

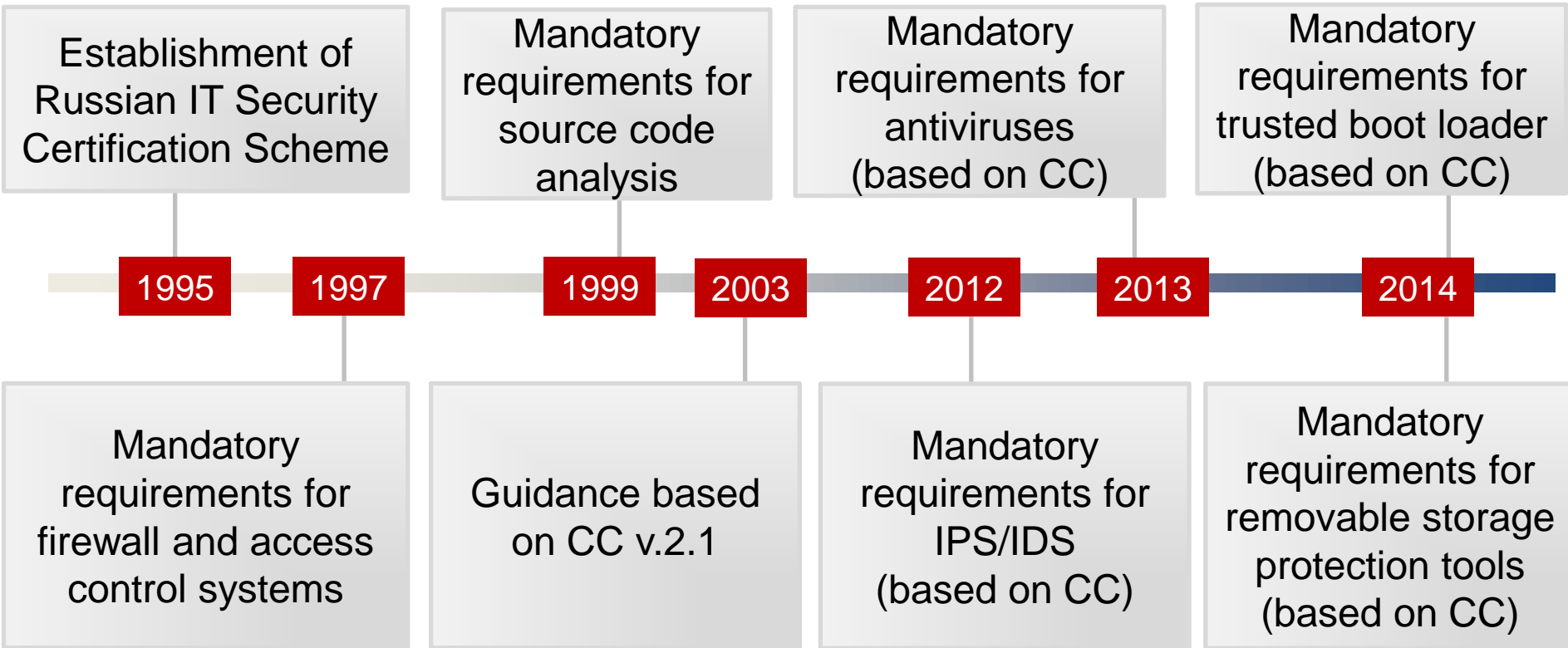
# Secure software development in the Russian IT Security Certification Scheme

Alexander Barabanov, Alexey Markov, Valentin Tsirlov

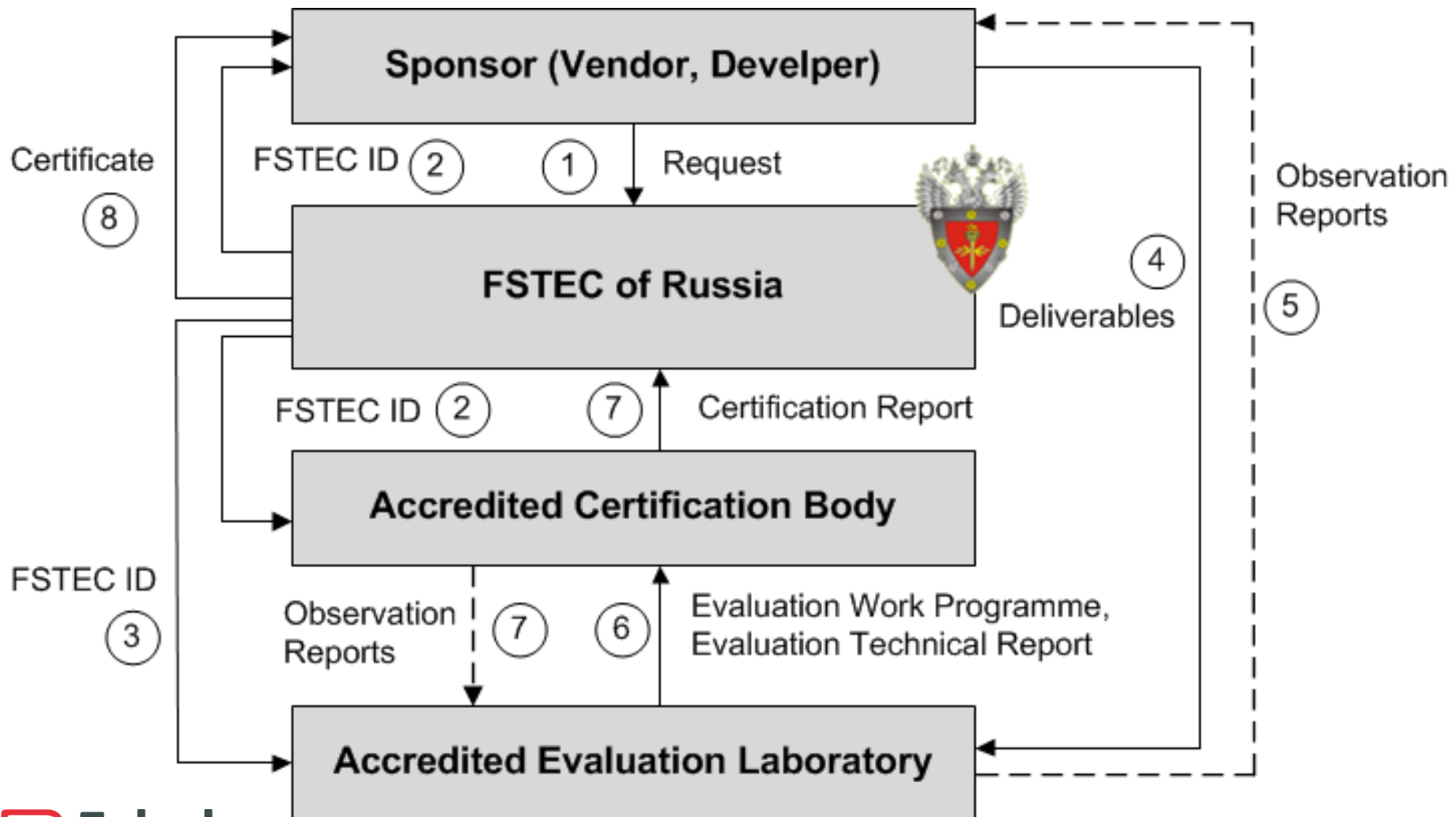
# Agenda

- Brief overview
- Current status of the Russian IT Security Certification Scheme
- Steps Toward Common Criteria Approach and Secure Software Development
- Final Remarks

