Kristiania

Programme description

Master in Cyber Security, Experience-based

2024

90 ECTS
Session-based
Part-time

Studiet er akkreditert av Styret:16.02.2023 (styresak 02.5),
følgesak i rektoratet 17.04.2023 (sak 3.22.34)
Studiet ble godkjent av Utdanningsutvalget:19.01.2023(UU/EIT-sak 3/23)
Programbeskrivelsen er godkjent i Lokalt utdanningsutvalg:11.06.2024(LU/EIT-sak 60/24)

Table of contents

1. Introduction

Master in Cyber Security, Experience-based (90 ECTS) is a programme designed for professionals with relevant industry experience for the domain of modern cybersecurity. The programme is offered as a 3-year part-time program. The content and progression in the courses allow students to join courses as session-based modules. The courses will have a variety of physical attendance and digital format with both mandatory and non-mandatory gatherings. The programme emphasizes analysis and understanding of the cyber threats picture, and how to implement best practices and standards in industrial and organizational processes. The students will be mastering skills in deploying, managing and auditing Information and Communications Technology (ICT) systems, cybersecurity software and hardware solutions, as well as analysing and managing consumer and prosumer security. The goal of the programme is to train future cyber security professionals and enhance previous knowledge in the field through flexible online learning and attractive pool of elective courses.

The study programme will cover the following directions of professional development, that students will be able to focus on the following areas within information security:

- Secure Software Development and Cloud: a tremendous amount of ICT and Operational Technology (OT) solutions have moved to Cloud, and a whole industry has changed the approach over the last decade
- Operational Security: the vast number of interconnected devices create critical national infrastructure as well as end-user smart infrastructure
- Incident Response: modern cyber security incidents management is not only about reactive Digital Forensics, yet maintaining the defence of the cyber-physical perimeter in an agile environment

Moreover, the students who seek advancement in career development will be able to work in the following domains connected to information security as described by the European Cybersecurity Skills Framework (ECSF):

- Chief Information Security Officer (CISO)
- Cybersecurity Implementer
- Cyber Threats Intelligence Specialist
- Penetration Tester
- Cyber Incident Responder
- Digital Forensics Investigator

Upon completion of the Master's programme, the following job opportunities will be available to students, however not limited to:

- Police IT Services
- Cybersecurity consultant
- IT administrator
- Cybersecurity Analyst
- Security Manager

- Incident Response analysts

Kristiania University College has the necessary competence and staff members with relevant qualifications and research portfolios to teach and supervise students in cyber security. A particular emphasis is put on qualification development through training and certifications in the field of information security to deliver the most relevant and up-to-date knowledge to our students. The study will be intricately connected to the cyber security laboratory (SmartSecLab) and all research groups at the School of Economics, Innovation and Technology working in the corresponding domain (MOTEL, AISE and others). It is a well-recognized national and international environment with an extensive network of cooperation partners and funded projects in cyber security.

The career development opportunities that are available to students after finishing the master program:

- Professional certifications (CISSP, CISA, ISO27001, etc.) as the programme structure is coherent with major professional development courses and programs

Master in Cyber Security, Experience-based is offered as a 3-year part-time program. Therefore, it is well suited for a person with a full-time job while studying. Most of the courses are session-based modules with non-mandatory gatherings, where the format can be physical as well as digital. Some of the courses in the programme might be offered as online courses as well, which is subject to development of new areas and demand for such courses. The concluding Master thesis is also flexible as the student may choose to complete the course in one or two semesters.

1.1 Formal requirements

To be qualified for enrolment in the experience-based Master in Cyber Security program, applicants must meet the following requirements:

- The candidate must have a bachelor's degree in the fields of Software Engineering, Information Security, Computer Science, Information Technology, Information Systems, Human Computer Interaction, or other relevant field with an average grade of minimum examination grade of C, which is equal to minimum 2.7 ECTS.
- At least 2 years of relevant professional practical experience related to any of the fields of IT is required.

2. Learning Outcomes

All study programs at Kristiania University College have established an overall learning outcome that every student is expected to achieve after completing the study. Learning outcomes describe what the student is expected to know, be able to and be able to do because of the learning processes associated with the study. Learning outcomes are described in the category's knowledge, skills, and general competence.

