

Faculty: FACULTY OF TELECOMMUNICATIONS AND MANAGEMENT
Department: INFORMATION TECHNOLOGIES
Professional Field: 5.3.COMMUNICATION AND COMPUTER ENGINEERING
Specialty: CYBERSECURITY OF COMMUNICATION TECHNOLOGIES
Educational-qualification degree: Bachelor
LEARNING COURSE DESCRIPTION

1. **Course title:** PROTECTION OF INFORMATION IN E- COMMERS
2. **Course code:** B.43.031.2
3. **Type of the course:** compulsory
4. **Level:** Bachelor
5. **Year of study:** 2
6. **Semester:** 4
7. **Number of credits:** 6
8. **Name of the lecturer(s):** Biserov Zahari, PhD
9. **Course learning outcomes:**

The aim of the course is to acquire in a systematic way the theoretical and practical knowledge about the prevention and protection of information in e-commerce.

Students who have completed their training during the course must acquire:

Basic knowledge of processes for identifying, minimizing and eliminating threats related to information in e-commerce. This discipline contributes to building analysis capabilities, a proper approach and understanding of security processes in general, and in particular information protection in e-commerce, and has its place in the Cyber Security High-Tech.

Students who have completed their training during the course must acquire:

Practical skills responding to the changing security environment and in particular protection of information in e-commerce, according to the need for a new order of priorities in the security policy. It is necessary to incorporate the full potential of society by applying new forms of interaction between the person, the society and the state. Extending the social scope of security policy in all its aspects poses new challenges to the overwhelming majority of staff in the private and public sectors, academics and lawmakers.

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

- they must have the skills to work in depth and apply the regulatory framework guaranteeing the protection of information in e-commerce;
- Implement good practices for the technological detection and prevention of incidents in cyberspace and ensure cyber-security of high technology.

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 work in the exercises. The lectures are richly illustrated with graphic material, which is represented by presentations with a multimedia projector and supplemented with examples that appear on a whiteboard.

Practical exercises are held in the computer labs of the department, equipped with the necessary applications and devices, and simulation software.

11. Prerequisites:

Entrance links are the general knowledge acquired in the secondary education and the personal experience of each student as well as the technical subjects taught in previous semesters.

12. Course contents: The course focuses on the essence and the specifics of the theoretical fundamentals of security, practical skills for identifying the threats, managing the risk processes in defense of the information in the e-commerce.

13. Bibliography

Basic literature:

1. Biserov, Z., Risk factors and processes for information security, report of the International Scientific Conference on "Modern Security and Modern Technologies", NBU, Sofia. March 2019
2. Biserov, Z., Cyberattacks and Information Warfare, report of the International Scientific Conference on "Modern Security and Modern Technologies", NBU, Sofia. March 2019
3. Law on Protection of Competition, prom. DV. No. 102 of November 28, 2008, last amended. DV. no. 88 of 9 November 2010
4. Personal Data Protection Act, prom. DV. issue 1 of 4 January 2002, last amended DV. issue 7 of January 19, 2018
5. Law on Electronic Government Prom. DV. issue 46 of 12 June 2007, last amended DV. issue 88 of 23 October 2018
6. Electronic Commerce Act. Prom. DV. issue 51 of June 23, 2006, supplement DV. issue 94 of 13 November 2018, amended DV. issue 17 of February 26, 2019
7. Electronic Document and Electronic Certification Services Act. Prom. DV. No. 34 of April 6, 2001, as amended. DV. issue 1 of January 3, 2019, amended DV. issue 58 of July 23, 2019
8. Ordinance on the minimum requirements for network and information security; Prom. DV. issue 101 of 25 November 2008, amended and ext. DV. issue 5 of January 17, 2017, revoked DV. issue 59 of July 26, 2019

Additional literature:

1. Biserov, Z., Basic approaches to constructing information security policies in e-commerce, report of the International Scientific Conference on "Broad Security", NBU, Sofia. March 2020. Collection of scientific papers
2. Biserov, Z. Classification of modern threats to information security, report of the International Scientific Conference on "Broad Security", NBU, Sofia. March 2020. Proceedings.
3. Biserov, Z. Information - the main object of security, report of the Fifth International Scientific Conference TIEM 2020 of VUTP, Sofia. 2020
4. Krastev, D. Legal regulation of the category of biometric personal data, In: Collection of reports from the annual university scientific conference of Vasil Levski National University, Vol. 8, 2020,
5. Krastev, D. Use of biometric data for workplace control, In: Collection of reports from the annual university scientific conference of Vasil Levski National University, Vol. 8, 2020,
6. Krastev, D. Relationship between the concepts of information security and "cybersecurity", In: Collection of reports "Current security issues", Vasil Levski National University, Vol. 6, 2020,
7. Krastev, D. Systems for video surveillance at the borders of the Republic of Bulgaria, In: Collection of reports "Current security issues", Vasil Levski National High School, Vol. 6, 2020,

14. Assessment methods and criteria: Students receive certification after completing the lecture course, based on fulfilled work criteria, by solving tests, case studies and practical assignments.

The course ends with a written exam.

Weight of the assessment: 50% of the test and 50% of the written work.

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