in the future, for example by developing 5G networks.

7.4 Future Prospects for Software

In the future, the Russian authorities will try to increase the use of Russian software, which is thought to speed up the migration of commercial organizations to Russian software [290]. The first stage of this is planned to be a switch to Russian operating systems. In 2021, 66 percent of state-owned companies had not yet started migrating to Russian software. The most important reasons for switching to Russian software are independence from foreign suppliers and cyber security risks [290].

In 2021, it was estimated that the transition to Russian software would be slow and take at least more than five years [290]. The most likely scenario

[77] A parallel import is a non-counterfeit product imported from another country without the permission of the intellectual property owner. Parallel imports are often referred to as grey product.

is that Russia will not be able to fully switch to Russian software and still have Western software in use by 2030.

The main problems in switching to Russian software have been identified as the high cost of modifications and the lack of human resources to do the work. In addition, special software (e.g. production control systems), which has not yet been developed at all for the Linux operating system, poses problems for migration to Russian software in the future.

The easiest software to replace in Russia are antivirus and other information security software systems. In 2022, the FSTEC's register of approved information security systems contained around 2,000 different security solutions approved for use in Russia [291]. Around 400 new Russian information security solutions have been approved for the FSTEK register in the last two years [291].

As regards software for mobile devices, Russia plans to move to Aurora operating systems by 2030 [292]. By 2030, the aim is to develop a wireless ecosystem consisting of three versions of the Aurora operating system for different portable smart devices and users [293]. However, experts suspect that the equipment needed for this ecosystem would have to be sourced from China [294].

7.5 Future Prospects for the Russian Internet Segment

The war in Ukraine has led to changes in the Russian Internet segment. This has been reflected, for example, in the difficulty of accessing many Russian critical ICT infrastructure operator's websites from outside Russia. This is partly because Russia has introduced its own TLS certificates. Moreover, the use of DDoS attack prevention systems has increased significantly in Russia. In addition, the security of critical ICT infrastructure will be enhanced by using only email addresses belonging to the Russian Internet domain (.ru) [295].

Russia has further tightened control over their Internet segment, for example by developing systems for authorities in order to react more effectively to banned content on the Internet [296] [297]. This trend is likely to continue in the future. The centralized network monitoring systems described at the beginning of this publication, are under constant development [298].

8 Conclusions

If there is a Russian ICT device on display, one should not assume it to be entirely composed of Russian components, but rather one should ask what percentage of the components in the device are in fact Russian. This publication has shown that Russia is highly dependent on foreign ICT products.

Russia's situation in terms of ICT technology development will not improve in the coming years as Russia's R&D activities are plagued by a number of chronic problems. However, it is likely that in the future, despite the sanctions, Russia will obtain significant amounts of ICT technology from abroad.

Russia still has a functioning ICT infrastructure as a whole, but this may change as the ICT infrastructure, which is mainly Western equipment, will need to be upgraded in the coming years. The availability of optical fibers, network devices and mobile network base stations, among other things, will affect the performance of the Russian communications networks in the future.

Sufficient availability of advanced semiconductors will be particularly important for Russia in the future, because all areas of ICT infrastructure are dependent on semiconductors. Russia will not be able to produce advanced semiconductor products in the coming years; making it highly dependent on semiconductor imports from China.

As regards the Russian Internet segment and cyberspace, Russia is tightening its control over the Internet by developing more effective network monitoring and surveillance equipment. Russia's cyberspace may become more closed in the future but at the same time more independent from foreign countries and their Internet services.

9 References

[1] Федеральная служба по техническому и экспортному контролю, "Методический документ. Методика оценки угроз безопасности информации. ФСТЭК (5.2.2021).," 2021. [Online]. Available: https://fstec.ru/en/component/attachments/download/2919 (Accessed: 27.1.2023), pp. 65-69.

[2] КонсультантПлюс, "Федеральный закон "О связи" от 07.07.2003 N 126-ФЗ (последняя редакция)," 2023. [Online]. Available: http://www.consultant.ru/document/cons_doc_LAW_43224/ (Accessed: 26.1.2023).

[3] И. Королев, "Власти распространят «закон Яровой» на технологические сети. CNews (20.4.2021).," 2021. [Online]. Available: https://www.cnews.ru/news/top/2021-04-20_na_tehnologicheskie_seti?ysclid=leqpai5byt996337346 (Accessed: 02.3.2023).

[4] Федеральная служба по надзору в сфере связи, информационных технологий и массовых коммуникаций, "Реестр операторов, занимающих существенное положение в сети связи общего пользования. Роскомнадзор (22.10.2022).," 2022. [Online]. Available: https://rkn.gov.ru/communication/register/p197/ (Accessed: 31.1.2023).

[5] Wikipedia contributors, "Оператор связи. Wikipedia, the free encyclopedia (20.1.2023).," 2023. [Online]. Available: https://ru.wikipedia.org/?curid=172374&oldid=127988474 (Accessed: 31.1.2023).

[6] iFreedomLab, "Полная история регулирования интернета в России: от 80-х и до наших дней. iFreedomLab (27.2.2023).," 2023. [Online]. Available: https://ifreedomlab.net/campaignes/istoriya-regulirovaniya-svyazi/ (Accessed: 02.3.2023).

[7] Президент России, "Федеральный закон от 01.05.2019 г. № 90-ФЗ. О внесении изменений в Федеральный закон «О связи» и Федеральный закон «Об информации, информационных технологиях и о защите информации». Президент России (1.5.2019).," 2019. [Online]. Available: http://www.kremlin.ru/acts/bank/44230/page/2 (Accessed: 31.1.2023).

[8] И. Королев, "Власти запрещают в России современные интернет-протоколы, потому что они мешают блокировать сайты. CNews (21.9.2020).," 2022. [Online]. Available: https://www.cnews.ru/news/top/2020-09-21_vlasti_zapreshchayut_v_rossii (Accessed: 1.2.2023).

[9] Министерство цифрового развития, связи и массовых коммуникаций Российской Федерации, "TLS-сертификаты доступны для установки на смартфоны, компьютеры и планшеты. События (19.9.2022).," 2022. [Online]. Available: https://digital.gov.ru/ru/events/41990/ (Accessed: 1.2.2023).

[10] Федеральная служба по надзору в сфере связи, информационных технологий и массовых коммуникаций, "О принятии мер в отношении сервисов обхода ограничения доступа к противоправному контенту. Роскомнадзор (3.9.2021).," 2021. [Online]. Available: https://rkn.gov.ru/news/rsoc/news73836.htm (Accessed: 1.2.2023).

[11] ТАСС, ""Ростелеком" предлагает сотовым операторам РФ VPN-сервис для защищенного взаимодействия. ТАСС (8.11.2022).," 2022. [Online]. Available: https://tass.ru/ekonomika/16271179 (Accessed: 1.2.2023).

[12] I. Kuzin, "Как внедряют СОРМ в России и за рубежом. Itglobal (25.5.2020).," 2020. [Online]. Available: https://itglobal.com/ru-kz/company/blog/sorm-worldwide-experience/ (Accessed: 1.2.2023).

[13] CamSlider Privacy protection, "Что такое СОРМ и как уберечь личную жизнь от спецслужб. CamSlider Privacy protection (18.1.2021).," 2021. [Online]. Available: https://camslider.ru/chto-takoye-sorm-i-kak-zashchitit-lichnuyu-zhizn-ot-spetssluzhb/ (Accessed: 7.2.2023).

[14] VAS Experts, "СОРМ. Программно-аппаратные комплексы для осуществления оперативно-розыскных мероприятий (ОРМ).," 2023. [Online]. Available: https://vasexperts.ru/products/sorm/ (Accessed: 2.2.2023).

[15] Роскомсвобода, "СОРМ ОРИ: интернет-сервисы подключаются к пульту ФСБ. Роскомсвобода (27.6.2019).," 2019. [Online]. Available: https://roskomsvoboda.org/post/sorm-ori-internet-servisyi-podklyuchayut/ (Accessed: 1.2.2023).

[16] Яхонт, "Комлект СОРМ Виток OSINT.," 2023. [Online]. Available: https://yakhont-shd.ru/catalog-sorm/vitok-osint/ (Accessed: 18.4.2023).

[17] НОРСИ-ТРАНС, "Виток-OSINT. Информационно-поисковая система "Виток-OSINT".," 2023. [Online]. Available: https://norsi-trans.ru/catalog/osint/vitok-osint/ (Accessed: 18.4.2023).

[18] Telecom Times - Телеком Таймс, "Обзор СОРМ компаний в РФ и перспективы развития рынка. Telecom Times - Телеком Таймс (18.5.2021).," 2021. [Online]. Available: https://telecomtimes.ru/2021/05/corm-russia/ (Accessed: 02.3.2023).

[19] Министерство цифрового развития, связи и массовых коммуникаций Российской Федерации, "Приказ №83 16.4.2014.," 2014. [Online]. Available: https://digital.gov.ru/ru/documents/4249/ (Accessed: 2.2.2023).

[20] Министерство цифрового развития, связи и массовых коммуникаций Российской Федерации, "Приказ №573 29.10.2018.," 2018. [Online]. Available: https://minjust.consultant.ru/files/41292 (Accessed: 2.2.2023).

[21] М. Алехина, "Силовики за 5 лет стали почти втрое чаще запрашивать биллинги телефонов. Почему у правоохранителей упал интерес к прослушке, но вырос — к данным о соединениях. РБК (29.4.2021).," 2021. [Online]. Available: https://www.rbc.ru/politics/29/04/2021/60894a599a794763d0aef31a (Accessed: 3.2.2023).

[22] ПРОТЕЙ, "CORM.," 2018. [Online]. Available: https://protei.ru/sites/default/files/2019-12/COPM_2018_rus.pdf (Accessed: 3.2.2023), pp. 18.

[23] А. Гаврилюк, "Красное СОРМово. Роскомнадзор предупредил провайдеров о штрафах за отсутствие спецоборудования. Коммерсантъ (14.4.2021).," 2021. [Online]. Available: https://www.kommersant.ru/doc/4771775 (Accessed: 3.2.2023).

[24] Ю. Тишина, "Провайдеров накачали «суверенным интернетом». Коммерсантъ (18.9.2020).," 2020. [Online]. Available: https://www.kommersant.ru/doc/4494156 (Accessed: 3.2.2023).

[25] Федеральная служба по надзору в сфере связи, информационных технологий и массовых коммуникаций, "Заключения по системам фильтрации трафика. Роскомнадзор (8.9.2017).," 2017. [Online]. Available: https://rkn.gov.ru/communication/p922/ (Accessed: 3.2.2023).

[26] Роскомсвобода, "«Суверенность» войдёт в Рунет с Урала. Роскомсвобода (27.9.2019).," 2019. [Online]. Available: https://roskomsvoboda.org/50031/ (Accessed: 3.2.2023).

