

General

Search this site

КОНТАКТНЫЕ ТЕЛЕФОНЫ





TSLSZ FSB Russia organizes GIS certification and accreditation of testing laboratories.

Organization accredited as a testing laboratory in certification of the FSB of Russia:

- 1. certification system for cryptographic protection of information (ROSS RU.0001.030001).
- 2. <u>certification system for information security requirements for the safety of information constituting a state secret (ROSS RU.0003.01BI00).</u>

On GIS certification and accreditation can get advice over the phone: 8 (499) 140-41-17.

Web-reception



If you have questions about our service, please use this service

Helpline: (495) 224-2222, (495) 914-43-69 (round the clock)

E-mail: fsb@fsb.ru

Mailing address: Moscow. 107031, st. Bolshaya Lubyanka home third

© 2009. © Center for licensing, certification

and the Protection of State Secrets Russia. 1999 - 2009 r.



TERNEWEL

organizations accredited in the certification of the cryptographic protection of information POCC RU.0001.030001 as test laboratories for the certification tests (as of May 1. 0 4 .201 3)

Name and address Organization	Registration number certificate of accreditation, its validity	Area Accreditation
The Federal State Unitary Enterprise "Scientific and Technical Center" Basis " Federal Security Service of the Russian Federation " 248009, g Kaluga, Grabtsevskoe highway, 31	AF-080 29.09.2008 29.09.2013	Name of tested product 1. Hardware and hardware-software encryption tools designed to provide cryptographic protection of information during its storage and transmission over communication channels. 2. Hardware and hardware-software encryption tools designed to protect against unauthorized access to information during processing and storage. 3. Hardware and hardware-software encryption tools designed to protect against spoofing, including simulation protection means. 4. Encrypted communication equipment. 5. Information and telecommunication systems of the state authorities of the Russian Federation in which the protection of information is carried out—the use of the protected equipment and organizational measures without the use of methods of cryptographic transformations. 5. Information and telecommunication systems of the state authorities of the Russian Federation, which protects the information from the—the use of encryption (cryptographic) means. 7. Passive and active technical protection of information for use in information and telecommunication systems. NAME OF TESTS 1. Engineering and cryptographic research products at pp 1, 2, 3. 2. Special studies on the production pp 1, 2, 3, 4, 5, 6, 7. 3. Studies linear signal pp 1, 2, 3, 6. 4. Accessibility of the products according to claim 4. 5. Special engineer the product of claim 7.

Military Unit 54939	AF-082	Name of tested product Encrypted communication equipment.
g Moscow	01.12.2008 01.12.2013	NAME OF TESTS Special works.

			Name of tested product
CI	Closed		1. Hardware, software, and hardware and software encryption tools designed to provide cryptographic
			protection of information during its storage and transmission over communication channels.
	int-Stock		2. Hardware, software, and hardware and software encryption tools designed to protect against
	ompany		unauthorized access to information during processing and storage.
"0	t. Petersburg	AF-084 13.10.2008	3. Hardware, software, and hardware and software encryption tools designed to protect against
	gional center		spoofing, including simulation protection means.
	information		4. Hardware, software, and hardware and software digital signature.
security"	13.10.2003	5. Encrypted communication equipment.	
		6. Information and telecommunication systems of the state authorities of the Russian Federation in	
19	195220,		which the protection of information is carried out the use of the protected equipment and
St. Petersburg, ul. Obrucheva, 1		organizational measures without the use of methods of cryptographic transformations.	
		7. Information and telecommunication systems of the state authorities of the Russian Federation,	
			which protects the information from the the use of encryption (cryptographic) means.

Passive and active technical protection of information for use in and NFORMATION and telecommunication systems. Equipment institutional digital automatic telephone exchanges for use in government of the Russian Federation; specialized monitoring tools (blocking) control signals transmitted over interoffice trunks. 10. Firewalls. 11. Software and hardware-software systems that implement the functions of the certification center. 12. Software and NFORMATION and telecommunication systems, interacting with certified cryptographic protection of information. 13. Software designed for use in and NFORMATION and telecommunication systems authorities of the Russian Federation. 14. The hardware and software modules trusted boot the PC. NAME OF TESTS 1. Cryptographic research products at pp 1, 2, 3, 4, 10, 14. 2. Engineering and cryptographic research products at pp 1, 2, 3, 4, 10, 14. 3. Special studies on the production pp 1, 2, 3, 4, 6, 7, 8, 10, 14. 4. Studies linear signal output by pp 1, 2, 3, 4, 6, 10, 14. 5. Accessibility of the products of claim 5. 6. Special engineering analysis products at pp 5, 6, 7, 8, 9.13. 7. Studies of hardware and software product of claim 9 for compliance with information security 8. Studies of the functional properties of the product according to claims 6, 7, 10-14 for compliance with information security requirements. Name of tested product

		Of cash registers with specially developed and applied only in its structure by means of cryptographic protection of fiscal data, including protected electronic control tape.
Limited Liability Company "NTC Alpha Project" 127473, Str. Seleznevskaya, 15, page 1	AF-090 20.03.2009 20.03.2014	NAME OF TESTS 1. Test of the check-out equipment with built-in electronic control tape to secure compliance "with technical requirements to control cash machines on the part of the electronic control tape protected." 2. Checking the operation of the electronic control tape secure in the check-out equipment for compliance with the specification protected electronic control tape. 3. To verify compliance with maintenance work on protected electronic control tape consisting of cash registers in the technical documentation of cash registers, the current regulations on protected electronic control tape. 4. Test of the check-out equipment with built-in cryptographic fiscal data for compliance with cash control technique in terms of incorrigibility fiscal data. 5. To verify compliance with maintenance work on means of cryptographic protection of data in the fiscal cash register equipment listed in the technical documentation of cash registers, regulations on the use of cryptographic protection.

Name of tested product 1. Hardware, software, and hardware and software encryption tools designed to provide cryptographic protection of information during its storage and transmission over communication channels. 2. Hardware, software, and hardware and software encryption tools designed to protect against unauthorized access to information during processing and storage. The Federal 3. Hardware, software, and hardware and software encryption tools designed to protect against State Unitary spoofing, including simulation protection means. Enterprise 4. Hardware, software, and hardware and software digital signature. AF-091 5. Encrypted communication equipment. "Kalugapribor" Information and telecommunication systems of the state authorities of the Russian Federation in 01.06.2009 which data protection is provided by the protected equipment and organizational measures without the 248017, Moscow 01.06.2014 use of cryptographic methods of conversion. Kaluga, ul. 7. Information and telecommunication systems of the state authorities of the Russian Federation, Moskovskaya which protects the information using encryption (cryptographic) means. 249 8. Passive and active technical protection of information for use in information and telecommunication systems. Equipment institutional digital automatic telephone exchanges, intended for the treatment of information that does not contain information constituting a state secret, and use in the bodies of state

power of the Russian Federation; specialized monitoring tools (blocking) control signals transmitted over interoffice trunks.
NAME OF TESTS
1. Special studies on the production pp 1, 2, 3, 4, 6, 7, 8.
2. Studies linear signal output by pp 1, 2, 3, 4, 6.
3. Accessibility of the products of claim 5.
4. Special engineering analysis products at pp 5, 6, 7, 8, 9.
5. Studies of hardware and software product of claim 9 for compliance with information security
requirements.

Public corporation "All-Russian Scientific Research Institute of Automation	AF-098	Name of tested product 1. Firewalls. 2. Software and hardware-software systems that implement the functions of the certification center. 3. Software and NFORMATION and telecommunication systems, interacting with certified encryption (cryptographic) means. 4. Software designed for use in and NFORMATION and telecommunication systems authorities of the
management in non-industrial field name V.V.Solomatina " 117638, Str. Sivashskaya, etc. 4, Bldg. 2	06.11.2009 11/06/2014	Russian Federation. NAME OF TESTS Studies of the functional properties of the products for compliance with information security requirements.
Institution of the Russian Academy of Sciences Institute of Informatics Problems of the Russian	AF-099 18.01.2010 18.01.2013	Name of tested product 1. Software and hardware-software systems that implement the functions of the certification center. 2. Software and NFORMATION and telecommunication systems, interacting with certified encryption (cryptographic) means. 3. Software designed for use in and NFORMATION and telecommunication systems authorities of the Russian Federation.

Institute of Informatics Problems of the Russian Academy of Sciences 119333, Str. Vavilov, etc. 44, Bldg. 2	AF-099 18.01.2010 18.01.2013 (Under extension)	 Software and NFORMATION and telecommunication systems, interacting with certified encryption (cryptographic) means. Software designed for use in and NFORMATION and telecommunication systems authorities of the Russian Federation. NAME OF TESTS Studies of the functional properties of the products for compliance with information security requirements.
		Name of tested product
Closed Joint-Stock Company "RNT" 129515, g Moscow, Ostankino Street 2 nd, etc. 6	AF-100 22.06.2009 06/22/2014	 Hardware, software, and hardware and software encryption tools designed to provide cryptographic protection of information when it is transmitted over the communication channels. Hardware, software, and hardware and software encryption tools designed to protect against unauthorized access to information during processing and storage. Hardware, software and hardware and software encryption tools designed to protect against spoofing, including simulation protection means. Hardware, software, and hardware and software digital signature. Encrypted communication equipment. Information and telecommunication systems of the state authorities of the Russian Federation in which data protection is provided by the protected equipment and organizational measures without the use of cryptographic methods of conversion. Information and telecommunication systems of the state authorities of the Russian Federation, which protects the information from the the use of encryption (cryptographic) means. Passive and active technical protection of information for use in information and

		 Software information and telecommunication systems, which cooperates with certified cryptographic protection of information. Software designed for use in information and telecommunication systems, organs of state power of the Russian Federation. The hardware and software modules trusted boot the PC. NAME OF TESTS Special studies on the production pp 1-9, 14. Special work with the production of Claim 5. Special engineering analysis products at pp 5, 6, 7, 8, 12, 13. Studies of the functional properties of the product according to claims 6, 7, 9-14, for compliance with information security requirements.
Limited Liability Company "M-STANDARD holding" 105318, Moscow, ul. Scherbakovskaya, 53, building 4	AF-101 26.03.2010 26.03.2013 (Under extension)	Name of tested product 1. Information and telecommunication systems of the state authorities of the Russian Federation in which data protection is provided by the protected equipment and organizational measures without the use of cryptographic methods of conversion. 2. Information and telecommunication systems of the state authorities of the Russian Federation, which protects the information using encryption (cryptographic) means. 3. Equipment institutional digital automatic telephone exchanges and specialized monitoring tools (blocking) control signals transmitted over interoffice trunks for use in government of the Russian Federation in the processing of information not subject to protection under the laws of the Russian Federation. 4. Firewalls. 5. Software and NFORMATION and telecommunication systems, interacting with certified encryption (cryptographic) means. 6. Software designed for use in information and telecommunication systems, organs of state power of the Russian Federation. NAME OF TESTS 1. Special engineering analysis products at pp 1 and 2. 2. Studies of hardware and software product of claim 3 for compliance with information security requirements. 3. Studies of the functional properties of the product according to claims 4 - 6 for compliance with information security requirements. SPECIAL CONDITIONS The validity of this certificate of accreditation also extends to the branch of the Limited Liability Company "M - STANDARD holding" in St. Petersburg 197376, St. Petersburg, river embankment Karpovki house 5, the housing 22.
Closed Joint-Stock Company "TELROS" 194156, St. Petersburg	AF-102 01.05.2010 01.05.2013	Name of tested product 1. Hardware, software, and hardware and software encryption tools designed to provide cryptographic protection of information when it is transmitted over the communication channels. 2. Hardware, software, and hardware and software encryption tools designed to protect against unauthorized access to information during processing and storage. 3. Hardware, software, and hardware and software encryption tools designed to protect against spoofing, including simulation protection means. 4. Hardware, software, and hardware and software of the electronic signature. 5. Encrypted communication equipment. 6. Information and telecommunication systems of the state authorities of the Russian Federation in which data protection is provided by the protected equipment and organizational measures without the use of cryptographic methods of conversion. 7. Information and telecommunication systems of the state authorities of the Russian Federation, which protects the information from the the use of encryption (cryptographic) means. 8. Passive and active technical protection of information for use in information and telecommunication systems.

telecommunication systems.

10. Systems for detection of computer attacks.

11. Software and hardware-software systems that implement the functions of the certification center.

9. Firewalls.

Petersburg,

Bolshoy Prospect St. Sampson, House 87, letter

A

01.05.2013

8. Passive and active technical protection of information for use in information and telecommunication systems.

9. Equipment institutional digital automatic telephone exchanges and specialized monitoring tools (blocking) control signals transmitted over interoffice trunks for use in government of the Russian Federation for Information Processing, not to be protected in accordance with the laws of the Russian Federation.

10. Firewalls.

11. Systems for detection of computer attacks.

12. Software information and telecommunication systems, which cooperates with certified encryption (cryptographic) means.

13. Software designed for use in information and telecommunication systems, organs of state power of the Russian Federation.

14. The hardware and software modules trusted boot the PC.

15. Of cash registers with specially developed and applied only in its structure by means of cryptographic protection of fiscal data, including protected electronic control tape.

 NAME OF TESTS
NAME OF TESTS 1. Engineering and cryptographic research products at np 1 2 3 4 10 14
2. Special studies on the production pp 1, 2, 3, 4, 6, 7, 8, 10, 14.
3. Studies linear signal output by pp 1, 2, 3, 4, 14.
4. Accessibility of the products according to claim 3
1. Engineering and cryptographic research products at pp 1, 2, 3, 4, 10, 14. 2. Special studies on the production pp 1, 2, 3, 4, 6, 7, 8, 10, 14. 3. Studies linear signal output by pp 1, 2, 3, 4, 14. 4. Accessibility of the products according to claim 5 5. Special engineering analysis products at pp 6, 7, 8, 12, 13. 6. Studies of hardware and software product of claim 9 for compliance with information security
requirements. 7. Studies of the functional properties of the product according to claims 10-13 for compliance
Informationnov security
8. Test of the check-out equipment with built-in electronic control tape to secure compliance "with technical requirements to control cash machines on the part of the electronic control tape protected." 9. Checking the operation of the electronic control tape secure in the check-out equipment for compliance with the specification protected electronic control tape. 10. To verify compliance with maintenance work on protected electronic control tape consisting of cash registers in the technical documentation of cash registers, the current regulations on protected
19 Checking the operation of the electronic control tage secure in the check-out equipment for
compliance with the specification protected electronic control tape.
10. To verify compliance with maintenance work on protected electronic control tape consisting of each registers in the technical documentation of each registers; the current regulations on protected
11. Test of the check-out equipment with built-in cryptographic fiscal data for compliance with cash control technique in terms of incorrigibility fiscal data. 12. To verify compliance with maintenance work on means of cryptographic protection of data in the fiscal cash register equipment listed in the technical documentation of cash registers, regulations on the
12. To verify compliance with maintenance work on means of cryptographic protection of data in the
fiscal cash register equipment listed in the technical documentation of cash registers, regulations on the
SPECIAL CONDITIONS
Studies of the functional properties of the product according to claims 10 and 11 are limited to
Studies of the functional properties of the product according to claims 10 and 11 are limited to conducting research of telecommunication equipment of digital telephone service that implements the functions of firewall and detection of computer attacks, for compliance with information security
requirements.

		Name of tested product
Clara I		1. Software systems that implement the functions of the certification center.
Closed		2. Software information and telecommunication systems, interacting with certified encryption
Joint-Stock	AE 104	(cryptographic) means.
Company	AF-104	3. Software designed for use in information and telecommunication systems, organs of state power of
"C:1 COM"	05.07.2010	the Russian Federation.
"Signal-COM"	05.07.2010	NAME OF TESTS
125315,	05.07.2013	Studies of the functional properties of the products for compliance with information security
Moscow, ul.		requirements.
Usievicha, 19		1
Usieviciia, 19		SPECIAL CONDITIONS
		The validity of this certificate of accreditation applies only to the research of information security that
		does not contain information constituting a state secret.

		Name of tested product
		1. Hardware, software, and hardware and software encryption tools designed to provide cryptographic
		protection of information when it is transmitted over the communication channels.
		2. Hardware, software, and hardware and software encryption tools designed to protect against
		unauthorized access to information during processing and storage.
		3. Hardware, software, and hardware and software encryption tools designed to protect against
		spoofing, including simulation protection means.
		4. Hardware, software, and hardware and software digital signature.
Limited Liability		5. Information and telecommunication systems of the state authorities of the Russian Federation in
Company		which data protection is provided by the protected equipment and organizational measures without the
		use of cryptographic methods of conversion.
scientific and	AF-108	6. Information and telecommunication systems of the state authorities of the Russian Federation,
technical		which protects the information from the the use of encryption (cryptographic) means.
enterprise	22.11.2010	7. Firewalls.
"Kriptosoft"	22/11/2013	8. Systems for detection of computer attacks.
		9. Software and hardware-software systems that implement the functions of the certification center.
440026, Penza		10. Software information and telecommunication systems, which cooperates with certified encryption
city. Lermontov,		(cryptographic) means.
3		11. Software designed for use in information and telecommunication systems, organs of state power of
		the Russian Federation.
		12. The hardware and software modules trusted boot the PC.
		NAME OF TESTS
		1. Cryptographic research products at pp 1, 2, 3, 4, 7, 12.

2. Engineering and cryptographic research products at pp 1, 2, 3, 4, 7, 12.

3. Special engineering analysis products at pp 5, 6, 10, 11.

	4. Studies of the functional properties of the product according to claims 7-12 for compliance with information security requirements.
	SPECIAL CONDITIONS Cryptographic research products at pp 1, 2, 3, 4, 7, 12, could only be carried out in support of the engineering and cryptographic hardware cryptographic research and studies of the qualities of cryptographic key structures, project development time tactical and technical requirements for key pads, calculating allowable signal / noise ratio for cryptographically danger signals during a specialized organization of special investigations.
Limited Liability	
Company The company AF-10	Name of tested product 1. Software and NFORMATION and telecommunication systems in which information is processed, not containing information constituting a state secret, interacting with certified cryptographic protection
"ANKAD" 24.09.20	of information.
124498, 09/24/20 Moscow Moscow, Zelenograd, 4806, 5, page 20	
	Name of tooted and dust
Federal state military educational institution of higher education "Military Space Academy named after AF Mozhaysky" of the Ministry of Defense of the Russian Federation 197082, St. Petersburg, ul. Zhdanov, etc.	Federation; specialized monitoring tools (blocking) control signals transmitted over interoffice trunks. 8. Firewalls.
13	 Engineering and cryptographic research products at pp 1, 2, 3, 4, 8, 13. Special engineering analysis products at pp 5, 6, 11, 12. Studies of hardware and software product of claim 7 for compliance with information security requirements. Studies of the functional properties of the product according to claims 8-13 for compliance with information security requirements.
Closed Joint-Stock	Name of tested product 1. Hardware, software, and hardware and software encryption (cryptographic) means
Company AF-11	
"EUREKA" 20.02.20 191023, g St.	11 intended to protect against unauthorized access to information during processing and storage.

