PATVIRTINTA
Vilniaus universiteto Kauno fakulteto tarybos
2025 m. balandžio 9 d. nutarimu
Nr. (1.15 E) 620000-TPN-11

# COURSE UNIT (MODULE) DESCRIPTION

| Course unit title | Course unit code |
|---|---|
| **The Art of Manipulation: Social Engineering Threats** | |

| Lecturer (s) | Department where course unit is delivered |
|---|---|
| Assoc. prof. dr. Ilona Veitaitė | Kaunas Faculty<br>Institute of Social Sciences and Applied Informatics |

| Cycle | Type of the course unit |
|---|---|
| First | General University Studies |

| Mode of delivery | Semester or period when the course unit is delivered | Language of instruction |
|---|---|---|
| Face-to-face / online study | Autumn or Spring semesters | English |

| Prerequisites and corequisites | |
|---|---|
| **Prerequisites:** | **Corequisites:** |

| Number of ECTS credits allocated | Student's workload | Contact work hours | Individual work hours |
|---|---|---|---|
| 5 | 130 | 48 | 82 |

| Purpose of the course unit | | |
|---|---|---|
| This course aims to provide students with a comprehensive understanding of social engineering threats, their psychological and technological foundations, and their impact on cybersecurity. Through theoretical learning and practical exercises, students will develop critical thinking skills to identify, analyze, and mitigate social engineering attacks in various environments. As part of general university studies, this course fosters awareness of human vulnerabilities in cybersecurity, enhances digital literacy, and prepares students to apply security principles in both personal and professional settings. | | |
| **Learning outcomes of course unit** | **Teaching and learning methods** | **Assessment methods** |
| Understand the fundamental principles of social engineering, its history, and techniques used by attackers. | Lectures, case studies, discussions. | Practical assignments, Seminar participation, Case study analysis, Exam. |
| Identify and analyze various social engineering attacks and their psychological underpinnings. | Lectures, real-world case studies, discussions. | |
| Develop strategies to prevent and mitigate social engineering threats in personal and organizational settings. | Practical exercises, security awareness training through case studies. | |

| Course content: breakdown of the topics | Contact work hours | | | | | | | Self-study work: time and assignments | |
|---|---|---|---|---|---|---|---|---|---|
| | Lectures | Tutorials | Seminars | Practice classes | Laboratory | Practice | **All contact work** | **Individual work** | **Assignments** |
| Introduction to the course. Introduction to Social Engineering: History and Evolution. The origins and historical context of social engineering; Evolution of attack techniques over time; Notable cases in history. | 2 | | | | | | **2** | **2** | Theory material analysis. Slides prepared based on K.Mitnick, Ch.Hadnagy, R.B.Cialdini. |
| Psychological Principles Behind Social Engineering. Cognitive biases and how they are exploited; Influence techniques used in manipulation; Emotional triggers in social engineering. | 2 | | | | | | **2** | **2** | Theory material analysis. Slides prepared based on K.Mitnick, Ch.Hadnagy, R.B.Cialdini. |
| Common Social Engineering Techniques (Phishing, Pretexting, Baiting, etc.). Types of social engineering attacks; Real-world examples and their impact; Recognizing and mitigating attacks; Analysis of real-life phishing and baiting cases, identifying the techniques used and discussing potential countermeasures | 2 | | | 2 | | | **4** | **6** | Theory material analysis. Slides prepared based on K.Mitnick, Ch.Hadnagy, R.B.Cialdini. Analysis of real-life cases. |
| Cybersecurity and Human Weakness: Why Social Engineering Works. Human factor in cybersecurity breaches; The role of trust in deception; Psychological manipulation vs. technological vulnerabilities | 2 | | | | | | **2** | **2** | Theory material analysis. Slides prepared based on K.Mitnick, Ch.Hadnagy, R.B.Cialdini. Analysis of real-life cases. |
| Phishing and Spear Phishing: Techniques and Countermeasures. Anatomy of a phishing attack; Differences between phishing and spear phishing; Best practices for detection and prevention. | 2 | | | 2 | | | **4** | **6** | Theory material analysis. Slides prepared based on K.Mitnick, B.Schneier, J.W.H.Bullee, M.Junger, R.B.Cialdini. Analysis of real-life cases. Practical task (Phishing Email Simulation): Students will analize phishing emails, tracking results to understand the effectiveness of different phishing strategies. |
| Identity Theft and Impersonation Attacks. How personal data is stolen and misused; Impersonation techniques and fraud; Identity protection strategies. | 2 | | | 2 | | | **4** | **8** | Theory material analysis. Slides prepared based on K.Mitnick, B.Schneier, J.W.H.Bullee, M.Junger, R.B.Cialdini. Practical (Real-world Scenarios): Students will conduct an investigation on a fabricated identity theft |

| | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|
| | | | | | | | | | case, documenting how attackers gather and exploit sensitive information. |
| Social Engineering in the Workplace: Insider Threats. Role of employees in security breaches; Social engineering through HR and internal communication, Security awareness training methods. | 2 | | | 2 | | | **4** | **6** | Theory material analysis. Slides prepared based on K.Mitnick, B.Schneier, J.W.H.Bullee, M.Junger, R.B.Cialdini. Analysis of identification and counter insider threat scenarios within an organization. |
| Seminar: Case Study Analysis – Major Social Engineering Attacks. Analyzing well-known social engineering incidents; Lessons learned from past breaches; Strategies for improving organizational resilience. | | | 2 | | | | **2** | **8** | Seminar/Discussion |
| AI and Deepfake Technology in Social Engineering. The rise of AI-driven deception; Deepfake technology and its applications, Countermeasures against AI-based attacks | 2 | | | | | | **2** | **2** | Theory material analysis. Slides prepared based on K.Mitnick, B.Schneier, M.Schmitt, I.Flechais, R.B.Cialdini. |
| Protecting Personal and Organizational Security: Defence Strategies. Multi-layered security approaches; Zero-trust security models; Training employees against manipulation. | 2 | | | 2 | | | **4** | **8** | Theory material analysis. Slides prepared based on K.Mitnick, B.Schneier, M.Schmitt, I.Flechais, R.B.Cialdini. Practical task (Security Protocol Implementation): Analysis of security measures evaluation and effectiveness. |
| The role of social media in social engineering Attacks. Social media as a tool for attackers; Data harvesting and OSINT techniques; Privacy settings and risk management. | 2 | | | 2 | | | **4** | **8** | Theory material analysis. Slides prepared based on K.Mitnick, B.Schneier, M.Schmitt, I.Flechais, R.B.Cialdini. Practical task (Social Media Analysis): Students will analyze their own or a given social media profile to identify risks and create a report on how attackers could exploit shared information. |
| Ethical Hacking and Penetration Testing Against Social Engineering. Ethical hacking principles; Social engineering in penetration testing; Red teaming vs. blue teaming approaches. | 2 | | | 2 | | | **4** | **6** | Theory material analysis. Slides prepared based on K.Mitnick, B.Schneier, M.Schmitt, I.Flechais, R.B.Cialdini. Analysis of social engineering penetration testing to assess security awareness. |
| Cyber Law and Legal Implications of Social Engineering. Legal frameworks and | 2 | | | | | | **2** | **2** | Theory material analysis. Slides prepared based |

| | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|
| regulations; Ethical dilemmas in cybersecurity; Case law examples and real-world prosecutions. | | | | | | | | | on Ch.Hadnagy, B.Schneier, M.Schmitt, I.Flechais, R.B.Cialdini. |
| Seminar: Analyzing Real-life Social Engineering Incidents. Reviewing current and past social engineering cases; Discussion on the impact of human errors in cybersecurity; Brainstorming solutions for improving awareness and prevention. | | | 2 | | | | **2** | **8** | Seminar/Discussion |
| Future Trends and Evolving Social Engineering Threats. The next generation of social engineering threats; AI and automation in cybercrime; Innovations in cybersecurity defence mechanisms. | 2 | | | | | | **2** | **2** | Theory material analysis. Slides prepared based on Ch.Hadnagy, B.Schneier, M.Schmitt, I.Flechais, R.B.Cialdini. |
| Course Summary, Q&A, and Exam Preparation. Recap of key topics covered in the course. | 2 | | | 2 | | | **4** | **6** | Open Q&A session for students; Preparation tips for the final exam. |
| **Total** | **28** | | **4** | **16** | | | **48** | **82** | |

| **Assessment strategy** | **Comparative weight percentage** | **Date of examination** | **Assessment criteria** |
|---|---|---|---|
| Seminars (S) | 2x20% | Individual time during the semester | During the semester, students prepare and make presentations on real-life cases according to specific requirements. These presentations are discussed during the seminars. Evaluation criteria for the seminars:<br>- ability to reveal the main aspects of the chosen research problem, appeal to scholarly literature;<br>- ability to present the chosen research problem in a logical, well-structured, and argumentative way;<br>- ability to paraphrase the scholarly material and present it in a comprehensible and suggestible way;<br>- ability to participate in the discussions during presentations of the other students;<br>- ability to raise important issues and questions;<br>- ability to reason one's opposite point of view<br>- compliance with task requirements.<br>Scale of evaluation from 1 to 10 points. |
| Practical Tasks (PT) | 4x10% | Individual time during the semester | The following aspects of the PT are assessed: whether all tasks have been completed, the quality of the tasks, and the quality of their relation to task requirements. Scale of evaluation from 1 to 10 points. |
| Exam (E) | 20% | Examination session | The exam consists of open questions and practical exercises. Scale of evaluation from 1 to 10 points. |
| **Final Grade = S x 0,4 + PT x 0,4 + E x 0,2** | | | |
| *Based on the highest interim results, the lecturer may offer a high final grade instead of taking the exam.* | | | |
| **Exam grade must be ≥ 5** | | | |
| *The use of an Artificial Intelligence (AI) must be based on "The Guidelines on Artificial Intelligence Usage at Vilnius University" and its improvements. The use of any AI model must be disclosed, so if an AI generative model has been used in a text, paper, report or other work, this must be clearly stated (with appropriate citations and/or a declaration of the use of an AI generative model). Failure to disclose the use of an AI generative model in an academic work is considered academic dishonesty. In order to ensure that generative AI tools have not been used in the preparation of the essay (i.e. the content of the essay has not been generated by the AI tools), if not disclosed, the lecturer has the right to ask follow-up questions, to use the AI detection tools and, if necessary, to modify or cancel the grade of the assignment.* | | | |

| **Author** | **Year** | **Title** | **Number of periodical publication** | **The place of publication and** |
|---|---|---|---|---|

| | | | or publication Volume | publisher or online link |
|---|---|---|---|---|
| Kevin Mitnick | 2002 | The Art of Deception | - | Wiley, New York, USA |
| Kevin Mitnick | 2005 | The Art of Intrusion | - | Wiley, New York, USA |
| Christopher Hadnagy | 2018 | Social Engineering: The Science of Human Hacking | - | Wiley, Hoboken, USA |
| Bruce Schneier | 2015 | Data and Goliath: The Hidden Battles to Collect Your Data and Control Your World | - | W. W. Norton & Company, New York, USA |
| Jan-Willem H. Bullée, Marianne Junger | 2020 | Social Engineering | The Palgrave Handbook of International Cybercrime and Cyberdeviance | Springer Nature |
| Marc Schmitt, Ivan Flechais | 2024 | Digital deception: generative artificial intelligence in social engineering and phishing | Artificial Intelligence Review | Department of Computer Science, University of Oxford, Oxford, UK |
| Cialdini, Robert B. | 2021 | Influence: The Psychology of Persuasion | - | Harper Business, New York, USA |