[27] RDP, "Компания.," 2023. [Online]. Available: https://www.rdp.ru/company/ (Accessed: 6.2.2023).

[28] Федеральная служба по надзору в сфере связи, информационных технологий и массовых коммуникаций, "ЕДИНЫЙ РЕЕСТР. Роскомнадзор (8.9.2017).," 2023. [Online]. Available: https://eais.rkn.gov.ru/registerdata/ (Accessed: 6.2.2023).

[29] Ю. Тишина, "«Владелец забора отвечает за то, что на нем написано». Коммерсантъ (25.5.2021).," 2021. [Online]. Available: https://www.kommersant.ru/doc/4826455 (Accessed: 6.2.2023).

[30] А. Курашева, "Государство потратит 1,2 млрд рублей на создание новейшей системы контроля трафика в интернете. Ведомости (6.11.2022).," 2022. [Online]. Available: https://www.vedomosti.ru/technology/articles/2022/11/07/949049-gosudarstvo-potratit-12-mlrd-rublei-na-sozdanie-sistemi-kontrolya-trafika (Accessed: 6.2.2023).

[31] VAS Experts, "Требования к реализации. Структура решения СОРМ-2 при установке СКАТ DPI в разрыв трафика.," 2023. [Online]. Available: https://vasexperts.ru/products/sorm/sorm-2/ (Accessed: 7.2.2023).

[32] IT и СОРМ, "IT и СОРМ. Twitter (14.9.2021).," 2021. [Online]. Available: https://t.me/itsorm/2197 (Accessed: 7.2.2023).

[33] Роскомсвобода, "Громкие блокировки через ТСПУ: разбираемся, что это такое. Роскомсвобода (16.9.2021)," 2021. [Online]. Available: https://roskomsvoboda.org/cards/card/tspu-blokrovki-runet/ (Accessed: 7.2.2023).

[34] О. .. Демидов, "Как блокировка Telegram стала угрозой для Рунета. РБК (24.4.2018).," 2018. [Online]. Available: https://www.rbc.ru/newspaper/2018/04/20/5ad8bcc59a7947e9e16be396 (Accessed: 7.2.2023).

[35] Ю. Мельникова, "Twitter: первая ласточка в фазаньей охоте Роскомнадзора. ComNews (11.3.2021).," 2021. [Online]. Available: https://www.comnews.ru/content/213477/2021-03-11/2021-w10/twitter-pervaya-lastochka-fazaney-okhote-roskomnadzora (Accessed: 7.2.2023).

[36] RDP, "Продукты.," 2023. [Online]. Available: https://www.rdp.ru/products/ (Accessed: 7.2.2023).

[37] Ю. Мельникова, "ТСПУ по правилам и без. ComNews (31.3.2021).," 2021. [Online]. Available: https://www.comnews.ru/content/213851/2021-03-31/2021-w13/tspu-pravilam-i-bez (Accessed: 7.2.2023).

[38] КонсультантПлюс, "Федеральный закон "О безопасности критической информационной инфраструктуры Российской Федерации" от 26.07.2017 N 187-ФЗ (последняя редакция).," 2017. [Online]. Available: http://www.consultant.ru/document/cons_doc_LAW_220885/ (Accessed: 7.2.2023).

[39] NCIRCC, "About CERT.GOV.RU.," 2023. [Online]. Available: https://cert.gov.ru/en/ (Accessed: 9.2.2023).

[40] Security Vision, "Защита критической информационной инфраструктуры (конспект лекции). Security Vision (15.3.2021).," 2021. [Online]. Available: https://www.securityvision.ru/blog/zashchita-kriticheskoy-informatsionnoy-infrastruktury-konspekt-lektsii/ (Accessed: 9.2.2023).

[41] Я. Шпунт, "ГосСОПКА наращивает подключения. Cnews (16.9.2022).," 2022. [Online]. Available: https://www.comnews.ru/content/222196/2022-09-16/2022-w37/gossopka-naraschivaet-podklyucheniya (Accessed: 9.2.2023).

[42] Cyber Media, "Нужны ли системе ГосСОПКА аналоги? Cyber Media (19.10.2022).," 2022. [Online]. Available: https://securitymedia.org/info/nuzhny-li-sisteme-gossopka-analogi.html (Accessed: 10.2.2023).

[43] Перспективный мониторинг, "Что такое ГосСОПКА.," 2023. [Online]. Available: https://amonitoring.ru/service/gossopka/ (Accessed: 9.2.2023).

[44] Tadviser, "Государственная система обнаружения,предупреждения и ликвидации последствийкомпьютерных атак ГосСОПКА. Tadviser

(1.9.2022).," 2022. [Online]. Available: https://www.tadviser.ru/a/175416 (Accessed: 9.2.2023).

[45] Positive Technologies, "Построение центра ГосСОПКА. Комплексное решение для создания центра ГосСОПКАи взаимодействия с НКЦКИ.," 2023. [Online]. Available: https://www.ptsecurity.com/ru-ru/solutions/center-gossopka/?utm_source=pt-nad&utm_medium=related-products&utm_campaign=gossopka (Accessed: 9.2.2023).

[46] ФСТЭК России, "Банк данных угроз безопасности информации.," 2023. [Online]. Available: https://bdu.fstec.ru/threat (Accessed: 10.2.2023).

[47] Ассоциация Документальной Электросвязи, "ЦМУ ССОП. Нормативно-правовое и информационное обеспечение.," 2019. [Online]. Available: http://ict19.rans.ru/images/present/Kalyakin.pdf (Accessed: 10.2.2023).

[48] Государственная дума, "Закон о «суверенном Рунете»: ответы на главные вопросы. Новости (8.4.2021).," 2021. [Online]. Available: http://duma.gov.ru/news/51194/ (Accessed: 10.2.2023).

[49] Федеральная служба по надзору в сфере связи, информационных технологий и массовых коммуникаций, "Twitter замедлен штатно. Новости Роскомнадзора (11.3.2021).," 2021. [Online]. Available: https://rkn.gov.ru/news/rsoc/news73480.htm (Accessed: 10.2.2023).

[50] Новые известия, "Государство закупает китайское оборудование для исполнения закона о надежном интернете. Новые известия (11.1.2022).," 2022. [Online]. Available: https://newizv.ru/news/2020-01-11/importozameschenie-v-internete-kitay-vmesto-ssha-301183 (Accessed: 13.2.2023).

[51] Федеральная служба по надзору в сфере связи, информационных технологий и массовых коммуникаций, "Инструкции по работе с подсистемами ЦМУ ССОП. Роскомнадзора (1.3.2021).," 2021. [Online]. Available: https://25.rkn.gov.ru/p32296/p32298/p33732/ (Accessed: 13.2.2023).

[52] Интерфакс, "Центр управления сетью связи в РФ займется глобальными хакерскими атаками. Интерфакс (20.10.2021).," 2021. [Online]. Available: https://www.interfax.ru/russia/885877 (Accessed: 13.2.2023).

[53] Meduza, "Какие VPN самые надежные? Как понять, что сервис сотрудничает со спецслужбами? Могут ли Россию вообще отключить от нормального интернета? Meduza (29.7.2022).," 2022. [Online]. Available: https://meduza.io/feature/2022/07/29/kakie-vpn-samye-nadezhnye-kak-ponyat-chto-servis-sotrudnichaet-so-spetssluzhbami-mogut-li-rossiyu-voobsche-otklyuchit-ot-normalnogo-interneta (Accessed: 7.2.2023).

[54] European Parliamentary Research Service, "'Splinternets': Addressing the renewed debate on internet fragmentation. European Parliamentary Research Service (July 2022).," 2022. [Online]. Available: https://www.europarl.europa.eu/RegData/etudes/STUD/2022/729530/EPRS_STU(2022)729530_EN.pdf (Accessed: 10.2.2023).

[55] Д. Беловодьев, "Центр слежки. Специальный отдел Роскомнадзора контролирует разговоры россиян о войне и Путине в интернете.Расследование "Системы". Настоящее Время (8.2.2022).," 2023. [Online]. Available: https://www.currenttime.tv/a/russia-leak-internet-censorship/32262160.html (Accessed: 10.2.2023).

[56] Н. Королев, "Не ходя вокруг да «Окулус». Коммерсант (17.8.2022).," 2022. [Online]. Available: https://www.kommersant.ru/doc/5514297 (Accessed: 23.2.2023).

[57] М. Тюняева (Бочкарёва), "Роскомнадзор готовится запустить систему обезвреживания инфобомб в интернете. Ведомости (20.2.2023).," 2023. [Online]. Available: https://www.vedomosti.ru/technology/articles/2023/02/20/963570-roskomnadzor-gotovitsya-zapustit-sistemu-obezvrezhivaniya-infobomb (Accessed: 23.2.2023).

[58] Роскомсвобода, "«Ростех» приобрел платформу для вычисления владельцев анонимных телеграм-каналов и будет предлагать эту услугу силовикам. Роскомсвобода Новости (22.3.2023).," 2023. [Online]. Available: https://roskomsvoboda.org/post/doc-rth-rf/ (Accessed: 27.3.2023).

[59] P. Sauer, "Privacy fears as Moscow metro rolls out facial recognition pay system. The Guardian (15.10.2021).," 2021. [Online]. Available: https://www.theguardian.com/world/2021/oct/15/privacy-fears-moscow-metro-rolls-out-facial-recognition-pay-system (Accessed: 23.2.2023).

[60] Роскомсвобода, "Власти хотят собирать биометрические данные россиян без их согласия. Роскомсвобода Новости (9.8.2022).," 2022. [Online]. Available: https://roskomsvoboda.org/post/prinuditelnaya-biometria/ (Accessed: 23.2.2023).

[61] К. Чачин, ""Ростелеком" модернизировал магистральные линии. itWeek (26.10.2004).," 2004. [Online]. Available: https://www.itweek.ru/infrastructure/article/detail.php?ID=68730 (Accessed: 17.2.2023).

[62] С. Л. Гавлиевский, В. Г. Карташевский, Д. В. Проскура, Д. С. Сахарчук and М. Ю. Сподобаев., "Принципы построения мультисервисной сети ПАО «Ростелеком». Москва: Горячая линия – Телеком.," 2018. [Online]. Available: https://www.techbook.ru/book.php?id_book=989&ysclid=le8gmk7r4a956081851 (Accessed: 17.2.2023).

[63] RusCable, "J’son & Partners представил исследование состояния и развития магистральных ВОЛС в России. RusCable (19.1.2022).," 2022. [Online]. Available: https://mobile.ruscable.ru/news/2022/1/19/_Json_Partners_predstavil_issledovanie_sostoyani/ (Accessed: 20.2.2023).