Petersburg, ul. Pea, etc. 32, l. And, of. 15H		 Hardware, software, and hardware and software of the electronic signature. Encrypted communication equipment. Information and telecommunication systems of the state authorities of the Russian Federation in which the protection of information is carried out the use of the protected equipment and organizational measures without the use of methods of cryptographic transformations. Information and telecommunication systems of the state authorities of the Russian Federation, which protects the information from the the use of encryption (cryptographic) means. Passive and active technical protection of information for use in information and telecommunication systems. Equipment institutional digital automatic telephone exchanges, intended to convey information that does not contain information constituting a state secret, in public authorities of the Russian Federation; specialized monitoring tools (blocking) control signals transmitted over interoffice trunks. Firewalls. Systems for detection of computer attacks. Software information and telecommunication systems, in order to ensure protection of information the use of encryption (cryptographic) means. Software designed for use in information and telecommunication systems, organs of state power of the Russian Federation. NAME OF TESTS Special studies on the production pp 1, 2, 3, 4, 6, 7, 8, 10. Studies linear signal output by pp 1, 2, 3, 4, 6. Accessibility of the products of claim 5. Special engineering analysis products at pp 5, 6, 7, 8, 9, 12, 13. Studies hardware product of claim 9 for compliance with information security requirements. Studies of the functional properties of the product according to claims 10-13 for compliance with information security requirements.
Closed Joint-Stock Company "Atlas maps" 129085, Moscow, Prospekt Mira house 105, page 1	AF-112 12.04.2011 04/12/2014	Name of tested product Of cash registers with specially developed and applied only in its structure by means of cryptographic protection of fiscal data, including protected electronic control tape. NAME OF TESTS 1. Test of the check-out equipment with built-in electronic control tape to secure compliance "with technical requirements to control cash machines on the part of the electronic control tape protected." 2. Checking the operation of the electronic control tape secure in the check-out equipment for compliance with the specification protected electronic control tape. 3. To verify compliance with maintenance work on protected electronic control tape consisting of cash registers in the technical documentation of cash registers, the current regulations on protected electronic control tape. 4. Test of the check-out equipment with built-in cryptographic fiscal data for compliance with cash control technique in terms of incorrigibility fiscal data. 5. To verify compliance with maintenance work on means of cryptographic protection of data in the fiscal cash register equipment listed in the technical documentation of cash registers, regulations on the use of cryptographic protection.
The International		Name of tested product 1. Information and telecommunication systems of the state authorities of the Russian Federation in

The International Centre for	
Informatics and	
Electronics	AF-113
(InterEVM)	20.05.2011
100557	05/20/2016
123557	
g Str.	
Presnensky Val,	
September 1	

- 1. Information and telecommunication systems of the state authorities of the Russian Federation in which the protection of information is carried out—the use of the protected equipment and organizational measures without the use of methods of cryptographic transformations.
- 2. Information and telecommunication systems of the state authorities of the Russian Federation, which protects the information using encryption (cryptographic) means.
- 3. Equipment institutional digital automatic telephone exchanges for use in government of the Russian Federation; specialized monitoring tools (blocking) control signals transmitted over interoffice trunks.
- 4. Firewalls.
- 5. Software and hardware-software systems that implement the functions of the certification center, intended to protect the information that does not contain information constituting a state secret.

		 Software information and telecommunication systems, which cooperates with certified encryption (cryptographic) means. Software designed for use in and NFORMATION and telecommunication systems authorities of the Russian Federation. NAME OF TESTS Special engineering analysis products at pp 1, 2, 3, 5. Research software product of claim 3 for compliance with information security requirements. Studies of the functional properties of the product according to claims 4, 5, 6, 7 for compliance with information security requirements.
Closed Joint-Stock Company "Multidisciplinary Innovation Enterprise "SVEMEL" 125438, Moscow, 4th Likhachevsky per., 15, p 3	AF-115 07.03.2011 03/07/2016	Name of tested product 1. Information and telecommunication systems of the state authorities of the Russian Federation in which data protection is provided by the protected equipment and organizational measures without the use of cryptographic methods of conversion. 2. Information and telecommunication systems of the state authorities of the Russian Federation, which protects the information using encryption (cryptographic) means. 3. Passive and active technical protection of information for use in information and telecommunication systems. 4. Equipment institutional digital automatic telephone exchanges for use in government of the Russian Federation; specialized monitoring tools (blocking) control signals transmitted over interoffice trunks. 5. Firewalls. 6. Software information and communications systems, which cooperates with certified encryption (cryptographic) means. 7. Software designed for use in information and telecommunication systems, organs of state power of the Russian Federation. 8. The hardware and software modules trusted boot the PC. NAME OF TESTS 1. Special studies on the production pp 1, 2, 3, 5, 8. 2. Studies hardware product of claim 4 for compliance with information security requirements. 3. Research software product of claim 4 for compliance with information security requirements. 4. Studies of the functional properties of the product according to claims 5-8 for compliance with information security requirements.
Federal State Unitary Enterprise "Research and Production Enterprise" Gamma " 117420 g Str. Trade union, etc. 78, pp. 4	AF-116 30 .05.2011 05/30/2016	Name of tested product 1. Hardware, software, and hardware and software encryption tools designed to provide cryptographic protection of information when it is transmitted over the communication channels. 2. Hardware, Software, and hardware and software encryption tools designed to protect against unauthorized access to information during processing and storage. 3. Hardware, software, and hardware and software encryption tools designed to protect against spoofing, including simulation protection means. 4. Hardware, software, and hardware and software digital signature. 5. Encrypted communication equipment. 6. Information and telecommunication systems of the state authorities of the Russian Federation in which data protection is provided by the protected equipment and organizational measures without the use of cryptographic methods of conversion. 7. Information and telecommunication systems of the state authorities of the Russian Federation, which protects the information using encryption (cryptographic) means. 8. Passive and active technical protection of information for use in and NFORMATION and telecommunication systems. 9. Equipment institutional digital automatic telephone exchanges for use in government of the Russian Federation; specialized monitoring tools (blocking) control signals transmitted over interoffice trunks. 10. Firewalls.

		 Systems for detection of computer attacks. Software systems that implement the functions of the certification center. Software and NFORMATION and telecommunication systems, which cooperates with certified encryption (cryptographic) means. Software designed for use in and NFORMATION and telecommunication systems authorities of the Russian Federation. The hardware and software modules trusted boot the PC. NAME OF TESTS Engineering and cryptographic research products at pp 1, 2, 3, 4, 7, 10, 15. Special studies on the production pp 1, 2, 3, 4, 6, 7, 8, 10, 15. Special work with the production of Claim 5. Special engineering analysis products at pp 5, 6, 7, 8, 9. Studies of hardware and software product of claim 9 for compliance with information security requirements. Studies of the functional properties of the product according to claims 10-15 for compliance with information security requirements. SPECIAL CONDITIONS Engineering and cryptographic research products at pp 1, 2, 3, 4, 7, 10, 15 and study the functional properties of the product according to claim 12 restricts research in information security, does not contain information constituting a state secret.
Closed Joint-Stock Company "The Moscow branch of Penza Research Institute of Electrical Engineering " 127018 g Str. Sushchevskiy Val, 16, pp. 5, 2nd Floor	AF-117 15.04.2011 15.04.2016	Name of tested product 1. Software and hardware and software encryption tools designed to provide cryptographic protection of information when it is transmitted over the communication channels. 2. Software and hardware and software encryption tools designed to protect against unauthorized access to information during processing and storage. 3. Software and hardware and software encryption tools designed to protect against spoofing, including simulation protection means. 4. Software and hardware and software digital signature. 5. Application software systems that implement the functions of the certification center. 6. Software information and telecommunication systems, which cooperates with certified encryption (cryptographic) means. NAME OF TESTS 1. Engineering and cryptographic research products at pp 1, 2, 3, 4. 2. Special engineering analysis products at pp 5 and 6. 3. Studies of the functional properties of the product according to claims 5, 6 on compliance with information security requirements. SPECIAL CONDITIONS Research products are limited to conducting research of information security that does not contain information constituting a state secret.
Closed Joint-Stock Company "All-Union Institute of fiber-optic communication systems and processing information " 105066, Moscow, ul. Lower Krasnoselskaya 13, pp. 1	AF-118 20.07.2011 20/07/2014	Name of tested product 1. Hardware, software, and hardware and software encryption tools designed to provide cryptographic protection of information when it is transmitted over the communication channels. 2. Hardware, software, and hardware and software encryption tools designed to protect against unauthorized access to information during processing and storage. 3. Hardware, software, and hardware and software encryption tools designed to protect against spoofing, including simulation protection means. 4. Hardware, software, and hardware and software digital signature. 5. Encrypted communication equipment. 6. Information and telecommunication systems of the state authorities of the Russian Federation in which data protection is provided by the protected equipment and organizational measures without the use of cryptographic methods of conversion. 7. Information and telecommunication systems of the state authorities of the Russian Federation, which protects the information from the the use of encryption (cryptographic) means. 8. Passive and active technical protection of information for use in information and telecommunication systems. 9. Equipment institutional digital automatic telephone exchanges for use in government of the Russian Federation; specialized monitoring tools (blocking) control signals transmitted over interoffice trunks.

10. Software information and telecommunication systems, which cooperates with certified encryption (cryptographic) means. 11. Software designed for use in information and telecommunication systems, organs of state power of the Russian Federation. 12. The hardware and software modules trusted boot the PC. NAME OF TESTS 1. Engineering and cryptographic research products at pp 1, 2, 3, 4, 7, 12. 2. Special studies on the production pp 1, 2, 3, 4, 6, 7, 8, 12. 3. Accessibility of the products of claim 5. Special engineering analysis products at pp 5, 6, 7, 8, 9. 5. Studies of hardware and software product of claim 9 for compliance with information security requirements. 6. Studies of the functional properties of the product according to claims 10-12 for compliance with information security requirements. SPECIAL CONDITIONS

	i	n information security, does not contain information constituting a state secret.
		Name of tested product
Federal State Unitary		 Hardware, software, and hardware and software encryption tools designed to provide cryptographic protection of information when it is transmitted over the communication channels. Hardware, software, and hardware and software encryption tools designed to protect against unauthorized access to information during processing and storage. Hardware, software, and hardware and software encryption tools designed to protect against spoofing, including simulation protection means. Hardware, software, and hardware and software digital signature. Encrypted communication equipment. Information and telecommunication systems of the state authorities of the Russian Federation in which data protection is provided by the protected equipment and organizational measures without the use of cryptographic methods of conversion. Information and telecommunication systems of the state authorities of the Russian Federation, which protects the information using encryption (cryptographic) means. Passive and active technical protection of information for use in information and
Enterprise		telecommunication systems.
"Scientific- Production Center" Delta "	AF-September 11 21.07.2011 25.10.2013	 Equipment institutional digital automatic telephone exchanges for use in government of the Russian Federation; specialized monitoring tools (blocking) control signals transmitted over interoffice trunks. Software anti-virus tools. Software and hardware-software systems that implement the functions of the certification center. Software information and telecommunication systems, which cooperates with certified encryption (cryptographic) means. Software designed for use in information and telecommunication systems, organs of state power of the Russian Federation. The hardware and software modules trusted boot the PC. NAME OF TESTS Cryptographic research products at pp 1, 2, 3, 4, 14. Engineering and cryptographic research products at pp 1, 2, 3, 4, 14. Special studies on the production pp 1, 2, 3, 4, 6, 7, 8, 14. Studies linear signal output by pp 1, 2, 3, 4, 7, 14. Special engineering analysis products at pp. 5, 6, 7, 8, 9. Studies of hardware and software product of claim 9 for compliance with information security requirements. Studies of the functional properties of the product according to claims 10-14 for compliance with information security requirements.

Limited Liability	AF-120	Name of tested product
Company	02.08.2011	Information and telecommunication systems of the state authorities of the Russian

Cryptographic research products at pp 1, 2, 3, 4, 14, can only be carried out in support of its special investigations and studies of the linear signal.

"Center of Information Security" 141090, Moscow region., City Jubilee Street. Pioneer, etc. Quarter	20.04.2014	Federation in which data protection is provided by the protected equipment and organizational measures without the use of cryptographic methods of conversion. 2. Information and telecommunication systems of the state authorities of the Russian Federation, which protects the information using encryption (cryptographic) means. 3. Passive and active technical protection of information for use in information and telecommunication systems. 4. Firewalls. 5. Software information and telecommunication systems, which cooperates with certified cryptographic protection of information. 6. Software designed for use in information and telecommunication systems, organs of state power of the Russian Federation. 7. The hardware and software modules trusted boot PC. NAME OF TESTS 1. Engineering and cryptographic research product according to claim 7. 2. Special studies on the production pp 1, 3, 7. 3. Studies linear signal output according to claim 7. 4. Special engineering analysis products at pp 1, 2, 3. 5. Studies haye functional properties of the product according to claims 4, 5, 6, 7 for compliance with information security requirements.
		Name of tested product 1. Hardware, software, and hardware and software encryption tools designed to provide cryptographic protection of information when it is transmitted over the communication channels. 2. Hardware, software, and hardware and software encryption tools designed to protect against unauthorized access to information during processing and storage. 3. Hardware, software, and hardware and software encryption tools designed to protect against spoofing including simulation protection means.

		Name of tested product
		1. Hardware, software, and hardware and software encryption tools designed to provide cryptographic protection of information when it is transmitted over the communication channels.
		2. Hardware, software, and hardware and software encryption tools designed to protect against unauthorized access to information during processing and storage.
		3. Hardware, software, and hardware and software encryption tools designed to protect against spoofing, including simulation protection means.
		4. Hardware, software, and hardware and software digital signature.
Federal State		5. Encrypted communication equipment.
Unitary		6. Information and telecommunication systems of the state authorities of the Russian Federation in
Enterprise		which data protection is provided by the protected equipment and organizational measures without the use of cryptographic methods of conversion.
"Research	AF-121	7. Information and telecommunication systems of the state authorities of the Russian Federation,
Institute"	15.03.2011	which protects the information from the the use of encryption (cryptographic) means.
Quantum "	15.03.2016	8. Passive and active technical protection of information for use in information and
105420		telecommunication systems.
125438 Moscow,		9. Software information and telecommunication systems, which cooperates with certified encryption (cryptographic) means.
4th Likhachevsky		10. Software designed for use in information and telecommunication systems, organs of state power of
per., 15		the Russian Federation.
		NAME OF TESTS
		1. Cryptographic research products at pp 1, 2, 3, 4.
		2. Engineering and cryptographic research products at pp 1, 2, 3, 4.
		3. Special studies on the production pp 1, 2, 3, 4, 6, 7, 8.
		4. Studies linear signal output by pp 1, 2, 3, 4, 7.
		5. Accessibility of the products of claim 5.
		6. Special engineering analysis products at pp 6, 7, 9, 10. 7. Studies of the functional properties of the product according to claims 9, 10 for compliance with information security requirements.

State state educational institution higher education Academy of the Federal Security Service of the Russian Federation 302034, Moscow Eagle	AF-122 28.10.2011 01.08.2014	Name of tested product 1. Software and hardware and software encryption tools designed to provide cryptographic protection of information when it is transmitted over the communication channels. 2. Software and hardware and software encryption tools designed to protect against unauthorized access to information during processing and storage. 3. Information and telecommunication systems of the state authorities of the Russian Federation in which data protection is provided by the protected equipment and organizational measures without the use of cryptographic methods of conversion. 4. Information and telecommunication systems of the state authorities of the Russian Federation, which protects the information using encryption (cryptographic) means. 5. Firewalls. 6. Software and hardware-software systems that implement the functions of the certification center.
Woscow Lagic	I	

Street. Priborostroi - Consequently, etc. 35		 Software information and telecommunication systems, which cooperates with certified cryptographic protection of information. Software designed for use in information and telecommunication systems, organs of state power of the Russian Federation. NAME OF TESTS Engineering and cryptographic research products at pp 1 and 2. Special engineering analysis products at pp 3, 4, 7, 8. Studies of the functional properties of the product according to claims 3-8 on compliance with information security requirements.
Limited Liability Company "Unser PRO" 119192, Moscow, Michurinsky prospect etc. 19, Building 1, Apt. 29	AF-123 07.12.2011 07/12/2014	Name of tested product 1. Information and telecommunication systems of the state authorities of the Russian Federation in which data protection is provided by the protected equipment and organizational measures without the use of cryptographic methods of conversion. 2. Information and telecommunication systems of the state authorities of the Russian Federation, which protects the information from the the use of encryption (cryptographic) means. 3. Software information and telecommunication systems, which cooperates with certified encryption (cryptographic) means. 4. Software designed for use in information and telecommunication systems, organs of state power of the Russian Federation. NAME OF TESTS 1. Special engineering analysis products at pp 1 and 2. 2. Studies of the functional properties of the product according to claims 3 and 4 in compliance with information security requirements.
Federal State Unitary Enterprise "Central Research Institute Economics, Computer Science and Control Systems " 123104, Moscow, Tver Boulevard, 7/2	AF-124 07.12.2011 07/12/2014	Name of tested product 1. Information and telecommunication systems of the state authorities of the Russian Federation in which data protection is provided by the protected equipment and organizational measures without the use of cryptographic methods of conversion. 2. Information and telecommunication systems of the state authorities of the Russian Federation, which protects the information from the the use of encryption (cryptographic) means. 3. Firewalls. 4. Systems for detection of computer attacks. 5. Software and hardware-software systems that implement the functions of the certification center. 6. Software information and telecommunication systems, which cooperates with certified encryption (cryptographic) means. 7. Software designed for use in information and telecommunication systems, organs of state power of the Russian Federation. NAME OF TESTS 1. Special engineering analysis products at pp 1 and 2. 2. Studies of the functional properties of the product according to claims 3-7 for compliance with information security requirements.
Federal State Unitary Enterprise "Gostehstroy" 123242, Moscow, Acad. Kapranov , 3, page 1	AF-125 12 .12.2011 12 .12.2014	Name of tested product 1. Information and telecommunication systems of the state authorities of the Russian Federation in which data protection is provided by the protected equipment and organizational measures without the use of cryptographic methods of conversion. 2. Information and telecommunication systems of the state authorities of the Russian Federation, which protects the information from the the use of encryption (cryptographic) means. 3. Passive and active technical protection of information for use in information and telecommunication systems. 4. Equipment institutional digital automatic telephone exchanges for use in government of the Russian Federation; specialized monitoring tools (blocking) control signals transmitted over interoffice trunks. 5. Software designed for use in information and telecommunication systems, organs of state

		power of the Russian Federation. NAME OF TESTS 1. Special studies on the production pp 1, 2, 3. 2. Special engineering analysis products at pp 1, 2, 3. 3. Studies of hardware and software product of claim 4 for compliance with information security requirements. 4. Studies of the functional properties of the product according to claim 5 for compliance with information security requirements.
Closed Joint-Stock Company "Informtekhnika and Communication" 107066, Str. Lower Krasnoselskaya 35	AF-126 12/12/20 11 12.12.201 6	Name of tested product 1. Information and telecommunication systems of gov't p GOVERNMENTAL authorities of the Russian Federation in which information security impl e identified with the use of the protected equipment and organizational measures without the use of cryptographic methods of conversion. 2. Information and telecommunication systems of gov't p GOVERNMENTAL authorities of the Russian Federation, which provides protection and n formation using encryption (cryptographic) means. 3. Passive and active technical protection of information for use in information and telecommunication B with themes. 4. Equipment institutional digital automatic telephone exchanges for use in government of the Russian Federation; specialized monitoring tools (blocking) control signals transmitted over interoffice connected and relatively lines. 5. Software information and telecommunication systems, which cooperates with certified encryption (cryptographic) means. 6. Software designed for use in MR mation and communication systems of the state authorities of the Russian Federation. NAME OF TESTS 1. Special engineering analysis products at pp 1-4. 2. Studies of hardware and software product of claim 4 on compliance and information security n. 3. Studies of the functional properties of the products for compliance with information security requirements for pp 1-6.
Closed Joint-Stock Company "Orbit" 350063, g Address: Str. Komsomolskaya 40	AF-127 04.10.2011 04/10/2016	Name of tested product 1. The hardware and the hardware and software encryption (cryptographic) means intended to protect information that does not contain information constituting a state secret when it is communicated through the channels of communication. 2. The hardware and the hardware and software encryption (cryptographic) means intended to protect against unauthorized access to information that does not contain information constituting a state secret, during processing and storage. 3. The hardware and the hardware and software encryption (cryptographic) means intended to protect information that does not contain information constituting a state secret, against the imposition of false information, including the means of simulation protection. 4. The hardware and the hardware and software of digital signature designed to protect information that does not contain information constituting a state secret. 5. Encrypted communication equipment. 6. Information and telecommunication systems of the state authorities of the Russian Federation in which data protection is provided by the protected equipment and organizational measures without the use of cryptographic methods of conversion. 7. Information and telecommunication systems of the state authorities of the Russian Federation, which protects the information using encryption (cryptographic) means. 8. Passive and active technical protection of information for use in and NFORMATION and telecommunication systems. 9. Equipment institutional digital automatic telephone exchanges for use in government of the Russian Federation; specialized monitoring tools (blocking) control signals transmitted over interoffice trunks. 10. Firewalls. 11. Software information and telecommunication systems, which cooperates with certified encryption (cryptographic) means. 12. Software designed for use in and NFORMATION and telecommunication systems authorities of the Russian Federation.

