Practical InfoSec Technology Applications + Advanced Cyber Training (Hands-On)

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

Required preliminary preparation of students:

- completion of training under the program "Basic practices of ensuring information security + CYBER TRAINING".

The form of study is full-time (daytime).
The cost of training – 3500 BYN.

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

The duration of the program is 50 academic hours.

Course curriculum

Item No.	Course Topic Titles
	Incident Response Methodology
1.	Cybersecurity, information security, and data protection. Experience in countering cybercrime (case studies from the Republic of Belarus and the Russian Federation).
2.	Typical corporate information system architecture.
3.	Advanced cyberattacks. MITRE ATT&CK Framework. Cyber Kill Chain model. Indicators of Compromise (IoCs).
4.	Information security lifecycle.
	Active Directory
1.	Active Directory domains. Domain Group Policy.
2.	Working with AD Group Policies.
3.	Domain authentication. Typical attacks on authentication protocols.
4.	Typical attacks on Active Directory.
	Introduction to LDAP
1.	Introduction to LDAP.
2.	LDAP security. Monitoring and debugging LDAP. LDAP data backup and recovery.
3.	LDAP server installation and configuration.
4.	LDAP data models.
5.	Integration with other services.
6.	LDAP recovery.
7.	LDAP debugging and hardening.
	System recovery
1.	Leveraging recovery after threat containment.
2.	Implementing defensive measures during infrastructure attacks.
3.	Service restoration after threat containment.
4.	Information security incident investigation methodology in SIEM. Typical use cases.
	Cyber Training Exercises (Hands-On Cyber Range)
1.	Ransomware attack scenario simulation on the cyber range. Results analysis, debriefing, and scenario review.
2.	Configuring defensive measures within the infrastructure.
3.	Script-based attack scenario simulation on the cyber range. Validation of the implemented security controls with infrastructure availability restoration. Results analysis, lessons learned, and attack breakdown.