Lecture-14. Incident prevention and response

Purpose of the Lecture

The purpose of this lecture is to provide students with a comprehensive understanding of the principles, methods, and stages of preventing and responding to information security incidents. The lecture aims to form practical knowledge about how to identify potential threats, implement preventive measures, and organize effective response processes to minimize damage and restore normal operations of information systems.

National Coordinating Center for Information Security (NCCIB) - a structural subdivision of the republican state enterprise on the right of economic management "State Technical Service" of the National Security Committee of the Republic of Kazakhstan;

The subjects of the system are state bodies authorized to resolve information security issues or respond to information security incidents, the NCCIB, the Operational Headquarters, the owners of the "electronic government" informatization objects, the owners of the KVOIKI, the operational information security centers (OCIS), information security incident response services.

In order to prevent and prevent incidents in the field of informatization and communication, on a planned basis, it conducts explanatory work on information security incidents, for this purpose it collects, analyzes and summarizes information from system subjects and other sources, including foreign and international organizations in the field of information security.

In order to identify and suppress IS threats, the OCIS monitors the ICI connected to it and informatization objects. The interaction of the OCIB on the issues of monitoring the information security of informatization objects is provided by the NCCIB.

The subjects of the system to increase the level of security 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 regulating the field of information security.

In order to ensure response to information security incidents, the owners of the objects of informatization of "electronic government", the owners of KVOIKI, OCIB develop and approve response plans that provide for measures to handle information security threats (risks), ensure continuous operation and restore the operability of assets associated with processing tools information, and the following mandatory activities to:

1) organization and implementation of measures to prevent the emergence of an information security crisis;
2) collection and analysis of data on the state of information security in the information and communication infrastructure;
3) interaction with OCIB and NCCIB;
4) supporting measures to ensure business continuity and resilience to external changes;
5) informing the interested subjects of the system on the detected information security incidents 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 subject of the system;
7) measures to preserve digital traces of information security incidents (logs, reports and forms);

8) establishing the causes of information security incidents;

9) actions to be taken following an information security incident;

10) elimination of the cause of the information security incident;

11) recovery procedures.

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

The owners of the objects of informatization of "electronic government" and KVOIKI send a copy of the approved plans for responding to information security incidents to the authorized body for ensuring information security. On issues of information security incidents, the owners and owners of KVOIKI and objects of informatization of "electronic government" interact with NCCIB through the round-the-clock call-center 1400 or the official website www.kz-cert.kz.

According to the decision of the owners of the objects of informatization of "electronic government", KVOIKI, the response services to information security incidents and (or) OCIS can be involved in responding to information security incidents.

The owners of the objects of informatization of "electronic government", KVOIKI, after the completion of the response, begin to implement the measures provided for by the plan to restore the system, including using the recommendations of the authorized body for information security and the NCCIB. For the purpose of effective interaction, the owners of objects of informatization of "electronic government", KVOIKI determine responsible officials for ensuring information security. The contact details of the persons are sent to the NCCIB. NCCIB is informed about all cases of replacement of the responsible official or his contacts within 48 hours.

Information security incident response

Actions of authorized bodies to respond to information security incidents

NCCIB in cases of receiving information about information security incidents at informatization objects in accordance with information security incidents established by the Rules for monitoring the information security of "electronic government" informatization objects and critically important ICI objects and the Rules for the exchange of information necessary to ensure information security between operational centers ensuring information security and the National Coordinating Center for Information Security, informs the national security authorities of the Republic of Kazakhstan.

In cases of urgency and which could lead to the commission of grave and especially grave crimes, as well as crimes prepared and committed by a criminal group, the Chairman of the National Security Committee of the Republic of Kazakhstan, his deputies or heads of territorial bodies of the National Security Committee of the Republic of Kazakhstan or persons replacing them , 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, followed by notification of the authorized body in the field of communications and the General Prosecutor's Office of the Republic of Kazakhstan within 24 hours.

In emergency situations of a social, natural and man-made nature, the introduction of a state of emergency or martial law, the authorized body for ensuring information security coordinates the management of Internet resources and ICI objects.

Response measures to cross-border IS incidents are coordinated with the authorized body for foreign policy activities and are carried out in accordance with international treaties ratified by the Republic of Kazakhstan.