Limitad		13. The hardware and software modules trusted boot the PC. NAME OF TESTS 1. Special studies on the production pp 1, 2, 3, 4, 5, 6, 7, 8, 10, 13. 2. Accessibility of the products of claim 5. 3. Special engineering analysis products at pp 5, 6, 7, 8, 9. 4. Studies of hardware and software product of claim 9 for compliance with information security requirements. 5. Studies of the functional properties of the product according to claims 10-12 for compliance with information security requirements.
Limited Liability Company "Optiona 195220, St. Petersbur ul. Gzhatska etc. 21, letter B	ly" AF-128 01.02.2012 01/02/2017 g,	
public corporation "Penza Research Institute of Electrical Engineeri 440026, Penza city Sovetskay 9	AF-129 f 15.03.2012 01/07/2015	Name of tested product 1. Hardware, software, and hardware and software encryption tools designed to provide cryptographic protection of information when it is transmitted over the communication channels. 2. Hardware, software, and hardware and software encryption tools designed to protect against unauthorized access to information during processing and storage. 3. Hardware, software, and hardware and software encryption tools designed to protect against spoofing, including simulation protection means. 4. Hardware, software, and hardware and software digital signature. 5. Encrypted communication equipment. 6. Information and telecommunication systems of the state authorities of the Russian Federation in which data protection is provided by the protected equipment and organizational measures without the use of cryptographic methods of conversion. 7. Information and telecommunication systems of the state authorities of the Russian Federation, which protects the information using encryption (cryptographic) means. 8. Passive and active technical protection of information for use in information and telecommunication systems. 9. Equipment institutional digital automatic telephone exchanges for use in government of the Russian Federation; specialized monitoring tools (blocking) control signals transmitted over interoffice trunks. 10. Firewalls. 11. Software and hardware-software systems that implement the functions of the certifying center. 12. Software information and telecommunication systems, interacting with certified encryption (cryptographic) means. 13. Software designed for use in information and telecommunication systems, organs of state power of the Russian Federation. 14. The hardware and software modules trusted boot the PC. NAME OF TESTS 1. Cryptographic research products at pp 1, 2, 3, 4, 10, 14. 2. Engineering and cryptographic research products at pp 1, 2, 3, 4, 10, 14. 3. Special studies on the products of claim 5. 4. Accessibility of the products of claim 5. 4. Accessibility of the

		 7. Studies of hardware and software product of claim 9 for compliance with information security requirements. 8. Studies of the functional properties of the product according to claims 10-14 for compliance with information security requirements.
		Name of tested product
Public corporation "Perm Telephone Plant" TELTA " 614990, Penza city. Okulov, etc. 80	AF-130 15.03.2012 15/03/2017	 Information and telecommunication systems of the state authorities of the Russian Federation in which data protection is provided by the protected equipment and organizational measures without the use of cryptographic methods of conversion. Equipment institutional digital automatic telephone exchanges for use in government of the Russian Federation; specialized monitoring tools (blocking) control signals transmitted over interoffice trunks. Passive and active technical protection of information for use in information and telecommunication systems. Software designed for use in and NFORMATION and telecommunication systems authorities of the Russian Federation.
		 NAME OF TESTS Special studies on the production pp 1 and 3. Special engineering analysis products at pp 1, 2, 3. Studies of hardware and software product of claim 2 for compliance with information security requirements. Studies of the functional properties of the product according to claims 1, 4 in compliance with information security requirements.

Public corporation		Name of tested product
"Saturn"	AF-132	1. Information and telecommunication systems of the state authorities of the Russian Federation in which data protection is provided by the protected equipment and organizational measures without the use of cryptographic methods of conversion.
107,553, g Str. Much	10.04.2012 10/04/2017	<i>11</i> 6 1
CHerkizovskaja, 21, Building 1		NAME OF TESTS
		Special research products.

Limited Liability Company		Name of tested product
"Center for Special Systems Engineering" 127521 g Str. Oktyabrskaya 72	AF-133 11.04.2012 11/04/2017	 Firewalls. Systems for detection of computer attacks. Software and hardware-software systems that implement the functions of the certification center. Software information and telecommunication systems, interacting with certified encryption (cryptographic) means. Software designed for use in information and telecommunication systems, organs of state power of the Russian Federation. NAME OF TESTS Studies of the functional properties of the products for compliance with information security requirements.

Federal State	AF 134	Name of tested product

	4/08/20 12 8.04.201 7	 Hardware, software, and hardware and software encryption tools designed to provide cryptographic protection of information when it is transmitted over the communication channels. Hardware, software, and hardware and software encryption tools designed to protect against unauthorized access to information during processing and storage. Hardware, software, and hardware and software encryption tools designed to protect against spoofing, including simulation protection means. Hardware, software, and hardware and software of the electronic signature. Encrypted communication equipment. Information and telecommunication systems of the state authorities of the Russian Federation in which data protection is provided by the protected equipment and organizational measures without the use of cryptographic methods of conversion. Information and telecommunication systems of the state authorities of the Russian Federation, which protects the information using encryption (cryptographic) means. Passive and active technical protection of information for use in information and telecommunication systems. Equipment institutional digital automatic telephone exchanges for use in government of the Russian Federation; specialized monitoring tools (blocking) control signals transmitted over interoffice trunks. Firewalls. Systems for detection of computer attacks. Software and NFORMATION and telecommunication systems, interacting with certified encryption (cryptographic) means. Software and NFORMATION and telecommunication systems, organs of state power of the Russian Federation. The hardware and software modules trusted boot the PC. NAME OF TESTS Cryptographic research products at pp 1, 2, 3, 4, 10, 15. Epcineering and cryptographic research products at pp 1, 2, 3, 4, 10, 15. Special studies on the productio
--	--------------------------	--

Closed Joint-Stock Company	
"Besant"	
125171, Moscow, 5th Passage Voykovskiy, etc 2	2.

AF-135

15.06.2012

15/06/2017

Name of tested product

Of cash registers with specially developed and applied only in its structure by means of cryptographic protection of fiscal data, including protected electronic control tape.

NAME OF TESTS

- 1. Test of the check-out equipment with built-in electronic control tape to secure compliance "with technical requirements to control cash machines on the part of the electronic control tape protected."
- 2. Checking the operation of the electronic control tape secure in the check-out equipment for compliance with the specification protected electronic control tape.
- 3. To verify compliance with maintenance work on protected electronic control tape consisting of cash registers in the technical documentation of cash registers, the current regulations on protected electronic control tape.
- 4. Test of the check-out equipment with built-in cryptographic fiscal data for compliance with cash control technique in terms of incorrigibility fiscal data.
- 5. To verify compliance with maintenance work on means of cryptographic protection of data in the fiscal cash register equipment listed in the technical documentation of cash registers, regulations on the use of cryptographic protection.

Closed Joint-Stock Company "Kalugapriborsvyaz 248017, g Kaluga, st.	AF-136	NAME OF TESTS
Moskovskaya 249	7	2. Conducting research software tools for compliance with information security requirements.
Włoskovskaya 249		2. Conducting research software tools for compliance with information security requirements.
Closed Joint-Stock Company "Scientific and Production Association" Echelon " 107023, Str. Electrozavod- Skye, d 24, p	AF-137 01.06.2012 06/01/2017	Name of tested product 1. Information and telecommunication systems of the state authorities of the Russian Federation in which data protection is provided by the protected equipment and organizational measures without the use of cryptographic methods of conversion. 2. Information and telecommunication systems of the state authorities of the Russian Federation, which protects the information using encryption (cryptographic) means. 3. Firewalls. 4. Software information and telecommunication systems, interacting with certified encryption (cryptographic) means. 5. Software designed for use in information and telecommunication systems, organs of state power of the Russian Federation. NAME OF TESTS 1. Special engineer the product according to claims 1, 2.
1		2. Studies of the functional properties of the product according to claims 3 - 5 for compliance with information security requirements.
Limited Liability Company "Center of Information Security" mask " 119607, Moscow, Michurinsky Pr, d 27, h. 2	AF-138 15.06.2012 15.06.2015	 Name of tested product Information and telecommunication systems of the state authorities of the Russian Federation in which data protection is provided by the protected equipment and organizational measures without the use of cryptographic methods of conversion. Information and telecommunication systems of the state authorities of the Russian Federation, which protects the information using encryption (cryptographic) means. Passive and active technical protection of information for use in information and telecommunication systems. Firewalls. Systems for detection of computer attacks. Software designed for use in information and telecommunication systems, organs of state power of the Russian Federation. NAME OF TESTS Special studies on the production pp 1 and 3. Special engineering analysis products at pp 1, 2, 3. Studies of the functional properties of the product according to claims 4 - 6 on compliance with information security requirements.
Public corporation "FINANCE AND INFORMATION TECHNOLOGY" 119180,	AF-139 14.08.2012 14/08/2015	Name of tested product 1. Information and telecommunication systems of the state authorities of the Russian Federation in which data protection is provided by the protected equipment and organizational measures without the use of cryptographic methods of conversion. 2. Information and telecommunication systems of the state authorities of the Russian Federation in order to ensure the protection of information with the use of encryption (cryptographic) means. 3. Firewalls.

Tails per.

, 11-A

Moscow, 1st

4. Systems for detection of computer attacks.

5. Software and hardware-software systems that implement the functions of the certification center.

7. Software designed for use in information and telecommunication systems, organs of state power of the Russian Federation. NAME OF TESTS 1. Special engineer the product according to claims 1, 2, 6, 7. 2. Studies of the functional properties of the product according to claims 3-7 for compliance with information security requirements. Name of tested product Hardware, software, and hardware and software encryption tools designed to provide cryptographic protection of information when it is transmitted over the communication channels. Hardware, software, and hardware and software encryption tools designed to protect against unauthorized access to information during processing and storage. Hardware, software, and hardware and software encryption tools designed to protect against spoofing, including the simulation protection. Hardware, software, and hardware and software digital signature. Limited Information and telecommunication systems of the state authorities of the Russian Federation in which Liability data protection is performed using secure equipment and organizational measures without the use of Company cryptographic methods of conversion. Information and telecommunication systems of the state authorities of the Russian Federation in order to AF-140 "Genk" ensure the protection of information with the use of encryption (cryptographic) means. 10.08.2012 Software information and telecommunication systems, which cooperates with certified encryption 107113. 06/23/2016 (cryptographic) means. Moscow, 8. Software designed for use in information and telecommunication systems, organs of state power of the ul. Russian Federation. Sokolniki 9. The hardware and software modules trusted boot the PC. Val, 38 NAME OF TESTS 1. Engineering and cryptographic research products at pp 1, 2, 3, 4, 9. 2. Special engineer the product according to claims 5, 6. 3. Studies of the functional properties of the product according to claims 5, 6, 7, 8, 9 for compliance with information security requirements. SPECIAL CONDITIONS The validity of this certificate of accreditation is limited to the study of information security that does not contain information constituting a state secret. Name of tested product Hardware, software, and hardware and software encryption tools designed to provide cryptographic protection of information when it is transmitted over the communication channels. Hardware, software, and hardware and software encryption tools designed to protect against unauthorized access to information during processing and storage. Hardware, software, and hardware and software encryption tools designed to protect against spoofing, including simulation protection means. Public Hardware, software, and hardware and software of the electronic signature. corporation AF-141 Encrypted communication equipment. Information and telecommunication systems of the state authorities of the Russian "Concern" 30.0812 Federation in which data protection is provided by the protected equipment and organizational Automatic " .20

measures without the use of cryptographic methods of conversion.

telecommunication systems.

over interoffice trunks.

10. Firewalls.

center.

Information and telecommunication systems of the state authorities of the Russian

9. Equipment institutional digital automatic telephone exchanges for use in government of the Russian Federation; specialized monitoring tools (blocking) of control signals transmitted

11. Software and hardware-software systems that implement the functions of the certification

Passive and active technical protection of information for use in information and

Federation, which protects the information using encryption (cryptographic) means.

(cryptographic) means.

.0 8 30 .201

127106, Str.

Botany, etc. 25

6. Software information and telecommunication systems, which cooperates with certified encryption

Software information and telecommunication systems, which cooperates with certified encryption (cryptographic) means.
 Software designed for use in information and telecommunication systems, organs of state power of the Russian Federation.
 The hardware and software modules trusted boot the PC.

NAME OF TESTS

Name of tested product

Contar

- 1. Cryptographic research products at pp 1, 2, 3, 4, 10, 14.
- 2. Engineering and cryptographic research products at pp 1, 2, 3, 4, 10, 14.
- 3. Special studies on the production pp 1, 2, 3, 4, 6, 7, 8, 10, 14.
- 4. Studies linear signal output by pp 1, 2, 3, 4, 10, 14.
- 5. Accessibility of the products of claim 5.
- 6. Special engineer the product according to claims 6, 7, 8, 12, 13.
- 7. Studies of hardware and software products as claimed in claim 9 for compliance with information security requirements.
- 8. Studies of the functional properties of the products at pp 10-14 for compliance with information security requirements.

Limited liability corre t "The Centre for Modern Technologies of Information Security"	AF-1 42 30 .0 8 .201 2 30 .08.201 5	 Information and telecommunication systems of the state authorities of the Russian Federation in which data protection is provided by the protected equipment and organizational measures without the use of cryptographic methods of conversion. Information and telecommunication systems of the state authorities of the Russian Federation, which protects the information using encryption (cryptographic) means. Passive and active technical protection of information for use in information and telecommunication systems.
127550, Str. Pryanishnikova House 23A	3	NAME OF TESTS 1. Special studies on the production pp 1, 2, 3. 2. Special engineer the product according to claims 1, 2, 3.

Center		
providing		
information "Energy"	AF-143	Name of tested product Hardware and software encryption tools and software designed to provide cryptographic protection of
Federal Security		information when it is transmitted over the communication channels.
Service of the	10 .10.2012	NAME OF TESTS
Russian	2 0. 04 .201	1. Engineering and cryptographic research.
Federation	3	2. Special studies.
142800,		3. Research line signal.
Moscow region,		
Stupino		

Public	AF-144	Name of tested product
corporation		1. Hardware, software, and hardware and software encryption tools designed to provide
	04 .10.2012	cryptographic protection of information when it is transmitted over the communication

		channels.
		2. Hardware, software, and hardware and software encryption tools designed to protect
		against unauthorized access to information during processing and storage.
		3. Hardware, software, and hardware and software encryption tools designed to protect
		against spoofing, including simulation protection means.
		4. Hardware, software, and hardware and software of the electronic signature.
		5. Information and telecommunication systems of the state authorities of the Russian
		Federation in which data protection is provided by the protected equipment and organizational
		measures without the use of cryptographic methods of conversion.
		6. Information and telecommunication systems of the state authorities of the Russian
		Federation in order to ensure the protection of information with the use of encryption
"Information		(cryptographic) means.
technology and		7. Firewalls.
communication		8. Systems for detection of computer attacks.
systems"		9. Software and hardware-software systems that implement the functions of the certification
127297 ~	04 .10.201	center.
127287, g. , Moscow,	5	10. Software information and telecommunication systems, which cooperates with certified encryption (cryptographic) means.
Petrovsky		11. Software designed for use in information and telecommunication systems, organs of
Old-Razumovsky		state power of the Russian Federation.
passage, 1/23, p		12. The hardware and software modules trusted boot the PC.
1		12. The hardware and software modules trusted boot the Fe.
		NAME OF TESTS
		1. Cryptographic research products at pp 1, 2, 3, 4, 7, 9, 12.
		2. Engineering and cryptographic research products at pp 1, 2, 3, 4, 7, 9, 12.
		3. Special engineering analysis products at pp 5, 6, 9.
		4. Studies of the functional properties of the product according to claims 7, 8, 9, 10, 11, 12 on the
		eligibility information security.
		SPECIAL CONDITIONS
		Cryptography, engineering and cryptographic research products at pp 1, 2, 3, 4, 7, 9, 12, and
		the study of the functional properties of the product according to claim 12, restricts research
<u> </u>	L	in information security, does not contain information constituting a state secret.

