CyberEast: Action on Cybercrime for Cyber Resilience
in the Eastern Partnership region

CyberEast Launching Conference
(19-20 September 2019, Brussels, Belgium)

Presentation of the Information Security Concept of the Republic of Belarus 18.03.2019

Vladimir Maroz
**Deputy Director of the Institute
for re-training and qualification upgrading of judges,
prosecutors and legal professionals at the
Belarusian State University**

Why there was a need for the adoption of the Concept?

The formation of the information society is one of the national priorities of the Republic of Belarus

1. Influence of the information sphere on social processes:

economic,

political,

social.

2. The impact of information technology on the realization of human rights.
3. The information sphere is one of the most dynamically developing and promising areas of the world economy. It is represented in all four “baskets” of the world market: the market of goods, services, capital, intellectual property.

Threats to:

– Human Rights;

– public order and morality;

– national security.

The Philosophy of the Concept

1. Information technology (the "information society") is not able to replace society itself. They are secondary to society and its members. The focus on the application and regulation of information technologies must be given the understanding that they are just a means of social development, but not its purpose, understanding how their capabilities (i.e. the capabilities of this particular method of transmitting information and communication) can be used to improve public welfare or to infringe on human rights and freedoms, public order and morality or national security.
2. Information security is a status of protection of the interests of a person, society and the state not only from cybercrime, but also from other threats that arise in connection with the use of information technology.
3. The task of law as a regulator of information relations is to prevent harm to a person, society and the state.

Legal basis of the Concept

1. Constitution of the Republic of Belarus,
2. Legislation in the sphere of national security (National Security Concept, app. by the Decree of the President of the Republic of Belarus 09.11.2010 № 575),
3. Legislation in the sphere of informatization, digital economy development, information society, science and technologies (The Law of the Republic of Belarus dd. 10.11.2008 № 455-3 «On information, informatization and information protection»; Decree of the President of the Republic of Belarus dd. 21.12.2017 № 8 «On digital economy development», State Programme for digital economy and information society development for 2016-2020 years», app. bylaw of the Council of Ministers of the Republic of Belarus dd. 23.03.2016 № 235),
4. Legislation in the sphere of intellectual property rights and others.

Information Security

– status of protection of balanced interests of
man,
society and
state
against internal and
external threats
in the
Information field.

In order to ensure information security, it is necessary to determine

1) Information field?
2) Interests of man, society and state in the information field?
3) Internal and External threats for these interests in the information field?
4) Status of protection of balanced interests of man, society and state in the information sphere (subjects, methods etc.)?

Information sphere: elements

Information Space – the area of activity related to the creation, transformation, transmission, use, storage of information that affects, inter alia, the individual and public consciousness and the information itself.

Information Space Security!

Information Infrastructure – a set of technical means, systems and technologies for the creation, transformation, transmission, use and storage of information

Information Infrastructure Security!

Information Security Objects – interests of man, society and state

1) Constitutional Human Rights and Freedoms;
2) material and spiritual values of society, system of public relations protected by law;
3) independence, territorial integrity, sovereignty, constitutional system of the State.

Basic national interests of the Republic of Belarus in the information sphere

– realization of the constitutional rights of citizens to receive, store and disseminate complete, reliable and timely information;

– formation and progressive development of the information society;

– equal participation of the Republic of Belarus in world information relations;

– transformation of the information industry into an export-oriented sector of the economy;

– effective public policy information support;

– ensuring the reliability and stability of the operation of vital objects of informatization (VOI)

(p. 14 National Security Concept).

Internal sources of threats in the information sphere

– dissemination of false or intentionally distorted information that could harm national interests of the Republic of Belarus;

– the dependence of the Republic of Belarus on the import of information technologies, means of informatization and information protection, their uncontrolled use in systems whose failure or destruction can cause damage to national security;

– mismatch of the quality of national content to the world level;

– insufficient development of the state system for regulating the implementation and use of information technology;

– increased crime using information and communications technology;

– insufficient effectiveness of public policy information support;

– imperfection of the security system for vital objects of informatization (VOI)

(p. 34 National Security Concept).

External sources of threats in the information sphere

– openness and vulnerability of the information space of the Republic of Belarus from external influences

– dominance of leading foreign countries in the global information space, monopolization of key segments of information markets by foreign information structures;

– information activities of foreign states, international and other organizations, individuals, detrimental to national interests of the republic of Belarus, purposeful formation of informational reasons for its discredit;

– the growth of information confrontation between leading world centers of power, the preparation and conduct by foreign countries of the struggle in the information space;

– development of information manipulation technologies

– hindering the dissemination of national content of the Republic of Belarus abroad;

– wide dissemination in the world information space of mass culture samples that contradict universal human and national spiritual and moral values

– attempts of unauthorized access from outside to information resources of the Republic of Belarus, causing damage to its national interests

(p. 42 National Security Concept)

Information Security System

– set of interacting

actors and

means, used by them to carry out activities to protect and realize national interests of the Republic of Belarus and ensuring the safety of man, society and the state.

