

Faculty: FACULTY OF TELECOMMUNICATIONS AND MANAGEMENT
Department: INFORMATION TECHNOLOGIES
Professional Field: 5.3.Communication and Computer Engineering
Specialty: COMPUTER ADMINISTRATION OF SOFTWARE APPLICATIONS
Educational-qualification degree: PROFESSIONAL BACHELOR

LEARNING COURSE DESCRIPTION

1. **Course title:** FIREWALLS
2. **Course code:** P.16.035.1
3. **Type of the course:** compulsory
4. **Level:** Professional Bachelor
5. **Year of study:** third
6. **Semester:** fifth
7. **Number of credits:** 4,5
8. **Name of the lecturer (s):** Assoc. Prof. PhD Irina Topalova,

9. **Course learning outcomes:** The aim of the course is to acquaint students with the theoretical and practical aspects of modern types of network security threats, modern methods and technical means to mitigate threats, types of firewalls, and their practical application. The course addresses issues related to the ideology and design of firewalls when implementing them in the network structure. The students who have completed their training in the course must acquire:

Basic knowledge of the types of attack detection techniques, the types of firewalls and their capabilities.

Practical skills for application of the acquired functionalities of modern technical means for detection and prevention of attacks in real security systems, as well as for implementation of firewalls in the communication systems.

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

- know modern methods and tools to mitigate threats, as well as network security audit tools;
- use local and server-based automated security features on network devices;
- know the types and technologies of firewalls;
- design, configure and test VPN tunnel types;
- configure technical adaptive network security features - ASA - (Adaptive Security Appliance).
- work with Device Manager, ASA Security Device Manager (ASDM) and Hillstone.

10.Teaching methods: The lectures are conducted in the classical way, as the students get acquainted with the material. The statements are illustrated with examples that make it easier for students to practice. The lectures are richly illustrated with graphic material, which is represented by presentations with a multimedia projector. Practical exercises are held in the computer labs of the department, equipped with the necessary network devices and software packages for simulation.

11. Prerequisites: The inputs are acquired knowledge of *Networks and Protocols 1* ", " *Networks and Protocols 2* " and " *Load Balancing of network traffic* ", etc. taught in previous semesters technical subjects.

12. Course contents: The course focuses on acquiring knowledge of the functionalities of modern technical means of detecting attacks, technologies in firewalls, and for their proper integration into the network structure of communication systems to provide reliable protection. In practical terms, the course includes the basic elements and specific implementations of various technical means of detecting attacks and designing firewalls in modern communications networks.

13. Bibliography

Basic literature:

1. Omar Santos, Jazib Frahim, Cisco ASA Security Contexts, 2015, Cisco Press.
2. Cisco IOS XR Fundamentals by Dawit Birhanu, Mark Ghattas, Syed Natif Nawaz, Mobeen Tahir, Chapter 5. Cisco IOS XR Monitoring and Operations, 2017.
3. Joseph Muniz, Nadhem AlFardan, Gary McIntyre, Overview of Security Operations Center Technologies, 2015, Cisco Press.
4. Sean Wilkins, Cisco ASA Access Lists Concepts and Configuration, 2013, Cisco Press.
5. Hillstone E-2000 Series Next-Generation Firewall, User Manuel, www.hillstonenet.com, 2018.

Additional literature:

6. Monitoring and Troubleshooting With Cisco Prime LAN Management Solution 4.1, Copyright © 2011 Cisco Systems, Inc. All rights reserved.
7. <https://www.capterra.com/network-monitoring-software/>, 2018.
8. <http://sectools.org/sploits.html>, 2018.
9. Rowayda, A. Sadek; M Sami, Soliman; Hagar, S Elsayed, Effective anomaly intrusion detection system based on neural network with indicator variable and rough set reduction. International Journal of Computer Science Issues, 2014.
10. Keerthi Latha, Learn About Intrusion Detection and Prevention, © 2016 by Juniper Networks, Inc. All rights reserved, 2016.

14. Assessment methods and criteria: The final assessment is based on the points obtained during the semester, the correspondence between the number of points and the six-point assessment is presented in Table 1. On the announced date for completion of the final grade, the students develop one or two questions of the discipline in writing and solve a case study in a practical assignment.

Table 1.

Number of points	Assessment According to the 6-point Scale System
0 – 10	Fail 2 (F)
11 – 20	Fail 2 (FX)
21 – 26	Satisfactory 3.00 (E)
27 – 31	Satisfactory 3.00 (D)
32 – 40	Good 4.00 (C)
41 – 48	Very good 5.00 (B)
over 49 points	Excellent 6.00 (A)

15. Language of instruction: *Bulgarian/English*