COURSE DESCRIPTION CARD - SYLLABUS

Course name
Security of ICT Systems [S1Teleinf1>BSI]

Course

Field of study
Teleinformatics

Year/Semester
3/6

Area of study (specialization)
–

Profile of study
general academic

Level of study
first-cycle

Course offered in
Polish

Form of study
full-time

Requirements
compulsory

Number of hours

Lecture
15

Laboratory classes
30

Other
0

Tutorials
0

Projects/seminars
0

Number of credit points

3,00

Coordinators

prof. dr hab. inż. Mieczysław Jessa
mieczyslaw.jessa@put.poznan.pl

Lecturers

Prerequisites

A student starting this subject should have basic systematized knowledge about the operation of ICT networks and the ability to obtain information from literature, databases and other sources in Polish or English.

Course objective

The aim of teaching the subject is to provide students with knowledge about security attributes, basic threats to data transmitted and processed in an ICT system, about administrative methods of data protection, international standards for data security and knowledge and about cryptographic methods of data protection.

Course-related learning outcomes

Knowledge:
1. Has knowledge of security attributes, threats to data sent and processed in the ICT system.
2. Knows basic international standards for data security, risk analysis methods, risk management methods and data security management methods.
3. Knows the basic concepts of cryptography, has knowledge of cryptographic methods of data

protection, understands the importance of cryptography to ensure the security of data transmitted in ICT networks and collected in databases.

Skills:
1. Can predict the consequences of the lack of security of data sent and collected in the ICT system.
2. Knows how to work in a group on solving the problem of data protection and ICT network against unauthorized access or modification.

Social competences:
1. It shall be ready to acquire new knowledge necessary to ensure the security of ICT systems.
2. Has a sense of responsibility for the security of the designed ICT systems and is aware of the potential dangers for other people or society of their inadequate security.

Methods for verifying learning outcomes and assessment criteria

Learning outcomes presented above are verified as follows:

The knowledge acquired as part of the lecture is verified on the basis of a written credit, consisting of 5 open questions, identically scored. The passing threshold is 50% of the points. The distribution of thresholds for grades 2 to 5 is even. A set of questions is drawn individually from a set of issues. Credit issues, on the basis of which open questions are developed, are sent to students by e-mail using university e-mail. The assessment from the laboratory is the arithmetic average of the assessments from the three implemented implementations supplemented by reports from the conducted tests.

Programme content

The lecture program is divided into three parts. In the first part, students will learn the basic requirements for ICT systems, security attributes, threat classification, threat categories, threats characteristic of wired and wireless ICT networks. The second part is devoted to administrative methods of data protection. Students will learn about the three-level reference model, basic norms and standards in the area of security, risk definition, qualitative, quantitative, deductive and inductive risk analysis methods, learn risk management methods, methods of managing the security of ICT
systems, including the PDCA scheme and the principles of conducting an ICT security audit. Part Three deals with cryptographic methods of data protection. Students will learn the basic concepts of cryptography such as symmetric, asymmetric, hybrid cryptographic system, unconditional,
computational, provable security, Kerckhoffs postulate, block cipher, stream cipher, learn about the modes of operation (use) of block ciphers (ECB, CBC, CFB, OFB, CTR), get acquainted with the concept and construction of a stream cipher, one-time-pad cipher, with examples of block and stream ciphers,
with an encryption scheme with an RSA public key, Rabin, ElGamal ciphers, learns about the advantages and weaknesses of symmetric (with a secret key) and asymmetric (with a public key) encryption methods, learns the concept and basic properties of the hash function, learns about the
methods of attack against the hash function (dictionary attack and attack using the birthday paradox), learns examples of the use of cryptographic methods in ICT.
The laboratory includes the implementation in a real environment of sample methods of encryption and attacks , random number generation, production of a secure pseudorandom numbers and evaluation of the properties of the output bit streams using statistical tests (distinguishing attack implementation).

Course topics

The lecture program is divided into three parts. In the first part, students will learn the basic requirements for ICT systems, security attributes, threat classification, threat categories, threats characteristic of wired and wireless ICT networks. The second part is devoted to administrative methods of data protection. Students will learn about the three-level reference model, basic norms and standards in the area of security, risk definition, qualitative, quantitative, deductive and inductive risk analysis methods, learn risk management methods, methods of managing the security of ICT
systems, including the PDCA scheme and the principles of conducting an ICT security audit. Part Three deals with cryptographic methods of data protection. Students will learn the basic concepts of cryptography such as symmetric, asymmetric, hybrid cryptographic system, unconditional,
computational, provable security, Kerckhoffs postulate, block cipher, stream cipher, learn about the modes of operation (use) of block ciphers (ECB, CBC, CFB, OFB, CTR), get acquainted with the concept and construction of a stream cipher, one-time-pad cipher, with examples of block and stream ciphers,

with an encryption scheme with an RSA public key, Rabin, ElGamal ciphers, learns about the advantages and weaknesses of symmetric (with a secret key) and asymmetric (with a public key) encryption methods, learns the concept and basic properties of the hash function, learns about the
methods of attack against the hash function (dictionary attack and attack using the birthday paradox), learns examples of the use of cryptographic methods in ICT.
The laboratory includes the implementation in a real environment of sample methods of encryption and attacks , random number generation, production of a secure pseudorandom numbers and evaluation of the properties of the output bit streams using statistical tests (distinguishing attack implementation).

Teaching methods

1. Lecture: a multimedia presentation, illustrated with examples given on the board.
2. Laboratory: classic problem.

Bibliography

Basic:
1. A. Białas, Bezpieczeństwo informacji i usług w nowoczesnej instytucji i firmie, WNT, Warszawa, 2007.
2. K. Liderman, Analiza ryzyka i ochrona informacji w systemach komputerowych, PWN, Warszawa, 2008.
3. K. Liderman, Bezpieczeństwo informacyjne, nowe wyzwania, PWN, 2017.
4. A. J. Menezes, P. C. van Oorschot, S. A. Vanstone „Kryptografia stosowana”, WNT, Warszawa 2005.
5. B. Schneier „Kryptografia dla praktyków”, WNT, Warszawa, 2002.
6. W. Stallings „Kryptografia i bezpieczeństwo sieci komputerowych”, Wyd. V, Helion 2012.

Additional:
1. R. Andersson, Inżynieria zabezpieczeń, WNT, 2005.
2. J. Stokłosa, T. Bilski, T. Pankowski, Bezpieczeństwo danych w systemach informacyjnych, PWN, 2001.
3. J. A. Buchmann „Wprowadzenie do kryptografii”, PWN, 2006.
4. M. Karbowski, Podstawy kryptografii, Helion, 2014.
5. M. Kutyłowski, W-B. Strothmann „Kryptografia, teoria i praktyka zabezpieczania systemów komputerowych”, Read Me, Warszawa, 1999.
6. N. Ferguson, B. Schneier „Kryptografia w praktyce”, Helion, 2004.

Breakdown of average student's workload

	Hours	ECTS
Total workload	90	3,00
Classes requiring direct contact with the teacher	49	2,00
Student's own work (literature studies, preparation for laboratory classes/ tutorials, preparation for tests/exam, project preparation)	41	1,00