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

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

The Head of the Operational Headquarters is the Deputy Chairman of the National Security Committee, who is in charge of the field of information security or is acting in his capacity. The Deputy Head of the Operational Headquarters is the head of the department, the authorized body in the field of ensuring information security, which ensures the implementation of state policy in the field of ensuring information security or acting in his capacity. By decision of the head of the Operational Headquarters, representatives of state bodies and other organizations may be included in its composition.

Based on the initial analysis of the information security crisis, the head of the NCCIB proposes to the head of the Operational Headquarters a 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.

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

- determining the procedure for actions of authorized departments of state bodies and organizations to respond to an information security crisis;
- making adjustments to the actions of the forces and means of authorized divisions of state bodies and organizations to localize and eliminate the crisis situation of information security;
- coordination of organizational and technical response to crisis situations in the field of information security;
- development and organization of measures to restore the functioning of the information and communication infrastructure, the operation of which was disrupted during the information security crisis;
- organization of official and technical investigations and proceedings to establish the causes and conditions for the emergence of an information security crisis;
- notification of owners and owners of informatization objects about information security incidents through the media.

As for other methods of prevention, they come down to the use of technical measures to protect information and IP, mainly in the form of specialized software.

Consider some existing programs and solutions designed specifically for these purposes:

- ***Kaspersky Threat Management and Defense*** is a solution in the form of a single platform for rapid threat detection, incident investigation, response and infrastructure recovery using a set of interconnected security solutions and services:
- ***Kaspersky Anti Targeted Attack*** is a specialized platform for countering complex threats at all levels of the IT infrastructure, which includes a full-featured set of technologies for detecting previously unknown threats and targeted attacks and tools for comparing various indicators of compromise to detect attacks of increased complexity.
- ***Kaspersky Endpoint Detection and Response*** An advanced solution for detecting incidents in the workplace and actively responding to them through the organization of centralized management in the corporate network.
- ***Kaspersky Security for Business*** is a multi-level protection for workstations and servers that provides comprehensive protection for the corporate network and contains many

advanced technologies, such as behavior analysis, dynamic white lists, built-in file or entire disk encryption, finding and fixing vulnerabilities, and many others.

- ***Kaspersky Secure Mail Gateway*** is a solution that combines an email system and its protection tools into a ready-to-use virtual security appliance. The product provides email protection against known and unknown threats, including spam, phishing and all kinds of malicious attachments.
- ***Kaspersky Private Security Network*** is a local reputation database that meets stringent security requirements and has all the benefits of a cloud-based security network, but without transferring data outside the local network.
- ***Kaspersky Industrial Cybersecurity*** - a solution for industrial enterprises, protects industrial enterprises from cyber threats, ensures the security of industrial environments and the continuity of production processes, minimizes downtime and delays in technological processes
- ***Kaspersky Fraud Prevention***, a solution mainly for financial institutions, not only eliminates the consequences of a fraudulent incident, but gives organizations the opportunity to take preventive measures to prevent attackers from achieving their goal. The platform actively blocks attempts by cybercriminals to steal user data, eliminating the threat of fraud before it gets real. The solution console also allows the bank's anti-fraud officers to gather accurate information about each incident, including the credentials used to access the account.
- ***Kaspersky Embedded Systems Security*** is a security solution for ATMs, POS systems and self-service kiosks. Built with current threats, device functionality, operating system features, connectivity, and embedded systems architecture in mind.

Control Questions

1. What is the purpose of incident prevention and response?
2. What are the main preventive measures in information security?
3. What are the key stages of the incident response process?
4. How does containment differ from eradication and recovery?
5. What is the role of the Incident Response Team (IRT/CSIRT)?
6. What principles ensure an effective incident response?
7. Which legal and regulatory frameworks govern incident management?

Recommended Literature

1. ISO/IEC 27035:2016. *Information Security Incident Management.*
2. NIST SP 800-61 Rev. 2. *Computer Security Incident Handling Guide.*
3. Tipton, H. F., & Krause, M. (2019). *Information Security Management Handbook.* CRC Press.
4. Peltier, T. R. (2016). *Information Security Policies, Procedures, and Standards.* Auerbach Publications.

5. Law of the Republic of Kazakhstan “On Informatization” (2015).

6. Solove, D. J. (2021). *Understanding Privacy and Cyber Law.* Aspen Publishing.