CONCERN
AVTOMATIKA

CONCERN OF OPPORTUNITIES

CONCERN
AVTOMATIKA

The Avtomatika Concern is an industrial company supplying integrated high-tech solutions with a high degree of information security for business and government.

The Concern's mission is to develop products and services aimed at creation of a comfortable environment for the development of customers' business, increase of the availability of communication services, safe transmission, processing and storage of information and improvement of the quality of life.

Avtomatika Concern
General Director

Vladimir Kabanov

DEAR COLLEAGUES!

The Avtomatika Concern is one of the leading enterprises of Russia in the field of information security. We intend to take the lead in the direction of "information security" of the national program "Digital Economy", and also aim at the continuous development and expansion of the high-tech products line for civil and dual usage.

The Avtomatika Concern has been entrusted with strategic tasks at the state level, such as the development and production of encryption equipment, the development of information cryptographic protection, the creation of special-purpose management systems, and the development and implementation of modern methods of protection against cyber threats.

Since 2018, the Concern has started diversification of production, and research and development in promising areas: creation of 5G communication networks, industrial Internet of Things IIoT, quantum cryptography, neural networks, artificial intelligence and digitalization of vehicles.

At the same time, complex tasks are being solved not only in national security ensuring, but also in import substitution, creating a line of trusted domestic telecommunications equipment and computing equipment based on Elbrus microprocessors.

Our customers are the Ministry of Emergency Situations of Russia, the Ministry of Industry and Trade, the Ministry of Defence, the Ministry of Health, the Ministry of Communications, the Pension Fund of Russia, the CEC of the Russian Federation, the Federal Protective Service, the Federal Security Service, the Federal Medical-Biological Agency, and regional authorities. In addition, the Concern's products are used by the largest defence industry enterprises and state-owned companies, such as Roskosmos, Rosseti, Rostelecom, Russian Railways, United Aircraft Corporation and Russian Post. Also, our solutions are used by mobile operators Megafon and VimpelCom, retail representatives, including Dixie and Magnet.

The results of our work confirm the correctness of the chosen path of strategic development: according to the results of 2018 the Concern ranked first among holding companies of the Rostec State Corporation radio-electronic cluster, demonstrating the highest revenue growth – up to 45%. The growth of the financial indicators of the Holding is due to the implementation of large-scale projects in civilian markets, inter alia in the field of the digital economy.

About the Concern

The Avtomatika Concern is a holding company, developing the systems and complexes intended for information protection. The holding designs, manufactures and modernizes facilities and systems of secure communications, develops technologies and methods for cryptographic information protection, automated control systems and hardware and software complexes, develops IT solutions for customers in various sectors of the economy.

The cooperation of research and production companies, formed under the auspices of the Avtomatika Concern, can solve the unique customers tasks and, most importantly, to present competitive and demanded integrated solutions and products to the market.

FIELDS OF ACTIVITY

- Communications and data transmission
- Computer Engineering
- Transport
- Trade
- Medicine
- Education
- Security
- Military-industrial complex

BASIC COMPETENCES

Development and implementation of complex projects in the field of information security

Serial production of electronic equipment, including secure communications

Development and implementation of information systems, telecommunication equipment and computing technology

R&D, research and development in promising areas (5G networks, industrial Internet of Things IIoT, quantum cryptography, neural networks and artificial intelligence)

CUSTOMERS

- Governments
- Commercial structures
- Uniformed agencies
- Russian defence enterprises
- State corporations
- Individuals
- Foreign customers

Our uniqueness

MORE THAN **70** YEARS OF EXPERIENCE

CENTRE OF COMPETENCE OF ROSTEC
STATE CORPORATION IN IT AND CYBER SECURITY

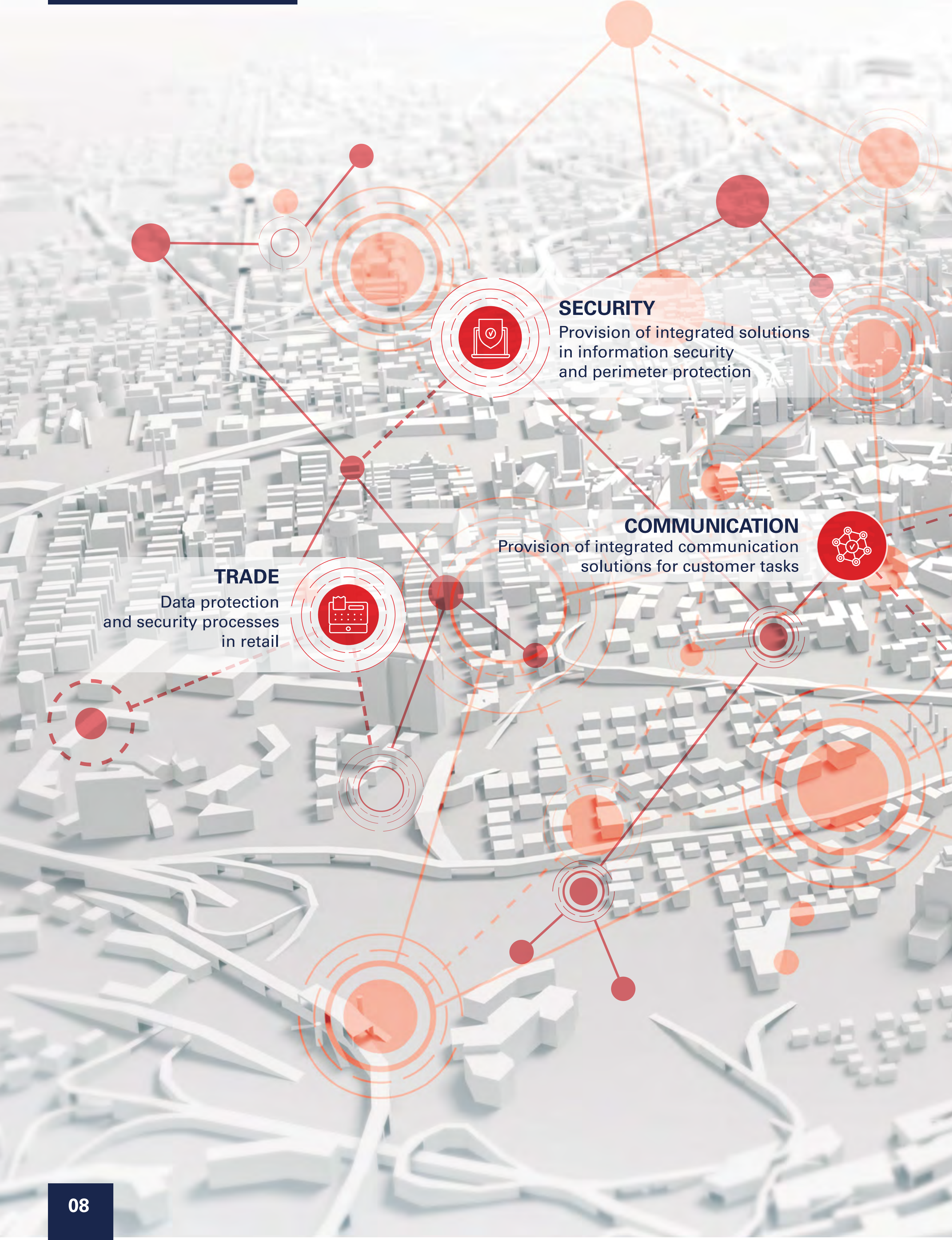
THERE ARE 36 DOCTORS OF SCIENCES

THERE ARE **36** DOCTORS OF SCIENCES

147 CANDIDATES OF SCIENCES

AMONG ENTERPRISE EXPERTS THE HOLDING EMPLOYS OVER **11,000** EMPLOYEES

- FLEXIBLE PRICE POLICY
- PROVISION OF NECESSARY SUPPORTING DOCUMENTATION FOR PRODUCTS
- TRAINING OF THE CUSTOMER’S PERSONNEL PRODUCTS HANDLING
- MODERNIZATION AND CUSTOM DEVELOPMENT SERVICES
- WARRANTY SERVICE SUPPORT



SECURITY

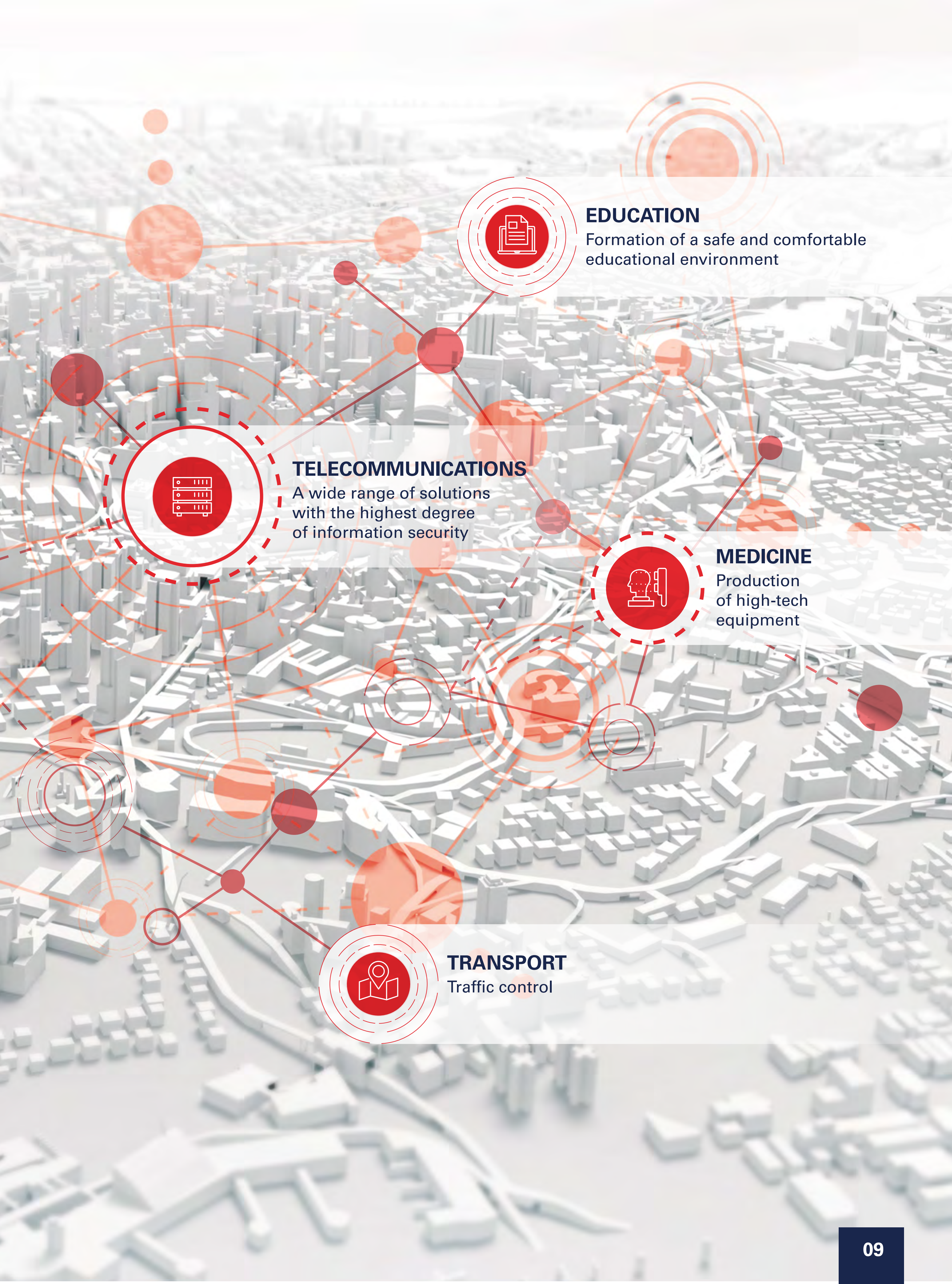
Provision of integrated solutions in information security and perimeter protection