[64] Ростелеком, "«Ростелеком» завершил строительство подводной волоконно-оптической линии связи до Калининграда. Новости компании (17.2.2021).," 2021. [Online]. Available: https://www.company.rt.ru/press/news/d458230/ (Accessed: 21.2.2023).

[65] Ростелеком, "Завершено строительство первой очереди новой магистральной линии связи «Транзит Европа — Азия нового поколения». Новости компании (27.12.2022).," 2022. [Online]. Available: https://www.company.rt.ru/press/news/d465528/?backurl=/press/ (Accessed: 21.2.2023).

[66] А. Самсонова and Л. Коник, "ВОЛС в Арктике: третий пошел. ComNews (21.4.2021).," 2021. [Online]. Available: https://www.comnews.ru/content/214220/2021-04-21/2021-w16/vols-arktike-tretiy-poshel (Accessed: 21.2.2023).

[67] ComNews, "Магистральные сети связи в России, 2021. ComNews (20.12.2021)," 2021. [Online]. Available: https://www.comnews.ru/content/217974/2021-12-20/2021-w51/magistralnye-seti-svyazi-rossii-2021 (Accessed: 21.2.2023).

[68] PCH Packet Clearing House, "Internet Exchange Point Growth by Country. Internet Exchange Points - Feb 2023.," 2023. [Online]. Available: https://www.pch.net/ixp/summary_growth_by_country#!mt-sort=ixp_current,desc!mt-pivot=ixp_current (Accessed: 23.2.2023).

[69] Ростелеком, "Технические требования. Информация и документы.," 2023. [Online]. Available: https://zakupki.rostelecom.ru/info_docs/tz/ (Accessed: 23.2.2023).

[70] Tadviser, "Реестр телекоммуникационного оборудования российского происхождения (ТОРП).," 2021. [Online]. Available: https://www.tadviser.ru/a/455722 (Accessed: 24.2.2023).

[71] Tadviser, "Единый реестр российской радиоэлектронной продукции.," 2022. [Online]. Available: https://www.tadviser.ru/a/466690 (Accessed: 24.2.2023).

[72] Ростелеком, "Требования к оборудованию магистральной транспортной сети. Информация и документы.," 2023. [Online]. Available: https://zakupki.rostelecom.ru/info_docs/tz/magistr/ (Accessed: 23.2.2023).

[73] T8, "Компания T8.," 2023. [Online]. Available: https://t8.ru/?page_id=3144 (Accessed: 23.2.2023).

[74] А. Барсков, "Российский рынок DWDM: лямбда за лямбдой. ИКС Медиа (5.2.2020).," 2020. [Online]. Available: https://www.iksmedia.ru/articles/5643321-Rossijskij-rynok-DWDM-lyambda-za.html (Accessed: 24.2.2023).

[75] T8, "BACKBONE DWDM NETWORKS.," 2023. [Online]. Available: https://t8.ru/?page_id=10525&lang=en (Accessed: 24.2.2023).

[76] Rostelecom, "Backbone Network.," 2023. [Online]. Available: https://www.company.rt.ru/en/about/net/magistr/ (Accessed: 24.2.2023).

[77] Rostelecom, "Rostelecom’s MPLS network.," 2023. [Online]. Available: https://www.company.rt.ru/en/about/net/mpls/ (Accessed: 24.2.2023).

[78] MForum, "Сети 4G/LTE в России действуют в 83 регионах (обновляемый список всех сетей LTE в России). MForum (31.12.2022).," 2020. [Online]. Available:

http://www.mforum.ru/news/article/100885.htm (Accessed: 27.2.2023).

[79] Э. Касми, "Больше никаких «иностранцев». В России грядет тотальный запрет на зарубежные базовые станции для 4G. CNews (6.8.2021).," 2021. [Online]. Available: https://www.cnews.ru/news/top/2021-08-06_bolshe_nikakih_inostrantsev (Accessed: 27.2.2023).

[80] Н. Горнов, "Сотовая связь: фабрика виртуальных операторов забуксовала (полный текст). Коммерческие вести (29.2.2020).," 2020. [Online]. Available: https://kvnews.ru/news-feed/sotovaya-svyaz-fabrika-virtualnyh-operatorov-zabuksovala-polnyy-tekst (Accessed: 27.2.2023).

[81] CNews Analytics, "Обзор: Телеком 2020. CNews (29.10.2020).," 2020. [Online]. Available: https://www.cnews.ru/reviews/telekom_2020 (Accessed: 08.3.2023).

[82] ComNews Vision, "Охват территории РФ спутниками связи и вещания. ComNews Vision (10.3.2021).," 2021. [Online]. Available: https://www.comnews.ru/content/211284/2021-03-10/2021-w10/okhvat-territorii-rf-sputnikami-svyazi-i-veschaniya (Accessed: 06.3.2023).

[83] Russian Satellite Communications Company, "Company," 2023. [Online]. Available: https://eng.rscc.ru/about/ (Accessed: 08.3.2023).

[84] Thales, "Russian Express-80 and Express-103 communications satellites embarking Thales Alenia Space payloads, successful launched. Thales (31.7.2020).," 2020. [Online]. Available: https://www.thalesgroup.com/en/worldwide/space/press_release/russian-express-80-and-express-103-communications-satellites (Accessed: 08.3.2023).

[85] Gazprom Space Systems, "About Company.," 2021. [Online]. Available: https://www.gazprom-spacesystems.ru/en/about/ (Accessed: 08.3.2023).

[86] Thales, "Thales Alenia Space to build Yamal-601 satellite for Gazprom Space Systems. Thales (31.7.2014).," 2014. [Online]. Available: https://www.thalesgroup.com/en/worldwide/space/press_release/thales-alenia-space-build-yamal-601-satellite-gazprom-space-systems (Accessed: 08.3.2023).

[87] Satellite system GONETS, "Mobile Satellite Communications.," 2023. [Online]. Available: https://gonets.ru/eng/ (Accessed: 08.3.2023).

[88] M. Krutov and S. Dobrynin, "In Russia's War On Ukraine, Effective Satellites Are Few And Far Between. Radio Free Europe/Radio Liberty (11.4.2022).," 2022. [Online]. Available: https://www.rferl.org/a/russia-satellites-ukraine-war-gps/31797618.html (Accessed: 08.3.2023).

[89] Union of Concerned Scientists, "UCS Satellite Database. Reports & Multimedia / Feature (Updated May 1, 2022).," 2022. [Online]. Available: https://www.ucsusa.org/resources/satellite-database (Accessed: 08.3.2023).

[90] Ростелеком, "Карта покрытия сети Ростелеком в квартиры.," 2023. [Online]. Available: https://rt-internet.ru/map (Accessed: 27.2.2023).

[91] G. Abdrakhmanova, K. Vishnevskiy, L. Gokhberg, O. Demidkina, A. Demyanova, Y. Dranev, G. Kovaleva, M. Kotsemir, I. Kuznetsova, I. Kuchin, I. Lola, O. Ozerova, G. Ostapkovich, T. Ratay, Z. Ryzhikova, E. Streltsova, J. Turovets, K. Utyatina, S. Fridlyanova, K. Fursov and N. Schugal, "Digital Economy Indicators in the Russian Federation: 2020 : Data Book.," 2020. [Online]. Available: https://issek.hse.ru/mirror/pubs/share/387609461.pdf (Accessed: 27.2.2023), pp. 136-141.

[92] nPerf, "Tele2/Rostelecom 3G / 4G / 5G bitrates map, Russian Federation. Last update : 02/27/2023.," 2023. [Online]. Available: https://www.nperf.com/en/map/RU/-/169054.Tele2Rostelecom/download/ (Accessed: 27.2.2023).

[93] Федеральная служба по надзору в сфере связи, информационных технологий и массовых коммуникаций, "Мониторинг и управление. Сбор сведений.," 2023. [Online]. Available: https://service.rkn.gov.ru/monitoring/datacollection (Accessed: 28.2.2023).

[94] ДВДМ.РУ, "Internet eXchange (Точки обмена трафиком). Список точек обмена трафиком России (Russian's Internet eXchange).," 2023. [Online]. Available: https://www.dwdm.ru/wiki/19?ysclid=lentjvdudd751402571 (Accessed: 28.2.2023).

[95] RIPE NCC, "Country Comparison.," 2023. [Online]. Available: https://stat.ripe.net/specials/country-comparison (Accessed: 28.2.2023).

[96] Db-ip.com, "AS12389 PJSC Rostelecom. AS 12389 ROSTELECOM-AS.," 2023. [Online]. Available: https://db-ip.com/as12389 (Accessed: 28.2.2023).

[97] Ассоциация Документальной Электросвязи, "Отчет о Фактическом состоянии маршрутизации внутрироссийского трафика через зарубежные сети.," 2017. [Online]. Available: https://www.rans.ru/images/news/Traffic_30112017.pdf (Accessed: 28.2.2023).

[98] IDIDB, "AS connectivity graph by country according to whois RIR database. Updated: 2023-02-28.," 2023. [Online]. Available: https://www.ididb.ru/en/connectivity/#countries (Accessed: 28.2.2023).

[99] ComNews, "Магистральные сети связи в России. ComNews (21.10.2020).," 2020. [Online]. Available: https://www.comnews.ru/content/211042/2020-10-21/2020-w43/magistralnye-seti-svyazi-rossii (Accessed: 28.2.2023).

[100] N. Campbell and C. Gahnberg, "Internet Impact Brief: Impact of Ukraine's Requests to Block Russia's Access to the Internet. Internet Society (18.3.2022).," 2022. [Online]. Available: https://www.internetsociety.org/resources/2022/impact-of-ukraines-requests-to-block-russias-access-to-the-internet/ (Accessed: 28.2.2023).

[101] Рамблер, "Что такое НСДИ. Объясняем простыми словами. Рамблер (19.11.2021).," 2021. [Online]. Available: https://news.rambler.ru/internet/47610920-chto-takoe-nsdi-obyasnyaem-prostymi-slovami/?ysclid=leo4e47mtp912599866 (Accessed: 01.3.2023).

[102] Федеральная служба охраны Российской Федерации, "Приказ от 07 сентября 2016 г. № 443.," 2016. [Online]. Available: http://www.gov.ru/rsnet/pr_fso_443_07092016.pdf (Accessed: 01.3.2023).

[103] Министерство цифрового развития, связи и массовых коммуникаций Российской Федерации, "Единая сеть передачи данных для госорганов.," 2018. [Online]. Available: https://digital.gov.ru/ru/activity/directions/67/ (Accessed: 01.3.2023).

[104] Tadviser, "Единая сеть передачи данных (ЕСПД) для госорганов. Russian State Network, RSNet. Tadviser (23.7.2019).," 2019. [Online]. Available: https://www.tadviser.ru/a/53423 (Accessed: 01.3.2023).

