On approval of the National anti-crisis plan for responding to information security incidents

Unofficial translation

Resolution of the Government of the Republic of Kazakhstan dated August 9, 2018 No. 488.

Unofficial translation

In accordance with subparagraph 6-1) of article 6 of the Law of the Republic of Kazakhstan "On informatization" dated November 24, 2015 the Government of the Republic of Kazakhstan RESOLVES:

1. To approve the attached the National anti-crisis plan for responding to information security incidents.

2. This resolution shall come into effect ten calendar days after the day of its first official publication.

Prime Minister of the Republic of Kazakhstan *B. Sagintayev*

Approved
by Resolution No. 488 of
the Government of the
Republic of Kazakhstan
dated August 9, 2018

National anti-crisis plan for responding to information security incidents Chapter 1. General provisions

1. National anti-crisis plan for responding to information security incidents (hereinafter referred to as the plan) determines the order of actions of the entities of the system to reduce the impact of information security incidents on the state of information security while minimizing violations of their work.

2. This plan does not apply to protected information systems, classified as state secrets in accordance with the legislation of the Republic of Kazakhstan on state secrets, as well as to telecommunications of special purpose and / or governmental, presidential, secret, encrypted and coded communications.

3. In this plan the following concepts shall be used:

1) facilities of information and communication infrastructure (hereinafter referred to as the ICI facilities) – information systems, technological platforms, hardware and software systems, telecommunications networks, as well as support systems for the smooth operation of hardware and information security;

2) critical objects of information and communication infrastructure (hereinafter referred to as COICI) - objects of ICI, violation or termination of the functioning of which leads to illegal collection and processing of personal data of limited access and other information

containing secret protected by law, social and (or) technogenic nature or significant negative consequences for defense, security, international relations, economy, individual spheres of economy or life of the population living in the relevant territory, including infrastructure: heat supply, power supply, gas supply, water supply, industry, healthcare, communications, banking, transport, hydraulic structures, law enforcement, "electronic government";

3) information security incident response system (hereinafter referred to as the system) – a set of forces and means of ensuring information security, designed to implement a nationwide set of measures to protect electronic information resources, information systems, and information and communication infrastructure from technological failures or unauthorized exposure as a result of computer attacks, and liquidation of their consequences;

4) information security incident (hereinafter referred to as the IS incident) – separately or serially disruptions in the operation of the information and communication infrastructure or its separate objects, posing a threat to their proper functioning and (or) conditions for the unlawful acquisition, copying, distribution, modification, destruction or blocking of electronic information resources;

5) crisis situation in the field of information security – IS incident or real precondition for its occurrence at ICI facilities, which can lead to the impossibility or restriction of the provision of public services, an emergency situation of a social and (or) technogenic nature, or significant negative consequences for defense, security, international relations, the economy, certain sectors of the economy, the infrastructure of the Republic of Kazakhstan, or for the livelihoods of the population living in the relevant territory;

6) national coordination center of information security (hereinafter referred to as NCCIS) - structural subdivision of the joint-stock company "State technical service";

7) system entities – government agencies authorized to resolve information security or response to IS incident, NCCIS, Operational headquarters, owners of "e-government" information facilities, the CIOICI owners, information security operational centers (hereinafter referred to as the ISOC), Information security incident response services;

8) computer attack – a deliberate attempt to implement the threat of tampering information, electronic resources, information systems, or to access them using a software or firmware (or interworking protocol).

Other concepts used in the plan correspond to the concepts used in the legislation of the Republic of Kazakhstan in the field of informatization and communication.

Footnote. Paragraph 3 as amended with the resolution of the Government of the RK dated 01.10.2020 № 630; dated 26.10.2022 No. 849 (shall enter into force upon expiry of ten calendar days after the day of its first official publication).

Chapter 2. Preventive actions

4. In order to prevent incidents in the field of informatization and communication, the NCCIS conducts explanatory work on IS incidents on a planned basis. In this regard, it

collects, analyzes and compiles information from system entities and other sources, including foreign and international organizations in the field of information security.

5. ISOC in order to identify and suppress IS threats monitors the connected information and communication infrastructure and information facilities.

6. ISOC interoperability in monitoring the provision of information security for information objects provided by NCCIS.

7. The system entities to improve the level of protection of electronic information resources, software, information systems and the information and communication infrastructure supporting them are guided by the Uniform requirements in the field of information and communication technologies and information security, as well as other regulatory legal acts governing the field of information security.

