Module Specification

Cyber Security and Data Protection [TSI]

Version: 2021-22, v1.0, 26 Oct 2021

Contents

Part 1: Information

Module title: Cyber Security and Data Protection [TSI]

Module code: UFCE91-12-M

Level: Level 7

For implementation from: 2021-22

UWE credit rating: 12

ECTS credit rating: 6

Faculty: Faculty of Environment & Technology

Department: FET Dept of Computer Sci & Creative Tech

Partner institutions: Transport and Telecommunication Institute

Delivery locations: Transport and Telecommunication Institute Latvia

Field: Computer Science and Creative Technologies

Module type: Standard

Pre-requisites: None

Excluded combinations: None

Co-requisites: None

Continuing professional development: No

Professional, statutory or regulatory body requirements: None

Part 2: Description

Overview: Aims to provide students with an understanding of the duties, roles and responsibilities of professionals within the cybersecurity and data protection industries.

Features: Not applicable

Educational aims: To provide students with an understanding of the role and principles of cybersecurity and data protection, as well as related technologies, tools, legal regulations and standards.

Outline syllabus: Basic concepts and terminology of cybersecurity. Cybersecurity domains. Common Threats
Models of information security. Confidentiality, integrity and availability. Data states
Cybersecurity countermeasures. Security policy.
IT Security management framework
Cybersecurity Threats, vulnerabilities and attacks. Tactics, techniques and procedures used by cyber criminals
Technologies and procedures for data integrity providing. Concepts of hashing, digital signatures and digital certificates.
Technologies and procedures for services availability and business continuity. Concepts of high availability
Technologies and procedures for data integrity providing. Concepts of hashing, digital signatures and digital certificates.
Cybersecurity domains and methods of security audit
Legislation and legislative responsibility in the field of information security. Personal data: GPDR regulation

Part 3: Teaching and learning methods

Teaching and learning methods: Learning and teaching will be provided to students in two forms: lectures and practical classes. During lectures, theoretical aspects of the course will be provided to students by the teaching staff. Lectures will be supported by presentation published and available to the students on e.tsi.lv under the module section. The module is based on CISCO materials and will intensively utilize materials of the Cisco Networking Academy.

Module Learning outcomes: On successful completion of this module students will achieve the following learning outcomes.

MO1 Demonstrate an understanding of the current threat landscape with supporting case studies.

MO2 Evaluate current legislation and information security policy, procedures, and standards (such as ISO/IEC2700)

MO3 Evaluate and apply common security countermeasures such as device hardening, firewall configuration,

MO4 Design, implement and configure common security safeguards such as VLANS, Firewall configuration and route planning.

Hours to be allocated: 120

Contact hours:

Independent study/self-guided study = 112 hours

Face-to-face learning = 48 hours

Total = 160

Reading list: The reading list for this module can be accessed at readinglists.uwe.ac.uk via the following link https://rl.talis.com/3/uwe/lists/D3F267FC-0C96-C0A8-3835-4A8D2862BCB3.html?lang=en-gb&login=1

Part 4: Assessment

Assessment strategy: The module consists of 3 assessments:

Component A – Written examination for 2h. The examination will contain theoretical questions and practical tasks.

Component B – Portfolio (practical assignment) During module students should develop and complete individual works. The practical classes from CISCO Networking Academy.

Component B – Portfolio of MCQ tests. The MCQ will be adopted from CISCO Networking Academy.

The resit will be similar to the main sit.

Assessment components:

Examination - Component A (First Sit)

Description: Exam

Weighting: 30 %

Final assessment: Yes

Group work: No

Learning outcomes tested: MO1, MO2

Portfolio - Component B (First Sit)

Description: 8-Practical assignment

Weighting: 50 %

Final assessment: No

Group work: No

Learning outcomes tested: MO3, MO4

In-class test - Component B (First Sit)

Description: Cisco MCQ tests

Weighting: 20 %

Final assessment: No

Group work: No

Learning outcomes tested: MO1, MO2, MO3, MO4

Examination - Component A (Resit)

Description: Exam

Weighting: 30 %

Final assessment: Yes

Group work: No

Learning outcomes tested: MO1, MO2

Portfolio - Component B (Resit)

Description: Resit relevant labs from the 8 sat on the first sit

Weighting: 50 %

Final assessment: No

Group work: No

Learning outcomes tested: MO3, MO4

In-class test - Component B (Resit)

Description: Resit relevant Cisco MCQ tests

Weighting: 20 %

Final assessment: No

Group work: No

Learning outcomes tested: MO1, MO2, MO3, MO4

Part 5: Contributes towards

This module contributes towards the following programmes of study:

Computer Science (Data Analytics and Artificial Intelligence) {Double Degree} [Feb][FT][TSI][2yrs] MSc 2021-22