[105] J. Kukkola, "Digital Soviet Union. The Russian national segment of the Internet as a closed national network shaped by strategic cultural ideas. National Defence University. Series 1: Research Publications No. 40. Helsinki: National Defence University.," 2020. [Online]. Available: https://www.doria.fi/handle/10024/177157 (Accessed: 02.3.2023), pp. 345.

[106] Ростелеком, "«Ростелеком» подключил к безопасному интернету более 47 тысяч школ и техникумов. Новости компании (28.2.2023).," 2023. [Online]. Available: https://www.company.rt.ru/press/news/d466289/ (Accessed: 06.3.2023).

[107] Министерство цифрового развития, связи и массовых коммуникаций Российской Федерации, "Уточненный годовой отчет о ходе реализации и оценке эффективностигосударственной программы Российской Федерации «Информационное общество». Дата составления отчета 20.04.2021.," 2021. [Online]. Available: https://digital.gov.ru/uploaded/files/utochnennyj-godovoj-otchet-2020.pdf (Accessed: 01.3.2023).

[108] Министерство цифрового развития, связи и массовых коммуникаций Российской Федерации, "Государственные услуги и информационные системы.," 2023. [Online]. Available: https://digital.gov.ru/ru/activity/govservices/#section-infosys (Accessed: 02.3.2023).

[109] Министерство цифрового развития, связи и массовых коммуникаций Российской Федерации, "Национальная система управления данными.," 2021. [Online]. Available: https://digital.gov.ru/ru/activity/directions/1061/?utm_referrer=https://www.google.fi/.

[110] Министерство цифрового развития, связи и массовых коммуникаций Российской Федерации, "Единая система межведомственного электронного взаимодействия (СМЭВ).," 2023. [Online]. Available: https://digital.gov.ru/ru/activity/govservices/infosystems/22/ (Accessed: 02.3.2023).

[111] НСУД, "Единая информационная платформа. Национальной системы управления данными.," 2023. [Online]. Available: https://nsud.gosuslugi.ru/ (Accessed: 02.3.2023).

[112] Правительства Российской Федерации, "Концепция создания и функционирования национальной системы управления

данными. Распоряжение от 3 июня 2019 г. № 1189-р.," 2019. [Online]. Available: http://static.government.ru/media/files/jYh27VIwiZs44qa0IXJlZCa3uu7qqLzl.pdf (Accessed: 03.3.2023).

[113] О. Нечеухин, "Государственные информационные системы (ГИСы): практические вопросы защиты информации. Контур Журнал (2.3.2015).," 2015. [Online]. Available: https://kontur.ru/articles/1609 (Accessed: 02.3.2023).

[114] Н. Краснушкина, "Госданным прописали архитектуру. Коммерсантъ (30.11.2018).," 2018. [Online]. Available: https://www.kommersant.ru/doc/3814604 (Accessed: 02.3.2023).

[115] Госуслуги, "ГИС ЖКХ – вся информация о коммунальных услугах на одном портале.," 2017. [Online]. Available: https://www.gosuslugi.ru/help/news/2017_10_09_gis_gkh (Accessed: 02.3.2023).

[116] Госуслуги, "Портал государственных услуг Российской Федерации.," 2023. [Online]. Available: https://esia.gosuslugi.ru/login/ (Accessed: 02.3.2023).

[117] Казначейство России, "Регламент подключения и интеграции с ГАС «Управление».," 2015. [Online]. Available: https://roskazna.gov.ru/upload/iblock/885/reglament-podklyucheniya-i-integratsii-gas-_upravlenie_.pdf?ysclid=les5onbz93976912635 (Accessed: 03.3.2023).

[118] Федеральная служба по надзору в сфере связи, информационных технологий и массовых коммуникаций, "РУКОВОДСТВО ПОЛЬЗОВАТЕЛЯ. «Личный кабинет Портала заявителей». Общие принципы работы.," 2020. [Online]. Available: https://25.rkn.gov.ru/docs/25/sm33732/instrukcija__portal_zajavitelej.pdf (Accessed: 02.3.2023), pp. 43.

[119] D-Russia.ru, "Официально опубликована концепция развития платформы «ГосТех». D-Russia.ru (25.10.2022).," 2022. [Online]. Available: https://d-russia.ru/oficialno-opublikovana-koncepcija-razvitija-platformy-gosteh.html (Accessed: 02.3.2023).

[120] Министерство цифрового развития, связи и массовых коммуникаций Российской Федерации, "Расширен состав участников эксперимента по переходу на ГЕОП. Мониторинг СМИ (25.10.2021).," 2021. [Online]. Available: https://digital.gov.ru/ru/events/41336/ (Accessed: 02.3.2023).

[121] Министерство цифрового развития, связи и массовых коммуникаций Российской Федерации, "Цифровизацию госорганов будут контролировать из ГосОблака.," 2021. [Online]. Available: https://digital.gov.ru/ru/events/41168/ (Accessed: 02.3.2023).

[122] Министерство цифрового развития, связи и массовых коммуникаций Российской Федерации, "Государственная единая облачная платформа.," 2019. [Online]. Available: https://d-russia.ru/wp-content/uploads/2019/09/enfiadzhan.pdf?ysclid=les4suumay477786300 (Accessed: 02.3.2023).

[123] К. Холупова, "Минцифры срочно ищет серверы и СХД для «Гособлака». Cnews (29.11.2022).," 2022. [Online]. Available: https://www.cnews.ru/news/top/2022-11-28_mintsifry_ishchet_servery_i_shd (Accessed: 06.3.2023).

[124] Tadviser, "Мультисервисная транспортная сеть связи (МТСС). Закрытый сегмент передачи данных (ЗСПД). Tadviser (2016).," 2016. [Online]. Available: https://www.tadviser.ru/a/338039 (Accessed: 06.3.2023).

[125] К. Рябов, "Мультисервисная транспортная сеть связи для министерства обороны. Военное обозрение (13.3.2019).," 2019. [Online]. Available: https://topwar.ru/155340-multiservisnaja-transportnaja-set-svjazi-dlja-ministerstva-oborony.html (Accessed: 06.3.2023).

[126] J. Kukkola, "Rakenteellisen kyberasymmetrian strategiset vaikutukset: Venäjän kansallinen internetsegmentti sotilasstrategisena ilmiönä. Puolustusvoimien tutkimuslaitos. Julkaisuja 13.," 2021. [Online]. Available: https://puolustusvoimat.fi/documents/1951253/2815786/PVTUTKL julkaisuja 13.pdf/7e420587-b27c-6899-954a-045b613779aa/PVTUTKL julkaisuja 13.pdf?t=1633685935839 (Accessed: 06.3.2023), pp. 150-151.

[127] И. Елков, "Как работает ситуационный центр президента. Редакция Российской газеты (11.10.2017).," 2017. [Online]. Available: https://rg.ru/2017/10/11/kak-rabotaet-situacionnyj-centr-prezidenta.html (Accessed: 06.3.2023).

[128] И. Королев, "Как государство потратит 101 миллиард на цифровое госуправление. Cnews (11.2.2020).," 2020. [Online]. Available: https://www.cnews.ru/news/top/2020-02-11_kak_gosudarstvo_potratit (Accessed: 06.3.2023).

[129] Ростелеком, "Национальный киберполигон. Безопасное будущее цифровой России.," 2021. [Online]. Available: https://cybermir.ru/ (Accessed: 06.3.2023).

[130] Ростелеком, "Дмитрий Чернышенко: «На пяти киберполигонах пройдут учения в 2021 году». Новости компании (14.5.2021).," 2021. [Online]. Available: https://www.company.rt.ru/press/news/d459207/ (Accessed: 06.3.2023).

[131] РБК, "Киберучения в национальном масштабе: как работают киберполигоны в России. РБК (1.11.2022).," 2022. [Online]. Available: https://www.rbc.ru/technology_and_media/01/11/2022/635bfe3f9a794799a7e0b42e (Accessed: 06.3.2023).

[132] M. Newton, "Russian Data Localization Laws: Enriching “Security” & the Economy. Henry M. Jackson School of International Studies, University of Washington (28.2.2018).," 2018. [Online]. Available: https://jsis.washington.edu/news/russian-data-localization-enriching-security-economy/ (Accessed: 13.3.2023).

[133] Д. Воейков, "МВД проектирует мегаЦОД. Возможно на российских процессорах. CNews (29.4.2020).," 2020. [Online]. Available: https://www.cnews.ru/news/top/2020-04-29_mvd_proektiruet_megatsod (Accessed: 15.3.2022).

[134] И. Юзбекова, "Google начала переносить серверы в российские дата-центры. РБК (10.4.2015).," 2015. [Online]. Available: https://www.rbc.ru/technology_and_media/10/04/2015/5522a9f69a794752a5f478fa (Accessed: 14.3.2023).

[135] TASS, "Yandex, FSB find acceptable encryption key solution — media watchdog. TASS (6.6.2019).," 2019. [Online]. Available: https://tass.com/economy/1062262 (Accessed: 14.3.2023).

[136] В. Бахур, "Российские ЦОДы будут отчитываться по «суверенному Рунету» перед Роскомнадзором. CNews (31.8.2020).," 2020. [Online]. Available: https://www.cnews.ru/news/top/2020-08-31_operatory_rossijskih_tsodov (Accessed: 14.3.2023).

[137] А. Барсков, "Определение ЦОДа в законе «О связи». ИКС Медиа (21.6.2021).," 2021. [Online]. Available: https://www.iksmedia.ru/news/5838950-Opredelenie-CZODa-v-zakone-O-svyazi.html (Accessed: 13.3.2023).

[138] А. Курашева and Е. Кинякина, "ЦОДы останутся без лицензий на связь. Ведомости (13.3.2023).," 2023. [Online]. Available: https://www.vedomosti.ru/technology/articles/2022/06/16/926751-tsodi-ostanutsya-bez-litsenzii (Accessed: 13.3.2023).

[139] Rostelecom, "Крупнейшая геораспределенная сеть дата-центров Tier III в России.," 2023. [Online]. Available: https://dcnetwork.ru/ (Accessed: 15.3.2022).

[140] DataLine, "О нас.," 2023. [Online]. Available: https://www.dtln.ru/kompaniya/about (Accessed: 14.3.2023).

[141] Правительство Российской Федерации, "Распоряжение от 7 октября 2015 г. № 1995-р Москва.," 2015. [Online]. Available: https://d-russia.ru/wp-content/uploads/2015/10/2015_DataCenter_Concept.pdf (Accessed: 14.3.2023).

[142] А. Барсков, "97% компаний в России не используют инфраструктурные облака. ИКС Медиа (23.12.2022).," 2022. [Online]. Available: https://www.iksmedia.ru/articles/5927557-97-kompanij-v-Rossii-ne-ispolzuyut.html (Accessed: 14.3.2023).

