General information on accreditation

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. certification system for information security requirements for the safety of information constituting a state secret (ROSS RU.0003.01BI00).

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
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 04.2013)

<table>
<thead>
<tr>
<th>Name and address Organization</th>
<th>Registration number certificate of accreditation, its validity</th>
<th>Area Accreditation</th>
</tr>
</thead>
</table>
| The Federal State Unitary Enterprise | 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 without the use of methods of cryptographic transformations.  
6. Information and telecommunication systems of the state authorities of the Russian Federation, which protect the information from the use of encryption (cryptographic) means.  
7. Passive and active technical protection of information for use in information and telecommunication systems. |
| Military Unit 54939 g Moscow | AF-082 01.12.2008 01.12.2013 | Name of tested product  
Encrypted communication equipment. |
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.  
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 the protection of information is carried out without the use of methods of cryptographic transformations.  
7. Information and telecommunication systems of the state authorities of the Russian Federation, which protect the information from the use of encryption (cryptographic) means. |
8. Passive and active technical protection of information for use in and telecommunication systems.
10. Firewalls.
11. Software and hardware-software systems that implement the functions of the certification center.
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 requirements.
8. Studies of the functional properties of the product according to claims 6, 7, 10-14 for compliance with information security requirements.

Limited Liability Company
"NTC Alpha Project"
127473, Str. Seleznevskaia, 15, page 1

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 Federal State Unitary Enterprise
"Kalugapribor"
248017, Moscow Kaluga, ul. Moskovskaya 249

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.
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, 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.

<table>
<thead>
<tr>
<th>Public corporation</th>
<th>Name of tested product</th>
<th>AF-098</th>
<th>06.11.2009 11/06/2014</th>
</tr>
</thead>
</table>
| "All-Russian Scientific Research Institute of Automation management in non-industrial field name V.V.Solomatina " | 1. Firewalls.  
2. Software and hardware-software systems that implement the functions of the certification center.  
4. Software designed for use in and NFORMATION and telecommunication systems authorities of the Russian Federation. | AF-099 | 18.01.2010 18.01.2013 (Under extension) |
| Institution of the Russian Academy of Sciences  
Institute of Informatics Problems of the Russian Academy of Sciences | 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. | AF-100 | 22.06.2009 06/22/2014 |
| Closed Joint-Stock Company  
"RNT" | 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 | 129515, g Moscow, Ostankino Street 2 nd, etc. 6 |
<table>
<thead>
<tr>
<th>Limited Liability Company</th>
<th>Name of tested product</th>
</tr>
</thead>
<tbody>
<tr>
<td>&quot;M-STANDARD holding&quot;</td>
<td>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.</td>
</tr>
<tr>
<td>105318, Moscow, ul. Scherbakovskaya, 53, building 4</td>
<td>2. Information and telecommunication systems of the state authorities of the Russian Federation, which protects the information using encryption (cryptographic) means.</td>
</tr>
<tr>
<td></td>
<td>5. Software and NFORMATION and telecommunication systems, interacting with certified encryption (cryptographic) means.</td>
</tr>
</tbody>
</table>

**NAME OF TESTS**

1. Special studies on the production pp 1-9, 14.
2. Special work with the production of Claim 5.
3. Special engineering analysis products at pp 5, 6, 7, 8, 12, 13.
4. Studies of the functional properties of the product according to claims 6, 7, 9-14, 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.

---

<table>
<thead>
<tr>
<th>Closed Joint-Stock Company</th>
<th>Name of tested product</th>
</tr>
</thead>
<tbody>
<tr>
<td>&quot;TELROS&quot;</td>
<td>1. Hardware, software, and hardware and software encryption tools designed to provide cryptographic protection of information when it is transmitted over the communication channels.</td>
</tr>
<tr>
<td>194156, St. Petersburg, Bolshoy Prospect St. Sampson, House 87, letter A</td>
<td>2. Hardware, software, and hardware and software encryption tools designed to protect against unauthorized access to information during processing and storage.</td>
</tr>
<tr>
<td>AF-102</td>
<td>3. Hardware, software, and hardware and software encryption tools designed to protect against spoofing, including simulation protection means.</td>
</tr>
<tr>
<td>01.05.2010 - 01.05.2013</td>
<td>4. Hardware, software, and hardware and software encryption tools designed to protect against spoofing, including simulation protection means.</td>
</tr>
<tr>
<td></td>
<td>5. Encrypted communication equipment.</td>
</tr>
<tr>
<td></td>
<td>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.</td>
</tr>
<tr>
<td></td>
<td>7. Information and telecommunication systems of the state authorities of the Russian Federation, which protects the information using encryption (cryptographic) means.</td>
</tr>
<tr>
<td></td>
<td>8. Passive and active technical protection of information for use in information and telecommunication systems.</td>
</tr>
<tr>
<td></td>
<td>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.</td>
</tr>
<tr>
<td></td>
<td>10. Firewalls.</td>
</tr>
<tr>
<td></td>
<td>11. Systems for detection of computer attacks.</td>
</tr>
<tr>
<td></td>
<td>12. Software designed for use in information and telecommunication systems, which cooperates with certified encryption (cryptographic) means.</td>
</tr>
<tr>
<td></td>
<td>14. The hardware and software modules trusted boot the PC.</td>
</tr>
<tr>
<td></td>
<td>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.</td>
</tr>
<tr>
<td>Name of tested product</td>
<td>Name of tested product</td>
</tr>
<tr>
<td>------------------------</td>
<td>------------------------</td>
</tr>
<tr>
<td>1. Software systems that implement the functions of the certification center.</td>
<td>1. Hardware, software, and hardware and software encryption tools designed to provide cryptographic protection of information when it is transmitted over the communication channels.</td>
</tr>
<tr>
<td>2. Software information and telecommunication systems, interacting with certified encryption (cryptographic) means.</td>
<td>2. Hardware, software, and hardware and software encryption tools designed to protect against unauthorized access to information during processing and storage.</td>
</tr>
<tr>
<td>3. Software designed for use in information and telecommunication systems, organs of state power of the Russian Federation.</td>
<td>3. Hardware, software, and hardware and software encryption tools designed to protect against spoofing, including simulation protection means.</td>
</tr>
<tr>
<td>NAME OF TESTS</td>
<td>NAME OF TESTS</td>
</tr>
<tr>
<td>1. Cryptographic research products at pp 1, 2, 3, 4, 7, 12.</td>
<td>1. Cryptographic research products at pp 1, 2, 3, 4, 7, 12.</td>
</tr>
<tr>
<td>2. Engineering and cryptographic research products at pp 1, 2, 3, 4, 7, 12.</td>
<td>2. Engineering and cryptographic research products at pp 1, 2, 3, 4, 7, 12.</td>
</tr>
<tr>
<td>3. Special engineering analysis products at pp 5, 6, 10, 11.</td>
<td>3. Special engineering analysis products at pp 5, 6, 10, 11.</td>
</tr>
<tr>
<td>SPECIAL CONDITIONS</td>
<td>SPECIAL CONDITIONS</td>
</tr>
<tr>
<td>The validity of this certificate of accreditation applies only to the research of information security that does not contain information constituting a state secret.</td>
<td>The hardware and software modules trusted boot the PC.</td>
</tr>
<tr>
<td>Name of tested product</td>
<td>Name of tested product</td>
</tr>
<tr>
<td>------------------------</td>
<td>------------------------</td>
</tr>
<tr>
<td>1. Software designed for use in and INFORMATION and telecommunication systems authorities of the Russian Federation in which information is processed, not containing information constituting a state secret.</td>
<td>1. Software and NFORMATION and telecommunication systems in which information is processed, not containing information constituting a state secret, interacting with certified cryptographic protection of information.</td>
</tr>
<tr>
<td>2. Software designed for use in and INFORMATION and telecommunication systems authorities of the Russian Federation in which information is processed, not containing information constituting a state secret.</td>
<td>2. Software designed for use in and NFORMATION and telecommunication systems authorities of the Russian Federation in which information is processed, not containing information constituting a state secret.</td>
</tr>
<tr>
<td>5. Systems for detection of computer attacks.</td>
<td>5. Systems for detection of computer attacks.</td>
</tr>
<tr>
<td>6. Software and hardware-software systems that implement the functions of the certification center.</td>
<td>6. Software and hardware-software systems that implement the functions of the certification center.</td>
</tr>
<tr>
<td>7. Software information and telecommunication systems, which cooperates with certified encryption (cryptographic) means.</td>
<td>7. Software information and telecommunication systems, which cooperates with certified encryption (cryptographic) means.</td>
</tr>
<tr>
<td>9. The hardware and software modules trusted boot the PC.</td>
<td>9. The hardware and software modules trusted boot the PC.</td>
</tr>
<tr>
<td>NAME OF TESTS</td>
<td>NAME OF TESTS</td>
</tr>
<tr>
<td>1. Engineering and cryptographic research products at pp 1, 2, 3, 4, 8, 13.</td>
<td>1. Engineering and cryptographic research products at pp 1, 2, 3, 4, 8, 13.</td>
</tr>
<tr>
<td>2. Special engineering analysis products at pp 5, 6, 11, 12.</td>
<td>2. Special engineering analysis products at pp 5, 6, 11, 12.</td>
</tr>
<tr>
<td>3. Studies of hardware and software product of claim 7 for compliance with information security requirements.</td>
<td>3. Studies of the functional properties of the product according to claims 7-12 for compliance with information security requirements.</td>
</tr>
<tr>
<td>4. Studies of the functional properties of the product according to claims 8-13 for compliance with information security requirements.</td>
<td>4. Studies of the functional properties of the product according to claims 8-13 for compliance with information security requirements.</td>
</tr>
</tbody>
</table>
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 the protection of information is carried out using the use of the protected equipment and 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 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, 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.
10. Firewalls.
11. Systems for detection of computer attacks.
12. Software information and telecommunication systems, in order to ensure protection of information using encryption (cryptographic) means.

