Russian IT Security Certification Scheme: New Trends

Alexander Barabanov and Mikhail Fedorov

June, 3rd, 2014
Russian IT Security Certification Scheme: who takes part in the certification process?
Russian IT Security Certification Scheme: major approaches to certification

- Black box testing to ensure that it works as it should
- Testing of source code for the absence of software vulnerabilities

Certification of the functionality

Certification for the absence of non-declared functions (NDF)
Current status: Certified Products by Types

- Firewall: 38%
- Access Control Systems: 17%
- Embedded Access Control: 15%
- Software: 9%
- Network System: 6%
- Operating System: 5%
- Antivirus: 3%
- DBMS: 2%
- IPS/IDS: 2%

2011-2013 Evaluation Timeline
Trend #1: Steps Toward Common Criteria Approach

1. The Legal Act
2. Approved Protection Profile
3. Target of Evaluation
4. IT Security Environment
5. Security Target
6. Evidences
Trend #2: Certificate Assurance Maintenance

- Certified update infrastructure
- Security impact analysis
Trend #3: Steps toward Bug Free Software

- ISO/IEC 27001 compatibility
- ISO/IEC 27001
- Common Criteria
- "Best Practices"
- Implementation of the SDL in early stages
- GOST “Information protection. Secure Software Development Requirements”