Russian IT Security Certification Scheme: Steps Toward Common Criteria Approach

Alexander Barabanov[1], Alexey Markov[1], Valentin Tsirlov[1]

[1] NPO Echelon, CJSC, Moscow, Russia
{a.markov,a.barabanov}@npo-echelon.ru

Abstract. This paper is dedicated to the Russian IT Security Certification Scheme; it shortly describes history, structure and features of the Scheme, provides statistics of certification tests administered and information about certification scheme evolution in view of the Common Criteria approach used in the Russian Scheme.

Keywords: Certification, Russian IT Security Certification Scheme, IT security facility, Common Criteria.

1 Introduction

Russian IT Security Certification Scheme was established in 1995. The Scheme offers evaluation and certification services to sponsors, developers and vendors. Key participants of the Scheme are:

- Sponsors (developers, vendors) which requests and funds an evaluation and a certification;
- Accredited Testing Labs (Commercial Evaluation Facilities) which carry out the evaluations, and the establishment of approved techniques and procedures;
- Certification Bodies which certify the results of evaluations of IT products;
- Federal Certification Body (FSTEC of Russia) which monitors all evaluations conducted under the Scheme.

Relationships between major participants in the process are shown in Fig 1.

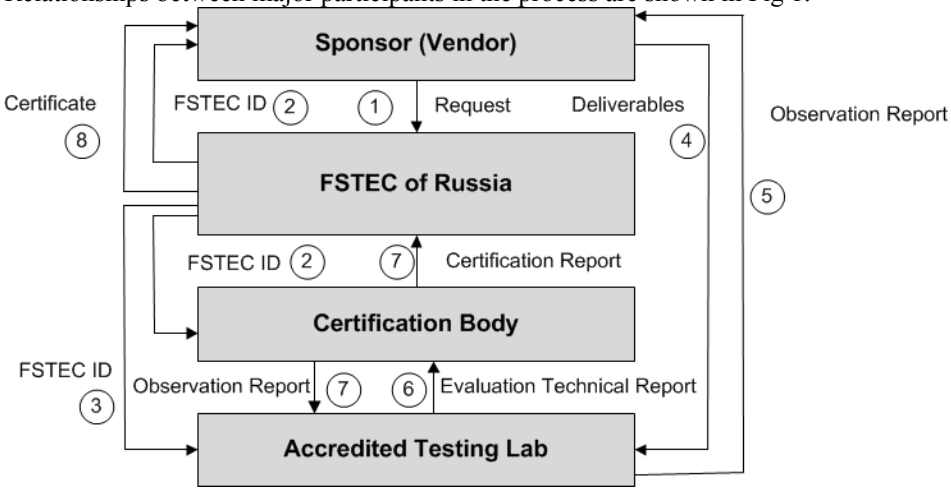

Fig. 1. The chart of relationships between participants in the Scheme

To date the certification system accredited: 40 Accredited Test Labs and 9 Certification Bodies. It should be noted that certification bodies may include both commercial and governmental agencies. Kinetic profile of test laboratories and certification bodies is shown in Fig. 2 and Fig. 3 respectively.

