JÖNKÖPING UNIVERSITY
School of Engineering

PROGRAMME SYLLABUS Preliminary, not confirmed

Cybersecurity (one year master), 60 credits

Programmestart: Autumn 2024

School of Engineering, Box 1026, SE-551 11 Jönköping • VISIT Gjuterigatan 5, Campus
PHONE +46 (0)36-10 10 00 • E-MAIL registrator@ju.se • www.ju.se/eng

PROGRAMME SYLLABUS Preliminary, not confirmed

Cybersecurity (one year master), 60 credits

Cybersäkerhet (magister), 60 högskolepoäng

Programme code:	TACS4	**Programmestart:**	Autumn 2024
Confirmed by:	Not confirmed	**Education Cycle:**	Second-cycle level
Version:	1		

Title of qualification

Degree of Master (60 credits) with a major in Computer Science, specialisation in Cybersecurity.

Programme overview

Background

Cybersecurity breaches are heavily affecting our society, and the protection of assets has become big business. We see cybersecurity-related issues daily in the news, such as ransomware attacks, identity theft and data breaches. In recent years, we have seen more financially-motivated adversaries and state-sponsored attacks, making it an uneven playing field, especially for smaller organisations with limited resources. Cybersecurity is considered a horizontal market which implies it cuts through vertical sectors, such as manufacturing, automotive, banking, education, healthcare, retail, and more. This means there is a need to protect assets virtually anywhere in society. One prime example is the manufacturing sector which has its aim set at Industry 5.0, where the common theme is digitalisation, connectivity, and automation. With such transformation comes increased dependency on hardware and software that controls and monitors industrial equipment, Operational Technology (OT). Such OT is at the core of production, and their functioning is critical to operation. To fully leverage OT, such systems are often connected to networks and have humans in the loop. With the introduction of OT comes a new range of challenges connected to cybersecurity.

The increased focus and need for cybersecurity solutions have created significant demand for skilled professionals.

This master's programme in cybersecurity helps students acquire the skills required to take on the challenge of protecting our society.

Objectives

The programme is intended for students with a bachelor's degree in computer science, computer engineering, informatics, information systems or similar. By introducing students to core technologies and concepts in the field, the programme will help them understand, use and implement solutions that address cybersecurity-related issues.

The programme aims to provide knowledge that enhances the skills and abilities of students with different IT-related backgrounds by providing broad cybersecurity skills and the possibility to select a focus in several courses that align with personal interests or backgrounds.

Areas of employment after graduation

This master's programme in cybersecurity prepares students for third-cycle courses and research projects or work in the industry. With the experience provided by the programme, students will be able to undertake a variety of roles, such as cybersecurity specialist, cybersecurity engineer, cybersecurity manager, or cybersecurity consultant.

Research
A Master's degree qualifies to apply for further third-cycle education leading to a licentiate or doctoral degree.

Research supporting the programme
Within the Department of Computer Science & Informatics, there is a strong focus on research related to cybersecurity. Cybersecurity is a topic that affects all sectors of society. Here, the focus is especially on cybersecurity and privacy in the industrial and public sectors, where most of the cybersecurity research in the department is conducted. Furthermore, there is a particular focus on human aspects among the staff where contributions on, for example, awareness, management, usable security and social engineering have been made.

Cybersecurity is a multi- and interdisciplinary field of study that draws on principles from different subjects, such as computing (e.g., artificial intelligence, privacy, software development), social sciences (e.g., psychology, ethics, economy), and many more.

The programme is also closely connected to the thematic areas of Jönköping University's SPARK Research Environment, especially to the sub-environments 1 (Integrated Product and Production Development for Sustainability and Resilience) and 3 (Human-Centered Industrial AI). In these sub-environments are the core areas of digitalisation and digital transformation of products and services, all utterly dependent on cybersecurity. This also makes cybersecurity a foundation to facilitate research between schools and departments, the industry and the public sector.

