

Faculty: FACULTY OF TELECOMMUNICATIONS AND MANAGEMENT
Department: INFORMATION TECHNOLOGIES
Professional Field: 5.3 COMMUNICATION AND COMPUTER TECHNOLOGY
Specialty: CYBER SECURITY OF HIGH TECHNOLOGIES
Educational-qualification degree: PROFESSIONAL BACHELOR

LEARNING COURSE DESCRIPTION

1.Course title:Cloud Infrastructure Security

2.Course code: P.18.043.1

3.Type of the course: compulsory

4.Level: *Professional Bachelor*

5.Year of study: 3

6.Semester: 6

7.Number of credits: 4

8.Name of the lecturer: Assist. Prof. Strahil Sokolov, Eng. PhD

9.Course learning outcomes:

The aim of the course is to give students a systematic theoretical and practical knowledge of the role of protection of cloud infrastructures, cryptocurrencies and distributed systems based on trust. Students who have completed the course must have skills in working with systems based on the protection of cloud infrastructures and practical skills in working with decentralized applications. Students who have completed their training in the discipline must acquire:

Basic knowledge of:

- the protection of cloud infrastructures
- protection mechanisms
- regulations and practical application for protection

Practical skills for

- Work with modern infrastructure for research of cyber protection of cloud infrastructures
- Design of cloud infrastructure protection

Competencies: Upon successful completion of the course students should be able to:

To know the basic tasks and principles of cloud infrastructure protection;

Know the concept of attacks against cloud infrastructure;

To work with programs and systems for protection of cloud infrastructure.

10.Teaching methods:

The method of teaching is through lectures, block or two lesson per week for 15 weeks and practical exercises in block or two lesson per week for 15 weeks.

11. Prerequisites:

Students should have prior knowledge of Basics of Programming, Linux OS, Linux Administration, Server Protection Workshop, Cloud Technologies

12. Course contents:

Introduction to the course is studied in the course. Basics of cloud computing and architectural features. Architectural and technological influences of cloud computing. Security risks Security design and architecture for cloud infrastructures. Basic concepts and principles for security design. Secure insulation. Complete data protection. End-to-end access control. Monitoring and audit. A quick look at the CSA, NIST and ENISA guidelines for Cloud Security. Generalized type of attack vectors and cyber threats Secure isolation of physical and logical infrastructure. Calculation, network and storage. Multitenancy, virtualization strategies. Strategies for network segmentation between users. Strategies for data storage isolation Data protection in cloud infrastructure and services. Information life cycle. Data protection for confidentiality and integrity. Encryption, Data Editing, Tokenization, Dimming, PKI and Key. Management, ensuring data deletion. Procedures for retaining, deleting and archiving data for cloud infrastructure users. Data protection strategies

Implement access control for services based on cloud infrastructure. Implement access control strategies. Authentication and authorization. Role-based access control, multifactor authentication. OS protection, providing remote access, Secure kernel OS boot. Firewalls, IDS, IPS and copper points Monitoring, audit and management. Proactive monitoring of the activity, reaction in case of incidents. Monitoring for unauthorized access, malicious traffic, abuse of system privileges, intrusion detection, events and alerts. Identity management. User management. Security and event management information

Introduction to cloud infrastructure protection design models. Introduction to design models and architectural models for cloud computing. Platforms for virtualization and cloud virtualization. Conducting a test on the subject. Introduction to identity management in cloud infrastructures. User identification, authentication and authorization in the cloud. Identity providers and service users. Cloud computing security models. Trusted platform. Geo-marking. Platform level encryption in a cloud virtual machine. Reliable cloud resource pools. Secure cloud interfaces. Control of access to cloud resources. Protection against cloud data breach. Data encryption in the cloud during transfer Cloud computing security models - II. Access management and trust. Secure internet access on site. Secure external cloud connection. Cloud service denial protection. Protection against hijacking of cloud traffic. Automatically determined perimeter. Cloud authentication gateway. Federated cloud authentication. Cloud key management. Trust auto identification service. Monitoring and registration. Independent audit in the cloud Policy, compliance and risk management in cloud computing. Cloud security assessment and audit reports. Laws and regulatory mandates. Personal identifying information and data confidentiality. Cloud compliance assessment and reporting Cloud Service Providers - Technology Review. Summary of the course. Presentation of reports and study of the practical applicability of the protection of cloud infrastructures.

13. Bibliography

Basic literature:

1. **Securing The Cloud: Cloud Computing Security Techniques and Tactics by Vic (J.R.) Winkler (Syngress/Elsevier) - 978-1-59749-592-9**
2. **Cloud Computing Design Patterns by Thomas Erl (Prentice Hall) - 978-0133858563**

Additional literature:

1. **Krutz, Ronald L., and Russell Dean Vines. *Cloud security: A comprehensive guide to secure cloud computing*. Wiley Publishing, 2010.**
2. **Ko, Ryan, and Raymond Choo. *The cloud security ecosystem: technical, legal, business and management issues*. Syngress, 2015.**
3. **Ransome, James F. *Cloud Computing: Implementation, Management, and Security*. CRC Press, 2017.**

14. Assessment methods and criteria:

The course ends with an exam.

1. Requirements for the assessment of the six-point system

The total number of points from the written exam that can be reached is 100. Each of the questions in the final exam carries 3 points, and the answer to the open question can carry up to 10 points.

2. Formation of the final mark

The formation of the final grade is carried out on the basis of a point system as the maximum number of points that students can receive is 100 and can include various activities.

Forming an assessment in the training course at each of the above stages, according to the points obtained and their ranking according to the six-point system is given in Table 1.

Table 1.

Number of points	Assessment According to the 6-pointScale System
------------------	---

0 – 20	Fail 2 (F)
20 – 39	Fail 2 (FX)
40 – 49	Satisfactory 3.00 (E)
50 – 59	Satisfactory 3.00 (D)
60 – 69	Good 4.00 (C)
70 – 84	Very good 5.00 (B)
85 – 100	Excellent 6.00 (A)

15. Language of instruction:Bulgarian/English