International exchange program
"Basic Practices for Ensuring Information Security"

The International Education Center of the Republican Unitary Enterprise "National Traffic Exchange Center" invites managers and specialists whose competence includes issues of state regulation and information security to training.

We offer:
1. turnkey training, including accommodation, meals with a choice of menus, transfers and leisure activities;
2. a course with an emphasis on practical exercises;
3. training from lecturers-practitioners, including representatives of the regulator in the field of information security;
4. government-issued document.

The language of training – upon request.

The number of participants in one group is no more than 14 people.

Time	Event
Day 1	
	Meeting at the Minsk-2 airport, hotel accommodation, registration of participants, introductory meeting.
20.00-22.00	Welcome dinner from the Organizers.
Day 2	
8.00-8.45	Breakfast.
9.00-9.15	Presentation of the Program.
9.15-10.00	Lecture: Fundamentals of information security (IS). Confidentiality, integrity, availability. IS tasks. IS management. IS management system.
10.00-11.35	Lecture: Directions of development of information security in the Russian Federation and international practice.
11.45-13.15	Lecture: Principles of comprehensive information security: -4 basic approaches to layered protection; -security policies; -risk management; -access control and password management; -hardening , trusted systems.

Time	Event
13.15-14.15	Lunch.
14.30-16.20	Practice: Demo: password strength assessment: password selection methods using "brute force", dictionary, etc. Using the utility "john the ripper".
16.30-18.30	Practice: Getting to know the platform: Interface, Kali Linux, Infrastructure Inventory. Talking to the Experts.
19.00-20.00	Dinner.
Day 3	
8.30-9.30	Breakfast.
10.00-11.30	Linux OS security architecture: - types of linux; - command shell; - user management, password storage, privilege escalation; - rights management: rwx.
11.40-13.00	Practice: Configuring access rights to shared resources for remote users.
13.15-14.15	Lunch.
14.30-16.00	Lecture: Monitoring and detecting attacks: - security logs; - security utilities.
16.10-18.30	Practice: Searching for traces of attacks on compromised hosts, analyzing event logs.
19.00-20.00	Dinner.
Day 4	
8.00-8.45	Breakfast.
9.00-9.45	Lecture: Secure Network Architecture.
9.45-10.30	Lecture: Network traffic analysis.
10.40-12.00	Practice: Analysis of unknown traffic in wireshark.
12.15-13.15	Lunch.
13.30-15.00	Practice: Setting up blocking of unwanted traffic in iptables.
15.10-15.50	Lecture: Intrusion Detection Systems.
16.00-17.30	Practice: Setting up detection of suspicious traffic in suricata.
18.00-19.00	Dinner.
19.00-21.00	Excursion program.
Day 5.	
8.30-9.30	Breakfast.

Time	Event
10.00-11.30	Lecture: Vulnerability Management and Security Analysis Definitions: - threat, vulnerability, incident; - CVE, CWE, FSTEC BDU; - CVSS, ROI, ROSI; - local and network security analysis.
11.40-13.00	Practice: Security analysis using security scanners: visible addresses (hping3), open ports (nmap), vulnerable services (GVM/ ScanOval / linys / Retina).
13.15-14.15	Lunch.
14.30-15.15	Lecture: Protection against malicious code and exploits: - attack matrix; - examples of attacks and virus operation; - protection strategies.
15.15-16.00	Lecture: Endpoint protection: antiviruses; firewalls; HIDS/HIPS; DLP.
16.10-18.30	Practice: Configuring an antivirus complex using KSC as an example: - installing KSC; - deploying KES; - searching for eicar in the infrastructure.
19.00-20.00	Dinner.
Day 6	
8.30-9.30	Breakfast.
10.00-11.30	Lecture: Basics of Incident Management: - 6-Step Incident Response Process - Business Continuity Analysis (BIA) - Contingency Planning: Continuity Plan and Recovery Plan.
11.40-13.00	Lecture: Information Security Event and Incident Management - Log Monitoring Strategy - Log Analysis Basics - SIEM Operation Principle.
13.15-14.15	Lunch.
14.30-16.00	Practice: " Getting to know SIEM: - working with SIEM; - viewing/filtering events.

Time	Event
16.10-18.30	Practice: Scenario on the cyber range: One day in the life of a SOC operator.
19.00-20.00	Dinner.
Day 7	
8.00-8.45	Breakfast.
09.00-10.30	Practice: Investigation of the "Cipherman" incident.
10.40-12.00	Practice: Investigation of the "Cipherman" incident.
12.15-13.15	Lunch.
13.30-15.00	Practice: Configuring protective measures in the infrastructure."
15.10-16.10	Practice: Script attack. Testing the implemented protection system.
16.10-17.30	Lecture: Teamwork. Working on mistakes. Analysis of attacks.
17.30-18.00	A series of questions and answers. Final remarks on the results of the program.
18.00-19.30	Presentation of state-issued educational documents to students. Summing up the results of the Program with the participation of the management of the Operational and Analytical Center under the President of the Republic of Belarus and representatives of specialized Belarusian organizations/enterprises. * At the suggestion of the audience, authorized representatives of other Belarusian departments and organizations that did not participate in the lecture portion of the Program may be invited.
20.00-22.00	Dinner from the Organizers.
Day 8	
8.00-8.45	Breakfast (lunch if necessary).
	Transfer to Minsk-2 airport.

The cost for one participant: 1,850 (one thousand eight hundred and fifty) US dollars in equivalent and includes: transfer from/to Minsk-2 airport, training in specially equipped classrooms, accommodation in comfortable single and/or double rooms of the Forum hotel and educational complex of the Ministry of Finance of the Republic of Belarus (https://forumhotel.by/about/), 3 meals a day with a choice of menu, cultural program.

*The Program may be subject to adjustments depending on current logistics and individual wishes of the listeners.