**NAME OF TESTS**

1. Special studies on the production pp 1, 2, 3, 4, 6, 7, 8, 10.
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, 12, 13.
5. Studies hardware product of claim 9 for compliance with information security requirements.
6. 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, Propekt Mira house 105, page 1

<table>
<thead>
<tr>
<th>Name of tested product</th>
</tr>
</thead>
<tbody>
<tr>
<td>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.</td>
</tr>
</tbody>
</table>

**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 Centre for Informatics and Electronics (InterEVM)**
123557 g Str. Presnensky Val, September 1

<table>
<thead>
<tr>
<th>Name of tested product</th>
</tr>
</thead>
<tbody>
<tr>
<td>Information and telecommunication systems of the state authorities of the Russian Federation in which the protection of information is carried out using the use of the protected equipment and organizational measures without the use of methods of cryptographic transformations.</td>
</tr>
</tbody>
</table>

**NAME OF TESTS**

1. Information and telecommunication systems of the state authorities of the Russian Federation, which protects the information using encryption (cryptographic) means.
2. Equipment institutional digital automatic telephone exchanges for use in government of the Russian Federation; specialized monitoring tools (blocking) control signals transmitted over interoffice trunks.
3. Firewalls.
4. 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.
<table>
<thead>
<tr>
<th>Name of tested product</th>
<th>NAME OF TESTS</th>
</tr>
</thead>
<tbody>
<tr>
<td>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.</td>
<td>1. Special studies on the production pp 1, 2, 3, 5, 8.</td>
</tr>
<tr>
<td>2. Information and telecommunication systems of the state authorities of the Russian Federation, which protects the information using encryption (cryptographic) means.</td>
<td>2. Studies hardware product of claim 4 for compliance with information security requirements.</td>
</tr>
<tr>
<td>3. Passive and active technical protection of information for use in information and telecommunication systems.</td>
<td>3. Research software product of claim 4 for compliance with information security requirements.</td>
</tr>
<tr>
<td>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.</td>
<td>4. Studies of the functional properties of the product according to claims 5-8 for compliance with information security requirements.</td>
</tr>
<tr>
<td>5. Firewalls.</td>
<td></td>
</tr>
<tr>
<td>6. Software information and communications systems, which cooperates with certified encryption (cryptographic) means.</td>
<td></td>
</tr>
<tr>
<td>7. Software designed for use in information and telecommunication systems, organs of state power of the Russian Federation.</td>
<td></td>
</tr>
<tr>
<td>8. The hardware and software modules trusted boot the PC.</td>
<td></td>
</tr>
<tr>
<td>Name of tested product</td>
<td></td>
</tr>
<tr>
<td>1. Hardware, software, and hardware and software encryption tools designed to provide cryptographic protection of information when it is transmitted over the communication channels.</td>
<td>1. Special studies on the production pp 1, 2, 3, 5, 8.</td>
</tr>
<tr>
<td>2. Hardware, software, and hardware and software encryption tools designed to protect against unauthorized access to information during processing and storage.</td>
<td>2. Studies hardware product of claim 4 for compliance with information security requirements.</td>
</tr>
<tr>
<td>3. Hardware, software, and hardware and software encryption tools designed to protect against spoofing, including simulation protection means.</td>
<td>3. Research software product of claim 4 for compliance with information security requirements.</td>
</tr>
<tr>
<td>4. Hardware, software, and hardware and software digital signature.</td>
<td>4. Studies of the functional properties of the product according to claims 5-8 for compliance with information security requirements.</td>
</tr>
<tr>
<td>5. Encrypted communication equipment.</td>
<td></td>
</tr>
<tr>
<td>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.</td>
<td></td>
</tr>
<tr>
<td>7. Information and telecommunication systems of the state authorities of the Russian Federation, which protects the information using encryption (cryptographic) means.</td>
<td></td>
</tr>
<tr>
<td>8. Passive and active technical protection of information for use in and NFORMATION and telecommunication systems.</td>
<td></td>
</tr>
<tr>
<td>10. Firewalls.</td>
<td></td>
</tr>
</tbody>
</table>
11. Systems for detection of computer attacks.
12. Software systems that implement the functions of the certification center.
13. Software and NFORMATION and telecommunication systems, which cooperates with certified encryption (cryptographic) means.
15. 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, 10, 15.
2. Special studies on the production pp 1, 2, 3, 4, 6, 7, 8, 10, 15.
3. Studies linear signal output by pp 1, 2, 3, 4, 6, 10, 15.
4. Special work with the production of Claim 5.
5. Special engineering analysis products at pp 5, 6, 7, 8, 9.
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 claim 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

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

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 use of encryption (cryptographic) means.
8. Passive and active technical protection of information for use in information and telecommunication systems.
| 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.
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.
6. Studies of the functional properties of the product according to claims 10-12 for compliance with information security requirements.

**SPECIAL CONDITIONS**

Special studies on the production pp 1, 2, 3, 4, and special work product of claim 5 restricts research in information security, does not contain information constituting a state secret.

---

<table>
<thead>
<tr>
<th>Name of tested product</th>
<th>1. Information and telecommunication systems of the state authorities of the Russian Federation.</th>
</tr>
</thead>
<tbody>
<tr>
<td>2. Information and telecommunication systems of the state authorities of the Russian Federation, which protects the information using encryption (cryptographic) means.</td>
<td></td>
</tr>
<tr>
<td>3. Passive and active technical protection of information for use in information and telecommunication systems.</td>
<td></td>
</tr>
<tr>
<td>5. Software anti-virus tools.</td>
<td></td>
</tr>
<tr>
<td>6. Software and hardware-software systems that implement the functions of the certification center.</td>
<td></td>
</tr>
<tr>
<td>7. Software information and telecommunication systems, which cooperates with certified encryption (cryptographic) means.</td>
<td></td>
</tr>
<tr>
<td>8. Software designed for use in information and telecommunication systems, organs of state power of the Russian Federation.</td>
<td></td>
</tr>
<tr>
<td>9. The hardware and software modules trusted boot the PC.</td>
<td></td>
</tr>
</tbody>
</table>

**NAME OF TESTS**

1. Cryptographic research products at pp 1, 2, 3, 4, 14.
2. Engineering and cryptographic research products at pp 1, 2, 3, 4, 14.
3. Special studies on the production pp 1, 2, 3, 4, 6, 7, 8, 14.
4. Studies linear signal output by pp 1, 2, 3, 4, 7, 14.
5. Special work with the production of Claim 5.
6. Special engineering analysis products at pp 5, 6, 7, 8, 9.
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.

**SPECIAL CONDITIONS**

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.
<table>
<thead>
<tr>
<th>Name of tested product</th>
<th>1. Software and hardware-software systems that implement the functions of the certification center.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name of tested product</td>
<td>1. Software and hardware and software encryption tools designed to provide cryptographic protection of information when it is transmitted over the communication channels.</td>
</tr>
<tr>
<td>Name of tested product</td>
<td>2. Software and hardware and software encryption tools designed to protect against unauthorized access to information during processing and storage.</td>
</tr>
<tr>
<td>Name of tested product</td>
<td>3. Information and telecommunication systems of the state authorities of the Russian Federation, which protects the information from the use of encryption (cryptographic) means.</td>
</tr>
<tr>
<td>Name of tested product</td>
<td>4. Information and telecommunication systems of the state authorities of the Russian Federation, which protects the information using encryption (cryptographic) means.</td>
</tr>
<tr>
<td>Name of tested product</td>
<td>5. Firewalls.</td>
</tr>
<tr>
<td>Name of tested product</td>
<td>6. Software information and telecommunication systems, which cooperates with certified cryptographic protection of information.</td>
</tr>
<tr>
<td>Name of tested product</td>
<td>7. Software designed for use in information and telecommunication systems, organs of state power of the Russian Federation.</td>
</tr>
<tr>
<td>Name of tested product</td>
<td>8. Passive and active technical protection of information for use in information and telecommunication systems.</td>
</tr>
<tr>
<td>Name of tested product</td>
<td>9. Software information and telecommunication systems, which cooperates with certified encryption (cryptographic) means.</td>
</tr>
<tr>
<td>Name of tested product</td>
<td>10. Software designed for use in information and telecommunication systems, organs of state power of the Russian Federation.</td>
</tr>
</tbody>
</table>

