



Training course outline

ITU and
Institute for Security and Safety (ISS) at the Brandenburg University of Applied Sciences

Title	Cybersecurity Techniques
Modality	Online self-paced
Dates	January 15 – December 31, 2022
Duration	Flexible
Registration deadline	There are no deadlines for course registration. The course could be taken any time within indicated timeframe. An enrollment is happening continuously.
Training fees	USD 249,00
Description	<p>This online course will provide theoretical and practical knowledge of it and cyber security and security methods for computer, network and electronic communication.</p> <p>The course consists of various chapters and will cover fundamentals, such as IT versus ICS, threats and their sources, authentication, computer access control, cryptography, network security, network firewall concepts, intrusion detection.</p> <p>The student will get a comprehensive view on security in the cyber space.</p>
Code	22OS28028EUR-E

1.LEARNING OBJECTIVES

Upon the successful completion of this course, students will be able to explain and give examples of IT and cybersecurity as well as apply and use computer and communication security measures. They will be able to utilize different intrusion detection methods and establish network management practice.

2. LEARNING OUTCOMES

As a result of the course, participants will acquire:

- knowledge of computer security elements fundamentals;
- knowledge of computer access control;
- knowledge of security architecture;
- knowledge of technical measures for network and host security;



- knowledge of network management best practices;
- knowledge of physical protection role in computer security.

3.TARGET POPULATION

The course is designed to be a great value for managers, engineers and employees from regulators, government organizations, private companies and academia, who want to get further career in the cybersecurity area or need to extend their expertise with cybersecurity related topics.

4.ENTRY REQUIREMENTS

There are no prerequisites.

5.TUTORS/INSTRUCTORS

Name of tutor(s)/instructor(s)	Contact details
Dmytro Cherkashyn	d.cherkashyn@uniss.org

6.TRAINING COURSE CONTENTS

Main modules of this course will cover following topics:

1. Computer security and access control
 - Prevention;
 - Physical security;
 - Computer operating systems;
 - Access control principles;
 - Remote maintenance.
2. Authentication and cryptography
 - Authentication methods;
 - Practical application.
3. Computer security architecture
 - Threats and vulnerabilities to computing infrastructure;
 - Consequence analysis;
 - Security levels, multilevel security;
 - Security zones.
4. Network security
 - Network devices and services;
 - Expected threats;
 - Firewalls;
 - VPNs;
 - Secure LAN;
 - E-mail communication.
5. Intrusion detection and information recovery
 - Common intrusion methods;
 - Network attacks;
 - Intrusion detection;
 - Responses to intrusion;



- Computer forensics;
- Recovery plan.
- 6. Network management practice
 - Automated vulnerability detection;
 - Scanning techniques and approaches;
 - Countermeasures against network threats.

7. TRAINING COURSE SCHEDULE

There is no fixed schedule

8. METHODOLOGY (Didactic approach)

The course is self-paced online course with lecturing materials accompanied with different media. Each page of the course includes link to external sources of information, which could be used to get deeper knowledge of some particular topics. Each course module has a self-assessment quiz.

9. EVALUATION AND GRADING

Evaluation of participant success will happen through the final test of multiple-choice quizzes. Only participants who have successfully completed final test with a pass mark of 80% shall be awarded the ITU Certificate.

10. TRAINING COURSE COORDINATION

Course coordinator:	ITU coordinator:
Name: Dmytro Cherkashyn	Name: Jaroslaw Ponder
Email address: d.cherkashyn@uniss.org	Email address: eurregion@itu.int