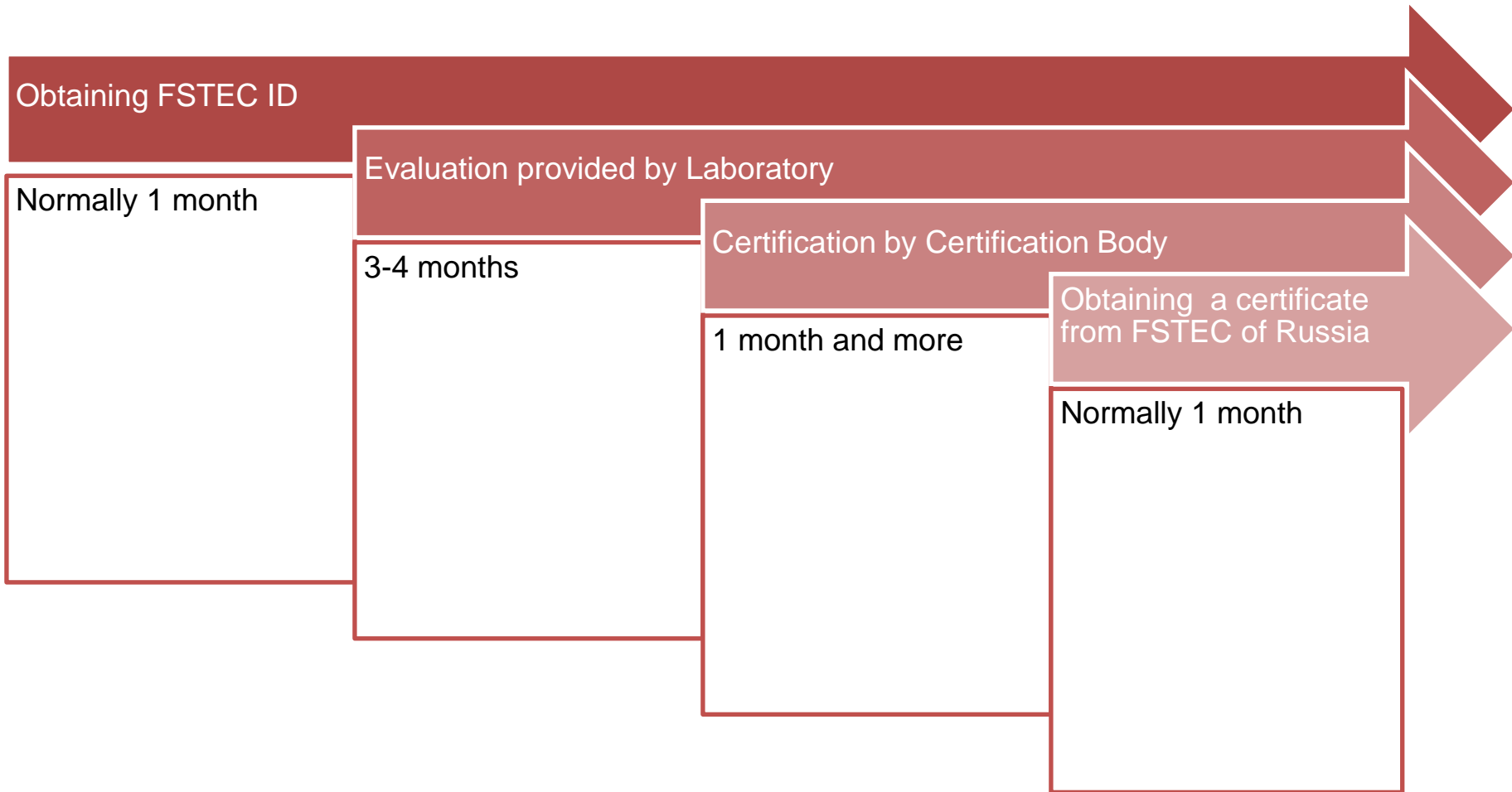
# Brief overview: Historical Perspective



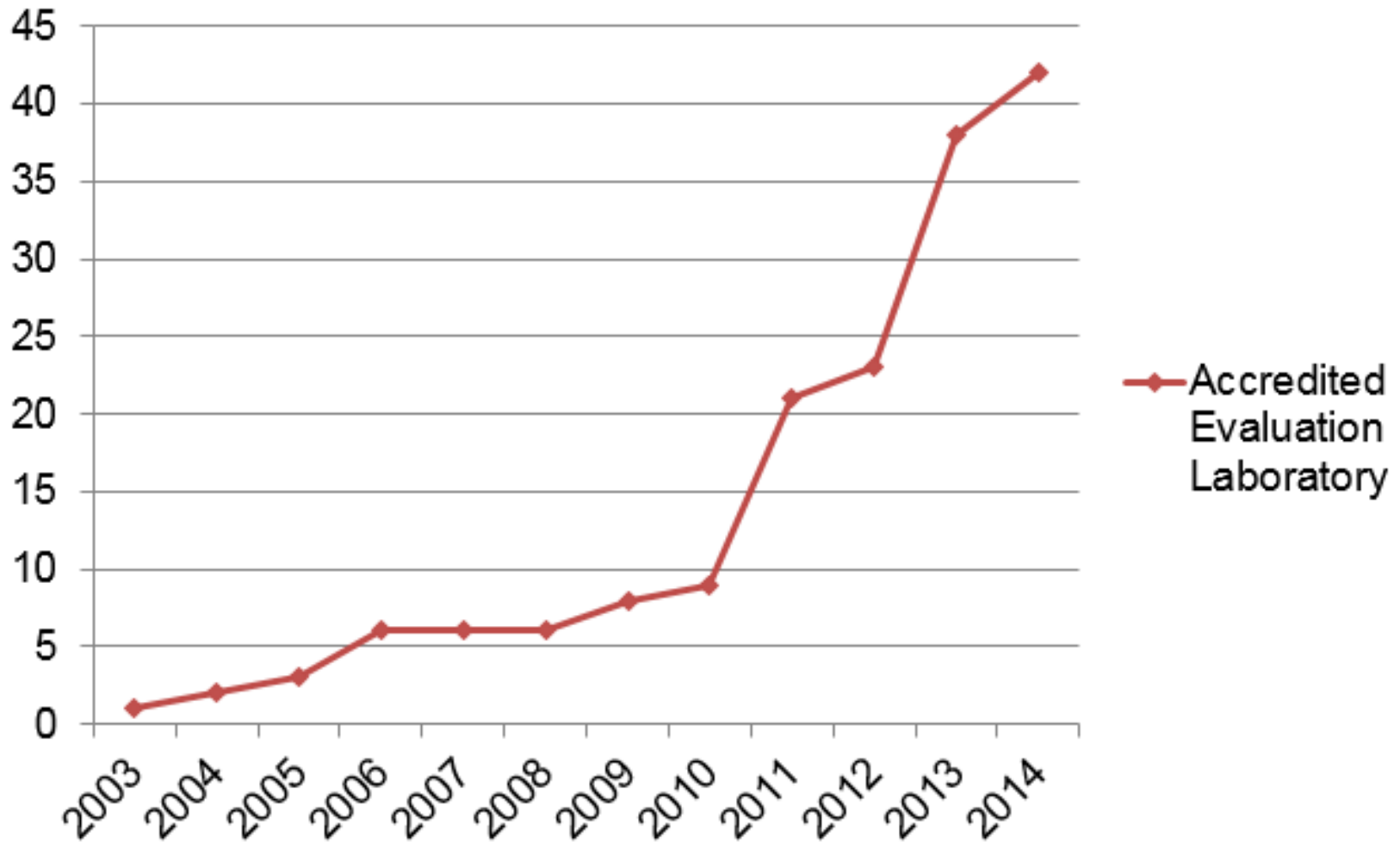
# Brief overview: who takes part in the certification process?



