

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

LEARNING COURSE DESCRIPTION

1. Course title: SECURITY OF ELECTRONIC PAYMENT CARDS

2. Course code: B.43.041.2

3. Type of the course: selectable

4. Level: bachelor

5. Year of study: 3

6. Semester: 5

7. Number of credits: 4,5

8. Name of the lecturer: Assoc. Prof. Dr. Eng. Ivan Ivanov

9. Course learning outcomes:

The aim of the course is to give students in a systematized form theoretical and practical knowledge about the most popular microprocessor «plastic» cards. The course introduces students to the standards and features of these cards. The lectures cover the EMV standard, data, file structure, encryption and key management for secure data transmission.

Students completing the course should have the skills to assess the risk and security of microprocessor cards, theoretically explain pin and cardholder verification methods, and perform basic card customization and migration tasks. Also to be able to freely compare between different maps.

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

- to assess security;
- apply the EMV standard;
- to customize the cards.

10. Teaching methods:

The lectures are conducted by acquainting the students with the material provided in the curriculum. The lectures are illustrated with graphic and video material, with illustrative examples and tasks, which are presented through presentations with a multimedia projector.

The practical exercises are conducted in the laboratories of the department, equipped with modern computers and network devices, and each student works independently.

Before each practical session, students are informed about the need for preliminary training on the topic.

11. Prerequisites:

Students should have in-depth knowledge of Engineering Mathematics, Fundamentals of Security, Fundamentals of Cryptography, Linux and Object Oriented Programming.

12. Course contents:

Current topics related to "plastic" card basics and standards, general characteristics, communication protocols and physical security assessment of microprocessor cards, card file structure, EMV standard, PIN code encryption, processing technologies and applications are covered in the course. of transactions, cardholder verification, card customization and life cycle and procedures and risk assessment when using a terminal.

13. Bibliography

Basic literature:

1. Goldovsky I. M, Microprocessor cards of the EMV standard, 2016.
2. Cristian Radu, Implementing Electronic Card Payment Systems. Artech House (October 31, 2012)
3. Sherif M, Protocols for Secure Electronic Commerce. CRC Press, 2018.

4. Susanto H, Almunawar M, Information Security Management Systems. Apple Academic Press, 2018.

Additional literature:

1. Ken E. Sigler, James L. Rainey, III, Securing an IT Organization through Governance, Risk Management, and Audit. Auerbach Publications, 2016.

14. Assessment methods and criteria:

The evaluation of the discipline is formed through a point system, the maximum number of points that students can receive is 100 (see table 1). Knowledge, skills and competence are evaluated by conducting written control works to check the theoretical and practical assimilation of the learning material, the performance of the students during the practical exercises, as well as their ability to independently solve the tasks set in the practical exercises. The discipline ends with a written exam.

Table 1.

Number of points	Assessment According to the 6-point Scale 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*