Załącznik nr 2 do Zarządzenia Nr 915 z 2019 r. Rektora PB

COURSE DESCRIPTION CARD

<table>
<tr><td colspan="10">Faculty of Electrical Engineering</td></tr>
<tr><td>Field of study</td><td colspan="6">Electrical and Electronics Engineering</td><td>Degree level and programme type</td><td>bachelor's degree</td></tr>
<tr><td>Specialization/ diploma path</td><td colspan="6">-</td><td>Study profile</td><td>-</td></tr>
<tr><td rowspan="2">Course name</td><td colspan="6" rowspan="2">Security and Reliability of Network Systems</td><td>Course code</td><td>IS-FEE-10035S</td></tr>
<tr><td>Course type</td><td>elective</td></tr>
<tr><td rowspan="2">Forms and number of hours of tuition</td><td>L</td><td>C</td><td>LC</td><td>P</td><td>SW</td><td>FW</td><td>S</td><td>Semester</td><td>summer</td></tr>
<tr><td>30</td><td></td><td></td><td></td><td>15</td><td></td><td></td><td>No. of ECTS credits</td><td>4</td></tr>
<tr><td>Entry requirements</td><td colspan="9">-</td></tr>
<tr><td>Course objectives</td><td colspan="9">Acquiring knowledge of methods and techniques used to provide secure access, transmission and storage of information.</td></tr>
<tr><td>Course content</td><td colspan="9">Fundamentals of cryptography. Conditions of providing data confidentiality and integrity. Symmetric and asymmetric cipher algorithms e.g. DES, RSA. Hash functions. Digital signatures. Idea of Public Key Infrastructure (PKI). Sources and types of security threats to network systems. Security threats to host and server applications. Security threats to web applications. Methods of protection against selected kinds of threats. Firewall systems, antivirus protection, intrusion detection systems (IDS), idea of honeypots. Methods of authentication and authorization in network systems. Conception of security politics. Examples of complex security politics. Security audit and penetration tests. Systems for data backuping and restoring. Array of disks (RAID). Network storage systems: Storage Area Network (SAN), Network Area Storage (NAS).</td></tr>
<tr><td>Teaching methods</td><td colspan="9">lecture, specialization workshop.</td></tr>
<tr><td>Assessment method</td><td colspan="9">lecture: tests;
specialization workshop: evaluating the student's performance in classes, presentation on given subject.</td></tr>
<tr><td>Symbol of learning outcome</td><td colspan="7">Learning outcomes</td><td colspan="2">Reference to the learning outcomes for the field of study</td></tr>
<tr><td>LO1</td><td colspan="7">explains features, types, and applications of encryption algorithms and hash functions and distinguishing their functionalities;</td><td colspan="2"></td></tr>
<tr><td>LO2</td><td colspan="7">describes technologies used for providing secure users and devices authentication in network systems;</td><td colspan="2"></td></tr>
<tr><td>LO3</td><td colspan="7">characterizes methods of providing information confidentiality and integrity;</td><td colspan="2"></td></tr>
<tr><td>LO4</td><td colspan="7">depicts technologies used in information systems to provide secure and reliable data storage;</td><td colspan="2"></td></tr>
<tr><td>LO5</td><td colspan="7">identifies and characterizes sources and types of threats to network systems</td><td colspan="2"></td></tr>
<tr><td>LO6</td><td colspan="7">setts up simple networks, configuring network settings in PC workstations and in choosing the proper means that can be used to protect data systems against the particular threats and explains their features;</td><td colspan="2"></td></tr>
</table>

LO7	prepares multimedia presentation on given subject connected with module content.	
Symbol of learning outcome	**Methods of assessing the learning outcomes**	**Type of tuition during which the outcome is assessed**
LO1	tests on lecture content, evaluating the student's performance in classes	**L, SW**
LO2	tests on lecture content, evaluating the student's performance in classes	**L, SW**
LO3	tests on lecture content, evaluating the student's performance in classes	**L, SW**
LO4	tests on lecture content	**L**
LO5	tests on lecture content	**L**
LO6	tests on lecture content	**L**
LO7	evaluating the student's presentations	**SW**
Student workload (in hours)		**No. of hours**
Calculation	**attending the class sessions**	**45**
	preparation for specialization worshop	**15**
	work on presentations	**20**
	preparation for and participation in exams/tests	**20**
	TOTAL:	**100**

Quantitative indicators	**HOURS**	**No. of ECTS credits**
Student workload – activities that require direct teacher participation	**45**	**1,5**
Student workload – practical activities	**50**	**2**

Basic references	**1. Stallings W.: Cryptography and network security: principles and practice. Prentice Hall, 2010.** **2. Anderson R. J.: Security engineering: a guide to building dependable distributed systems. Wiley, 2008.** **3. Cole E., Krutz R. L., Conley J.: Network security bible. J. Wiley & Sons, 2005**
Supplementary references	**1. Chestwick W. R., Bellovin S. M., Rubin A. D.: Firewalls and internet security. Addison Wesley, 2003.** **2. Pipkin D. L.: Information security: protecting the global enterprise. Prentice Hall PTR, 2000.**

Organisational unit conducting the course	**Department of Photonics, Electronics and Lighting Technology**	**Date of issuing the programme**
Author of the programme	**Andrzej Zankiewicz, Ph.D. Eng.**	**26.01.2020**

L – lecture, C – classes, LC – laboratory classes, P – project, SW – specialization workshop, FW - field work, S – seminar