STUDY MODULE DESCRIPTION FORM

Name of the module/subject	Code
Security management in information systems	**1010331571010334974**

Field of study	Profile of study (general academic, practical)	Year /Semester
Information Engineering	**(brak)**	**4 / 7**

Elective path/specialty	Subject offered in:	Course (compulsory, elective)
Security of Information Technology (IT)	**Polish**	**obligatory**

Cycle of study:	Form of study (full-time, part-time)
First-cycle studies	**full-time**

No. of hours

Lecture: **30**	Classes: **-**	Laboratory: **-**	Project/seminars: **15**	No. of credits **5**

Status of the course in the study program (Basic, major, other)	(university-wide, from another field)
(brak)	**(brak)**

Education areas and fields of science and art	ECTS distribution (number and %)
technical sciences	**5 100%**

Responsible for subject / lecturer:

dr inż. Anna Grocholewska-Czuryło
email: anna.grocholewska-czurylo@put.poznan.pl
tel. 61-665 35 31
Faculty of Electrical Engineering
ul. Piotrowo 3A 60-965 Poznań

Prerequisites in terms of knowledge, skills and social competencies:

1	**Knowledge**	K_W01:Has basic knowledge in the area of mathematics covering algebra, analysis, logic, probabilistic and elements of discreet and applied mathematics.
		K_W15:Has structured knowledge based on a theoretical foundation in the area of teleinformatics, protocols and services in telecommunication networks.
2	**Skills**	K_U01: Is able to search for information in literature, databases and other sources; is able to integrate acquired information, interpret it, draw conclusions and formulate and argument opinions.
		K_U02:Is able to work alone or in a team; is able to estimate the time needed to complete the assigned project; is able to develop and carry out a schedule ensuring that deadlines are met.
3	**Social competencies**	K_K02: Is aware of the importance and understands non-technical aspects and effects of computer science engineer performance and associated responsibility for the decisions taken.

Assumptions and objectives of the course:

As part of the course students will be familiarized with teleinformatics security management system design in a modern company, so carrying out a risk analysis and proposing suitable security measures and incident prevention based on norms and standards.

Study outcomes and reference to the educational results for a field of study

Knowledge:

1. Has structured knowledge based on a theoretical foundation in the area of data protection and information systems security. - [K_W13]

2. Have basic knowledge of administering IT systems. - [K_W14]

Skills:

1. Is able to apply appropriate data protection methods and ensure security of the information system. - [K_U17]

2. Is able to prepare documentation on engineering task realization and is able to prepare a paper describing the results of the realized task. - [K_U03]

Social competencies:

1. Is aware of the importance and understands non-technical aspects and effects of computer science engineer performance and associated responsibility for the decisions taken. - [K_K02]

Assessment methods of study outcomes

Written or/and oral examination based on lecture and project.

Course description

Threats classification of network, cryptographic and operational threats. Risk analysis and management. Defining and discussing methods of reachning and maintaining a complex level of confidentiality, integrity, accessibility, accountability, authenticity and relibility, based on norms and project guidelines, and operation of such systems. Designing integrated security management systems based on the knowledge of preceding courses on protection mechanisms. During the course students will design components of security management system.

Project (update 2017):

Developing a security management system in a chosen environment. Project and documentation should include inventory of IT resources, type of data being processed (GIODO system analysis), risk analysis, selection of security solutions, action against security breaches (confidentiality, integrity, availability).

Applied methods of education:

- work in teams of up to 2 people,

- a cyclical presentation of work progress,

- discussions on proposed solutions in the whole group and individually with the team

Basic bibliography:

1. Bezpieczeństwo informacji i usług w nowoczesnej instytucji i firmie, Białas A., WNT, Warszawa 2006

2. Teoria bezpieczeństwa systemów komputerowych, Pieprzyk J., Hardjono T., Seberry J., Helion, 2003

Additional bibliography:

1. Normy ISO (13335, 2700x)

2. Bezpieczny system w praktyce. Wyższa szkoła hackingu i testy penetracyjne, Weidman G., Helion 2014.

Result of average student's workload

Activity	Time (working hours)
1. Participation in lectures	30
2. Participation in project	15
3. Peparation for the exam	30
4. Preparation for the project	30
5. Exam	2
6. Consultations	13

Student's workload

Source of workload	hours	ECTS
Total workload	120	5
Contact hours	60	3
Practical activities	45	2