Inter-regional public institution "Institute of Engineering Physics" 142210, Moscow region., Serpukhov, Big Hammer Lane., 1A	AF-145 22 .10.20 12 22 .10.201 7	Name of tested product 1. Information and telecommunication systems of the state authorities of the Russian Federation in which data protection is provided by the protected equipment and organizational measures without the use of cryptographic methods of conversion. 2. Information and telecommunication systems of the state authorities of the Russian Federation in order to ensure the protection of information with the use of encryption (cryptographic) means. 3. Equipment institutional digital automatic telephone exchanges and specialized monitoring tools (blocking) control signals transmitted over interoffice trunks for use in government of the Russian Federation in the processing of information not subject to protection under the laws of the Russian Federation. 4. Software information and telecommunication systems, which cooperates with certified encryption (cryptographic) means. 5. Software designed for use in information and telecommunication systems, organs of state power of the Russian Federation. NAME OF TESTS 1. Special engineer the product according to claims 1, 2, 4, 5. 2. Studies of hardware and software products according to claim 3 for compliance with information security requirements. 3. Studies of the functional properties of the product according to claims 4, 5 for compliance with information security requirements.
--	----------------------------------	---

Limited	AF-146	Name of tested product
Liability	AF-140	1. Firewalls.
Company	20/12/2012	2. Systems for detection of computer attacks.
"R-Alpha"	12/20/2017	3. Software information and telecommunication systems, which cooperates with certified encryption
K-Aipila		

123060, g. Str. Raspletina, d 4, Bldg. 1		(cryptographic) means. 4. Software designed for use in information and telecommunication systems, organs of state power of the Russian Federation. NAME OF TESTS Studies of the functional properties of the test products for compliance with information security requirements.
Closed Joint-Stock Company "AST" 115522, Moscow, Proletarian avenue, 8, Bldg. 2	AF-July 14 15. 01 .201 3 15. 01 .201 6	Name of tested product 1. Information and telecommunication systems of the state authorities of the Russian Federation in which data protection is provided by the protected equipment and organizational measures without the use of cryptographic methods of conversion. 2. Information and telecommunication systems of the state authorities of the Russian Federation in order to ensure the protection of information with the use of encryption (cryptographic) means. 3. Firewalls. 4. Systems for detection of computer attacks. 5. Software information and telecommunication systems, which cooperates with certified encryption (cryptographic) means. 6. Software designed for use in information and telecommunication systems, organs of state power of the Russian Federation. NAME OF TESTS 1. Special engineer the product according to claims 1, 2, 5, 6. 2. Studies of the functional properties of the product according to claims 3-6 for compliance with information security requirements.
Limited Liability Company "Research Centre of Certification" 127106, g Moscow, Str. Botany, etc. 25	AF-148 13.04.2013 13/04/2018	Name of tested product 1. Hardware, software, and hardware and software encryption tools designed to provide cryptographic protection of information when it is transmitted over the communication channels. 2. Hardware, software, and hardware and software encryption tools designed to protect against unauthorized access to information during processing and storage. 3. Hardware, software, and hardware and software encryption tools designed to protect against spoofing, including simulation protection means. 4. Hardware, software, and hardware and software of the electronic signature. 5. Encrypted communication equipment. 6. Information and telecommunication systems of the state authorities of the Russian Federation in which data protection is provided by the protected equipment and organizational measures without the use of cryptographic methods of conversion. 7. Information and telecommunication systems of the state authorities of the Russian Federation in order to ensure the protection of information with the use of encryption (cryptographic) means. 8. Passive and active technical protection of information for use in information and telecommunication systems. 9. Equipment institutional digital automatic telephone exchanges for use in government of the Russian Federation; specialized monitoring tools (blocking) of control signals transmitted over interoffice trunks. 10. Software anti-virus tools. 11. Firewalls. 12. Systems for detection of computer attacks. 13. Software and hardware-software systems that implement the functions of the certification center. 14. Software and hArdware-software systems that implement the functions of the certification center. 14. Software designed for use in information and telecommunication systems, organs of state power of the Russian Federation. 16. The hardware and software modules trusted boot the PC. NAME OF TESTS 1. Cryptographic research products at pp 1, 2, 3, 4, 11, 16. 2. Engineering and cryptographic research products at pp 1, 2, 3, 4, 11, 16. 3. Special

 Studies of hardware products according to claim 9 for compliance with information security requirements. Studies of software product according to claim 9 for compliance with information security requirements. Studies of the functional properties of the products at pp 10-16 for compliance with information security requirements.

public corporation "Research and Production	AF-149	Name of tested production of info 1. Hardware of info 2. Hardware of access to inform 3. Hardware including simulated and the including simulated of the including simulated simulated simulated simulated of t
Enterprise" Signal " 193019, g St. Petersburg, ul. Knippovich, etc. 4	03.04.2013 04/03/2014	6. Information in which data provided without the use of the control of the contr

oduct

- e and hardware-software encryption tools designed to provide cryptographic ormation when it is transmitted over the communication channels.
- and hardware-software encryption tools designed to protect against unauthorized nation during processing and storage.
- and hardware-software encryption tools designed to protect against spoofing, tion protection means.
- are and the hardware and software of the electronic signature.
- communication equipment.
- and telecommunication systems of the state authorities of the Russian Federation rotection is performed using secure equipment and of organizational measures of cryptographic methods of conversion.
- and telecommunication systems of the state authorities of the Russian Federation re the protection of information with the use of encryption (cryptographic) means.
- and cryptographic research products at pp 1, 2, 3, 4.
- dies on the production pp 1, 2, 3, 4, 6, 7.
- ar signal output by pp 1, 2, 3, 4, 7.
- of the products of claim 5.
- 5. Special engineering analysis products at pp 5, 6, 7.



TERNEWEL

organizations accredited in the certification of information security safety requirements for the information constituting a state secret ROSS RU $.0003.01\ BI00$ as a testing laboratory for the certification tests

(As of May 1. 0 4 .201 3)

Name and address Organization	Registration number certificate of accreditation, its validity	Area Accreditation
The testing laboratory; The Federal State Unitary Enterprise "Kalugapribor" 248017, Moscow Kaluga, ul. Moskovskaya 249	GIS. RU. LI0025 01.06.2009 01.06.2014	Name of tested product 1. Technical means of protecting information, including monitoring the effectiveness of the security measures of information: 1.1. Protection of information against interception of acoustic signals propagating in air, water, solid media. 1.2. Protection of information against interception of electromagnetic signals, including the interception of spurious electromagnetic emanations (TEMPEST), arising from the work of the technical means of recording, storing, processing, and documentation of information. 1.3. Protection of information against interception of the electrical signals generated in the cable communications: - TEMPEST at the expense of the work of technical means of recording, storing, processing, and documentation of information; - due to the effect of electro-acoustic signal conversion means and the auxiliary systems. NAME OF TESTS Conduct studies of functional properties of products for compliance with regulatory requirements of the Federal Security Service of the Russian Federation.

The testing laboratory; Limited Liability Company	GIS. RU. LI0030 05.09.2009 05/09/2014	Name of tested product 1. Technical protection of information, including a la counter the effectiveness of the measures of information security: 1.1. Protection of information against interception of electromagnetic si g nals, including the interception of stray electromagnetic radiation and n and vodka (TEMPEST), arising from
"Center of		the work of the technical means of recording storing processing and

Information Security"

141090, Moscow reg., City Jubilee Street. Pioneer, etc. Quarter documentation of information.

- 1.2. Protection of information against interception of acoustic signals propagating in air, water, solid media.
- 1.3. Protection of information against interception of the electrical signals generated in the cable communications:
- TEMPEST at the expense of the work of technical means of recording, storing e tion, processing and documentation of information;
- due to the effect of electro-acoustic signal conversion means and the auxiliary systems.
- 1.4. Technical means to detect and identify specific Technical and iCal funds intended for secret information, have a tablished in the construction of buildings and facilities (premises, vehicles), engineering communications, interior, in household appliances, in the technical means of recording, storing, processing and document ing and information and communication systems in an open area.
- 2. Software data protection from unauthorized access (unauthorized access) and software tabs:
- 2.1. Programs that provide concurrent access to information.
- 2.2. Program identification and authentication of terminals and uses ers on various grounds (the password, the additional code word for bi metric data, etc.), including a program to improve the reliability of identification (authentication).
- 2.3. Screening programs are functioning security system and inform tion and integrity protection from unauthorized access.
- 2.4. Program for the protection of various auxiliary facilities (except for anti-virus programs).
- 2.5. Protection Programs PC operating systems (modular avenue of programmatic interpretation, etc.).
- 2.6. Program integrity wide and application software.
- 2.7. Programs whistleblower resources.
- 2.8. Destruction program, residual information in memory devices (memory, video memory, etc.) after completing her and use.
- 2.9. Control program and restore the file structure of the data.
- 2.10. Simulation program of a system or blocking in outcrop servation and tamper evidence.
- 2.11. Programs determine the facts and tamper alarm (with transfer of communication) of their discovery.
- 3. Protected program information processing means:
- 3.1. Application packages workstations.
- 3.2. Databases computer networks.
- 3.3. Software tools for automated control systems.
- 3.4. Software tools for the identification of the manufacturer software (information) of the product, including the identification of copyright.
- 4. Software and hardware data protection:
- 4.1. Software and hardware detection and localization of de first

consequence of software and software-engineering bookmarks. NAME OF TESTS Conduct studies of functional properties of products for compliance with regulatory requirements of the Federal Security Service of the Russian Federation. Name of tested product 1. Software data protection from unauthorized access (unauthorized access) and software tabs: 1.1. Programs that provide concurrent access to information. 1.2. Program identification and authentication of terminals and uses ers on various grounds (the password, the additional code word for bi metric data, etc.), including a program to improve the reliability of identification (authentication). 1.3. Screening programs are functioning security system and inform tion and integrity protection from unauthorized access. 1.4. Program for the protection of various auxiliary facilities (except for anti-virus programs). 1.5. Protection Programs PC operating systems (modular avenue of programmatic interpretation, etc.). 1.6. Program integrity wide and application software. 1.7. Programs whistleblower resources. 1.8. Destruction program, residual information in memory devices (memory, video memory, etc.) after completing her and use. Scientific GIS. RU. Scientific LI0031
Conduct studies of functional properties of products for compliance with regulatory requirements of the Federal Security Service of the Russian Federation. Name of tested product 1. Software data protection from unauthorized access (unauthorized access) and software tabs: 1.1. Programs that provide concurrent access to information. 1.2. Program identification and authentication of terminals and uses ers on various grounds (the password, the additional code word for bi metric data, etc.), including a program to improve the reliability of identification (authentication). 1.3. Screening programs are functioning security system and inform tion and integrity protection from unauthorized access. 1.4. Program for the protection of various auxiliary facilities (except for anti-virus programs). 1.5. Protection Programs PC operating systems (modular avenue of programmatic interpretation, etc.). 1.6. Program integrity wide and application software. 1.7. Programs whistleblower resources. 1.8. Destruction program, residual information in memory devices (memory, video memory, etc.) after completing her and use.
with regulatory requirements of the Federal Security Service of the Russian Federation. Name of tested product 1. Software data protection from unauthorized access (unauthorized access) and software tabs: 1.1. Programs that provide concurrent access to information. 1.2. Program identification and authentication of terminals and uses ers on various grounds (the password, the additional code word for bi metric data, etc.), including a program to improve the reliability of identification (authentication). 1.3. Screening programs are functioning security system and inform tion and integrity protection from unauthorized access. 1.4. Program for the protection of various auxiliary facilities (except for anti-virus programs). 1.5. Protection Programs PC operating systems (modular avenue of programmatic interpretation, etc.). 1.6. Program integrity wide and application software. 1.7. Programs whistleblower resources. 1.8. Destruction program, residual information in memory devices (memory, video memory, etc.) after completing her and use.
Russian Federation. Name of tested product 1. Software data protection from unauthorized access (unauthorized access) and software tabs: 1.1. Programs that provide concurrent access to information. 1.2. Program identification and authentication of terminals and uses ers on various grounds (the password, the additional code word for bi metric data, etc.), including a program to improve the reliability of identification (authentication). 1.3. Screening programs are functioning security system and inform tion and integrity protection from unauthorized access. 1.4. Program for the protection of various auxiliary facilities (except for anti-virus programs). 1.5. Protection Programs PC operating systems (modular avenue of programmatic interpretation, etc.). 1.6. Program integrity wide and application software. 1.7. Programs whistleblower resources. 1.8. Destruction program, residual information in memory devices (memory, video memory, etc.) after completing her and use.
Name of tested product 1. Software data protection from unauthorized access (unauthorized access) and software tabs: 1.1. Programs that provide concurrent access to information. 1.2. Program identification and authentication of terminals and uses ers on various grounds (the password, the additional code word for bi metric data, etc.), including a program to improve the reliability of identification (authentication). 1.3. Screening programs are functioning security system and inform tion and integrity protection from unauthorized access. 1.4. Program for the protection of various auxiliary facilities (except for anti-virus programs). 1.5. Protection Programs PC operating systems (modular avenue of programmatic interpretation, etc.). 1.6. Program integrity wide and application software. 1.7. Programs whistleblower resources. 1.8. Destruction program, residual information in memory devices (memory, video memory, etc.) after completing her and use.
1. Software data protection from unauthorized access (unauthorized access) and software tabs: 1.1. Programs that provide concurrent access to information. 1.2. Program identification and authentication of terminals and uses ers on various grounds (the password, the additional code word for bi metric data, etc.), including a program to improve the reliability of identification (authentication). 1.3. Screening programs are functioning security system and inform tion and integrity protection from unauthorized access. 1.4. Program for the protection of various auxiliary facilities (except for anti-virus programs). 1.5. Protection Programs PC operating systems (modular avenue of programmatic interpretation, etc.). 1.6. Program integrity wide and application software. 1.7. Programs whistleblower resources. 1.8. Destruction program, residual information in memory devices (memory, video memory, etc.) after completing her and use.
access) and software tabs: 1.1. Programs that provide concurrent access to information. 1.2. Program identification and authentication of terminals and uses ers on various grounds (the password, the additional code word for bi metric data, etc.), including a program to improve the reliability of identification (authentication). 1.3. Screening programs are functioning security system and inform tion and integrity protection from unauthorized access. 1.4. Program for the protection of various auxiliary facilities (except for anti-virus programs). 1.5. Protection Programs PC operating systems (modular avenue of programmatic interpretation, etc.). 1.6. Program integrity wide and application software. 1.7. Programs whistleblower resources. 1.8. Destruction program, residual information in memory devices (memory, video memory, etc.) after completing her and use.
1.1. Programs that provide concurrent access to information. 1.2. Program identification and authentication of terminals and uses ers on various grounds (the password, the additional code word for bi metric data, etc.), including a program to improve the reliability of identification (authentication). 1.3. Screening programs are functioning security system and inform tion and integrity protection from unauthorized access. 1.4. Program for the protection of various auxiliary facilities (except for anti-virus programs). 1.5. Protection Programs PC operating systems (modular avenue of programmatic interpretation, etc.). 1.6. Program integrity wide and application software. 1.7. Programs whistleblower resources. 1.8. Destruction program, residual information in memory devices (memory, video memory, etc.) after completing her and use.
1.2. Program identification and authentication of terminals and uses ers on various grounds (the password, the additional code word for bi metric data, etc.), including a program to improve the reliability of identification (authentication). 1.3. Screening programs are functioning security system and inform tion and integrity protection from unauthorized access. 1.4. Program for the protection of various auxiliary facilities (except for anti-virus programs). 1.5. Protection Programs PC operating systems (modular avenue of programmatic interpretation, etc.). 1.6. Program integrity wide and application software. 1.7. Programs whistleblower resources. 1.8. Destruction program, residual information in memory devices (memory, video memory, etc.) after completing her and use.
ers on various grounds (the password, the additional code word for bi metric data, etc.), including a program to improve the reliability of identification (authentication). 1.3. Screening programs are functioning security system and inform tion and integrity protection from unauthorized access. 1.4. Program for the protection of various auxiliary facilities (except for anti-virus programs). 1.5. Protection Programs PC operating systems (modular avenue of programmatic interpretation, etc.). 1.6. Program integrity wide and application software. 1.7. Programs whistleblower resources. 1.8. Destruction program, residual information in memory devices (memory, video memory, etc.) after completing her and use.
metric data, etc.), including a program to improve the reliability of identification (authentication). 1.3. Screening programs are functioning security system and inform tion and integrity protection from unauthorized access. 1.4. Program for the protection of various auxiliary facilities (except for anti-virus programs). 1.5. Protection Programs PC operating systems (modular avenue of programmatic interpretation, etc.). 1.6. Program integrity wide and application software. 1.7. Programs whistleblower resources. 1.8. Destruction program, residual information in memory devices (memory, video memory, etc.) after completing her and use.
identification (authentication). 1.3. Screening programs are functioning security system and inform tion and integrity protection from unauthorized access. 1.4. Program for the protection of various auxiliary facilities (except for anti-virus programs). 1.5. Protection Programs PC operating systems (modular avenue of programmatic interpretation, etc.). 1.6. Program integrity wide and application software. 1.7. Programs whistleblower resources. 1.8. Destruction program, residual information in memory devices (memory, video memory, etc.) after completing her and use.
The testing laboratory; Public corporation "All-Russian 1.3. Screening programs are functioning security system and inform tion and integrity protection from unauthorized access. 1.4. Program for the protection of various auxiliary facilities (except for anti-virus programs). 1.5. Protection Programs PC operating systems (modular avenue of programmatic interpretation, etc.). 1.6. Program integrity wide and application software. 1.7. Programs whistleblower resources. 1.8. Destruction program, residual information in memory devices (memory, video memory, etc.) after completing her and use.
tion and integrity protection from unauthorized access. 1.4. Program for the protection of various auxiliary facilities (except for anti-virus programs). 1.5. Protection Programs PC operating systems (modular avenue of programmatic interpretation, etc.). 1.6. Program integrity wide and application software. 1.7. Programs whistleblower resources. 1.8. Destruction program, residual information in memory devices (memory, video memory, etc.) after completing her and use.
The testing laboratory; Public corporation "All-Russian 1.4. Program for the protection of various auxiliary facilities (except for anti-virus programs). 1.5. Protection Programs PC operating systems (modular avenue of programmatic interpretation, etc.). 1.6. Program integrity wide and application software. 1.7. Programs whistleblower resources. 1.8. Destruction program, residual information in memory devices (memory, video memory, etc.) after completing her and use.
The testing laboratory; Public corporation GIS. RU. for anti-virus programs). 1.5. Protection Programs PC operating systems (modular avenue of programmatic interpretation, etc.). 1.6. Program integrity wide and application software. 1.7. Programs whistleblower resources. 1.8. Destruction program, residual information in memory devices (memory, video memory, etc.) after completing her and use.
1.5. Protection Programs PC operating systems (modular avenue of programmatic interpretation, etc.). 1.6. Program integrity wide and application software. 1.7. Programs whistleblower resources. 1.8. Destruction program, residual information in memory devices (memory, video memory, etc.) after completing her and use.
laboratory; Public corporation "All-Russian 1.5. Protection Programs PC operating systems (modular avenue of programmatic interpretation, etc.). 1.6. Program integrity wide and application software. 1.7. Programs whistleblower resources. 1.8. Destruction program, residual information in memory devices (memory, video memory, etc.) after completing her and use.
Public corporation "All-Russian GIS. RU. programmatic interpretation, etc.). 1.6. Program integrity wide and application software. 1.7. Programs whistleblower resources. 1.8. Destruction program, residual information in memory devices (memory, video memory, etc.) after completing her and use.
corporation 1.7. Programs whistleblower resources. 1.8. Destruction program, residual information in memory devices (memory, video memory, etc.) after completing her and use.
"All-Russian GIS. RU. 1.8. Destruction program, residual information in memory devices (memory, video memory, etc.) after completing her and use.
"All-Russian GIS. RU. 1.8. Destruction program, residual information in memory devices (memory, video memory, etc.) after completing her and use.
The Russian Co. 1
Scientific 1 10021 1.9. Control program and restore the file structure of the data.
Scientific Liousi Program and research at the state of the same
Research 1.10. Simulation program of a system or blocking in outcrop
Institute of 06.11.2009 servation and tamper evidence.
Automation 11/06/2014 1.11. Programs determine the facts and tamper alarm (with transfer
management in of communication) of their discovery.
non-industrial 2. Protected program information processing means:
field name 2.1. Application packages workstations.
V.V.Solomatina " 2.2. Databases computer networks.
2.3. Software tools for automated control systems.
117638, Str. 2.4. Software tools for the identification of the manufacturer
Sivashskaya, etc. software (information) of the product, including the identification of
4, Bldg. 2 copyright.
3. Software and hardware data protection:
3.1. Software and hardware tools to protect information from Nesa
only authorized to copy, including:
- protection of storage media;
- means to prevent copying of the software, with the admission to to
the PC.
3.2. Software and hardware interrupts user program in violation of
the rules of access, including:
- forced termination of the program;
- Lock your computer.
3.3. Software and hardware issuing an alarm when n about the

Registration Tool incorrect references to people and prot inated information; - means the organization of control over the actions of PC users. NAME OF TESTS Conduct studies of functional properties of products for compliance with regulatory requirements of the Federal Security Service of the Russian Federation. Name of tested product
1. Technical means of protecting information, including monitoring the effectiveness of the security measures of information:
1.1. Protection of information against interception of electromagnetic signals, including the interception of spurious electromagnetic emanations (TEMPEST), arising from the work of the technical means of recording, storing, processing, and documentation of information.
1.2. Protection of information against interception of the electrical signals generated in the cable communications:
- At the expense of TEMPEST by the work of technical means of recording, storing, processing, and documentation of information.
- Due to the effect of electro-acoustic signal conversion means and the auxiliary systems. auxiliary systems.
2. . . Technical equipment and systems in the secure execution, including:
2.1. Means scrambling or encryption masking telematics information transmitted over communication channels. 2.1. Means scrambing of encryption masking telematics information transmitted over communication channels.