COMMUNICATION

Provision of integrated communication solutions for customer tasks

TRADE

Data protection and security processes in retail



EDUCATION

Formation of a safe and comfortable educational environment

TELECOMMUNICATIONS

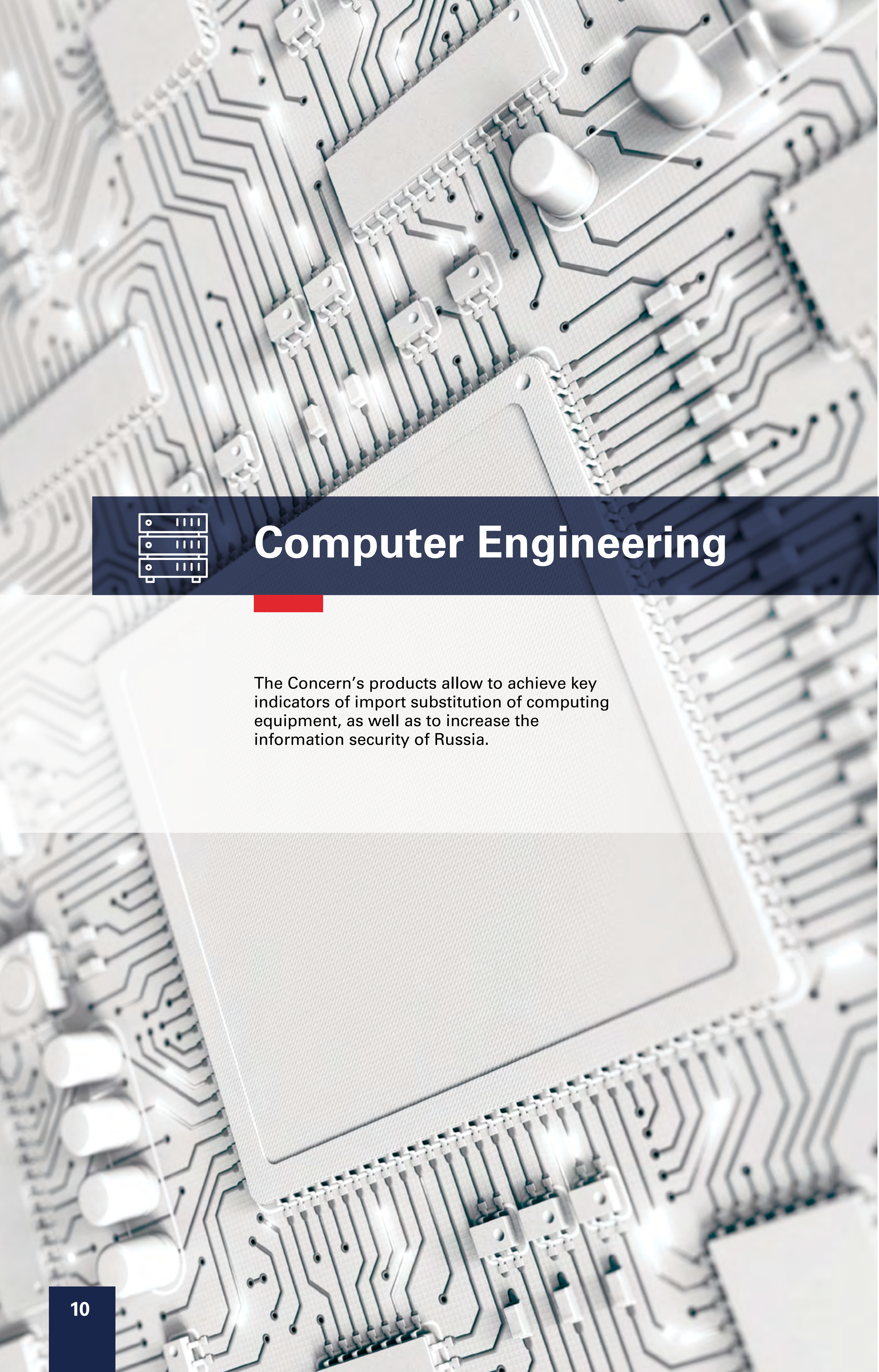
A wide range of solutions with the highest degree of information security

MEDICINE

Production of high-tech equipment

TRANSPORT

Traffic control



Computer Engineering

The Concern's products allow to achieve key indicators of import substitution of computing equipment, as well as to increase the information security of Russia.

Servers based on Elbrus microprocessors

(INEUM Elbrus-4.4, INEUM Elbrus 841/842)

KEY FEATURES

- The highest level of information security
- Russian own architecture
- Russian microprocessor
- No viruses
- Ability to run x86 code
- High performance, multiprocessing support

Infrastructure servers based on Elbrus-4S and Elbrus-8S microprocessors are intended to organize file servers, domain controllers, web servers, database servers, remote desktop servers, high-performance clusters, firewalls to meet the needs of the IT infrastructure. Elbrus microprocessor-based servers are a full-fledged replacement for foreign servers. As a base operating system, Russian OS based on the Linux kernel can be used.

SPECIFICATIONS

	INEUM Elbrus-4.4	**INEUM Elbrus 841/842**
Microprocessor and main chipset	4 Elbrus-4S microprocessors (4 cores Elbrus, up to 750 MHz)	4 Elbrus-8S microprocessors (8 Elbrus cores, up to 1,300 MHz)
RAM	up to 192 GB ESS DDR3-1600	up to 256 GB DDR-1600 ECC
External Interfaces	2 1000Base-T RJ-45 Ethernet ports 1 Ethernet port for Naval Management Module 2 USB 2.0 peripheral ports 1 RS-232 console port 1 video port with VGA connector	3 1000Base-T RJ-45 Ethernet ports 1 Ethernet port for Naval Management Module 2 USB 2.0 peripheral ports 1 RS-232 console port 1 video port with VGA connector
Internal Interfaces	2 PCI Express 1.0 x16 slots 2 PCI 2.0 33/66 MHz slots 1 slot for remote control module format SO-DIMM 8 SATA 2.0 ports 1 AC'97 Audio block 1 USB 2.0 port 2 USB 2.0 sockets 2 RS-232 sockets	3 PCI Express 2.0 x16 slots 2 PCI 2.0 33/66 MHz slots 1 slot for remote control module format SO-DIMM 1 M.2 slot for trusted loading module 8 SATA 3.0 ports 2 USB 2.0 sockets 1 RS-232 socket 1 HSTLM connector
System unit	Case format 19 /1 U, 2U	Case format 19»/1 U, 2U

Data storage systems based on Elbrus microprocessors

(INEUM Elbrus HD 823, INEUM Elbrus SHD 8124)

KEY FEATURES

- The highest level of information security
- Fully domestic DSS of primary, secondary and higher level of performance
- Easy migration from foreign to domestic equipment
- The maximum share of the Russian component

The one-controller data storage system INEUM Elbrus HD 823 is a dual-processor server equipped with a high-performance 16-disk subsystem.

Dual-controller data storage system INEUM Elbrus SHD 8124 is based on single-processor server boards with Elbrus-8S microprocessor and support for "hot swapping" to organize reliable data storage and usage.

As a management software for DSS organizing, it is possible to install enterprise-level software RAIDIX and distributed Ceph software optimized for work on microprocessors of the Elbrus series.

SPECIFICATIONS

	INEUM Elbrus HD 823	**INEUM Elbrus SHD 8124**
Microprocessor and main chipset	Two Elbrus-8S microprocessors, 8 Elbrus cores each Clock frequency 1,200 MHz 2 controller peripherals KPI-2	Two hot-swap storage controllers, each containing: 1 Elbrus-8S microprocessor, 8 Elbrus cores, 1,200 MHz clock frequency 1 controller for peripherals KPI-2
RAM	128 GB RDIMM ECC DDR3-1600	Two hot-swap storage controllers, each containing: 32 GB RDIMM ECC DDR3-1600
Network interfaces	Two hot-swap storage controllers, each containing: 4 1000Base-T Ethernet ports (integrated into KPI-2, excluding controlling ports) 2 Ethernet 10GBase-CX1 ports	Two hot-swap storage controllers, each containing: 3 1000Base-T Ethernet ports (integrated into KPI-2, excluding controlling ports) 2 Ethernet 10GBase-CX1 ports
Data storage systems	1 LFF SATA system disk Ability to install up to 2 LFF SATA disks 16 bays for SFF SATA/SAS disks, unlimited disk capacity	2 LFF SATA system disks 20 bays for SFF SATA/SAS disks, unlimited disk capacity

Computer complexes and workstations based on Elbrus microprocessors

(Elbrus 101-RS, Elbrus 401-RS, Elbrus 801-RS)

KEY FEATURES

- The highest level of information security
- No viruses
- Own Russian architecture
- Ability to run x86 code

Elbrus computer complexes are intended for the equipment of automated workplaces (AWP) of operators, thin clients, the organization of microservers and information terminals, applications in industrial automation and in systems with increased requirements to information security. It is possible to execute all workstations in a Tower type case or in a Monoblock type case.

As a base operating system, it is possible to use Russian operating systems on the Linux kernel, or to use the Windows operating system in x86 codes for a PC based on the Elbrus-8S microprocessor.

SPECIFICATIONS

	Elbrus 101-RS	Elbrus 401-RS	Elbrus 801-RS
Microprocessor	Elbrus-1 S+ (1 Elbrus core, up to 1,000 MHz)	Elbrus-4S (4 Elbrus cores, up to 800 MHz)	Elbrus-8S (8 Elbrus cores, up to 1,200 MHz)
RAM	16 GB ECC DDR3-1600	24 GB DDR3-600 ECC	32 GB DDR3-1600 ECC
Video subsystem	Built-in (2 HDMI ports)	Radeon R5 (HDMI, VGA, DVI)	Radeon R5 (HDMI, VGA, DVI)
External Interfaces	3 1000Base-T Ethernet ports 6 USB 2.0 ports 1 RS-232 port 6 Audio 5.1 ports	1 1000Base-T Ethernet port 4 USB 2.0 ports 1 RS-232 port 6 Audio 5.1 ports	3 1000Base-T Ethernet ports 6 USB 2.0 ports RS-232 port 6 Audio 5.1 ports
Internal Interfaces	1 mini PCI Express 2.0 x4 slot PCI Express 2.0 x16 slot 2 LVDS ports 1 HD Audio port 1 USB 2.0 socket 7 SATA 3.0 connectors 1 mSATA slot	1 PCI Express 1.0 x8 slot 2 PCI 2.0 33/66 MHz slots 4 SATA 2.0 connectors	2 PCI Express 2.0 x16 slots 1 PCI Express 2.0 x4 slot 1 PCI 2.0 slot 33/66 MHz 1 HSTLM (USB) slot 8 SATA 3.0 ports
System unit	nettop format case	mini-tower format case	mini-tower format case

Petaflops-level supercomputer based on Elbrus-8S microprocessors

Elbrus supercomputers are used to perform complex computational tasks in various areas that require the highest possible level of information security, including the processing of Big Data and deep analytics, creation and support of the cloud platforms operation.

Four-processor blade servers are based on Elbrus-8S eight-core microprocessor and a motherboard of our own design. All servers have unique functionality for remote diagnostics and control. Built-in monitoring system and proprietary power management algorithms increase fault tolerance.

The developed platform already has in its composition a power subsystem at the level of a separate server, taking into account the possibility of operation in difficult conditions with an extended voltage range and an increased level of interference.

The use of direct liquid cooling made it possible to reduce the size of a single blade server and to place up to 153 compute nodes in one standard rack with a height of 42U.

At the same time, the average annual PUE of such a system, reflecting the level of energy efficiency, is less than 1.06. That is, cooling consumes less than 6% of the total electricity consumed, which is a very high result for the HPC industry.

The total performance of one computing rack based on the Elbrus-8S microprocessor is about 75 TFlops (in double precision). It is possible to use various switching technologies, including the domestic machine-to-machine network to combine these racks into a single powerful computing cluster. The cabinet construction allows you to replace computing nodes, power supplies and hydro-regulation modules in the "hot-swapping" mode without interrupting the operation of the complex.

KEY FEATURES

- Domestic solution based on Russian microprocessors and self-developed motherboard
- The highest level of information security
- High performance for various complex calculating operations
- High installation density and compact solution
- Application of domestic direct liquid cooling technology
- Noiseless operation, no special requirements for the room
- Increased fault tolerance
- "Hot Swapping" mode without interrupting the of complex operation
- Easy initial deployment, easy system maintenance and upgrade
- Significant reduction in operating costs (saving of energy costs, footprint and maintenance)

Kupol Data Storage System

KEY FEATURES

- The optimal cost per unit of data storage
- Modular architecture for flexible scaling of stored data
- All key elements are duplicated to ensure reliable data storage.
- The system has been tested in the pilot areas of leading Russian telecom operators.

The Kupol DSS is a domestic secure data storage system for large and extra-large volumes with the possibility of certification for operations with data of any security category. The system has been successfully tested within the pilot areas of several federal telecom operators and is currently used to store data traffic as a part of the 374-FZ Yarovaya-Ozerova implementation.

The product was created by Russian engineers. All rights to software, working design documentation and the overall design of the system are owned by residents of the Russian Federation.

The Kupol DSS is supplied in the form of a fully pre-licensed and ready-to-use hardware and software complex.

SPECIFICATIONS

Power consumption	from 0.6 kW/1 PB of data
Capacity of one system	up to 18 PB
Number of I/O operations	8,000,000 (IOPS) per second
Maximum carrier, size	14 TB
Maximum volume, size	8 PB

Bulat B-DSS series Data Storage Systems

Convergent middle-class storage systems for large OLTP/OLAP databases, file sharing and cloud computing in government, financial, telecommunications, energy and multimedia industries.

KEY FEATURES

- Provide convergence in five areas: SAN and NAS, heterogeneous devices, storage from entry level to top class, HDD and SSD, as well as data storage and backup
- The simplest management platform, supports several product models with a graphical interface and is available for Windows, iOS and Android versions
- Provides industry-leading features: solutions scale up to eight controllers, 1 TB cache, 15 PB storage capacity, with various types of interfaces, including 16 Gbp/s FC, 56 Gbp/s InfiniBand, PCIe 3.0, 12 Gbp/s SAS, and intelligent I/O cards
- Protect customers' initial investments and reduce TCO for multiple applications, different product models and fast business growth

SPECIFICATIONS

	B-DSS-100-K	B-DSS-200	B-DSS-300	B-DSS-400VD	B-DSS-500VD
Number of controllers	1	1	1	2	2
Controller height	1U	2U	2U	2U	4U
Cache size per control module	up to 768 GB	up to 1,024 GB	up to 1,024 GB	up to 1,024 GB	up to 1,024 GB
Number of ports (per control module)	10	24	24	10	22
Supported host ports	8/16 Gbit/s Fibre Channel, 10 Gbit/s FCoE, 1/10 Gbit/s Ethernet, 56 Gbit/s InfiniBand, SAS 12 Gbit/s				
Number of discs max.	980				

HELIOS Platform for development of converged IT infrastructure

Helios is a set of integrated devices controlled by ECP Veil corporate cloud platform for creating a converged IT infrastructure of an enterprise.

Allows you to virtually combine the resources of the entire IT infrastructure in a single computing centre. With a converged infrastructure, the IT service of any institution can centrally manage software-defined resources: computing, network, and storage resources.