**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.
<table>
<thead>
<tr>
<th>Limited Liability Company</th>
<th>Name of tested product</th>
<th>Name of tested product</th>
</tr>
</thead>
<tbody>
<tr>
<td>&quot;Unser PRO&quot;</td>
<td>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.</td>
<td>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.</td>
</tr>
<tr>
<td>119192, Moscow, Michurinsky prospect etc. 19, Building 1, Apt. 29</td>
<td>2. Information and telecommunication systems of the state authorities of the Russian Federation, which protects the information from the use of encryption (cryptographic) means.</td>
<td>2. Information and telecommunication systems of the state authorities of the Russian Federation, which protects the information from the use of encryption (cryptographic) means.</td>
</tr>
<tr>
<td></td>
<td>3. Software information and telecommunication systems, which cooperates with certified encryption (cryptographic) means.</td>
<td>3. Software information and telecommunication systems, which cooperates with certified encryption (cryptographic) means.</td>
</tr>
<tr>
<td></td>
<td>NAME OF TESTS</td>
<td>NAME OF TESTS</td>
</tr>
<tr>
<td></td>
<td>1. Special engineering analysis products at pp 1 and 2.</td>
<td>1. Special engineering analysis products at pp 1 and 2.</td>
</tr>
<tr>
<td></td>
<td>2. Studies of the functional properties of the product according to claims 3 and 4 in compliance with information security requirements.</td>
<td>2. Studies of the functional properties of the product according to claims 3 and 4 in compliance with information security requirements.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Federal State Unitary Enterprise</th>
<th>Name of tested product</th>
<th>Name of tested product</th>
</tr>
</thead>
<tbody>
<tr>
<td>&quot;Central Research Institute Economics, Computer Science and Control Systems&quot;</td>
<td>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.</td>
<td>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.</td>
</tr>
<tr>
<td>123104, Moscow, Tver Boulevard, 7/2</td>
<td>2. Information and telecommunication systems of the state authorities of the Russian Federation, which protects the information from the use of encryption (cryptographic) means.</td>
<td>2. Information and telecommunication systems of the state authorities of the Russian Federation, which protects the information from the use of encryption (cryptographic) means.</td>
</tr>
<tr>
<td></td>
<td>3. Firewalls.</td>
<td>3. Firewalls.</td>
</tr>
<tr>
<td></td>
<td>5. Software and hardware-software systems that implement the functions of the certification center.</td>
<td>5. Software and hardware-software systems that implement the functions of the certification center.</td>
</tr>
<tr>
<td></td>
<td>6. Software information and telecommunication systems, which cooperates with certified encryption (cryptographic) means.</td>
<td>6. Software information and telecommunication systems, which cooperates with certified encryption (cryptographic) means.</td>
</tr>
<tr>
<td></td>
<td>7. Software designed for use in information and telecommunication systems, organs of state power of the Russian Federation.</td>
<td>7. Software designed for use in information and telecommunication systems, organs of state power of the Russian Federation.</td>
</tr>
<tr>
<td></td>
<td>NAME OF TESTS</td>
<td>NAME OF TESTS</td>
</tr>
<tr>
<td></td>
<td>1. Special engineering analysis products at pp 1 and 2.</td>
<td>1. Special engineering analysis products at pp 1 and 2.</td>
</tr>
<tr>
<td></td>
<td>2. Studies of the functional properties of the product according to claims 3-7 for compliance with information security requirements.</td>
<td>2. Studies of the functional properties of the product according to claims 3-7 for compliance with information security requirements.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Federal State Unitary Enterprise</th>
<th>Name of tested product</th>
<th>Name of tested product</th>
</tr>
</thead>
<tbody>
<tr>
<td>&quot;Gostehstroy&quot;</td>
<td>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.</td>
<td>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.</td>
</tr>
<tr>
<td>123242, Moscow, Acad. Kapranov, 3, page 1</td>
<td>2. Information and telecommunication systems of the state authorities of the Russian Federation, which protects the information from the use of encryption (cryptographic) means.</td>
<td>2. Information and telecommunication systems of the state authorities of the Russian Federation, which protects the information from the use of encryption (cryptographic) means.</td>
</tr>
<tr>
<td></td>
<td>3. Passive and active technical protection of information for use in information and telecommunication systems.</td>
<td>3. Passive and active technical protection of information for use in information and telecommunication systems.</td>
</tr>
<tr>
<td></td>
<td>5. Software designed for use in information and telecommunication systems, organs of state power of the Russian Federation.</td>
<td>5. Software designed for use in information and telecommunication systems, organs of state power of the Russian Federation.</td>
</tr>
</tbody>
</table>
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"

<table>
<thead>
<tr>
<th>Name of tested product</th>
<th>Name of tested product</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. Information and telecommunication systems of governmental authorities of the Russian Federation in which information security is identified with the use of the protected equipment and organizational measures without the use of cryptographic methods of conversion.</td>
<td>1. Information and telecommunication systems of government 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.</td>
</tr>
<tr>
<td>2. Information and telecommunication systems of governmental authorities of the Russian Federation, which provides protection and information using encryption (cryptographic) means.</td>
<td>2. Information and telecommunication systems of the state authorities of the Russian Federation, which protects the information using encryption (cryptographic) means.</td>
</tr>
<tr>
<td>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.</td>
<td>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.</td>
</tr>
<tr>
<td>5. Software information and telecommunication systems, which cooperates with certified encryption (cryptographic) means.</td>
<td>5. Software information and telecommunication systems, which cooperates with certified encryption (cryptographic) means.</td>
</tr>
</tbody>
</table>

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.

### Closed Joint-Stock Company "Orbit"

<table>
<thead>
<tr>
<th>Name of tested product</th>
<th>Name of tested product</th>
</tr>
</thead>
<tbody>
<tr>
<td>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.</td>
<td>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.</td>
</tr>
<tr>
<td>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.</td>
<td>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.</td>
</tr>
<tr>
<td>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.</td>
<td>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.</td>
</tr>
<tr>
<td>4. The hardware and the hardware and software of digital signature designed to protect information that does not contain information constituting a state secret.</td>
<td>4. The hardware and the hardware and software of digital signature designed to protect information that does not contain information constituting a state secret.</td>
</tr>
<tr>
<td>5. Encrypted communication equipment.</td>
<td>5. Encrypted communication equipment.</td>
</tr>
<tr>
<td>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.</td>
<td>6. Information and telecommunication systems of the state authorities of the Russian Federation, which protects the information using encryption (cryptographic) means.</td>
</tr>
<tr>
<td>7. Information and telecommunication systems of the state authorities of the Russian Federation, which protects the information using encryption (cryptographic) means.</td>
<td>7. Information and telecommunication systems of the state authorities of the Russian Federation, which protects the information using encryption (cryptographic) means.</td>
</tr>
<tr>
<td>10. Firewalls.</td>
<td>10. Firewalls.</td>
</tr>
<tr>
<td>11. Software information and telecommunication systems, which cooperates with certified encryption (cryptographic) means.</td>
<td>11. Software information and telecommunication systems, which cooperates with certified encryption (cryptographic) means.</td>
</tr>
<tr>
<td>Limited Liability Company</td>
<td>Name of tested product</td>
</tr>
<tr>
<td>---------------------------</td>
<td>------------------------</td>
</tr>
<tr>
<td>&quot;Optionally&quot;</td>
<td>AF-128</td>
</tr>
<tr>
<td>195220, St. Petersburg, ul. Gzhatskaya, etc. 21, letter B</td>
<td>01.02.2012 01/02/2017</td>
</tr>
<tr>
<td></td>
<td>Name of tested product</td>
</tr>
<tr>
<td></td>
<td>1. Software anti-virus tools.</td>
</tr>
<tr>
<td></td>
<td>2. Firewalls.</td>
</tr>
<tr>
<td></td>
<td>4. Software and hardware-software systems that implement the functions of the certifying center, intended to protect the information does not contain information constituting a state secret.</td>
</tr>
<tr>
<td></td>
<td>5. Software and information and telecommunication systems, interacting with certified encryption (cryptographic) means.</td>
</tr>
<tr>
<td></td>
<td>NAME OF TESTS</td>
</tr>
<tr>
<td></td>
<td>Studies of the functional properties of the products for compliance with information security requirements.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>public corporation</th>
<th>Name of tested product</th>
</tr>
</thead>
<tbody>
<tr>
<td>&quot;Penza Research Institute of Electrical Engineering&quot;</td>
<td>AF-129</td>
</tr>
<tr>
<td>440026, Penza city. Sovetskaya 9</td>
<td>15.03.2012 01/07/2015</td>
</tr>
<tr>
<td></td>
<td>Name of tested product</td>
</tr>
<tr>
<td></td>
<td>1. Hardware, software, and hardware and software encryption tools designed to provide cryptographic protection of information when it is transmitted over the communication channels.</td>
</tr>
<tr>
<td></td>
<td>2. Hardware, software, and hardware and software encryption tools designed to protect against unauthorized access to information during processing and storage.</td>
</tr>
<tr>
<td></td>
<td>3. Hardware, software, and hardware and software encryption tools designed to protect against spoofing, including simulation protection means.</td>
</tr>
<tr>
<td></td>
<td>4. Hardware, software, and hardware and software digital signature.</td>
</tr>
<tr>
<td></td>
<td>5. Encrypted communication equipment.</td>
</tr>
<tr>
<td></td>
<td>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.</td>
</tr>
<tr>
<td></td>
<td>7. Information and telecommunication systems of the state authorities of the Russian Federation, which protects the information using encryption (cryptographic) means.</td>
</tr>
<tr>
<td></td>
<td>8. Passive and active technical protection of information for use in information and telecommunication systems.</td>
</tr>
<tr>
<td></td>
<td>10. Firewalls.</td>
</tr>
<tr>
<td></td>
<td>11. Software and hardware-software systems that implement the functions of the certifying center.</td>
</tr>
<tr>
<td></td>
<td>12. Software information and telecommunication systems, interacting with certified encryption (cryptographic) means.</td>
</tr>
<tr>
<td></td>
<td>14. The hardware and software modules trusted boot the PC.</td>
</tr>
<tr>
<td></td>
<td>NAME OF TESTS</td>
</tr>
<tr>
<td></td>
<td>1. Cryptographic research products at pp 1, 2, 3, 4, 10, 14.</td>
</tr>
<tr>
<td></td>
<td>2. Engineering and cryptographic research products at pp 1, 2, 3, 4, 10, 14.</td>
</tr>
<tr>
<td></td>
<td>3. Special studies on the production pp 1, 2, 3, 4, 6, 7, 8, 10, 14.</td>
</tr>
<tr>
<td></td>
<td>4. Studies linear signal output by pp 1, 2, 3, 4, 7, 14.</td>
</tr>
<tr>
<td></td>
<td>5. Accessibility of the products of claim 5.</td>
</tr>
<tr>
<td></td>
<td>6. Special engineering analysis products at pp 5, 6, 7, 13, 14.</td>
</tr>
</tbody>
</table>
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.