[143] Н. Рудычева, "Количество российских компаний, использующих облачную инфраструктуру, утроилось. Cnews (28.12.2022).," 2022. [Online]. Available: https://www.cnews.ru/articles/2022-12-27_opublikovany_rezultaty_issledovaniya?ysclid=lf82ca2w3086767 4416 (Accessed: 14.3.2023).

[144] П. Лебедев, "Обзор: Центры обработки данных 2022. Обещанное удвоение российского рынка ЦОД откладывается на неопределенный срок CNews (15.7.2022).," 2022. [Online]. Available: https://www.cnews.ru/reviews/rynok_tsod_2022/articles/obeshchannoe_udvoenie_rossijskogo_rynka (Accessed: 14.3.2023).

[145] П. Лебедев, "Обзор: Центры обработки данных 2022. Нехватка оборудования затормозит, но не остановит запуск новых ЦОД. CNews (15.7.2022).," 2022. [Online]. Available: https://www.cnews.ru/reviews/rynok_tsod_2022/articles/nehvatka_oborudovaniya_zatormozit (Accessed: 14.3.2023).

[146] Rostelecom, "Data Centers.," 2021. [Online]. Available: https://rt-dc.ru/en/about/data-centers/ (Accessed: 29.9.2021).

[147] CNews, "Госструктурам запретят строить новые ЦОД, чтобы поддержать облачных провайдеров. CNews (26.5.2021).,"

2021. [Online]. Available: https://www.cnews.ru/articles/2021-05-24_gosstrukturam_zapretyat_stroit_novye?ysclid=lf9h2q68x2510006653 (Accessed: 15.3.2022).

[148] З. Мамедьяров and Н. Ульянов, "«Без этого мы не страна». Тема недели микропроцессор «Эльбрус». Эксперт 21–27 сентября 2020 № 39 (1177).," 2020. [Online]. Available: http://www.mcst.ru/files/5f96f6/bcdece/61a407/582dc6/zaur_mamedyarov_nikolay_ulyanov_-_expert_39_1177.pdf (Accessed: 15.3.2022) pp. 19.

[149] Yandex Cloud, "Yandex Cloud.," 2023. [Online]. Available: https://cloud.yandex.ru/ (Accessed: 15.3.2022).

[150] Yandex Cloud, "Yandex Cloud CDN.," 2023. [Online]. Available: https://cloud.yandex.ru/services/cdn (Accessed: 15.3.2022).

[151] A. .. Popova, "Russian Search Giant Yandex Struggles to Survive. Center for European Policy Analysis (10.3.2022).," 2022. [Online]. Available: https://cepa.org/article/russian-search-giant-yandex-struggles-to-survive/ (Accessed: 16.3.2022).

[152] J. Byrne, G. Somerville, J. Byrne, J. Watling and N. &. B. J. Reynolds, "Silicon lifeline western electronics at the heart of russia's war machine. Royal United Services Institute for Defence and Security Studies (August 2022).," 2022. [Online]. Available: https://static.rusi.org/RUSI-Silicon-Lifeline-final-updated-web_1.pdf (Accessed: 23.3.2023) pp. 13..

[153] Asianometry, "Why Russia Can't Replace TSMC. Youtube video (4.3.2022).," 2022. [Online]. Available: https://www.youtube.com/watch?v=N_4R4X7AWtU (Accessed: 27.3.2023).

[154] Y. Lee, N. Shirouzu and D. Lague, "Silicon Fortress. T-Day the battle for Taiwan. Taiwan chip industry emerges as battlefront in U.S.-China showdown. Reuters (27.12.2021).," 2021. [Online]. Available: https://www.reuters.com/investigates/special-report/taiwan-china-chips/ (Accessed: 17.3.2022).

[155] И. Чеберко, "США запретил поставку чибов для российских спутников. Известия (11.3.2014).," 2014. [Online]. Available: https://iz.ru/news/567232 (Accessed: 17.3.2022).

[156] В. Громова, "Клишас заявил о провале программы импортозамещения в России. РБК (19.5.2022).," 2022. [Online]. Available:

https://www.rbc.ru/politics/19/05/2022/6285f0c79a7947c127bab983?ysclid=lfci0l8h7f765505084 (Accessed: 17.3.2022).

[157] Т. Захаров, "Про импортозамещение. Habr (8.1.2022).," 2022. [Online]. Available: https://habr.com/en/post/599671/ (Accessed: 17.3.2022).

[158] В. Конявский and С. Конявская, Доверенные информационные технологий. От архитектуры к системам и средствам. URSS: Москва. pp. 87., 2019.

[159] Правительства Российской Федерации, "Распоряжение от 17 января 2020 г. № 20-р. Стратегия развития электронной промышленности Российской Федерации на период до 2030 года.," 2020. [Online]. Available: http://government.ru/docs/38795/ (Accessed: 20.3.2022).

[160] Ю. Ковалевский, "Рынок микроэлектроники в России есть. Нужно только научиться с ним правильно работать. Электроника НТБ (Выпуск #4/2022).," 2022. [Online]. Available: https://www.electronics.ru/journal/article/9345 (Accessed: 21.3.2023).

[161] РОСЭЛ, "Обеспечиваем технологическую независимость России.," 2020. [Online]. Available: https://ruselectronics.ru/ (Accessed: 20.3.2022).

[162] Минпромторг России, "Каталог продукции.," 2023. [Online]. Available: https://gisp.gov.ru/goods/#/ (Accessed: 20.3.2023).

[163] КонтурСнаб, "ОКПД-2. 26 Оборудование компьютерное, электронное и оптическое.," 2023. [Online]. Available: https://snab.kontur.ru/classifiers/okpd2/26 (Accessed: 20.3.2022).

[164] Д. Воейков, "Власти вводят новые критерии «отечественности» для электроники. Использование российских чипов больше не обязательно. CNews (27.2021).," 2021. [Online]. Available: https://www.cnews.ru/news/top/2021-07-02_vlasti_vvodyat_novye_kriterii (Accessed: 20.3.2022).

[165] Минпромторг России, "Программно-аппаратный комплекс «Соболь» версия 3.0, форм-фактор платы Mini PCI Express Half (14.4.2022).," 2022. [Online]. Available: https://gisp.gov.ru/goods/#/product/2504491 (Accessed: 20.3.2023).

[166] OFAC, "OFAC. Office of Foreign Assets Control. Sanctions List Search.," 2023. [Online]. Available: https://sanctionssearch.ofac.treas.gov/ (Accessed: 22.3.2023).

[167] Н. Королев and Т. Корнев, "Семь пядей в чип. «Микрону» выделят 7 млрд руб. на масштабирование. Коммерсантъ (5.9.2022).," 2022. [Online]. Available: https://www.kommersant.ru/doc/5546809 (Accessed: 22.3.2023).

[168] Н. Королев, "«Микрон» надеется подрасти. Завод планирует удвоить производство к 2025 году. Коммерсантъ (22.4.2022).," 2022. [Online]. Available: https://www.kommersant.ru/doc/5318409 (Accessed: 22.3.2023).

[169] А. Балашова, "Эксперты оценили почти в ₽800 млрд затраты на развитие микроэлектроники. РБК (15.11.2022).," 2022. [Online]. Available: https://www.rbc.ru/technology_and_media/15/11/2022/63726ae29a79478eebf51ee2 (Accessed: 22.3.2023).

[170] Amur Mikron, "Первый российский RISC-V микроконтроллер MIK32 АМУР.," 2023. [Online]. Available: https://www.mcu.mikron.ru/ (Accessed: 28.3.2023).

[171] А. Воронцов, "В России выпущен первый собственный чип, но спасёт ли он автопром? У экспертов к микросхеме возникли большие вопросы. Quto (9.12.2021).," 2021. [Online]. Available: https://quto.ru/journal/news/v-rossii-vypushen-pervyi-sobstvennyi-chip-no-spasyot-li-on-avtoprom-09-12-2021.htm (Accessed: 28.3.2023).

[172] АО НИИМА Прогресс, "О предприятии.," 2023. [Online]. Available: https://i-progress.tech/about/ (Accessed: 23.3.2023).

[173] Tadviser, "РТИ.," 2017. [Online]. Available: https://www.tadviser.ru/a/86932 (Accessed: 22.3.2023).

[174] Н. Королев, "Полупроводы полупроводников. Как российская микроэлектроника развивается на фоне зарубежной. Коммерсантъ (13.12.2022).," 2022. [Online]. Available: https://www.kommersant.ru/doc/5706740 (Accessed: 22.3.2023).

[175] Tadviser, "НМ-Тех.," 2021. [Online]. Available: https://www.tadviser.ru/a/538697 (Accessed: 22.3.2023).

[176] NM-Tech, "About Company.," 2023. [Online]. Available: https://nm-tech.org/eng#about (Accessed: 22.3.2023).

[177] АО НТЦ Модуль, "О КОМПАНИИ.," 2023. [Online]. Available: https://www.module.ru/company/about (Accessed: 23.3.2023).

[178] АО НТЦ Модуль, "СБИС 1879ВМ5Я (NM6406).," 2023. [Online]. Available: https://www.module.ru/products/1/3-18795-nm6406 (Accessed: 23.3.2023).

[179] АО НТЦ Модуль, "Микросхема интегральная К1879ВМ5Я Руководство по эксплуатации ЮФКВ.431282.006РЭ.," 2012. [Online]. Available: https://www.module.ru/uploads/products/18795-8a285d33c8.pdf (Accessed: 23.3.2023).

[180] НИИСИ РАН, "Разработка СБИС.," 2023. [Online]. Available: https://www.niisi.ru/devel.htm (Accessed: 24.3.2023).

[181] АО КБ Корунд-М, "Перспективные ЭВМ семейства БАГЕТ.," 2017. [Online]. Available: http://nesmelov.com/images/portfolio/polygraphy/korund-m.pdf (Accessed: 24.3.2023).

[182] Н. Никифоров, "Разбираемся, на что способна линейка российских процессоров «КОМДИВ» и чем она лучше CPU AMD и Intel. Overclockers.ru (8.2.2022).," 2022. [Online]. Available: https://overclockers.ru/blog/remont_accumulyatora_noutbuka/show/62943/razbiraemsya-na-chto-sposobna-linejka-rossijskih-processorov-komdiv-i-chem-ona-luchshe-cpu-amd-i-intel (Accessed: 24.3.2023).

[183] С. .. Аряшев, "Технологии QNX и КПДА в России. «Отечественные системы на кристалле с архитектурой Комдив64. Текущее состояние. Перспективы развития»НИИСИ РАН (13.4.2017).," 2017. [Online]. Available: https://www.niisi.ru/aryashev_komdiv642017.pdf (Accessed: 24.3.2023).

