# Work4Ce Module 02 – Digital Technologies

# Updated Course: CYBER SECURITY

# *This syllabus is a product of the Work4Ce project M02 Digital Technologies developed by the Academy of the State Customs Committee of the State Customs Committee of the Republic of Azerbaijan (ASCCA). The syllabus updates the curriculum of the ASCCA BA degree programme Information Security (in particular, the previous Cyber Security course of the BA programme has been updated).*

The "Introduction to Cybersecurity" course provides a comprehensive foundation in cybersecurity principles, practices, and challenges. Designed for beginners, it equips students with the knowledge and skills needed to understand cyber threats, secure systems, and apply fundamental defense strategies. The course includes both theoretical and practical components to ensure learners can analyze, mitigate, and respond to security incidents effectively.

In today’s interconnected world, cybersecurity is a critical field that safeguards personal data, corporate assets, and national security. This course begins with an introduction to the evolving landscape of cyber threats and progresses to hands-on training in key cybersecurity tools and techniques. Students will explore topics such as network security, cryptography, incident response, and ethical considerations, ensuring a well-rounded understanding of the discipline.

This course is ideal for individuals aspiring to pursue a career in cybersecurity, IT professionals looking to enhance their skills, or anyone interested in protecting digital information in both personal and professional contexts. By the end of this course, students will have the foundational knowledge to advance to specialized areas in cybersecurity or to prepare for entry-level certifications.

### **Overall Learning Outcome:**

Upon successful completion of this course, students will have a thorough understanding of cybersecurity fundamentals and be capable of applying foundational security practices in real-world scenarios. They will be equipped to:

* Identify and mitigate common cyber threats and vulnerabilities.
* Implement strategies for safeguarding networks, systems, and sensitive data.
* Understand the ethical, legal, and technical aspects of cybersecurity.
* Utilize essential cybersecurity tools and frameworks effectively.
* Develop critical thinking skills to evaluate and respond to emerging security challenges.

# SYLLABUS[[1]](#footnote-1)

**Core course, obligatory (ASCCA - 4 ECTS)**

#### **Week 1: Introduction to Cybersecurity**

* Overview of cybersecurity
* Importance of cybersecurity in today’s digital world
* Key terms and concepts

#### **Week 2: Cyber Threat Landscape**

* Types of cyber threats (e.g., malware, phishing, ransomware)
* Understanding threat actors and motives

#### **Week 3: Fundamental Security Principles**

* Confidentiality, Integrity, Availability (CIA Triad)
* Security models and frameworks

#### **Week 4: Cybersecurity and Networking Basics**

* Overview of networking concepts
* Common network vulnerabilities

#### **Week 5: Risk Management and Vulnerability Assessment**

* Introduction to risk management
* Identifying and assessing vulnerabilities

#### **Week 6: Access Control and Authentication**

* Access control mechanisms
* Multi-factor authentication

#### **Week 7: Cryptography Fundamentals**

* History and principles of cryptography
* Symmetric vs. asymmetric encryption

#### **Week 8: Securing Systems and Applications**

* Operating system security
* Secure software development practices

#### **Week 9: Network Security**

* Firewalls and intrusion detection systems
* Virtual Private Networks (VPNs)

#### **Week 10: Cybersecurity Tools and Techniques**

* Overview of popular tools (e.g., Wireshark, Nessus, Metasploit)
* Practical lab exercises

#### **Week 11: Social Engineering and Human Factors**

* Understanding social engineering attacks
* Best practices for security awareness

#### **Week 12: Ethical and Legal Aspects of Cybersecurity**

* Cyber laws and regulations
* Ethical hacking principles

#### **Week 13: Incident Response and Recovery**

* Steps in the incident response process
* Post-incident analysis and recovery

#### **Week 14: Cybersecurity Trends and Emerging Threats**

* Exploring AI and machine learning in cybersecurity
* IoT security challenges

#### **Week 15: Web Security**

* Overview of web application security
* Common vulnerabilities (e.g., SQL injection, XSS, CSRF)
* Secure coding practices and web security tools
* Final course review and exam preparation

## Books:

1. ”Network Security Essentials” by William Stallings
2. ”The Web Application Hacker's Handbook” by Dafydd Stuttard and Marcus Pinto
3. ”Practical Malware Analysis” by Michael Sikorski and Andrew Honig
4. ”Cybersecurity and Cyberwar” by P.W. Singer and Allan Friedman
5. ”Computer Security: Principles and Practice” by William Stallings and Lawrie Brown
6. ”Hacking: The Art of Exploitation” by Jon Erickson
7. ”Metasploit: The Penetration Tester’s Guide” by David Kennedy et al.
8. ”Applied Cryptography” by Bruce Schneier
9. ”Security Engineering” by Ross Anderson
10. ”Social Engineering: The Science of Human Hacking” by Christopher Hadnagy
11. ”Blue Team Handbook: Incident Response Edition” by Don Murdoch
12. ”Cybersecurity for Beginners” by Raef Meeuwisse
13. ”The Basics of Hacking and Penetration Testing” by Patrick Engebretson
14. ”Introduction to Cybersecurity” by Paul Grisham

1. Language of instruction: Azerbaijani [↑](#footnote-ref-1)