<table>
<thead>
<tr>
<th>Public corporation</th>
<th>Name of tested product</th>
</tr>
</thead>
<tbody>
<tr>
<td>&quot;Perm Telephone Plant&quot; TELTA &quot;</td>
<td>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.</td>
</tr>
<tr>
<td>614990, Penza city. Okulov, etc. 80</td>
<td>Equipment institutional digital automatic telephone exchanges for use in government of the Russian Federation; specialized monitoring tools (blocking) control signals transmitted over interoffice trunks.</td>
</tr>
<tr>
<td>15.03.2012 15/03/2017</td>
<td>Passive and active technical protection of information for use in information and telecommunication systems.</td>
</tr>
<tr>
<td></td>
<td>Software designed for use in and NFORMATION and telecommunication systems authorities of the Russian Federation.</td>
</tr>
<tr>
<td></td>
<td>NAME OF TESTS</td>
</tr>
<tr>
<td></td>
<td>1. Special studies on the production pp 1 and 3.</td>
</tr>
<tr>
<td></td>
<td>2. Special engineering analysis products at pp 1, 2, 3.</td>
</tr>
<tr>
<td></td>
<td>3. Studies of hardware and software product of claim 2 for compliance with information security requirements.</td>
</tr>
<tr>
<td></td>
<td>4. Studies of the functional properties of the product according to claims 1, 4 in compliance with information security requirements.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Public corporation</th>
<th>Name of tested product</th>
</tr>
</thead>
<tbody>
<tr>
<td>&quot;Saturn&quot;</td>
<td>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.</td>
</tr>
<tr>
<td>107,553, g Str. Much Cherkizovskaja, 21, Building 1</td>
<td>Passive and active technical protection of information for use in information and telecommunication systems.</td>
</tr>
<tr>
<td>10.04.2012 10/04/2017</td>
<td>NAME OF TESTS</td>
</tr>
<tr>
<td>Special research products.</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Limited Liability Company &quot;Center for Special Systems Engineering&quot;</th>
<th>Name of tested product</th>
</tr>
</thead>
<tbody>
<tr>
<td>127521 g Str. Oktyabrskaya 72</td>
<td>Firewalls.</td>
</tr>
<tr>
<td>AF-133</td>
<td>Systems for detection of computer attacks.</td>
</tr>
<tr>
<td>11.04.2012 11/04/2017</td>
<td>Software and hardware-software systems that implement the functions of the certification center.</td>
</tr>
<tr>
<td></td>
<td>Software information and telecommunication systems, interacting with certified encryption (cryptographic) means.</td>
</tr>
<tr>
<td></td>
<td>Software designed for use in information and telecommunication systems, organs of state power of the Russian Federation.</td>
</tr>
<tr>
<td></td>
<td>NAME OF TESTS</td>
</tr>
<tr>
<td></td>
<td>Studies of the functional properties of the products for compliance with information security requirements.</td>
</tr>
</tbody>
</table>
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 using encryption (cryptographic) means.
8. Passive and active technical protection of information for use in information and telecommunication systems.
10. Firewalls.
11. Systems for detection of computer attacks.
12. Software and hardware-software systems that implement the functions of the certification center.
15. The hardware and software modules trusted boot the PC.

NAME OF TESTS
1. Cryptographic research products at pp 1, 2, 3, 4, 10, 15.
2. Engineering and cryptographic research products at pp 1, 2, 3, 4, 10, 15.
3. Special studies on the production pp 1, 2, 3, 4, 6, 7, 8, 10, 15.
4. Studies linear signal output by pp 1, 2, 3, 4, 7, 15.
5. Special work with the production of Claim 5.
6. Special engineer the product according to claims 5, 6, 7, 8, 9, 12.
7. Studies of hardware products according to claim 9 for compliance with information security requirements.
8. Studies of software product according to claim 9 for compliance with information security requirements.
9. Studies of the functional properties of the products at pp 10-15 for compliance with information security requirements.

SPECIAL CONDITIONS
<table>
<thead>
<tr>
<th>Company</th>
<th>Name of Tested Product</th>
<th>Name of Tests</th>
</tr>
</thead>
</table>
| Closed Joint-Stock Company "Kalugapriborsvyaz" | Equipment institutional digital automatic telephone exchanges for use in the bodies of state power at the state of the Russian Federation; specialized monitoring tools (blocking) control signals transmitted over interoffice trunks. | 1. Conducting research hardware for compliance with information security requirements.  
2. Conducting research software tools for compliance with information security requirements.                                                                 |
| Closed Joint-Stock Company "Scientific and Production Association" Echelon | Name of Tested Product                                                                                                                                                                                                 | Name of Tests                                                                                                                                                                                                 |
| Closed Joint-Stock Company "Scientific and Production Association" Echelon | Name of Tested Product                                                                                                                                                                                                 | Name of Tests                                                                                                                                                                                                 |
| Limited Liability Company "Center of Information Security" mask | Name of Tested Product                                                                                                                                                                                                 | Name of Tests                                                                                                                                                                                                 |
| Public corporation "FINANCE AND INFORMATION TECHNOLOGY" | Name of Tested Product                                                                                                                                                                                                 | Name of Tests                                                                                                                                                                                                 |

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.  
7. Software and hardware-software systems that implement the functions of the certification center.
<p>| | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>6.</td>
<td>Software information and telecommunication systems, which cooperates with certified encryption (cryptographic) means.</td>
</tr>
<tr>
<td>7.</td>
<td>Software designed for use in information and telecommunication systems, organs of state power of the Russian Federation.</td>
</tr>
</tbody>
</table>

**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

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 the simulation protection.
4. Hardware, software, and hardware and software digital signature.
5. Information and telecommunication systems of the state authorities of the Russian Federation in which data protection is performed using secure 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 (cryptographic) means.
7. Software information and telecommunication systems, which cooperates with certified encryption (cryptographic) means.
8. Software designed for use in information and telecommunication systems, organs of state power of the Russian Federation.
9. The hardware and software modules trusted boot the PC.

### 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**

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 using encryption (cryptographic) means.
8. Passive and active technical protection of information for use in information and telecommunication systems.
10. Firewalls.
11. Software and hardware-software systems that implement the functions of the certification center.
12. Software information and telecommunication systems, which cooperates with certified encryption (cryptographic) means.
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, 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.

<table>
<thead>
<tr>
<th>Limited liability corrected</th>
<th>Name of tested product</th>
</tr>
</thead>
</table>
| "The Centre for Modern Technologies of Information Security" | 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. |
| AF-1 42  
30.08.2012  
30.08.2015 | NAME OF TESTS  
1. Special studies on the production pp 1, 2, 3.  
2. Special engineer the product according to claims 1, 2, 3. |

<table>
<thead>
<tr>
<th>Center providing information &quot;Energy&quot;</th>
<th>Name of tested product</th>
</tr>
</thead>
<tbody>
<tr>
<td>Federal Security Service of the Russian Federation</td>
<td>Hardware and software encryption tools and software designed to provide cryptographic protection of information when it is transmitted over the communication channels.</td>
</tr>
</tbody>
</table>
| AF-143  
10.10.2012  
20.04.2013 | NAME OF TESTS  
1. Engineering and cryptographic research.  
2. Special studies.  
3. Research line signal. |

<table>
<thead>
<tr>
<th>Public corporation</th>
<th>Name of tested product</th>
</tr>
</thead>
</table>
| AF-144  
04.10.2012 | 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. 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 (cryptographic) means.
7. Firewalls.
8. Systems for detection of computer attacks.
9. Software and hardware-software systems that implement the functions of the certification center.
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. 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 in information security, does not contain information constituting a state secret.
### Closed Joint-Stock Company

**"AST"**

115522, Moscow, Proletarian avenue, 8, Bldg. 2

<table>
<thead>
<tr>
<th>Name of tested product</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>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.</td>
<td></td>
</tr>
<tr>
<td>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.</td>
<td></td>
</tr>
<tr>
<td>3. Firewalls.</td>
<td></td>
</tr>
<tr>
<td>4. Systems for detection of computer attacks.</td>
<td></td>
</tr>
<tr>
<td>5. Software information and telecommunication systems, which cooperates with certified encryption (cryptographic) means.</td>
<td></td>
</tr>
</tbody>
</table>