Knowledge
The candidate…

- has advanced knowledge in the main fields of cyber security, understands modern toolkit and technologies used to protect information and infrastructure
- can analyse modern computer systems and evaluate the level of implemented security controls
- has in-depth knowledge of theoretical approaches and corresponding practical methods
- can analyse a self-defined problem within cyber security in context of existing research literature.

Skills
The candidate …

- can analyse the current state of the art in cyber security and develop own research projects
- can critically analyse available cyber security solutions and refine their knowledge based on the existing theoretical frameworks and tools
- can independently develop a project following NIST cyber security framework and relevant industrial standards
- is able the choose an adequate research method to answer an academic problem within cyber security

General competence
The candidate …

- can analyse problems related to ethics and legality of the application of cyber security tools
- can apply knowledge and skills achieved through work life in new areas within cyber security through an academic perspective
- is able to present an extensive work on a specific cyber security problem both in writing and orally
- can communicate terminology and problem areas from the domains in cyber security both in technical and non-technical terms
- can initiate and lead the innovation work in the field of cyber security practice and implementation

3. Structure of the program

Experience-based Master in Cyber Security is a 90 ECTS programme at Kristiania. 15 ECTS are common courses, 30 ECTS are program-specific cyber security-dedicated courses. Common- and programme specific courses are designed to be offered with a wide range of teaching methods, from session-based physical to a digital teaching with non-mandatory gatherings. The programme can be completed over three years (part-time). The format of mandatory courses and electives are subject to changes and may be offered as online courses.

The programme includes two elective courses (15 ECTS). These can be taken as a part of the exchange programme at the partner university abroad with the details given in the Section 5.

Furthermore, a student has an opportunity to focus on building competence in the following recommended areas based on the selected elective courses: (i) Secure Software Development and Cloud, (ii) Operational Security, (iii) Incident Response.

The master's programme concludes with dedicated work on a master's thesis project (30 ECTS). The Master thesis may be completed within one or two semesters with flexible formats of participation. It is a requirement to pass the common course Research Methods before starting to work on the Master thesis.

The courses are thought as modules, meaning that the students usually will complete one module before starting the next. Therefore, an example of the study model with relevant semesters is indicated in the table below. This can be adjusted to meet the individual needs of students to facilitate flexibility in learning process.

Semester	**Master in Cyber Security, Experience-based** (part-time)	
1. semester	Ethics, sustainability, and society 7.5 ECTS	Network Security / CISCO CyberOps 7.5 ECTS
2. semester	Research Methods 7.5 ECTS	Incident Response and Investigations 7.5 ECTS
3. semester	Secure Software Development 7.5 ECTS	Elective / Exchange 7.5 ECTS
4. semester	AI for Cyber Security 7.5 ECTS	Elective / Exchange 7.5 ECTS

5. (and possibly 6.) semester	Master Thesis 30 ECTS

Table 2. Course matrix for part-time study – an example of the recommended progression

Mandatory courses	Elective courses/Exchange

3.1 Academic progression

Master in Cyber Security, Experience-based is a complete second-degree master's programme built on Kristiania University College's own Bachelor's programme in Cyber Security and Information Technology. Although the courses are presented as in a specific sequence in table 1, the courses may be completed in any sequence, with one exception: Research Methods must be passed before taking the Master thesis course. Through the common- and subject area courses, students will develop skills and competence in cyber security while building and managing versatile software products across a full range of network solutions. They will master knowledge in applying artificial intelligence and open-source intelligence for extensive data analysis while looking for traces of incidents. Through the electives, students will have opportunities to master their skills in different focus area directions. Please visit the Kristiania website for updates on course schedules and elective information.

