THESIS SUMMARY

**"*Information Security Solutions Against Social Engineering*"**

Author: *Radu Moinescu*
E-mail: *radu.moinescu@gmail.com*, phone: *+40.721.507.524*
Ph.D. supervisor: *Univ. prof. eng. Ciprian Răcuciu, PhD*

The doctoral thesis presents a rigorous analysis of the intersection of psychology, technology, and cybersecurity, with a particular focus on social engineering attacks. The research examines how attackers exploit human vulnerabilities to compromise computer systems and analyzes effective defense strategies against these attacks.

*The introductory chapter* addresses the complexity of cybersecurity in a deeply digitalized context, emphasizing the essential role of the human factor and highlighting the inherent limitations in achieving absolute security in cyberspace.

*Chapter 2* provides a detailed description of the concept of social engineering, including the techniques and methods used to manipulate users in order to obtain sensitive information. It also analyzes the psychological impact of these techniques, such as persuasion and human error, and discusses the goals and conditions conducive to successful attacks.

*Chapter 3* investigates the relationships between social engineering and psychological factors, such as anxiety, depression, stress, and personality traits. The study identifies strong correlations between negative emotional states and users' vulnerability to attacks, using statistical analyses to validate the hypotheses. The conclusions emphasize the importance of psychological support and education to mitigate risks.

*Chapter 4* analyzes the techniques used in cyberattacks, presenting relevant historical examples and exploring the relationship between social engineering and information exfiltration. Case studies provide valuable lessons about exploited vulnerabilities. Comparative analysis reveals weaknesses in defense systems.

*Chapter 5* focuses on technological and strategic measures to prevent attacks, emphasizing innovative solutions such as Zero Trust Network Access and Content Disarm and Reconstruction. A comparative analysis of current technologies is carried out, accompanied by practical implementation examples.

*Chapter 6* expands the perspective on information security, examining organizational culture and theory, such as classical security models and measures of protection against electromagnetic interception. The importance of education and organizational adaptability to emerging threats is emphasized.

*Chapter 7* explores the use of artificial intelligence in cybersecurity, discussing both the benefits and risks associated with it. It examines how artificial intelligence can enhance both defensive and offensive capabilities, highlighting the need for ethical and balanced implementation.

*Chapter 8* examines the use of automated technologies, such as "*Tropes*" software, and the role of the human factor in defending against attacks. The importance of a "*human firewall*" based on awareness and training is highlighted, along with experimental solutions for detecting phishing.

*Chapter 9* summarizes the research results, highlighting the original contributions, including the development of new techniques for preventing and identifying attacks. Future research directions are proposed, and the conclusions emphasize the interdisciplinary impact of the study on the fields of cybersecurity and psychology, demonstrating its theoretical and practical relevance.

Key issues addressed:

- *Social engineering*: Defining and classifying techniques, analyzing attacker motivations, and identifying commonly exploited human vulnerabilities.
- *Psychology of attacks*: Exploring the mechanisms by which attackers manipulate emotions, trust, and the use of persuasion techniques.
- *Attack technologies*: Analyzing a variety of tools, including malware, phishing, ransomware, and zero-day attacks.
- *Defense against attacks*: Presenting technological and human measures to protect against social engineering attacks.
- *Artificial intelligence*: Discussing the potential of artificial intelligence in detecting and preventing attacks, as well as the risks associated with its use for malicious purposes.

The thesis makes a significant contribution to the field of cybersecurity, highlighting the need for a multidisciplinary approach that integrates technology, psychology and the human factor. A thorough understanding of the mechanisms underlying social engineering attacks allows the development of effective strategies to mitigate these threats.