#### card of course

|  |  |
| --- | --- |
| Subject name | * + - 1. **Security of IT systems**
 |

**1. The placement of the subject in the study system**

|  |  |
| --- | --- |
| 1.1. Field of study | **Computer science** |
| 1.2. Form and path of study | **Full-time/Part-time** |
| 1.3. Level of education | **First-cycle studies** |
| 1.4. Study profile | **Practical** |

|  |  |
| --- | --- |
| 1.5. Specialty | **-** |
| 1.6. Subject Coordinator | **Dr Karol Kuczyński** |

**2. General characteristics of the subject**

|  |  |
| --- | --- |
| 2.1. Belonging to a subject group | **Directional** |
| 2.2. Number of ECTS | **1** |
| 2.3. Language of lectures | **English** |
| 2.4. Semesters in which the subject is taught | **IV** |
| 2.5.Criteria for selecting course participants | **-** |

1. **Learning outcomes and course delivery**
	1. **Subject Objectives**

|  |  |
| --- | --- |
| **No.** | **Subject Objectives** |
|
| C1 | Familiarization with the main problems of IT systems security. |
| C2 | Familiarization with methods of detecting and preventing security problems in IT systems. |
| C3 | Mastering the principles of designing a secure IT infrastructure. |
| C4 | Identifying threats to the security of IT systems and developing the ability to appropriately respond to emerging incidents. |

* 1. **Subject-specific learning outcomes, divided into knowledge , skills and competences , with reference to the directional learning outcomes**

|  |  |  |  |
| --- | --- | --- | --- |
| **No.** | **Description of subject learning outcomes** | **Reference to directional effects****learning (symbols)** | **Method of implementation (mark "X")** |
| **ST** | **NST** |
| **Classes at the University** | **Activities on the platform** | **Classes at the University** | **Activities on the platform** |
| After passing the course, the student knows and understands **the knowledge** |
| W1 | Has detailed knowledge of the main security issues of information systems. | INF\_W05INF\_W13INF\_W14INF\_W15 |  | X |  | X |
| W2 | Has knowledge of the life cycle and maintenance of IT systems to ensure the desired level of security. |  | X |  | X |
| W3 | Knows the protocols and standards regarding the security of IT systems. |  | X |  | X |
| W4 | Has detailed knowledge of methods for preventing incidents that violate the security of IT systems. |  | X |  | X |
| After passing the course, the student is **able** to: |
| U1 | Is able to identify threats to the security of IT systems and respond to them appropriately. | INF\_U02INF\_U25 |  | X |  | X |
| U2 | Is able to critically analyze an IT system with respect to security. |  | X |  | X |
| U3 | Is able to implement standard IT system security mechanisms. |  | X |  | X |
| U4 | Is able to identify and interpret the phenomenon of incidents occurring in IT systems. |  | X |  | X |
| After completing the course, the student is ready to take part in **social competences.** |
| K1 | Understands the need for continuous improvement of knowledge in the field of IT systems security. | INF\_K05 |  | X |  | X |
| K2 | Conduct in accordance with ethical principles and draws attention to the achievements and traditions of the profession |  | X |  | X |

**3.3. Forms of teaching and their number of hours - Full-time studies (ST), Part-time studies (NST)**

|  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **Path** | **Lecture** | **Exercises** | **Design** | **Workshop** | **Laboratory** | **Seminar** | **Lecturer** | **Classes conducted using distance learning methods and techniques in the form of a lecture** | **Other** | **ECTS points** |
| **ST** |  |  |  |  |  |  |  | 20 |  | 1 |
| **NST** |  |  |  |  |  |  |  | 10 |  | 1 |

**3.4. Content of education** (separately for each form of classes: (W, ĆW, PROJ, WAR, LAB, LEK, OTHER). It should be marked (X) how the given content will be implemented (classes at the university or classes on the e-learning platform conducted using distance learning methods and techniques)

**TYPE OF CLASS: LECTURE**

|  |  |  |  |
| --- | --- | --- | --- |
| **No.** | **Content of the course** | **Reference to subject-specific learning outcomes** | **Method of implementation (mark "X")** |
| **ST** | **NST** |
| **Classes at the University** | **Activities on the platform** | **Classes at the University** | **Activities on the platform** |
| **1.** | Examples of IT security problems. | **W1** |  | **X** |  | **X** |
| **2.** | Vulnerabilities and threats, their classification and sources of up-to-date information. | **W1, W2** |  | **X** |  | **X** |
| **3.** | Security fundamentals: confidentiality, integrity, availability; data protection at rest, during transmission and during processing; security mechanisms: technologies, policies and procedures, human factors. | **W1, W3, W4** |  | **X** |  | **X** |
| **4.** | Threat detection (port scanners, vulnerability scanners, antivirus software, IPS/IDS systems). | **U1, U2** |  | **X** |  | **X** |
| **5.** | Network infrastructure security (including remote access to network devices). | **U2** |  | **X** |  | **X** |
| **6.** | Cryptographic security mechanisms (encryption algorithms, hash functions, digital signatures and certificates). | **U3** |  | **X** |  | **X** |
| **7.** | VPN, IPsec solutions . | **U1, U2** |  | **X** |  | **X** |
| **8.** | LAN security (at ISO/OSI layer 2). | **U2, U3** |  | **X** |  | **X** |
| **9.** | Security issues specific to wireless technologies. | **U4** |  | **X** |  | **X** |
| **10.** | Methods of preventing incidents. | **U4, K1, K2** |  | **X** |  | **X** |
| **11.** | Summary of classes and discussion of grades. |  |  | **X** |  | **X** |

