COURSE DESCRIPTION CARD - SYLLABUS

Course name
Security of Database Management Systems [S1Cybez1>BSZBD]

Course

Field of study Cybersecurity	Year/Semester 4/7
Area of study (specialization) –	Profile of study general academic
Level of study first-cycle	Course offered in Polish
Form of study full-time	Requirements elective

Number of hours

Lecture 16	Laboratory classes 30	Other 0
Tutorials 0	Projects/seminars 12	

Number of credit points

4,00

Coordinators

dr hab. inż. Mariusz Żal
mariusz.zal@put.poznan.pl

dr hab. inż. Sławomir Hanczewski
slawomir.hanczewski@put.poznan.pl

Lecturers

Prerequisites

• Knowledge of relational databases (RDBMS) and SQL language (SELECT, INSERT, UPDATE, DELETE, JOIN) • Basic database operations: table creation, indexing, primary and foreign keys • Familiarity with at least one database management system (e.g., MySQL, PostgreSQL, SQL Server, Oracle) • Knowledge of basic encryption algorithms (AES, RSA, SHA) • Authentication and authorization mechanisms for users in IT systems • Familiarity with Linux and Windows operating systems at the user level • Ability to work with the terminal (CLI) and basic commands for file and process management • User and permission management in operating systems

Course objective

The aim of the course "Security of Database Management Systems" is to provide students with knowledge and practical skills in protecting databases from threats and attacks. Students will learn to identify potential risks, implement security mechanisms, and respond to security incidents in database management systems (DBMS).

Course-related learning outcomes

Knowledge:
Knows authentication and authorization methods in DBMS [K1_W12]
Knows cryptographic algorithms used in database management systems [K1_W13]
Knows the types of attacks on database systems and the ways to prevent them [K1_W10]

Skills:
Is able to plan and conduct security tests of DBMS, collect necessary data, interpret them, and present conclusions [K1_U04]
When selecting security techniques for DBMS, is able to recognize their system and non-technical aspects, including ethical, economic, and legal considerations [K1_U07]

Social competences:
Understands the importance of enhancing professional, personal, and social competencies; is aware that knowledge and skills in the field of cybersecurity evolve rapidly [K1_K01]
Is aware of the significance of individual work and the necessity of adhering to professional ethics; is able to work in a team [K1_K05]

Methods for verifying learning outcomes and assessment criteria

Learning outcomes presented above are verified as follows:

Lecture: Knowledge gained during the lecture is assessed through an exam, conducted either in a written or an oral form. In the written exam, students must answer 7-10 questions (a combination of multiple-choice and open-ended), each carrying different point values. There are three or four separate scoring groups. In the case of the oral exam, a student draws one question from each scoring group. During the oral exam, for each drawn question, the student may be asked an additional follow-up question related to the one drawn. The grade for each question (including both the main and the follow-up question) reflects the scope of the answer and the depth of understanding of the topic. A set of 50-60 questions is prepared for each exam. To pass, a student must earn at least 50% of the total possible points.
Projects: Skills acquired through project work are assessed based on the projects presented. The evaluation considers the student’s engagement in project preparation, the tools used, and the additional knowledge the students had to acquire. Projects can be done individually or in pairs. The grading scale ranges from 2.0 to 5.0.
Laboratories: Skills gained in laboratory classes are assessed on an ongoing basis. In each lab session, the correctness of the completed exercises is graded on a scale of 0 to 10 points. To pass the lab component, a student must earn at least 50% of the total possible points.

Percentage of Points	Grade
<=50%	2,0
51% - 60%	3,0
61% - 70%	3,5
71% - 80%	4,0
81% - 90%	4,5
91% - 100%	5,0

Programme content

As part of the course, the student learns the principles of creating and managing secure database systems. They become familiar with the mechanisms that can be used for this purpose. Additionally, they gain an understanding of the tasks of a database management system administrator and the responsibilities associated with this role.

Course topics

1. Introduction to Database Security
2. Security Models and Access Policies
3. User Authentication and Authorization
4. Data Encryption and Protection
5. Audit and Monitoring of Database Activity

6. Threats and Attacks on Databases
7. Backups and Data Recovery
8. Cloud Security and NoSQL Databases
9. Legal Aspects and Data Protection Regulations
10. Practical Aspects of DBMS Security
11. Modern Technologies and Trends in DBMS Security
The laboratory topics are aligned with the lecture content.

Teaching methods

Lectures: Multimedia presentations illustrated with examples provided on the board.
Laboratory exercises: Practical exercises in groups, utilizing network devices and virtualized environments.

Bibliography

Basic:
1.Strengholt Piethein, Zarządzanie danymi w zbiorach o dużej skali. Nowoczesna architektura z siatką danych i technologią Data Fabric, Helion, 2024

Additional:
1. Diaz Christopher, Database Security: Problems and Solutions, Mercury Learning & Information, 2022.

Breakdown of average student's workload

	Hours	ECTS
Total workload	118	4,00
Classes requiring direct contact with the teacher	58	2,00
Student's own work (literature studies, preparation for laboratory classes/ tutorials, preparation for tests/exam, project preparation)	60	2,00