2.2. Hardware video transmission on the optical channel.

3. Software data protection from unauthorized access and program bookmarks:

3.1. Programs that provide concurrent access to information.

3.2. Programme identification and authentication user terminals and for different characteristics (password extra codeword, biometric data, etc.), including a program for improving reliability of authentication (authentication).

3.3. Verification program of the system of information security and integrity protection from unauthorized access.

3.4. Program for the protection of various auxiliary facilities (for except anti-virus programs).

3.5. Protection Programs PC operating systems (modular software interpretation, etc.).

3.6. Program integrity wide and application software.

3.7. Programs whistleblower resources.

3.8. Destruction program, residual information in memory devices (memory, video memory, etc.) upon completion of its use.

3.9. Control program and restore the files of the data structure.

3.10. Simulation program information processing means: The testing laboratory; Closed GIS. RU. Joint-Stock LI0032 Company 01.02.2010 "RNT" 01.02.2015 facts.

4. Protected program information processing means:
4.1. Application packages workstations (AWS).
4.2. Databases computer networks.
4.3. Software tools for automated control systems (ACS).
4.4. Software tools for the identification of the manufacturer software (information) of the product, including the identification of copyright.
5. Software and hardware data protection:
5.1. Software and hardware tools to protect information from unauthorized copying, including:
- Protection of storage media;
- means to prevent copying of the software installed on the PC. 129515, g Moscow, Street Ostankino, etc. 6 - means to prevent copying of the software installed on the PC. 5.2. Software and hardware cryptographic and steganographic data protection (including means of concealment of information) in its storage media and data during transmission over communication channels. channels.
5.3. Software and hardware interrupts user program in violation of the rules of access, including:
- Forced termination of the program;
- Lock your computer.
5.4. Software and hardware data erasure, including:
- Erasing the residual information produced in the processing of sensitive information in memory and magnetic storage media;
- Secure erase obsolete information from magnetic media.
5.5. Software and hardware issue an alarm when an unauthorized access to information, including:
- Registration Tool incorrect references of users to protected information: information;
- A means of organizing control over the actions of PC users.
5.6. Software and hardware detection and localization of the action of

torture of unauthorized access to information, including:

software and software-engineering bookmarks. NAME OF TESTS Conduct studies of functional properties of products for compliance with regulatory requirements of the Federal Security Service of the Russian Federation.

The testing laboratory;

Closed Joint-Stock Company

GIS. RU.

LI0034

01.05.2010

01.05.2013

"TELROS"

194156, St. Petersburg, Bolshoy Prospect St. Sampson, 87, letter A Name of tested product

- 1. Technical means of protecting information, including monitoring the effectiveness of the security measures of information:
- 1.1. Protection of information against interception of electromagnetic signals, including the interception of spurious electromagnetic emanations (TEMPEST), arising from the work of the technical means of recording, storing, processing, and documentation of information.
- 1.2. Protection of information against interception of the electrical signals generated in the cable communications:
- TEMPEST at the expense of the work of technical means of recording, storing, processing, and documentation of information;
- due to the effect of electro-acoustic signal conversion means and the auxiliary systems.
- 2. Technical equipment and systems in the secure execution, including:
- 2.1. Hardware video transmission on the optical channel.
- 3. Software data protection from unauthorized access (unauthorized access) and software tabs:
- 3.1. Programs that provide concurrent access to information.
- 3.2. Program identification and authentication of terminals and users on different grounds (the password, the additional code word for bi metric data, etc.), including a program to improve the reliability of identification (authentication).
- 3.3. Screening programs are functioning security system and inform tion and integrity protection from unauthorized access.
- 3.4. Program for the protection of various auxiliary facilities (except for anti-virus programs).
- 3.5. Protection Programs PC operating systems (modular avenue of programmatic interpretation, etc.).
- 3.6. Program integrity wide and application software.
- 3.7. Programs whistleblower resources.
- 3.8. Destruction program, residual information in memory devices (memory, video memory, etc.) after completing her and use.
- 3.9. Control program and restore the file structure of the data.
- 3.10. Simulation program of a system or blocking in outcrop servation and tamper evidence.
- 3.11. Programs determine the facts and tamper alarm (with transfer of communication) of their discovery.
- 4. Protected program information processing means:
- 4.1. Application packages workstations.
- 4.2. Databases computer networks.

4.3. Software tools for automated control systems.
4.4. Software tools for the identification of the manufacturer software
(information) of the product, including the identification of copyright.
5. Software and hardware data protection:
5.1. Software and hardware tools to protect information from Nesa
only authorized to copy, including:
- protection of storage media;
- means to prevent copying of the software, with the admission to on
the PC.
5.2. Software and hardware interrupts user program in violation of the
rules of access, including:
- forced termination of the program;
- Lock your computer.
5.3. Software and hardware issuing an alarm when n about the torture
of unauthorized access to information, including:
- Registration Tool incorrect references to people and prot inated
information;
- means the organization of control over the actions of PC users.
5.4. Software and hardware detection and localization of de first
consequence of software and software-engineering bookmarks.
NAME OF TESTS
Conduct studies of functional properties of products for compliance
with regulatory requirements of the Federal Security Service of the
Russian Federation.

The testing laboratory; Limited Liability Company scientific and technical enterprise "Kriptosoft" 440026, Penza city. Lermontov, 3	GIS. RU. LI0039 22.11.2010 22/11/2013	Name of tested product 1. Software data protection from unauthorized access (unauthorized access) and software tabs: 1.1. Programs that provide concurrent access to information. 1.2. Program identification and authentication of terminals and uses ers on various grounds (the password, the additional code word for bi metric data, etc.), including a program to improve the reliability of identification (authentication). 1.3. Screening programs are functioning security system and inform tion and integrity protection from unauthorized access. 1.4. Program for the protection of various auxiliary facilities, with the exception of anti-virus programs. 1.5. Protection Programs PC operating systems (modular avenue of programmatic interpretation, etc.). 1.6. Program integrity wide and application software. 1.7. Programs whistleblower resources. 1.8. Destruction program, residual information in memory devices (memory, video memory, etc.) after completing her and use.
---	--	---

		 1.9. Control program and restore the file structure of the data. 1.10. Simulation program of a system or blocking in outcrop servation and tamper evidence. 1.11. Programs determine the facts and tamper alarm (with transfer of communication) of their discovery. 2. Protected program information processing means: 2.1. Application packages workstations. 2.2. Databases computer networks. 2.3. Software tools for automated control systems. 2.4. Software tools for the identification of the manufacturer software (information) of the product, including the identification of copyright. 3. Software and hardware data protection: 3.1. Software and hardware tools to protect information from Nesa only authorized to copy, including: protection of storage media; means to prevent copying of the software, with the admission to on the PC. 3.2. Software and hardware interrupts user program in violation of the rules of access, including:
The testing laboratory; Federal state military educational institution of higher education "Military Space Academy named after AF Mozhaysky" of the Ministry of	GIS. RU. LI0040 21.03. 2011 09.05.2013	Name of tested product 1. Software data protection from unauthorized access (unauthorized access) and software tabs: 1.1. Programs that provide concurrent access to information. 1.2. Program identification and authentication of terminals and uses ers on various grounds (the password, the additional code word for bi metric data, etc.), including a program to improve the reliability of identification (authentication). 1.3. Screening programs are functioning security system and inform tion and integrity protection from unauthorized access. 1.4. Program for the protection of various auxiliary facilities (except for anti-virus programs). 1.5. Protection Programs PC operating systems (modular avenue of programmatic interpretation, etc.). 1.6. Program integrity wide and application software. 1.7. Programs whistleblower resources. 1.8. Destruction program, residual information in memory devices (memory, video memory, etc.) after completing her and use. 1.9. Control program and restore the file structure of the data. 1.10. Simulation program of a system or blocking in outcrop servation and tamper evidence.

1.11. Programs determine the facts and tamper alarm (with transfer of communication) of their discovery. 2. Protected program information processing means:2.1. Application packages workstations. Databases computer networks. Software tools for automated control systems. 2.4. Software tools for the identification of the manufacturer software (information) of the product, including the identification of copyright. 3. Software and hardware data protection: Software and hardware tools to protect information from Nesa only authorized to copy, including: protection of storage media; means to prevent copying of the software, with the admission to on the PC. Defense of the 3.2. Software and hardware cryptographic and steganogr cific and information security (including the means of concealment of information) in its storage media and data during transmission over Russian **Federation** communication channels. Software and hardware interrupts user program in violation of the rules of access, including: 197082, St. forced termination of the program; Petersburg, ul. Lock your computer. 3.4. Software and hardware data erasure, including: Zhdanov, etc. - erasing the residual information produced in the processing of sensitive information in memory and magnetic storage media;
- secure erase obsolete information from magnetic media. 13 3.5. Software and hardware issuing an alarm when n about the torture of unauthorized access to information, including: Registration Tool incorrect references to people and prot inated information; means the organization of control over the actions of PC users. Software and hardware detection and localization of de first consequence of software and software-engineering bookmarks. NAME OF TESTS Conduct studies of functional properties of products for compliance with regulatory requirements of the Federal Security Service of the Russian Federation. Name of tested product

		Name of fested product
		1. Technical means of protecting information, including monitoring the effectiveness of the security measures of information:
		the effectiveness of the security measures of information:
		L.I., Protection of information against interception of the optical
		signals (images) in the visible, infrared and ultraviolet wavelengths.
The testing		1.2. Protection of information against interception of acoustic signals
The testing		propagating in air, water, solid media.
laboratory;		1.3. Protection of information against interception of electromagnetic
laboratory,		signals, including the interception of spurious electromagnetic
		emanations (IEMPESI), arising from the work of the technical means
		of recording, storing, processing, and documentation of information.
Closed		1.4. Protection of information against interception of the electrical
Closed		signals generated in the cable communications:
Joint-Stock		In Protection of information against interception of the optical signals (images) in the visible, infrared and ultraviolet wavelengths. 1.2. Protection of information against interception of acoustic signals propagating in air, water, solid media. 1.3. Protection of information against interception of electromagnetic signals. including the interception of spurious electromagnetic emanations (IEMPEST), arising from the work of the technical means of recording, storing, processing, and documentation of information. 1.4. Protection of information against interception of the electrical signals generated in the cable communications: - TEMPEST at the expense of the work of technical means of recording, storing, processing, and documentation of information:
Joint Stock	GIS. RU.	recording, storing, processing, and documentation of information;
Company	ois. Ro.	recording, storing, processing, and documentation of information; - due to the effect of electro-acoustic signal conversion means and the
	LI0041	I ALIXILIALV SVSIPILIS
	LI00+1	1.5. Lechnical means of detection and identification of special
WEXT DEXT A II		technical, means intended for secret information, installed in buildings
"EUREKA"		and lacinges (premises, venicles), engineering communications,
	20.02.2011	1.5. Technical means of detection and identification of special technical means intended for secret information, installed in buildings and facilities (premises, vehicles), engineering communications, interior, in household appliances, in the technical means of recording, storing processing and decumentation of the processing and decumentation.
		storing, processing, and documentation of information, communication
101022	20/02/2016	storing, processing, and documentation of information, communication systems, and in an open area. 2. Technical equipment and systems in the secure execution.
191023,		Technical equipment and systems in the secure execution,
~ C4		including: 2.1. Means scrambling or encryption masking telematics information
g St.		2.1. Means scrambling or encryption masking telematics information transmitted over communication channels, in terms of carrying out special inspections, special studies and research on the existence of
Data nalas na sal		checial inspections special studies and research on the evictories of
Petersburg, ul.		undeclared capabilities;
Dag 242 22 1		2.2. Encryption tools telematic information does not contain
Pea, etc. 32, 1.		information constituting a state secret fransmitted through
And of 15II		information. Constituting a state secret, transmitted through communication channels, in terms of carrying out special inspections,
And, of. 15H		communication channels, in terms of carrying out special inspections, special studies and research on the existence of undeclared capabilities; 2.3. Hardware video transmission on the optical channel.
		2.3 Hardware video transmission on the ontical channel
		2.3. Hardware video transmission on the optical channel. 3. Technical means of protecting information from unauthorized
		access (NSD)
		3.1. Protective equipment, including:
I	I	1 2.11. 11000011.0 oquipinono, moraum5.

Electronic locks television systems and security controls intruder detection for disruptive effects. - special means for transporting and storing the physical media (tapes treamers, magnetic and optical flaks, etc.) - special means for transporting and storing the physical media (tapes treamers, magnetic and optical flaks, etc.) - trograms that provide concurrent access to information. 4.2. Program identification and authentication of terminals and users on different grounds (the password the additional code word biometric data, etc. etc.) including a program to improve the reliability of identification (authentication). 4.3. Verification program of the system of information security and integrity protection from unauthorized access. 4.4. Program for the protection of various auxiliary facilities, with the exception of software anti-virus tools. 4.5. Protection Programs PC operating systems (modular software interpretation, etc. etc.). 4.6. Program integrity wide and application software. 4.7. Programs whistleblower resources. 4.8. Destruction program, residual information in memory devices (memory, video memory, etc. n) after its use. 4.9. Control program and restore the file structure of the data. 4.10. Simulation program of the system or lock tamper detection facts. 4.11. Programs determine the facts and tamper alarm (communication) of their discovery. 5. Protected program information processing means: 2.1. Application packages workstations. 2.2. Databases computer networks. 3.3. Software tools for automated control systems. 3.4. Software and hardware data protection: 6.1. Software and hardware tools to protect information from unauthorized copying, including: - protection, of storage media - means to prevent copying of the software installed on the PC. 6.2. Software and hardware data erasure, including: - crassing the residual information from including including and processing of the software and hardware data erasure, including: - crassing the residual information from including inc
4.1. Programs that provide concurrent access to information. 4.2. Program identification and authentication of terminals and users on different grounds (the password, the additional code word biometric data, etc. etc.), including a program to improve the reliability of identification (authentication). 4.3. Verification program of the system of information security and integrity protection from unauthorized access. 4.4. Program for the protection of various auxiliary facilities, with the exception of software anti-virus tools. 4.5. Protection Programs PC operating systems (modular software interpretation, etc. etc.). 4.6. Program integrity wide and application software. 4.7. Programs whistleblower resources. 4.8. Destruction program, residual information in memory devices (memory, video memory, etc. n) after its use. 4.9. Control program and restore the file structure of the data. 4.10. Simulation program of the system or lock tamper detection
4.1. Programs that provide concurrent access to information. 4.2. Program identification and authentication of terminals and users on different grounds (the password, the additional code word biometric data, etc. etc.), including a program to improve the reliability of identification (authentication). 4.3. Verification program of the system of information security and integrity protection from unauthorized access. 4.4. Program for the protection of various auxiliary facilities, with the exception of software anti-virus tools. 4.5. Protection Programs PC operating systems (modular software interpretation, etc. etc.). 4.6. Program integrity wide and application software. 4.7. Programs whistleblower resources. 4.8. Destruction program, residual information in memory devices (memory, video memory, etc. n) after its use. 4.9. Control program and restore the file structure of the data. 4.10. Simulation program of the system or lock tamper detection
4.1. Programs that provide concurrent access to information. 4.2. Program identification and authentication of terminals and users on different grounds (the password, the additional code word biometric data, etc. etc.), including a program to improve the reliability of identification (authentication). 4.3. Verification program of the system of information security and integrity protection from unauthorized access. 4.4. Program for the protection of various auxiliary facilities, with the exception of software anti-virus tools. 4.5. Protection Programs PC operating systems (modular software interpretation, etc. etc.). 4.6. Program integrity wide and application software. 4.7. Programs whistleblower resources. 4.8. Destruction program, residual information in memory devices (memory, video memory, etc. n) after its use. 4.9. Control program and restore the file structure of the data. 4.10. Simulation program of the system or lock tamper detection
4.1. Programs that provide concurrent access to information. 4.2. Program identification and authentication of terminals and users on different grounds (the password, the additional code word biometric data, etc. etc.), including a program to improve the reliability of identification (authentication). 4.3. Verification program of the system of information security and integrity protection from unauthorized access. 4.4. Program for the protection of various auxiliary facilities, with the exception of software anti-virus tools. 4.5. Protection Programs PC operating systems (modular software interpretation, etc. etc.). 4.6. Program integrity wide and application software. 4.7. Programs whistleblower resources. 4.8. Destruction program, residual information in memory devices (memory, video memory, etc. n) after its use. 4.9. Control program and restore the file structure of the data. 4.10. Simulation program of the system or lock tamper detection
4.1. Programs that provide concurrent access to information. 4.2. Program identification and authentication of terminals and users on different grounds (the password, the additional code word biometric data, etc. etc.), including a program to improve the reliability of identification (authentication). 4.3. Verification program of the system of information security and integrity protection from unauthorized access. 4.4. Program for the protection of various auxiliary facilities, with the exception of software anti-virus tools. 4.5. Protection Programs PC operating systems (modular software interpretation, etc. etc.). 4.6. Program integrity wide and application software. 4.7. Programs whistleblower resources. 4.8. Destruction program, residual information in memory devices (memory, video memory, etc. n) after its use. 4.9. Control program and restore the file structure of the data. 4.10. Simulation program of the system or lock tamper detection
4.6. Program integrity wide and application software. 4.7. Programs whistleblower resources. 4.8. Destruction program, residual information in memory devices (memory, video memory, etc. n) after its use. 4.9. Control program and restore the file structure of the data. 4.9. Simulation program of the system or lock tamper detection
4.6. Program integrity wide and application software. 4.7. Programs whistleblower resources. 4.8. Destruction program, residual information in memory devices (memory, video memory, etc. n) after its use. 4.9. Control program and restore the file structure of the data. 4.9. Simulation program of the system or lock tamper detection
4.6. Program integrity wide and application software. 4.7. Programs whistleblower resources. 4.8. Destruction program, residual information in memory devices (memory, video memory, etc. n) after its use. 4.9. Control program and restore the file structure of the data. 4.9. Simulation program of the system or lock tamper detection
4.6. Program integrity wide and application software. 4.7. Programs whistleblower resources. 4.8. Destruction program, residual information in memory devices (memory, video memory, etc. n) after its use. 4.9. Control program and restore the file structure of the data. 4.9. Simulation program of the system or lock tamper detection
4.6. Program integrity wide and application software. 4.7. Programs whistleblower resources. 4.8. Destruction program, residual information in memory devices (memory, video memory, etc. n) after its use. 4.9. Control program and restore the file structure of the data. 4.9. Simulation program of the system or lock tamper detection
4.6. Program integrity wide and application software. 4.7. Programs whistleblower resources. 4.8. Destruction program, residual information in memory devices (memory, video memory, etc. n) after its use. 4.9. Control program and restore the file structure of the data. 4.10. Simulation program of the system or lock tamper detection
4.6. Program integrity wide and application software. 4.7. Programs whistleblower resources. 4.8. Destruction program, residual information in memory devices (memory, video memory, etc. n) after its use. 4.9. Control program and restore the file structure of the data. 4.10. Simulation program of the system or lock tamper detection
4.6. Program integrity wide and application software. 4.7. Programs whistleblower resources. 4.8. Destruction program, residual information in memory devices (memory, video memory, etc. n) after its use. 4.9. Control program and restore the file structure of the data. 4.9. Simulation program of the system or lock tamper detection
4.6. Program integrity wide and application software. 4.7. Programs whistleblower resources. 4.8. Destruction program, residual information in memory devices (memory, video memory, etc. n) after its use. 4.9. Control program and restore the file structure of the data. 4.10. Simulation program of the system or lock tamper detection
4.8. Destruction program, residual information in memory devices (memory, video memory, etc. n) after its use. 4.9. Control program and restore the file structure of the data. 4.10. Simulation program of the system or lock tamper detection
4.8. Destruction program, residual information in memory devices (memory, video memory, etc. n) after its use. 4.9. Control program and restore the file structure of the data. 4.10. Simulation program of the system or lock tamper detection
4.8. Destruction program, residual information in memory devices (memory, video memory, etc. n) after its use. 4.9. Control program and restore the file structure of the data. 4.10. Simulation program of the system or lock tamper detection facts. 4.11. Programs determine the facts and tamper alarm (communication) of their discovery. 5. Protected program information processing means: 5.1. Application packages workstations. 5.2. Databases computer networks. 5.3. Software tools for automated control systems
(memory, video memory, etc. n) after its use. 4.9. Control program and restore the file structure of the data. 4.10. Simulation program of the system or lock tamper detection facts. 4.11. Programs determine the facts and tamper alarm (communication) of their discovery. 5. Protected program information processing means: 5.1. Application packages workstations. 5.2. Databases computer networks. 5.3. Software tools for automated control systems
4.9. Control program and restore the file structure of the data. 4.10. Simulation program of the system or lock tamper detection facts. 4.11. Programs determine the facts and tamper alarm (communication) of their discovery. 5. Protected program information processing means: 5.1. Application packages workstations. 5.2. Databases computer networks. 5.3. Software tools for automated control systems
4.10. Simulation program of the system of lock tamper detection facts. 4.11. Programs determine the facts and tamper alarm (communication) of their discovery. 5. Protected program information processing means: 5.1. Application packages workstations. 5.2. Databases computer networks. 5.3. Software tools for automated control systems
4.11. Programs determine the facts and tamper alarm (communication) of their discovery. 5. Protected program information processing means: 5.1. Application packages workstations. 5.2. Databases computer networks. 5.3. Software tools for automated control systems
(communication) of their discovery. 5. Protected program information processing means: 5.1. Application packages workstations. 5.2. Databases computer networks. 5.3. Software tools for automated control systems
5. Protected program information processing means: 5.1. Application packages workstations. 5.2. Databases computer networks. 5.3. Software tools for automated control systems
5.1. Application packages workstations. 5.2. Databases computer networks. 5.3. Software tools for automated control systems
5.2. Databases computer networks. 5.3. Software tools for automated control systems
1 3 3 Software foots for altiomated control systems
2.9. Software tools for the identification of the manufacturar of twere
J.4. Sollwale tools for the product including the identification of convigint
6 Software and hardware data protection:
6.1. Software and hardware tools to protect information from
unauthorized copying, including:
- protection of storage media - means to prevent copying of the
Software instanced on the PC.
1 u.l. s of access including.
- forced termination of the program - Lock vour computer
6.3. Software and hardware data erasure, including:
- erasing the residual information produced in the processing of
sensitive information in memory and magnetic storage media;
- secure erase obsolete information from magnetic media. 6.4. Software and hardware issue an alarm when an unauthorized access to information, including: Registration Tool incorrect references of users to protected
0.4. Software and nardware issue an alarm when an unauthorized
access to information, including. - Registration Tool incorrect references of users to protected
- means the organization of control over the actions of PC users.
6.5. Software and hardware detection and localization of the action of
software and software-engineering bookmarks.
NAME UP LESTS. Conduct studies of functional properties of products for compliance
with regulatory requirements of the Federal Security Service of the
- means the organization of control over the actions of PC users. 6.5. Software and hardware detection and localization of the action of software and software-engineering bookmarks. NAME OF LESTS Conduct studies of functional properties of products for compliance with regulatory requirements of the Federal Security Service of the Russian Federation.

