Information
Security
Association

Our aim is to create productive environment to satisfy all the needs of citizens, business and local authorities in information security products and technologies.

Chairman of council
G.V. Emelyanov
Corresponding member of the Cryptographic Academy of Russia,
Corresponding member of Russian Engineering Academy

-       **Interregional public organization "Information Security Association" (ISA) was established in 2002 following the decision of the Federal Agency for Government Communication & Information and the State Technical Commission of Russia.**

-       **ISA actively cooperates with:**

- **the Device of the Security Council of the Russian Federation,**
- **FSB of Russia,**
- **Federal service of technical and export control (FSTEC),**
- **Federal agency of information technologies (FAIT),**
- **other ministries and departments,**
- **other financial and economic structures.**

-       **Articles of the Information Security Association (ISA) allow:**

- **to carry out the international projects,**
- **to be a member of different international public associations,**
- **to carry out foreign trade activities.**

3

ISA is licensed by the FSB of Russia and the State Technical Commission of Russia for the activities at the information security market. The license gives rights:

- **to provide information security services, in particular the security over the sensitive confidential data**
- **To carry out research and developing projects relevant to information security products.**
- **to carry out projects that involve using the state secret data;**
- **To research, develop & market cryptographic products**
- **To provide after-sales technical support**

ISA is ready to assist with the development of business contacts that may lead to:

- quicker marketability of the products;
- setting up joint ventures;
- the organization of seminars, conferences and exhibitions;
- training of IT specialists.

The enterprises making up the ISA give the full spectrum of services in design and support of integrated complex information security systems.

- Integral magazine
- IDS-Technology
- Aladdin Software Security R.D
- DialagueSience
- Jet Infosystems
- Inelt
- ComFax
- Swemel
- Moscow Department of Penza Research Electrotechnical Institute (MD PREI)
- Scientific-and-production enterprise "Information Safety System Technologies"
- Special Computer-aided Design Bureau (OKB SAPR)
- Orbita
- RNT
- Saint Petersburg Regional Center for Protection of Information (SPRCPI ZAO)
- SecurIT
- Certificate Authority
- Kami
- Eureca
- Andek
- Infotecs
- Optima
- Elvis-plus

- Ancud
- Validata
- SPURT ltd
- Infocript
- CryptoPro
- Computerization means and systems testing laboratory Ltd (LISSI Co. Ltd)
- Mezhdunarodnaya kniga - security papers (MK-SP)
- Systematic
- Stel Computer Sestems
- Scientific and Training Center of Information Security of Privolzhskky Federal District
- Kalugapribor
- Concern Systemprom
- Automatiki NII GUP
- Quant R&D Institute
- Gamma
- "Scientific-Technical Center "Atlas" Nizhni Novgorod Branch
- "Scientific-Technical Center "Atlas" Penza Branch
- "Scientific-Technical Center "Atlas" St. Petersburg Branch
- Penza Research Electrotechnical Institute (PREI)
- Central research institute of black metallurgy by P. Bardin (MAC RF "TsSRI Chermet")
- Abitel

The main activities of the ISA are determined by the services that the organizations comprising the ISA are able to provide:

- Complex protection of information resources of corporate systems
- Application of cryptographic tools
- Information protection against outflow via technical channels
- Delivery of complex systems and tools of information security
- Delivery of protected technical tools
- Independent audit of information security of information objects
- Carrying out of researches and developments
- Management of export deliveries
- A professional training

7

Complex information security of corporate systems resources.

The creation of complex systems of information security of local computer networks, the corporate automated systems constructed on the basis of general purpose networks, including the Internet, includes:

- A predesign stage / planning (audit of information-communication systems regarding information security, analysis of the initial data, preparation of offers to the customer);
- Designing of the complex information security systems;
- Implementation of complex information security system (delivery, installation of technical tools, training of the stuff);
- Application of cryptographic tools;
- Writing up procedures manuals, preparation for certification for the information security requirements;
- Pre-certification testing of corporate systems to ensure they comply with information security requirements;
- Guarantee and warranty service
- Outsourcing of the information corporate security systems

Results: The creation of protected automated systems including management of complex information security system

Application of cryptographic tools

The wide spectrum of cryptographic tools developed by the enterprises of ISA is used to create complex information security systems. These tools are:

- information security of data transmission
- information security in local (corporate) computer networks, including networks with outputs into the general network
- protected storage of the information databases, magnetic disks, etc.
- security of the information flows in their transfers between network users, remote access to the databases, etc.
- identification and authentication of users for the differentiation of access (including using of electronic tools with a key information - e-token, touch memory, smarts - cards)
- information security against a falsification of electronic documents due to use of the electronic digital signatures and cryptography with an open key (PKI).

Information protection against outflow via technical channels

- specialist audit and specialist hardware tools research which allow to detect if any unauthorized electronic tools were introduced into the communication channels and to define dangerous zones of information interception using the channel CERI (collateral electromagnetic radiations and inducings);
- information security of premises that are allocated for the confidential use
- delivery & installation of the information security systems to block the outflow of sensitive date using a channel CERI (collateral electromagnetic radiations and inducings), power and grounding (generators of noise, filters, etc.) networks
- information security of telephone sets using an installation of devices that block an unauthorized insertion of microphones into telephones (in case using a digital automatic telephone exchanges)
- information security of telephone sets using the channel of electro-acoustic transformations and high-frequency imposing.

Delivery of complex information security systems and tools

- information security tools against the unauthorized access (hardware, software tools)
- development & management of information security policies that allow monitoring and control of the users of the **automated systems**
- information gathering about applications of the system
- detection & provision of prompt solutions to the events compromise the information security policy set on users' workstations
- intrusions detection systems that provide an automatic detection and blockage of network attacks both external and internal
- analysis of the security of the systems that allows the discovery and repairs of weaknesses of the automated systems
- various implementation of protected e-mail boxes
- protected access points to the Internet
  for the corporate automated systems

Delivery of protected computer equipment

The Association carries out a delivery of tools that are EMI-proof according to customers' technique requirements for processing of information of any secrecy level. These tools can be used at any objects of informatization without any further testing.

Independent information security audit of object of informatization

- **overall audit of information / communication systems using expert and tool methods**
- **assessment of overall efficiency of security systems and tools**
- **audit report comprising:**
- **the analysis of network and information resources security,**
- **estimations of system vulnerability,**
- **recommendations for the perfection of information security system.**

Carrying out of researches and developments

The research and development works will be carried out at the ISA or ISA partners' test basises and scientific laboratories.

Management of export deliveries

Management of export deliveries of information security tools will be carried out in accordance with the current legislation. During the export contracts the Association will take the responsibility to organize all necessary examinations and compliances with the Russian authorities.

Professional training

- **Degree level courses**
- **Training courses for qualified staff to allow continued professional development**
- **Seminars on specific topic areas**

Welcome to cooperation

Information

Security

Association

Kvant, ISA
15, 4-th Lihachevskij lane
Moscow 125438
Russia
tel/fax: +7 (095) 156-7102
tel. +7 (095) 154-6155, 782-3357,
http://www.azi.ru, e-mail: azi@azi.ru