1. CYBERSECURITY

1.1 LEGAL MEASURES

1.1.1 CRIMINAL LEGISLATION
Specific legislation on cybercrime has been enacted through the following instrument:
- Criminal code (Chapter 28: Articles 272-274)

1.1.2 REGULATION AND COMPLIANCE
Specific legislation related to cybersecurity has been enacted through the following normative legal instruments (these instruments contain measures to combat spam, protect legal entity and individual information, technical and legislative regulation and others):

- Order of the Russian President No 557-rp of 15.11.2005 "On signing the Convention on cybercrime"
- Federal Law No FZ -152 "On Personal Data Protection"
- Federal Law No 97-FZ of 05.05.2014 "On amending the Federal Law "On Information, Information Technologies and Protection of Information" and some legislative acts of the Russian Federation on streamlining the exchange of information with the use of information and telecommunication networks", as well as a number of subordinate acts are available at: (http://97-fz.rkn.gov.ru)
- GOST R 56205-2014 "Industrial communication networks. Network and system security (cybersecurity)"
- Resolution of the Russian Government of 26.06.1995 No 608 "On certification of means for protection of information". New system is at the stage of concept, Presidential Decree No 31s "On establishment of the State System for detection, prevention and elimination of consequences of cyberattacks on information resources of the Russian Federation"
- Concept of the State System for detection, prevention and elimination of consequences of cyberattacks on information resources of the Russian Federation (adopted by the Russian President 12.12.2014 No K 1274)
- Federal Law No 38-FZ, Article 18 "On Advertising".

1.2 TECHNICAL MEASURES

1.2.1 CIRT
Russia has the Centre for Cyber Incident Response in Information Systems of Governmental Authorities. International name is GOV-CERT.RU. That Centre is coordinating the actions of involved companies and
governmental agencies in the field of detecting, preventing and suppression of illegal activity related to network resources of government bodies.

For that kind of illegal activity, which not touches network resources of government bodies, there are RU-CERT – the Russian Cyber Incidents Response Centre and CERT-GIB – 24-hour Cyber Incidents Response Centre. Main objective of those Centers is to reduce the level of threats to information security for users of the Russian segment of Internet. For this purpose RU-CERT is assisting to Russian and foreign legal entities and individuals in detecting, preventing and suppression of illegal activity and also performs collection, storage and processing of statistic data related to network resources located on the territory of the Russian Federation.

RU-CERT is the part of the international CSIRT/CERT associations: FIRST and Trusted Introducer, and acts as the Russian official contact point within these associations.

Beside of that, Russia has special Cyber Incidents Monitoring and Response Centre in the field of credit and financial (FinCERT). FinCERT is a part of head security and data protection department of the Bank of Russia.

FinCERT performs collection of data on cybersecurity from financial companies, analysis of that data, ensuring feedback with credit and financial companies on possible threats to information security, and development of recommendation on reflecting cyberattacks. FinCERT cooperates with operational bodies of Russian Federal Security Service (FSB). Also, one of the major objective of FinCERT is reducing the illegal writing off of amounts from credit cards.

1.2.2 STANDARDS
Russia has officially approved national (and sector specific) cybersecurity frameworks for implementing internationally recognized cybersecurity standards, specifically Federal Agency on Technical Regulating and Metrology (Rosstandart)

1.2.3 CERTIFICATION
Russia has officially approved national (and sector specific) cybersecurity frameworks for the certification and accreditation of national and public professional agencies. Resolution of the Government of the Russian Federation No.608, June 26, 1995 "On certification of information protection tools". The new system is at the concept stage, and there is Presidential Decree No. 31s "On establishment of the State System for detection, prevention and elimination of consequences of cyberattacks on information resources of the Russian Federation".

1.3 ORGANIZATION MEASURES

1.3.1 POLICY

Also, there were developed Basic Principles for State Policy of the Russian Federation in the field of International Information Security (2013), Basic Principles for State Policy of the Russian Federation in the field of International Information Security (2020) and Draft Concept of the Russian Cyber Security Strategy.
1.3.2 ROADMAP FOR GOVERNANCE
Russia does not currently have any national governance roadmap for cybersecurity.

