The Future of Cryptography and IT Security Standardization

Academy of Cryptography of the Russian Federation

Alexander Bondarenko

Alexey Smirnov

Order of the Government of the Russian Federation

«On approval of the program «Digital economy of the Russian Federation» № 1632-p, 28th April 2017

Resolution of the Government of the Russian Federation

«On the management system of implementation of the national program «Digital economy of the Russian Federation», № 234, 2nd March 2019

National Program Structure

- Digital environment regulatory controls
- Digital infrastructure
- Human resources for digital economy
- Information security
- Digital technologies
- Digital public administration

Federal project “Information security"

- Establishment of a sustainable and secure information and telecommunication infrastructure for the high-speed transmission, processing and storage of large volumes of data, accessible to all organizations and households
- Use of primarily domestic software by government agencies, local governments and organizations

Threats

- Illegal access and use of a citizen's digital profile
- Collection of "sensitive" information about the activities, preferences and interests of citizens in the Internet
- Emergence of new security threats while using the new digital technologies assumed for implementation by the national program "Digital Economy"

Protection principles (1/2)

- Systematic approach for identification of security threats and their origin
- The process of identifying information security threats should cover all protection objects and segments
- Each digital infrastructure segment should be provided with a specific attacker threat model, taking into account the technological peculiarities of the segment and organizational measures

Protection principles (2/2)

- The boundaries of responsibility of the actors and the rules for their interaction in the process of identifying information security threats should be defined

- It is necessary to clarify the origin and relevance of threats throughout the entire life cycle of the digital infrastructure

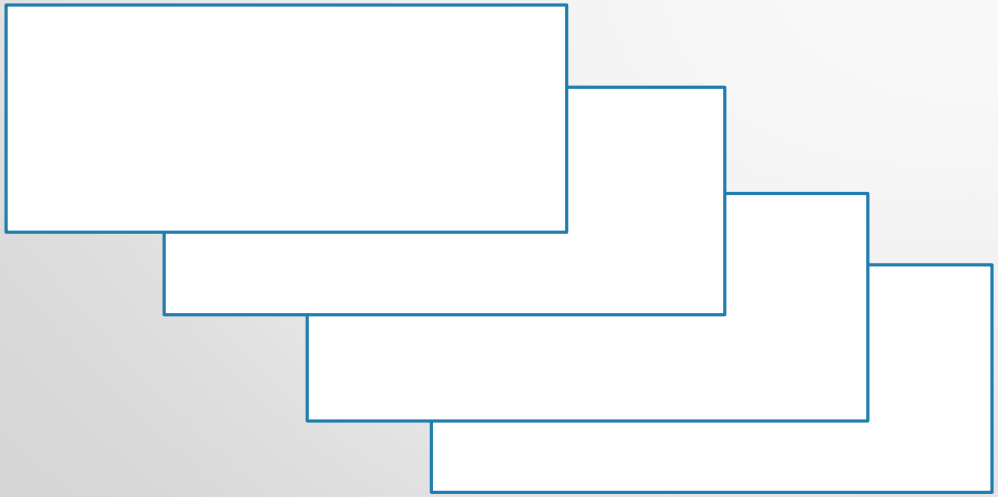
Academy of Cryptography of the Russian Federation

- Academy is one of the implementers of the federal project «Information security»

- The main goal:

  Information-analytical support and coordination of the participation of Russian experts in the activities of major international organizations involved in the development of standards in the field of cryptography and information technology security

Scientific research center



Laboratory of cryptography and IT security standardisation challenges

(Лаборатория проблем стандартизации в области криптографии и безопасности информационных технологий)

Research directions for 2019-2020 (1/2)

- Cryptographic mechanism for information protection in high frequency devices
- Cryptographic mechanisms in payment systems
- Cryptographic mechanism in wireless networks
- Perspective methods for cryptographic data protection
- Design challenges of modern data centers

Research directions for 2019-2020 (2/2)

- Challenges in design and unification of operating systems
- Challenges in unification of information security policies in cloud technologies
- Challenges in detection of information security incidents
- Information security aspects of the new digital technologies assumed for implementation by the national program "Digital Economy“
- Challenges in development systems of detection, prevention and elimination of consequences of computer attacks

Cooperation with standardisation committees and organisations

- TC 26 «Cryptography and security mechanisms»
- TC 362 «Information protection»
- TC 194 «Cyber-physical systems»

- ISO/IEC JTC 1 SC 27
- ITU
- IETF

Questions?