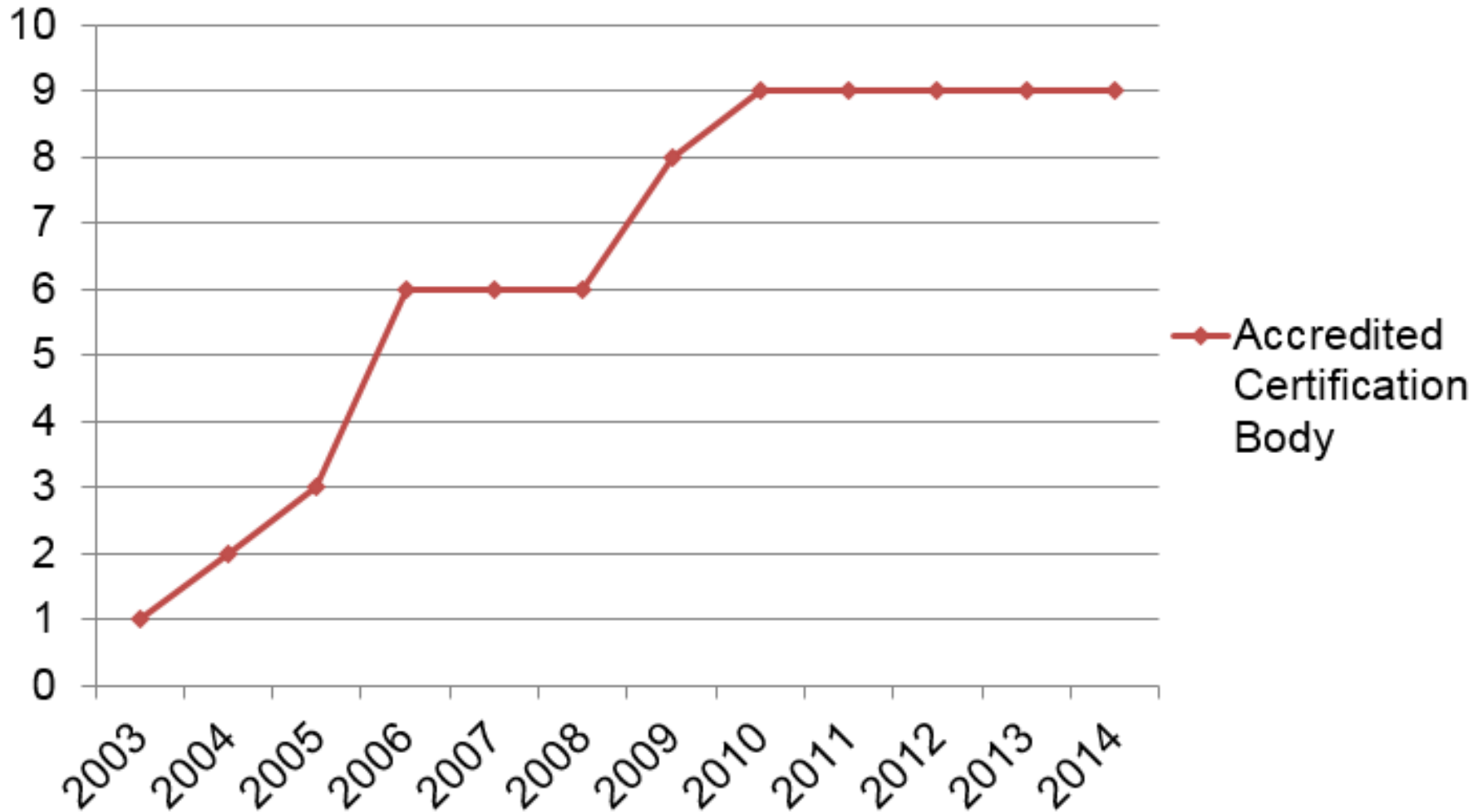
# Brief overview: typical timeline



# Brief overview: Accredited Evaluation Laboratories



# Brief overview: Accredited Certification Bodies



# Brief overview:

## Classical Major Approaches to Evaluation

### Evaluation of the security functionality

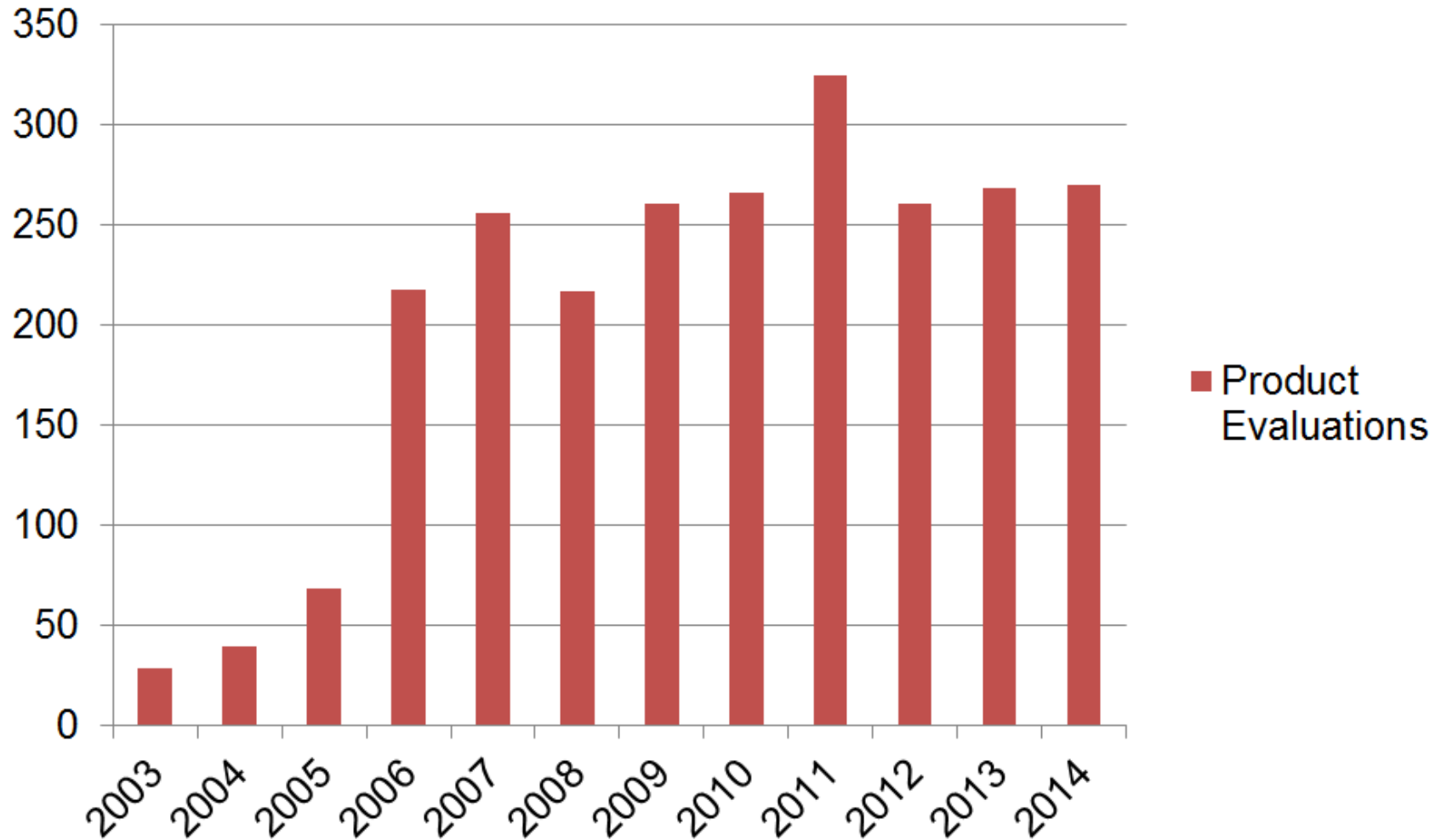
- Black box testing to ensure that TOE works as it should

### Evaluation for the absence of non-declared functions

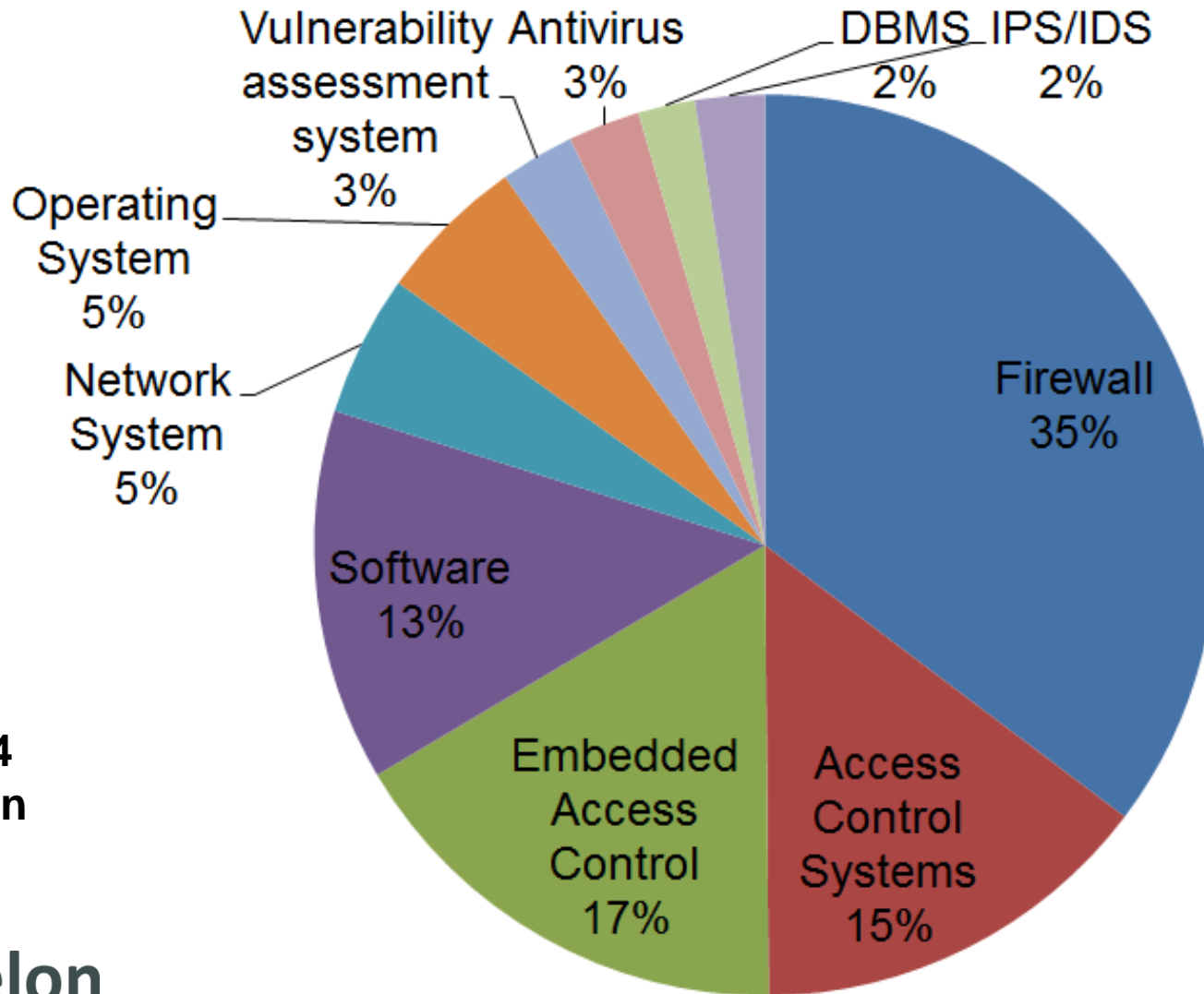
- Testing of source code for the absence of software vulnerabilities