**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

<table>
<thead>
<tr>
<th>Name of tested product</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. Hardware, software, and hardware and software encryption tools designed to provide cryptographic protection of information when it is transmitted over the communication channels.</td>
<td></td>
</tr>
<tr>
<td>2. Hardware, software, and hardware and software encryption tools designed to protect against unauthorized access to information during processing and storage.</td>
<td></td>
</tr>
<tr>
<td>3. Hardware, software, and hardware and software encryption tools designed to protect against spoofing, including simulation protection means.</td>
<td></td>
</tr>
<tr>
<td>4. Hardware, software, and hardware and software of the electronic signature.</td>
<td></td>
</tr>
<tr>
<td>5. Encrypted communication equipment.</td>
<td></td>
</tr>
<tr>
<td>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.</td>
<td></td>
</tr>
<tr>
<td>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.</td>
<td></td>
</tr>
<tr>
<td>8. Passive and active technical protection of information for use in information and telecommunication systems.</td>
<td></td>
</tr>
<tr>
<td>10. Software anti-virus tools.</td>
<td></td>
</tr>
<tr>
<td>11. Firewalls.</td>
<td></td>
</tr>
<tr>
<td>13. Software and hardware-software systems that implement the functions of the certification center.</td>
<td></td>
</tr>
<tr>
<td>15. Software designed for use in information and telecommunication systems, organs of state power of the Russian Federation.</td>
<td></td>
</tr>
<tr>
<td>16. The hardware and software modules trusted boot the PC.</td>
<td></td>
</tr>
</tbody>
</table>

**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 on the production pp 1, 2, 3, 4, 6, 7, 8, 11, 16.
4. Studies linear signal output by pp 1, 2, 3, 4, 7, 16.
5. Special work with the production of Claim 5. |
6. Special engineer the product according to claims 5, 6, 7, 8, 9, 13.
7. Studies of hardware products according to claim 9 for compliance with information security requirements.
8. Studies of software product according to claim 9 for compliance with information security requirements.
9. Studies of the functional properties of the products at pp 10-16 for compliance with information security requirements.

Name of tested product
1. Hardware and hardware-software encryption tools designed to provide cryptographic protection of information when it is transmitted over the 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. The hardware and the 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 performed using secure equipment and of 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.

NAME OF TESTS
1. Engineering and cryptographic research products at pp 1, 2, 3, 4.
2. Special studies on the production pp 1, 2, 3, 4, 6, 7.
3. Studies linear signal output by pp 1, 2, 3, 4, 7.
4. Accessibility of the products of claim 5.
5. Special engineering analysis products at pp 5, 6, 7.
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 1.04.2013)

<table>
<thead>
<tr>
<th>Name and address Organization</th>
<th>Registration number certificate of accreditation, its validity</th>
<th>Area Accreditation</th>
<th>Name of tested product</th>
</tr>
</thead>
<tbody>
<tr>
<td>The testing laboratory;</td>
<td>GIS. RU. LI0025</td>
<td>01.06.2009 01.06.2014</td>
<td>The Federal State Unitary Enterprise</td>
</tr>
<tr>
<td>&quot;Kalugapribor&quot;</td>
<td>Moscow Kaluga, ul. Moskovskaya 249</td>
<td>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.</td>
<td></td>
</tr>
</tbody>
</table>

NAME OF TESTS

<table>
<thead>
<tr>
<th>Name and address Organization</th>
<th>Registration number certificate of accreditation, its validity</th>
<th>Area Accreditation</th>
<th>Name of tested product</th>
</tr>
</thead>
<tbody>
<tr>
<td>The testing laboratory;</td>
<td>GIS. RU. LI0030</td>
<td>05.09.2009 05/09/2014</td>
<td>Limited Liability Company</td>
</tr>
<tr>
<td>&quot;Center of&quot;</td>
<td>Moscow Kaluga, ul. Moskovskaya 249</td>
<td>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.</td>
<td></td>
</tr>
</tbody>
</table>

NAME OF TESTS
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, 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 established in the construction of buildings and facilities (premises, vehicles), engineering communications, interior, in household appliances, in the technical means of recording, storing, processing and documenting 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 users on various grounds (the password, the additional code word for biometric data, etc.), including a program to improve the reliability of identification (authentication).
   2.3. Screening programs are functioning security system and information 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
NAME OF TESTS

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 various grounds (the password, the additional code word for biometric data, etc.), including a program to improve the reliability of identification (authentication).
   1.3. Screening programs are functioning security system and information 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 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
torture of unauthorized access to information, including:
- Registration Tool incorrect references to people and protected information;
- means the organization of control over the actions of PC users.

**NAME OF TESTS**

<table>
<thead>
<tr>
<th>The testing laboratory;</th>
<th>Name of tested product</th>
</tr>
</thead>
<tbody>
<tr>
<td>Closed Joint-Stock Company</td>
<td>Name of tested product</td>
</tr>
<tr>
<td>GIS RU. Li0032</td>
<td>1. Technical means of protecting information, including monitoring the effectiveness of the security measures of information:</td>
</tr>
<tr>
<td>129515, g Moscow, Street 2nd Ostankino, etc.</td>
<td>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.</td>
</tr>
<tr>
<td>01.02.2010</td>
<td>1.2. Protection of information against interception of the electrical signals generated in the cable network communications:</td>
</tr>
<tr>
<td>01.02.2015</td>
<td>- At the expense of TEMPEST by the work of technical means of recording, storing, processing, and documentation of information.</td>
</tr>
<tr>
<td></td>
<td>- Due to the effect of electro-acoustic signal conversion means and the auxiliary systems.</td>
</tr>
<tr>
<td></td>
<td>2. Technical equipment and systems in the secure execution, including:</td>
</tr>
<tr>
<td></td>
<td>2.1. Means scrambling or encryption masking telematics information transmitted over communication channels.</td>
</tr>
<tr>
<td></td>
<td>2.2. Hardware video transmission on the optical channel.</td>
</tr>
<tr>
<td></td>
<td>3. Software data protection from unauthorized access and program bookmarks:</td>
</tr>
<tr>
<td></td>
<td>3.1. Programs that provide concurrent access to information.</td>
</tr>
<tr>
<td></td>
<td>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).</td>
</tr>
<tr>
<td></td>
<td>3.3. Verification program of the system of information security and integrity protection from unauthorized access.</td>
</tr>
<tr>
<td></td>
<td>3.4. Program for the protection of various auxiliary facilities (for example, anti-virus programs).</td>
</tr>
<tr>
<td></td>
<td>3.5. Protection Programs PC operating systems (modular software interpretation, etc.).</td>
</tr>
<tr>
<td></td>
<td>3.6. Program integrity wide and application software.</td>
</tr>
<tr>
<td></td>
<td>3.7. Programs whistleblower resources.</td>
</tr>
<tr>
<td></td>
<td>3.8. Destruction program, residual information in memory devices (memory, video memory, etc.) upon completion of its use.</td>
</tr>
<tr>
<td></td>
<td>3.9. Control program and restore the files of the data structure.</td>
</tr>
<tr>
<td></td>
<td>3.10. Simulation program of the system or lock tamper detection facts.</td>
</tr>
<tr>
<td></td>
<td>4. Protected program information processing means:</td>
</tr>
<tr>
<td></td>
<td>4.1. Application packages workstations (AWS).</td>
</tr>
<tr>
<td></td>
<td>4.2. Databases computer networks.</td>
</tr>
<tr>
<td></td>
<td>4.3. Software tools for automated control systems (ACS).</td>
</tr>
<tr>
<td></td>
<td>4.4. Software tools for the identification of the manufacturer software (information) of the product, including the identification of copyright.</td>
</tr>
<tr>
<td></td>
<td>5. Software and hardware data protection:</td>
</tr>
<tr>
<td></td>
<td>5.1. Software and hardware tools to protect information from unauthorized copying, including:</td>
</tr>
<tr>
<td></td>
<td>- Protection of storage media;</td>
</tr>
<tr>
<td></td>
<td>- means to prevent copying of the software installed on the PC.</td>
</tr>
<tr>
<td></td>
<td>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.</td>
</tr>
<tr>
<td></td>
<td>5.3. Software and hardware interrupts user program in violation of the rules of access, including:</td>
</tr>
<tr>
<td></td>
<td>- forced termination of the program;</td>
</tr>
<tr>
<td></td>
<td>- Lock your computer.</td>
</tr>
<tr>
<td></td>
<td>5.4. Software and hardware data erasure, including:</td>
</tr>
<tr>
<td></td>
<td>- Erasing the residual information produced in the processing of sensitive information in memory and magnetic storage media;</td>
</tr>
<tr>
<td></td>
<td>- Secure erase obsolete information from magnetic media.</td>
</tr>
<tr>
<td></td>
<td>5.5. Software and hardware issue an alarm when an unauthorized access to information, including:</td>
</tr>
<tr>
<td></td>
<td>- Registration Tool incorrect references to users to protected information;</td>
</tr>
<tr>
<td></td>
<td>- A means of organizing control over the actions of PC users.</td>
</tr>
</tbody>
</table>
| | 5.6. Software and hardware detection and localization of the action of
**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 biometric data, etc.), including a program to improve the reliability of identification (authentication).
   3.3. Screening programs are functioning security system and information 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

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 users on various grounds (the password, the additional code word for biometric data, etc.), including a program to improve the reliability of identification (authentication).
   1.3. Screening programs are functioning security system and information 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:
   - 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.