		Name of tested product
The testing laboratory;	20.05.2011 05/20/2016	1. Software data protection from unauthorized access (unauthorized access) and software tabs:
3 ,		1.1. Programs that provide concurrent access to information.
The International Centre for		1.2. Program identification and authentication of terminals and uses ers on various grounds (the password, the additional code word for bi metric data, etc.), including a program to improve the reliability of identification (authentication).
Informatics and Electronics		1.3. Screening programs are functioning security system and inform tion and integrity protection from unauthorized access.
		1.4. Program for the protection of various auxiliary facilities, with the exception of software anti-virus tools.
(InterEVM)		1.5. Protection Programs PC operating systems (modular avenue of programmatic interpretation, etc.).
123557		1.6. Program integrity wide and application software.
g Str.		1.7. Programs whistleblower resources.
Presnensky Val,		1.8. Destruction program, residual information in memory devices
19		(memory, video memory, etc.) after completing her and use.
		1.9. Control program and restore the file structure of the data.
		1.10. Simulation program of a system or blocking in outcrop

	servation and tamper evidence.
	1.11. Programs determine the facts and tamper alarm (with transfer of communication) of their discovery.
	2. Protected program information processing means:
	2.1. Application packages workstations.
	2.2. Databases computer networks.
	2.3. Software tools for automated control systems.
	2.4. Software tools for the identification of the manufacturer software (information) of the product, including the identification of copyright.
	NAME OF TESTS
	Conduct studies of functional properties of products for compliance
	with regulatory requirements of the Federal Security Service of the
	Russian Federation.

Name of tested product

Program identification and authentication of terminals and

	i	1
		1. Technical means of protecting information, including monitoring
		the effectiveness of the security measures of information.
		1.1. Protection of information against interception of
		electromagnetic signals, including the interception of spurious
The testing		electromagnetic emanations (TEMPEST), arising from the work of
laboratory;		the technical means of recording, storing, processing, and
		documentation of information.
Closed		1.2. Protection of information against interception of the electrical
Joint-Stock		signals generated in tons of koprovodyaschih communications:
Company	GIS. RU.	- TEMPEST at the expense of the work of technical means of
	LI0043	recording, storing, processing, and dock at mentirovaniya
"Multidisciplinary		information;
Innovation	07.03.2011	- due to the effect of electro-acoustic signal conversion means and
Enterprise	03/07/2016	the auxiliary systems.
"SVEMEL"		2. Technical means of protecting information from unauthorized
		access (NSD).
125438,		2.1. Protective equipment, including:
Moscow, 4th		- electronic locks;
Likhachevsky per.		- the device identification;
15, Building 3		- plastic identification cards.
		3. Software data protection from unauthorized access and program
		bookmarks.
		3.1. Programs that provide concurrent access to information.
	1	

users differ h nym features (password, the additional code word,
biometric data, etc.), including a program to improve the reliability
of identification (authentication).
3.3. Screening programs are functioning system of information
protection and control purposes alia means of protection against
unauthorized access.
3.4. Program for the protection of various auxiliary facilities
(except for anti-virus programs).
3.5. Protection Programs PC operating systems (modular software
tion and interpretation, etc.).
3.6. Program integrity and system-wide application software e tion.

- 3.7. Programs whistleblower resources.
- 3.8. Destruction program, residual information in memory devices (opera tive and memory, video memory, etc.) upon completion of its use.
- 3.9. Control program and restore the file structure of the data.
- 3.10. Simulation program of the system or lock tamper detection facts.
- 3.11. Programs determine the facts and tamper alarm (communication) of their detection of b.
- 4. Protected processing software information.
- 4.1. Application packages workstations.
- 4.2. Databases computer networks.
- 4.3. Software tools for automated control systems.
- 4.4. Software tools for the identification of the manufacturer software (information) of the product, including the identification of copyright.
- 5. Software and hardware data protection.
- Software and hardware information security for about feasting, including:
- protection of storage media;
- means to prevent copying of the software installed on the PC.

NAME OF TESTS

Conduct studies of functional properties of products for compliance with regulatory requirements of the Federal Security Service of the Russian Federation.

The testing		Name of tested product
laboratory;		1. Technical means of protecting information, including monitoring the effectiveness of the security measures of information:
las stately,	GIS. RU.	1.1. Protection of information against interception of acoustic signals
The Federal		propagating in air, water, solid media. 1.2. Protection of information against interception of electromagnetic
	LI0044	signals, including the interception of spurious electromagnetic
State Unitary		signals, including the interception of spurious electromagnetic emanations (TEMPEST), arising from the work of the technical means
Enterprise	30.05.2011	of recording, storing, processing, and documentation of information.
	05/30/2016	1.3. Protection of information against interception of the electrical signals generated in the cable communications:
"Research and	03/30/2010	1 - TEMPEST at the expense of the work of technical means of
Production		recording, storing, processing, and documentation of information; - due to the effect of electro-acoustic signal conversion means and the
Enterprise"		auxiliary systems.
Enterprise		1.4. Technical means of detection and identification of special

Gamma " 117420 Str. Trade union, etc. 78, pp. 4	technical means intended for secret information, installed in buildings and facilities (premises, vehicles), engineering communications, inferior, in household appliances, in the technical means of recording, storing, processing, and documentation of information, communication systems, and in an open area. 2. Software data protection from unauthorized access (unauthorized access) and software tabs; 2.1. Programs that provide concurrent access to information. 2.2. Programs me identification and authentication user terminals and for different characteristics (password extra codeword, biometric data, etc.), including a program for improving reliability of authentication (authentication). 2.3. Verification program of the system of information security and integrity protection from unauthorized access. 2.4. Program for the protection of various auxiliary facilities (except for anti-virus programs). 2.5. Protection Programs PC operating systems (modular software interpretation, etc.). 2.6. Program integrity wide and application software. 2.7. Programs whistleblower resources. 2.8. Destruction program, residual information in memory devices (memory, video memory, etc.) upon completion of its use. 2.9. Simulation program of the system or lock tamper detection facts. 2.10. Programs determine the facts and tamper alarm (communication of their discovery. 3. Protected program information processing means: 3.1. Application packages workstations. 3.2. Databases computer networks. 3.3. Software tools for automated control systems. 3.4. Software and hardware atat protection: 4.1. Software and hardware data protection: 4.2. Software and hardware tools to protect information from unauthorized copying including: - protection of storage media; - means to prevent copying of the software installed on the PC. 4.2. Software and hardware data erasure, including: - forced termination of the program; - Lock your computer. 4.3. Software and hardware data erasure, including: - erasing the residual information produ
	software and software-engineering bookmarks.

The testing laboratory;		Name of tested product
•		1. Software data protection from unauthorized access (unauthorized
Closed	GIS. RU.	access) and software tabs:
Joint-Stock	LI0045	1.1. Programs that provide concurrent access to information.
Company		1.2. Program identification and authentication of terminals and uses
	15.04.2011	ers on various grounds (the password, the additional code word for bi
"The Moscow	15.04.2016	metric data, etc.), including a program to improve the reliability of
branch of Penza		identification (authentication).
Research		1.3. Screening programs are functioning security system and inform
Institute of		tion and integrity protection from unauthorized access.
	1	

ı

	1.4. Program for the protection of various auxiliary facilities (except
	for anti-virus programs).
	1.5. Program integrity monitoring software application.
Electrical	1.6. Programs whistleblower resources.
Engineering "	1.7. Control program and restore the file structure of the data.
	1.8. Programs determine the facts and tamper alarm (with transfer of
127018	communication) of their discovery.
g Str.	NAME OF TESTS
Sushchevskiy	Conduct studies of functional properties of products (except
Val, 16, pp.	cryptographic research) for compliance with regulatory requirements
5, 2nd Floor	of the Federal Security Service of the Russian Federation.
	SPECIAL CONDITIONS
	Research products are limited to conducting research of information
	security that does not contain information constituting a state secret.

The testing laboratory; Closed Joint-Stock Company "All-Union Institute of fiber-optic communication systems and processing information " 105066, Moscow, ul. Lower Krasnosel'skaya, etc. 13, pp. 1	for bi metric data, etc.), including a program to improve the reliability of identification (authentication). 3.3. Screening programs are functioning security system and inform tion and integrity protection from unauthorized access. 3.4. Program for the protection of various auxiliary facilities (except
--	--

- protection of storage media; - means to prevent copying of the software, with the admission to on the PC. 5.2. Software and hardware cryptographic and steganogr cific and information security (including the means of concealment of information) in its storage media and data during transmission over communication channels. 5.3. Software and hardware interrupts user program in violation of the rules of access, including: - forced termination of the program; - Lock your computer. 5.4. Software and hardware data erasure, including: - erasing the residual information produced in the processing of sensitive information in memory and magnetic storage media; - secure erase obsolete information from magnetic media. 5.5. Software and hardware issuing an alarm when n about the torture of unauthorized access to information, including: - Registration Tool incorrect references to people and prot inated information; - means the organization of control over the actions of PC users. 5.6. Software and hardware detection and localization of de first consequence of software and software-engineering bookmarks. NAME OF TESTS Conduct studies of functional properties of products (except cryptographic research) for compliance with regulatory requirements of the Federal Security Service of the Russian Federation.				
--	--	--	--	--

		T							
		Name of tested product							
		1. Technical protection of information, including a la counter the effectiveness of the measures of information security:							
		1.1. Protection of information against interception of the optical							
		signals (images) in the visible, infrared and ultraviolet wavelengths.							
		1.2. Protection of information against interception of electromagnetic signals, including the interception of stray electromagnetic radiation							
		1.1. Protection of information against interception of the optical signals (images) in the visible, infrared and ultraviolet wavelengths. 1.2. Protection of information against interception of electromagnetic signals, including the interception of stray electromagnetic radiation and n and vodka (TEMPEST), arising from the work of the technical many of recording storing processing and documentation of							
		means of recording, storing, processing, and documentation of information.							
		1.3. Protection of information against interception of the electrical							
The testing	GIS. RU.	signals generated in the cable communications:							
laboratory;		- TEMPEST at the expense of the work of technical means of recording, storing e tion, processing and documentation of							
		information;							
Federal State		- due to the effect of electro-acoustic signal conversion means and the auxiliary systems.							
Unitary		2. Software data protection from unauthorized access (unauthorized							
Enterprise	GIS. RU.	access) and software tabs:							
	LI0047	2.1. Programs that provide concurrent access to information. 2.2. Program identification and authentication of terminals and uses							
"Scientific-		2.2. Program identification and authentication of terminals and uses ers on various grounds (the password, the additional code word for bi metric data, etc.), including a program to improve the reliability of							
Production	21.07.2011 25.10.2013	metric data, etc.), including a program to improve the reliability of identification (authentication).							
Center" Delta "		2.3. Screening programs are functioning security system and infortion and integrity protection from unauthorized access.							
Center Detta		2.4. Program for the protection of various auxiliary facilities,							
110571		Including anti-virus software							
119571,		2.5. Protection Programs PC operating systems (modular avenue of programmatic interpretation, etc.).							
Moscow,		2.6. Program integrity wide and application software.							
Leninsky		2.6. Program integrity wide and application software. 2.7. Programs whistleblower resources.							
Prospect, 119,		2.8. Destruction program, residual information in memory devices (memory, video memory, etc.) after completing her and use. 2.9. Control program and restore the file structure of the data.							
Bldg. 1		2.9. Control program and restore the file structure of the data.							
		2.10. Simulation program of a system or blocking in outcrop servation and tamper evidence.							
		2.11. Programs determine the facts and tamper alarm (with transfer of)							
		communication) of their discovery.							
		3. Protected program information processing means: 3.1. Application packages workstations.							
		3.2. Databases computer networks.							
		3.3. Software tools for automated control systems. 3.4. Software tools for the identification of the manufacturer software							
		(information) of the product, including the identification of copyright.							

		 4. Software and hardware data protection: 4.1. Software and hardware tools to protect information from Nesa only authorized to copy, including: protection of storage media; means to prevent copying of the software, with the admission to on the PC. 4.2. Software and hardware cryptographic and steganogr cific and information security (including the means of concealment of information) in its storage media and data during transmission over communication channels. 4.3. Software and hardware interrupts user program in violation of the rules of access, including: forced termination of the program; Lock your computer. 4.4. Software and hardware issuing an alarm when n about the torture of unauthorized access to information, including: Registration Tool incorrect references to people and prot inated information; means the organization of control over the actions of PC users. NAME OF TESTS Conduct studies of functional properties of products for compliance with regulatory requirements of the Federal Security Service of the Russian Federation.
The testing laboratory; Limited Liability Company "Research Centre of Certification" 127106, g Str. Botany, etc. 25	GIS. RU. LI0048 13.04.2011 13.04.2016	Name of tested product 1. Technical protection of information, including a la counter the effectiveness of the measures of information security: 1.2. Protection of information against interception of acoustic signals propagating in air, water, solid media. 1.3. Protection of information against interception of electromagnetic si g nals, including the interception of stray electromagnetic radiation and n and vodka (TEMPEST), arising from the work of the technical means of recording, storing, processing, and documentation of information. 1.4. Protection of information against interception of the electrical signals generated in the cable communications: - TEMPEST at the expense of the work of technical means of recording, storing e tion, processing and documentation of information; - due to the effect of electro-acoustic signal conversion means and the auxiliary systems. 2. Technical equipment and systems in the secure execution, including: 2.1. Means scrambling or encryption mask and Telem cal information transmitted over communication channels. 3. Software data protection from unauthorized access (unauthorized access) and software tabs: 3.1. Programs that provide concurrent access to information. 3.2. Program identification and authentication of terminals and uses

		ers on various grounds (the password, the additional code word for bi metric data, etc.), including a program to improve the reliability of identification (authentication). 3.3. Screening programs are functioning security system and inform tion and integrity protection from unauthorized access. 3.4. Program for the protection of various auxiliary facilities, including anti-virus software. 3.5. Protection Programs PC operating systems (modular avenue of programmatic interpretation, etc.). 3.6. Program integrity wide and application software. 3.7. Programs whistleblower resources. 3.8. Destruction program, residual information in memory devices (memory, video memory, etc.) after completing her and use. 3.9. Control program and restore the file structure of the data. 3.10. Simulation program of a system or blocking in outcrop servation and tamper evidence. 3.11. Programs determine the facts and tamper alarm (with transfer of communication) of their discovery. 4. Protected program information processing means: 4.1. Application packages workstations (AWS). 4.2. Databases computer networks. 4.3. Software tools for automated control systems. 5. Software and hardware data protection: 5.1. Software and hardware cryptographic and steganogr cific and
		information) in its storage media and data during transmission over communication channels. NAME OF TESTS Conduct studies of functional properties of products for compliance with regulatory requirements of the Federal Security Service of the
		Russian Federation.
The testing laboratory; State state educational institution higher education Academy of the Federal Security Service of the Russian Federation	GIS. RU. LI0049 28.10.2011 01.08.2014	Name of tested product 1. Software data protection from unauthorized access (unauthorized access) and software tabs: 1.1. Programs that provide concurrent access to information. 1.2. Program identification and authentication of terminals and uses ers on various grounds (the password, the additional code word for bi metric data, etc.), including a program to improve the reliability of identification (authentication). 1.3. Screening programs are functioning security system and inform tion and integrity protection from unauthorized access. 1.4. Program for the protection of various auxiliary facilities (except for anti-virus programs). 1.5. Protection Programs PC operating systems (modular avenue of