Chapter 3. Actions of owners of critical information and communication infrastructure facilities and “e- government” information facilities

8. In order to ensure response to IS incidents with levels of criticality from 0 to 5, owners of “e-government" information facilities, CIOICI, ISOC owners develop and approve response plans, which include measures to deal with threats (risks) of information security, ensure continuous operation and recovery the health of assets associated with information processing facilities, and the following mandatory measures for:

1) organizing and conducting measures to prevent the emergence of a crisis situation of information security;

2) collection and analysis of data on the state of information security in the information and communication infrastructure;

3) interacting with ISOC and NCCIS;

4) supporting measures to ensure continuity of work and resilience to external changes;

5) informing the system stakeholders on the issues of information security incidents detected and their elimination;

6) the procedure for eliminating information security incidents and their consequences, minimizing the impact on the information and communication infrastructure of the system entity;

7) measures for saving the digital traces of information security incidents (magazines, reports and forms);

8) determining the causes of information security incidents;

9) the actions to be taken after the information security incident;

10) eliminate the cause of an IS incident;

11) recovery procedures.

Other activities may be included based on the characteristics of the information and communication infrastructure and (or) technological processes of the subjects of the system.

9. Owners of e-government informatization facilities and CIOICI send a copy of the approved information security incident response plans to the authorized information security authority.

10. On IS issues, the owners of CIOICI and e-government informatization facilities interact with NCCIS through the around-the-clock 1400 call center or the official www.kz-cert.kz website.

11. According to the decision of the owners of "electronic government" informatization facilities and CIOICI, the information security incident response services and (or) ISOC may be involved in response to information security incidents.

12. The “electronic government” informatization facilities and CIOICI, owners after the completion of the response, start implementing the measures provided for by the plan to restore the system, including using the recommendations of the authorized agency for information security and the NCCIS.

13. For the purpose of effective interaction, the “electronic government” informatization facilities and CIOICI owners determine responsible officials for ensuring information security .

Contact details of officials are sent to NCCIS. The NCCIS is informed about all cases of replacement of the responsible official or their contacts within 48 hours.

Chapter 4. Information security incident response

Paragraph 4.1. Actions of authorized agencies to respond to information security incidents

14. NCCIS in cases of receiving information on information security incidents at information facilities, in accordance with 3, 4 and 5 levels of information security incidents, established by the Rules for monitoring of information security of e-government informatization facilities and critical ICI facilities and the Information Exchange Rules required for information security, between operational information security centers and the National Information Security Coordination Center, informs the national security agencies of the Republic of Kazakhstan.

15. In urgent cases and that can result in the commission of serious and extremely serious crimes, as well as crimes being prepared and committed by a criminal group, the Chairman of the National Security Committee of the Republic of Kazakhstan, his deputies or the heads of territorial bodies of the National Security Committee of the Republic of Kazakhstan or their substitutes , has the right to suspend the operation of networks and (or) means of communication, the provision of communication services, access to Internet resources and (or) information posted on them in the interests of all subjects of operational investigative activities with subsequent notification to the authorized body in the field of communications and the General Prosecutor's Office of the Republic of Kazakhstan within 24 hours.

16. In emergency situations of social, natural and technogenic nature, the introduction of state of emergency or martial law, the authorized body for ensuring information security coordinates the management of Internet resources and ICI facilities.

17. Measures to respond to IS cross-border incidents are coordinated with the authorized body on foreign policy activities and implemented in accordance with international treaties ratified by the Republic of Kazakhstan..

Paragraph 4.2. Actions of the Operational headquarters

18. In order to coordinate information crisis response activities in the field of information security, an operational headquarters for information security crisis response is created on the basis of NCCIS (hereinafter referred to as the Operational Headquarters).

19. Prior to the convening of the Operational Headquarters, NCCIS, together with the forces and means of the owners of critical ICI facilities and e-government informatization facilities, conducts primary response to a crisis situation in order to prevent the spread and minimize its consequences.

20. The head of the Operational Headquarters is the Deputy Chairman of the National Security Committee supervising the area of information security or his acting official. The deputy head of the Operational Headquarters is the head of the department, the authorized body in the field of information security, ensuring the implementation of state policy in the field of information security or his acting official.

21. By decision of the head of the Operational Headquarters, it may include representatives of state bodies and other organizations.

22. Based on the initial analysis of the information security crisis, the head of the NCCIS proposes to the head of the Operational Headquarters the decision to convene the Operational Headquarters to organize and implement a set of measures to prevent it and localize the consequences of an information security incident..

23. The main tasks of the Operational Headquarters in a crisis situation are:

determination of the procedure for the actions of authorized divisions of state bodies and organizations in responding to the information security crisis situation;

making adjustments to the actions of the forces and means of authorized divisions of state bodies and organizations for localizing and eliminating information security crisis situations;

coordination of organizational and technical response to crises in the field of information security;

development and organization of measures to restore the functioning of the information and communication infrastructure, which work was disrupted during a crisis situation of information security;

organizing of official and technical investigations and proceedings to establish the causes and conditions for the emergence of a crisis situation of information security;

informing owners of information facilities about information security incidents via the mass media.