3.2 Courses

Courses	ECTS	Description
Ethics, sustainability, and society	7,5	The main aim of this course is to provide students with the fundamental knowledge of ethics and sustainability necessary for responsible innovation and the development of modern technologies in modern society. The central topics include the role of ethics in responsible innovation and the development of information technology (IT); social, economic, and environmental impacts of innovations and modern technologies; and how IT development and innovation can contribute to achieving the UN Sustainable Development Goals. In covering ethical and sustainability issues, the course addresses the perspectives of various stakeholders at the individual level (IT developers, innovators, consumers, investors), the organizational level (commercial, public, and non-governmental organizations), and the societal level (local and regional communities, nations, international society). Group work on viable solutions to real-life ethical and sustainability challenges constitutes an essential part of the course.
Secure Software Development	7,5	Modern software is an overly complex system performing various tasks such as data analysis in healthcare systems, analysing camera images in self-driving cars and even controlling gates in water damns. With increasing complexity, it is imperative to understand and integrate cyber security in every aspect of the software development lifecycle. The objective of the course is to give students an understanding of the core cyber security principles in CD/CI as well as DevSecOps to plan, develop and manage agile software products.
Network Security / CISCO CyberOps	7,5	Computer networks and communication technologies such as WiFi are changing our daily life by connecting almost all computing devices to the Internet, as the main infrastructure. Hence, there is a high demand for candidates with the specialized knowledge and skills needed to administer devices and applications in a secure infrastructure, recognize network vulnerabilities, and mitigate security threats. Cybersecurity Operations (CyberOps) is the process of ensuring a strong cyber defense. CyberOps supports organizations in implementing and maintaining solutions, as well as executing security processes so that cyber risk is properly managed. This course focuses on the latest operational skills and knowledge needed for securing networks as well as jobs in Security Operations Centers (SOCs). In particular, the course deals with security concepts, common network and application operations and attacks, and the types of data needed to investigate security incidents. This course follows the National Initiative for Cybersecurity Education (NICE) Cybersecurity Workforce Framework; this ensures a consistent communication language for cybersecurity education, training, and

		workforce development.
Research methods	7,5	This course is intended as an introduction to research methodology and the research process. This introduction gives the students an overview of the basic concept, methods, and practice of research. Research is a cyclical process where new and carefully planned investigations build and extend on established work. The aim is to provide students with a fundamental understanding of research as a conceptual, empirical, and practical approach to gathering new insight and knowledge. The content provides a broad overview of how researchers work in the economy, innovation, and technology. It presents students with relevant methods from these domains, along with their possibilities and limitations. Students will learn a systematic approach to empirical investigation, including literature search, research design and methodology, qualitative and quantitative analyses, and the presentation and evaluation of results. After the course, students can study and interpret existing research on a topic and suggest approaches to broaden or deepen knowledge within a given topic.
AI for Cyber security	7,5	Cybersecurity became an inseparable part of our modern digitalized life. With all the connected devices we witness a tremendous increase in the amount of data that often hide traces of attacks or illegal activities. Not only hard to process such data by human experts, but also impossible to comprehend all possible details and contextual information related to unwanted cyber activities. In this course, students will be introduced to fundamental concepts and models from Artificial Intelligences such that clustering, classification, and regression that can be applied to most of the data contained areas in cybersecurity. These include, but not limited to, computer viruses' analysis, network traffic, financial crime investigations, etc. AI helps to improve the speed and efficiency of data processing and therefore is being integrated in many modern industrial cybersecurity solutions.
Incident Response and Investigations	7,5	Incident response (IR) is an approach to handling various categories of security incidents, cyber threats, and data leakage. The incident response methodology aims to identify, analyze, and minimize the cost of a cyberattack or a live incident by mitigation techniques. A well-designed IR plan can fix a potential vulnerability to prevent future attacks and propagation of the attacks. The response is a part of incident handling, which looks at the logistics, communications, synchronicity, and planning required to resolve an incident. This course includes investigation, reporting, analysis, and response.

Table 3. Compulsory courses

3.3 Electives

15 ECTS electives will give students flexibility in specializing in topics they want, either in cyber security or aligned master programs. There is an ongoing process with the development of the courses on the master level depending on the current needs in the industry. Therefore, the students have access to the most up-to-date topics in the information technologies and cyber security through the following courses. The list of the elective courses to be offered at Kristiania University College in the Table 3 is subject to changes considering the modern technologies' development and cyber security trends. To facilitate the selection of the electives, the students will be offered a set of three recommended focus areas identified in the program's structure above to focus on building a corresponding career path.

