Lecture-13. The concept and types of incidents

Purpose of the Lecture

The purpose of this lecture is to introduce students to the concept, classification, and characteristics of information security incidents. The lecture aims to develop an understanding of what constitutes an incident, how it differs from other security events, what types of incidents can occur, and how organizations should respond to them to ensure the protection and stability of information systems.

Information security incident - individually or serially occurring failures in the operation of the information and communication infrastructure or its individual objects, creating a threat to their proper functioning and (or) conditions for the illegal receipt, copying, distribution, modification, destruction or blocking of EIR.

A computer attack is a targeted attempt to implement the threat of unauthorized impact on information, an electronic resource, an information system or gaining access to them using software or software and hardware (or internetworking protocols).

It is important to understand that liability is not always due to the presence of an incident - for example, the creation of a malicious program - a virus, does not in itself entail an incident, but is the basis for liability. On the other hand, not all incidents are considered a completed offense, since the mere fact of only a threat of IS violation without the onset of consequences cannot be the basis for prosecution.

For training and classification purposes, the following types of incidents are distinguished:

By type of activity, IS incidents are divided into:

- single
- periodic repetitive (serial)
- interconnected (set)
- mass

According to the object of impact, information security incidents are divided into:

- directly affecting the entire IS
- directly affecting individual IS components
- affecting auxiliary / third-party ICs

According to the consequences, information security incidents are divided into illegal:

- obtaining EIR information
- copying EIR
- distribution of EIR
- EIR modifications
- destruction of EIR information
- - EIR blocking

Crisis situation in the field of information security - an information security incident or real prerequisites for its occurrence at ICI facilities, which may lead to the impossibility or restriction of the provision of public services, an emergency of a social and (or) man-made nature, or significant negative consequences for defense, security, international relations, economy, certain areas of the economy, infrastructure of the Republic of Kazakhstan or for the life of the population living in the relevant territory;

In accordance with the classification established in the Republic of Kazakhstan, the following types of incidents are also distinguished:

- Denial of Service (DoS, DDoS); - unauthorized access and modification of content;

- botnet;
- virus attack;
- exploitation of vulnerabilities;
- compromise of means of authentication/authorization;
- phishing;
- another.

An example of an incident and investigation:

VimpelCom and Sherlock

A number of employees (former and current) of the mobile operator Vimpelcom organized the sale of information about the details of telephone conversations and other proprietary information about subscribers. To this end, they organized the sherlock.ru website on the Internet. Having discovered this site, VimpelCom employees independently collected evidence of the site's criminal activities and transferred the case to the Ministry of Internal Affairs. Employees of the Ministry of Internal Affairs opened a criminal case and, together with VimpelCom, identified the organizers of this criminal business. And later the main suspect was caught red-handed.

The most important criterion by which the grading of information security incidents is the level of criticality. Depending on the level of criticality of an information security incident, incidents are divided into:

Severity level		Definition
Critical	Level 5 (black)	Inevitable incidents that will lead to the impossibility of providing services, significant negative consequences for electronic information resources, information systems, telecommunications networks and other informatization objects.
Serious	Level 4 (red)	Possible incidents that will lead to the impossibility of providing services, significant negative consequences for electronic information resources, information systems, telecommunications networks and other informatization objects.
High	Level 3 (orange)	Possible incidents that will lead to a significant restriction in the provision of services, a significant deterioration in the situation or significant negative consequences for electronic information resources, information systems, telecommunications networks and other informatization objects.
Average	Level 2 (yellow)	Probable incidents that will lead to the restriction of the provision of public services, deterioration of the situation or negative consequences for electronic information resources, information systems, telecommunications networks and other informatization objects.
Short	Level 1 (green)	Unlikely incidents that will lead to the restriction of the provision of services, deterioration of the situation or minor negative consequences for electronic information resources, information systems, telecommunications networks and other informatization objects.

		More information about this source text. For more information, enter the source text: - Post a review - Side panels - Story - Saved - Suggest a translation - Disable selected method
Not critical	Level 0 (white)	Minor incidents that do not affect electronic information resources, information systems, telecommunications networks and other informatization objects.

It is obvious that the very fact of identifying an incident without a reaction to it and an investigation calls into question the possibility of bringing the perpetrators to the appropriate type of responsibility.

Control Questions

1. What is an information security incident?
2. How does an incident differ from a security event?
3. What are the main classification criteria for incidents?
4. What are typical examples of IS incidents?
5. What are the main stages of incident response?
6. What principles underlie incident management?
7. What measures can help prevent incidents in information systems?

Recommended Literature

1. ISO/IEC 27035:2016. *Information Security Incident Management.*
2. Tipton, H. F., & Krause, M. (2019). *Information Security Management Handbook.* CRC Press.
3. Peltier, T. R. (2016). *Information Security Policies, Procedures, and Standards.* Auerbach Publications.
4. Solove, D. J. (2021). *Understanding Privacy and Cyber Law.* Aspen Publishing.
5. Law of the Republic of Kazakhstan “On Informatization” (2015).
6. National Cybersecurity Strategy of the Republic of Kazakhstan.