Actors:

– State by legislative, executive and judicial authorities;

– public (civil society) and

private (business) organizations;

– citizens

(p. 57 National Security Concept).

The main directions of ensuring the security of information infrastructure

Security:

– national segment of the Internet,

– vital objects of informatization and information systems,

– an effective response to cybercrime

(p. 64 Information Security Concept)

Internet Security

Directions:

– creation of a unified state monitoring system for the national segment of the Internet with the simultaneous formation of a cloud platform for the provision of integrated information security services to the public sector and the business community in the interests of automated accounting of cyber incidents and the rapid exchange of information about them between authorized state bodies, telecommunication operators and **Computer Security Incident Response Team** (**CSIRT**);

– creation and operation of a national certification authority, the root certificate of which will be trusted for major operating systems and web browsers;

– organization of the functioning of the IP reputation assessment service to provide real-time information to Internet service providers about the addresses used for cyber attacks;

– ensuring a balance between reliable identification of users, recording their actions and creating conditions for the safe collection, processing, provision, storage and dissemination of personal data in the national segment of the Internet;

– formation and development of national cyber risk insurance markets and penetration testing services

(ch. 17 Information Security Concept).

Security of VOI

Directions:

– determination of the most significant objects of informatization, the failure of functioning or disruption of which can lead to significant negative consequences for national security in the political, economic, social, information, environmental and other fields (VOI)

(Decree of the President of the Republic of Belarus dd. 25.10.2011 № 486);

– creation of individual safety models for each VOI taking into account systematic general safety requirements;

– integration into the state monitoring system of the national segment of the Internet of industry-specific systems for monitoring and controlling cyber threats;

– use of regularly updated, genuine licensed software obtained from trusted sources

(ch. 18 Information Security Concept).

Security of state information systems

– determination of the procedure for the creation and operation of state information systems (SIS);

– achieving the necessary level of protection of e-government services and cyber stability of state information systems at the stages of their safe design and operation, as well as through the introduction of their reasonable unification in the construction and modernization of these systems;

– use of regularly updated, genuine licensed software obtained from trusted sources;

– protection of limited information, ensuring the security of personal data and state information resources;

– the exception of the storage and processing of information classified as state or official secret in publicly accessible forms, including in information systems that have access to the Internet and other open computer networks

(ch. 18 Information Security Concept).

Security of non-governmental information systems

– collection, processing, provision and dissemination of personal data based on the principle of "default security";

– in the conditions of physical impossibility and inappropriateness to completely separate from the Internet and other publicly accessible networks information systems and resources containing information constituting commercial, professional, banking and other secrets protected by law, information on the private life of an individual, personal data, adoption of necessary legal, organizational and administrative and technical measures to minimize the number of cyber incidents and harm from them in these systems;

– improvement of information protection requirements, including further development of a system for confirming the conformity of technical and cryptographic information protection means, as well as licensing of activities in the field of technical information protection;

– improving the requirements for the subjects of information relations engaged in the collection, processing and storage of these data

(ch. 23 Information security Concept).

Counter Cybercrime

– effective functioning of the system for the prevention, detection, suppression and investigation of cybercrime;

– ensuring compliance with the norms of the Criminal Code of the Republic of Belarus with the level of social development, global trends in legal regulation and international best practices (ch. 31 CC “Crimes Against Information Security” and others)

– harmonization and unification of approaches to countering cybercrimes with the best foreign practices, development of common standards for law enforcement practice;

– intensification of regional and international cooperation in the field of cybersecurity;

– increasing trust between law enforcement agencies, public and private sector organizations, educational and scientific institutions, combining their efforts in the prevention, detection, suppression and investigation of cybercrimes;

– reduction of motivation for committing cybercrime by eliminating the conditions for the formation of illegal schemes as a measure of prevention and prevention of cybercrime;

– prevention of cybercrime through popularization among the population, especially youth, of intolerance to antisocial behavior in the information space, conducting outreach to the media and the Internet in order to create a safe national information ecosystem;

– to increase legal awareness and reduce vulnerability to cyberattacks, teaching the basics of information behavior

(ch. 19 Information Security Concept)

Objectives are defined. To work…

The Concept defines strategic objectives and priorities in the field of information security.

The Concept serves as the basis for the formation of state policy, the development of measures to improve the information security system, constructive interaction, consolidate efforts and increase the effectiveness of protecting national interests in the information sphere.

Thank you!

e-mail: morozv@bsu.by