# Current status of the Russian Scheme: Products Evaluations

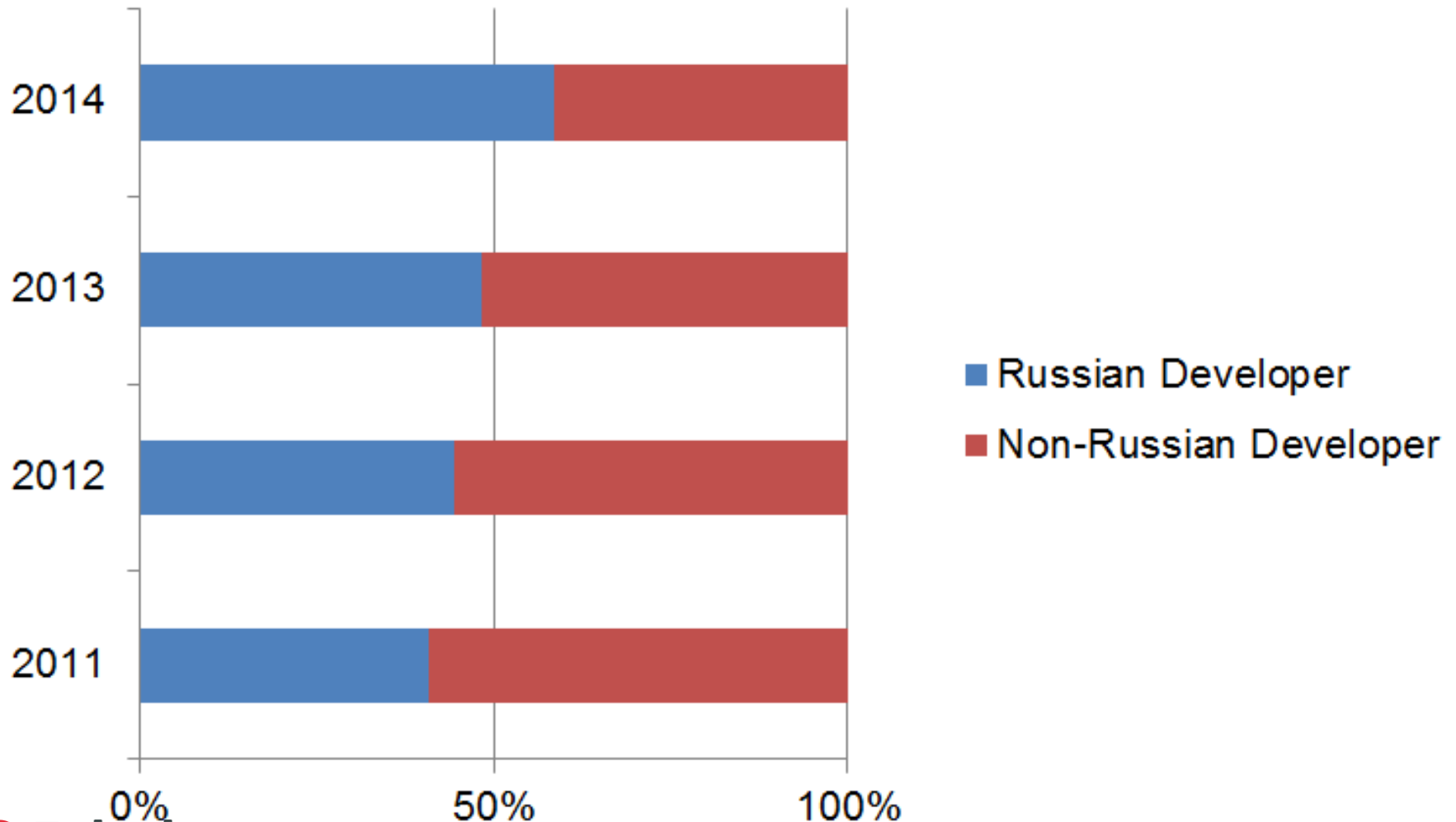


# Current status of the Russian Scheme: Certified Products by Types

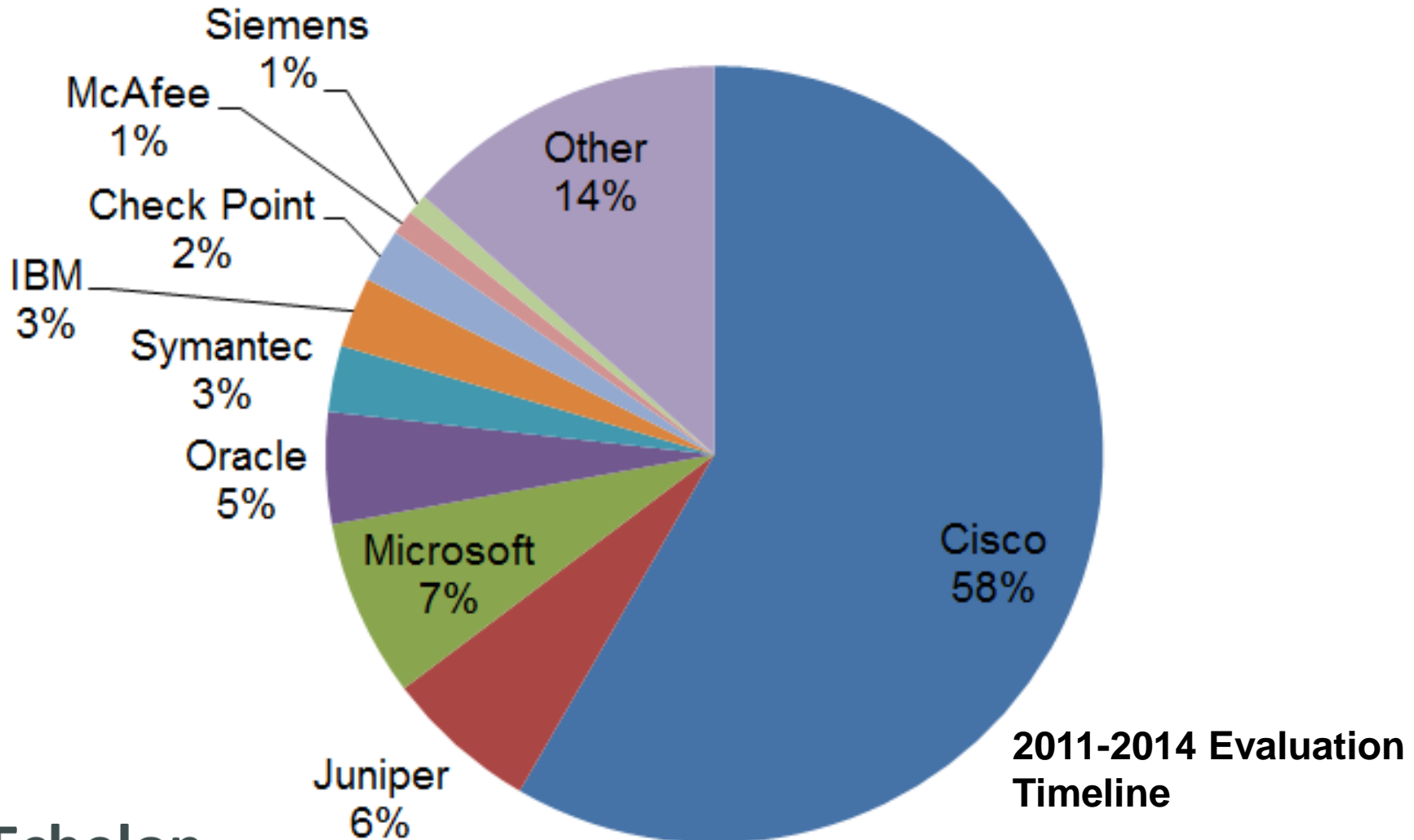


**2011-2014  
Evaluation  
Timeline**

# Current status of the Russian Scheme: Russian