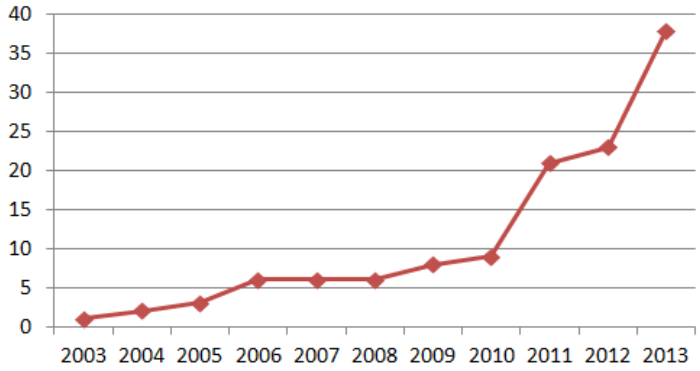

Fig. 2. Increasing number of accredited test laboratories

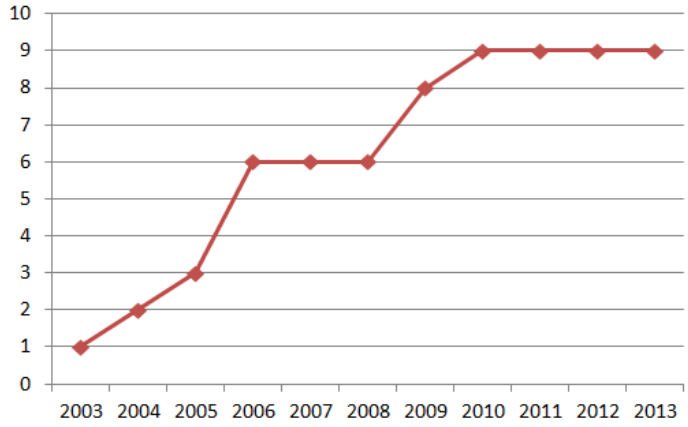

Fig. 3. Increasing number of accredited certification bodies

Current approaches to evaluation may be generally classified as follows [1]:

- structural testing: source code analyses (static and dynamic analyses) in order to reveal software errors, non-declared opportunities and software bugs and flaws;
- functional testing is a test conducted to determine if the requirements of a specification are met (black or grey box testing).

Aside from that, we would like to emphasize available procedure for inspection of certified products manufacture.
Basic «classic» regulations used in the Scheme include:

- the mandatory document of 1992 which sets out requirements to Target of Evaluation (TOE) against unauthorized access to information (identification/authentication, access control etc.); this document is based on the Orange Book approach;
- the mandatory document of 1997 which lays down requirements to firewall;
- the mandatory document of 1999 which sets out requirements to search for undeclared opportunities (static, dynamic source code analysis).

If an TOE to be certified is neither a firewall nor an access control system it is certified for compliance with specifications originated by the test object developer. Recognizing necessity to reform the certification system so as to ensure repeatability and reproducibility of test results, enhance confidence in certificates, FSTEC of Russia adopted the Common Criteria approach to be the basis for origination of new generation documents.

2 The New FSTEC of Russia Approach

The first attempted to use Common Criteria [5] approach was made by FSTEC of Russia in 2002 and included by origination and approval of mandatory documents of FSTEC of Russia which comprise authentic translation of 3 parts of Common Criteria and Common Methodology for Information Technology Security Evaluation. The work also included steps targeted at harmony between the Russian and European regulations, in particular, origination of state standards which comprise authentic translation of the European standards ISO/IEC 15408, ISO/IEC 18045 and ISO/IEC TR 15446 (Fig. 4).

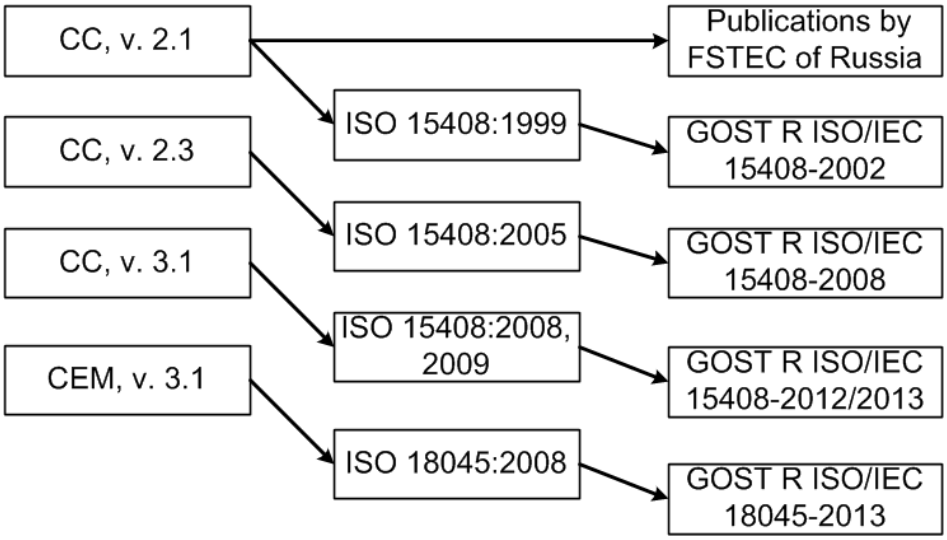

Fig. 4. Correspondence between international standards and Russian GOST

Since 2012 the FSTEC of Russia has been insistently introducing TOE certification according to the Common Criteria procedure. Each type of TOE` has a document (regulations) which contains requirements to information security and sets up security categories with minimum requirements. For each type of TOE and category the FSTEC of Russia creates and approves Protection Profiles (Fig. 5). In 2011-2013 the FSTEC of Russia originated requirements to intrusion detection systems and antivirus [1, 2].