Courses	**ECTS**	
M2M infrastructure security	7,5	This course provides an overview on the security aspects of machine-to-machine communication. The main topics in the course are Internet of things (IoT) concepts and architectures, privacy and security aspects for IoT, data-centric IoT protocols – MQTT, MQTT-SN, CoAP and AMQP, security protocols, e.g., TLS and DTLS for ensuring security in data-centric IoT protocols, Link-layer IoT protocols – ZigBee, Wi-Fi, BLE, security aspects of ZigBee, Wi-Fi, BLE, overview of machine-type communication (MTC) and related security aspects.
Critical Infrastructure and Operational Security	7,5	The course focuses on the critical ICT infrastructures aspects and operational security of enterprise systems, i.e., cyber risk in critical infrastructures, digital information security architecture of enterprise systems, modeling enterprise security infrastructure, security measures and controls for ensuring operational security, and emerging topics in critical infrastructure and operational security (e.g., AI, cloud, Blockchain, etc.).
Mobile Computing and Internet of Things	7,5	Students will gain in depth knowledge of mobile computing and introduce the Internet of Things (IoT). Students will further acquire knowledge of theories/models of mobile and pervasive computing applications, technologies and common research paradigms in mobile and pervasive computing such as context awareness, computing in an environment with limited resources, sensor-based interaction, and smart-device management. They will acquire skills in application design, architecture and implementation. Students will be expected to be able to analyse, discuss and critically reflect upon theories and research issues in mobile computing and internet of things.

Cyber Security for Business Operations	7,5	Cybersecurity became an inseparable part of our digitalized life, including business operations in a modern society. In this course, students will be introduced to fundamental concepts from cybersecurity and various needs that businesses have with respect to digitalization and keeping the data sage and protected. Special emphasis is placed on general principles within cybersecurity, existing forms of attack, protection mechanisms and known incidents. Students will also learn about risk, access control, cryptography, cloud security, digital forensics and incident response. Furthermore, the students will gain knowledge about how privacy, GDPR and corresponding legislation works, and the consequences of these regulations on companies and enterprises when it comes to establishing a holistic approach on all levels: Executive Level, Security Operations, Process Management. Finally, the course will focus on understanding the security culture, software development and outsourcing in the Internet of Things and Operational Technologies.
Ethical Hacking	7,5	Ethical hacking within an organization is a strategic cybersecurity process that involves authorized professionals, known as ethical hackers or penetration testers, systematically probing the organization's information systems to identify and address potential security vulnerabilities. This technical approach requires a good understanding of networking protocols, operating systems, and application architectures. Ethical hackers employ a range of specialized tools and methodologies to simulate real-world cyberattacks, aiming to uncover weaknesses that could be exploited by malicious actors. The process typically begins with scoping, where the objectives of the ethical hacking engagement are defined. Subsequently, the technical experts conduct reconnaissance, actively scan for vulnerabilities, and enumerate system details. Using tools like penetration testing frameworks (e.g., Metasploit or Kali Linux) and vulnerability scanners, they meticulously assess potential weaknesses, often emulating the tactics of actual adversaries. The findings are then compiled into a detailed report, providing technical insights into the identified vulnerabilities, their potential impact on the organization's security, and actionable recommendations for mitigation. Through ethical hacking, organizations can proactively enhance their defensive capabilities, ensuring a robust and resilient cybersecurity posture. In this course, students will learn advanced techniques applicable also in modern organizations who employ disruptive technologies like Cloud and Internet of Things.

Table 4. Elective courses

3.4 Master Thesis (30 ECTS)

Course 30 ECTS	Description
Master thesis	The master thesis is a research project in which students will apply the knowledge acquired during their studies. It is a crafted scholarly document presenting research questions and original arguments based on scientific methods under the guidance of an advisor. The thesis gives the student the opportunity to demonstrate expertise in their chosen research area. Students will acquire specialized problem-solving skills, being able to plan and conduct the steps in the research and/or development process at a high methodological standard. They shall take responsibility to conduct a well planned and executed project.

Table 5. Master thesis

4. Teaching and assessment methods

4.1 Pedagogical platform and implementation of teaching

Master in Cyber Security, Experience-based is designed so that the sum of the topics and study work with these will lead the students towards the intended learning outcomes described in chapter 2. in the programme description. The pedagogical platform's goal is to facilitate and encourage learning.

The individual courses are put together to show a breadth of knowledge, skills and general competence that reflects the field of practice. Some courses are more oriented towards knowledge exchange, others more oriented towards building specific skills, while others include more skills in links between theory and practice. The experience-based master's programme in cyber security is created as a continuation of the bachelor's in cyber security at Kristiania University College as well as more thematically focused and industry-oriented in comparison to 120 ECTS Master in Cyber Security.