vs. Non-Russian Developers

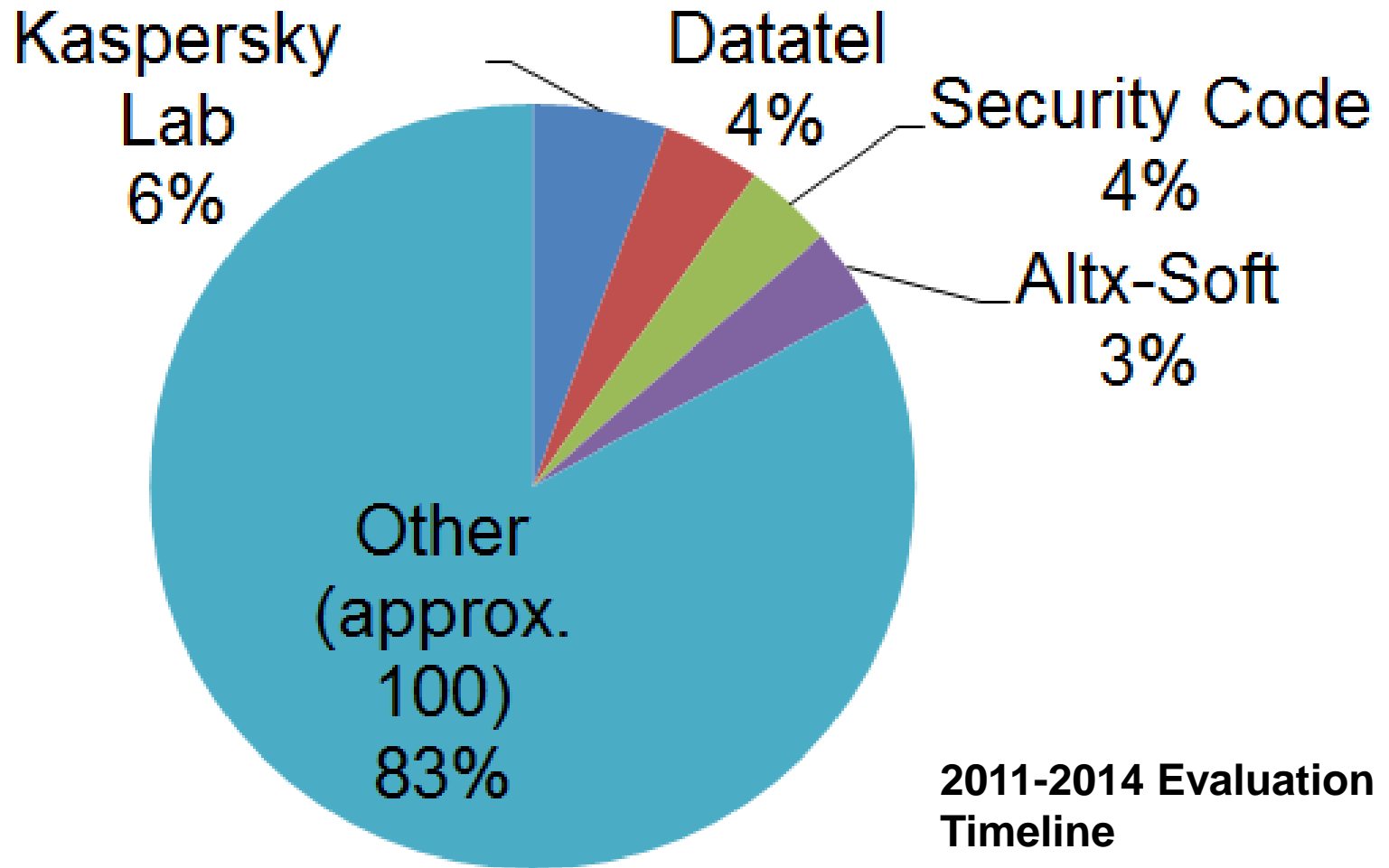


# Current status of the Russian Scheme: Non-Russian Developers (2)

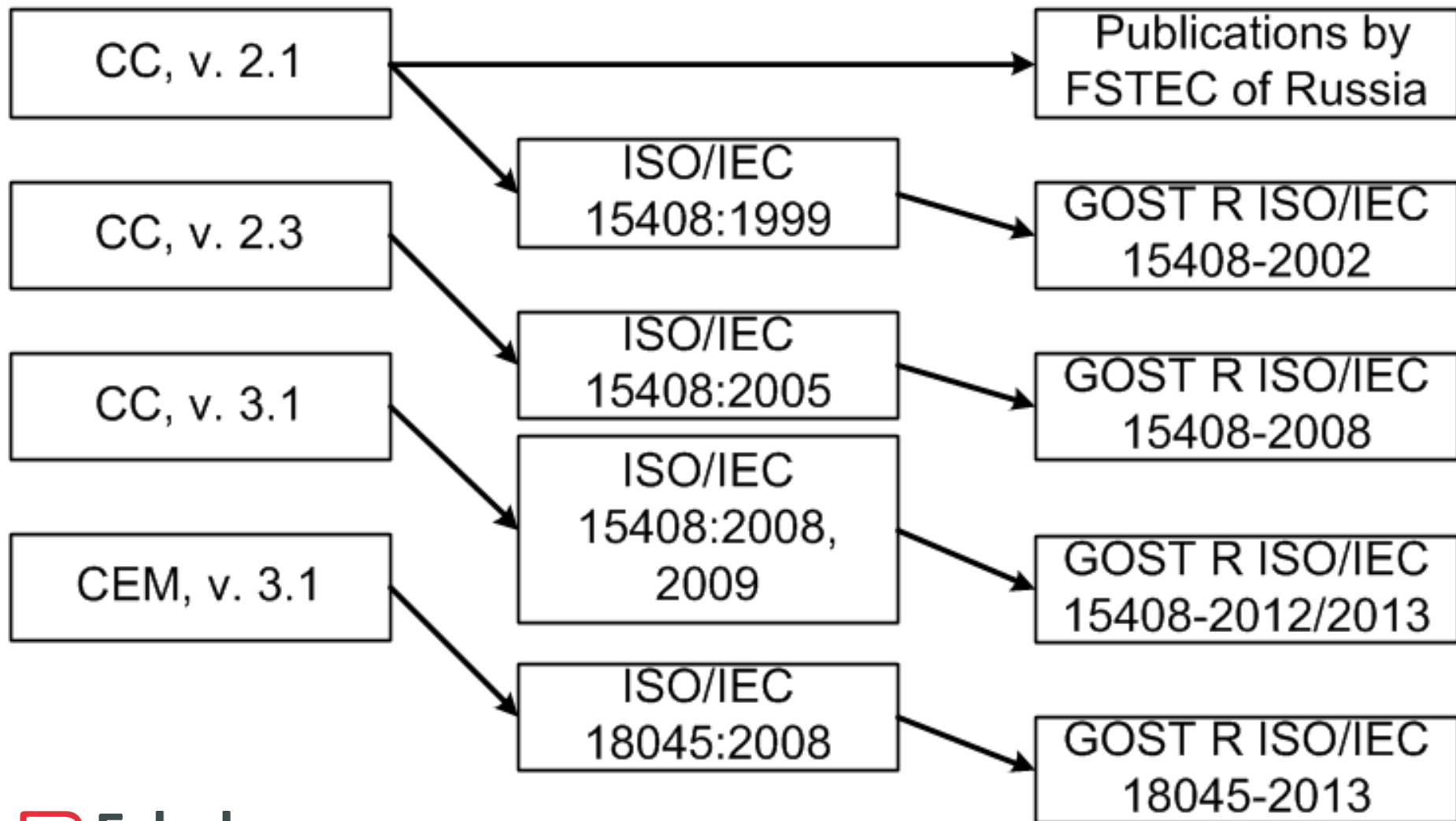


2011-2014 Evaluation  
Timeline

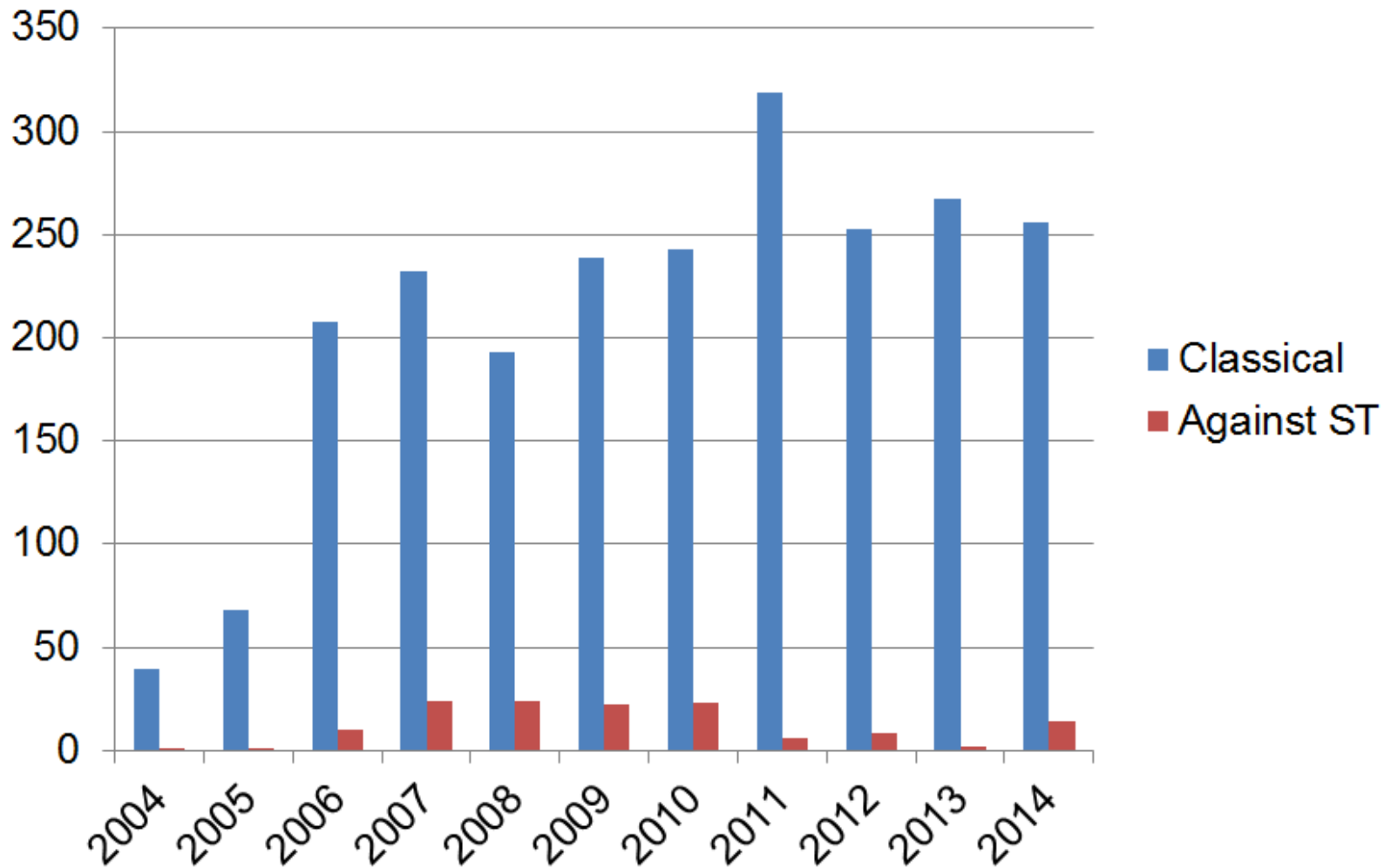
# Current status of the Russian Scheme: Russian Developers



