

MINISTRY OF INFORMATION TECHNOLOGY AND COMMUNICATIONS
OF THE REPUBLIC OF MOLDOVA



**Ensuring Cyber Security
of the Republic of Moldova**

The dimensions of cyber security

(Norton Report)

378 mln.
victims per year

1 mln. +
victims per day

594 mln.
victims per year

1.630 mln.
victims per day

12
victims per second

2015



19
victims per second

2016

The global cost of cybercrime

(Norton Report 2016)

348 mln

identities were exposed

36%

have shared the password to their banking account

51%

banking information in the cloud is riskier than not wearing a seatbelt

51%

online bullying as more likely than being bullied at school or work

Statistics of Special Telecommunication Center on incidents and cyber attacks in Moldova



3.125.495

SPAM emails were blocked

35.770

Virused emails were blocked

1.878.181

DdoS attempts of attacks

8.239

Possible infections of computers
with malicious programs

199.109

Attempts to use improperly
different web applications

Information Society in the Republic of Moldova

ANRCETI

121,6%

Mobile penetration

ANRCETI

99%

3G coverage

ANRCETI

46%

4G coverage

OOKLA

11/16

Rating RM
V m, Internet

ANRCETI

75%

Internet penetration

GDP
111.5 bln. lei
about **8.0%**
ICT



Strategic and legislative framework

Policy Documents:

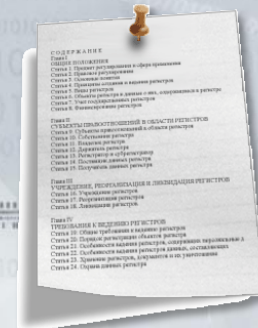
- ✓ *National Strategy for Information Society development "Digital Moldova 2020"*
- ✓ *National Security Strategy of the Republic of Moldova, etc.*

The legal framework:

- ✓ *Law on Informatization and State Information Resources*
- ✓ *Law on Electronic Communications*
- ✓ *Law on Personal Data Protection*
- ✓ *Law on preventing and combating cybercrime , etc.*

International Agreements:

- ✓ *Association Agreement between the Republic of Moldova and the European Union*
- ✓ *Recommendations of the International Telecommunication Union*
- ✓ *Council of Europe Conventions, etc.*

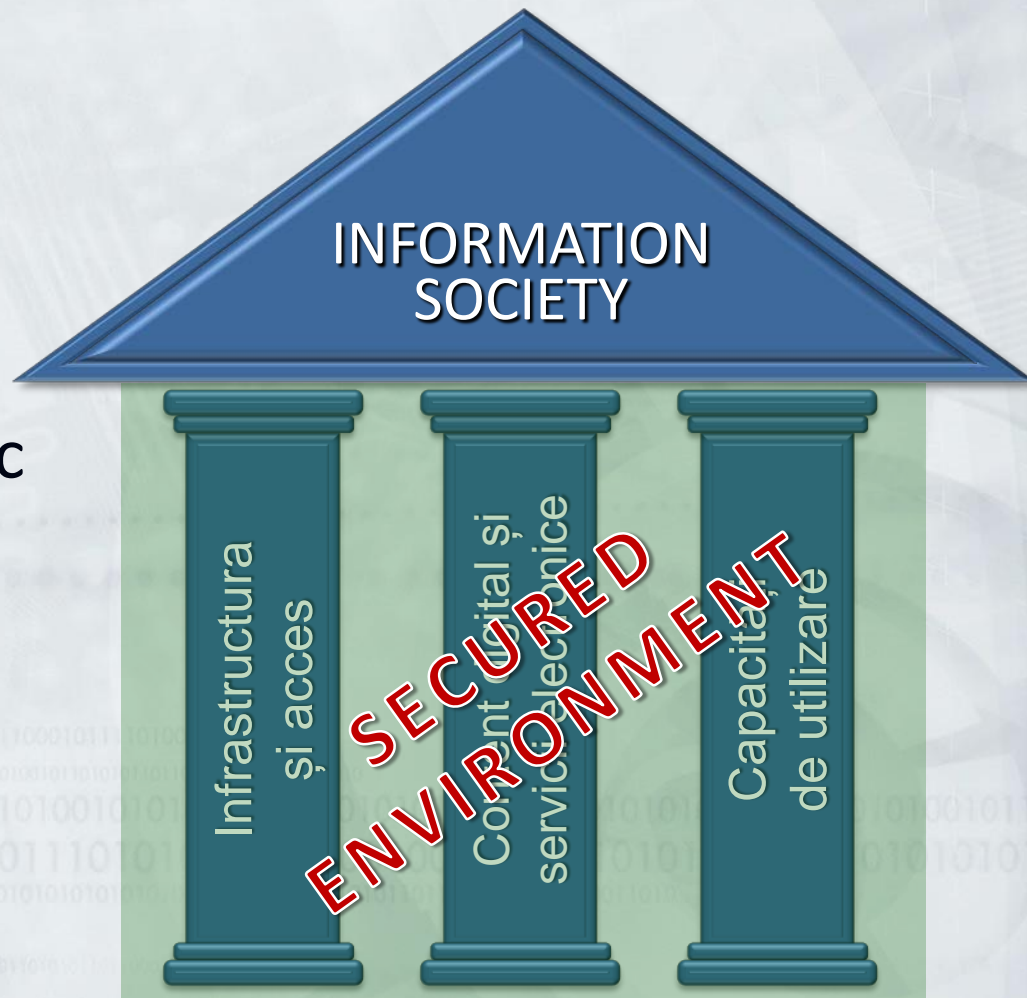




Moldova
Digitală

OVERALL OBJECTIVE:

