**INTRODUCTION TO CYBERSECURITY**

**Training format**

The course is based on the principles of active learning: lectures, practical seminars, attack and defense simulations, case analysis, team projects. The emphasis is on the application of knowledge in the real world and interdisciplinary interaction.

**Typical research questions of the course:**

* What are the main types of cyber threats and how to protect yourself from them?
* How to ensure data security in personal, corporate and government contexts?
* How can cybersecurity technologies be used to protect democracy and human rights?
* What are the social, ethical and legal implications of modern digital security practices?

**Assessment and deliveries**

The deliveries, on which course assessment and success (3 ECTS credit points in total) is based, are assessed as follows:

* Participation in classes and practices (individually; 20%).
* Team project – cyber incident analysis or cyber defense simulation (group work; 40%).
* Individual essay or research report (40%) – threat analysis, security policies, or ethical aspects of cybersecurity.

**Entry requirements for participation**

The course is open to students of all majors, especially useful for those studying IT, law, social sciences, or management. Prior technical training is not required, but is encouraged.

**Form of tuition**

The Introduction to Cybersecurity course combines theoretical knowledge with practical application. It includes lectures, interactive discussions, simulations of real situations, case analysis, as well as group project work related to the development of elements of cyber defense policies or modeling security incidents. The course is focused on an interdisciplinary approach and solving practical problems in a team.

*Estimated time budget*

This is an intensive 10-week course of 3 ECTS, which requires regular attendance of lectures and practical classes, as well as active participation in group projects that are carried out outside of classroom time. The total workload is about 70 hours, of which about 30 are classroom work and 40 are independent preparation, research and project activities.

*Learning outcomes (with* *Dublin Descriptors):*

At the end of the course, students will:

A. Know the basic concepts of cybersecurity, types of cyber threats, principles of information protection and understand their impact at the individual, organizational and societal levels (knowledge and understanding).

B. Apply basic cyber defense tools in everyday digital practice, taking into account both technical and behavioral aspects of security (application of knowledge and understanding).

C. Analyze modern risks and challenges in the field of cybersecurity, make informed decisions on digital security, weighing technical, ethical, legal and social factors (critical thinking, formation of judgments).

D. Work as a team on incident modeling projects, cyber threat research, or the development of information security policy elements, effectively presenting the results (communication and collaborative skills).

E. Develop the ability to act responsibly in the digital environment: (i) explore challenges and solutions in the face of cyber risks, (ii) consider the ethical, legal and democratic aspects of digital interaction, (iii) promote safe and ethical online behavior (soft skills, responsible digital behavior, problem solving).

**Learning outcomes according to the Louis framework**

The Louis framework is used in EURIDICE education to strengthen the general – higher order – academic and personal learning outcomes. It is based on the AAC&U-Value approach and adopted/adapted for higher education for societal impact by the Aurora Universities Alliance.

* Critical thinking
* Ethical reasoning
* Global Digital Literacy
* Active participation in the digital society

**Lecturing team**

* **Maryna Yesina,** Ph.D., Associate Professor, Acting Head of the Department of Cybersecurity of Information Systems, Networks and Technologies, V.N. Karazin Kharkiv National University (General Supervisor of the course): m.v.yesina@karazin.ua.
* **Vladyslav Vilihura,** PhD, Senior Lecturer of the Department of Cybersecurity of Information Systems, Networks and Technologies, V.N. Karazin Kharkiv National University: v.v.vilihura@karazin.ua.

Dr. Olena Mykolenko (General course coordinator, olenamykolenko@karazin.ua).

**Virtual classroom**

All classes will be held in a mixed format using Zoom, Moodle and specialized cyber simulators (where possible).

**Creative Commons**

All materials in this course are created by Maryna Yesina and Vladyslav Vilihura.