Basic practices of information security + CYBER TRAINING

The goal of the program is to provide participants with an in-depth practical study of network computer security issues.

Course graduates receive a state-issued certificate of advanced training in cybersecurity.

Target audience:

- specialists of information security incident monitoring centers;
- licensees of the Operational and Analytical Center under the President of the Republic of Belarus and applicants for a license for activities in the technical protection of information;
- technical specialists of departments implementing measures for technical and/or cryptographic protection of information in organizations, including at critical information technology facilities.

Required preliminary preparation of students:

- general ideas about information systems, legal, organizational and technical aspects of ensuring information security of computer systems;
- basic knowledge of IP networks, main protocols and services of the TCP/IP stack;
- skills in working with Windows or Linux OS .

The form of study – full-time (daytime).
The cost of training one student – 2700 BYN.

Training is conducted at the address: Minsk, Cl. Zetkin St., 24, 11th floor, in accordance with the schedule of the educational process.

The duration of the program is 56 academic hours.

Course curriculum

Item No.	Course Topic Titles
	Fundamentals of information security.
1.	Objectives and tasks. Program overview. Fundamentals and objectives of information security. Information security management. Information security management system. Directions of development of information security in international practice.
2.	Practical aspects of implementing an information security management system at an enterprise. Risk-based approach.
3.	Practice: description of business processes, definition of the scope of the information security management system. Stages of the information security risk management process. Practice: asset valuation.
	Management of information security risks and incidents.
4.	Information security risk assessment. Processing information security risks. Lecture: Basics of working with information security incidents.
5.	Lecture: Management of information security events and incidents. Practice: Introduction to SIEM. Viewing and filtering events. Cyber Range Scenario: a day in the life of a SOC Operator. Analysis of results, discussion and analysis of the scenario.
	OS security.
6.	Lecture: Linux OS Security Architecture. Practice: Setting up access rights to shared resources for remote users. Lecture: Monitoring and detecting attacks in Linux OS.
7.	Practice: Searching for traces of attacks on compromised hosts, analyzing Linux OS event logs. Lecture: Monitoring and detecting attacks in Windows OS. Practice: searching for traces of attacks on compromised hosts, analyzing event logs.
	Network security.
8.	Lecture: Architecture of a secure network. Lecture: Network traffic analysis. Practice: analyzing unknown traffic in wireshark.

9.	Practice: Configuring blocking of unwanted traffic in iptables. Lecture: Intrusion Detection Systems. Practice: Setting up suspicious traffic detection in suricata.
	Cyber training .
10.	Scenario at a cyber-range: attack by a ransomware virus. Analysis of results, discussion and analysis of the scenario.
11.	Setting up protective measures in the infrastructure. Scenario on the cyber-range: attack by scripts. Testing the implemented protection system. Analysis of results, work on errors. Analysis of attacks.