National Center for Digital Economy

Trust and Security in the Digital Economy: Lessons from Russia

Tatiana Ershova
Director
NCDE, Lomonosov Moscow State University

Second Regional Internet Freedom Summit

Struga, Macedonia, 22 March 2018

Key Factors Affecting the Development of the Digital Economy

Non-digital Factors	Digital Factors

• Public Policy and Strategic Planning
• Leadership and Institutions
• Legislation, Regulation and Standards
• Human Capital
• R&D and Innovation
• Business Environment
• Trust and Security in the Digital Environment
	• Digital Infrastructure
	• Shared Digital Platforms and Services
	• New / Emerging Digital Technologies
	• Digital Sector of Economy
	  • ICT Sector
	  • Sector of Content and Media
	• Digital Transformation of the Public Sector
	  • Digital Government
	  • Digital Healthcare
	  • Digital Education
	  • Digital Culture
	• Digital Transformation of Business
	• Digital Citizens / Consumers

Trust and Security in the Digital Economy – the Concept

- Secure information infrastructure:
  - network security
  - management of data security (accessibility, integrity, confidentiality), including:
    - trust to cloud services
    - critical user errors
    - authenticity of online transactions
- Increasing the confidence of citizens and businesses in digital technologies:
  - ensuring the privacy of online work and mastering the ways to protect it
  - overcoming obstacles to the effective use of documents and making transactions in electronic form
  - protection of user data and consumer rights
  - anti-spam protection
  - development of secure and reliable apps

National Center for Digital Economy

At the Global Level (1)

- Geneva Declaration of Principles: Building the Information Society: a global challenge in the new Millennium (WSIS, 12 December 2003), B5: Building confidence and security in the use of ICTs, pp. 35-37:
  - strengthening the trust framework, including information security and network security, authentication, privacy and consumer protection, is a prerequisite for the development of the Information Society and for building confidence among users of ICTs
  - a global culture of cyber-security needs to be promoted, developed and implemented in cooperation with all stakeholders and international expert bodies
    - these efforts should be supported by increased international cooperation
- Geneva Plan of Action, C5, p. 12:
  - confidence and security are among the main pillars of the Information Society
- Global Cybersecurity Agenda (International Telecommunication Union), 2007
  - legal, technical and procedural measures, institutions, capacity-building, international cooperation

National Center for Digital Economy

At the Global Level (2)

- The Budapest Convention on Cybercrime, 23 November 2001, signed by over 50 states, (Russia did not join)
- The concept of CIS cooperation in the field of information security (approved by the Council of Heads of CIS States, 10 October 10, 2008)
- The member states of the Shanghai Cooperation Organization introduced ‘Rules of Conduct in the field of Ensuring International Information Security’ as an official UN document (January 2015)
- Russia presented a draft UN convention ‘On Cooperation in Countering Informational Crime’ (2016)
  - excludes trans-border access to stored computer data during cybercrime investigations by the special services of various nations to protect national security and sovereignty

Russia’s Position in the International Ranking

ITU Global Cybersecurity Index
165 countries

No.	Country	Score
1	Singapore	0.925
2	USA	0.919
3	Malaysia	0.893
…		
9	Canada	0.818
10	Russia	0.788
11	Japan	0.786

At the National Level (1)

- National policy in the field of information security
  - the state policy in the sphere of information security is defined in the Doctrine of Information Security approved by the decree of the President of the Russian Federation in 2016
  - the information security policy is constantly updated and implemented in full
- Solving legal issues in the field of cybersecurity
  - protection of personal data, maintenance of 'black lists' and control of providers is carried out by the Federal Service for Supervision in the sphere of Communication, Information Technology and Mass Communications (Roskomnadzor, Federal Laws FZ 152 and FZ 139)
  - information security (non-cryptographic methods) in information and telecommunications infrastructure systems is controlled by the Federal Service for Technical and Export Control
  - the provision of information security (including the use of engineering and cryptographic means) is carried out by the Federal Security Service
  - the investigation of cybercrime is under the jurisdiction of the Ministry of Internal Affairs
  - each agency has its own certification and requirements for security and data protection solutions, but:
    - the certification process is different
    - but they are closely linked and mutually agreed