[184] АО КБ Корунд-М, "ПЭВМ Уран-2.2.," 2023. [Online]. Available: https://kbkorund.ru/catalog/uran-2-2 (Accessed: 24.3.2023).

[185] АО НПЦ ЭЛВИС, "ПРОЦЕССОРЫ «МУЛЬТИКОР».," 2023. [Online]. Available: https://elvees.ru/chip (Accessed: 27.3.2023).

[186] И. Кузьмин, "Чипы под санкциями. Способна ли Россия обеспечить себя микроэлектроникой. Секрет фирмы (12.4.2022).," 2022. [Online]. Available: https://secretmag.ru/technologies/chipy-pod-sankciyami-sposobna-li-rossiya-obespechit-sebya-mikroelektronikoi.htm (Accessed: 27.3.2023).

[187] Гравитон, "Сервер Гравитон С2000Э.," 2023. [Online]. Available: https://graviton.ru/catalog/server_solutions/servers/server-line1/server-graviton-s2000e (Accessed: 27.3.2023).

[188] A. Shilov, "Russian-Made Baikal M1-Based Laptop Shows Up in Pre-Production. Tom's Hardware (12.8.2022).," 2022. [Online]. Available: https://www.tomshardware.com/news/russian-baikal-m1-based-pre-production-laptop-shows-up#xenforo-comments-3773758 (Accessed: 27.3.2023).

[189] В. Филатов, "Первый тест: на что способен российский процессор Baikal-M. CNews Zoom (24.4.2020).," 2020. [Online]. Available: https://zoom.cnews.ru/publication/item/63333 (Accessed: 27.3.2023).

[190] А. Степин, "Серверы на базе «Эльбрус» не прошли тесты Сбербанка, но не всё потеряно. Servernews (14.12.2021).," 2021. [Online]. Available: https://servernews.ru/1055898 (Accessed: 27.3.2023).

[191] АО МЦСТ, "Микропроцессоры и СБИС.," 2023. [Online]. Available: http://mcst.ru/chips?f[0]=field_availability:33&f[1]=field_processor_architecture:29 (Accessed: 27.3.2023).

[192] TOP500, "TOP500 LIST - NOVEMBER 2022.," 2022. [Online]. Available: https://www.top500.org/lists/top500/list/2022/11/ (Accessed: 28.3.2023).

[193] Э. Касми, "Россия внезапно ворвалась в мировой топ самых мощных суперкомпьютеров. CNews (16.11.2021).," 2021. [Online]. Available: https://www.cnews.ru/news/top/2021-11-16_rossijskie_superkompyutery (Accessed: 28.3.2023).

[194] Е. Черкесов, "«Т-платформы» – банкрот. Окончательно и бесповоротно. CNews (3.10.2022).," 2022. [Online]. Available: https://www.cnews.ru/news/top/2022-10-03_t-platformy_bankrot (Accessed: 28.3.2023).

[195] М.Видео-Эльдорадо, "От Й до Я: история создания отечественных смартфонов. Хабр (1.11.2021).," 2021. [Online]. Available: https://habr.com/ru/company/mvideo/blog/586684/ (Accessed: 28.3.2023).

[196] В. Чернышева, "На российском процессоре "Скиф" выпустят аналоги iPhone и iPad. Редакция «Российской газеты

(13.9.2021).," 2021. [Online]. Available: https://rg.ru/2021/09/13/na-rossijskom-processore-skif-vypustiat-analogi-iphone-i-ipad.html (Accessed: 28.3.2023).

[197] Д. Воейков, "РЖД закупает втрое дороже рынка смартфоны на российской ОС. Cnews (22.12.2021).," 2021. [Online]. Available: https://www.cnews.ru/news/top/2021-12-21_rzhd_v_35_raza_dorozhe_rynka (Accessed: 28.3.2023).

[198] QTECH, "QMP-M1-N IP68.," 2023. [Online]. Available: https://www.qtech.ru/catalog/mobilnye_ustroystva/smartfony/qmp_m1_n_ip68/#properties (Accessed: 28.3.2023).

[199] А. Патракова, "Российский «смартфон для параноиков» оказался не нужен. Его почти не покупают даже в условиях дефицита. CNews (25.4.2022).," 2022. [Online]. Available: https://www.cnews.ru/news/top/2022-04-25_rossijskij_smartfon_dlya (Accessed: 28.3.2023).

[200] Tadviser, "AYYA T1 (smartphone).," 2022. [Online]. Available: https://tadviser.com/a/e.php?id=628197 (Accessed: 28.3.2023).

[201] Р. Кильдюшкин, "Xiaomi стал крупнейшим поставщиком смартфонов в России. Газета.Ru (16.5.2023).," 2023. [Online]. Available: https://www.gazeta.ru/tech/news/2023/05/16/20418560.shtml (Accessed: 17.5.2023).

[202] SBC Group, "Решения собственной разработки.," 2023. [Online]. Available: http://www.sbcgroup.ru/solutions.html (Accessed: 29.3.2023).

[203] Яхонт, "Решения по поставке оборудования.," 2023. [Online]. Available: https://yakhont-shd.ru/solutions/ (Accessed: 18.4.2023).

[204] Яхонт, "Каталог СОРМ.," 2023. [Online]. Available: https://yakhont-shd.ru/catalog-sorm/ (Accessed: 18.4.2023).

[205] НОРСИ-ТРАНС, "Импортонезависимые решения на базе российской аппаратной платформы.," 2019. [Online]. Available: http://www.sec21.rans.ru/images/present/minakov.pdf (Accessed: 18.4.2023).

[206] Tadviser, "Яхонт-УВМ Э-серия Серверы хранения и обработки данных.," 2022. [Online]. Available: https://www.tadviser.ru/a/445572 (Accessed: 18.4.2023).

[207] ЭДЕЛЬВЕЙС, "Комплектующие ЭДЕЛЬВЕЙС.," 2023. [Online]. Available: https://edelweiss-

tech.ru/product/komplektuyushchie-edelveys/ (Accessed: 28.3.2023).

[208] GS Nanotech, "SSD.," 2023. [Online]. Available: http://gsnanotech.ru/products/ssd/ (Accessed: 29.3.2023).

[209] Rostec, "Ростех начал серийно производить защищенные роутеры. Новости (17.10.2022).," 2022. [Online]. Available: https://rostec.ru/news/rostekh-nachal-seriyno-proizvodit-zashchishchennye-routery/ (Accessed: 29.3.2023).

[210] InfoDiode, "АМТ InfoDiode. Информационная безопасность государственных информационных систем, организаций финансовой отрасли, объектов КИИ и АСУ ТП.," 2023. [Online]. Available: https://infodiode.ru/ (Accessed: 18.4.2023).

[211] Ancud, "DIOD 1000-SX.," 2023. [Online]. Available: https://ancud.ru/products/trusted-devices/diod/diod-1000sx.html (Accessed: 18.4.2023).

[212] Президент Российской Федерации, "Указ Президента Российской Федерации от 30.03.2022 № 166 "О мерах по обеспечению технологической независимости и безопасности критической информационной инфраструктуры Российской Федерации".," 2022. [Online]. Available: http://publication.pravo.gov.ru/Document/View/0001202203300001?index=0&rangeSize= (Accessed: 18.4.2023).

[213] А. Балашова, "Доля российского софта в госкомпаниях оказалась вдвое ниже нормативов. РБК (27.12.2021).," 2021. [Online]. Available: https://www.rbc.ru/technology_and_media/27/12/2021/61c21e289a79479e8562641b (Accessed: 18.4.2023).

[214] КАТАЛОГ Совместимости Российского Программного Обеспечения, "Импортозамещение. В этом разделе можно ознакомиться с тем, какие продукты предлагаются отечественными разработчиками для замещения определённых иностранных продуктов.," 2023. [Online]. Available: https://catalog.arppsoft.ru/replacement (Accessed: 18.4.2023).

[215] Реестр программного обеспечения, "Единый реестр российских программ для электронных вычислительных машин и баз данных.," 2022. [Online]. Available: https://reestr.digital.gov.ru/reestr/ (Accessed: 29.4.2022).

[216] А. Патракова, "Минцифры определило три самых популярных российских Linux. Cnews (1.11.2022).," 2022.

[Online]. Available: https://www.cnews.ru/news/top/2022-11-01_razrabotchikov_po_zastavyat?ysclid=laksoiqswu217187088 (Accessed: 20.4.2023).

[217] RUSSOFT Association, "Positions of Russian software companies in the global IT market.," 2021. [Online]. Available: https://russoft.org/wp-content/uploads/2021/12/1_Positions_of_Russian_software_companies_in_the_global_IT_market.pdf (Accessed: 18.4.2023)..

[218] Д. Савосин, "Спрос на российское программное обеспечение со стороны компаний подскочил на 300%. RB (9.3.2022).," 2022. [Online]. Available: https://rb.ru/news/russian-software-market/ (Accessed: 18.4.2023).

[219] Рамблер, "Около 50% россиян довольны качеством российского софта. Рамблер (7.6.2022).," 2022. [Online]. Available: https://news.rambler.ru/internet/48787153-okolo-50-rossiyan-dovolny-kachestvom-rossiyskogo-softa/ (Accessed: 18.4.2023).

[220] Kraftway, "Kraftway BIOS.," 2023. [Online]. Available: https://kraftway.ru/products/10/vstroennoe-po-materinskoy-platy/kraftway-bios/#appearance (Accessed: 19.4.2023).

[221] Numa, "Numa BIOS.," 2023. [Online]. Available: https://numatech.ru/products/bios/ (Accessed: 19.4.2023).

[222] RusBITech-Astra LLC, "OPERATING SYSTEMS.," 2023. [Online]. Available: https://astralinux.ru/en/products/ (Accessed: 19.4.2023).

[223] РусБИТех-Астра, "«Мобильная Астра» представлена на форуме «Армия-2022».," 2022. [Online]. Available: https://astralinux.ru/news/category-news/2022/mobilnaya-astra-predstavlena-na-forume-armiya-2022/?ysclid=lakty6rpp549644855 (Accessed: 20.4.2023).

[224] А. Васильев, "Первые 9 российских АЭС перевели на систему Astra Linux. А скоро поменяют и сами компьютеры – на Baikal или «Эльбрус». Банки Сегодня (30.6.2021).," 2021. [Online]. Available: https://bankstoday.net/last-news/pervye-9-rossijskih-aes-pereveli-na-sistemu-astra-linux-a-skoro-pomenyayut-i-sami-kompyutery-na-baikal-ili-elbrus (Accessed: 20.4.2023).

[225] А. Блинов, "Крым импортозамещается. «РусБИТех» и «Крымтехнологии» приступили к сотрудничеству. SPBITRU

(22.7.2015).," 2015. [Online]. Available: https://spbit.ru/news/n119990/ (Accessed: 19.4.2023).

