

Faculty: FACULTY OF TELECOMMUNICATIONS AND MANAGEMENT
Department: INFORMATION TECHNOLOGIES
Professional Field: 5.3.COMMUNICATION AND COMPUTER ENGINEERING
Specialty: CYBERSECURITY IN COMMUNICATION TECHNOLOGIES
Educational-qualification degree: BACHELOR

LEARNING COURSE DESCRIPTION

1. **Course title:** INFORMATION SECURITY MANAGEMENT
2. **Course code:** B.43.042.1
3. **Type of the course:** mandatory
4. **Level:** Bachelor
5. **Year of study:** third
6. **Semester:** 6
7. **Number of credits:** 4.5
8. **Name of the lecturer(s):** Assoc. Prof. Dragomir Krastev and Assoc. Prof. Dr. Zahari Biserov
9. **Course learning outcomes:**

The aim of the course is for students to gain in a systematic way theoretical and practical knowledge about the measures for prevention and protection of information security.

Students who have completed their training in the discipline must acquire:

Basic knowledge of the processes of identifying, minimizing and eliminating threats to information security. This discipline contributes to building the ability to analyze, correct approach and understanding of security processes in general and in particular the protection of information security and has its place in the specialty "Cybersecurity of high technology".

Practical skills responding to the changing security environment and in particular the protection of information security, in line with the need for a new order of security policy priorities. It is necessary to include the full potential of society through the application of new forms of interaction between the individual, society and the state. Expanding the social scope of security policy in all its aspects poses new challenges to the majority of private and public sector employees, researchers and lawmakers.

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

- must have skills for thorough work and application of the regulatory framework guaranteeing the protection of information security;
- apply good practices for technological detection and prevention of information security incidents.

10. Mode of delivery:

The lectures are conducted in the classical way and the students get acquainted sequentially with the provided material. The statements are illustrated with examples that make the work of the students in the exercises as easy as possible. The lectures are richly illustrated with graphic material, which is presented through presentations with a multimedia projector and are complemented by examples, which are displayed on a whiteboard.

The practical exercises are conducted in the computer laboratories of the department, equipped with the necessary applications and devices, and simulation software.

11. Prerequisites:

Input links are the general knowledge acquired in secondary education and from the personal experience of each student, as well as from the technical disciplines taught in the previous semesters.

12. Course content:

The course emphasizes the nature and specifics of the theoretical foundations of information security protection, practical skills for identifying threats, risk management and management of the processes of creating an information security management system.

13. Bibliography

Basic literature:

1. Law on Protection of Classified Information.
2. Cyber Security Act.
3. Law on the Functioning and Protection of the National Security System.
4. Ordinance on the minimum requirements for network and information security.
5. 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
6. Biserov, Z., Cyberattacks and Information Warfare, report of the International Scientific Conference on "Modern Security and Modern Technologies", NBU, Sofia. March 2019
7. Denchev, St. Information and Security, S. 2019

Additional literature:

1. Biserov, Z. Security system of the administrative-territorial unit, Monograph, Military Publishing House, Sofia 2016
2. 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
3. Biserov, Z. Classification of modern threats to information security, report of the International Scientific Conference on "Broad Security", NBU, Sofia. March 2020. Proceedings.
4. Biserov, Z. Information - the main object of security, report of the Fifth International Scientific Conference TIEM 2020 of VUTP, Sofia. 2020
5. 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,
6. 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,
7. 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,
8. 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 – 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*