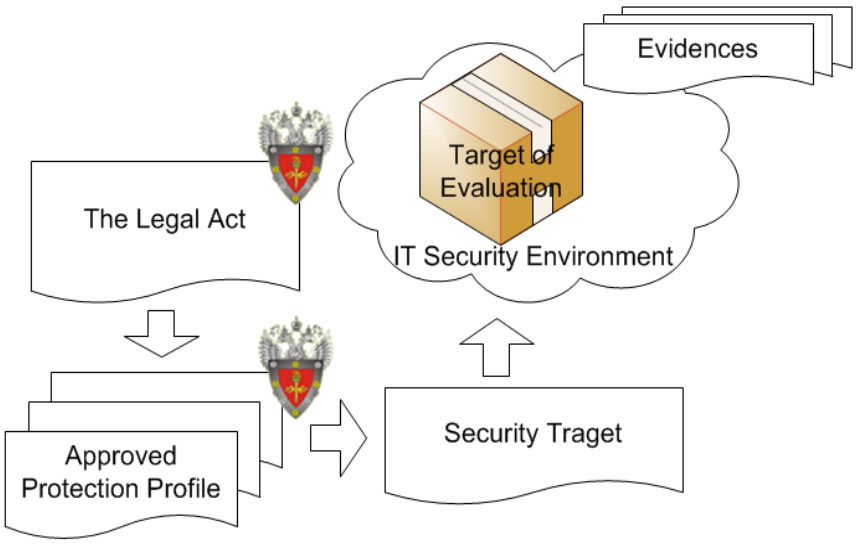

Fig. 5. Establishing of information security requirements in accordance with new approach of FSTEC of Russia

3 Russian IT Security Certification Scheme: some statistics

Below we provide statistics of Russian IT Security Certification Scheme obtained after processing the information accessible in the official site of FSTEC of Russia [3] and the results of comparative analysis of the certification system of FSTEC of Russia and Common Criteria certification system [4].

Fig. 6 shows the number of certifications made in the certification system of FSTEC of Russia and certifications made under Common Criteria Certification Scheme.

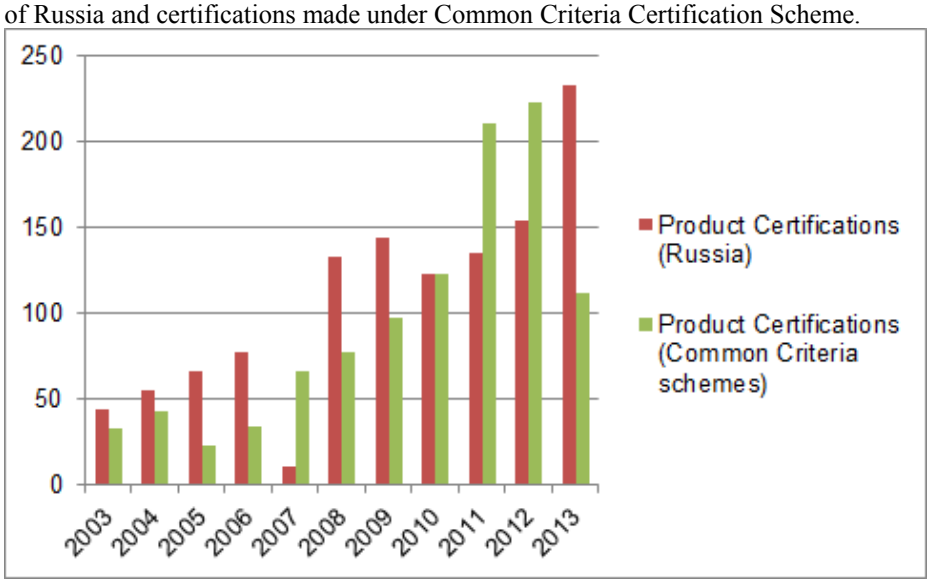

Fig. 6. Number of certifications (year-by-year)

Fig. 7 shows shares of certifications made under Russian IT Security Certification Scheme) and types of TOE: firewal is the undisputed leader.