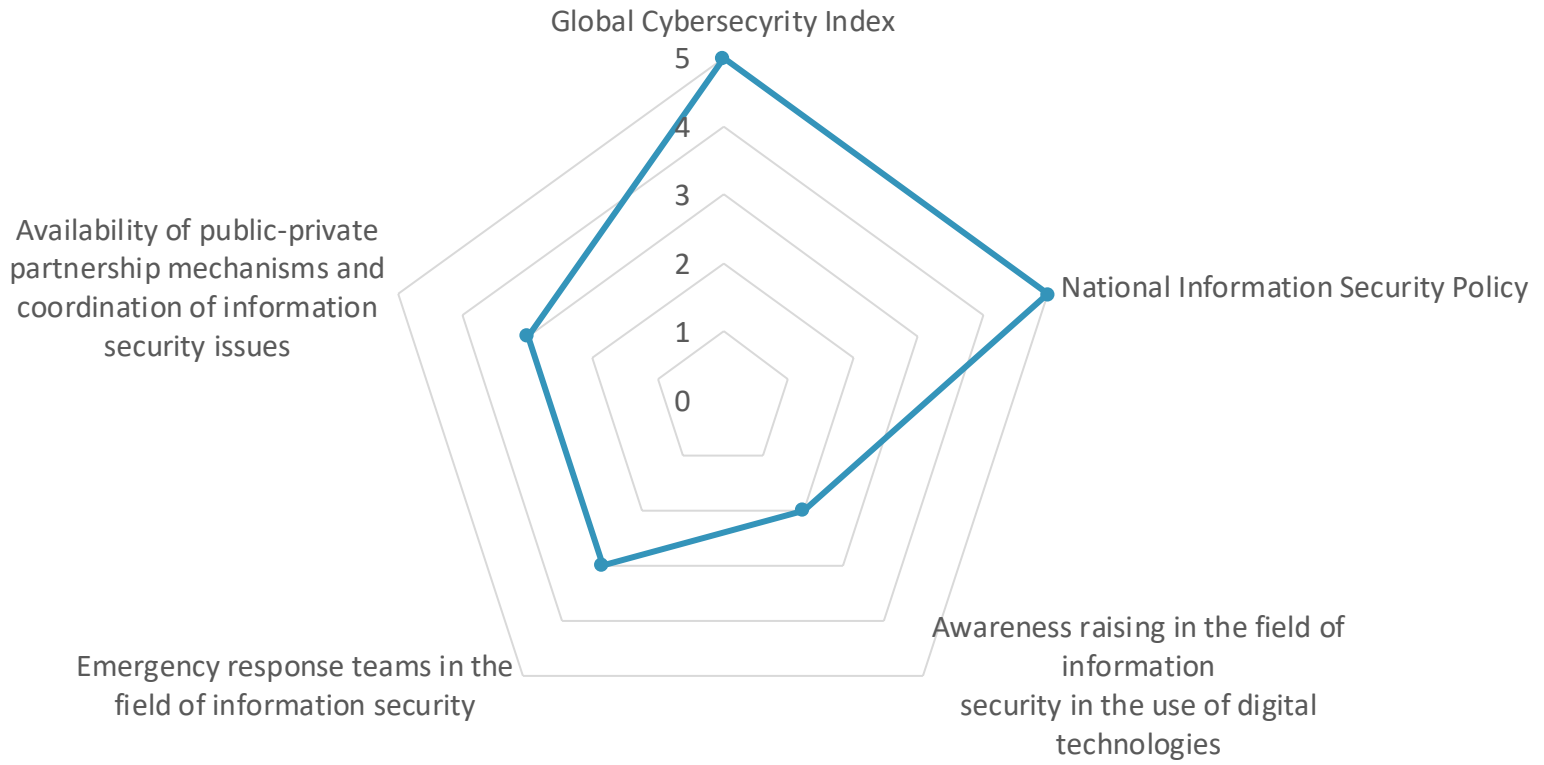
National Center for Digital Economy

At the National Level (2)

- Technical measures to ensure information security
  - centers for responding to computer incidents (CERTs) are established and functioning at the state and sectoral levels
  - centers for responding to computer incidents for the citizens are NOT created
    - the citizens may be subject to computer attacks, including those through social networks and messengers that are not in the jurisdiction of the Russian Federation
- Security of critical information infrastructure
  - is carried out in accordance with the law (Federal Law 'On the Security of the Critical Information Infrastructure of the Russian Federation' FZ 187 of 12 July, 2017) and the requirements to ensure the protection of information in automated control systems for production and technological processes in critical facilities, potentially hazardous facilities, as well as facilities representing increased danger to life and health of people and the environment
  - activities to protect the critical infrastructure is carried out using public-private partnership mechanisms
    - but there are few such mechanisms, and coordination of information security issues is insufficient
- Raising awareness of citizens and organizations about information security in the use of digital technologies
- there are no special programs of this kind in Russia
- relevant activities are carried out mainly by popularizing secure digital products and services – Internet banking, e-government services, etc.

