DA2215 Theory of Science and Scientific methods in Cybersecurity 3.0 credits

Vetenskapsteori och vetenskaplig metodik inom cybersäkerhet

This is a translation of the Swedish, legally binding, course syllabus.

If the course is discontinued, students may request to be examined during the following two academic years

Establishment

The official course syllabus is valid from the autumn semester 2024 in accordance with the decision from the director of first and second cycle education: J-2024-0737.Decision date: 2024-04-04

Grading scale

P, F

Education cycle

Second cycle

Main field of study

Computer Science and Engineering

Additional regulations

Those who, at the start of the course, have not completed or been actively participating in 4,5 credits method equivalent to AK2030 must read AK2030 in parallel with DA2215.

Specific prerequisites

Knowledge in cybersecurity, 7.5 higher education credits, equivalent to completed course DD2391.

Knowledge of the role of the cybersecurity engineer in society, equivalent to active participation in DD2303.

Note that knowledge of scientific methodology, 4,5 credits, equivalent to AK2030, also needs to be read before or in parallel with the course, see under the heading additional regulations

Active participation in a course offering where the final examination is not yet reported in Ladok is considered equivalent to completion of the course.
Registering for a course is counted as active participation.
The term 'final examination' encompasses both the regular examination and the first re-examination

Language of instruction

The language of instruction is specified in the course offering information in the course catalogue.

Intended learning outcomes

After passing the course, the student should be able to

- relate the different parts of scientific method, how they relate to one another, contribute and not contribute to scientificity in security
- assess, analyse, and discuss the quality in, and ethical aspects of, knowledge generation related to digital systems and in particular the security of these systems
- apply scientific methodology to show how to answer issues in the cybersecurity field
- plan and carry out assignments within given time frames and available resources
- write short, clear and arguing texts based on own analysis as well as given material.

in order to be able to contribute to scientifically based development.

Course contents

The course highlights, how different parts of the scientific methodology are relevant for cybersecurity in different situations. The focus is to analyse how scientific methods influence our knowledge of issues in cybersecurity, including their relation to different aspects of the subjects

- gender equality, diversity and equal conditions
- sustainability,
- ethical dilemmas.

This course is reported in the form of written assignments and active seminar participation.

Examination

- INL1 - Seminars and assignments, 3.0 credits, grading scale: P, F

Based on recommendation from KTH's coordinator for disabilities, the examiner will decide how to adapt an examination for students with documented disability.

The examiner may apply another examination format when re-examining individual students.

Other requirements for final grade

Active participation in all compulsory activities and passed home assignments.

Ethical approach

- All members of a group are responsible for the group's work.
- In any assessment, every student shall honestly disclose any help received and sources used.
- In an oral assessment, every student shall be able to present and answer questions about the entire assignment and solution.