1.3.3 RESPONSIBLE AGENCY
Russian Federal Security Service (FSB), Federal Guard Service (FSO), Federal Service for Technical and Export Control (FSTEC), Ministry of Internal Affairs (MVD), Ministry of Defense (MoD) and the Foreign Intelligence Service (SVR) are the officially recognized institutions responsible for implementation of national cybersecurity strategy, policy and roadmap in Russia. In addition, part of the functions is delegated to the Federal Service for Supervision of Communications, Information Technology, and Mass Media (Roscomnadzor) and to the Ministry of Telecom and Mass Communications of the Russian Federation (Minsvyaz).

1.3.4 NATIONAL BENCHMARKING
Each government entity in Russia performs an annual audit of its own networks and systems depending on the requirements of the information.

1.4 CAPACITY BUILDING

1.4.1 STANDARDISATION DEVELOPMENT
Russia has officially recognized national or sector-specific research and development (R&D) programs/projects for cybersecurity standards, best practices and guidelines to be applied in either the private or the public sector through the ITU-T Study Group 17.

1.4.2 MANPOWER DEVELOPMENT
There are several higher education institutions specializing in this field in Russia.

The Russian Law Academy of the Ministry of Justice of the Russian Federation provides higher education at information law, informatics and mathematics department. In addition, the Academy offers professional training courses for employees of the corresponding industry.

Core training is carried out at the Moscow University of the Ministry of Internal Affairs of the Russian Federation, Information Security Department.

1.4.3 PROFESSIONAL CERTIFICATION
The mentioned above (1.4.2) higher education institutions institutions provide professional certification in this field.

1.4.4 AGENCY CERTIFICATION
The mentioned above (1.4.2) higher education institutions serve as certification agencies in this field.

1.5 COOPERATION

1.5.1 INTRA-STATE COOPERATION
To facilitate sharing of cybersecurity assets across borders or with other nation states, the Russian company in incident response business CIRT (CERT-GIB) has officially recognized partnerships with the League of Safer Internet and the National Coordination Centre.
1.5.2 INTRA-AGENCY COOPERATION
In the public sector Russian Federal Security Service (FSB) is officially cooperating with the following organizations on the matters of cybersecurity:

- Federal Service for Technical and Export Control (FSTEC)
- Ministry of Defence (MoD)
- Ministry of Internal Affairs (MVD)
- Federal Service for Supervision of Communications, Information Technology, and Mass Media (Roskomnadzor)
- Ministry of Telecom and Mass Communications of the Russian Federation (Minsvyaz)

1.5.3 PUBLIC SECTOR PARTNERSHIP
Russia has all officially recognized national or sector-specific programs for sharing cybersecurity data within the public sector (the Agreement between the Governments of Member States of the Shanghai Cooperation Organization on Cooperation in the Field of International Information Security, Yekaterinburg, 16 June 2009).

1.5.4 INTERNATIONAL COOPERATION
The Russian Federation is officially participating in regional and/or international platforms and forums on cybersecurity. For instance: http://www.cert.ru/ru/about.shtml

2. CHILD ONLINE PROTECTION

2.1 NATIONAL LEGISLATION
Specific legislation on child online protection has been enacted through the following instruments:

Federal Law of the Russian Federation No. 436-FZ on Protection of Children from Information Harmful to Their Health and Development

Presidential Decree No. 761 of 1 June 2012, on the National Strategy of Action for Children for 2012-2017

2.2 UN CONVENTION AND PROTOCOL
Russia has acceded, with no declarations or reservations to articles 16, 17(e) and 34(c), to the Convention on the Rights of the Child.

Russia has signed but not ratified (as of 14th December 2014), the Optional Protocol to The Convention on the Rights of the Child on the Sale of Children, Child Prostitution and Child Pornography.

2.3 INSTITUTIONAL SUPPORT
Russia does not have any officially recognized agency that provides institutional support on child online protect.

There is Smart Internet Foundation in Russia.

2.4 REPORTING MECHANISM
Cyber Security and Incident Response Team for the governmental networks of the Russian Federation (GOV-CERT.RU ( *)) provides space in its website to report a computer incident.

Safer Internet Centre for Russia ( *) provides space ( *) in its website to report online illegal content.

The Friendly RUNET Foundation ( *) provides space ( *) in its website to report online illegal content.
DISCLAIMER: Please refer to http://www.itu.int/en/Pages/copyright.aspx
More information is available on ITU website at http://www.itu.int/en/ITU-D/Cybersecurity/Pages/default.aspx
Last updated on 22th January 2015