**3.5. Methods of verifying learning outcomes** (indication and description of methods of conducting classes and verification of achievement of learning outcomes and method of documentation)

|  |  |  |  |
| --- | --- | --- | --- |
| **Subject Effects** | **Teaching methods** | **Methods of verifying learning outcomes** | **Documentation methods** |
| **KNOWLEDGE** |
| **W1-W4** | informative, conversational lecture with the use of multimedia | Use of materials and content included in the lecture to pass the colloquium (test colloquium and open task enabling a statement on a given topic ) | Colloquium sheet |
| **SKILLS** |
| **U1-U4** | informative, conversational lecture with the use of multimedia | Using materials and content from the lecture to pass the colloquium (test colloquium and open task allowing for a statement on a given topic) | Colloquium sheet |
| **SOCIAL COMPETENCES** |
| **K1-K2** | informative, conversational lecture with the use of multimedia | Using materials and content from the lecture to pass the colloquium (a test-based colloquium and an open-ended task that allows for a statement on a given topic) | Colloquium sheet |

\*

**3.6. Assessment criteria for the achieved learning outcomes**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Learning effect** | **For a grade of 3 or " zal ."****the student knows and understands/is able to/is ready to** | **For a grade of 3.5, the student knows and understands/is able to/is ready to** | **For a grade of 4, the student knows and understands/is able to/is ready to** | **For a grade of 4.5, the student knows and understands/is able to/is ready to** | **For a grade of 5, the student knows and understands/is able to/is ready to** |
| W | 51-60% of knowledge indicated in learning outcomes | 61-70% of knowledge indicated in learning outcomes | 71-80% of knowledge indicated in learning outcomes | 81-90% of knowledge indicated in learning outcomes | 91-100% of knowledge indicated in learning outcomes |
| U | 51-60% of skills indicated in learning outcomes | 61-70% of skills indicated in learning outcomes | 71-80% of skills indicated in learning outcomes | 81-90% of skills indicated in learning outcomes | 91-100% of skills indicated in learning outcomes |
| K | 51-60% of skills indicated in learning outcomes | 61-70% of skills indicated in learning outcomes | 71-80% of skills indicated in learning outcomes | 81-90% of skills indicated in learning outcomes | 91-100% of skills indicated in learning outcomes |

**3.7. Literature**

**Basic:**

1. National Institute of Standards and Technology, “Security and Privacy Controls for Information Systems and Organizations” (NIST SP 800-53) - National Institute of Standards and Technology (NIST), CreateSpace, Scotts Valley, 2017.
2. National Institute of Standards and Technology, An Introduction to Information Security (NIST SP 800-12) - National Institute of Standards and Technology (NIST), CreateSpace, Scotts Valley, 2017
3. Kurs *Introduction to Cybersecurity*, dostępny on-line na platformie netacad.com
4. red. Sajdak M., Wprowadzenie do bezpieczeństwa IT, t. 1, wyd. Securitum, 2023

**Supplementary:**

# NIST Computer Security Incident Handling Guide, on-line: https://csrc.nist.gov/pubs/sp/800/61/r3/ipd

1. Kurs Ethical Hacker, dostępny on-line na platformie netacad.com
2. Kurs Cybersecurity Essentials, dostępny on-line na platformie netacad.com

**4. Student workload - ects points balance**

|  |  |
| --- | --- |
| **Types of student activity** | **Student Load** |
| **ST** | **NST** |
| **Classes requiring direct contact between the student and the academic teacher at the university premises** | **20** | **10** |
| Classes included in the study plan | 20 | 10 |
| **Student's own work** | **5** | **15** |
| Ongoing preparation for classes, preparation of project work/presentations/etc. | 3 | 8 |
| Preparation for passing classes | 2 | 7 |
| **TOTAL STUDENT HOURLY LOAD** | **25** | **25** |
| **Number of ECTS points** | **1** | **1** |

|  |  |
| --- | --- |
| Last change date | 30/09/2024 |
| The changes were introduced | INF Education Quality Team |
| The changes were approved | Arkadiusz Gwarda, M.A. |