KEY FEATURES

- Quick deployment
- Easy configuration and management
- Resource Efficiency
- Fault tolerance
- Business continuity
- Scalability
- Technical support
- Ability to choose a hardware platform
- Reliability and safety management
- Original software designed for specific tasks
- Russian development

SPECIFICATIONS

HELIOS EXPRESS®	Helios Express® is offered in configurations of three full-size 2U servers or a complex with 4 full-fledged servers in a 2U package, providing significant savings in space and power consumption. Servers are clustered by a 1.2-switch, which is already included in the complex
HELIOS BUSINESS®	The delivery of Gelios Business® is possible in the form of six full-size 2U servers clustered by 1.2-switches, or in the form of a high-density 7U power-saving blade platform with six or ten blade servers and integrated 10G Ethernet switch. Additionally, you can order a 19" cabinet to create a turnkey computer system, in which servers with an uninterruptible power supply will already be installed and connected
HELIOS DATA-CENTRE®	The Helios Data Centre® line represents a ready-to-use complex in the configuration of two high-density energy-saving 7U blade platforms for ten blade servers clustered by a 10G Ethernet 1.2-switch housed in a 19” cabinet with an uninterruptible power supply

Each Helios® can include a high-performance data storage system to enable the large numbers of virtual machines to run with disk data allocation on shared storage

Corporate cloud platform ECP VEIL

ECP Veil is designed to create and manage the IT infrastructure of distributed data centres of an enterprise.

The platform includes all the basic functions for the effective provision of computing resources to employees of the enterprise according to the IaaS model, and also provides opportunities for scaling and automating of administration combined with fault tolerance and energy efficiency of the system.

ECP Veil is a profitable investment in development for companies that require the rapid deployment of IT infrastructure and simple management of it.

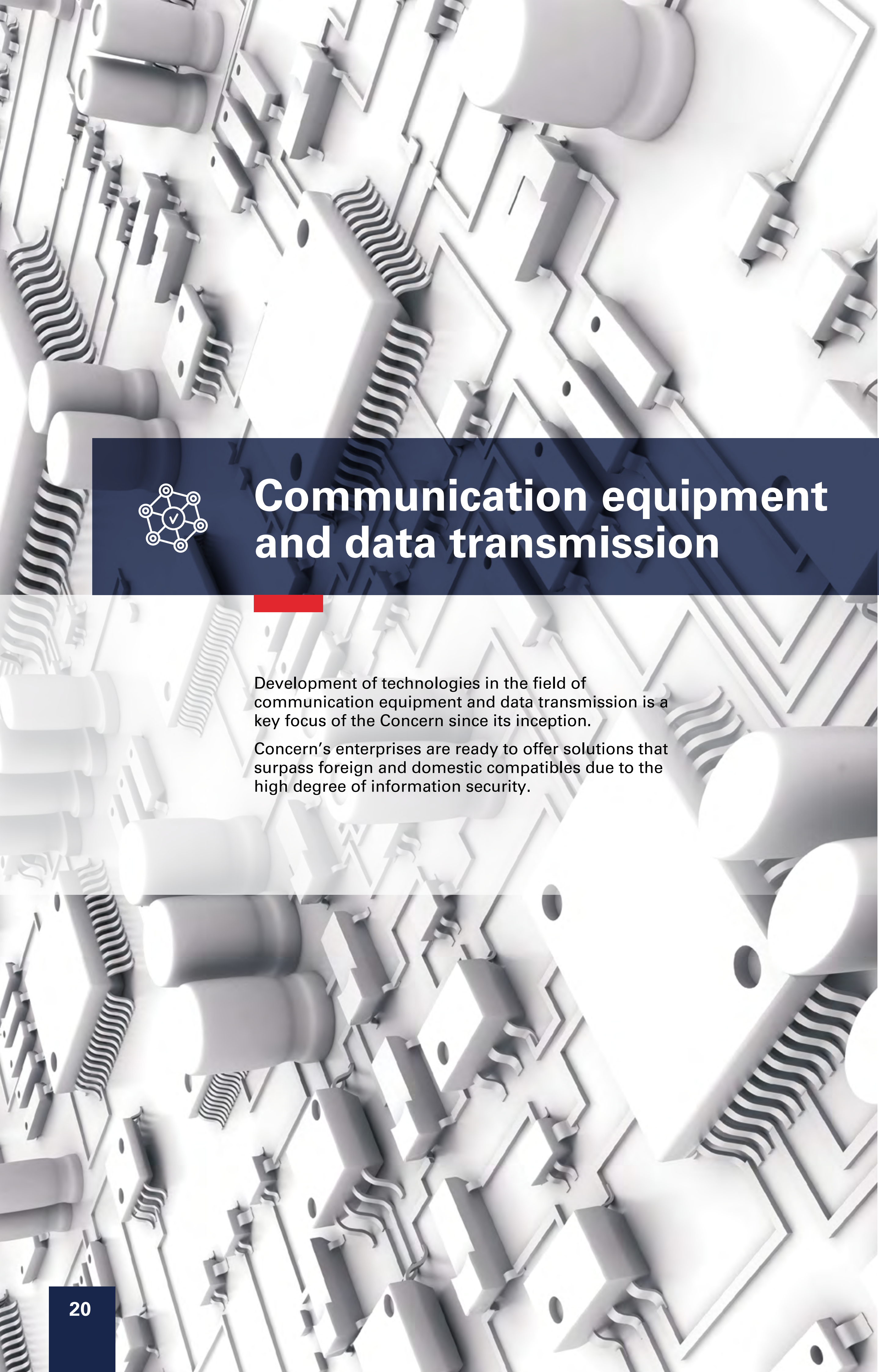
KEY FEATURES

- Domestic development included in the unified register of Russian programs for electronic computers and databases (ERPP)
- Virtual IT infrastructure managed by ESR Veil can be installed, configured and ready to launch the necessary services within an hour
- Provides the possibility of the equipment service and hot-swapping without interrupting the work of services due to the possibility of their flexible placement on any servers
- Built-in mechanisms for fault tolerance of the platform minimize the downtime of business services deployed based on it

Enterprise Cloud Platform VeiL
Платформа виртуализации IT-и телеком инфраструктуры
масштаб
VeiL Enterprise Cloud Platform

SPECIFICATIONS

Infrastructure Management	Administration of a local cluster of servers from a single web interface, administration of geographically distributed locations from a single web interface, automated configuration of physical servers when added to virtual infrastructure
Virtual Machine Management	Creating a virtual machine from a disk image, creating a virtual machine from an optical disk image, cloning, “live migration”, support for snapshots, forwarding PCI and USB devices, dynamic addition and removal of resources
Virtual Network Management	Distributed virtual switch, support for network interface aggregation, creating overlay L2-networks for the interaction of virtual machines in a geographically distributed infrastructure
Storage Management	Support for virtual machine data storage on file or block devices on a virtualization server; support for virtual machine data storage on external storage systems connected via file and block access protocols
Built-in network services	DHCP-server, firewall, NAT
Support for access to storage systems	NFS, iSCSI, shared iSCSI, FC
Monitoring	Logging of all system events, collecting metrics via SNMP, uploading logs to monitoring systems
Access Control	Support for Active Directory services, LDAP, support for single SSO sign-on, role-based access control system
Fault tolerance	Support for automatic recovery of virtual machines, support for VM disaster-resistant copies at independent geographically distributed locations, support for redundancy of the server controller



Communication equipment and data transmission

Development of technologies in the field of communication equipment and data transmission is a key focus of the Concern since its inception.

Concern’s enterprises are ready to offer solutions that surpass foreign and domestic compatibles due to the high degree of information security.

Network, telecommunication and electrical cabinets

Cabinets are designed for installation of network and telecommunication 19” equipment of the Evromekhanika standard or electrical products.

KEY FEATURES

- Russian production, optimal production and service time
- Possible cabinet construction and filling according to customer requirements
- Can be supplied complete with various accessories, passive components of the structured cabling and uninterruptible power supplies of various capacities.
- Cabinets can be adapted to the requirements of a specific customer and can be made according to his terms of reference

SPECIFICATIONS

Version	Floor and wall
Wide range of sizes	Width: 600-1,000 mm Depth: 400 -1,200 mm Height: 3U - 48U
Additional equipment	
Shelves	Console, extendable, full-size Made of 1.5 mm sheet steel and perforated
Free unit stubs	Made of 1.2 mm sheet steel
Ventilation panels	Installed in the cabinet roof. There are also panels for air drawing through the cabinet with installation on 19” profiles
Front and rear glazed and metal doors	83% perforated (rear hinged doors), handles with lock
Support angles for equipment installation	Made of 1.2 mm sheet steel
Cable Organizers	Horizontal, vertical, with rings, combs, etc.
Other	Lighting panels, socket blocks, power cables, grounding bus in 19" version, grounding cords, fasteners, cable ties for fastening cords and cables

BULAT BS7510 High Performance Routing Switch

KEY FEATURES

- Non-blocking switching matrix with powerful caching capabilities
- High port density at 1U:48x10Gbase + 6x40Gbase
- Wide range of supported features and protocols
- Power redundancy by 1+1 scheme
- Redundancy of cooling modules by 1+3 scheme

The BULAT switch BS7510 series is a powerful device for building modern data centres and deploying the latest cloud services. The product has a single non-blocking architecture and provides high speed packet switching. The BS7510 series is a secure foundation for building of enterprise-class cloud networking solutions.

SPECIFICATIONS

Ports	48x10GBase (SFP+), 6x40Gbase (QSFP+)
Switching matrix performance	1.28 Tbyte/sec
Memory buffer	12 Mbyte
Table capacity, MAC addresses	32K/288K
Maximum Ethernet frame size, Byte	9K
Number of ACL entries	4K
Routing table capacity, number of routes	IPv4: 16K/112K IPv6: 8K/56K

Kronos firewall with intrusion detection functions

KEY FEATURES

- Functions in convergent networks: data, voice, video
- Continuous monitoring and intrusion detection in near real-time mode
- The possibility of selecting a hardware platform for customer requirements

Kronos is a family of firewall complexes designed for reliable protection of departmental and corporate communication networks from external network threats and intrusions. This model range includes complexes made on hardware platforms of both foreign and Russian production using domestic circuit solutions. The complexes can be used to perform packet filtering of traffic, network address translation and setting of demilitarized zones (DMZ), as well as creating a secure communication channel based on a public network (VPN).

SPECIFICATIONS

Routing capacity	1.3 to 25 Gb/s depending on the model
Firewall capacity	0.09 to 3 Gb/s depending on the model
IPS capacity	10 to 2,048 Mbyte/s depending on the model
Number of simultaneous connections	1.8 to 8.9 mln depending on the model
Embedded interfaces	(1 -2)x1 GbE, RJ45 1 x1 GbE, SFP depending on the model
Expansion modules	2.4,6x1 GbE (RJ45, SFP) 2.4x1 OGbE (RJ45, SFP+) depending on the model
Housing	Desktop - for the younger model. For other models - 1 U, 3U
Input power	100-240 V, 50-60 Gz

Cruise-K protected telephone communications device

Cruise-K is an office IP-phone that implements both confidential and open conversations.

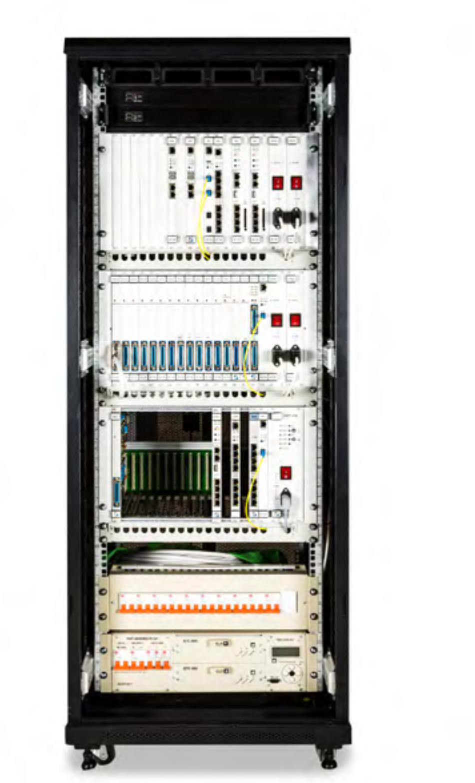
It provides for conducting duplex telephone conversations in two modes: closed mode with cryptographic protection of information when interacting with similar equipment and open mode when communicating with a regular IP-phone.

KEY FEATURES

- The first commercial IP-phone with crypto protection in Russia
- The best coding quality of speech information with sufficiently high compression
- High quality speech reproduction at low speeds
- The machine uses a key system: RIK-2 card electronic key carrier, the basic Russian intellectual card is made on the basis of a domestic microcontroller KB5004VE 1
- Category “trusted product”: encryption algorithm certification; a system using hardware and software to ensure the processing of information of a different category (for internal use, commercial, open) by a group of users without violating access rights
- Ensuring communication between subscribers in both open and closed mode, which is a unique technology that has no analogues
- The impossibility of unauthorized secret removal of information transmitted
- Domestic product

SPECIFICATIONS

Speech codecs	MR-CELP at a speed of 4.8 kb/s for work in the mode of secret communication; G.729 G.711 for open communication
System	Key system is used: electronic key carrier - RIK-2 card
Certificate	Certificate of Conformity of the Federal Security Service of the Russian Federation
Other	It can be used in communication networks with Internet access or local area networks with many equidistant subscribers. The product operates by providing a static (white) or virtual (cloud) IP address. The connection is established using the SIP protocol, which describes a method for establishing and terminating a user Internet session, including the exchange of multimedia content. The device implemented means of cryptographic information protection (CIPM) class KB.



Proton-KA Office-Production Automatic Telephone Station

Universal hardware and software system for the organization and development of multi-service switching and access nodes. Combines channel switching technologies (TDM) and information packet switching technologies (IP). Due to the implementation of a similar system of on-screen menus and algorithms for the operation of digital telephones, it completely replaces imported Siemens PBXs (Unify) Hicom300 / HiPath4000 / OpenScape4000.