[226] Известия, "Операционная система Astra Linux получила сертификацию в Белоруссии. Известия (18.2.2021).," 2021. [Online]. Available: https://iz.ru/1126339/2021-02-18/operatcionnaia-sistema-astra-linux-poluchila-sertifikatciiu-v-belorussii (Accessed: 20.4.2023)..

[227] П. Буренин, П. Девянин, Е. Лебеденко, В. Проскурин and А. Цибуля, "Безопасность операционной системы специального назначения. Astra Linux Special Edition. Москва: Горячая линия – Телеком.," 2019. [Online]. Available: https://astralinux.ru/information/library/publications/bezopasnost-operaczionnoj-sistemyi-speczialnogo-naznacheniya-astra-linux-special-edition (Accessed: 20.4.2023) pp. 11.

[228] A. Surkov, "Mono и ОС МСВС. Habr (2.10.2015).," 2015. [Online]. Available: https://habr.com/ru/post/268131/ (Accessed: 20.4.2023).

[229] Известия, "ФСБ и Минобороны одобрили использование российского софта. Известия (24.5.2019).," 2019. [Online]. Available: https://iz.ru/881429/2019-05-24/fsb-i-minoborony-odobrili-ispolzovanie-rossiiskogo-softa (Accessed: 20.4.2023).

[230] Военное обозрение, "Все компьютеры Минобороны будут переведены на российское ПО. Военное обозрение (9.1.2018).," 2018. [Online]. Available: https://topwar.ru/133359-vse-kompyutery-minoborony-budut-perevedeny-na-rossiyskoe-po.html (Accessed: 20.4.2023).

[231] АО НППКТ, "ОСнова.," 2023. [Online]. Available: https://xn–80ad6adbq.xn–p1acf/ (Accessed: 20.4.2023).

[232] СПЕЦСОФТЗАЩИТА, "ОСНОВА.," 2023. [Online]. Available: https://www.softdefence.ru/item/8-osnova? (Accessed: 20.4.2023).

[233] А. Уваров, "Российская система ОСнова - как основа защищенной инфраструктуры. Технический блог специалистов ООО"Интерфейс" (3.8.2022).," 2022. [Online]. Available: https://interface31.ru/tech_it/2022/08/rossiyskaya-sistema-osnova—kak-osnova-zashhishhennoy-infrastruktury.html (Accessed: 20.4.2023).

[234] Базальт СПО, "Альт СП. Дистрибутив для рабочих станций и серверов,сертифицированный ФСТЭК.," 2023. [Online].

Available: https://www.basealt.ru/alt-8-sp-sertifikat-fstehk/description (Accessed: 20.4.2023).

[235] Базальт СПО, "Выполненные проекты.," [Online]. Available: https://www.basealt.ru/projects (Accessed: 20.4.2023).

[236] РЕД СОФТ, "РЕД ОС. Российская операционная система общего назначения для серверов и рабочих станций.," 2023. [Online]. Available: https://redos.red-soft.ru/?ysclid=l2zom7n1j1 (Accessed: 25.4.2023).

[237] Ростелеком, "«Ростелеком» переходит на операционную систему «РЕД ОС». Новости компании (22.12.2020).," 2020. [Online]. Available: https://www.company.rt.ru/press/news/d457641/ (Accessed: 25.4.2023).

[238] N. Lomas, "Finland's Jolla, maker of Sailfish OS, is trying to cut ties with Russia. Techcrunch (1.3.2022).," 2022. [Online]. Available: https://techcrunch.com/2022/03/01/jolla-cut-ties-russia/?guce_referrer=aHR0cHM6Ly93d3cuZ29vZ2xlLmZpLw&guce_refe&guccounter=2 (Accessed: 26.4.2023).

[239] Tadviser, "Aurora OS (formerly SailfishOS).," 2023. [Online]. Available: https://tadviser.com/a/e.php?id=272511 (Accessed: 26.4.2023).

[240] ОС Аврора, "Главная / Устройства.," 2023. [Online]. Available: https://auroraos.ru/devices (Accessed: 26.4.2023).

[241] Открытая мобильная платформа, "Как ОС Аврора работает в Почте России.," 2023. [Online]. Available: https://www.omp.ru/case-rusian-post (Accessed: 26.4.2023).

[242] Г. Дорофеев, "В России нашли нового национального «убийцу» Android. Готовятся к выходу первые смартфоны на ОС РОСА. CNews (21.4.2023).," 2023. [Online]. Available: https://www.cnews.ru/news/top/2023-04-21_v_rossii_nashli_novuyu_natsionalnuyu (Accessed: 26.4.2023).

[243] НТЦ ИТ РОСА, "О компании.," 2023. [Online]. Available: https://www.rosalinux.ru/about/ (Accessed: 26.4.2023).

[244] NAVITEL, "Navitel Navigator with maps for Linux.," 2023. [Online]. Available: https://navitel.com/en/buy/apps-pnd (Accessed: 26.4.2023).

[245] Цифровые платформы, "NAVITEL Embedded Linux," 2023. [Online]. Available: https://platforms.su/platform/5438 (Accessed: 26.4.2023).

[246] А. Курилов, "В России запущены уже три магазина приложений. Чем они отличаются?. 4PDA (30.5.2022).," 2022. [Online]. Available: https://4pda.to/2022/05/30/400139/v_rossii_zapuscheny_uzhe_tri_magazina_prilozhenij_chem_oni_otlichayutsya/ (Accessed: 28.4.2023).

[247] Цифровые платформы, "АНО «Цифровые платформы» запускает работу по замене Google Play – NashStore. Цифровые платформы (29.3.2022).," 2022. [Online]. Available: https://diplatforms.ru/news/350 (Accessed: 26.4.2023).

[248] Д. Чебакова and В. Полякова, "Минцифры и VK анонсировали запуск магазина приложений RuStore. РБК (18.5.2022).," 2022. [Online]. Available: https://www.rbc.ru/technology_and_media/18/05/2022/6284c8b69a794762883c5690 (Accessed: 26.4.2023).

[249] NashStore, "Наше время - Наш стор. Альтернативный магазин приложений для Android.," 2022. [Online]. Available: https://nashstore.ru/ (Accessed: 28.4.2023).

[250] TJournal, "Проблемы модерации, ошибки и треш-игры: как прошёл запуск NashStore — «российского аналога» Google Play. Tjournal (17.5.2022).," 2022. [Online]. Available: https://tjournal.ru/internet/624251-problemy-moderacii-oshibki-i-tresh-igry-kak-proshel-zapusk-nashstore-rossiyskogo-analoga-google-play (Accessed: 28.4.2023).

[251] RuStore, "Официальныймагазин приложенийдля Android. Гарантированный безопасныйдоступ к приложениям.," 2023. [Online]. Available: https://www.rustore.ru/ (Accessed: 28.4.2023).

[252] RuMarket, "Все приложения.," 2023. [Online]. Available: https://ruplay.market/apps/ (Accessed: 28.4.2023).

[253] Russoft, "Маркетплейс российского программного обеспечения.," 2023. [Online]. Available: https://russoft.ru/ (Accessed: 28.4.2023).

[254] В. Бахур, "Пять отечественных разработчиков представили многоместные импортонезависимые рабочие станции для МФЦ. CNews (23.6.2021).," 2021. [Online]. Available: https://www.cnews.ru/news/line/2021-06-23_pyat_otechestvennyh_razrabotchikov?ysclid=lh7aarqdar8835128 (Accessed: 3.5.2023).

[255] Д. Степанов, "Создано первое решение для МФЦ на «Эльбрусах», отечественной СУБД и российском Linux. Cnews (30.4.2020).," 2020. [Online]. Available: https://www.cnews.ru/news/top/2020-04-30_sozdano_pervoe_kompleksnoe (Accessed: 3.5.2023).

[256] МойОфис, "Профессиональный 2. «МойОфис Профессиональный 2» – комплекс безопасных приложений и систем для профессиональных коммуникаций и работы с документами в облаке и офлайн на любых устройствах.," 2023. [Online]. Available: https://myoffice.ru/products/professional/ (Accessed: 3.5.2023).

[257] Д. Воейков, "ФСО закупает «Мой офис» на 10 тыс. мест вместо традиционного MS Office. CNews (3.8.2021).," 2021. [Online]. Available: https://www.cnews.ru/news/top/2021-08-03_fso_zakupaetsya_moim_ofisom (Accessed: 3.5.2023).

[258] Р7-Офис, "Р7-Офис.," 2023. [Online]. Available: https://r7-office.ru/ (Accessed: 3.5.2023).

[259] Свемел, "Операционная система «Циркон 37К».," 2023. [Online]. Available: https://swemel.ru/products-and-services/programmnyij-kompleks-terminalnogo-dostupa-«czirkon-36kt»/ (Accessed: 3.5.2023).

[260] Postgres Pro, "СУБД Postgres Pro.," 2023. [Online]. Available: https://postgrespro.ru/ (Accessed: 3.5.2023).

[261] КАТАЛОГ Совместимости Российского Программного Обеспечения, "Импортозамещение : Реляционные СУБД.," 2023. [Online]. Available: https://catalog.arppsoft.ru/replacement/section_6046270 (Accessed: 4.5.2023).

[262] М. Фролова, "Войти в IT: как в России проходит импортозамещение в сфере высоких технологий. Известия (30.3.2022).," 2022. [Online]. Available: https://iz.ru/1312422/mariia-frolova/voiti-v-it-kak-v-rossii-prokhodit-importozameshchenie-v-sfere-vysokikh-tekhnologii (Accessed: 3.5.2023).

[263] Я. Шпунт, "Грядет битва за наследство SAP. ComNews (20.4.2022).," 2022. [Online]. Available: https://www.comnews.ru/content/219892/2022-04-20/2022-w16/gryadet-bitva-za-nasledstvo-sap (Accessed: 4.5.2023).

[264] 1Ci, "Skyrocket Your Business. 1Ci provides flexible ERP and business digitisation solutions through the partner network spread

over 60+ countries all over the world.," 2023. [Online]. Available: https://www.1ci.com/company/ (Accessed: 4.5.2023).

[265] ИнфоСофт, "Опыт внедрений.," 2023. [Online]. Available: https://erp.is1c.ru/experience (Accessed: 4.5.2023).

[266] RTSoft, "НЕКОТОРЫЕ КРУПНЫЕ ПРОЕКТЫ.," 2023. [Online]. Available: https://www.rtsoft.ru/success-story/ (Accessed: 4.5.2023).

[267] Галактика, "«Галактика MES».," 2023. [Online]. Available: https://galaktika.ru/mes (Accessed: 4.5.2023).