Favorable conditions
for balanced and dynamic
Information Society
for 2014-2020



How do we ensure security in the virtual environment?

THE PROGRAM ON CYBER SECURITY



Areas of intervention

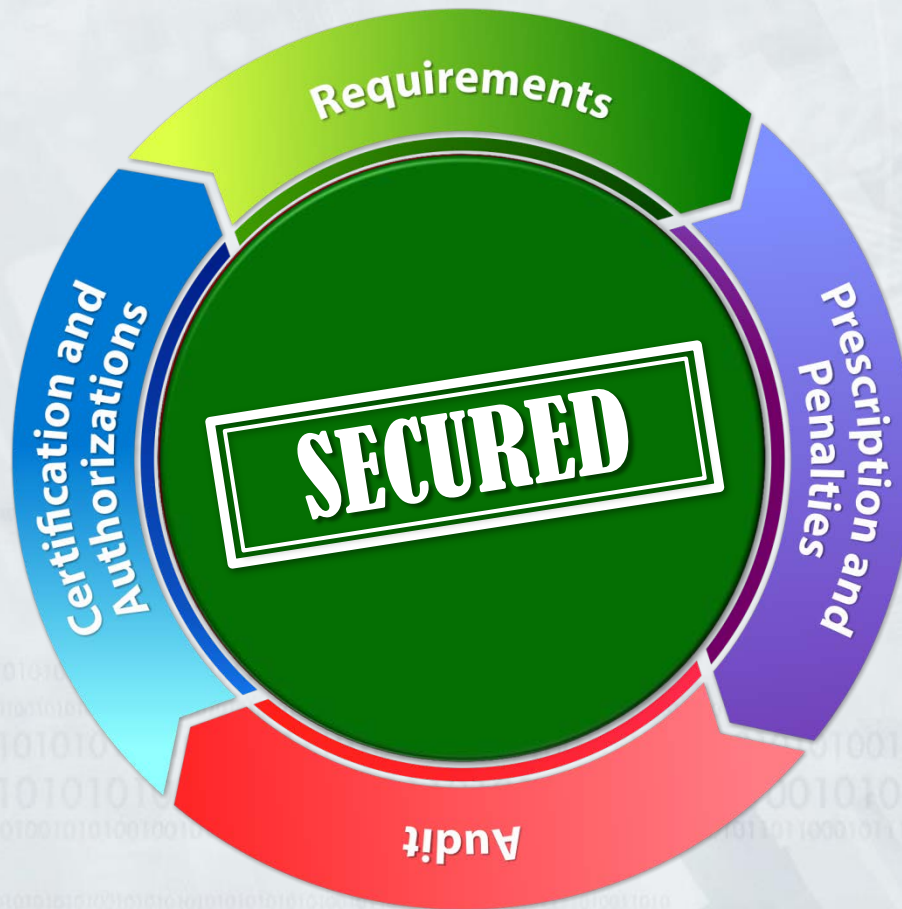
- 1 Safe processing, storing and accessing data
- 2 Security and integrity of electronic communications networks and services
- 3 Capabilities of prevention and emergency response (CERT)
- 4 Preventing and combating cybercrime
- 5 Strengthening cyber defense capabilities
- 6 Education and information
- 7 International cooperation and interaction

Next step – Program on ensuring cyber security

- Requirements
- Certification and Authorization
- Audit
- Prescriptions and sanctions



Ensuring cybersecurity



Principles of ensuring cyber security

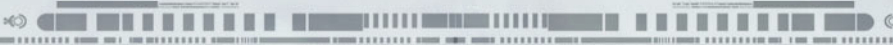
- ✓ Protection of fundamental rights
- ✓ Access for everyone
- ✓ Cyber resilience
- ✓ Multi-participatory management
- ✓ Sharing responsibilities



Requirements for cyber security

- Classification of the cyber security systems
- Organization of cyber security informational systems, resources, equipments and programs
- Regulatory procedures of cybersecurity for systems and penetration tests
- The cyber security policy, Plan of recovery, Guide of using emails, etc.

Next steps

- 
1. Adjusting legislative and regulatory framework
 2. Analysis and development of proposals for implementing the standards at national level
 3. Develop mandatory minimum requirements on cyber security
 4. Experts certification based on the standards
 5. Business cooperation and involvement

Ensuring cyber security of the Republic of Molgova

Thank you!



www.mtic.gov.md