KEY FEATURES

- Fully Russian development and manufacturing are confirmed by the status of telecommunications equipment of the Russian origin (TERO)
- Certification in the certification system of the Federal Security Service of Russia for compliance with the temporary requirements for the protection of equipment (including the communication server in the part of IP telephony) and control systems from computer attacks and information leakage through technical communication channels for A2 security level
- No need to purchase licenses, unlike foreign manufacturers
- Possibility of delivery of Siemens/Unify digital telephone sets modified by the protection device, intended for installation in dedicated premises up to category 1 inclusive

SPECIFICATIONS

Capacity	up to 5,760 ports (full accessible non-blocking switching field)
Reservation	Hot backup of the power system and control system. Backup of software in full to external media.
Inter-station interfaces	Ethernet, E1 (OKC7, EDSS1, Q.SIG, ECMAv2, including with the support of the functions of the CorNet-N, R2, R1.5, 2BCK, 1 VSY, physical lines (FXO, E&M, 1 BCK, 2 BCK, ADASE, ADASZHD, 600+750, TDNIADNV, etc.)
Subscriber interfaces	FXS (60 V/1,800 Ohm, BORCHST; MB), UpO (LG), UpOE (Siemens), Ethernet
Connection of subscriber terminals	Support for all types of subscriber devices: SIP-phones (including telephones with subscriber encryption), digital phone sets from Siemens/Unify, lines Optiset E, OptiPoint 500, OpenStage T, lines LDP, LDK of LG.

BS-430 Station

The BS-430 Station is a base station for operation as part of TETRA digital trunked mobile radio systems, providing communication between subscriber radio stations located in the service area and the TETRA network. The modular design of the elements layout allows to fully meet the requirements of consumers, both in terms of the number of subscribers being serviced and in integration with existing fixed and wireless communication systems.

KEY FEATURES

- The station meets modern requirements to the equipment of professional radio communication systems.
- Possibility of full operation offline, including subscriber control and authentication

SPECIFICATIONS

Frequency range, MHz	410-430 (450-470)
Number of carrier frequencies	up to 4
Power, W	up to 25
Sensitivity, dBmW	-115/-1 06
Spaced reception	double
Duplex separation, MHz	10
Bandwidth, kHz	25
Frequency Shift, kHz	-12.5; 0; +12.5
Modulation type	p/4 DQPSK
Frequency instability	0.2x10-6
Power supply	-48 V DC, 220 V AC
Power consumption, W	not more than 700
Resistance to external influences	GOST 16019-2001, version C1

IVA AVES S
server for secure video conferencing

The product allows users (including those geographically distant from each other) to access unified communications services using local (LAN) and global (WAN) data networks, the Internet. At the same time, users are able to see and hear their interlocutors in real time, demonstrate various contents to other participants of the event, exchange other information depending on the type of event. IVA AVES S operates on the basis of the special purpose operating system Astra Linux Special Edition.

KEY FEATURES

- Protection of processed information (Certificates of conformity of the Ministry of Defence of the Russian Federation and Federal Service for Technical and Export Control)
- Reliable communication of a large number of conference participants
- Scaling as needs increase
- Wide range of end devices
- Exchange of audio information, video information in real time both between individual users and between a group of users
- Personal and group text messaging
- Connection to video conferencing of subscribers working only in audio mode
- Demonstration of various contents to participants of the event.
- The maximum number of conference participants is determined by the number of licenses purchased

SPECIFICATIONS

Simultaneous operation of user terminals in high-definition video conferencing	40 subscriber terminals (with the possibility of increasing the number of participants, due to scaling)
Standards and protocols support	RTSP cctv cameras SMPP to send SMS through a plug-in gateway HTTP, FTP, UDP, ULPFEC
Video codecs	H.261, H.263, H.263+, H.263++, H.264, H.265 (HEVC) for SIP, VP8
Real-time content translation protocols	H.239, BFCP
Audio codecs	Opus; Speex; AAC (only for reading from file); G.711 u-Law; G.711 a-Law; G.722; G.729; G.722.1 Annex C.(G.722.1C/Siren 14) 48 kb/s, 32 kb/s, 24 kb/s; G.722.1 (Siren 7) 32 kb/s, 24 kb/s; G.723.1; G.728; G.726
Video standards	4K; 1,920x1,080px 60fps; 1,280x720px, 30fps; 960x540px 30fps; 640x360px 30fps; 4SIF (704 x 480px) / 4CIF (704 x 576px); SIF (352 x 240px) / CIF (352 x 288px); qVGA (320x240px); QSIF (176 x 120px) / QCIF (176 x 144px); VGA; SVGA; XGA
Signalling protocols	H.323, SIP, WebRTC technology

IVA LARGO terminal for secure video conferencing

IVA LARGO is intended for user participation in individual and group video conferences. The product provides customer participation in videoconferencing sessions, and the ability to hear and see other interlocutors in real time.

During video conferencing, the product has the ability to receive and display various contents, as well as transfer it to the video conference, and show it to other participants of the event. The product implements information protection tools that comply with the requirements of Federal Service for Technical and Export Control and Ministry of Defence of the Russian Federation and ensure the security of the information being processed.

KEY FEATURES

- Control via remote control panel or remote control via WEB interface
- Ability to automatically change the bandwidth and video quality
- Control of the layout and type of visible information from the video terminal
- Support of SIP, H.323, WebRTC; Ability to show content (media files, documents)
- Built-in MCU for 4 simultaneous connections
- High resolution support, up to 4K
- Automatic noise reduction
- Full duplex echo cancellation
- Dynamic synchronization of sound and image
- LDAP integration
- Ability to update software
- Interface language is Russian, English
- Supports oncoming work with servers of multipoint domestic and foreign manufacturers.
- Compatible with audio and video conference room systems
- Russian development
- Russian-language documentation and technical support
- Infrastructure development and service support localized in Russia
- Certificates of conformity of the Federal Service for Technical and Export Control and Ministry of Defence of the Russian Federation
- Declaration of TRCU, Ministry of Communications

SPECIFICATIONS

Supports the following video formats	4K 30/60 frames/sec; 1,080p 30/60fps; 720p 30/60fps; 4SIF/4CIF 30/60fps; SIF (352 x 240); CIF (352 x 288); QSIF (176 x 120); QCIF (176 x 144); w288p; w448p; w576p
Camera	PTZ camera, (included up to 1,080p30) or webcam, depending on the supply contract
Audio codecs	G.711 A/M, G.722, G.722.1 & Annex C, .723.1, G.728.G.729A
Video codecs	VP8, F4.265 (PIEVC) (for SIP protocol), FI.264 Baseline/Fligh profile, H.264 AVC, FI.263, H.263++, FI.261
Connection protocols	SIP, FI.323, WebRTC technology
Content transfer protocols	FI.239 and BFCP
Network protocols and Technologies	DNS, DHCP, LAN/Ethernet (RJ-45) 10/100/1,000 MByte
Built-in MCU (additional functionality, opening by license)	The maximum number of video conference participants is 4 in 1,080p30 format.
LDAP Integration	Microsoft Active Directory; Novell Directory; Astra Linux Directory

Security

Avtomatika Concern is the centre of competences in the field of cybersecurity of Rostec State Corporation. Ensuring of the security, not only informational, but physical also is one of the main activities of the company.

Arched metal detector MTD-KA

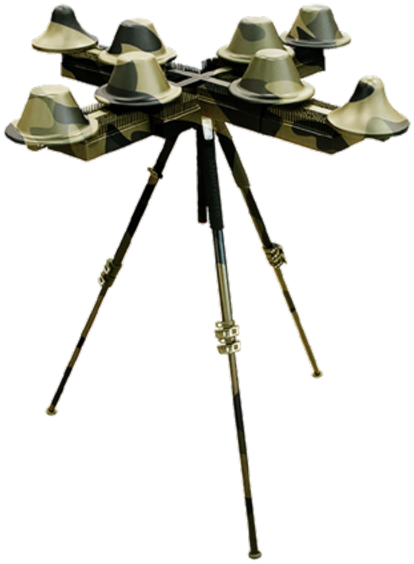
MTD-KA is designed to ensure public safety in places of mass gathering. Metal detector can detect prohibited metal objects. At the request of the customer it can be equipped with a video camera with a facial recognition system based on one of the fastest and most accurate algorithms in the world from the NtechLab company. When a match is found with a person from the monitoring list, notifications are instantly received by security officers. NtechLab software allows to process online video stream from an unlimited number of cameras simultaneously.

KEY FEATURES

- Simultaneous detection of several metal objects
- Two LED strips on both panels
- Definition of ferrous and non-ferrous metals
- Automatic adjustment of operating frequencies ensures the elimination of effects from various sources of electrical interferences
- Protection against false positives
- Sound and light alarm
- Smart counters for passenger traffic and the number of alarms triggered
- Sensitivity adjustment
- 12 detection zones

SPECIFICATIONS

Protection against unauthorized access	Password protected software
Distance between detectors	0.3 m with low sensitivity 0.5 m with high sensitivity
Mains voltage	AC 187 V ~ 242 V, 50/60 Gz
Signal frequency	7,000-8,999 Gz (adjustable)
Power consumption	12 W
Total gross weight	70 kg
External dimensions (HxWxD)	2,220x820x500 mm
Internal dimensions (HxWxD)	2,000x700x500 mm
Working temperature	from -20°C to +50°C



Kupol object complex for electronic UAV countermeasures

The Kupol is a portable/stationary complex for omnidirectional UAV countering 360°x180°. Designed to influence the channels of UAV navigation, control and transmission of information in order to hinder the functioning of the UAV in the airspace of the object.

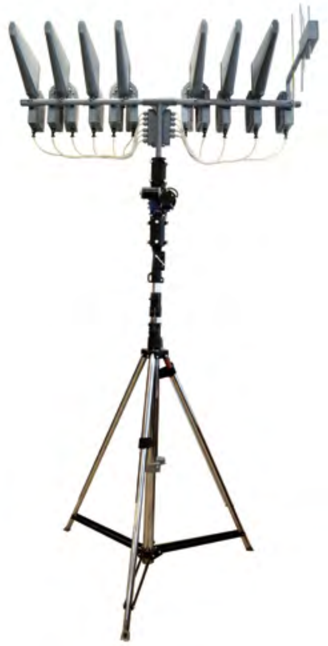
KEY FEATURES

- It is equipped with antenna feeder system of isotropic radiation, providing UAV countermeasures, omnidirectional 360°x180° (creating a "dome" irresistible for the UAV)
- Counteraction radius is not less than 2.5 km
- Weight is 13 kg, the closest analogue from competitors weighs more than 100 kg
- Deployment time is 4-5 minutes

SPECIFICATIONS

Complex operating frequency bands of simultaneous radio suppression	a) 420-460 MHz, P = 10 W;
	850-980 MHz, P = 10 W;
	1,165-1,250 MHz, P = 10 W;
	1,570-1,620 MHz, P = 10 W;
	2,400-2,485 MHz, P = 10 W;
	5,550-5,850 MHz, P = 10 W;
	b) GPS, GLONASS, Galileo (L5, E5ab, G3) channels: at frequencies:
	1,164-1,214 MHz, P = 10 W;
	c) GLONASS GPS, GLONASS, Galileo channels: (L1, E1, G1):
	at frequencies of 1,544-1,610 MHz, P = 10 W.
	80W integrated power

Outdoor equipment of the complex ensures operation	in the temperature range from -40°C to + 50°C; when exposed to atmospheric precipitation (rain) with an intensity of 5 mm/min; when exposed to sand and dust



Luch-PRO portable complex for UAV countering

KEY FEATURES

- Equipped with an antenna feeder system with directional radiation of 30°x60°, which ensures effective suppression of the UAV (copter type) at a distance of at least 6 km in the direct visibility
- Weight of 25 kg (without rotary support)

Luch-PRO is a stationary complex for countering a directional UAV. Designed to influence the channels of UAV navigation, control and transmit information in order to hinder the functioning of the UAV in the airspace of the object.

SPECIFICATIONS

Complex operating frequencies of simultaneous radio suppression	The energy potential of the subsystem: in the range of 0.3 + 1 GHz - not less than 150 W, in the range of 1 + 2 GHz - not less than 200 W, in the range of 2 + 6 GHz - not less than 150 W. Interference generated by the subsystem is amplified and radiated simultaneously in at least two bands. The accuracy of combining the frequency-targeted interference is at least 10% of the width of the suppressed signals high-frequency spectrum. The reaction time when creating a target frequency interference is not more than 100 ms. Transmitting antennas provide emission of interference with linear vertical polarization. The range of resistance is not less than 4 km.
The complex includes	antenna-feeder system - 1 set noise generator blocks - 1 set basic and rotary device of radio jamming subsystem - 1 set AWP on the basis of a controlling PC of a laptop type - 1 set
Outdoor equipment of the complex ensures operation	in the temperature range from -40 °C to + 50 °C; when exposed to atmospheric precipitation (rain) with an intensity of 5 mm/min; when exposed to sand and dust

Pishchal-PRO manpack complex for UAV countering

KEY FEATURES

- The combination of high effectiveness in countering the unlawful use of UAVs with the safety of the operator's health
- Ability to work both from stationary positions and in motion
- Does not require special training of the operator and is ready for combat use on a time scale close to real

Pishchal-PRO is a portable complex for UAV countering. Manpack handheld complex designed to disrupt the UAV flight mission by suppressing the communication channels, control and navigate the UAV from unprepared positions of the protected area.

