ITU Centres of Excellence Network for Europe

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

Online Training Course on

CYBERSECURITY TECHNIQUES

1 March – 31 December 2021

TRAINING COURSE OUTLINE

COURSE DESCRIPTION

Title	Cybersecurity Techniques
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.
Dates	1 March – 31 December 2021**
Duration	Flexible (about 4 weeks)
Registration deadline	There is no deadline for course registration. The course can be taken any time within indicated timeframe. An enrollment is happening continuously.
Training fees	USD 249
Course code	21OS26410EUR-E

DESCRIPTION OF THE TRAINING COURSE

This online course will provide theoretical and practical knowledge of IT and cyber security and security methods for computer, network and electronic communication.
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.
The student will get a comprehensive view on security in the cyber space.

The course will be a self-studying course with an Q&A session (video conference) near the end of the course.
****While the course dates are open until December, participants are expected to finalize the course within 3 months counting as of March 1st . The following cohorts of students will start June 1st, September 1st and November 1st.**

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.

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.

ENTRY REQUIREMENTS

There are no specific requirements for this course; some knowledge of IT basics would be an advantage though.

TUTORS/INSTRUCTORS

NAME OF TUTOR(S)/INSTRUCTOR(S)	CONTACT DETAILS
Dmytro Cherkashyn	d.cherkashyn@uniss.org

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.

TRAINING COURSE SCHEDULE

Three weeks of self-studying the contents, after that, a live Q&A Session will help to clarify remaining questions. In the last week, the students will take the final exam.

METHODOLOGY (Didactic approach)

The course is self-paced online course with lecturing materials accompanied with different media. Each page of the course includes links 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.
After completing the self-assessment, the students can discuss their remaining questions in an online live Q&A session (video conference) with their trainer before taking the final exam.

EVALUATION AND GRADING

Evaluation of participant success will happen through the final exam. They have to pass with at least 80% of correctly answered questions.

TRAINING COURSE COORDINATION

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

REGISTRATION AND PAYMENT

ITU Academy portal account

Registration and payment should be made online at the ITU Academy portal.
To be able to register for the course you **MUST** first create an account in the ITU Academy portal at the following address: https://academy.itu.int/index.php/user/register

Training course registration

When you have an existing account or created a new account, you can register for the course online at the following link: https://academy.itu.int/training-courses/full-catalogue/cybersecurity-techniques-1

You can also register by finding your desired course in our training catalogue https://academy.itu.int/index.php/training-courses/full-catalogue.

Payment

1. On-line payment

A training fee of USD 249 per participant is applied for this training. Payment should be made via the online system using the link mentioned above for training registration at https://academy.itu.int/training-courses/full-catalogue/cybersecurity-techniques-1 .

2. Payment by bank transfer

Where it is not possible to make payment via the online system, select the option for offline payment to generate an invoice using the same link as above. Download the invoice to make a bank transfer to the ITU bank account shown below. Then send the proof of payment/copy of bank transfer slip and the invoice copy to Hcbmail@itu.int and copy the course coordinator. **All bank transaction fees must be borne by the payer**.
Failure to submit the above documents may result in the applicant not being registered for the training.

3. Group payment

Should you wish to pay for more than one participant using bank transfer and need one invoice for all of them, create an account as **Institutional Contact. Institutional Contacts** are users that represent an organization. Any student can request to be an institutional contact or to belong to any existing organization.

To do this, head to your profile page by clicking on the **"My account"** button in the user menu. At the bottom of this page you should see two buttons:

a. If you want to **become an institutional contact**, click on the "**Apply to be an Institutional Contact"** button. This will redirect you to a small form that will ask for the organization name. After you fill the name of the organization you want to represent, click on **"continue"** and a request will be created. An ITU Academy manager will manually review this request and accept or deny it accordingly.

b. If you want to **belong to an existing organization**, click on the **"Request to belong to an Institutional Contact"** button. This will redirect you to a small form that will ask you to select the organization you want to join from an organization list. After you select the correct organization, click on **"continue"**, a request will then be created. The Institutional Contact that represents that organization will manually accept or deny your request to join the organization.

ITU BANK ACCOUNT DETAILS:	
Name and Address of Bank:	UBS Switzerland AG Case postale 2600 CH 1211 Geneva 2 Switzerland
Beneficiary:	Union Internationale des Télécommunications
Account number:	240-C8108252.2 (USD)
Swift:	UBSWCHZH80A
IBAN	CH54 0024 0240 C810 8252 2
Amount:	USD 249
Payment Reference:	CoE-EUR 26410 - P.40595.1.07

4. Other method of payment

If due to national regulations, there are restrictions that do not allow for payment to be made using options 1 & 2 above, please contact the ITU coordinator for further assistance.