NAME OF TESTS

| The testing laboratory;  |
| Federal state military educational institution of higher education |
| "Military Space Academy named after AF Mozhaysky" of the Ministry of |
| 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 various grounds (the password, the additional code word for biometric data, etc.), including a program to improve the reliability of identification (authentication). |
| 1.3. Screening programs are functioning security system and information 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. |

GIS. RU. LI0040
21.03. 2011 09.05.2013
1.1. 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 cryptographic and steganographic and information security (including the 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 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.

3.6. Software and hardware detection and localization of de first consequence of software and software-engineering bookmarks.

NAME OF TESTS
Electronic locks - television systems and security controls -
intruder detection or disruptive effects -
special means for transporting and storing the physical media (tape
streamers, magnetic and optical disks, etc.)
4. Software data protection from unauthorized access and program
bookmarks:
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. 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.) 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.
5.4. Software tools for the identification of the manufacturer software
information of the product, including the identification of copyright.
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 installed on the PC.
6.2. Software and hardware interrupts user program in violation of the
rules of access, including:
- forced termination of the program - Lock your 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
information;
- 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 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;
The International Centre for Informatics and
Electronics (InterEVM)

GIS. RU.
LI0042
20.05.2011
05/20/2016
123557
Str.
Presnensky Val, 19

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 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 informa-
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.
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.
1. 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**


<table>
<thead>
<tr>
<th>The testing laboratory;</th>
<th>GIS. RU. LI0043</th>
</tr>
</thead>
<tbody>
<tr>
<td>Closed Joint-Stock Company</td>
<td>07.03.2011</td>
</tr>
<tr>
<td>&quot;Multidisciplinary Innovation Enterprise &quot;SVEMEL&quot;</td>
<td>03/07/2016</td>
</tr>
<tr>
<td>125438, Moscow, 4th Likhachevsky per. 15, Building 3</td>
<td></td>
</tr>
</tbody>
</table>

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 tons of koprovodyaschih communications:
           - TEMPEST at the expense of the technical means of recording, storing, processing, and documentatment of information;
           - due to the effect of electro-acoustic signal conversion means and the auxiliary systems.
   2. Technical means of protecting information from unauthorized access (NSD).
       2.1. Protective equipment, including:
           - electronic locks;
           - the device identification;
           - plastic identification cards.
   3. Software data protection from unauthorized access and program bookmarks.
       3.1. Programs that provide concurrent access to information.
       3.2. Program identification and authentication of terminals and
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 (operative 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.

5.1. 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

<table>
<thead>
<tr>
<th>The testing laboratory;</th>
<th>Name of tested product</th>
</tr>
</thead>
<tbody>
<tr>
<td>The Federal State Unitary Enterprise</td>
<td>Technical means of protecting information, including monitoring the effectiveness of the security measures of information:</td>
</tr>
<tr>
<td>GIS. RU. LI0044</td>
<td>1. Protection of information against interception of acoustic signals propagating in air, water, solid media.</td>
</tr>
<tr>
<td>30.05.2011 05/30/2016</td>
<td>1.1. Protection of information against interception of acoustic signals propagating in air, water, solid media.</td>
</tr>
<tr>
<td>&quot;Research and Production Enterprise&quot;</td>
<td>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.</td>
</tr>
<tr>
<td></td>
<td>1.3. Protection of information against interception of the electrical signals generated in the cable communications:</td>
</tr>
<tr>
<td></td>
<td>- TEMPEST at the expense of the work of technical means of recording, storing, processing, and documentation of information;</td>
</tr>
<tr>
<td></td>
<td>- due to the effect of electro-acoustic signal conversion means and the auxiliary systems.</td>
</tr>
<tr>
<td></td>
<td>1.4. Technical means of detection and identification of special</td>
</tr>
</tbody>
</table>
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. 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 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 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 unauthorized copying, including:
       - protection of storage media;
       - means to prevent copying of the software installed 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.
   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;
       - means the organization of 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 (except cryptographic research) for compliance with regulatory requirements of the Federal Security Service of the Russian Federation.

The testing laboratory;
Closed Joint-Stock Company "The Moscow branch of Penza Research Institute of GIS. RU."
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 various grounds (the password, the additional code word for biometric data, etc.), including a program to improve the reliability of identification (authentication).
   1.3. Screening programs are functioning security system and information and integrity protection from unauthorized access.
1.4. Program for the protection of various auxiliary facilities (except for anti-virus programs).
1.5. Program integrity monitoring software application.
1.6. Programs whistleblower resources.
1.7. Control program and restore the file structure of the data.
1.8. Programs determine the facts and tamper alarm (with transfer of communication) of their discovery.

**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.

**SPECIAL CONDITIONS**

Research products are limited to conducting research of information security that does not contain information constituting a state secret.
5.1. Protection of storage media; means to prevent copying of the software, with the admission to the PC.
5.2. Software and hardware cryptographic and steganographic 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 unauthorized access to information, including:
- Registration Tool incorrect references to people and protected information;
- means the organization of control over the actions of PC users.
5.6. Software and hardware detection and localization of 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.

<table>
<thead>
<tr>
<th>Name of tested product</th>
<th>Technical protection of information, including a la counter the effectiveness of the measures of information security:</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. Technical protection of information, including a la counter the effectiveness of the measures of information security:</td>
<td></td>
</tr>
<tr>
<td>1.1. Protection of information against interception of the optical signals (images) in the visible, infrared and ultraviolet wavelengths.</td>
<td></td>
</tr>
<tr>
<td>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.</td>
<td></td>
</tr>
<tr>
<td>1.3. Protection of information against interception of the electrical signals generated in the cable communications:</td>
<td></td>
</tr>
<tr>
<td>- TEMPEST at the expense of the work of technical means of recording, storing, processing, and documentation of information;</td>
<td></td>
</tr>
<tr>
<td>- due to the effect of electro-acoustic signal conversion means and the auxiliary systems.</td>
<td></td>
</tr>
<tr>
<td>2. Software data protection from unauthorized access (unauthorized access) and software tabs:</td>
<td></td>
</tr>
<tr>
<td>2.1. Programs that provide concurrent access to information.</td>
<td></td>
</tr>
<tr>
<td>2.2. Program identification and authentication of terminals and users on various grounds (the password, the additional code word for biometric data, etc.), including a program to improve the reliability of identification (authentication).</td>
<td></td>
</tr>
<tr>
<td>2.3. Screening programs are functioning security system and information and integrity protection from unauthorized access.</td>
<td></td>
</tr>
<tr>
<td>2.4. Program for the protection of various auxiliary facilities, including anti-virus software.</td>
<td></td>
</tr>
<tr>
<td>2.5. Protection Programs PC operating systems (modular avenue of programmatic interpretation, etc.).</td>
<td></td>
</tr>
<tr>
<td>2.6. Program integrity wide and application software.</td>
<td></td>
</tr>
<tr>
<td>2.7. Programs whistleblower resources.</td>
<td></td>
</tr>
<tr>
<td>2.8. Destruction program, residual information in memory devices (memory, video memory, etc.) after completing her and use.</td>
<td></td>
</tr>
<tr>
<td>2.9. Control program and restore the file structure of the data.</td>
<td></td>
</tr>
<tr>
<td>2.10. Simulation program of a system or blocking in outcrop saving and tamper evidence.</td>
<td></td>
</tr>
<tr>
<td>2.11. Programs determine the facts and tamper alarm (with transfer of communication) of their discovery.</td>
<td></td>
</tr>
<tr>
<td>3. Protected program information processing means:</td>
<td></td>
</tr>
<tr>
<td>3.1. Application packages workstations.</td>
<td></td>
</tr>
<tr>
<td>3.2. Databases computer networks.</td>
<td></td>
</tr>
<tr>
<td>3.3. Software tools for automated control systems.</td>
<td></td>
</tr>
<tr>
<td>3.4. Software tools for the identification of the manufacturer software (information) of the product, including the identification of copyright.</td>
<td></td>
</tr>
</tbody>
</table>
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 steganographic 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 protected information;
   - means the organization of control over the actions of PC users.

**NAME OF TESTS**


---

**The testing laboratory;**

**Limited Liability Company**

"Research Centre of Certification"

127106, g Str. Botany, etc. 25

**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 signals, including the interception of stray electromagnetic radiation 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, 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
### 3. Protection Programs and System Security

3.1. Programs that provide concurrent access to information.
3.2. Program identification and authentication of terminals and users on various grounds (the password, the additional code word for biometric data, etc.), including a program to improve the reliability of identification (authentication).
3.3. Screening programs are functioning security system and information 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 steganographic and information security (including the means of concealment of information) in its storage media and data during transmission over communication channels.