SPECIFICATIONS

Interference Frequency ranges	Navigation systems: GLONASS, GPS, Galileo, Beidou Communication and control systems: 433 MHz 1SM; 915 MHz ISM; 1.5 GHz ISM; 2.4 GHz ISM; 5.8 GHz ISM / Wi-Fi
Suppression range	not less than 2,000 m, under the direct visibility
Power supply voltage	16 V
Battery capacity	10 A/h
Type of interference generated	Noisy, sighting in direction
Duration of continuous work	At least 1 hour
Working temperature range	From -20°C to + 40°C
Overall dimensions (W × H × D)	200x240x930 mm
Weight	Not more than 3.5 kg

Multiuser IP-intercom

KEY FEATURES

- Intellectual system of the on-door intercom, keyless entry, child safety, opening of the barrier, elevator call
- Advanced security features (apartment module, outdoor module, subscriber unit module), alerts, the effect of being at home anywhere in the world, phone events, secure keys of a smart intercom

The IP-intercom is equipped with a 4.5-inch colour display and a FullHD widescreen IP camera with a face recognition function, which allows you to automatically open the door without a key when the tenant approaches the entrance, as well as track outsiders' visits. Also, an intercom allows you to open the door with a mobile phone using G-Open technology and when connected to the Internet it integrates into a single network with a fire alarm system, which allows the device to automatically report to the emergency call centre about a possible fire and notify residents.

SPECIFICATIONS

DC mains voltage	12V
Life time	not less than 7 years
Overall dimensions	330x155x68.5 mm

NKM-2.10 navigation-cryptographic module of tachograph

Software-hardware cryptographic means, a block of CIPF tachograph Navigation cryptographic module NKM-2.10, is a component of the tachograph, designed to implement the cryptographic algorithms necessary to calculate a qualified electronic signature, conduct authentication procedures and ensure the protection of information processed and stored in the tachograph and subject to protection in accordance with the legislation of the Russian Federation.

KEY FEATURES

- Mutual authentication of tachograph cards and NKM-2.10
- Formation and transfer to the tachograph processor of data on coordinates, vehicle speed and current time
- Archiving of data on vehicle motion parameters and current time
- Archiving of data about the NKM-2.10 and tachograph events
- Archiving of data on request from the tachograph;
- Long-term storage of recorded data (for the last 365 days) in uncorrectable form in the archive of NKM-2.10
- Ensuring of the confidentiality, integrity and authentication of data downloaded from the NKM-2.10 archive to external media
- Management of control over access to the data of the archive NKM-2.10
- Ensuring of confidentiality, integrity and authentication of data transmitted between the tachograph and tachograph cards
- Key information storage

Cryptoserver software-hardware complex

KEY FEATURES

- Cryptoserver SHC is designed as a separate hardware module that is connected to the user’s LAN and AWP

Cryptoserver SHC provides cryptographic protection of confidential information and protection against unauthorized access.

The complex includes:

- Cryptographic system
- Means of protection against network attacks
- Means of protection against unauthorized access
- Audit system
- Access control system
- Interaction interface system
- with user: CORBA-interface
- and XML RPC-interface
- Digital certificate services

The software of the complex creates a closed software environment formed by these components.

Software and hardware complexes Atliks-VPN and Module-HSM

Atliks-VPN and Module-HSM are intended for the creation and interaction of highly secure virtual networks (VPN) based on IPSec protocol and X.509 standard using Russian cryptographic algorithms.

The Atliks-VPN and Module-HSM SHCs allow encryption, integrity and reliability of the transmitted information within the available IP networks (including the Internet).

KEY FEATURES

- The SHC hardware part is developed on the basis of a specialized platform.
- The SHC software part is made on the basis of a specially modified Linux operating system in order to increase its security against unauthorized impacts via communication channels
- The software provides for the implementation of the parties authentication, generation of communication session keys when building secure tunnels according to the IPSec protocol group using public key certificates and certificate revocation lists in the format X.509.V.3; implementation of data encryption (decryption) algorithms within the IPSec protocol group during transmission of protected IP packets and checking the integrity of the transmitted data blocks
- In terms of protection against unauthorized access, the SHC provides local and secure network (remote) administration procedure and administrator authentication; checking the integrity of the security-critical software of the complex during the initialization of work; the inability to get confidential information in an open network; audit of user actions
- In terms of protection against network attacks, the SHC provides filtering of incoming and outgoing IP-packets. The SHC provides for the possibility of unified centralized management of configurations, and also contains a Web-interface for diagnosing and managing

SPECIFICATIONS

	SHC Atliks-VPN	SHC Module-HSM
Key information entering	Russian Intellectual Card (RIC)	
The number of encryption keys	More than 1,077	
The number of subscribers in the network	5,000	1,000
The speed of the crypto tunnel	85 MB/s	10 MB/s
External interfaces	2xEthernet10 / 100TX Ethernet 100FX	2xEthernet 10/100TX Ethernet 10/100TX Ethernet 100FX
Dimensions	For 19” rack (EIA RS-310-C standard)	260x164x45 mm
Power supply	220/110 V	220/110 V
Power consumption	Up to 300 W	Up to 5 W

Swiss-M means of cryptographic protection of information

Subscriber modification

Server modification

Swiss-M is a product of cryptographic protection of information in data transmission networks. Designed to ensure the security of confidential information in IP-based networks IEEE 802.3/802.3u.

KEY FEATURES

- Encryption and prevention of false data entry for IP-packets
- Merging of each-every-one network segments
- Routing within network segment and between segments
- Hardware implementation of cryptographic algorithms
- Remote key management
- Network implementation for 5,000 subscribers:
  - simultaneous work – 50 subscribers
  - connect/disconnect of new ones – 10 subscribers per second

SPECIFICATIONS

Security class	KA 1/KB 2
Cryptographic algorithm	GOST 28147-89
Full packets encapsulation	
Encryption speed	server's CIPF - 94 MByte; subscriber's CIPF - 34 MByte
Support of traffic prioritization and marking	QoS

P220 noise generator

The P220 complex is a universal noise generator designed for the active protection of information objects by masking of transient electromagnetic pulse emanation (TEMPEST) with noise signals. Thermal noise is used as a noise source. The basic unit of the complex is the apparatus TAF07 (TAF07-1), in which the power supply and control unit TEI13 (TEI13-1) and from 2 to 10 GSH modules in various combinations are installed.

KEY FEATURES

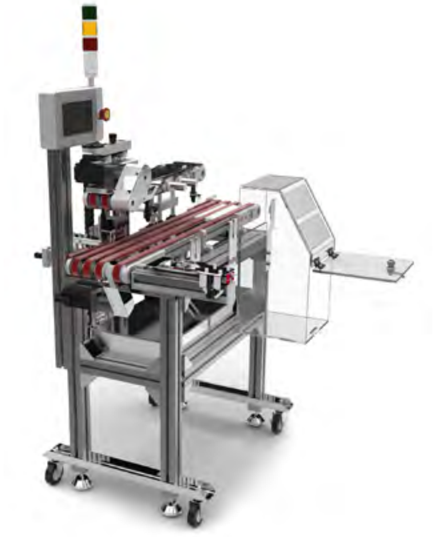
- Using thermal noise as a source of noise
- Frequency of maintenance work – once a year
- Offline control mode
- Mode of interaction with FAO06 remote control
- Automatic change of control modes
- Continuous round-the-clock work

SPECIFICATIONS

Noise output power	a) at the load (3.9 ± 0.2) ohms at the output of each channel of the TEI14, TEI 14-1 blocks not less than 1 W; b) at the load (10 ± 0.1) ohms at the output of TEI14-2 blocks not less than 0.5 W;
The possibility of replacing the Noise generator individual modules without turning off the general power supply of the device	yes
Separate smooth adjustment of the output noise signal level of each channel	yes
Power consumption of complexes (with ten single-channel NG modules, without remote control FAO 06)	- P220, P220-2 with power supply from the AC network from 187 to 242 V with a frequency of (50 ± 1) Hz not more than 90 W - P220, P220-2 with power from an external DC source from 18 to 30 V, not more than 80 W - P220-1, P220-3 with power from an external source of direct current voltage (60 ± 6) V, not more than 80 W
Overall dimensions	- apparatus TAF07 (TAF07-1) not more than 210x380x700 mm - FAO06 panel (in the frame) not more than 131x370x236 mm
Weight	- apparatus TAF07 (TAF07-1) with 10 GN modules not more than 30 kg - FAO06 console (with frame) not more than 8.5 kg

Trade

Data protection in the trade is a new direction in the Concern’s work. Among Russian retailers, products such as cash registers, fiscal memory device and other products that ensure the security of trading processes are already in demand.



Drugs labelling equipment

KEY FEATURES

- Mobile station, easily and quickly moved to any point of production
- The quality of applied codes meets international standards.
- Conducts control of printing errors, automatic rejects the invalid codes
- Upper pressure conveyor that allows you to precisely position and fix the pack
- Ability to label packages of different width and height
- Automatic scanner that does not require additional configuration when changing the size of the package

Equipment for drugs labelling – serialization station, provides a comprehensive solution for applying labelling on the secondary packaging, manages and controls the quality of printing. With this equipment you can apply barcodes, DataMatrix GS1 codes and the necessary human-readable information. The station provides digital marking of the secondary packaging by direct printing, rejects invalid packets in case the marking is incorrect or not readable.

SPECIFICATIONS

Two belts conveyor	Speed from 10 to 50 m/min. The length of the lower tape 1 m
Thermal Inkjet printer with single cartridge	Resolution 300 dpi, print height 12.7 or 25.4 mm
Automatic print control scanner	Resolution 1,280x1,024 pixels, external illumination
Pneumatic reject with receiving box	6 bar
Rejection confirmation system	Optical
Manual radio scanner for sampling	Resolution 752x480 pixels
Light and sound alarm	3 sections at the marking complex
Complex control panel	Sealed cabinet
Complex software	One license for the serialization complex

Cloud-1F cash register equipment

CRE Cloud-1F can be used in any trade organization, the service sector and work in premises, in open areas, under a canopy, when powered from an AC network with a voltage of 220 V and a frequency of 50 Hz through an adapter with output parameters 24.0V/2.0A.

CRE fulfils the requirements of 54-FZ, including the nature of the traveling trade without installing CRE directly on trains, reduces the number of serviced CRE at the places of stationary sale of tickets, goods and services, conducts online monitoring of products sold and sales management.

KEY FEATURES

- The open protocol of control over TCP/IP networks without the need to install drivers allows you to design the cashier's AWP for any operating system
- Work in automation systems, USAIS
- Work with the 1C: Enterprise software system is supported.
- Ensuring the possibility of encrypting fiscal documents in order to ensure the confidentiality of information transmitted to the operator of fiscal data
- Contains the keys of the fiscal sign, which provides the possibility of the formation of fiscal signs, the keys of recording fiscal data in unchangeable form and their non-volatile long-term storage, keys for checking fiscal signs, keys for decrypting and authenticating fiscal documents confirming the fact that the operator has received fiscal data of fiscal documents transmitted by CRE sent in CRE by the operator of fiscal data

SPECIFICATIONS

Continuous operating time	24 h/day
CRE readiness time for operating mode with self-testing	10 s
Maximum number of characters per check line	48
Print speed	50 mm/s
Life time	7 years
Passwords reserved modes	cashier, administrator 1, administrator 2, administrator 3, technical administrator
Availability of discounts/surcharges	rate not more than 99% / not more than 20%, integer
Formation of fiscal documents	check (strict security form) with the signs "Inflow", "Return of inflow", "Outflow", "Return of outflow"; correction check (strict security form) with the signs "Inflow", "Outflow"
Check tape	Thermochemical paper (ISO 9002 quality standard)
Average power consumption	20 W
Weight with adapter	1.5 kg
Overall dimensions	185x150x125 mm

AMS-300F, AMS-300.1F, AMS-700F cash register equipment

AMS-300F, AMS-300.1F, AMS-700F CRE is intended for application in the sphere of trade, and for usage in the sphere of services. The main CRE function is to account for the sales of goods and services.

KEY FEATURES

- Full functionality for the enterprises' settlement registration where the use of CRE is necessary
- Scanner, scales, teller terminal can be connected
- CRE comes with an electromechanical cash drawer
- Built-in battery (model AMS-700F)
- Full-fledged cashier's workplace, which does not require additional devices and a computer

SPECIFICATIONS

CRE interfaces:	Ethernet 10/100 Mbit. Communication with a computer, Internet, FDO, USAIS. WiFi module (optional). Communication with a computer, tablets, smartphones, Internet, FDO, USAIS. USB 2.0. Communication with a computer, connecting a barcode scanner. RS-232C. Connecting a barcode scanner, scales. Thermal printer for ribbon width of 57 mm

Fiscal memory device

(FMD)

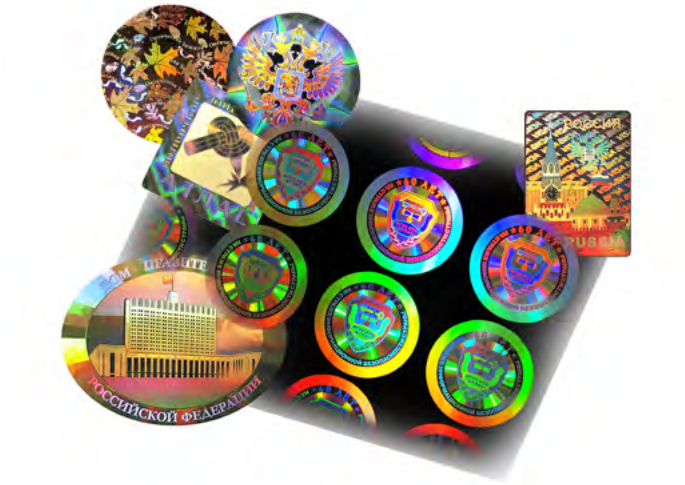
KEY FEATURES

- Encryption of fiscal data
- Accumulation of information about transactions in electronic form
- Creation and assignment of a fiscal characteristic
- Ability to work and record transactions offline with the subsequent transfer of all recorded information when a connection appears
- Supporting of the device owner electronic signature

FMD is a cryptographic module (element board), whose main function is to protect and encrypt all fiscal data, as well as accumulate the same in electronic form. The FMD is equipped with the key of the fiscal sign, has the ability to accumulate information in electronic form for its further transfer to the FDO and the FTS, which is due to changes in Federal Law No. 54 “On the use of cash register equipment”, that are reduced to the necessity of replacing the electronic control tape with FMD. This allows organizing work with both online cash registers and other types of cash registers.