302034, Moscow Eagle Street. Instrument making - light sensitivity, etc. 35		programmatic interpretation, etc.). 1.6. Program integrity wide and application software. 1.7. Programs whistleblower resources. 1.8. Destruction program, residual information in memory devices (memory, video memory, etc.) after completing her and use. 1.9. Control program and restore the file structure of the data. 1.10. Simulation program of a system or blocking in outcrop servation and tamper evidence. 1.11. Programs determine the facts and tamper alarm (with transfer of communication) of their discovery. 2. Protected program information processing means: 2.1. Application packages workstations. 2.2. Databases computer networks. 2.3. Software tools for automated control systems. 2.4. Software tools for the identification of the manufacturer software (information) of the product, including the identification of copyright. NAME OF TESTS Conduct studies of functional properties of products for compliance with regulatory requirements of the Federal Security Service of the Russian Federation.
The testing laboratory; Closed Joint-Stock Company "St. Petersburg regional center of information security" 195220, St. Petersburg, ul. Obrucheva, 1	GIS. RU. LI0050 13.10.2011 13/10/2016	Name of tested product 1. Technical equipment and systems in the secure execution, including: 1.1. Means scrambling or encryption mask and Telem cal information transmitted over communication channels. 2. Software data protection from unauthorized access (unauthorized access) and software tabs: 2.1. Programs that provide concurrent access to information. 2.2. Program identification and authentication of terminals and uses ers on various grounds (the password, the additional code word for bi metric data, etc.), including a program to improve the reliability of identification (authentication). 2.3. Screening programs are functioning security system and inform tion and integrity profection from unauthorized access. 2.4. Program for the protection of various auxiliary facilities (except for anti-virus programs). 2.5. Protection Programs PC operating systems (modular avenue of programmatic interpretation, etc.). 2.6. Program integrity wide and application software. 2.7. Programs whistleblower resources. 2.8. Destruction program, residual information in memory devices (memory, video memory, etc.) after completing her and use. 2.9. Control program and restore the file structure of the data. 2.10. Simulation program of a system or blocking in outcrop servation and tamper evidence. 2.11. Programs determine the facts and tamper alarm (with transfer of communication) of their discovery. 3. Protected program information processing means: 3.1. Application packages workstations. 3.2. Databases computer networks. 3.3. Software tools for automated control systems. 3.4. Software tools for the identification of the manufacturer software (information) of the product, including the identification of copyright. 4. Software and hardware data protection: 4.1. Software and hardware dots to protect information from Nesa only authorized to copy, including: protection of storage media; means to prevent copying of the software, with the admission to on

		the PC. 4.2. Software and hardware cryptographic and steganogr cific and information security (including the means of concealment of information) in its storage media and data during transmission over communication channels. 4.3. Software and hardware interrupts user program in violation of the rules of access, including: - forced termination of the program; - Lock your computer. 4.4. Software and hardware data erasure, including: - erasing the residual information produced in the processing of sensitive information in memory and magnetic storage media; - secure erase obsolete information from magnetic media. 4.5. Software and hardware issuing an alarm when n of torture unauthorized access to information, including: - Registration Tool incorrect references to people and prot inated information; - means the organization of control over the actions of PC users. 4.6. Software and hardware detection and localization of de first consequence of software and software-engineering bookmarks. NAME OF TESTS Conduct studies of functional properties of products for compliance with regulatory requirements of the Federal Security Service of the Russian Federation.
The testing laboratory; Limited Liability Company "Unser PRO" 119192, Moscow, Michurinsky prospect etc. 19, Building 1, Apt. 29	GIS. RU. LI005 1 07 .1 2 .2011 07 .1 2.2014	Name of tested product 1. Software data protection from unauthorized access (unauthorized access) and software tabs: 1.1. Programs that provide concurrent access to information. 1.2. Program identification and authentication of terminals and uses ers on various grounds (the password, the additional code word for bi metric data, etc.), including a program to improve the reliability of identification (authentication). 1.3. Screening programs are functioning security system and inform tion and integrity protection from unauthorized access. 1.4. Program for the protection of various auxiliary facilities (except for anti-virus programs). 1.5. Protection Programs PC operating systems (modular avenue of programmatic interpretation, etc.). 1.6. Program integrity wide and application software. 1.7. Programs whistleblower resources. 1.8. Destruction program, residual information in memory devices (memory, video memory, etc.) after completing her and use. 1.9. Control program and restore the file structure of the data. 1.10. Simulation program of a system or blocking in outcrop servation and tamper evidence. 1.11. Programs determine the facts and tamper alarm (with transfer of communication) of their discovery. 2. Protected program information processing means: 2.1. Application packages workstations. 2.2. Databases computer networks. 2.3. Software tools for automated control systems. 2.4. Software tools for the identification of the manufacturer software (information) of the product, including the identification of copyright. 3. Software and hardware data protection:

		 3.1. Software and hardware tools to protect information from Nesa only authorized to copy, including: protection of storage media; means to prevent copying of the software, with the admission to on the PC. 3.2. Software and hardware interrupts user program in violation of the rules of access, including: forced termination of the program; Lock your computer. 3.3. Software and hardware issuing an alarm when n about the torture of unauthorized access to information, including: Registration Tool incorrect references to people and prot inated information; means the organization of control over the actions of PC users. 3.4. Software and hardware detection and localization of de first consequence of software and software-engineering bookmarks. NAME OF TESTS Conduct studies of functional properties of products for compliance with regulatory requirements of the Federal Security Service of the Russian Federation.
The testing laboratory; Federal State Unitary Enterprise "Central Research Institute Economics, Computer Science and Control Systems" 123104, Moscow, Tver Boulevard, on 7/2	GIS. RU. LI005 2 07 .1 2 .2011 07 .1 2.2014	Name of tested product 1. Software data protection from unauthorized access (unauthorized access) and software tabs: 1.1. Programs that provide concurrent access to information. 1.2. Program identification and authentication of terminals and uses ers on various grounds (the password, the additional code word for bi metric data, etc.), including a program to improve the reliability of identification (authentication). 1.3. Screening programs are functioning security system and inform tion and integrity protection from unauthorized access. 1.4. Program for the protection of various auxiliary facilities (except for anti-virus programs). 1.5. Protection Programs PC operating systems (modular avenue of programmatic interpretation, etc.). 1.6. Program integrity wide and application software. 1.7. Programs whistleblower resources. 1.8. Destruction program, residual information in memory devices (memory, video memory, etc.) after completing her and use. 1.9. Control program and restore the file structure of the data. 1.10. Programs simulate the operation of a system or blocking in outcrop servation and tamper evidence. 1.11. Programs determine the facts and tamper alarm (with transfer of communication) of their discovery. 2. Protected program information processing means:

- 2.1. Application packages workstations.
 - 2.2. Databases computer networks.
 - 2.3. Software tools for automated control systems.
 - 2.4. Software tools for the identification of the manufacturer software (information) of the product, including the identification of copyright.
 - 3. Software and hardware data protection:
 - 3.1. Software and hardware tools to protect information from Nesa only authorized to copy, including:
 - protection of storage media;
 - means to prevent copying of the software, with the admission to on the PC.
 - 3.2. Software and hardware interrupts user program in violation of the rules of access, including:
 - forced termination of the program;
 - Lock your computer.
 - 3.3. Software and hardware issuing an alarm when n of torture unauthorized access to information, including:
 - Registration Tool incorrect references to people and prot inated information;
 - means the organization of control over the actions of PC users.
 - 3.4. Software and hardware detection and localization of de first consequence of software and software-engineering bookmarks.

NAME OF TESTS

Conduct studies of functional properties of products for compliance with regulatory requirements of the Federal Security Service of the Russian Federation.

The testing		Name of tested product 1. Information Security Technology (GIS), including the effectiveness of the control measures to protect the information.
laboratory;		1.1. GIS interception of acoustic signals propagating in air, water, solid
Federal State		media.
Unitary	GIS. RU.	1.2. Protection of information against interception of electromagnetic
Enterprise	LI005 3	signals, including the interception of spurious electromagnetic
		emanations (TEMPEST), arising from the work of the technical means
"Gostehstroy"	12 .1 2	of recording, storing, processing, and documentation of information.
	.2011	1.3. GIS interception of electrical signals generated in the cable
123242,	12 .1	communications:
Moscow, Acad.	2.2014	- TEMPEST at the expense of the work of technical means of
Kapranov		recording, storing, processing, and documentation of information;
, 3, page 1		- due to the effect of electro-acoustic signal conversion means and the
		auxiliary systems.
		2. Software data protection from unauthorized access (unauthorized

access) and software tabs:

		for different characteristics (password extra codeword, biometric data, etc.), including a program for improving reliability of authentication (authentication). 2.3. Verification program of the system of information security and integrity protection from unauthorized access. 2.4. Program for the protection of various auxiliary facilities (except for anti-virus programs). 2.5. Protection Programs PC operating systems (modular software interpretation, etc.). 2.6. Program integrity wide and application software. 2.7. Programs whistleblower resources. 2.8. Destruction program, residual information in memory devices (memory, video memory, etc.) upon completion of its use. 2.9. Control program and restore the file structure of the data. 2.10. Simulation program of the system or lock tamper detection facts. 2.11. Programs determine the facts and tamper alarm (communication) of their discovery. 3. Protected program information processing means: 3.1. Application packages workstations. 3.2. Software tools for automated control systems. NAME OF TESTS
The testing laboratory; Closed Joint-Stock Company "Informtekhnika and	GIS. RU. LI005 4 12 .1 2 .2011	NAME OF TESTS Conduct studies of functional properties of products for compliance with regulatory requirements of the Federal Security Service of the Russian Federation. Name of tested product 1. Software data protection from unauthorized access (unauthorized access) and software tabs: 1.1. Programs that provide concurrent access to information. 1.2. Program identification and authentication of terminals and users on different grounds (the password, the additional code word for bi metric data, etc.), including a program to improve the reliability of identification (authentication). 1.3. Screening programs are functioning security system and inform tion and integrity protection from unauthorized access. 1.4. Program for the protection of various auxiliary facilities (except
Communication" 107066, Str. Lower Krasnoselskaya 35	12 .1 2.2016	 1.4. Program for the protection of various auxiliary facilities (except for anti-virus programs). 1.5. Protection Programs PC operating systems (modular avenue of programmatic interpretation, etc.). 1.6. Program integrity wide and application software. 1.7. Programs whistleblower resources. 1.8. Destruction program, residual information in memory devices

(memory, video memory, etc.) after completing her and use.

2.1. Programs that provide concurrent access to information.

2.2. Programme identification and authentication user terminals and

1 0	Control	program	and	rectore	the f	ماة	etructure	of the	data
1.9.	Connor	Diogram	anu	restore	me i	пе	structure	or me	uata.

- 1.10. Simulation program of a system or blocking in outcrop servation and tamper evidence.
- 1.11. Programs determine the facts and tamper alarm (with transfer of communication) of their discovery.
- 2. Protected program information processing means:
- 2.1. Application packages workstations.
- 2.2. Databases computer networks.
- 2.3. Software tools for automated control systems.
- 2.4. Software tools for the identification of the manufacturer software (information) of the product, including the identification of copyright.

NAME OF TESTS

Conduct studies of functional properties of products for compliance with regulatory requirements of the Federal Security Service of the Russian Federation.

	•	
The testing laboratory; Closed Joint-Stock Company "Orbit" 350063, Moscow Address: Str. Komsomolskaya 40	GIS. RU. LI005 5 04 .1 0 .2011 04 .1 0.2016	Name of tested product 1. Technical means of protecting information, including monitoring the effectiveness of the security measures of information. 1.1. Protection of information against interception of acoustic signals propagating in air, water, solid media. 1.2. Protection of information against interception of electromagnetic signals, including the interception of spurious electromagnetic emanations (TEMPEST), arising from the work of the technical means of recording, storing, processing, and documentation of information. 1.3. Protection of information against interception of the electrical signals generated in the cable communications. - TEMPEST at the expense of the work of technical means of recording, storing, processing, and documentation of information; - due to the effect of electro-acoustic signal conversion means and the auxiliary systems. 1.4. Technical means of detection and identification of special technical means intended for secret information, installed in buildings and facilities (premises, vehicles), engineering communications, interior, in household appliances, in the technical means of recording, storing, processing, and documentation of information, communication systems, and in an open area. 2. Technical equipment and systems in the secure execution, including: 2. Technical equipment and systems in the secure execution, including: 3.1. Programs that proyide concurrent access to information. 3.2. Programs that proyide concurrent access to information. 3.3. Verification program for improving reliability of authentication (authentication), and authentication security and integrity protection from unauthorized access. 3.4. Program for the protection of various auxiliary facilities (except for anti-virus programs). 3.5. Protection Programs PC operating systems (modular software interpretation, etc.). 3.6. Program whistleblower resources. 3.7. Programs whistleblower resources. 3.8. Destruction program defection of the system of lock tamper detection.
		facts.
		3.11. Programs determine the facts and tamper alarm

(communication) of their discovery. 4. Protected program information processing means: 4.1. Application packages workstations. 4.2. Databases computer networks. 4.3. Software tools for automated control systems. 4.4. Software tools for automated control systems. 4.5. Software tools for automated control systems. 4.6. Software tools for the identification of the manufacturer softwa (information) of the product, including the identification of copyright 5. Software and hardware tools to protect information from unauthorized copyring, including: 5.1. Software and hardware tools to protect information from unauthorized copyring, including: 6. In means to prevent copyring of the software installed on the PC. 6. Software and hardware cryptographic and steganographic data protection (including means of concealment of information) in its storage media and data during transmission over communication storage media and data during transmission over communication of the rules of access, including: 6. Software and hardware interrupts user program in violation of the rules of access, including: 6. Forced termination of the program; 7. Lock your computer. 8. Software and hardware data erasure, including: 8. erasing the residual information produced in the processing of sensitive information in memory and magnetic storage media; 8. secure erase obsolete information from magnetic media. 8. Software and hardware issuing an alarm when trying to tamper information; including: 9. Registration Tool incorrect references of users to protected information; including: 9. Registration Tool incorrect references of users to protected information; including: 9. Registration Tool incorrect references of users to protected information; including: 9. Registration Tool incorrect references of users to protected information; including: 9. Registration Tool incorrect references of users to protected information; including: 9. Registration Tool incorrect references of users to protected information; including: 9. Registration Tool incorrect refer
--

			Name of tested product
			1. Software data protection from unauthorized access (unauthorized
T	he testing		access) and software tabs:
	aboratory;		1.1. Programs that provide concurrent access to information.
	•		1.2. Programme identification and authentication user terminals and
L	imited		for different characteristics (password extra codeword, biometric data,
L	iability	GIS. RU.	etc.), including a program for improving reliability of authentication
C	Company	LI00056	(authentication).
			1.3. Verification program of the system of information security and
"(Optionally"	01.02.2012	integrity protection from unauthorized access.
		01/02/2017	1.4. Program for the protection of various auxiliary facilities,
19	95220, St.		including anti-virus software.
P	etersburg, ul.		1.5. Protection Programs PC operating systems (modular software
G	zhatskaya, etc.		interpretation, etc.).
	21, letter D		1.6. Program integrity wide and application software.
			1.7. Programs whistleblower resources.
			1.8. Destruction program, residual information in memory devices

2.3. Software tools for automated control systems. 2.4. Software tools for the identification of the manufacturer software (information) of the product, including the identification of copyright. 3. Software and hardware data protection: 3.1. software and hardware to protect information from unauthorized copying, including: - protection of storage media; means to prevent copying of the software installed on the PC. 3.2. Software and hardware steganographic data protection (including means of concealment of information) in its storage media and data during transmission over communication channels. 3.3. Software and hardware interrupts user program in violation of the rules of access, including: - Forced termination of the program; - Lock your computer. 3.4. Software and hardware data erasure, including: erasing the residual information produced in the processing of sensitive information in memory and magnetic storage media; secure erase obsolete information from magnetic media. 3.5. Software and hardware issuing an alarm when trying to tamper information, including: Registration Tool incorrect references of users to protected information; means the organization of control over the actions of PC users. 3.6. software and hardware detection and localization of the action of software and software-engineering bookmarks. NAME OF TESTS Conduct studies of functional properties of products for compliance with regulatory requirements of the Federal Security Service of the Russian Federation. Name of tested product
1. Technical protection of information, including a la counter the effectiveness of the measures of information security:
1.1. Protection of information against interception of the optical signals (images) in the visible, infrared and ultraviolet wavelengths.
1.2. Protection of information against interception of acoustic signals propagating in air, water, solid media. The testing GIS. RU. laboratory; LI0057 The Federal 15.02.2012 **State Unitary** 02/15/2017 and n and vodka (TEMPEST), arising from the wo neans of recording, storing, processing, and documents Enterprise ormation.

Protection of information against interception of the electrical

(memory, video memory, etc.) upon completion of its use.

1.11. Programs determine the facts and tamper alarm

2. Protected program information processing means:

(communication) of their discovery.

2.2. Databases computer networks.

2.1. Application packages workstations.

facts.

1.9. Control program and restore the file structure of the data.1.10. Simulation program of the system or lock tamper detection

signals generated in the cable communications:

- TEMPEST at the expense of the work of technical means of recording, storing e tion, processing and documentation of information; due to the effect of electro-acoustic signal conversion means and the auxiliary systems.

1.5. Means of detection and identification of special technical means intended for secret information, have a fabilished in the construction of buildings and facilities (premises, vehicles), engineering communications, interior, in household applicances, in the technical means of recording, storing, processing and document ing and information and communication systems in an open area.

2. Technical equipment and systems in the sectire execution, including:

2. I. Means scrambling or encryption mask and Telem cal information transmitted over communication channels, in terms of carrying out special inspections, special studies and research on the existence of undeclared capabilities.

2. Hardware video transmission over optical kanalu, 3. software fools to protect information from unauthorized access (unauthorized access) and software tabs:

3.1. Programs that provide concurrent access to information.

3.2. Programs indeptification and authentication of terminals and users on different grounds (the password, the additional code word for bit indeptification, authentication).

3.3. Screening programs are functioning security system and inform tion and integrity protection from unauthorized access.

3.4. Programs for the protection of various fashion destination with the exception of antiquity software.

3.5. Protection Programs PC operating systems (modular avenue of priogrammatic interpretation, etc.)

3.6. programs mutegrity wide and application software.

3.7. Programs simplified the operation of a system or blocking in outrop servation and tamper evidence.

3.8. Programs determination of the facts and tamper alarm (with the transfer of communication) of their discovery.

4. Protected program information of the manufacturer software (unformation) o "Scientific and Technical Center" Atlas " 127018, Str. Obraztsova, etc. 38 the PC.

5.2. software and hardware cryptographic and steganogr cific and information security (including the means of concealment of information) in its storage media and data during transmission over communication channels.

5.3. software and hardware interrupts user program in violation of the rules of access, including:

- forced termination of the program;

- Lock your computer.

