Journal of Computer Virology and Hacking Techniques (2022) 18:1–2
https://doi.org/10.1007/s11416-021-00415-w

EDITORIAL

Editorial

Alexey E. Zhukov[1]

Published online: 18 January 2022

This special issue of Journal of Computer Virology and Hacking Techniques offers to its readers a selection of extended versions of talks presented at the RusCrypto conference, which has been held annually by the RusCrypto Association for more than 20 years.

The RusCrypto Association was established in 1999. The creation of a public organization that unites all those who are interested in the development of civil cryptography[1] was an objective necessity for Russian Federation.

The declaration on the establishment of the RusCrypto Association notes that the development of civil cryptography in Russia is a strategically important task. However, its solution is hindered by the lack of unity and cohesiveness of developers, manufacturers and consumers of cryptography. Therefore, it becomes relevant to create an organization that coordinates the efforts of researchers, developers, manufacturers and consumers of cryptographic solutions in order to balance the interests of the individual, society and the state and to answer to them. The RusCrypto Association was established as a public non-profit organization whose activities are aimed at creating a self-regulating community of specialists in cryptography and information security in order to balance the interests of society and the state.

The main tasks of the RusCrypto Association are:

- Promotion and popularization of the possibilities and the latest achievements of Russian and foreign cryptology.
- Support for promising theoretical research and applied developments in cryptology and related sciences.
- Making people from different areas (academics, industry, government) meet and exchange ideas and views.
- Consumer protection from low-quality solutions in information technology.
- Discussing and commenting the Russian standardization processes (GOST) in information security and contributing to them.
- Openness to cooperation with the international cryptographic community by welcoming with foreign experts and exchanging with them.
- Protection of the interests of Russia in the process of integration into the global information.

One of the most important aspects of the activities of the RusCrypto Association is the organization of annual scientific and practical conferences. Since 1999, the RusCrypto Association has held 23 conferences.

The RusCrypto conference is a platform for communication between a wide range of people related to information security issues. These are leading Russian and foreign experts in cryptography and information security, solution development companies, representatives of banks, investment funds and industrial enterprises, government officials, lawyers, and journalists.

Traditionally, the conference is attended by students of leading Russian universities specializing in information security.

The topics of the conference are not limited exclusively to theoretical issues of cryptography. The conference discusses the latest developments in the field of cryptographic algorithms and protocols, legal and economic and political aspects of the use of developments in the field of civil cryptography, discusses modern software and hardware solutions for information security, implementation issues, forensics issues. Companies participating in the conference present products that are related to data protection.

The business part of the event includes numerous breakout sessions, round tables (panel sessions) and master classes.

✉ Alexey E. Zhukov
aez_iu8@rambler.ru

[1] RusCrypto Association, Moscow, Russia

[1] *Civil cryptography* is a term used in Russia and means mass cryptography or cryptography for mass use. Other names: open cryptography, public cryptography – i.e. that part of cryptography that develops in the interests of individuals, society, and business. It differs from *state cryptography*, which ensures the interests of government departments.

The main topics of the sections and of the round tables are as follows:

- Cryptography and cryptanalysis.
- National and international standardization in the field of cryptographic information protection.
- Cryptographic solutions for mass use.
- Issues of information security within the framework of the national program «Digital Economy of the Russian Federation».
- Quantum cryptography: theory and practical application.
- High-speed encryption tools.
- Cryptography in IoT and M2M.
- Cryptography in cloud solutions.
- Information security and cryptography in payment systems.
- Security of solutions based on blockchain technologies. The use of Russian cryptography in data chain recording technologies and distributed registries.
- Academic research in information security.
- Trusted environments.
- Technologies of electronic document management.
- Legal aspects of the development and implementation of information security systems in modern legislation and law enforcement practice.
- Engineering, technical and legal aspects of digital forensics and forensic examination.
- Training of specialists in information security, including in mathematical and computer cryptology, in the public education system.
- Russian products for the Russian market: Import substitution and development of cryptographic information security tools.
- Current trends in the development of cryptography.
- Advanced research in the field of cybersecurity.

The working language of the conference is Russian (although it should be noted that foreign participants of the conference often make reports in their native language with the assistance of direct translation for the audience). Some Russian participants of the conference who, in the opinion of the program committee, presented the most interesting reports, kindly agreed to prepare articles in English based on the materials included in their reports. We offer these articles to the readers of the special issue of Journal of Computer Virology and Hacking Techniques.