GDAŃSK UNIVERSITY OF TECHNOLOGY

Subject card

| | | | |
|---|---|---|---|
| Subject name and code | Cybersecurity Basics, PG_00068775 | | |
| Field of study | Biomedical Engineering, Biomedical Engineering, Biomedical Engineering | | |
| Date of commencement of studies | February 2027 | Academic year of realisation of subject | 2027/2028 |
| Education level | second-cycle studies | Subject group | Optional subject group<br>Specialty subject group<br>Subject group related to scientific research in the field of study |
| Mode of study | Full-time studies | Mode of delivery | at the university |
| Year of study | 1 | Language of instruction | Polish |
| Semester of study | 2 | ECTS credits | 2.0 |
| Learning profile | general academic profile | Assessment form | exam |
| Conducting unit | Department of Computer Communications -> Faculty of Electronics Telecommunications and Informatics -> Faculties of Gdańsk University of Technology | | |
| Name and surname of lecturer (lecturers) | Subject supervisor | dr inż. Wojciech Gumiński | |
| | Teachers | dr inż. Wojciech Gumiński | |

**Lesson types**

| Lesson type | Lecture | Tutorial | Laboratory | Project | Seminar | SUM |
|---|---|---|---|---|---|---|
| Number of study hours | 15.0 | 0.0 | 15.0 | 0.0 | 0.0 | 30 |

E-learning hours included: 0.0

**Learning activity and number of study hours**

| Learning activity | Participation in didactic classes included in study plan | Participation in consultation hours | Self-study | SUM |
|---|---|---|---|---|
| Number of study hours | 30 | 3.0 | 17.0 | 50 |

**Subject objectives**

The main objective of the Cybersecurity Fundamentals course is to provide knowledge and skills in the field of protecting systems, networks and data from threats in cyberspace. The subject is to help understand threats, security principles and ways to prevent digital attacks.

**Learning outcomes**

| Course outcome | Subject outcome | Method of verification |
|---|---|---|
| [K7_W04] knows and understands, to an increased extent, the principles, methods and techniques of programming and the principles of computer software development or programming devices or controllers using microprocessors or other elements or programmable devices specific to the field of study, and organization of work of systems using computers or such devices | Student lists and describes security attributes. Student describes the differences between symmetric and asymmetric cryptography algorithms and can provide examples of their applications. | [SW1] Assessment of factual knowledge |
| [K7_U04] can apply knowledge of programming methods and techniques as well as select and apply appropriate programming methods and tools in computer software development or programming devices or controllers using microprocessors or programmable elements or systems specific to the field of study, making assessment and critical analysis of the prepared software as well as a synthesis and creative interpretation of information presented with it | The student is able to practically implement the learned security solutions in specific use scenarios. | [SU1] Assessment of task fulfilment<br>[SU5] Assessment of ability to present the results of task |

<table>
<tr><td>Subject contents</td><td>Course content – lecture<br>Lectures:<br>1. Introduction to Cybersecurity<br>2. Security Attributes<br>3. Basic Types of Threats<br>4. Legal Aspects of Cybersecurity<br>5. Basics of Cryptography<br>6. Symmetric and Asymmetric Cryptographic Algorithms<br>7. Practical Applications of Cryptographic Methods<br>8. Document Encryption and Digital Signatures<br>9. Public Key Infrastructure PKI and Its Applications<br>10. Security of Information Systems<br>11. Authentication and Authorization<br>12. Remote Access Security<br>13. Reliability and Continuity of Operation<br>14. Monitoring Systems<br>15. Analysis of Sample Use Cases<br>Laboratories:<br>1. Keys, Certificates and PKI<br>2. Encryption, Digital Signatures and PGP<br>3. Authentication and Encryption in Web Applications<br>4. Firewall<br>5. IDS/IPS Systems<br>6. Secure Remote Access VPN<br>7. System Monitoring and Event Log Analysis</td></tr>
<tr><td>Prerequisites and co-requisites</td><td></td></tr>
<tr><td>Assessment methods and criteria</td><td><table><tr><th>Subject passing criteria</th><th>Passing threshold</th><th>Percentage of the final grade</th></tr><tr><td>Laboratories</td><td>50.0%</td><td>50.0%</td></tr><tr><td>Exam</td><td>50.0%</td><td>50.0%</td></tr></table></td></tr>
<tr><td>Recommended reading</td><td><table><tr><td>Basic literature</td><td>Cybersecurity Essentials: Practical Tools for Today's Digital Defenders; Cochran Kodi A; 2024; Berkeley, CA: Apress L. P.<br>The Cyber Security Handbook Prepare for, respond to and recover from cyber attacks; Calder Alan, Perring Stephen; 2020; Ely: IT Governance Publishing<br>Cybersecurity for Dummies; Steinberg Joseph; 2025; Newark: John Wiley & Sons, Incorporated<br>Cyberbezpieczeństwo dla bystrzaków; Joseph Steinberg ; przekład: Grzegorz Werner; 2023; Gliwice : Helion<br>Cyberbezpieczeństwo w Polsce i na świecie; Katarzyna Chałubińska-Jentkiewicz, Agnieszka Brzostek, Waldemar Kitler, Katarzyna Badźmirowska-Masłowska; 2024; Towarzystwo Wiedzy Obronnej</td></tr><tr><td>Supplementary literature</td><td>Cybersecurity for eHealth: A Simplified Guide to Practical Cybersecurity for Non-Technical Healthcare Stakeholders & Practitioners; Ogu, Emmanuel C; 2021; United States: CRC Press<br>Cyberbezpieczeństwo w placówce medycznej; Piotr Glen, Michał Grabiec, Piotr Janiszewski, Agnieszka Kręcisz-Sarna, Przemysław Kucharzewski, Maciej Lipka, Michał Nosowski, Marzena Pytlarz-Pietraszko, Marcin Sarna, Jowita Sobczak; 2022; Warszawa: Wiedza i Praktyka sp. z o.o.<br>Boardroom Cybersecurity: A Director's Guide to Mastering Cybersecurity Fundamentals; Weis, Dan; 2024; Berkeley, CA: Apress L. P.</td></tr><tr><td>eResources addresses</td><td></td></tr></table></td></tr>
<tr><td>Example issues/ example questions/ tasks being completed</td><td>generating and verifying certificates; creating and verifying digital signatures; configuring the firewall and IDS/IPS systems; document encryption; practical use of Public Key Infrastructure.</td></tr>
<tr><td>Practical activites within the subject</td><td>Not applicable</td></tr>
</table>

Document generated electronically. Does not require a seal or signature.