[268] Консом групп, "MES «FORWARD». СИСТЕМА ОПЕРАТИВНОГО УПРАВЛЕНИЯ ПРОИЗВОДСТВОМ.," 2023. [Online]. Available: https://www.konsom.ru/solutions/informatsionnye-sistemy/mes-sistema/mes-forward-sistema-operativnogo-upravleniya-proizvodstvom/ (Accessed: 4.5.2023).

[269] Научно-производственная фирма «КРУГ», "Совместимость и аппаратные требования," 2023. [Online]. Available: https://www.krug2000.ru/products/ppr/scada-2000/compability.html (Accessed: 4.5.2023).

[270] Научно-производственная фирма «КРУГ», "Scada КРУГ-2000® - модульная интегрированная российская SCADA-система.," 2023. [Online]. Available: https://www.krug2000.ru/products/ppr/scada-2000.html (Accessed: 4.5.2023).

[271] Control Engineering, "Сравнение SCADA-систем российских разработчиков. Control Engineering (30.3.2022).," 2022. [Online]. Available: https://controlengrussia.com/scada-sistemy/sravnenie-scada/ (Accessed: 4.5.2023).

[272] Т. Исакова, "Киберзащита ударила по бюджетам. Коммерсант (31.5.2022).," 2022. [Online]. Available: https://www.kommersant.ru/doc/5380208 (Accessed: 4.5.2023).

[273] З. Карсанова and Ф. Каирова, "Научно-технический прогресс в России XXI века. Текст научной статьи по специальности «Экономика и бизнес» 2014.," 2014. [Online]. Available: https://cyberleninka.ru/article/n/nauchno-tehnicheskiy-progress-v-rossii-xxi-veka?ysclid=l9i4qq3dxm554635982 (Accessed: 5.5.2023) pp. 68.

[274] А. Шматко and Ю. Селиверстов, "Научно-техническое развитие в России: региональный аспект. Вестник БГТУ им. В.Г. Шухова 2017, №12.," 2017. [Online]. Available:

https://cyberleninka.ru/article/n/nauchno-tehnicheskoe-razvitie-v-rossii-regionalnyy-aspekt/pdf (Accessed: 5.5.2023) pp. 267.

[275] Л. Охотникова, "Национальная инновационная экономическая система России:условия формирования и тенденции развития. Вестник экономики, права и социологии, 2011, № 1.," 2011. [Online]. Available: https://cyberleninka.ru/article/n/natsionalnaya-innovatsionnaya-ekonomicheskaya-sistema-rossii-usloviya-formirovaniya-i-tendentsii-razvitiya/pdf (Accessed: 5.5.2023) pp. 67.

[276] А. Мельников, "Состояние и проблемы развития промышленного сектора экономики региона в условиях системного кризиса. Проблемы развития территории. Научный журнал ВолНЦ РАН ВЫП. 2 (88) 2017.," 2017. [Online]. Available: https://cyberleninka.ru/article/n/sostoyanie-i-problemy-razvitiya-promyshlennogo-sektora-ekonomiki-regiona-v-usloviyah-sistemnogo-krizisa/pdf (Accessed: 5.5.2023).

[277] Е. Илякова and Т. Савина, "Обеспечение научно-технического потенциала инновационного развития крупнейших отечественных корпораций: оценка, проблемы, тенденции. Национальные интересы: приоритеты и безопасность 7 (2016).," 2016. [Online]. Available: https://cyberleninka.ru/article/n/obespechenie-nauchno-tehnicheskogo-potentsiala-innovatsionnogo-razvitiya-krupneyshih-otechestvennyh-korporatsiy-otsenka-problemy/pdf (Accessed: 5.5.2023).

[278] Росстат, "Социально-экономические показатели по субъектам Российской Федерации. Росстат. Федеральная служба государственной статистики.," 2021. [Online]. Available: https://rosstat.gov.ru/folder/210/document/47652 (Accessed: 5.5.2023).

[279] M. Borak, "How Russia killed its tech industry. MIT Technology Review (4.4.2023).," 2023. [Online]. Available: https://www.technologyreview.com/2023/04/04/1070352/ukraine-war-russia-tech-industry-yandex-skolkovo/ (Accessed: 8.5.2023).

[280] Н. Королев, "Процессоры сложат в «Аквариус» Коммерсанть (10.10.2022).," 2022. [Online]. Available: https://www.kommersant.ru/doc/5606441 (Accessed: 8.5.2023).

[281] N. Taplin, "How Microchips Migrate From China to Russia. The Wall Street Journal (25.2.2023).," 2023. [Online]. Available:

https://www.strategicstudyindia.com/2023/03/how-microchips-migrate-from-china-to.html (Accessed: 8.5.2023).

[282] I. Talley and A. DeBarros, "China Aids Russia's War in Ukraine, Trade Data Shows. Despite sanctions, Moscow equips its jet fighters, submarines and soldiers with help of Chinese companies. The Wall Street Journal (4.2.2023).," 2023. [Online]. Available: https://www.wsj.com/articles/china-aids-russias-war-in-ukraine-trade-data-shows-11675466360?mod=article_inline (Accessed: 8.5.2023).

[283] M. Humphries, "Following US Sanctions, China Decides Its Future Lies With RISC Chips. PCMag (2.12.2022).," 2022. [Online]. Available: https://www.pcmag.com/news/following-us-sanctions-china-decides-its-future-lies-with-risc-chips (Accessed: 8.5.2023).

[284] Tadviser, "Chernyshenko: Russian fiber market is 76% occupied by foreign products.," 2021. [Online]. Available: https://tadviser.com/a/e.php?id=53753 (Accessed: 9.5.2023).

[285] Оптиковолоконные Системы, "О компании. Первый в России.," 2023. [Online]. Available: https://rusfiber.ru/o-kompanii/ (Accessed: 9.5.2023).

[286] Правительства Российской Федерации, "Дмитрий Чернышенко: Переход на полный цикл производства оптоволокна в Мордовии на 90% закроет потребность рынка. Новости (22.10.2022).," 2021. [Online]. Available: http://government.ru/news/43618/ (Accessed: 9.5.2023).

[287] RSpectr, "Операторы связи ждут появления отечественного телеком-оборудования. RSpectr (19.8.2022).," 2022. [Online]. Available: https://rspectr.com/novosti/operatory-svyazi-zhdut-poyavleniya-otechestvennogo-telekom-oborudovaniya (Accessed: 9.5.2023).

[288] Ю. Серебров, "TelecomDaily: в 2021 году сотовые операторы запустили около 82 тыс. БС. TelecomDaily (25.7.2022).," 2022. [Online]. Available: https://telecomdaily.ru/news/2022/07/25/telecomdaily-v-2021-godu-sotovye-operatory-zapustili-okolo-82-tys-bs (Accessed: 9.5.2023).

[289] RSpectr, "Базовые станции на вес золота. Как будут развиваться сотовые сети в условиях дефицита телеком-оборудования. RSpectr (27.7.2022).," 2022. [Online]. Available: https://rspectr.com/articles/bazovye-stanczii-na-ves-zolota (Accessed: 9.5.2023).

[290] Н. Рудычева, "Миграция на российскую ОС: основные сложности. Cnews (18.2.2021).," 2021. [Online]. Available: https://www.cnews.ru/articles/2021-02-17_migratsiya_na_rossijskuyu_os_osnovnye?ysclid=l9y11tsar7480810656 (Accessed: 9.5.2023).

[291] ФСТЭК России, "Государственный реестр сертифицированных средств защиты информации. (18.11.2022).," 2022. [Online]. Available: https://fstec.ru/tekhnicheskaya-zashchita-informatsii/dokumenty-po-sertifikatsii/153-sistema-sertifikatsii/591-gosudarstvennyj-reestr-sertifitsirovannykh-sredstv-zashchity-informatsii-n-ross-ru-0001-01bi00 (Accessed: 25.11.2022).

[292] Н. Демченко, "«Коммерсантъ» узнал об идее «Ростелекома» ограничить импорт смартфонов. РБК (27.10.2022).," 2022. [Online]. Available: https://www.rbc.ru/technology_and_media/27/10/2022/635a19289a794775c05186c3?ysclid=lakt4yzc80425539776 (Accessed: 10.5.2023).

[293] Хабр, "«Ростелеком» потратит 480 млрд рублей на мобильную экосистему с «Авророй». Хабр (17.11.2022).," 2022. [Online]. Available: https://habr.com/ru/news/t/699876/ (Accessed: 10.5.2023).

[294] Т. Корнев and Н. Королев, "«Авроре» снятся деньги. Коммерсантъ (17.11.2022).," 2022. [Online]. Available: https://www.kommersant.ru/doc/5669123 (Accessed: 10.5.2023).

[295] Роскомсвобода, "Критически значимым компаниям могут перекрыть письма с зарубежных IP. Роскомсвобода (21.3.2023).," 2023. [Online]. Available: https://roskomsvoboda.org/post/zapret-inostr-ip-pisem-kiishkam/ (Accessed: 12.5.2023).

[296] Роскомсвобода, "«Ростех» приобрел платформу для вычисления владельцев анонимных телеграм-каналов и будет предлагать эту услугу силовикам. Роскомсвобода (22.3.2023).," 2023. [Online]. Available: https://roskomsvoboda.org/post/doc-rth-rf/ (Accessed: 12.5.2023).

[297] Д. Дмитриев, "«Медуза» выяснила, что Роскомназдор еще в 2020 году создал систему для отслеживания антивоенных материалов в интернете. Медуза (13.4.2022).," 2022. [Online]. Available: https://meduza.io/feature/2022/04/13/meduza-vyyasnila-chto-roskomnazdor-esche-v-2020-godu-sozdal-

sistemu-dlya-otslezhivaniya-antivoennyh-materialov-v-internete (Accessed: 12.5.2023).

[298] Роскомсвобода, "«Ъ»: Роскомнадзор предлагает использовать ТСПУ для блокировки средств анонимизации. Роскомсвобода (25.3.2023).," 2023. [Online]. Available: https://roskomsvoboda.org/post/tspu-vs-virt-number/ (Accessed: 15.5.2023).

Puolustusvoimien tutkimuslaitos

Ylöjärven toimipiste
Esikunta, asetekniikkaosasto, räjähde- ja suojelutekniikkaosasto
PL 5, 34111 Lakiala

Riihimäen toimipiste
Doktriiniosasto, informaatiotekniikkaosasto, tutkimussuunnitteluyksikkö
PL 10, 11311 Riihimäki

Tuusulan toimipiste
Toimintakykyosasto
PL 5, 04401 Järvenpää

Puh. 0299 800

ISBN 978-951-25-3412-8 (painettu)
ISBN 978-951-25-3413-5 (verkkojulkaisu)
ISSN 2342-3129 (painettu)
ISSN 2342-3137 (verkkojulkaisu)

Puolustusvoimat
puolustusvoimat.fi/tutkimuslaitos