SPECIFICATIONS

Non-volatile timer	yes
Interfaces of interaction with CRE	RS-232, I2C, UART
Operating temperature	from -30°C to + 40°C
Shell protection	IP30 (GOST 14254-96)
Overall dimensions	30.2x30.2x9.4 mm
Net weight	no more than 15 g



Protected holographic products

Protected holographic products are computer-synthesized holograms of ultra-high degree of security. This product is used to protect goods and documents from counterfeiting and copying, to control the authenticity of various types of products, as well as image and decorative items with a holographic picture.

KEY FEATURES

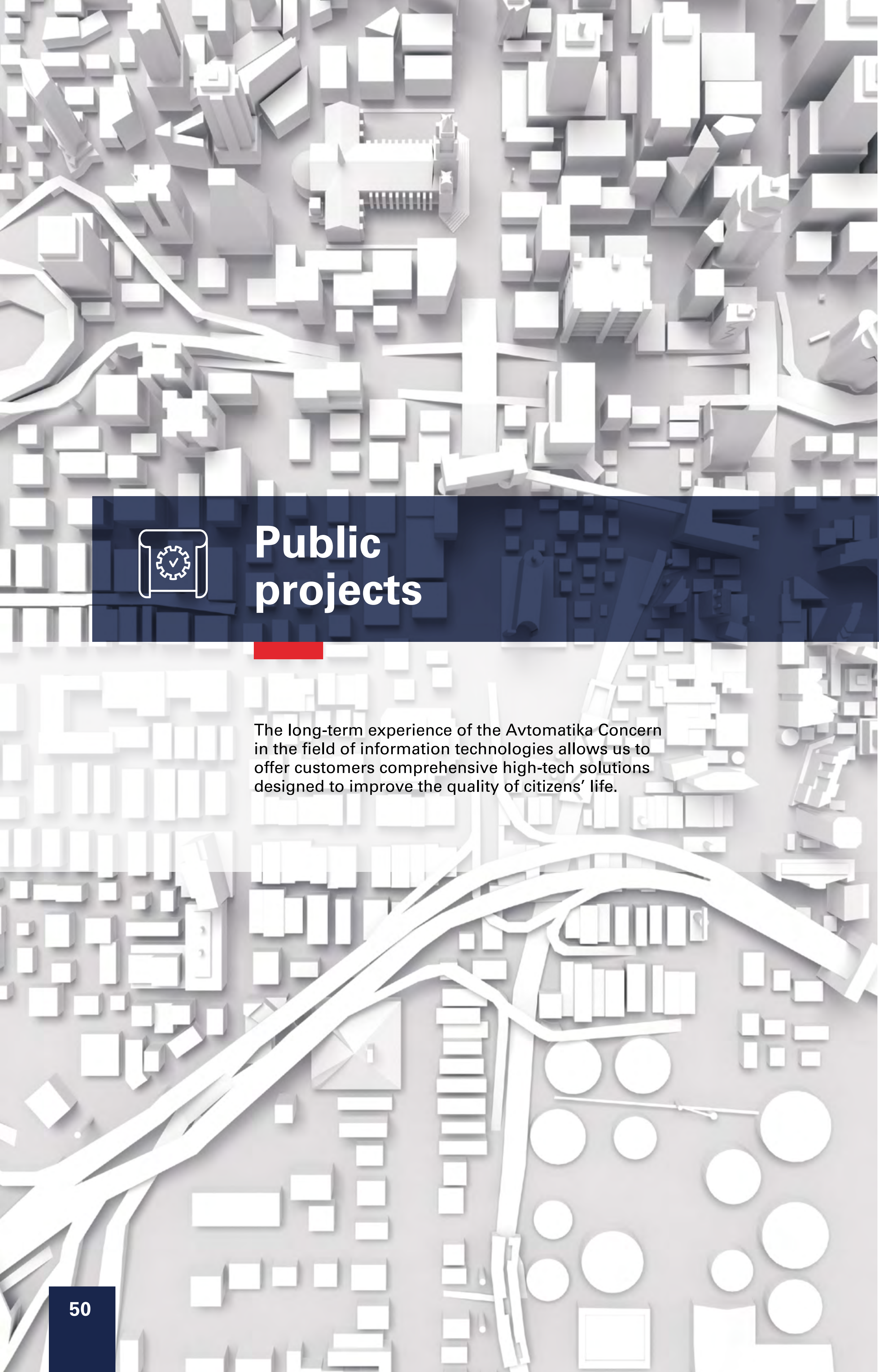
- Products are made of high-quality materials that ensure high-quality transfer of the original’s protective features and long-term use, possess various own protective features, copy-protection, self-destruction or partial destruction of information layers when attempting to separate the protective hologram from the surface of the protected product.

- The multilevel protection system of the hologram contains:

- Own unique hologram design
- Graphic elements (guilloche nets, microtexts, etc.) that cannot be repeated using traditional copying methods
- Hidden images visible when using special control devices
- Security features of the highest level of complexity with maximum recording density, distinguishable by professional diagnostic equipment
- Combination of various high-tech protective methods

SPECIFICATIONS

Product resolution	50 nm
Micro font height	less than 1 micron



Public projects

The long-term experience of the Avtomatika Concern in the field of information technologies allows us to offer customers comprehensive high-tech solutions designed to improve the quality of citizens’ life.

E-voting complex

(EVC)

EVC is designed for electronic voting without paper ballots and is used for all types of elections. The complex provides automated counting of votes, determination of voting results and drawing up a protocol of the precinct election commission on voting results. The EVC can include up to 16 touch sensing voting devices (SVD). The SVD platform is built entirely on the latest programmable 64-bit microcontrollers, thus avoiding the risks associated with the use of publicly available operating systems.

Microcontrollers are programmed at the time of device assembly, which prevents intervention in the program in the polling station.

There is the possibility of operation using a variety of external power sources (car battery, diesel generator, solar panel stand), as well as the possibility of several types of elections holding simultaneously.

KEY FEATURES

- Use of a one-time impersonal barcode key allows each voter to vote uniquely and anonymously.
- Barcode key can be a confirmation of participation in the voting, and its uniqueness guarantees the impossibility of re-voting
- Multilingual, intuitive interface is relevant for multinational states and different age groups of the population.
- Ability to display photos of candidates and emblems of political parties, output at the request of the voter, a brief reference about each candidate or political party
- There is a voter correction feature in the voting process, which eliminates the possibility of spoiled ballots
- Capacity up to 600 voters in 10 hours of voting

SPECIFICATIONS

Size	420x390x180 mm
Weight	5-6 kg
Range of operating temperatures	+5°C to +40°C
AC voltage	110-220 V
DC voltage	10.5-13.6 V
The operating time of the device on built-in batteries	up to 6 hours

Ballots Processing Complex

(BPC)

BPC is a device for automated counting of votes, the formation and printing of the final protocol. The complex is equipped with software and a special camera that detects holograms. It accepts and processes only the ballots of this particular polling station, automatically returns sheets that are not ballots, and also reads the image in the ultraviolet range. BPC is used in federal, regional and municipal elections in the Russian Federation.

KEY FEATURES

- The complex is equipped with an automatic ballots capture mechanism, a reading line, which allows real-time scanning and recognition of ballots
- The complex automatically marks invalid ballots
- The complex has the function of data transmission through a machine-readable QR-code
- The complex does not allow to draw several ballots simultaneously.
- The complex receives the initial data (ballots descriptor, protocol descriptor) and transfers the data of the final protocol on an external electronic storage medium

SPECIFICATIONS

Motherboard	own unique development based on the ARM microprocessor
Monitor	7 "diagonal, resolution 800x480 dpi, viewing angle 160 degrees, capacitive touch screen
Scan ruler	color, one-sided
Scanning ballots format	210 mm scan width, length up to 800 mm, resolution 300x200 dpi
Ballots maker	mechanical, does not require additional maintenance
External interfaces	USB 2.0-2 pc., HDMI, Ethernet
Internal power supply	capacity 1 Ah
Battery life	not less than 1 hour
Connection to a standard network	220 V
Output voltage	12 V
Overall characteristics	dimensions 60x45x16 cm, weight 6 kg
Additional features	work from the automobile accumulator, discharge program control, the automatic mode of energy saving
Range of operating temperatures	from +10°C to +45°C

Ultrasonic scanner ANGIODIN SONO-P

Ultrasonic scanner is a high-end digital ultrasonic portable system. It is used in cardiology, obstetrics, gynecology, mammology, urology, endocrinology, orthopedics, pediatrics, neurology, in transcranial studies, in the study of peripheral vessels, in the field of neurosonography, in abdominal studies, in studies of superficial organs.

KEY FEATURES

- Linear, convex, phased multi-frequency sensors from 1 to 15 MHz
- Shift sonoelastography
- Multi-angle composite image
- Multiple zoom
- Tissue doppler
- Colour mapping of pulsating blood flow Vel+X Evaluation of vascular elasticity WTrack
- Trapezoidal image for linear sensors
- Simultaneous connection of two sensors
- 3D scanning 3D/4D

SPECIFICATIONS

Display modes	B/ 2B /4B /B + M (including color anatomical) CD - color Doppler mapping PD - power doppler DPD - Directional Power Doppler TD - tissue doppler PW - pulse doppler CW - continuous wave doppler B + PW/CW - duplex B + CD/PD + PW/CW - Triplex
Scanning technologies and features	THI - tissue harmonic InvH - inverse harmonic automatic analysis of Doppler curves Vel + X - colour mapping of pulsating blood flow WTrack - vessel elasticity assessment ProView speckle noise suppression shear sonoelastography multi-view composite image panoramic scanning trapezoidal image for linear sensors image window tilt for Doppler modes HPRF – PW with high repetition rate ECG module 3D – freehand 3D scanning 4D – real-time 3D scanning

RuScan50 Ultrasonic diagnostic scanner

KEY FEATURES

- Russian production, optimum production and service time
- Accelerated guarantee and post-warranty service procedure
- Cheaper than imported counterparts
- Ability to use the latest advances in the field of three-dimensional echography
- Simple and compact system with innovative features

RuSkan50 is a high-end ultrasonic scanner with colour, energy, tissue, pulse and continuous wave doppler. The scanner conducts ultrasonic diagnostics and examinations of the human body. It is used in obstetrics, gynecology, abdominal examinations, mammology, urology, echocardiography, muscle-skeletal examinations, as well as pediatrics, neonatology, and transcranial examinations.

SPECIFICATIONS

LCD monitor	19" (40.8 cm)
Cardiopacket	optional
ECG module	optional

Scan modes	B, 2B, M, B + M, 4B;
	CFM - colour Doppler mapping;
	PD - power doppler (including 3D);
	Focused power doppler;
	PW - pulse doppler;
	HPRF - high-frequency impulse doppler;
	CW - continuous wave doppler.
	Tissue harmonic (registration of the 2nd harmonic of the echo signal, including using inverse technology);
	colour M-mode;
	Tissue Doppler - Tissue colour Doppler for assessment of myocardial contractility (optional)

Scanning technologies and features	Automatic analysis of Doppler curves; Scanning depth up to 32 cm; Steering - the ability to change the Doppler angle in CFM and PD modes; Duplex and triplex modes.

RuScan60 Ultrasonic diagnostic scanner

The RuScan 60 is a universal high/expert-class ultrasonic scanner that provides excellent quality of ultrasonic researches: LED monitor with a wide viewing angle, a touch-sensitive control panel, and the latest imaging technology and post-processing of the image. The compact design allows you to place the RuScan 60 near the patient's bed for maximum convenience.

The use of the RuScan 60 scanner in modern diagnostic centres and medical research institutes is recommended. The research area on the RuScan 60 scanner is obstetrics and gynecology, abdominal examinations and mammology, urology and echocardiography, superficial organs and vascular examinations, musculo-skeletal examinations, and nephrology, oncology and transcranial dopplerography.