Cyber Security is a rapidly developing area that requires considerable practice and exercises to align with the theoretical foundations. Therefore, forms of work, teaching and assessment in the individual courses have been chosen to provide a good and meaningful correspondence between the learning outcome that is desired to be achieved, the teaching methods used, and the exam that concludes the course.

The methodological choices also reflect the course's contribution to the study program. The students, therefore, encounter a varied set of learning activities throughout the study period, a variation that, in total, should reflect the field of practice the student is studying for. Moreover, students will enhance their learning through a combination of both individual and group assignments to highlight the importance of teamwork in the cyber security domain.

The Experience-based Master in Cyber Security emphasizes that students learn to use relevant methods from research and professional development work. This will contribute to the students, through their master's studies being able to complete an independent, limited research or development project under supervision and in line with current academic and ethical norms. To take care of this, the teaching will include emphasis commenting on, illustrating, and elaborating material from teaching materials, as well as providing guidance and additional material that is not available in printed form. Finally, the students will apply learnt material on a variety of problems and tasks in cyber security.

As with all higher education, Kristiania University College also sets requirements for students' independent learning work. Kristiania University sees it as a task to facilitate the students' work through good learning designs. At the same time, we emphasize that a teacher can only communicate and facilitate. The actual learning takes place with the individual student because of the student's work. In connection with the teaching, the student must

therefore expect a significant personal effort both in acquiring theoretical knowledge as well as practising and exercising cyber security tools and technologies.

While attending the experience-based master programme in cyber security, the educational model might include the following components to facilitate learning and skills enhancement:

- Online digital learning with optional digital gatherings
- Lectures to introduce the theoretical concepts and frameworks
- Seminars, oral presentations, and group works give students an opportunity to present, discuss and argue upon topics and achieve results
- Supervision and assessment to guide the learning process
- Digital follow-up through acceptable platforms
- Use cases work and project execution. Students will, in some courses, be able to suggest cases from their own workplace.
- Attendance of the specialized workshop offered by the research environment
- Independent practice, lab work and exercises
- Participation in the collaboration projects through the cyber security lab – both internally and externally
- Industry consultations and coordination for better alignment with industry needs

For students who need tutoring beyond scheduled courses, Kristiania University College has available subject resources, including administrative staff, librarians, digital learning resources (e.g., online movies) and student tutors. These can be contacted by the individual student if needed. In addition to literature and help with literature searches, the library also offers varied training in academic writing.

During the study process, there will be organized course-specific academic and industry events will be held, where guest lecturers, external organizations and business actors can participate. The corresponding cooperation projects can be managed by the course coordinator and/or students and supported by administrative resources. For an experience-based master's in cyber security, this is relevant for all the mandatory courses in the courses list. See the course description for more information. Moreover, the students will be encouraged to attend cybersecurity-related events whenever possible through special arrangements and agreements to broaden their understanding of the field and job opportunities.

4.2 Examination and assessment forms

Assessment is a situation where a submitted or presented work is assessed against a set of criteria. Criteria are given by the learning outcome that are defined for the individual subject. The assessment can be made by fellow students, teachers, or examiners. These will also be happy to give feedback, either as guiding feedback or as a grade (exam) with a thorough explanation.

At Kristiania University College, we distinguish between assessment as learning, assessment for learning and assessment of learning. The form of the work being assessed (the assessment form) can be the same in all three of these assessment situations, while the purpose varies.

In assessment as learning (fellow student assessment) and for learning (feedback from the teacher), the purpose is to shape a learning process to help the student to achieve the best possible learning outcome. We perceive this assessment as part of the teaching methods, which can be found in Chapter 4.1 above.

Learning assessment is a final assessment where the achieved learning results are assessed - in other words, the exam. The exam at Kristiania University College is defined as "An exam is a final assignment within a course or a limited sub-course". The submitted or presented work is assessed through an examination, and the result of the assessment must appear on the diploma.