### NAME OF TESTS


---

<table>
<thead>
<tr>
<th>The testing laboratory;</th>
<th>Name of tested product</th>
</tr>
</thead>
<tbody>
<tr>
<td>State state educational institution higher education</td>
<td>1. Software data protection from unauthorized access (unauthorized access) and software tabs:</td>
</tr>
<tr>
<td>Academy of the Federal Security Service of the Russian Federation</td>
<td>1.1. Programs that provide concurrent access to information.</td>
</tr>
<tr>
<td>GIS. RU. LI0049</td>
<td>1.2. Program identification and authentication of terminals and users on various grounds (the password, the additional code word for biometric data, etc.), including a program to improve the reliability of identification (authentication).</td>
</tr>
<tr>
<td>28.10.2011</td>
<td>1.3. Screening programs are functioning security system and information and integrity protection from unauthorized access.</td>
</tr>
<tr>
<td>01.08.2014</td>
<td>1.4. Program for the protection of various auxiliary facilities (except for anti-virus programs).</td>
</tr>
<tr>
<td></td>
<td>1.5. Protection Programs PC operating systems (modular avenue of</td>
</tr>
</tbody>
</table>
### 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 users on various grounds (the password, the additional code word for bimetric data, etc.), including a program to improve the reliability of identification (authentication).
      2.3. Screening programs are functioning security system and information 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.

### Name of Tests

4.2. Software and hardware cryptographic and steganographic 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 unauthorized access to information, including:
- Registration Tool incorrect references to people and protected information;
- means the organization of control over the actions of PC users.


NAME OF TESTS

| The testing laboratory; | GIS. RU. LI005 1 |
| Limited Liability Company "Unser PRO" | 07.12.2011 |
| 119192, Moscow, Michurinsky prospect etc. 19, Building 1, Apt. 29 | 07.12.2014 |

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 users on various grounds (the password, the additional code word for biometric data, etc.), including a program to improve the reliability of identification (authentication).
1.3. Screening programs are functioning security system and information 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**


<table>
<thead>
<tr>
<th>The testing laboratory; Federal State Unitary Enterprise &quot;Central Research Institute Economics, Computer Science and Control Systems&quot;</th>
<th>Name of tested product</th>
</tr>
</thead>
</table>
| GIS. RU. LI005 2 07.1.2.2011 07.1.2.2014 | 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 various grounds (the password, the additional code word for biometric data, etc.), including a program to improve the reliability of identification (authentication).
1.3. Screening programs are functioning security system and information 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

The testing laboratory;
Federal State Unitary Enterprise
"Gostehstroy"
123242, Moscow, Acad. Kapranov , 3, page 1

<table>
<thead>
<tr>
<th>GIS. RU. LI005 3</th>
</tr>
</thead>
<tbody>
<tr>
<td>12.12.2011</td>
</tr>
<tr>
<td>12.1.2014</td>
</tr>
</tbody>
</table>

Name of tested product
1. Information Security Technology (GIS), including the effectiveness of the control measures to protect the information.
1.1. GIS 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. GIS interception of 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. 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 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 Communication"
107066, Str. Lower Krasnoselskaya 35

GIS. RU. LI005 4
12.12.2011
12.1.2016

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 biometric data, etc.), including a program to improve the reliability of identification (authentication).
1.3. Screening programs are functioning security system and information 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.

NAME OF TESTS

The testing laboratory:
Closed Joint-Stock Company "Orbit"
350063, Moscow
Address: Str. Komsomolskaya 40

GIS. RU.
L1005 5
04.10.2011
04.02.2016

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:
2.1. 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. 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 (except for 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 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 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 unauthorized copying, including:
- protection of storage media;
- 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.
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 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.
5.6. Software and hardware detection and localization of the action of software and software-engineering bookmarks.

NAME OF TESTS

The testing laboratory;
Limited Liability Company GIS. RU.
"Optionally" LI00056
195220, St. Petersburg, ul. Gzhatskaya, etc. 21, letter D

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, including anti-virus software.
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. Destruction program, residual information in memory devices
(memory, video memory, etc.) upon completion of its use.

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

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

<table>
<thead>
<tr>
<th>The testing laboratory; The Federal State Unitary Enterprise</th>
<th>Name of tested product</th>
</tr>
</thead>
<tbody>
<tr>
<td>GIS. RU. Li0057</td>
<td>Technical protection of information, including a la counter the effectiveness of the measures of information security:</td>
</tr>
<tr>
<td>15.02.2012 02/15/2017</td>
<td>1. Protection of information against interception of the optical signals (images) in the visible, infrared and ultraviolet wavelengths.</td>
</tr>
<tr>
<td></td>
<td>1.1. Protection of information against interception of the optical signals (images) in the visible, infrared and ultraviolet wavelengths.</td>
</tr>
<tr>
<td></td>
<td>1.2. Protection of information against interception of electromagnetic signals, including the interception of stray electromagnetic radiation and radio and vodkat (TEMPESI), arising from the work of the technical means of recording, storing, processing, and documentation of information.</td>
</tr>
<tr>
<td></td>
<td>1.3. Protection of information against interception of electromagnetic signals, including the interception of stray electromagnetic radiation and radio and vodkat (TEMPESI), arising from the work of the technical means of recording, storing, processing, and documentation of information.</td>
</tr>
<tr>
<td></td>
<td>1.4. Protection of information against interception of the electrical</td>
</tr>
</tbody>
</table>
signals generated in the cable communications:  
- due to the work of technical means of recording, storing, processing and documenting information;  
- due to the effect of electro-acoustic signal conversion means and auxiliary systems.

1. Means of detection and identification of special technical means intended for secret information, have been established in the construction of buildings and facilities (premises, vehicles), engineering communications, interior in household appliances, in the technical means of recording, storing, processing and documenting information and communication systems in an open area.

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

1. Means scrambling or encryption mask and Telematic 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 canals.
3. Software tools to protect information from unauthorized access (unauthorized access) and software tabs:
   1. Programs that provide concurrent access to information.
   2. Program identification and authentication of terminals and users on different grounds (the password, the additional code word for biometric data, etc.), including a program to improve the reliability of identification (authentication).
   3. Screening programs are functioning security system and information integrity protection from unauthorized access.
   4. Program for the protection of various fashion destination with the exception of antivirus software.
   5. Protection Programs PC operating systems (modular avenue of programmatic interpretation, etc.).
   6. Program integrity wide and application software.
   7. Programs whistleblower resources.
   8. Programs residual destruction of residual information in memory devices (memory, video memory, etc.) after the completion of her and use.
   9. Monitoring programs and restore the file structure of the data.
   10. Programs simulate the operation of a system or blocking in our action and tamper evidence.
   11. Programs determination of the facts and tamper alarm (with the transfer of communication) of their discovery.

4. Protected program information processing means:

1. Application packages workstations.
2. Databases computer networks.
3. Software tools for automated control systems.
4. Software tools for the identification of the manufacturer software (information) of the product, including identification of copyright.

5. Software and hardware data protection:  
1. Software and hardware 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.
   2. Software and hardware cryptographic and steganographic and information security (including the means of concealment of information) in its storage media and data during transmission over communication channels.
   3. Software and hardware interrupts user program in violation of the rules of access, including:
      - forced termination of the program;
      - Lock your computer.
   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. Software and hardware issuing an alarm when n of torture NSD to information, including:
      - Registration Tool incorrect references to people and protinated information;
      - means the organization of control over the actions of PC users.

6. Software and hardware for protection against unauthorized access to systems operational-search measures (SORM) on the lines of communication:

1. In wireline communication systems.
2. In cellular communication systems.

NAME OF TESTS

SPECIAL CONDITIONS
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
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 noise 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, 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 Telemetry 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 cryptographic and steganographic and information security (including the 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 issuing an alarm when unauthorized access to information, including:
- Registration Tool incorrect references to people and protected information;
- means the organization of control over the actions of PC users.

NAME OF TESTS

| Name of tested product | 1. Technical means of protecting information, including monitoring the effectiveness of the measures taken for information security;  
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. Means scrambling mask telematics information transmitted over communication channels.  
3. Protected program information processing means:  
3.1. Application Packages workstations. |

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

NAME OF TESTS
<table>
<thead>
<tr>
<th>Name of tested product</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>1. Software data protection from unauthorized access (unauthorized access) and software tabs:</td>
<td></td>
</tr>
<tr>
<td>1.1. Programs that provide concurrent access to information.</td>
<td></td>
</tr>
<tr>
<td>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).</td>
<td></td>
</tr>
<tr>
<td>1.3. Verification program of the system of information security and integrity protection from unauthorized access.</td>
<td></td>
</tr>
<tr>
<td>1.4. Program for the protection of various auxiliary facilities (except for anti-virus programs).</td>
<td></td>
</tr>
<tr>
<td>1.5. Protection Programs PC operating systems (modular software interpretation, etc.).</td>
<td></td>
</tr>
<tr>
<td>1.6. Program integrity wide and application software.</td>
<td></td>
</tr>
<tr>
<td>1.7. Programme whistleblower resources.</td>
<td></td>
</tr>
<tr>
<td>1.8. Programs destruction of residual information in memory devices (memory, video memory, etc.) upon completion of its use.</td>
<td></td>
</tr>
<tr>
<td>1.9. Programs simulate the operation of a system or lock tamper detection facts.</td>
<td></td>
</tr>
<tr>
<td>1.10. Programs determination of the facts and tamper alarm (communication) of their discovery.</td>
<td></td>
</tr>
<tr>
<td>2. Protected program information processing means:</td>
<td></td>
</tr>
<tr>
<td>2.1. Application packages workstations.</td>
<td></td>
</tr>
<tr>
<td>2.2. Databases computer networks.</td>
<td></td>
</tr>
<tr>
<td>2.3. Software tools for automated control systems.</td>
<td></td>
</tr>
<tr>
<td>2.4. Software tools for the identification of the manufacturer</td>
<td></td>
</tr>
</tbody>
</table>
software (information) of the product, including the identification of copyright.

