



Subject card

|   |   |  |          |                                     |  |   |     |
|---|---|--|----------|-------------------------------------|--|---|-----|
| Subject name and code                       | Cybersecurity, PG_00062743  |  |          |                                     |  |   |     |
| Field of study                              | Technologies for Industry 5.0   |  |          |                                     |  |   |     |
| Date of commencement of studies             | October 2026  | Academic year of realisation of subject  |          |                                     |  | 2028/2029   |     |
| Education level                             | first-cycle studies   | Subject group  |          |                                     |  | Obligatory subject group in the field of study<br>Humanistic-social subject group |     |
| Mode of study                               | Full-time studies   | Mode of delivery   |          |                                     |  | at the university   |     |
| Year of study                               | 3   | Language of instruction  |          |                                     |  | Polish  |     |
| Semester of study                           | 6   | ECTS credits   |          |                                     |  | 2.0   |     |
| Learning profile                            | general academic profile  | Assessment form  |          |                                     |  | assessment  |     |
| 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 hab. inż. Jacek Rak   |          |                                     |  |   |     |
|   | Teachers  |  |          |                                     |  |   |     |
| Lesson types                                | Lesson type   | Lecture  | Tutorial | Laboratory                          | Project  | Seminar   | SUM |
|   | Number of study hours   | 15.0   | 0.0      | 0.0                                 | 0.0  | 15.0  | 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   |          | 2.0                                 |  | 18.0  | 50  |
| Subject objectives                          | The aim is to familiarize students with the basics of cybersecurity. The course includes a discussion of, among others, the following issues: security threats, in particular in the context of using Internet resources; types of attacks: learning/modifying content, impersonation, targeted and untargeted attacks, malware, botnet networks; analysis of security attributes such as confidentiality, authenticity, availability, data integrity, or non-repudiation and mechanisms for ensuring them; security policy; good security practices. |  |          |                                     |  |   |     |
| Learning outcomes                           | Course outcome  | Subject outcome  |          |                                     | Method of verification   |   |     |
|   | [K6_W04] demonstrates knowledge necessary to understand non-technical (legal, economic, ethical, environmental) conditions of engineering activities in the scope directly or indirectly related to the industrial revolution   | The student understands security threats, characterizes the major types of attacks, and knows security measures suitable for IT systems. |          |                                     | [SW3] Assessment of knowledge contained in written work and projects |   |     |
|   | [K6_U04] has the ability to perceive and take into account non-technical aspects (legal, economic, ethical, environmental, human factor and others) of engineering problems and tasks and create solutions that take them into account  | The student can propose security measures, taking threats to the network and systems environment into consideration.                     |          |                                     | [SU5] Assessment of ability to present the results of task           |   |     |
|   | [K6_W71] has general knowledge in humanistic, social, economic or legal sciences  | The student understands the importance of security policy as an essential security factor for the IT system.                             |          |                                     | [SW3] Assessment of knowledge contained in written work and projects |   |     |
|   | [K6_U71] is able to apply knowledge from humanistic, social, economic or legal sciences in order to solve problems in a social environment  | The student can propose security measures taking into consideration the specifics of the network and systems environment.                |          |                                     | [SU1] Assessment of task fulfilment                                  |   |     |

| Subject contents                | <p>Course content – lecture</p> <ol style="list-style-type: none"> <li>1. Network System Security Threats</li> <li>2. Security Attributes</li> <li>3. Attack Categories and Techniques</li> <li>4. Malware</li> <li>5. Botnets</li> <li>6. Firewall Types</li> <li>7. Firewall Configurations</li> <li>8. Access Control Systems</li> <li>9. Intrusion Detection Systems</li> <li>10. Virtual Private Networks (VPN)</li> <li>11. Security Policy</li> <li>12. Good Security Practices</li> <li>13. Maintaining the Security Level</li> <li>14. Security Level Assessment</li> <li>15. Audit</li> </ol> |  |  |                          |                   |                               |         |       |       |              |       |       |
|---------------------------------|---|--|--|--------------------------|-------------------|-------------------------------|---------|-------|-------|--------------|-------|-------|
| Prerequisites and co-requisites |   |  |  |                          |                   |                               |         |       |       |              |       |       |
| Assessment methods and criteria | <table border="1"> <thead> <tr> <th data-bbox="454 1377 794 1406">Subject passing criteria</th> <th data-bbox="799 1377 1139 1406">Passing threshold</th> <th data-bbox="1144 1377 1482 1406">Percentage of the final grade</th> </tr> </thead> <tbody> <tr> <td data-bbox="454 1413 794 1442">seminar</td> <td data-bbox="799 1413 1139 1442">50.0%</td> <td data-bbox="1144 1413 1482 1442">50.0%</td> </tr> <tr> <td data-bbox="454 1449 794 1478">written test</td> <td data-bbox="799 1449 1139 1478">50.0%</td> <td data-bbox="1144 1449 1482 1478">50.0%</td> </tr> </tbody> </table>            |  |  | Subject passing criteria | Passing threshold | Percentage of the final grade | seminar | 50.0% | 50.0% | written test | 50.0% | 50.0% |
| Subject passing criteria        | Passing threshold   | Percentage of the final grade  |  |                          |                   |                               |         |       |       |              |       |       |
| seminar                         | 50.0%   | 50.0%  |  |                          |                   |                               |         |       |       |              |       |       |
| written test                    | 50.0%   | 50.0%  |  |                          |                   |                               |         |       |       |              |       |       |
| Recommended reading             | <p>Basic literature</p>   | <ol style="list-style-type: none"> <li>1. Materiały wykładowe</li> <li>2. A. Białas: Bezpieczeństwo informacji i usług w nowoczesnej instytucji i firmie. WNT (2007)</li> <li>3. S. Enoka: Cyberbezpieczeństwo w małych sieciach. Helion (2024)</li> </ol>   |  |                          |                   |                               |         |       |       |              |       |       |
|                                 | <p>Supplementary literature</p>   | <p>J. Rak: Resilient Routing in Communication Networks A Systems Perspective, 2<sup>nd</sup> Edition. Springer (2024)<br/> K. Liderman: Analiza ryzyka i ochrona informacji w systemach komputerowych. PWN (2008)</p> <p>K. Liderman: Podręcznik administratora bezpieczeństwa teleinformatycznego. Mikom (2003)</p> |  |                          |                   |                               |         |       |       |              |       |       |
|                                 | eResources addresses  |  |  |                          |                   |                               |         |       |       |              |       |       |

|  |   |
|--|---|
| Example issues/<br>example questions/<br>tasks being completed | During the seminar, students, in groups of two, prepare and present their study of a selected topic in the area of cybersecurity. |
| Practical activities within<br>the subject                     | Not applicable  |

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