Objectives
On completion of the programme, the student must fulfil the learning outcomes for the degree of master (60 credits) as laid down in the Higher Education Ordinance:

General learning outcomes

Knowledge and understanding
1. demonstrate knowledge and understanding in the main field of study, including both an overview of the field and specialised knowledge in certain areas of the field as well as insight into current research and development work, and
2. demonstrate specialised methodological knowledge in the main field of study.

Competence and skills
3. demonstrate the ability to integrate knowledge and analyse, assess and deal with complex phenomena, issues and situations even with limited information,
4. demonstrate the ability to identify and formulate issues autonomously as well as to plan and, using appropriate methods, undertake advanced tasks within predetermined time frames,
5. demonstrate the ability in speech and writing to report clearly and discuss his or her conclusions and the knowledge and arguments on which they are based in dialogue with different audiences, and
6. demonstrate the skills required for participation in research and development work or employment in some other qualified capacity.

Judgement and approach
7. demonstrate the ability to make assessments in the main field of study informed by relevant disciplinary, social and ethical issues and also to demonstrate awareness of ethical aspects of research and development work,

8. demonstrate insight into the possibilities and limitations of research, its role in society and the responsibility of the individual for how it is used, and
9. demonstrate the ability to identify the personal need for further knowledge and take responsibility for his or her ongoing learning.

Programme-specific learning outcomes
On completion of the programme, the student must also fulfil the following programme-specific learning outcomes:

Knowledge and understanding
10. display knowledge of the area of cybersecurity and its related subject areas, and
11. display knowledge of the definitions, terminology, and concepts of cybersecurity.

Competence and skills
12. demonstrate skills in using tools for penetration testing and cybersecurity operations, and
13. demonstrate the ability to create risk and privacy impact assessments.

Judgement and approach
14. demonstrate an insight into the societal, legal and ethical aspects of cybersecurity operations, and
15. demonstrate the ability to suggest risk-based security controls to counter threats and vulnerabilities.

Contents
Programme principles
Instruction is in the form of lectures, seminars, exercises, laboratory sessions and project work. All courses are held in English. All final course examinations are in English.

The teaching approach in the programme is based, to a large extent, on learning from real-life scenarios and group learning. Lectures and labs often include examples from real projects, which put the theoretical material into a practical context. In course assignments, students work in groups to plan and implement a solution to a problem based on a real-life case. The resulting solution is reported in both written and oral form. This lays the ground for learning communication and leadership within a group.

The programme includes an independent degree project worth 15 higher education credits. Students, individually or in groups of two, prepare and present an assignment in cybersecurity, applying the knowledge accumulated during the programme and demonstrating the acquired skills. The degree project is carried out during the last term of the programme and can be done in close collaboration with a company or an organisation.

Programme progression
The course *Cybersecurity Overview* gives a holistic view of cybersecurity and its relation to other subject areas, such as information security and privacy. Also, an overview of general and industry-specific standards and frameworks within the area is given as a frame of reference. Cybersecurity denotes a specific focus on risks and vulnerabilities associated with critical infrastructures and related systems used for connecting them. Hence, a parallel course on *Critical Infrastructure and the Internet of Things* introduces the fundamentals in that area. More specifically, threats, vulnerabilities and security controls related to industrial control systems (e.g. SCADA and operational technology) and networks (e.g. Industrial Internet of Things).

Following are two courses with two distinct aims, *State-of-the-art and Research Methods in Cybersecurity* and *Ethical Hacking and Penetration Testing*. The concept of red team/blue team is central in *Ethical Hacking and Penetration Testing*, where the focus is on the red team, i.e., focus on offensive aspects of cybersecurity. Such aspects include hacking and penetration testing and the tools and methodologies associated. *State-of-the-art and Research Methods in*

Cybersecurity have two main parts. One aims to provide knowledge in state-of-the-art and emerging knowledge areas in cybersecurity. The other aims to introduce quantitative scientific methods in cybersecurity, focusing on descriptive statistics, sampling and survey design and regression analysis. The spring term starts with a course in *Digital Ethics and Privacy* and the *Final Project Work in Computer Science*. *Digital Ethics and Privacy* focuses on legal and societal aspects of cybersecurity with topics including, but not limited to, human values, vulnerabilities, or intersectionality, engaging students in critique-based thinking and analysis. Moreover, the course considers privacy, including legal and professional frameworks (e.g., privacy by design, or privacy impact assessment).