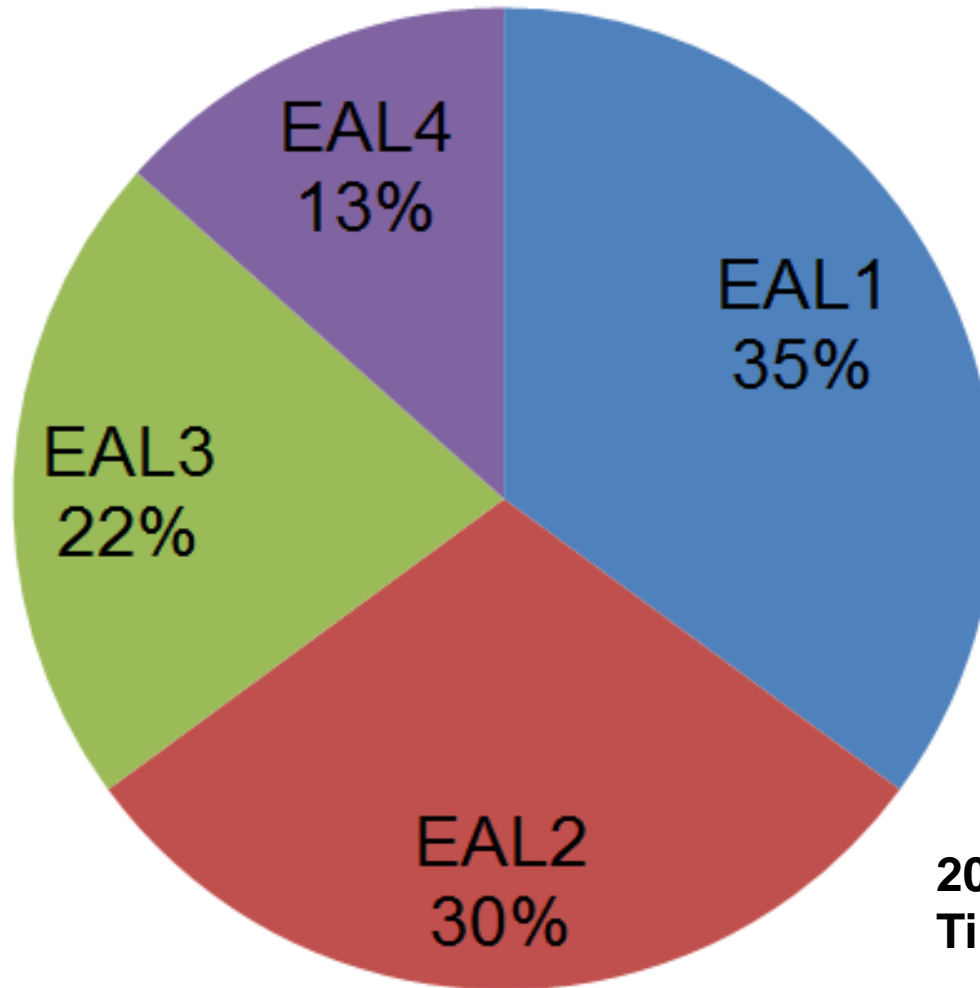
# Steps Toward Common Criteria Approach: Step #1 (1)



# Steps Toward Common Criteria Approach: Step #1 (2)



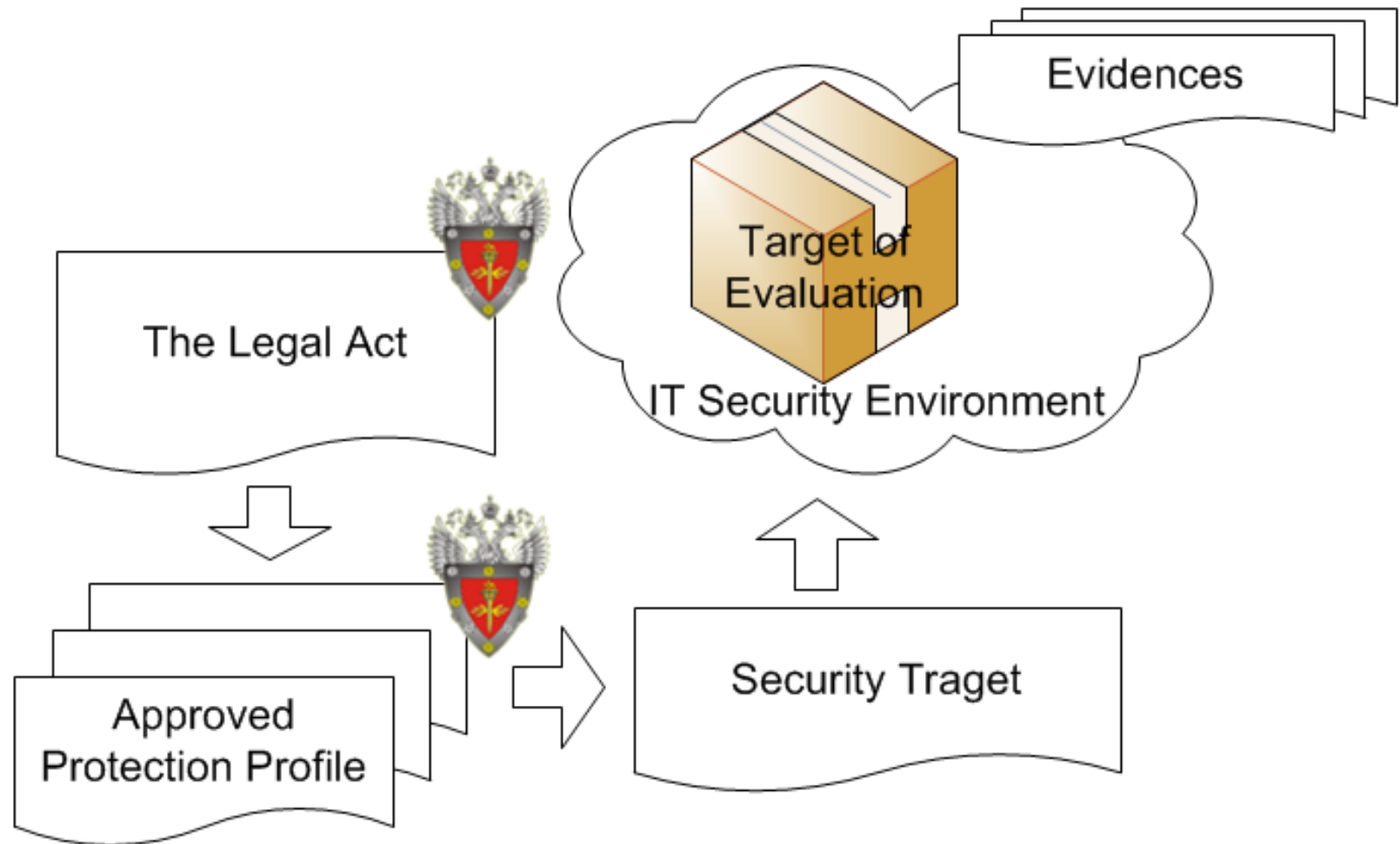
# Steps Toward Common Criteria Approach: Step #1 (3)