5.4. Software and hardware data erasure, including:

- erasing the residual information produced in the processing of sensitive information in memory and magnetic storage media;

- secure erase obsolete information from magnetic media.

5.5. software and hardware issuing an alarm when n of torture NSD to information, including:

- Registration Tool incorrect references to people and prot inated information;

- recovery the program of control over the actions of PC users. Registration Tool incorrect references to people and prot inated information;
- means the organization of control over the actions of PC users.
5.6. Software and hardware detection and localization of de first consequence of software and software-engineering bookmarks.
6. Software and hardware for protection against unauthorized access to systems operational-search measures (SORM) on the lines of communication:
6.1. In wireline communication systems.
6.2. In cellular communication systems.
8.3. In cellular communication systems.
8.4. In cellular communication systems.
8.5. Conduct studies of functional properties of products for compliance with regulatory requirements of the Federal Security Service of the Russian Federation.
8. PECIAL CONDITIONS.
9. The validity of this certificate of accreditation applies only to the Penza branch of the Federal State Unitary Enterprise "Scientific-Technical Center" Atlas ", 440601, Moscow Penza city. Sovetskaya 9 The testing GIS. RU. Name of tested product

Technical protection of information, including a la counter the

effectiveness of the measures of information security:

LI0058

laboratory;

public corporation "Penza Research Institute of Electrical Engineering" 440026, g Penza city. Sovetskaya 9	15.03.2012 01/07/2015	 1.1. Protection of information against interception of acoustic signals propagating in air, water, solid media. 1.2. Protection of information against interception of electromagnetic signals, including the interception of stray electromagnetic radiation and n and vodka (TEMPEST), arising from the work of the technical means of recording, storing, processing, and documentation of information. 1.3. Protection of information against interception of the electrical signals generated in the cable communications: TEMPEST at the expense of the work of technical means of recording, storing e tion, processing and documentation of information; due to the effect of electro-acoustic signal conversion means and the auxiliary systems. 2. Technical equipment and systems in the secure execution, including: 1. Means scrambling or encryption mask and Telem cal information transmitted over communication channels. 3. Protected program information processing means: 3.1. Application Packages workstations. 3.2. Databases computer networks. 3.3. Software tools for automated control systems. 4. Software and hardware data protection: 4.1. Software and hardware data protection: 4.2. Software and hardware interrupts user program in violation of the rules of access, including:
--	-----------------------	---

Russian Federation.

with regulatory requirements of the Federal Security Service of the

The testing laboratory; Public corporation "Perm Telephone Plant" TELTA " 614990, Penza city. Okulov, etc. 80	- due to the effect of electro-acoustic signal conversion means and the auxiliary systems. 2012 2012 7 due to the effect of electro-acoustic signal conversion means and the auxiliary systems.
--	--

		Conduct studies of functional properties of products for compliance with regulatory requirements of the Federal Security Service of the Russian Federation.
--	--	---

The testing laboratory;
Limited Liability Company
"Center for Special Systems Engineering"
127521 g Str. Oktyabrskaya 72

GIS. RU. LI00 61

1 1.0 4 12 .20

11 .0 4 7 .201 Name of tested product

- 1. Software data protection from unauthorized access (unauthorized access) and software tabs:
- 1.1. Programs that provide concurrent access to information.
- 1.2. Programme identification and authentication user terminals and for different characteristics (password extra codeword, biometric data, etc.), including a program for improving reliability of authentication (authentication).
- 1.3. Verification program of the system of information security and integrity protection from unauthorized access.
- 1.4. Program for the protection of various auxiliary facilities (except for anti-virus programs).
- 1.5. Protection Programs PC operating systems (modular software interpretation, etc.).
- 1.6. Program integrity wide and application software.
- 1.7. Programme whistleblower resources.
- 1.8. Programs destruction of residual information in memory devices (memory, video memory, etc.) upon completion of its use.
- 1.9. monitoring programs and restore the file structure of the data.
- 1.10. Programs simulate the operation of a system or lock tamper detection facts.
- 1.11. Programs determination of the facts and tamper alarm (communication) of their discovery.
- 2. Protected program information processing means:
- 2.1. Application packages workstations.
- 2.2. Databases computer networks.
- 2.3. Software tools for automated control systems.
- 2.4. Software tools for the identification of the manufacturer software (information) of the product, including the identification of copyright.

NAME OF TESTS

Conduct studies of functional properties of products for compliance with regulatory requirements of the Federal Security Service of the Russian

	Federation.
--	-------------

		Name of tested product
		1. Software data protection from unauthorized access (unauthorized
		access) and software tabs:
		1.1. Programs that provide concurrent access to information.
		1.2. Programme identification and authentication user terminals and
		for different characteristics (password extra codeword, biometric data,
The testing		etc.), including a program for improving reliability of authentication
laboratory;		(authentication).
		1.3. Verification program of the system of information security and
Closed		integrity protection from unauthorized access.
Joint-Stock	GIS. RU.	1.4. Program for the protection of various auxiliary facilities (except
Company	LI00 62	for anti-virus programs).
		1.5. Protection Programs PC operating systems (modular software
"Scientific and	01 .06.20	interpretation, etc.).
Production	12	1.6. Program integrity wide and application software.
Association"	01 .06.201	1.7. Programme whistleblower resources.
Echelon "	7	1.8. Programs destruction of residual information in memory devices
107022 - Cu		(memory, video memory, etc.) upon completion of its use.
107023, Str.		1.9. Programs simulate the operation of a system or lock tamper
Electrozavodskaya,		detection facts.
24, pp. 1		1.10. Programs determination of the facts and tamper alarm
		(communication) of their discovery.
		2. Protected program information processing means:
		2.1. Application packages workstations.
		2.2. Databases computer networks.
		2.3. Software tools for automated control systems.
		2.4. Software tools for the identification of the manufacturer

		software (information) of the product, including the identification of copyright. NAME OF TESTS Conduct studies of functional properties of products for compliance with regulatory requirements of the Federal Security Service of the Russian Federation.
"Center of Information Security" mask "	1. eff 1.1 pro 1.2 sig n a of 1.3 sig - rec S. RU. 100 63 2.1 acc 2.1 2 5.0 6 201 5 2.2 an 2.2 pro 2.3 an 2.4 pro 2.5 2.6 3. 3.1 3.2 3.3	1. Programs that provide concurrent access to information. 2. Screening programs are functioning security system and inform tion d integrity protection from unauthorized access. 3. Program for the protection of various auxiliary facilities (except for ti-virus programs). 4. Protection Programs PC operating systems (modular avenue of ogrammatic interpretation, etc.). 5. Program integrity wide and application software. 6. Programs whistleblower resources. Protected program information processing means: 1. Application Packages workstations.

		Federation.
The testing laboratory; Public corporation "FINANCE AND INFORMATION TECHNOLOGY" 119180, Moscow 1st Tails per., 11-A	GIS. RU. LI006 4 April 1 8 .0 .2012 1 4 .0 8 .2015	Name of tested product 1. Software data protection from unauthorized access (unauthorized access) and software tabs: 1.1. Programs that provide concurrent access to information. 1.2. Programme identification and authentication user terminals and for different characteristics (password extra codeword, biometric data, etc.), including a program for improving reliability of authentication (authentication). 1.3. Verification program of the system of information security and integrity protection from unauthorized access. 1.4. Program for the protection of various auxiliary facilities (except for anti-virus programs). 1.5. Protection Programs PC operating systems (modular software interpretation, etc.). 1.6. Program integrity wide and application software. 1.7. Programs whistleblower resources. 1.8. Programs destruction of residual information in memory devices (memory, video memory, etc.) upon completion of its use. 1.9. monitoring programs and restore the file structure of the data. 1.10. Programs simulate the operation of a system or lock tamper detection facts. 1.11. Programs determination of the facts and tamper alarm (communication) of their discovery. 2. Protected program information processing means: 2.1. Application packages workstations. 2.2. Databases computer networks. 2.3. Software tools for automated control systems. 2.4. Software and hardware data protection: 3.1. software and hardware data protection: 3.2. Software and hardware interrupts user program in violation of the rules of access, including: - protection of storage media; - means to prevent copying of the software installed on the PC. 3.2. Software and hardware data erasure, including: - forced termination of the program; - Lock your computer. 3.3. Software and hardware data erasure, including: - erasing the residual information from magnetic media. 3.4. Software and hardware issue an alarm when an unauthorized

		access to information, including: Registration Tool incorrect references of users to protected information; means the organization of control over the actions of PC users. NAME OF TESTS Conduct studies of functional properties of products for compliance with regulatory requirements of the Federal Security Service of the Russian Federation.
The testing laboratory; Limited Liability Company "Independent testing center - SPETSTEST" 249030, Kaluga region, Obninsk, Kiev highway, 64	GIS. RU. LI0065 23.08.2012 23/08/2015	Name of tested product 1. Technical means of protecting information, including monitoring the effectiveness of the security measures of information: 1.1. Protection of information against interception of acoustic signals propagating in air, water, solid media. 1.2. Protection of information against interception of electromagnetic signals, including the interception of spurious electromagnetic emanations (TEMPEST), arising from the work of the technical means of recording, storing, processing, and documentation of information. 1.3. Protection of information against interception of the electrical signals generated in the cable communications: - TEMPEST at the expense of the work of technical means of recording, storing, processing, and documentation of information; - due to the effect of electro-acoustic signal conversion means and the auxiliary systems. NAME OF TESTS Conduct studies of functional properties of products for compliance with regulatory requirements of the Federal Security Service of the Russian Federation.
The testing laboratory; Limited Liability Company "The Centre for Modern Technologies of Information Security" 127550, Str.	GIS. RU. LI006 6 30 .08.2012 30 .08.2015	Name of tested product 1. Technical protection of information, including a la counter the effectiveness of the measures of information security: 1.1. Protection of information against interception of acoustic signals propagating in air, water, solid media. 1.2. Protection of information against interception of electromagnetic signals, including the interception of stray electromagnetic radiation and n and vodka (TEMPEST), arising from the work of the technical means of recording, storing, processing, and documentation of information. 1.3. Protection of information against interception of the electrical signals generated in the cable communications:

Pryanishnikova House 23A		 TEMPEST at the expense of the work of technical means of recording, storing e tion, processing and documentation of information; due to the effect of electro-acoustic signal conversion means and the auxiliary systems. NAME OF TESTS Conduct studies of functional properties of products for compliance with regulatory requirements of the Federal Security Service of the Russian Federation.
The testing laboratory; Public corporation "Information technology and communication systems" 127287, g. , Moscow, Petrovsky Old-Razumovsky passage, 1/23, p 1	GIS. RU. LI0067 04.10.2012 04/10/2015	Name of tested product 1. Technical equipment and systems in the secure execution, including: 1.1. Means scrambling or encryption masking telematics information transmitted over communication channels. 2. Software data protection from unauthorized access (unauthorized access) and software tabs: 2.1. Programs that provide concurrent access to information. 2.2. Programme identification and authentication user terminals and for different characteristics (password extra codeword, biometric data, etc.), including a program for improving reliability of authentication (authentication). 2.3. Verification program of the system of information security and integrity protection from unauthorized access. 2.4. Program for the protection of various fashion purposes, other than anti-virus programs. 2.5. Protection Programs PC operating systems (modular software interpretation, etc.). 2.6. Program integrity wide and application software. 2.7. Programs whistleblower resources. 2.8. Destruction program, residual information in memory devices (memory, video memory, etc.) upon completion of its use. 2.9. Control program and restore the file structure of the data. 2.10. Programs simulate the operation of a system or lock tamper detection facts. 2.11. Programs determine the facts and tamper alarm (communication) of their discovery. 3. Protected program information processing means: 3.1. Application Packages workstations. 3.2. Databases computer networks. 3.3. Software tools for automated control systems. 3.4. Software tools for automated control systems. 3.5. Software tools for the identification of the manufacturer software (information) of the product, including the identification of copyright. 4. Software and hardware data protection:

		 4.1. Software and hardware cryptographic and steganographic data protection (including means of concealment of information) in its storage media and data during transmission over communication channels. 4.2. Software and hardware interrupts user program in violation of the rules of access, including: - Forced termination of the program; - Lock your computer. 4.3. Software and hardware data erasure, including: - erasing the residual information produced in the processing of sensitive information in memory and magnetic storage media; - secure erase obsolete information from magnetic media. 4.4. Software and hardware issue an alarm when an unauthorized access to information, including: - Registration Tool incorrect references of users to protected information; - A means of organizing control over the actions of PC users. 4.5. Software and hardware detection and localization of the action of software and software-engineering bookmarks. NAME OF TESTS Conduct studies of functional properties of products for compliance with regulatory requirements of the Federal Security Service of the Russian Federation. SPECIAL CONDITIONS Research products at pp 1.1 and 4.1 are limited to conducting research of information security that does not contain information
The testing laboratory; Inter-regional public institution "Institute of Engineering Physics" 142210, Moscow region., Serpukhov, Big Hammer Lane., 1A	GIS. RU. LI0068 22.10.2012 10/22/2017	Name of tested product 1. Technical protection of information, including a la counter the effectiveness of the measures of information security: 1.1. Protection of information against interception of electromagnetic signals, including the interception of stray electromagnetic radiation and n and vodka (TEMPEST), arising from the work of the technical means of recording, storing, processing, and documentation of information. 1.2. Protection of information against interception of the electrical signals generated in the cable communications: - TEMPEST at the expense of the work of technical means of recording, storing e tion, processing and documentation of information; - due to the effect of electro-acoustic signal conversion means and the auxiliary systems. 2. Software data protection from unauthorized access (unauthorized access) and software tabs: 2.1. Programs that provide concurrent access to information. 2.2. Program identification and authentication of terminals and uses ers on various grounds (the password, the additional code word for bi metric data, etc.), including a program to improve the reliability of identification (authentication). 2.3. Screening programs are functioning security system and inform tion and integrity protection from unauthorized access. 2.4. Program for the protection of various auxiliary facilities (except for anti-virus programs). 2.5. Protection Programs PC operating systems (modular avenue of programmatic interpretation, etc.). 2.6. Program integrity wide and application software.

Programs whistleblower resources. 2.8. Destruction program, residual information in memory devices (memory, video memory, etc.) after completing her and use. 2.9. Control program and restore the file structure of the data. 2.10. Programs simulate the operation of a system or blocking in outcrop servation and tamper evidence. 2.11. Programs determine the facts and tamper alarm (with transfer of communication) of their discovery. 3. Protected program information processing means: 3.1. Application Packages workstations. 3.2. Databases computer networks. Software tools for automated control systems. Software tools for the identification of the manufacturer software (information) of the product, including the identification of 4. Software and hardware data protection: 4.1. Software and hardware tools to protect information from Nesa only authorized to copy, including: protection of storage media; means to prevent copying of the software, with the admission to on the PC. 4.2. Software and hardware interrupts user program in violation of the rules of access, including: forced termination of the program; Lock your computer.

3. Software and hardware issuing an alarm when n about the torture of unauthorized access to information, including: Registration Tool incorrect references to people and prot inated information; means the organization of control over the actions of PC users. 4. 4. software and hardware detection and localization of de first consequence of software and software-engineering bookmarks. NAME OF TESTS Conduct studies of functional properties of products for compliance with regulatory requirements of the Federal Security Service of the Russian Federation. Name of tested product

		The street product
The testing laboratory;		1. Software data protection from unauthorized access (unauthorized access) and software tabs:
Closed Joint-Stock Company	GIS. RU. LI0069 15.01.2013 01/15/2016	1.1. Programs that provide concurrent access to information.1.2. Program identification and authentication of terminals and users on different grounds (the password, the additional code word for bi metric data, etc.), including a program to improve the reliability of
"AST"		identification (authentication). 1.3. Screening programs are functioning security system and inform
115522,		tion and integrity protection from unauthorized access.
Moscow,		1.4. Program for the protection of various auxiliary facilities (except
Proletarian		for anti-virus programs).
avenue, 8,		1.5. Protection Programs PC operating systems (modular avenue of
Bldg. 2		programmatic interpretation, etc.).
		1.6. Program integrity wide and application software.

outcrop servation and tamper evidence. 1.11. Programs determination of the facts and tamper alarm (with the transfer of communication) of their discovery. 2. Protected program information processing means: 2.1. Application packages workstations. 2.2. Databases computer networks. 2.3. Software tools for automated control systems. 2.4. Software tools for the identification of the manufacturer software (information) of the product, including the identification of copyright. 3. Software and hardware data protection: 3.1. software and hardware interrupts user program in violation of the rules of access, including: - forced termination of the program; - Lock your computer. 3.2. Software and hardware issuing an alarm when n about the torture of unauthorized access to information, including: Registration Tool incorrect references to people and prot inated information; means the organization of control over the actions of PC users. 3.3. Software and hardware detection and localization of software de th consequence bookmarks. NAME OF TESTS Conduct studies of functional properties of products for compliance with regulatory requirements of the Federal Security Service of the Russian Federation. The testing Name of tested product laboratory; 1. Software data protection from unauthorized access (unauthorized access) and software tabs: Limited Liability 1.1. Programs that provide concurrent access to information. GIS. RU. Company 1.2. Program identification and authentication of terminals and uses LI0070 ers on various grounds (the password, the additional code word for "M-STANDARD bi metric data, and so on), including a program to improve the 26.03.2013 holding" reliability of identification (authentication). 26/03/2018 1.3. Screening programs are functioning security system and inform 105318, Moscow, tion and integrity protection from unauthorized access. u1. 1.4. Program for the protection of various auxiliary facilities Scherbakovskaya, (except for anti-virus programs). 53, building 4

1.7. Programs whistleblower resources.

1.8. Programs destruction of residual information in memory devices (memory, video memory, etc.) after the completion of her and use.1.9. monitoring programs and restore the file structure of the data.1.10. Programs simulate the operation of a system or blocking in

- 1.5. Protection Programs PC operating systems (modular avenue of programmatic interpretation, etc.).
- 1.6. Program integrity wide and application software.
- 1.7. Programs whistleblower resources.
- 1.8. Programs destruction of residual information in memory devices (memory, video memory, etc.) after the completion of her and use.
- 1.9. monitoring programs and restore the file structure of the data.
- 1.10. Programs simulate the operation of a system or blocking in outcrop servation and tamper evidence.
- 1.11. Programs determination of the facts and tamper alarm (with the transfer of communication) of their discovery.
- 2. Protected program information processing means:
- 2.1. Application packages workstations.
- 2.2. Databases computer networks.
- 2.3. Software tools for automated control systems.
- 2.4. Software tools for the identification of the manufacturer software (information) of the product, including the identification of copyright.
- 3. Software and hardware data protection:
- 3.1. software and hardware interrupts user program in violation of the rules of access, including:
- forced termination of the program;
- Lock your computer.
- 3.2. Software and hardware issuing an alarm when n about the torture of unauthorized access to information, including:
- Registration Tool incorrect references to people and prot inated information;
- means the organization of control over the actions of PC users.
- 3.3. Software and hardware detection and localization of software de th consequence bookmarks.

NAME OF TESTS

Conduct studies of functional properties of products for compliance with regulatory requirements of the Federal Security Service of the Russian Federation.

SPECIAL CONDITIONS

The validity of this certificate of accreditation also extends to the branch of the Limited Liability Company "M - STANDARD holding" in St. Petersburg 197376, g. St. Petersburg, river embankment Karpovki house 5, the housing 22.