COURSE DESCRIPTION CARD - SYLLABUS

Course name
Security management in IT systems [N2Inf1-ZTI>ZBIT]

Course

Field of study
Computing

Year/Semester
1/2

Area of study (specialization)
Advanced Internet Technologies

Profile of study
general academic

Level of study
second-cycle

Course offered in
Polish

Form of study
part-time

Requirements
elective

Number of hours

Lecture
16

Laboratory classes
16

Other
0

Tutorials
0

Projects/seminars
0

Number of credit points

4,00

Coordinators

dr inż. Michał Apolinarski
michal.apolinarski@put.poznan.pl

Lecturers

Prerequisites

The student starting this subject should have knowledge of computer system architecture, operating systems operating principles, computer networks and data protection mechanisms. Should be able to obtain information from literature, databases and other sources and integrate the information obtained, interpret it, as well as draw conclusions and formulate and substantiate opinions.

Course objective

Students will become familiar with the design of ICT security management systems in a modern company, i.e. based on norms and standards, conducting risk analysis, audits (including penetration tests) and proposing the appropriate selection of security measures and methods for responding to incidents.

Course-related learning outcomes

Knowledge:
The student has detailed knowledge about:
- what criteria should be met by a secure IT system, how to assess the security of a given IT system and how to manage a specific level of security,
- how to carry out a risk analysis in an IT system (according to various methodologies),

- how to choose security masures in an IT system to achieve a particular level of security,
- how to conduct penetration tests and what tools to use,
- how to formulate a security policy for an example company.

Skills:
The student can:
- carry out a risk analysis according to selected methodology (classify IT system assets, assess potential threats and whether the IT system is susceptible to these threats),
- analyze and estimate the level of security of the security mechanisms used,
- propose and design a security policy for the entire IT system.

Social competences:
Student understands:
- how important is the use of appropriate security and protection methods (physical, cryptographic, organizational-administrative and legal),
- how important it is to apply security standards and norms,
- it is necessary to update ones knowledge in the field of security and is aware of the importance and understands the non-technical aspects and effects of IT engineer activities and the related responsibility for decisions.

Methods for verifying learning outcomes and assessment criteria

Learning outcomes presented above are verified as follows:

Learning outcomes presented above are verified as follows:
Knowledge acquired during the course is verified during a written 45-minute exam, consisting of 8 questions. Passing threshold: over 50% of points. Topics, which are the basis for final exam questions, are sent to students by e-mail at the beginning of the semester.
Skills acquired as part of the project classes are verified on an ongoing basis during the classes (when discussing the next stages and parts of the project and implementation) and by making a final assessment of the project and implementation and its documentation by the teacher.

Programme content

Course content:
1. Introduction to Information Security
2. Risk Management. Legal and Regulatory requirements.
3. Stages of the Risk Management Process
4. Risk Assessment Methods
5. Threats and Threat Modeling
6. Operational Security Management of Systems
7. Implementation of IT Systems

Course topics

Lecture
1. Introduction - the definition of what it means that the IT system is a safe and reliable system, how to assess security, relationships between security elements, standards, measures, norms and best practices (TCSEC, ITSEC, ISO, CC).
2. Classification of threats, both network, cryptographic and computer systems expoits. Determining the degree of systems" vulnerability (quantitative and qualitative methods).
3. Risk analysis and management. Defining and discussing ways to achieve and maintain the assumed level of confidentiality, integrity, availability, accountability, authenticity and reliability. Selection of appropriate precautionary measures. Examples of risk management processes in a company in a specific IT system.
4. Security policy - sample documents included in a security policy.
5. Audit - an example of an implementation of a security management system (COBIT, MARION, TISM, OSSTM, LP-A).
6. Penetration tests - techniques and selection of appropriate tools for conducting penetration tests.
7. Design and operation of secure systems based on standards and recommendations. Designing integrated security management systems based on knowledge from previous courses on protection

mechanisms.
Lab practicals
Development of the design and documentation of a security management system in a selected IT environment, including inventory of IT resources, type of data processed (system analysis in terms of UODO requirements); threat analysis and assessment of the system"s vulnerability to these threats, proposing security mechanisms that minimize the risk; post-implementation analysis; project cost estimate. Development of documentation for the security policy of the system under analysis.

Teaching methods

The lecture is conducted in an interactive way (with formulating questions for students) using multimedia presentations. Electronic version of course materials are made available to students.

The laboratory class is conducted in the form of consultations and verification of subsequent design stages. Tasks are carried out in teams.

Bibliography

Basic
Białas A., Bezpieczeństwo informacji i usług w nowoczesnej instytucji i firmie, WNT, Warszawa 2017 (sygnatura w Bibliotece PP W 113481)
Pieprzyk J., Hardjono T., Seberry J., Teoria bezpieczeństwa systemów komputerowych, Helion, 2003 (sygnatura w Bibliotece PP W 110215)
Księżopolski B., Szałachowski P., Audyt bezpieczeństwa systemów IT - ścieżka techniczna (rekonesans i skanowanie), Wyd. Uniwersytetu Marii Curie-Skłodowskiej, Lublin 2011 (sygnatura w Bilbiotece PP A 174729)
Additional
ISO Norms (13335, 2700x) (in the reading room of the PP library)
Weidman G., Bezpieczny system w praktyce. Wyższa szkoła hackingu i testy penetracyjne, Helion 2014. (reference number in PP library: W 155592)

Breakdown of average student's workload

	Hours	ECTS
Total workload	100	4,00
Classes requiring direct contact with the teacher	32	1,50
Student's own work (literature studies, preparation for laboratory classes/ tutorials, preparation for tests/exam, project preparation)	68	2,50