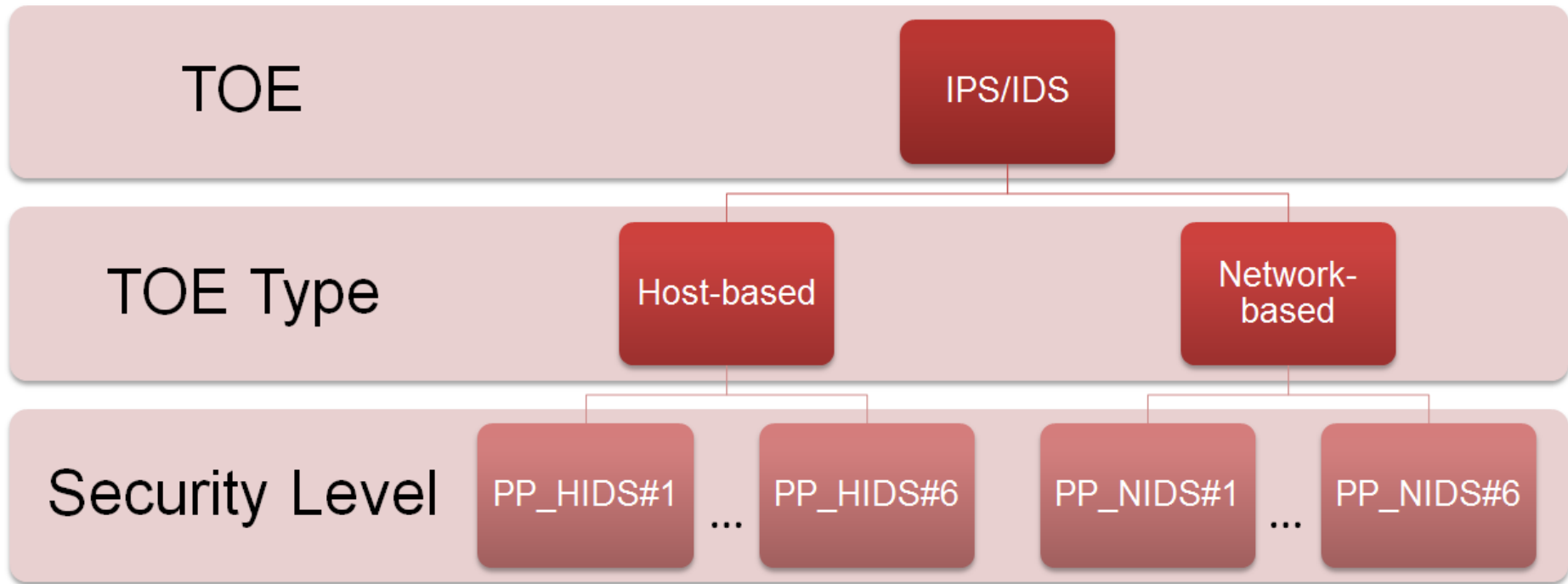
**2004-2014 Evaluation  
Timeline**



# Steps Toward Common Criteria Approach: Step #2 (1)



# Steps Toward Common Criteria Approach: Step #2 (2)



# Steps Toward Common Criteria Approach: Step #2 (3)

## FSTEC of Russia Approved Protection Profiles

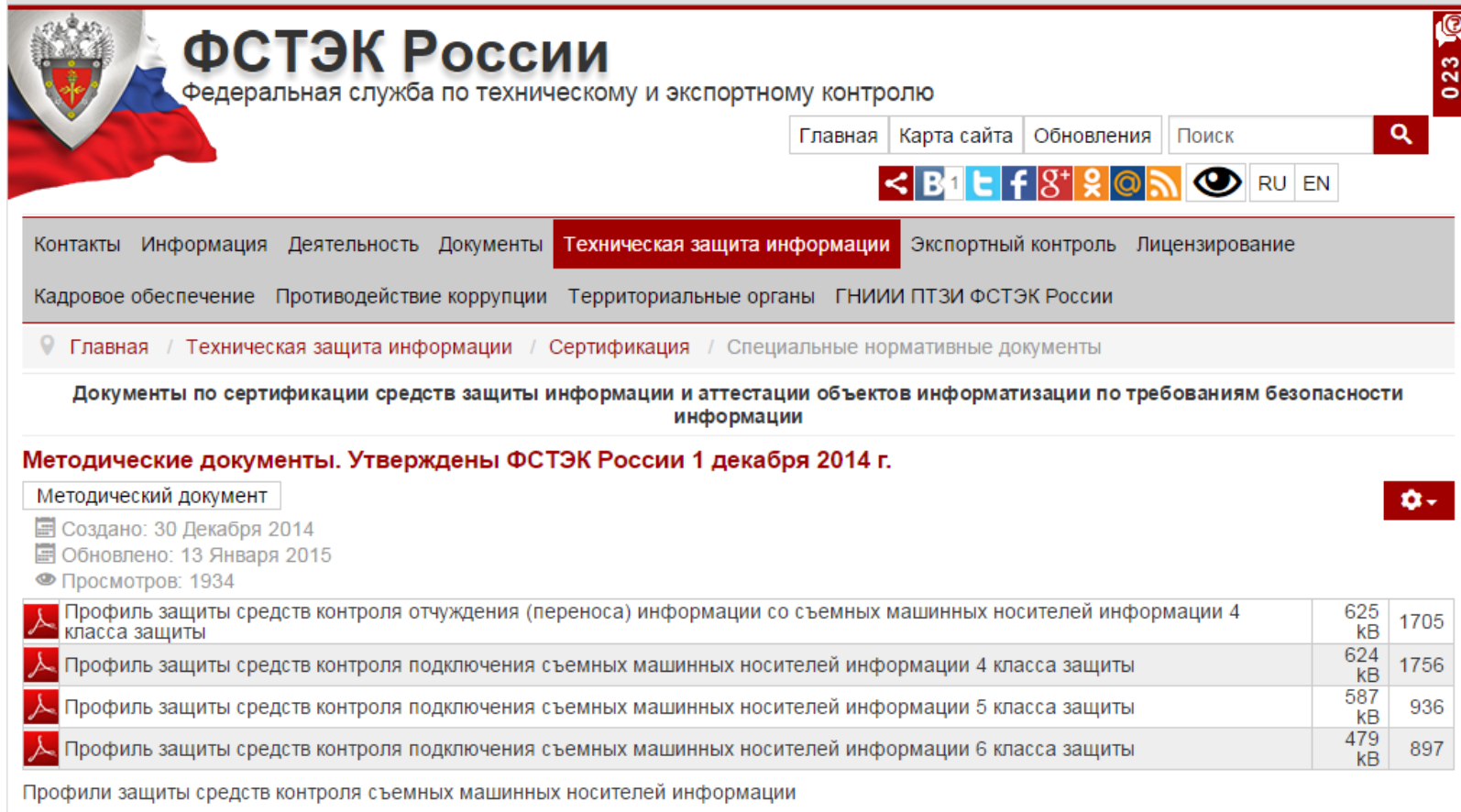
- PP for IPS/IDS
- PP for Antiviruses
- PP for Trusted Boot Loaders
- PP for Removable Storage Protection

## Protection Profiles in Development

- PP for Firewalls
- PP for Operating System
- PP for DBMS

# Steps Toward Common Criteria Approach: Step #2 (4)

<http://fstec.ru>



**ФСТЭК России**  
Федеральная служба по техническому и экспортному контролю

Главная | Карта сайта | Обновления | Поиск

Вконтакте | Одноклассники | Facebook | Google+ | Twitter | RSS | YouTube | RU | EN

Контакты | Информация | Деятельность | Документы | **Техническая защита информации** | Экспортный контроль | Лицензирование

Кадровое обеспечение | Противодействие коррупции | Территориальные органы | ГНИИИ ПТЗИ ФСТЭК России




Главная / Техническая защита информации / Сертификация / Специальные нормативные документы

**Документы по сертификации средств защиты информации и аттестации объектов информатизации по требованиям безопасности информации**

**Методические документы. Утверждены ФСТЭК России 1 декабря 2014 г.**

Методический документ

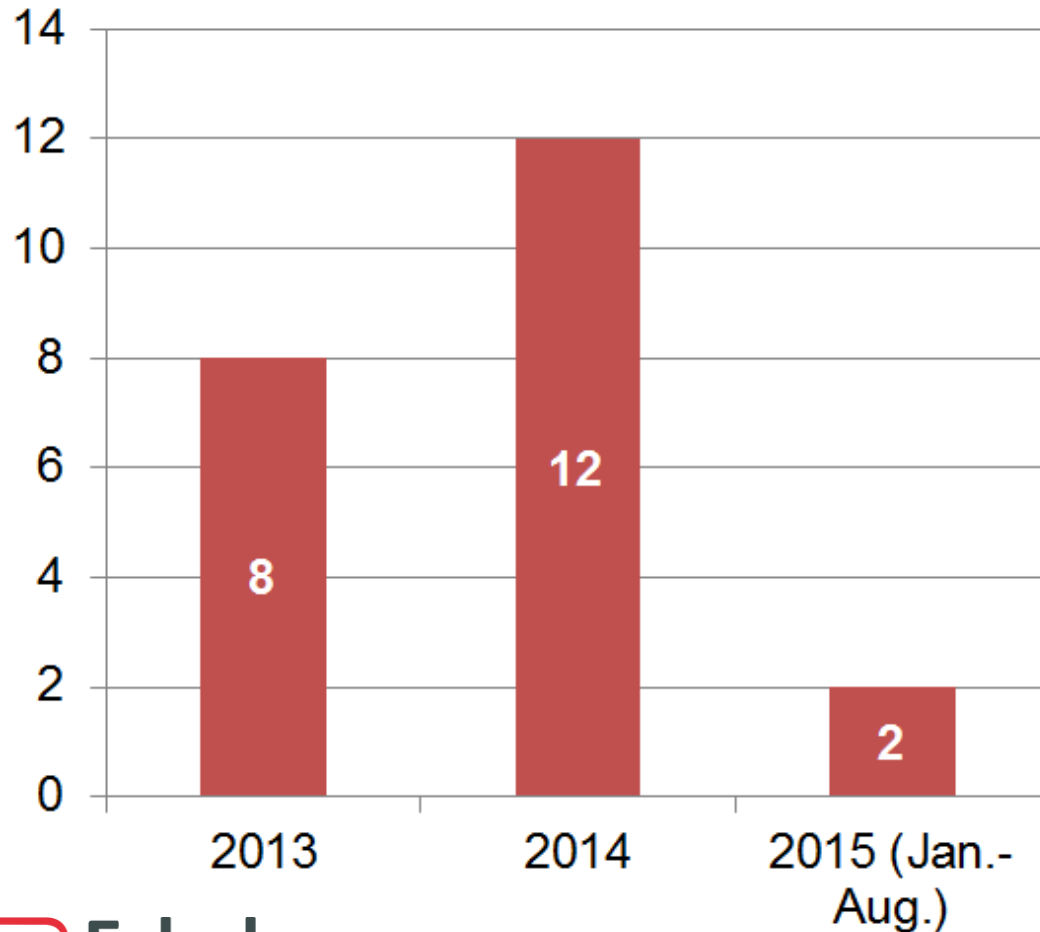
Создано: 30 Декабря 2014  
Обновлено: 13 Января 2015  
Просмотров: 1934