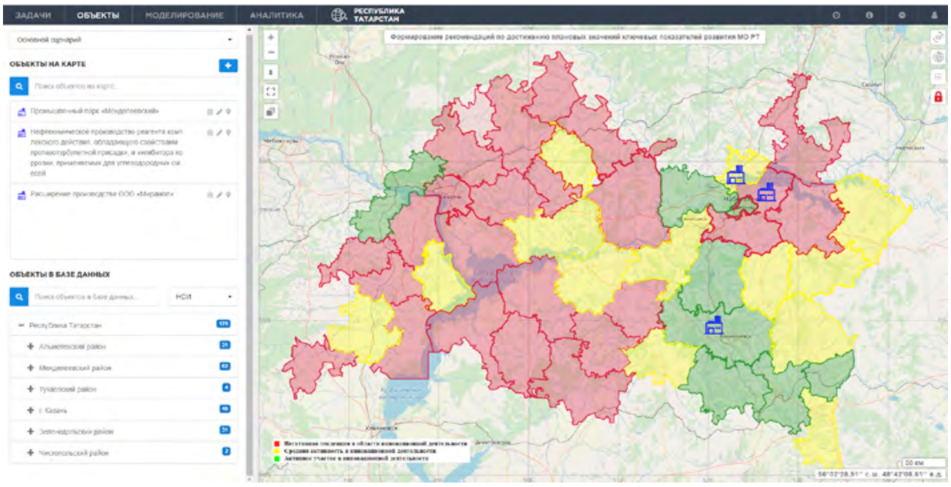
KEY FEATURES

- Russian production, optimal production and maintenance time
- Accelerated guarantee and post-warranty service procedure
- Cheaper than imported counterparts
- Ability to use the latest advances in the field of three-dimensional echography
- Simple and compact system with innovative features

SPECIFICATIONS

Widescreen LED monitor	high-resolution diode backlit monitor with wide viewing angle
Touch control panel	touch-screen
Cine memory	automatic video recording of a study fragment with the capabilities of “rewinding”, editing, performing calculations and then recording video to a file
Connectors	for simultaneous connection of up to 5 sensors (4 + 1 CW)
Built-in drive	DVD-RW
USB ports	for connecting of the peripheral devices and external disk drives
SonoView system	archiving and further viewing of static and dynamic images (image database), it is possible to copy images to DVD and USB flash drives, to take measurements in the archive

Information-analytical system of the Situation Centre of the Russian Federation constituent territory



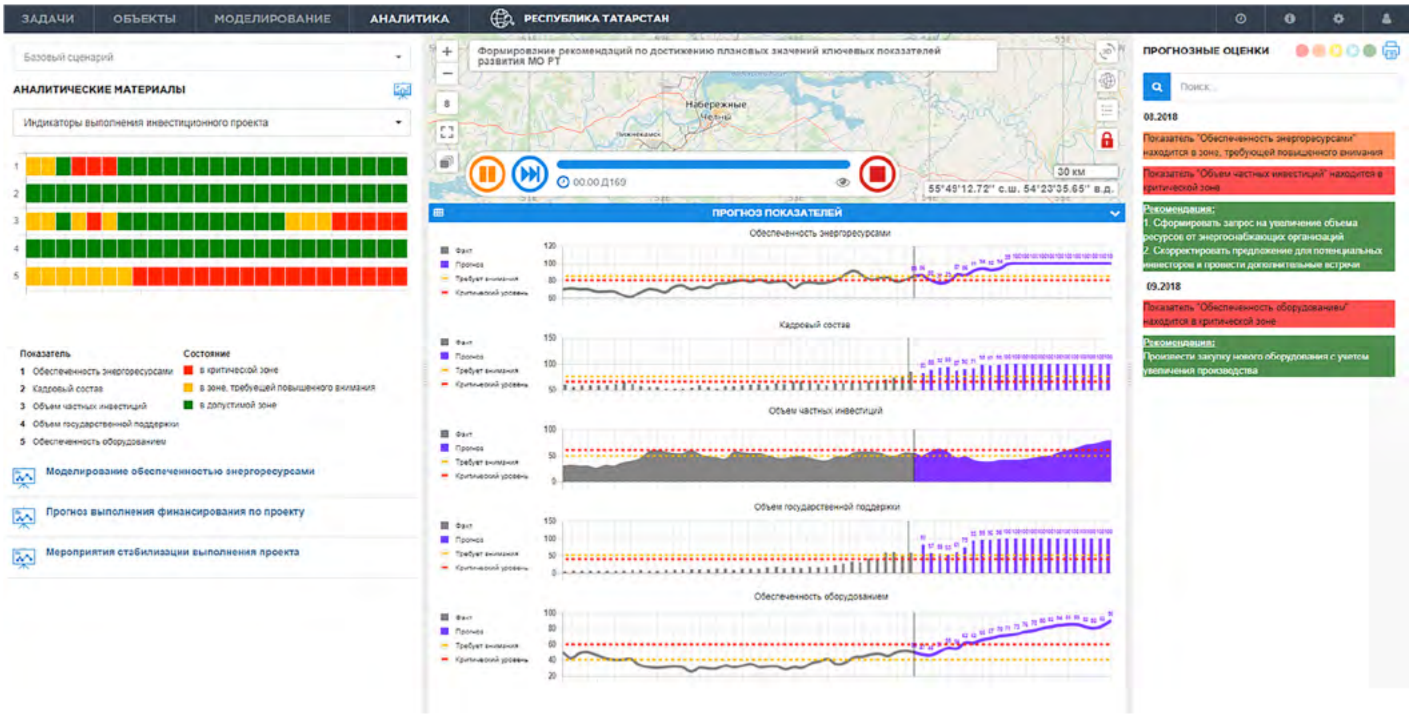
Information-analytical system of the Situation Centre of the Russian Federation constituent territory is created for the purpose of effective technological assistance of information and expert analytical support for the preparation and management of decision-making processes by the head of the Russian Federation constituent territory, heads of state authorities of the Russian Federation constituent territory, heads of local governments. The IAS contributes to the improvement of the management of the socio-economic and socio-political development of the region, ensures the integrated security of the region.

KEY FEATURES

- Monitoring and analysis of information on the implementation of decrees and orders of the President of the Russian Federation, including indicators for evaluating the performance of senior officials of the Russian Federation constituent territory
- Early detection and identification of relevant information on the Internet
- Analysis and forecasting of socio-economic development, socio-political situation, assessment of the integrated security state
- Analysis and forecasting of the feasibility of programs and projects of the Russian Federation constituent territory
- Automation of territorial development management, strategic planning and project management processes
- Solution of special tasks for automating the functions of region management in a period of danger and wartime

KEY CHARACTERISTICS

- Modelling and analysis of business processes and KPI-based management
- Ensuring coordination and interaction in case management
- More than 100 information and analytical models for analytical support for the development of management decisions drafts
- Building of an information-analytical system of a situational centre that allows combining systems to collect information from various sources and providing the ability to process information for various subsystems within a single architecture


ЗАДАЧИ
ОБЪЕКТЫ
МОДЕЛИРОВАНИЕ
АНАЛИТИКА
РЕСПУБЛИКА ТАТАРСТАН
Базовый сценарий
АНАЛИТИЧЕСКИЕ МАТЕРИАЛЫ
Индикаторы выполнения инвестиционного проекта
1
2
3
4
5
Моделирование обеспеченностью энергоресурсами
Прогноз выполнения финансирования по проекту
Мероприятия стабилизации выполнения проекта
Набережные Челны
Нижнекамск
00.00 Д169
30 км
55°49'12.72" с.ш. 54°23'35.65" в.д.
ПРОГНОЗ ПОКАЗАТЕЛЕЙ
Обеспеченность энергоресурсами
Кадровый состав
Объем частных инвестиций
Объем государственной поддержки
Обеспеченность оборудованием
Факт
Прогноз
Требует внимания
Критический уровень
120
100
80
60
150
50
0
40
20
ПРОГНОЗНЫЕ ОЦЕНКИ
Поиск

Формирование рекомендаций по достижению плановых значений ключевых показателей развития МО РТ

Показатель		Состояние
1	Обеспеченность энергоресурсами	🟥 в критической зоне
2	Кадровый состав	🟨 в зоне, требующей повышенного внимания
3	Объем частных инвестиций	🟩 в допустимой зоне
4	Объем государственной поддержки	
5	Обеспеченность оборудованием	

08.2018

Показатель "Обеспеченность энергоресурсами" находится в зоне, требующей повышенного внимания

Показатель "Объем частных инвестиций" находится в критической зоне

Рекомендация:
1. Сформировать запрос на увеличение объема ресурсов от энергоснабжающих организаций
2. Скорректировать предложение для потенциальных инвесторов и провести дополнительные встречи

09.2018

Показатель "Обеспеченность оборудованием" находится в критической зоне

Рекомендация:
Произвести закупку нового оборудования с учетом увеличения производства

APPLICATION AREA

Situation Centre of the Head of the Republic of Bashkortostan

Distributed Situation Centre of the Republic of Tatarstan

Pilot project of the SAC of the Ministry of Energy of Russia, in terms of the operational control of the fuel and energy facilities state during the period of state events of particular importance. A test of the operational situation monitoring subsystem was conducted during the presidential elections of the Russian Federation with the participation of 22 subjects of the Russian Federation and during the 2018 World Cup.

Building of a model of a unified automated geographically-distributed information system for assessing the state of radiation, chemical and biological protection in the Russian Federation constituent territory

Building of a prototype of an automated information system for assessing the implementation in the Russian Federation of strategic planning documents for the protection of the population and territories from emergency situations AIS Strategy

Automated monitoring and diagnostics system

(ANDS)

ANDS is a software complex that accomplishes the tasks of online monitoring of electrical equipment (transformers, electric motors) and maintenance on condition.

The complex generates warning and emergency signals by monitored parameters, conducts self-diagnostics of its own software and hardware, generates archives of long-term storage of diagnostic information, forms indicative reflection of the object technical condition assessment based on the analysis of the changes dynamics in monitored parameters.

KEY FEATURES

- The most modern technologies were applied in the development of ANDS: IoT, machine learning
- Supports the broadest list of industrial protocols that allows you to connect almost any equipment

System for collecting and analysing information on the technical condition of distributed infrastructure objects

(SATC VL)

SATC VL is a software complex that accomplishes the tasks of monitoring of distributed infrastructure facilities (power lines, roads, railways, pipelines, etc.) using UAVs, sensors and mobile devices.

The complex automates the work of units involved in the direct maintenance of facilities, receiving information from monitoring systems with reference to facilities and equipment. It integrates with existing corporate information systems (MRO, GIS, storage and others), maintains reference data guides for the monitoring of objects, displays information on violations related to objects and equipment on an electronic map (GIS), generates analytical reports with statistical data about identifies defects and provides summary information to management.

KEY FEATURES

- The most modern technologies were applied during the SATC VL development: IoT, BIG DATA, neural networks
- Aggregates data from various sources: UAVs, various telemetry sensors, mobile devices, etc.

Cryptobiocabina software and hardware complex

Cryptobiocabina software and hardware complex is a self-service device for citizens and is designed to provide the possibility of providing public services in the following parts:

- reception of the applicant's biometric parameters necessary for processing foreign passports of a new generation;
- issuance of new generation foreign passports, including two-factor biometric verification of the applicant's identity using the face image and finger papillary patterns recorded on the new generation foreign passport chip, as well as the activation of the new generation foreign passport chip.

CBC is a device in a single protected package with pre-installed system-wide and application software, including information security tools.

The transmission of data obtained using Cryptobiocabine HSC to the State system of passport and visa documents of a new generation is carried out through the Interdepartmental Electronic Interaction System (IEIS) in encrypted form.

The design features of Criptobiocabina HSC make it possible to expand its use, including for processing and issuing passports of a citizen of the Russian Federation and documents equivalent to it, Russian driving licenses, as well as any other documents of a new generation. In addition, it may be possible to collect additional biometric parameters of citizens for use in other informational biometric systems, including in the interests of credit and financial institutions.

KEY FEATURES

- Elimination of the possibility of registering biometric parameters that do not correspond to the person, whose data are given in the application form, for issuing a foreign passport (automatic photo recording of the fingerprinting moment using additional photographic equipment and transferring the received information to the State system of passport and visa documents of a new generation for control by State Department of Internal Affairs of Russia employees is provided)
- Prevention of substitution of biometric parameters when processing components of the registration of biometric parameters (methods of information introduction are limited by design features)
- Prevention of the possibility of issuing a foreign passport without verifying the identity of the holder (the passport chip is activated automatically after successful mandatory two-factor verification)
- Prevention of substitution, theft, reconfiguration of biometric components registration
- Prevention of the private key compromise, the leakage of biometric parameters during their transmission through communication channels, the possibility of replacing the protected information

Safe City hardware and software complex

Safe City is a comprehensive information system that provides forecasting, monitoring and warning of possible threats, as well as controls the elimination of the emergency consequences and offenses with integration under the management of actions of the information and control subsystems of various organizations (duty, dispatch, municipal services) ensuring their operational interaction in interests of the municipality.

The complex uses a unified systemic approach to ensuring of the integrated security of the public environment in the conditions of maintaining a high level of risks of man-made and natural character and the continuing trend of urbanization. Increases public safety.

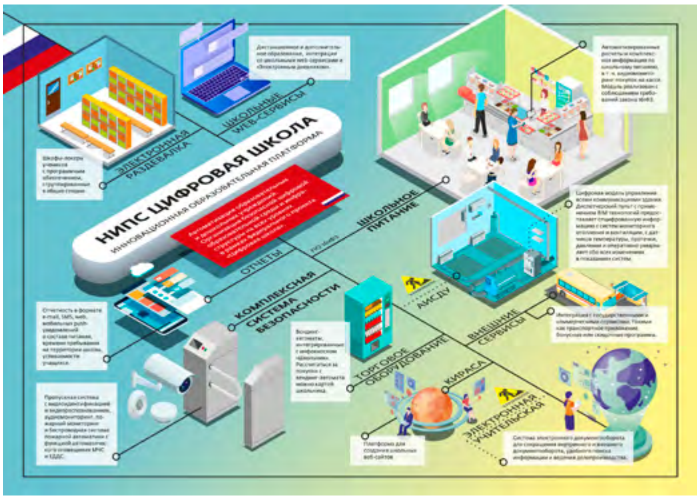
COMPLEX COMPONENTS

- Intelligent transport system:
  - Traffic management
  - Monitoring systems
  - Passenger traffic management
  - Smart parking
- Utilities:
  - Bright City
  - Smart counters / consumption analytics
  - Intelligent distribution systems
  - Ecomonitoring
- City services:
  - E-government
  - Informatization of education
  - Health informatization
  - Smart security
- Smart buildings:
  - Consumption optimization systems
  - Integrated communication systems
  - Smart lighting, AHP1
  - Automated internal parking

Digital School hardware and software complex

The complex includes a “smart” security system, electronic services and promotes digitalization of school infrastructure at all levels.

Digital School complex project can be implemented both for a separate educational institution and for the entire educational system of the region.



KEY FEATURES

The implementation of the Digital School project will allow educational institutions, including afterschool ones, to get the following benefits:

- Modern system of automated calculations and information and software complex for managing the school feeding system, which will increase the speed and quality of group meals organization
- Comprehensive security system, including access control and video identification control system at the entrance, audio monitoring, video monitoring integrated with the automated calculation system, fire monitoring with automatic signal video content transmission to the regional Emergency Directorate of the Ministry of Emergency Situations, as well as a wireless fire alarm system
- Daily informational reports in electronic form (web, E-mail, SMS, Mobile application) about the composition of the students’ meals, the time they stay on the school’s territory, and the overall performance
- Unified accounting and settlement system for additional school services (provision of access to internal information resources, such as a school portal, the Electronic Diary, school project management, and the centralization of payments collection by directions)
- Extended list of services for ID cards holders (recording of the transport application on the card, implementation of bonus or discount programs, etc.)
- Enhancing of the information security and technological independence from foreign server equipment when implementing a project based on the Russian platform Elbrus, the complex of information protection tools (CIPT) from unauthorized access is built into the core of the operating system

One of the unique features of this project is the system for settlements automating: mutual settlements, receipt of funds and payment for services is implemented in compliance with the requirements of Law 161 FZ.