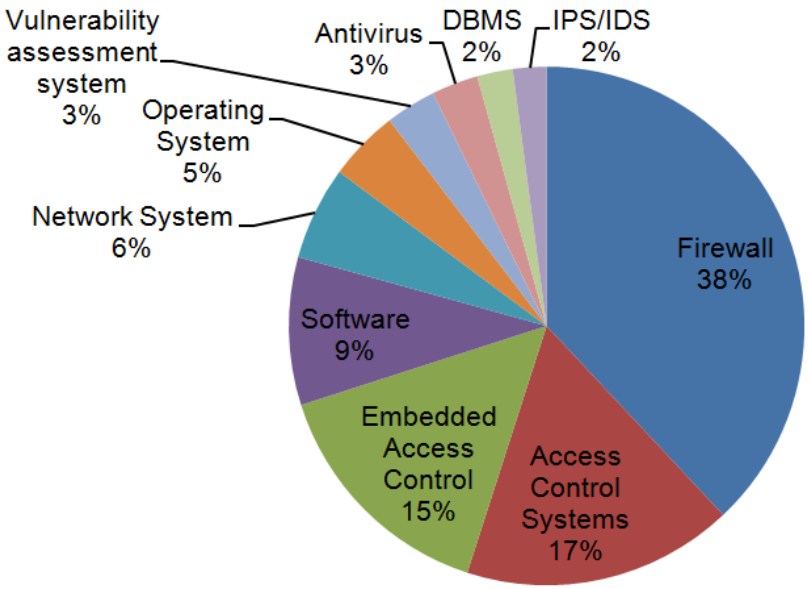

Fig. 7. Shares of certified TOE types (in 2011-2013, Russian IT Security Certification Scheme)

Shares of certifications according to TOE type and year are given in Fig. 8.

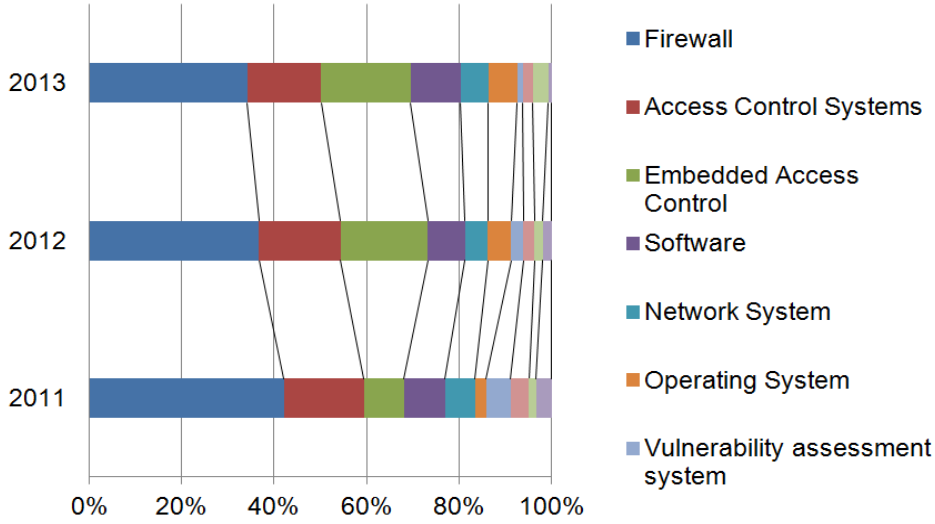

Fig. 8. Shares of certifications according to TOE type and year (in 2011-2013, Russian IT Security Certification Scheme)

Similar analysis of the Common Criteria certification Scheme has shown (Fig. 9) that the following type of TOE are first three by the number of certifications:

- software used in smart cards;
- multi-functional devices (printers);
- software used in computer networks (routers, switches).