 Профиль защиты средств контроля отчуждения (переноса) информации со съемных машинных носителей информации 4 класса защиты	625 kB	1705
 Профиль защиты средств контроля подключения съемных машинных носителей информации 4 класса защиты	624 kB	1756
 Профиль защиты средств контроля подключения съемных машинных носителей информации 5 класса защиты	587 kB	936
 Профиль защиты средств контроля подключения съемных машинных носителей информации 6 класса защиты	479 kB	897

Профили защиты средств контроля съемных машинных носителей информации

# Certifications against new FSTEC of Russia requirements: projects summary

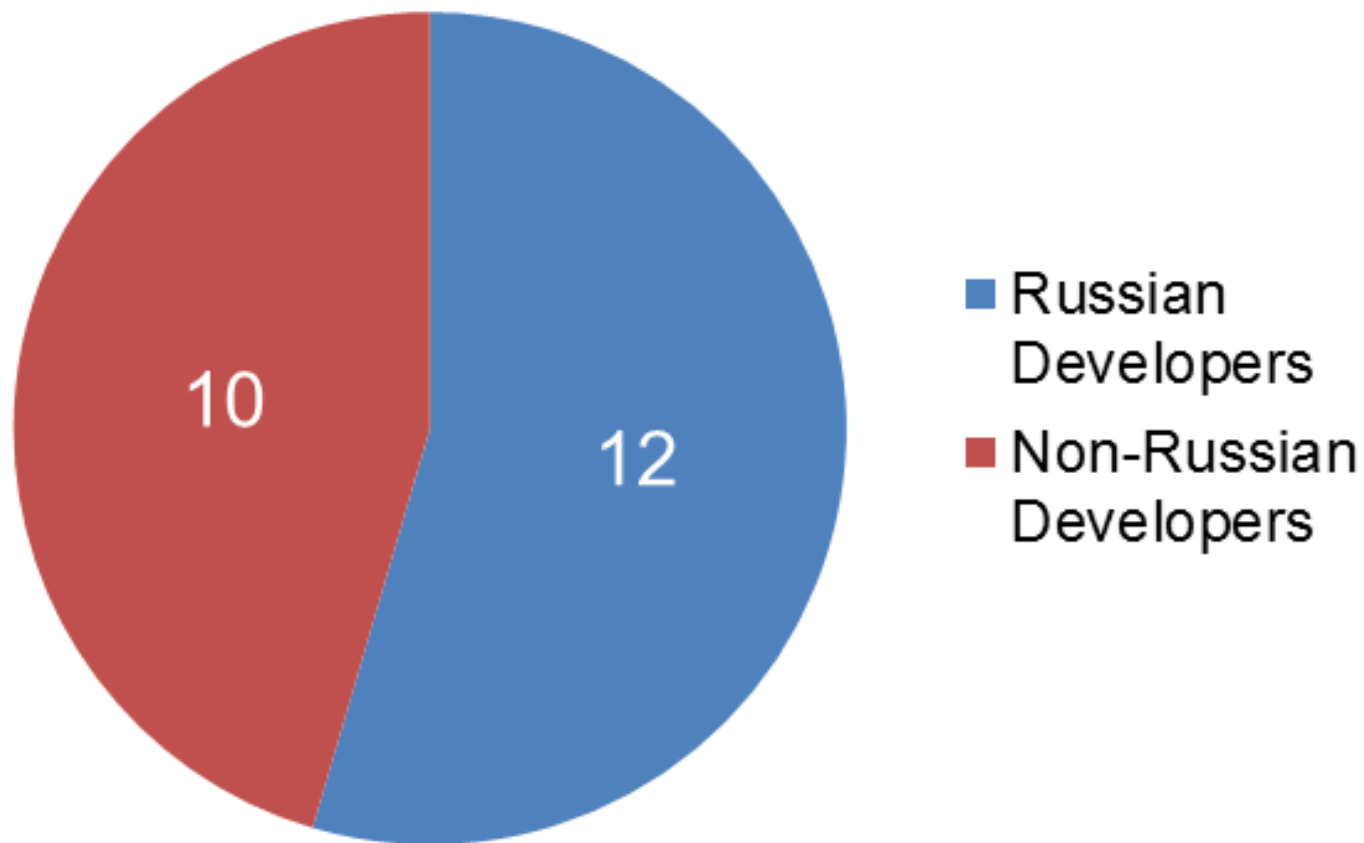
## Number of certifications



## Summary:

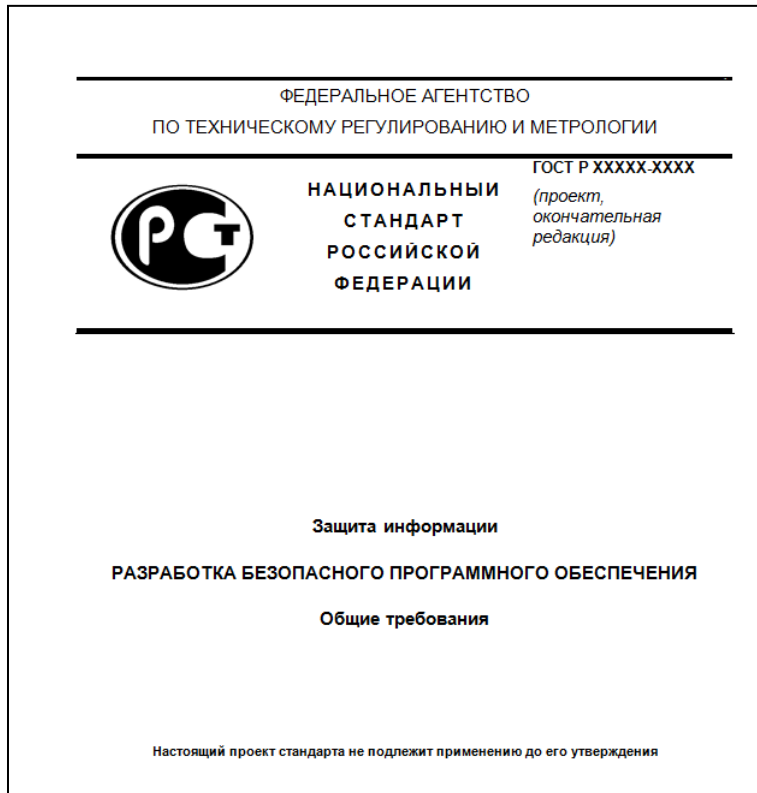
- **TOE Types:** IDS/IPS, Antivirus, Trusted boot loader
- **Vendors:** HP, McAfee, ESET, Trend Micro, PineApp, Kaspersky Lab, Cisco, Echelon, Altx-Soft, Secure Code
- **Number of active labs:** 4

# Certifications against new FSTEC of Russia requirements: Russian vs. non-Russian TOE



# Steps Toward Secure Software Development

## Russian standard «Information protection. Secure Software Development. General requirements» (draft)



## Proposed Secure Software Development Controls:

- information security threats modeling
- source code static/dynamic analysis
- source code review
- penetration testing
- ...

# Final Remarks

1. First certifications according to the new requirements were provided for non-Russian products.
2. More and more leading non-Russian developers provide the Russian Evaluations Laboratories with access to their source code, and this tendency shall be observed in the future.
3. Efficiency in detection of vulnerabilities in software submitted for certification will advance.
4. Russian developers will pay more for certification.
5. The number of actively working Evaluations Laboratories will degrade.



# Contact Information

- Alexander Barabanov, Ph.D., CISSP, CSSLP  
NPO Echelon  
[ab@cnpo.ru](mailto:ab@cnpo.ru)
- Alexey Markov, Dr.Sc., CISSP, Member of IEEE  
NPO Echelon  
[am@cnpo.ru](mailto:am@cnpo.ru)
- Valentin Tsirlov, Ph.D., CISSP, CISM  
NPO Echelon  
[z@cnpo.ru](mailto:z@cnpo.ru)

Thank you for your attention!