PREMIS software platform

Property & Real Estate Management Information System (PREMIS) is a software platform for customized business solutions that are compatible with all major software. The platform is designed to consolidate accounting and management information in electronic form and to organize business processes related to real estate, land and intellectual property on its basis.

PREMIS

Thanks to the wide range of possibilities, PREMIS provides:

- Low costs of training for employees and customers
- Ability to quickly adapt existing design developments to the PREMIS platform
- Low cost of integration with used accounting and financial management systems

KEY FEATURES

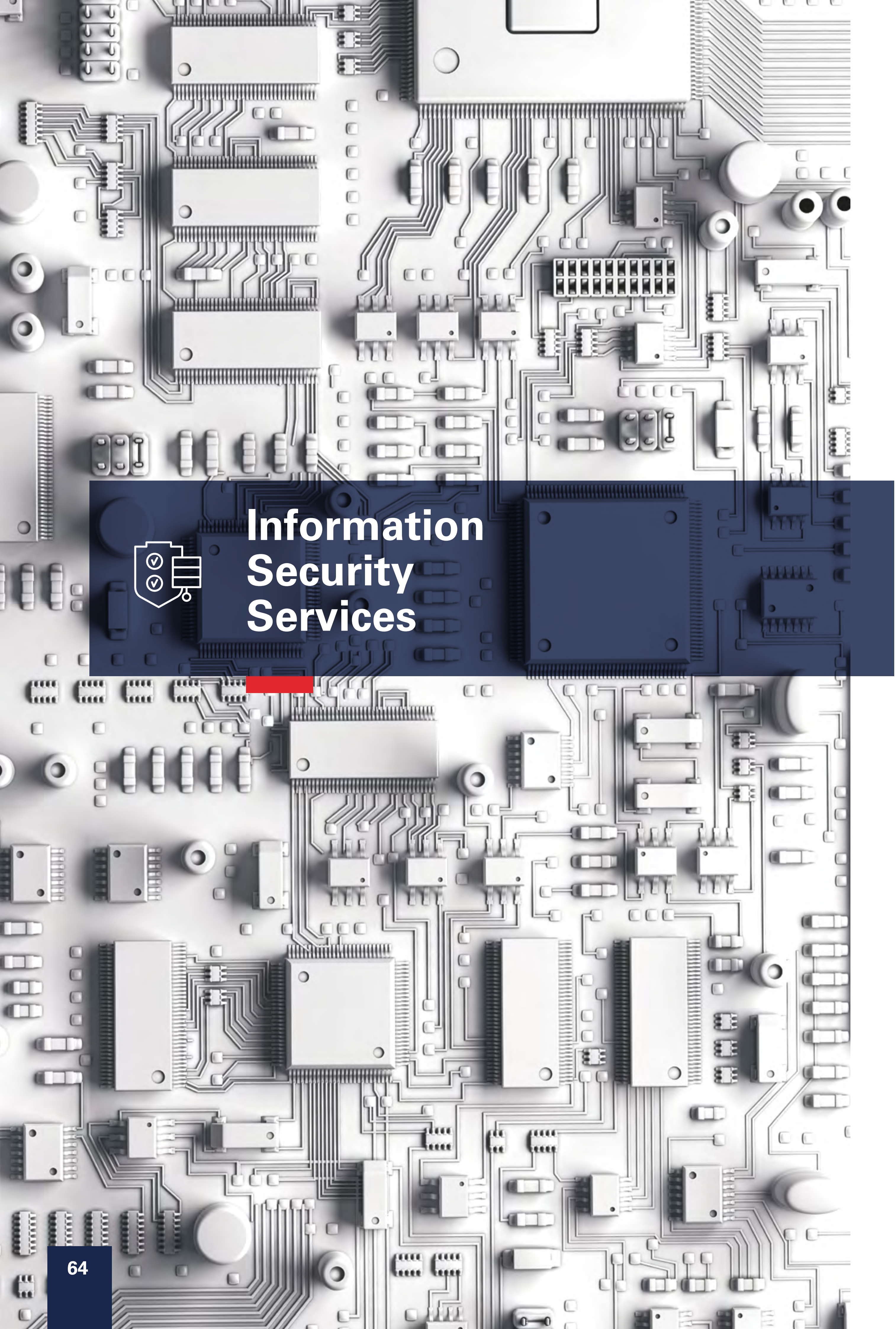
- The ability to get a ready business solution without long-term programming – from 3 working days
- Flexible architecture for building a solution that includes both platform built-in capabilities and customized solutions reflecting specific business requirements of the customer
- Data protection. The option of providing of access of different levels to any database objects. For data storage, MS SQL Server 2008–2016 R2 is used with the maximum degree of protection against failures and unauthorized access. All actions with the system database are recorded in special logs.
- Integration with other software products
- Usage of free software
- High accuracy of data in the system
- Increase of the manager productivity
- Low cost of implementation and use of the platform
- The Ministry of Communications of the Russian Federation included PREMIS in the Unified Registry of Russian Software. The platform is recommended as an analogue of import software, mandatory for use in procurement for state and municipal needs

FUNCTIONAL OPPORTUNITIES OF THE PLATFORM

- Management of reference information
- Management reporting
- CRM system
- Regulated accounting
- Centralized procurement and asset management
- Contract management
- Business analysis

ON THE BASIS OF THE PREMIS PLATFORM A LINE OF BUSINESS DECISIONS DEVELOPED, SUCCESSFULLY DECIDING THE MAIN TASKS OF THE ACCOUNTING AND MANAGEMENT ACTIVITIES OF THE HOLDING

- PREMIS: Commodity Flow Management
- PREMIS: Assets Management
- PREMIS: Product Quality Management
- PREMIS: Orders Management
- PREMIS: Development Program Management
- PREMIS: Automation of the Work of Collective Organs



Information Security Services

Certification subject to information security requirements (GIS, MIS, ISPD)

Penetration testing

Delivery, installation and configuration of information security tools

Technical support of information protection systems and tools

Special inspections of technical equipment / special inspections of premises

Special studies of technical equipment

Service in the secret unit

Categorization and formation of requirements to the protection of CII RF objects

Safety of significant objects

Construction of computer attack monitoring centres

Building of the information security management centres

Organization of secure communication channels

Participation in the development of information systems and tools, source code analysis of applications

Development of unique and porting of existing speech compression algorithms

Comprehensive cybersecurity audit

Certification of information objects processing information classified as a state secret for compliance with information security requirements

Certificates and licenses

Concern Avtomatika operates on the basis of licenses and permits of the Federal Security Service of the Russian Federation, the Federal Agency for Technical and Export Control, the Department of the Federal Security Service of Russia in Moscow and Moscow Region, the Ministry of Defence of the Russian Federation, the Federal Service for Defence Order, the Federal Space Agency, Ministry of the Russian Federation for Civil Defence, Emergencies and Disaster Relief, Ministry of Industry and Trade of the Russian Federation, Moscow City Health Department.

To implement the development, production, testing, installation, mounting, maintenance, repair, disposal and sale of weapons and military equipment.	0007587 series, No. 002479 VVT-OPR dated 30 August 2012	Validity: permanently	Licensing authority: Ministry of Industry and Trade of Russia
To perform works related to the use of information constituting a state secret.	GT 0094962 series, No. 29697 dated 16 March 2017	Validity: until 16 March 2022	Licensing authority: Department of the Federal Security Service of Russia in Moscow and Moscow Region
To create the means of protection of information containing data constituting the state secret.	GT 0104130 series, No. 16132C dated 3 August 2017	Validity: permanently	Licensing authority: Centre for licensing, certification and protection of state secrets of the Russian Federal Security Service
To implement the measures and (or) to provide the services in the field of the state secrets protection.	GT 0104131 series, No. 16133M dated 3 August 2017	Validity: until 2 August 2022	Licensing authority: Ministry of Industry and Trade of Russia
To implement the measures and (or) to provide the services in the field of the state secrets protection.	GT 0104139 series, No. 16153M dated 4 August 2017	Validity: 3 August 2022	Licensing authority: Ministry of Industry and Trade of Russia
To develop and produce confidential information security tools.	LSZ 0006356 series, No. 12397K dated 26 July 2012	Validity: permanently	Licensing authority: Centre for licensing, certification and protection of state secrets of the Russian Federal Security Service
To implement the measures and (or) to provide the services in the field of the state secrets protection.	GT 0072495 series, No. 14223M dated 15 April 2015	Validity: until 14 April 2020	Licensing authority: Centre for licensing, certification and protection of state secrets of the Russian Federal Security Service
To operate in the field of information security tools creating.	PV 301602 series, No. 1468 dated 2 May 2017	Validity: until 2 May 2022	Licensing authority: Ministry of Defence of the Russian Federation

To develop, produce, distribute, maintain encryption (cryptographic) tools, information systems and telecommunication systems that are protected using encryption (cryptographic) tools, to perform works, and provide information encryption services.	Series LSZ 0006357, No. 123984 dated 26 July 2012	Validity: permanently	Licensing authority: Centre for licensing, certification and protection of state secrets of the Russian Federal Security Service
To implement space activities.	Series 002695, No. 1603K dated 16 November 2011	Validity: permanently	Licensing authority: Federal Space Agency
To ensure technical protection of confidential information.	Series KI 0246, 012384 No. 1965 dated 5 March 2013	Validity: permanently	Licensing authority: Federal Agency for Technical and Expert Control
To implement measures and (or) to provide services in the field of state secrets protection (in terms of technical protection of information).	Series GT 0167008308, No. 3257 dated 5 August 2015	Validity: until 5 August 2020	Licensing authority: Federal Agency for Technical and Expert Control
To implement measures and (or) to provide services in the field of state secrets protection (in terms of countering foreign technical intelligence services).	GT series 0171008624, No. 933 dated 17 April 2016	Life time: 17 April 2021	Licensing authority: Federal Agency for Technical and Expert Control
To perform works related to the creation of information security tools.	Series GT 0167, No. 3258 dated 5 August 2015	Life time: until 5 August 2020	Licensing authority: Federal Agency for Technical and Expert Control
The right to carry out activities and (or) to provide services in the field of state secrets protection.	Series GT 0103326, No. 31865 dated 12 July 2018	Validity: until 16 March 2020	Licensing authority: Department of the Federal Security Service of Russia in Moscow and Moscow Region

Content

Enterprises managed by Concern Avtomatika JSC

MOSCOW

Concern Avtomatika JSC
25 Botanicheskaya ul., Moscow
+7 (495) 250-33-33, mail@ao-avtomatika.ru

FSUE NTC Atlas
38 Obraztsova ul., Moscow,
+7 (495) 689-41-42, atlas@stcnet.ru

National Technologies LLC
15c 16, Rochdelskaya ul., room 1 p. 1, Moscow,
+7 (495) 122-24-66, info@q-pol.ru

Bulat LLC
26 Ryabinova ul., Moscow
+7 (495) 419-13-90, info@opk-bulat.ru

RGT LLC
34, Ochakovskoe shosse, BC West Park, 3rd floor,
office 305, Moscow,
+7 (499) 682-64-71, info@relgeotech.ru

MTU Altair OJSC
2 Volgogradsky prospekt, Moscow
+7 (495) 674-92-85, info@mtualtair.ru

NCI LLC
38s1, Berezhkovskaya nab., Moscow,
+7 (495) 139-68-80, hotline@ncinform.ru

I.S. Brooke INEUM PJSC
24 Vavilova ul., Moscow
+7 (499) 135 33 21, ineum@ineum.ru

ST. PETERSBURG

NPP Signal JSC
4, Knipovich ul., St. Petersburg
+7 (812) 412-22-33, inbox@signal-spb.ru

NII Scale JSC
5 Kantemirovskaya ul., lit. A, St. Petersburg
+7 (812) 309-03-21, +7 (812) 295-51-65
info@mashtab.org

KALUGA

Kalugapribor JSC
249 Moscovskaya ul., Kaluga
+7 (4842) 507-714, kp@kalugapribor.ru

KEMZ JSC
121 Saltykov-Shchedrin ul., Kaluga
+7 (4842) 763-700 ext. 2210,
kemz@kaluga.ru

PENZA

PO Elektropribor JSC
69/1 Pobedy pr., Penza
+7 (800) 200-47-88, 118@electropribor-penza.ru

PNIEI JSC
9 Sovetskaya ul., Penza
+7 (8412) 59-33-35, info@pniei.penza.ru

NOVOSIBIRSK

NIPS PJSC
6/1 Akademika Lavrentieva pr., Novosibirsk
+7 (383) 3478302, nips@nips.ru

Branch of FSUE Research
and development centre Atlas
5 Frunze ul., of. 303, Novosibirsk
+7 (383) 211-92-76, ac@atlas-nsk.ru

SMOLENSK

SZR OJSC
7 Babushkina ul., Smolensk
+7 (4812) 29-91-25, szr@tumblers.ru

UFA

BPO Progress JSC
34 Kirovogradskaya ul., Ufa
+7 (347) 272-64-01, info@progressufa.ru

VORONEZH

VNII Vega JSC
7-B Moscow pr., Voronezh,
+7 (473) 262-27-03, vega@vniivega.ru

SAMARA

SIP RS JSC
26 Kirov pr., 3 floor, Samara,
+7 (846) 203-23-14, info@siprs.ru