



ITU Centres of Excellence Network for CIS
Belarusian State Academy of Communications
FACE-TO-FACE Training Course on
Cybersecurity of Web Sites and Web Applications
Minsk, Republic of Belarus
13-15 November 2019

COURSE OUTLINE

COURSE DESCRIPTION

Title	Cybersecurity of Web Sites and Web Applications
Objectives	This training course aims to introduce participants with the issues of network infrastructure and Internet services protection, as well as with best practices in the use of different network and program solutions aimed at the protection of web resources and the network in general. The training will consider possible web service attacks and their consequences (OWASP project and top 10 vulnerabilities), as well as possible variants of protection. The training will cover both theoretical instructions and practice.
Dates	13-15 November 2019
Duration	3 days
Registration deadline	11 November 2019
Training fees	USD 120
Course code	19WS24297CIS-R

LEARNING OUTCOMES

Upon completion of the course, participants will have notion of the network infrastructure and Internet services protection, appliance of different network and program solutions aimed at the protection of web resources and the network in general, categories of web service attacks and possible variants of protection, web server organization, structure, and components, basics of databases and languages of HTML, JavaScript и SQL.

TARGET POPULATION

The training is intended for professionals dealing with: information protection in telecommunications systems and networks; security of computer systems and networks; administration of network devices of information and communication systems; as well as for heads and specialists of cybersecurity departments. The training course will be also of interest for managers in the sphere of ICT, employees of regulatory bodies, service providing companies, professors of ICT-specialized universities.

TUTORS/INSTRUCTORS

NAME OF TUTOR	CONTACT DETAILS
Sergey Ilyuschenko	Email: serg-mephisto@mail.ru

EVALUATION

A recitation will be conducted on the last day of the course during the round table. It will consist of many questions, which are expected to be clearly answered. Evaluation of the participant advancement to provide a certificate upon completion of course will be mainly based on the results of the recitation, however, the answers to questions raised during discussions and practical sessions will be taken into consideration as well.

TRAINING SCHEDULE AND CONTENTS / AGENDA

13 November 2019, Wednesday

10:00-10:10	Opening remarks: <ul style="list-style-type: none">• Ministry of Communications and Informatization of the Republic of Belarus• Belarusian State Academy of Communicaitons
10:10-11:00	Session 1: Network Technologies and the Internet Session will cover issues, such as: network organization, packet switching network technologies and protocols, developments occurring in the networks. The session will present the most widely applied networking and network service protocols, service addressing, and network host communication principles.
11:00-11:30	Coffee break. Official photo
11:30-13:00	Session 1: Network Technologies and the Internet (continued)
13:00-14:00	Lunch
14:00-15:30	Session 2: Cybersecurity in the Internet Session will cover issues, such as: protection of network infrastructure and Internet services; general theory and principles of cybersecurity; network attacks and possible protection methods; choice of network elements protection means. The session includes practical session on network infrastructure protection.
15:30-16:00	Coffee break
16:00-17:30	Session 2: Cybersecurity in the Internet (continued)

14 November 2019, Thursday

09:30-11:00	Session 3: Network Attack Evolution and Application Protection Session will cover issues, such as: protection of network services and applications, vulnerability of Internet service protocols and, in particular, web services.
11:00-11:30	Coffee break
11:30-13:00	Session 4: Organization of Web Service Session aims at understanding of web service work for its further protection. The session will cover issues, such as: web server organization, structure, and components; basics of data bases and languages of HTML, JavaScript and SQL. The session includes practical session on web service organization and programming on languages of HTML, JavaScript, SQL
13:00-14:00	Lunch
14:00-15:30	Session 4: Organization of Web Service (continued)
15:30-16:00	Coffee break
16:00-17:30	Session 5: Web Service Attacks Session will cover issues of web service defense against attacks and present web service attacks, their consequences (OWASP project and top 10 vulnerabilities): authentication and authorization system evasion, injection of malicious codes (SQL- injection), cross-site scripting (XSS attacks), obtaining access to operation system (reverse SHELL) and others. The session will also present possible protection options. The Session includes practical session on defending against web service attacks.

15 November 2019 года, Friday

09:30-11:00	Session 5: Web Service Attacks (continued).
11:00-11:30	Coffee-break
11:30-13:00	Сессия 5: Web Service Attacks (continued)
13:00-14:00	Lunch
14:00-15:30	Session 6: Practical Recommendations for Web Resource Protection Session will present network and program solutions to protect web resources and the network in general.
15:30-16:00	Coffee break
16:00-17:00	Roundtable Roundtable is aimed at sharing opinions and experiences in the field of cybersecurity and, in particular, web services.
17:00-17:30	Wrap-up. Closure of the training

METHODOLOGY

The training will include lectures with a demonstration of presentations under the guidance of an instructor, case studies, group exercises and assignments.
All necessary materials will be issued by the teacher on the first day of the seminar.

COURSE COORDINATION

Course coordinator: Name: Oleg Khodasevich, Head, Department of Advanced Training, Belarusian State Academy of Communications Email: o.khodasevich@bsac.by	ITU coordinator: Name: Farid Nakhli, Programme Officer, Regional Office for CIS Region Email: farid.nakhli@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?option=com_hikashop&view=user&layout=form&Itemid=559&lang=en

Training 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-web-sites-and-web-applications>

You can also register by finding your desired course in our training catalogue

https://academy.itu.int/index.php?option=com_joomla&view=coursescatalogdomain&Itemid=478&lang=en

Payment

1. On-line payment

A training fee of USD 120 per participant is applied for this training. Payments 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-web-sites-and-web-applications>

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 120
Payment Reference:	CoE-19WS24297CIS-R-P.40594.1.05

4. Other methods 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.