Master in Cyber Security, Experience-based is a study programme with extensive range of topics and involved technologies. As students choose electives, the complete list of exam formats may vary. As students on the experience-base master may be working while studying, the most frequent exam form is a 4-week written home examination. The 4-week exam may be a project or assignment and may build upon tasks and assignments from the course. A 4-week time span will provide the student with flexibility on when to work on the exam in addition to other parallel activities, such as work. There will also be flexibility regarding individual or group-based exams. Other exam formats may include:

- Supervised examination
- Multiple choice questions
- Home exam (different time limits)
- Oral presentation
- Portfolio assessment
- Assignments through semester
- Master thesis project
- Project-based practical exams

Some of the courses might include compulsory assignments (one or more). A compulsory activity, if included in the course, is a requirement that must be approved to be eligible for the exam. The activity can either be a requirement that one or more reports or practical works must be submitted (work requirements) and/or a requirement for participation in defined activities and/or lectures and/or compulsory practice.

A compulsory activity is assessed as Approved / Not Approved and gives the right to sit for an examination in a course with compulsory activity requirement when such an activity is assessed as Passed. Furthermore, students will be eligible for feedback on the performance in the compulsory assignment. Otherwise, the student loses the right to an examination in the course until the activity (ies) has been assessed as Approved.

The assessment of the various exam forms will follow the Norwegian grading system with the scale A - F, where A is the best grade, E is the lowest pass grade and F is fail. Or the exam also may use a Pass / Fail evaluation, which will be decided for each course.

For additional information about the exam and compulsory activity, see Kristiania University College's website.

5. Internationalization and student exchange

In this context, internationalization is understood as placing the study programme in an international context and that the students are exposed to a multitude of perspectives. All the reading materials and lectures are given in English, and the study uses both Norwegian and international cases. The students shall write their Master Thesis in English. The programme uses international educators and guest lecturers. Our educators also conduct research with international co-authors and play an active role in both national and international conferences. Selected topics will be presented by guest lecturer from abroad or by companies with relevant use-cases and focus.

5.1 Internationalization

By internationalization here is meant that the study offer is placed in an international context and that the students of the experience-based master's in cyber security are exposed to a multitude of perspectives, also including, but not limited to, exchange at the international partner institutions.

The study offer is set in an international context and exposes students to a varied perspective from Norway and abroad. This is achieved through extensive use of international literature and cases in teaching. For specific schemes for internationalization, reference is made to the study's course descriptions. The courses wills be offered in English with the involvement of lecturers having internationally recognized research and industry experience in the field of cyber security. Selected topics will be presented by guest lecturer from abroad or by companies with relevant use-cases and focus.

For the specific internationalization schemes, please consult the corresponding subject descriptions.

5.2 Student exchange

The Experience-based Master in Cyber Security programme includes two elective courses (15 ECTS). As an alternative, a student can take both courses at partner university abroad as a part of the exchange component. For the whole semester exchange (30 ECTS), a student can attend equal to mandatory courses at partner university, where the learning outcomes of such courses matches with learning outcomes of the courses at Kristiania University College. Alternatively, there is a possibility to join two mandatory courses online at Kristiania University College with remote supervision together with two electives if students' choses to travel on exchange for the whole semester. The overall goal is to facilitate flexibility and meet needs that students might eventually have.

When it comes to the international student's exchange, Kristiania University College participates in the following mobility programs:

- Nordplus in the Nordic countries or the Baltic states
- ERASMUS+ in Europe
- «Study Abroad», for students in or outside Europe

As the experience-based Master programme in Cyber Security is a part-time programme with students expected to be working while studying, there is flexibility regarding exchange. Exchange will be offered for single courses. Students may exchange specific courses in the programme for similar courses within our partner universities. As the programme has two elective courses, finding relevant courses abroad is not a challenge. The list of partner university accepting students from Kristiania University College:

- Kingston University, UK
- Arcada University of Applied Sciences, Finland
- Seoul National University of Science and Technology, South Korea
- University of Hertfordshire, UK
- Assumption University, Thailand

Kristiania University College reserves the right to make changes to relevant study places and updated information is published on the university college's web. There are also a limited number of study places at the corresponding partner university available for the exchange. For nomination to exchange program, there are usually requirements for grades and motivation application. Requirements can also be set for documentation of creative work / portfolios and Kristiania University College can conduct interviews of applicants for exchange. Kristiania University College aims to send well-qualified and motivated students to reputable foreign institutions. For both on-site and online studies, the exchange is only site-based.

In addition to established international exchange programs, mentioned above, the students will be exposed to a range of opportunities through the cyber security research laboratory and corresponding environment at the faculty. The activities will include participation in the cyber security conferences on the national and international level, summer and winter school attendance, Capture The Flag (CTF) competitions and relevant cyber security events.