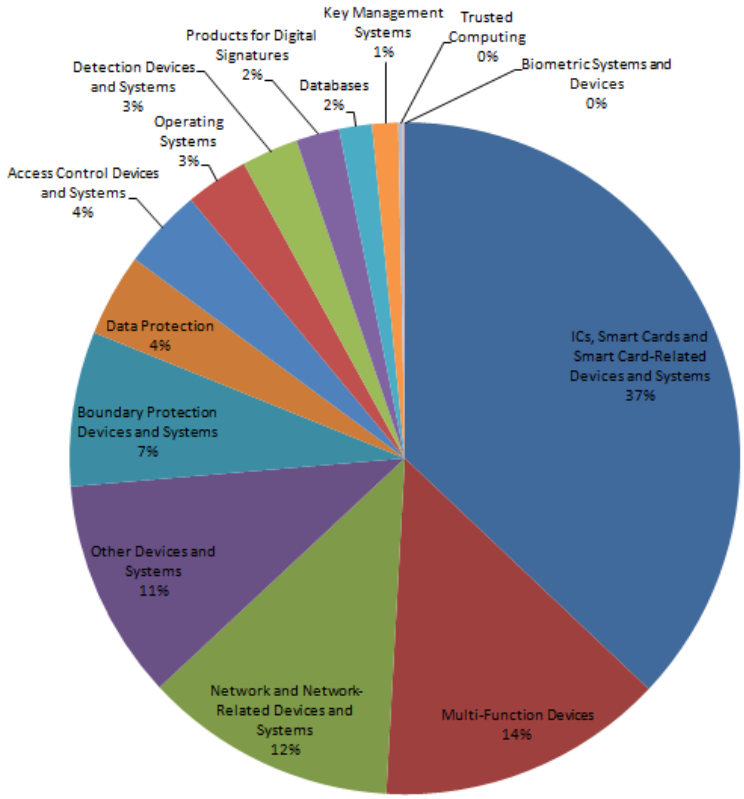

Fig. 9. Shares of certified TOE types (in 2011-2013, Common Criteria Certification Scheme)

Shares of certifications using «series» and «batch» patterns are given in Fig. 10.

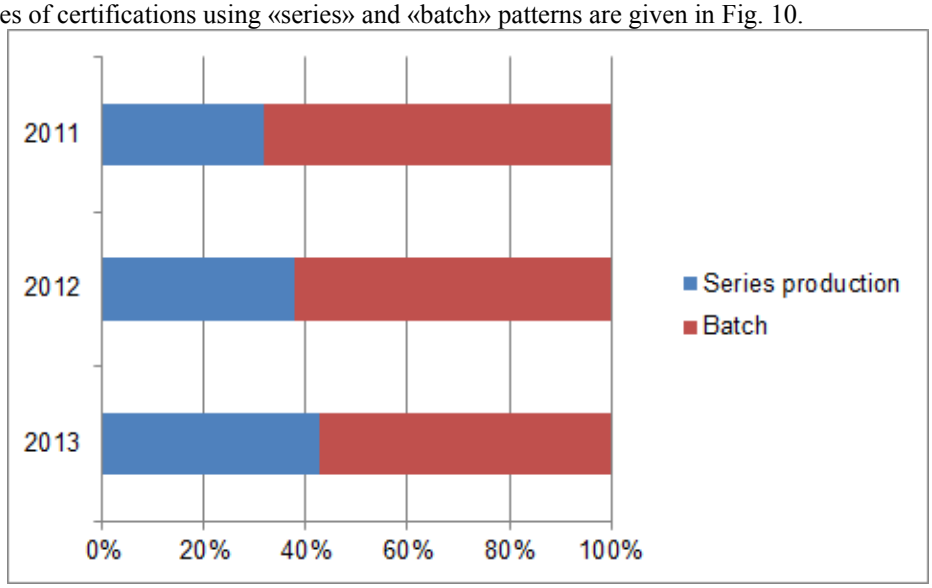

Fig. 10. Shares of certification patterns (in 2011-2013, Russian IT Security Certification Scheme)

Shares of certifications of Russian-made and foreign-made TOE is shown in Fig. 11.

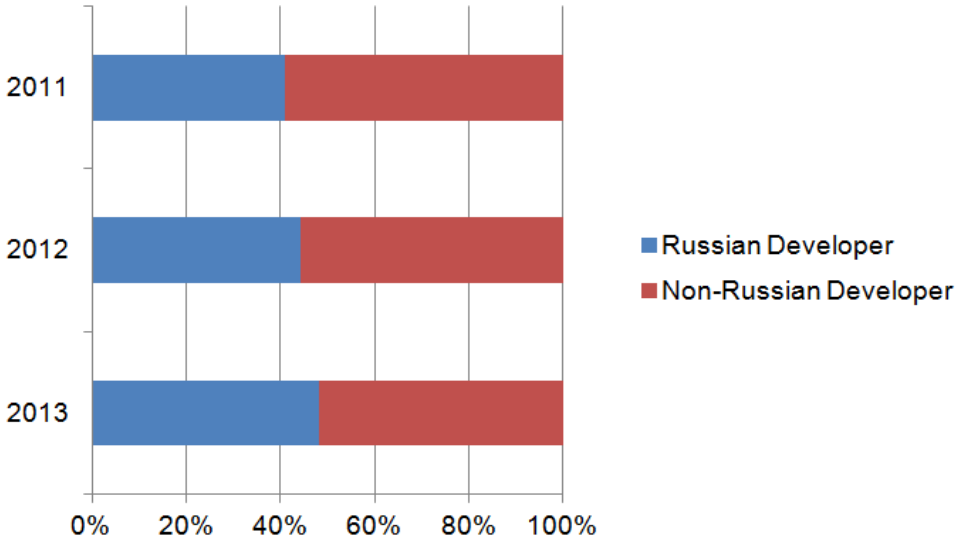

Fig. 11. Certifications of Russian-made and foreign-made TOE (in 2011-2013, Russian IT Security Certification Scheme))

Fig. 12 and 13 show foreign and Russian software developers most frequently certified under Russian IT Security Certification Scheme.

