Information security strategy of the Republic of Moldova for 2019-2024 and the Plan of actions for its implementation

Lisnic Sergiu,
Center for Combating Cyber Crimes of NII of GIP,
Republic of Moldova

Approval of the strategy:

- *22.11.2018 - The parliament approved the Information security strategy of the Republic of Moldova for 2019-2024 and the Plan of actions for its implementation*

- *18.02.2019 - Date of entry into force*

- *The strategy has 7 chapters and 117 points. It targets the fields that highlight the security of the information. The document contains the problems that Moldova has to face - cyber attacks.*

Vision and objectives of the strategy:

1. Ensuring the security of the cyber information space and investigating cybercrime
2. Ensuring the security of the media information space
3. Strengthening operational capabilities
4. Process efficiency of internal coordination and international cooperation in the field of information security

Pillar I: Ensuring the security of the cyber information space and investigating cybercrime

Pillar I priorities	Result indicators
1. **Creation of the National Cyber Security Incident Response Center (National CERT)**	1. The national center created, which elaborates policy documents and ensures the interaction between all the components of cyber security
2. **Designation of the entity that will act as Governmental Center for Government Cyber Security Incident Response (CERT Gov)**	2. The Government Center ensures the operation and protection of special networks at the level of Government and public authorities
3. **Strengthen cooperation between national CERT, CERT Gov and private CERTs**	3. Collaboration and sustainability agreements for the prevention and resolution of cyber security incidents

Pillar II: Ensuring the security of the media information space

Pillar II priorities	Result indicators
1. **Development of civic control tools to ensure information security**	1. Mechanism for interaction and involvement of experts in order to ensure the security of the information space
2. **Elaboration of the legal framework for determining the legal status of periodicals, press agencies and other entities operating in the Internet media space**	2. Law on modifying the existing legal framework
3. **Creation of the strategic information resource / platform for strategic communication**	3. Strategic communication information platform created

Pillar III: Strengthening operational capabilities

Pillar III priorities	Result indicators
1. **Creation, at national level, of the Coordinating Council for ensuring information security, in which it will be possible to identify strategic communication procedures**	1. The normative framework regarding the creation of the Coordinating Council for ensuring the information security, elaborated and approved
2. **Creation within the Armed Forces of the entity responsible for cyber defense at national level**	2. The normative framework regarding the creation within the Armed Forces of the entity responsible for cyber defense at national level, elaborated and approved
3. **Creating a specialized platform on hybrid threats to security**	3. Created and functional platform
4. **Develop and promote the legal framework for regulating the national critical infrastructure**	4. The legal framework for the regulation of the national critical infrastructure elaborated and approved

Pillar IV: Process efficiency of internal coordination and international cooperation in the field of information security

Pillar IV priorities	Result indicators
1. **Development and implementation of training programs addressed to employees with criminal investigation and prosecution responsibilities in the cyber space**	1. Specialists trained on the basis of EU practices
2. **Development of national and international cooperation in the field of cyber defense**	2. Negotiated and concluded legal framework for cooperation
3. **Establishing the mechanisms of international cooperation between the state authorities with responsibilities in combating cybercrime and international bodies in the segment of ensuring information security**	3. Consultation rounds; bilateral / multilateral agreements signed and concluded

Summary:

- *According to the action plan, each objective has institutions responsible for achieving them, deadline for implementation, as well as proposed actions.*

- *Starting with 2020, the ministries, institutions and other central administrative authorities will present annually, until March 1, to the Information and Security Service the information regarding the implementation of the Action Plan, according to the established competences.*

- *Annually, until March 31, the Information and Security Service will present to the Parliament a report on the implementation of the Strategy and the implementation of the Action Plan and will publish it on its official web page.*

Thank you!

Questions?