National Center for Digital Economy

Trust and Security as Part of the World Bank Digital Economy Country Assessment (DECA Russia, 2017)



General Assessment of the Current Situation and Conclusions

- Russia is actively engaged in issues of information security
- At the same time, insufficient attention is paid to the involvement of the citizens in this process: they are ‘detached’ from these problems, and this creates threats to information security due to lack of basic awareness
  - the consequence of this problem is the public’s distrust of online business, e-commerce and other important components of the digital economy
    - according to the Federal Service for Supervision of Consumer Rights Protection and Human Welfare (Rospotrebnadzor), 42% of Russian respondents do not trust trade via the Internet
- Overall assessment – ***good***

National Center for Digital Economy

Key Actions on ‘Information Security’ within the ‘Russian Digital Economy Program’ (Action Plan approved on 18 December 2017) (1)

- A clear task is set to provide technical, organizational and legal protection of the individual, business and state interests in the digital economy, including:
  - in the processing of personal data, large user data (including social networks and other means of social communication
    - legislative definition of rights and duties of participants in information interaction
    - ensuring control over the processing of and access to such data
    - imposing responsibility for proper processing and security of such data
  - legislative provision for the pre-installation of domestic anti-virus programs on all personal computers both imported and created on the territory of the Russian Federation
  - building a system of obtaining knowledge in the field of information security based on a national e-library

National Center for Digital Economy

Key Actions on ‘Information Security’ within the ‘Russian Digital Economy Program’ (2)

- With regard to the creation of technical tools to ensure the safe information interaction of citizens in the digital economy:
  - a specialized resource that provides Russian citizens with access to information about the use of their personal data, as well as the possibility of refusing such use
  - national knowledge base of indicators of harmful activity
  - antivirus scanner resource and checks for signs of malicious activity
  - national system of traffic filtering using information resources by children
  - a specialized resource designed to interact with authorized bodies in the area of data transmission on the signs of illegal activities in the field of information technology (computer fraud, imposed services of telecom operators, phishing schemes)
- In terms of creating organizational conditions and institutions:
  - national and regional computer incident response centers
  - mechanisms of state assistance to the growth of the market of information risk insurance services
  - system of expert organizations in the field of computer forensic

National Center for Digital Economy

Possible Additional Policy Measures (1)

- Targeted government efforts to raise awareness and understanding of cyber threats by society
  - support activities to protect from threats and mitigate the consequences for the citizens and orgs affected by cyberattacks and cyber fraud
    - providing people and companies with relevant and easy to implement recommendations
    - creating our own software
    - exchange of information on topical criminal threats
    - wide dissemination of this information
    - evaluation of the cost of cyber risks
    - formulating the obvious benefits of cybersecurity for business and the public
    - persuading orgs and citizens to take the necessary measures

National Center for Digital Economy

Possible Additional Policy Measures (2)

- Organization of cooperation to protect against threats and mitigate the consequences of cyberattacks and cyber fraud for citizens and orgs
  - involving authoritative personalities to expand the coverage of the society by the recommendations, increase their importance and trust to them
  - creating / using volunteer orgs / groups
  - creating blogs, social network groups, popular science programs on television
  - organizating cooperation between vendors, law enforcement agencies, representatives of industries and companies in order to prevent the emergence of groups of ‘deceived users’
  - involving organizations such as insurance companies, regulatory bodies, industry standardization bodies and investors that can influence business and the public in order to ensure cyber risks management on their part
  - developing and adopting cybersecurity standards and those for the protection of companies and citizens

National Center for Digital Economy

Contact Information

Tatiana Ershova

Director
National Center for Digital Economy
Lomonosov Moscow Sate University

Editor-in-Chief
Scientific and Analytical Journal ‘Information Society’

tatiana.ershova@digital.msu.ru

https://digital.msu.ru/
http://www.infosoc.iis.ru/