**NAME OF TESTS**

<table>
<thead>
<tr>
<th>The testing laboratory;</th>
<th>Name of tested product</th>
</tr>
</thead>
<tbody>
<tr>
<td>Limited Liability Company</td>
<td>1. Technical protection of information, including a la counter the effectiveness of the measures of information security:</td>
</tr>
<tr>
<td>&quot;Center of Information Security&quot; mask &quot;</td>
<td>1.1. Protection of information against interception of acoustic signals propagating in air, water, solid media.</td>
</tr>
<tr>
<td>119607, Moscow, Michurinsky Pr, d 27, h. 2</td>
<td>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.</td>
</tr>
<tr>
<td></td>
<td>1.3. Protection of information against interception of the electrical signals generated in the cable communications:</td>
</tr>
<tr>
<td></td>
<td>- TEMPEST at the expense of the work of technical means of recording, storing e tion, processing and documentation of information;</td>
</tr>
<tr>
<td></td>
<td>- due to the effect of electro-acoustic signal conversion means and the auxiliary systems.</td>
</tr>
<tr>
<td>GIS. RU. LI00 63</td>
<td>2. Software data protection from unauthorized access (unauthorized access) and software tabs:</td>
</tr>
<tr>
<td>May 1.0 6.2012 15.06 2015</td>
<td>2.1. Programs that provide concurrent access to information.</td>
</tr>
<tr>
<td></td>
<td>2.2. Screening programs are functioning security system and inform tion and integrity protection from unauthorized access.</td>
</tr>
<tr>
<td></td>
<td>2.3. Program for the protection of various auxiliary facilities (except for anti-virus programs).</td>
</tr>
<tr>
<td></td>
<td>2.4. Protection Programs PC operating systems (modular avenue of programmatic interpretation, etc.).</td>
</tr>
<tr>
<td></td>
<td>2.5. Program integrity wide and application software.</td>
</tr>
<tr>
<td></td>
<td>2.6. Programs whistleblower resources.</td>
</tr>
<tr>
<td></td>
<td>3. Protected program information processing means:</td>
</tr>
<tr>
<td></td>
<td>3.1. Application Packages workstations.</td>
</tr>
<tr>
<td></td>
<td>3.2. Databases computer networks.</td>
</tr>
<tr>
<td></td>
<td>3.3. Software tools for automated control systems.</td>
</tr>
</tbody>
</table>

**NAME OF TESTS**
<table>
<thead>
<tr>
<th>Number</th>
<th>Software Feature</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Software data protection from unauthorized access (unauthorized access) and software tabs:</td>
</tr>
<tr>
<td>1.1.</td>
<td>Programs that provide concurrent access to information.</td>
</tr>
<tr>
<td>1.2.</td>
<td>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).</td>
</tr>
<tr>
<td>1.3.</td>
<td>Verification program of the system of information security and integrity protection from unauthorized access.</td>
</tr>
<tr>
<td>1.4.</td>
<td>Program for the protection of various auxiliary facilities (except for anti-virus programs).</td>
</tr>
<tr>
<td>1.5.</td>
<td>Protection Programs PC operating systems (modular software interpretation, etc.).</td>
</tr>
<tr>
<td>1.6.</td>
<td>Program integrity wide and application software.</td>
</tr>
<tr>
<td>1.7.</td>
<td>Programs whistleblower resources.</td>
</tr>
<tr>
<td>1.8.</td>
<td>Programs destruction of residual information in memory devices (memory, video memory, etc.) upon completion of its use.</td>
</tr>
<tr>
<td>1.9.</td>
<td>monitoring programs and restore the file structure of the data.</td>
</tr>
<tr>
<td>1.10.</td>
<td>Programs simulate the operation of a system or lock tamper detection facts.</td>
</tr>
<tr>
<td>1.11.</td>
<td>Programs determination of the facts and tamper alarm (communication) of their discovery.</td>
</tr>
<tr>
<td>2.</td>
<td>Protected program information processing means:</td>
</tr>
<tr>
<td>2.1.</td>
<td>Application packages workstations.</td>
</tr>
<tr>
<td>2.2.</td>
<td>Databases computer networks.</td>
</tr>
<tr>
<td>2.3.</td>
<td>Software tools for automated control systems.</td>
</tr>
<tr>
<td>2.4.</td>
<td>Software tools for the identification of the manufacturer software (information) of the product, including the identification of copyright.</td>
</tr>
<tr>
<td>3.</td>
<td>Software and hardware data protection:</td>
</tr>
<tr>
<td>3.1.</td>
<td>software and hardware to protect information from unauthorized copying, including:</td>
</tr>
<tr>
<td></td>
<td>- protection of storage media;</td>
</tr>
<tr>
<td></td>
<td>- means to prevent copying of the software installed on the PC.</td>
</tr>
<tr>
<td>3.2.</td>
<td>Software and hardware interrupts user program in violation of the rules of access, including:</td>
</tr>
<tr>
<td></td>
<td>- forced termination of the program;</td>
</tr>
<tr>
<td></td>
<td>- Lock your computer.</td>
</tr>
<tr>
<td>3.3.</td>
<td>Software and hardware data erasure, including:</td>
</tr>
<tr>
<td></td>
<td>- erasing the residual information produced in the processing of sensitive information in memory and magnetic storage media;</td>
</tr>
<tr>
<td></td>
<td>- secure erase obsolete information from magnetic media.</td>
</tr>
<tr>
<td>3.4.</td>
<td>Software and hardware issue an alarm when an unauthorized access attempt is detected.</td>
</tr>
</tbody>
</table>
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

<table>
<thead>
<tr>
<th>The testing laboratory;</th>
<th>Name of tested product</th>
</tr>
</thead>
<tbody>
<tr>
<td>Limited Liability Company</td>
<td>1. Technical means of protecting information, including monitoring the effectiveness of the security measures of information:</td>
</tr>
<tr>
<td>&quot;Independent testing center - SPETSTEST&quot;</td>
<td>1.1. Protection of information against interception of acoustic signals propagating in air, water, solid media.</td>
</tr>
<tr>
<td>249030, Kaluga region, Obninsk, Kiev highway, 64</td>
<td>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.</td>
</tr>
<tr>
<td></td>
<td>1.3. Protection of information against interception of the electrical signals generated in the cable communications:</td>
</tr>
<tr>
<td></td>
<td>- TEMPEST at the expense of the work of technical means of recording, storing, processing, and documentation of information;</td>
</tr>
<tr>
<td></td>
<td>- due to the effect of electro-acoustic signal conversion means and the auxiliary systems.</td>
</tr>
</tbody>
</table>

NAME OF TESTS

<table>
<thead>
<tr>
<th>The testing laboratory;</th>
<th>Name of tested product</th>
</tr>
</thead>
<tbody>
<tr>
<td>Limited Liability Company</td>
<td>1. Technical protection of information, including a la counter the effectiveness of the measures of information security:</td>
</tr>
<tr>
<td>&quot;The Centre for Modern Technologies of Information Security&quot;</td>
<td>1.1. Protection of information against interception of acoustic signals propagating in air, water, solid media.</td>
</tr>
<tr>
<td>127550, Str.</td>
<td>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.</td>
</tr>
<tr>
<td></td>
<td>1.3. Protection of information against interception of the electrical signals generated in the cable communications:</td>
</tr>
</tbody>
</table>
Pryanishnikova House 23A

- 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

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 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

SPECIAL CONDITIONS
Research products at pp 1.1 and 4.1 are limited to conducting research of information security that does not contain information constituting a state secret.
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. 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.
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 interrupts user program in violation of the rules of access, including:
- forced termination of the program;
- Lock your computer.
4.3. 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

The testing laboratory;
Closed Joint-Stock Company "AST"
115522, Moscow, Proletarian avenue, 8, Bldg. 2

GIS. RU. LI0069
15.01.2013
01/15/2016

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 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. Programs whistleblower resources.
2. Programs destruction of residual information in memory devices (memory, video memory, etc.) after the completion of her and use.
3. Monitoring programs and restore the file structure of the data.
4. Programs simulate the operation of a system or blocking in outcrop servation and tamper evidence.
5. Programs determination of the facts and tamper alarm (with the transfer of communication) of their discovery.

2. Protected program information processing means:

3. Software and hardware data protection:

NAME OF TESTS


<table>
<thead>
<tr>
<th>The testing laboratory; Limited Liability Company &quot;M-STANDARD holding&quot; 105318, Moscow, ul. Scherbakovskaya, 53, building 4</th>
<th>Name of tested product</th>
</tr>
</thead>
<tbody>
<tr>
<td>GIS. RU. LI0070 26.03.2013 26/03/2018</td>
<td>1. Software data protection from unauthorized access (unauthorized access) and software tabs:</td>
</tr>
<tr>
<td></td>
<td>1. Programs that provide concurrent access to information.</td>
</tr>
<tr>
<td></td>
<td>1.2. Program identification and authentication of terminals and users on various grounds (the password, the additional code word for biometric data, and so on), including a program to improve the reliability of identification (authentication).</td>
</tr>
<tr>
<td></td>
<td>1.3. Screening programs are functioning security system and information and integrity protection from unauthorized access.</td>
</tr>
<tr>
<td></td>
<td>1.4. Program for the protection of various auxiliary facilities (except for anti-virus programs).</td>
</tr>
</tbody>
</table>
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 death consequence bookmarks.

NAME OF TESTS

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.