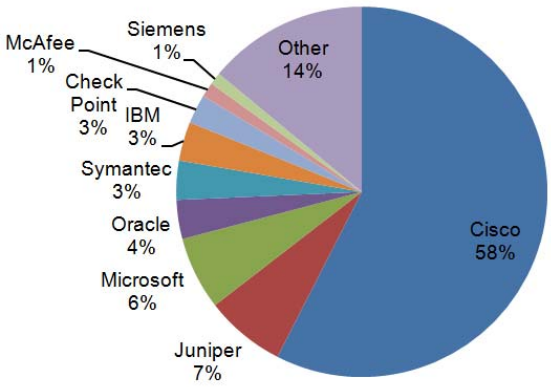

Fig. 12. Foreign software developers certified by FSTEC of Russia (in 2011-2013)

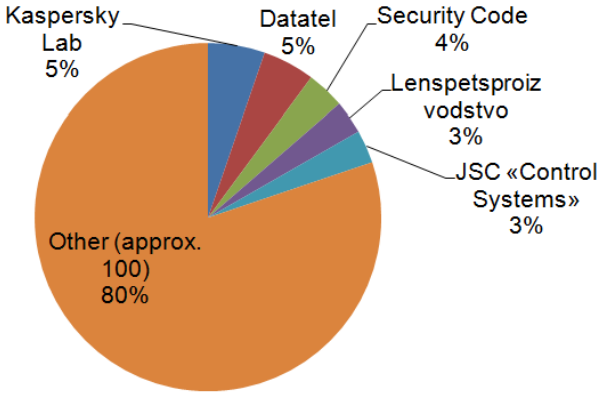

Fig. 13. Russian software developers certified by FSTEC of Russia (in 2011-2013)

Similar analysis for Common Criteria certification schemes is shown in Fig. 14.

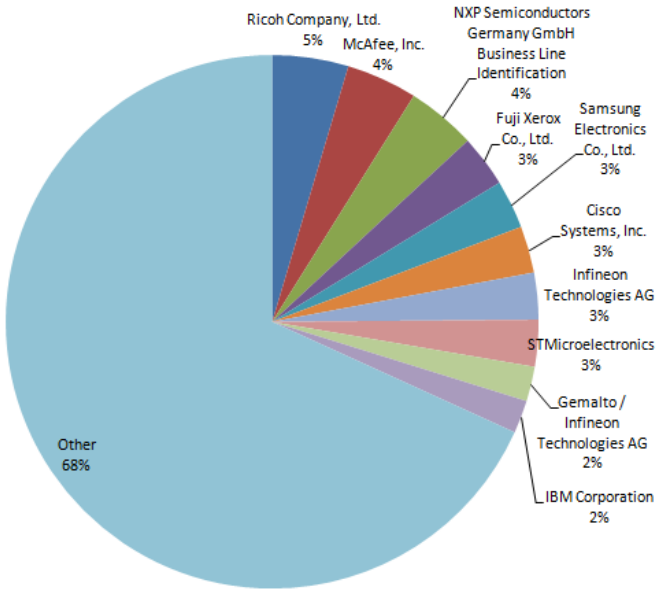

Fig. 14. Software developers certified under Common Criteria Certification Schemes (in 2011-2013)

Shares of certifications with and without access to source code for certifications under Common Criteria Certification Schemes and Russian IT Security Certification Scheme are shown in Fig 15.

