COURSE DESCRIPTION CARD - SYLLABUS

Course name
National information resources [S1Cybez1>KZI]

Course

Field of study
Cybersecurity

Year/Semester
2/3

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
0

Other
0

Tutorials
0

Projects/seminars
24

Number of credit points

3,00

Coordinators

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

prof. dr hab. inż. Mariusz Głąbowski
mariusz.glabowski@put.poznan.pl

dr Renata Dąbrowska
renata.dabrowska@put.poznan.pl

Lecturers

Prerequisites

• Basic knowledge of cybersecurity. • Familiarity with IT systems and fundamental concepts related to information security. • Ability to use tools for data analysis and operating system management (Linux, Windows).

Course objective

The aim of the course is to familiarize students with the concept of national information resources and their significance in the context of state cybersecurity. Students will gain knowledge about database systems managed by public administration authorities and special services, including their legal foundations, functionalities, and importance for national security. Special emphasis will be placed on information protection, data coordination between institutions, and incident response. The course combines theoretical elements with practical exercises focused on analysis, security design, and incident response related to national information resources.

Course-related learning outcomes

Knowledge:
• Understands fundamental concepts related to national information resources and their role in the state's cybersecurity system. [K1_W21]
• Recognizes the importance of critical infrastructure and key digital services for national security. [K1_W15]
• Is familiar with legal regulations concerning the protection of information resources in Poland, including the National Cybersecurity System Act (KSC), the NIS2 Directive, and regulations on classified information protection. [K1_W21]
• Understands the principles of operation of database systems managed by public administration authorities and special services. [K1_W21]
• Knows methods for securing data and information systems, as well as procedures for responding to cybersecurity incidents. [K1_W05]

Skills:
• Can identify key national information resources and assess their significance in the context of state security. [K1_U15]
• Is able to analyze and interpret legal regulations and standards related to the protection of information resources. [K1_U08]
• Can utilize tools for analyzing the security of information systems and risk assessment. [K1_U06]
• Is capable of designing basic security measures and incident response plans for national information resources. [K1_U07]
• Is aware of the necessity of planning and carrying out lifelong learning. [K1_U16]

Social competences:
• Understands the importance of protecting national information resources for national security. [K1_K05]
• Is aware of the ethical role in work related to the protection of public and sensitive information. [K1_K05]
• Is capable of making responsible decisions regarding risk management in the protection of information resources. [K1_K02]

Methods for verifying learning outcomes and assessment criteria

Learning outcomes presented above are verified as follows:

• Knowledge: A written test assessing familiarity with cultural models, professional ethics, and global technological challenges.
• Skills: Evaluation of a team project implementation and the prepared presentation of results, considering intercultural aspects.
In each form of the course assessment, the grade depends on the number of points the student earns relative to the maximum number of required points. Earning at least 50% of the possible points is a prerequisite for passing. The relationship between the grade and the number of points is defined by the Study Regulations. Additionally, the course completion rules and the exact passing thresholds will be communicated to students at the beginning of the semester through the university’s electronic systems and during the first class meeting (in each form of classes).

Programme content

Students participating in this course will gain knowledge about national information resources, their classification, and their significance for state cybersecurity. The course will cover the legal foundations

regulating data protection, including the National Cybersecurity System Act, NIS directives, and regulations concerning classified information protection.
Students will be introduced to selected database systems managed by public administration and special services, such as the National Criminal Information Center (Krajowe Centrum Informacji Kryminalnych - KCIK). The course will also address access to confidential and classified data, confidentiality clauses, and security clearance procedures issued by the Internal Security Agency (Agencja Bezpieczeństwa Wewnętrznego - ABW).
A strong emphasis will be placed on practical aspects of information protection, including security design, risk management, and incident response. Students will have the opportunity to explore coordination mechanisms for information management in Poland and analyze real-world cybersecurity incidents, evaluating the security measures and response strategies implemented.
The course will conclude with a team project, where participants will design a comprehensive security plan for a selected information resource.

Course topics

Lectures:
1. Introduction to Information and National Information Resources:
- Definition and significance of "information" in the context of national security.
- Information society - the role of information in the functioning of the state and its citizens.
- Classification of national information resources.
2. Legal Foundations of Information Resource Protection:
- National Cybersecurity System Act (KSC).
- NIS and NIS2 Directives and their impact on national regulations.
- GDPR (RODO) and regulations on classified information protection.
3. Database Systems of Public Administration and Special Services:
- Overview of selected database systems managed by public administration authorities (e.g., PESEL, CEIDG).
- Database systems of special and "police" services - National Criminal Information Center (KCIK), Police, and Border Guard systems.
4. Information Security and Data Protection:
- Data protection methods: encryption, authentication, access control.
- Organizational measures for information protection - procedures and best practices.
- Threats and common mistakes made by data administrators.
5. Access to Confidential and Classified Data:
- Principles of access to confidential and classified information.
- Confidentiality clauses in businesses and security requirements.
- Security clearances issued by the Internal Security Agency (ABW).
6. Information Coordination in Poland:
- Mechanisms for coordinating information between public administration and special services.
- Categories of processed information and their importance for national security.
- Strengths and weaknesses of the national information coordination system.
7. Risk Management and Incident Response:
- Risk assessment methods for information resources.
- Risk management process - identification, analysis, mitigation.
- Incident response procedures - role of CERT, CSIRT, SOC.
- Business Continuity Planning (BCP) and Disaster Recovery Planning (DRP).
8. Case Studies:
- Analysis of real-world incidents involving national information resources.
- Discussion on the effectiveness of security measures and incident response strategies.
Projects:
Students will complete team projects covering the following topics:
1. Developing a Security Plan for a Selected National Information Resource:
- Risk analysis, security design, incident response planning.
2. Cybersecurity Incident Simulation:
- Preparing an incident scenario, simulating an attack, and compiling a report on actions taken regarding information resources.
3. Review of Legal Regulations and Compliance Procedures:
- Analyzing existing laws and developing internal procedures for data protection and classified information management.

4. Analysis of National Information Resources:
- Preparing reports on selected aspects of national information resources.

Teaching methods

Lectures: Multimedia presentations with elements of discussion and case study analysis.
Team Projects: Implementation using IT tools.

Bibliography

Basic:
1. Ustawa o krajowym systemie cyberbezpieczeństwa, 2018 (z późniejszymi zmianami).
2. Dyrektywa Parlamentu Europejskiego i Rady (UE) 2016/1148 w sprawie bezpieczeństwa sieci i informacji (dyrektywa NIS).
3. ISO/IEC 27001:2013 - Systemy zarządzania bezpieczeństwem informacji.
4. NIST Special Publication 800-37 - Risk Management Framework for Information Systems and Organizations.

Additional:
1. Stallings, W. Network Security Essentials: Applications and Standards, Pearson, 2016.
2. Książki i raporty publikowane przez krajowe i międzynarodowe agencje ds. cyberbezpieczeństwa (np. CERT Polska, ENISA).
3. Materiały dostępne na stronach internetowych Narodowego Centrum Cyberbezpieczeństwa (NC Cyber).

Breakdown of average student's workload

	Hours	ECTS
Total workload	80	3,00
Classes requiring direct contact with the teacher	40	1,50
Student's own work (literature studies, preparation for laboratory classes/ tutorials, preparation for tests/exam, project preparation)	40	1,50