The spring term ends with a *Cybersecurity Operations and Incident Response* course. In this course, there is a focus on the blue team, i.e. the defensive aspects of cybersecurity. Such concepts include network security (including intrusion detection/prevention, firewalls, network admission control, and virtual private networks), standards and frameworks for incident response, digital forensics and digital evidence and monitoring.

During their *Final Project Work*, the students are expected to enhance and deepen their knowledge of modern trends and discoveries in cybersecurity and contribute their own results to this area. The Final Project Work requires students to exercise their ability to understand a problem, identify different solutions to the problem, and choose an appropriate solution.

Courses

Mandatory courses

Course Name	Credits	Main field of study	Specialised in	Course Code
Cybersecurity Operations and Incident Response	7.5	Computer Science	A1F	TCOS25
Digital Ethics and Privacy	7.5	Informatics	A1N	TEKR23
Ethical Hacking and Penetration Testing	7.5	Computer Science	A1F	TEHS24
Final Project Work in Computer Science	15	Computer Science	A1E	TEXT25
Critical Infrastructure and the Internet of Things	7.5	Computer Science	A1N	TKIR24
State-of-the-art and Research Methods in Cybersecurity	7.5	Computer Science	A1F	TFCS24
Cybersecurity Overview	7.5	Computer Science	A1N	TCSR24

Programme overview

Year 1

Semester 1		Semester 2	
Period 1	Period 2	Period 3	Period 4
Critical Infrastructure and the Internet of Things, 7.5 credits	Ethical Hacking and Penetration Testing, 7.5 credits	Digital Ethics and Privacy, 7.5 credits	Cybersecurity Operations and Incident Response, 7.5 credits
Cybersecurity Overview, 7.5 credits	State-of-the-art and Research Methods in Cybersecurity, 7.5 credits	Final Project Work in Computer Science, 15 credits	

Teaching and examination

Throughout the academic year, typically, two courses are taken in parallel. Examination forms and grades are given by each course module, respectively. The programme overview shows the programme structure for both years and may be changed during the programme. For updated programme overview visit http://www.ju.se

Prerequisites
The applicant must hold a minimum of a bachelor's degree (i.e., the equivalent of 180 ECTS credits at an accredited university) with at least 90 credits in Computer Science, Informatics, Information Systems, Computer Engineering, or the equivalent. Proof of English proficiency is required.

Qualification Requirements
To obtain a Degree of Master (60 credits) with a major in Computer Science, specialisation in Cybersecurity, students must complete a minimum of 60 credits in accordance with the current programme syllabus.
In addition, a Degree of Bachelor of Science in Engineering/Degree of Bachelor of Science or an equivalent Swedish or foreign qualification is required.

Quality Development
The School of Engineering's quality assurance process involves continuous development and quality assurance of degree programmes and courses. This means, among other things, that great importance is attributed to student feedback and that a proactive approach is taken to the development of degree programmes and courses. The quality assurance process is carried out following applicable steering documents.

Other Information
If formal competence is missing, the applicant's substantial competence is tested if the applicant has acquired equivalent knowledge in some other way. The aim is to assess the collective competence and if the applicant has the opportunity to meet selected training. Substantial competence can be about knowledge and experience from working life, long-term mobility or other courses.

A course included in the programme can be read separately, subject to availability. Prerequisites are stated in the syllabus.

Admission is under "Admission arrangements for first and second level" at Jönköping University.
This syllabus is based on "Regulations and guidelines for education at undergraduate, postgraduate and doctoral studies at Jönköping University".