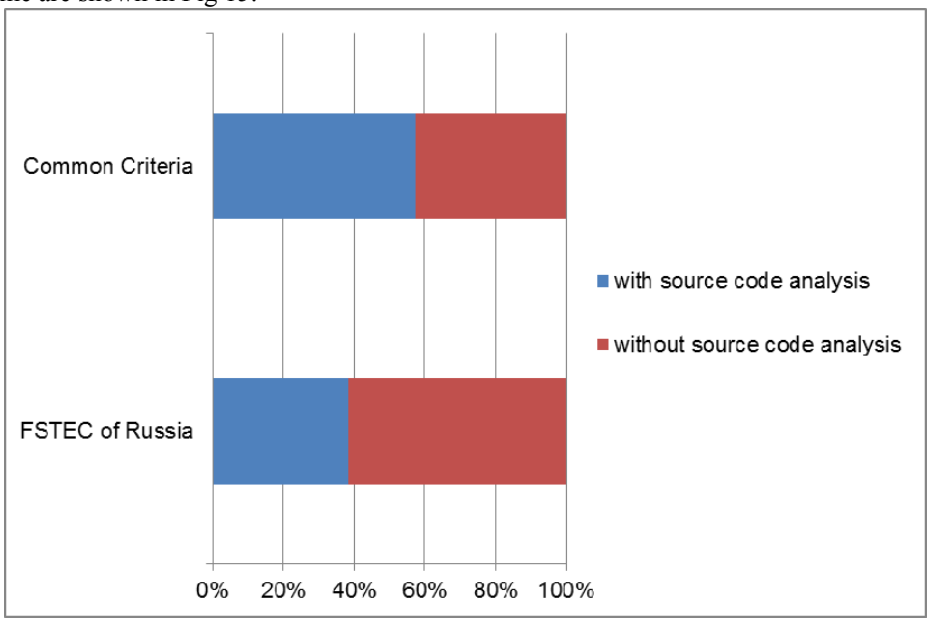

Fig. 15. Shares of certifications according to access to source code (in 2011-2013)

Shares of certifications according to Common Criteria approach in the Russian Scheme given in Fig. 16.

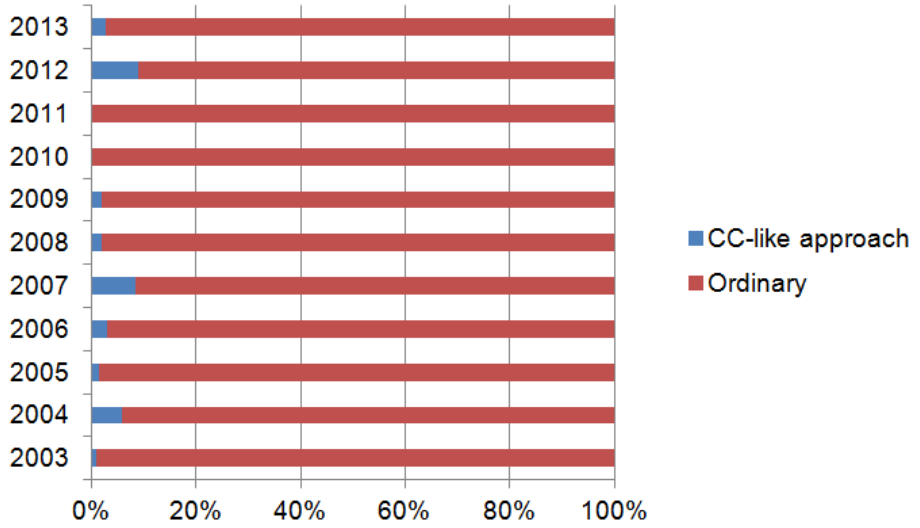

Fig. 16. Shares of certifications according to Common Criteria approach in Russian Scheme

Shares of certifications according to the evaluation assurance level (EAL) are shown in Fig. 17.

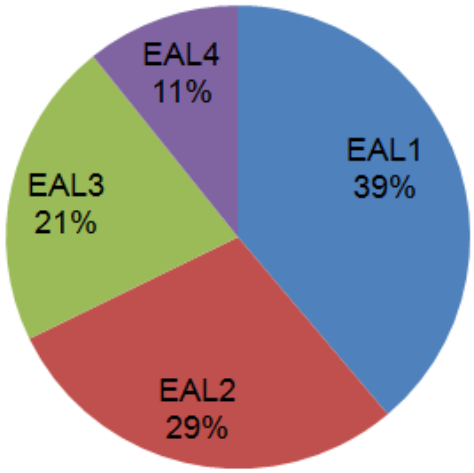

Fig. 17. Shares of certifications according to EAL (Russian IT Security Certification Scheme)

After the regulations setting information security requirements in compliance with Common Criteria have entered into force, both national and foreign developers used to certify their products according to new requirements. Foreign companies McAfee and Trend Micro appeared to be the first to get products certified. Safety Code LLC and Kaspersky Laboratory CJSC were among domestic developers which received the certificates of conformity from FSTEC of Russia.

Labor consumption in certification tests according to the new requirements need to be discussed individually. The analysis carried out by experts from the test laboratory of Echelon NPO CJSC makes it possible to conclude that predetermined labor consumption of the tests has not much changed as compared to the traditional approach. Fig. 18 shows distribution of resources available in a test laboratory for certification in compliance with new regulations (based on the analysis of performance of Echelon NPO CJSC accredited test laboratory).

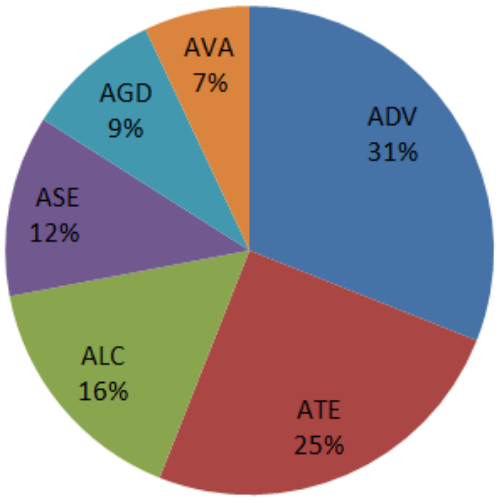

Fig. 18. Distribution of cost incurred by the test laboratory for certification in compliance with new regulations from FSTEC of Russia

4 Conclusions

Based on processed information from the official site of the FSTEC of Russia, one may reach the following conclusions concerning to Russian IT Security Certification Scheme.

1. First certifications according to the new requirements involved foreign-made TOE. The fact is the documents needed for certification in compliance with new requirements have been originated for certification in accordance with Common Criteria Certification Schemes.
2. The "batch" certification shall be gradually substituted by the "series" pattern since new regulations require applicants to maintain certified software at all stages of the life cycle.
3. More and more leading foreign developers provide the Russian test laboratories with an access to their source code, and this tendency shall be observed in future.
4. Introduction of new regulations shall enhance efficiency in detection of vulnerabilities in software submitted for certification. In the new documents the vulnerability assessment procedure is obligatory during certification with regard to all classes of security. In certification based on the traditional ruling documents the search for vulnerabilities is not an obligatory procedure and such search has been performed only by zealots for certification. For instance, the test laboratory in NPO Echelon revealed vulnerabilities in 50% (both the Russian-made and foreign-made) submitted for certification according to the new regulations. It should be noted that all vulnerabilities detected by NPO Echelon have been eliminated by developers.
5. The Russian developers shall pay more for certification. Even during certification for most popular Protection Class (Class 4) which has nothing to do with security of information comprising a state secret, EAL 3 is to be reached. The challenge is related to developer's evidences required which are relatively new (correlation with GOST is nearly absent) and procedures originated by FSTEC of Russia for developers are not available.
6. Costs of test laboratories for test procedures shall grow. The number of actively working laboratories will reduce since lack of procedures will make most of laboratories incapable of performing tests to satisfy new requirements.

Possibly, test laboratories will be accredited by the highest security class (EAL) for which the laboratory may perform tests.

References

1. A.V. Barabanov, A.S. Markov, V.L. Tsirlov Certification of intrusion detection systems // Open systems. DBMS - 2012. - № 3. - C. 31-33.
2. A.S. Markov, V.L. Tsirlov, A.V. Barabanov Methods for assessment of non-conformity of information security facilities / Edited by A.S. Markov - M.: Radio & Communication, 2012. - 192 p.
3. Official site of the FSTEC of Russia: *http://www.fstec.ru*
4. Common Criteria portal: https://www.commoncriteriaportal.org/
5. Wes J. Lloyd, «A Common Criteria Based Approach for COTS Component Selection», Special issue: 6th GPCE Young Researchers Workshop 2004.

About the authors

Alexander Barabanov - CISSP, CSSLP, Head of Certification and Testing Department in NPO Echelon.

Alexey Markov – Ph.D, CISSP, CEO and Founder of NPO Echelon.

Valentin Tsirlov – Ph.D, CISSP, CISM, AMBCI, Executive Director and Co-Founder of NPO Echelon.

NPO Echelon, CJSC is a Moscow-based leading Russian IT security Testing Laboratory. Established in 2007, NPO Echelon has for the last 5 years become a leading, reliable partner for software and hardware developers. Among our customers are SAP AG, IBM, Microsoft, Eset, McAfee, Symantec, Huawei, etc.