School of Informatics and Engineering
Cyber and Information Security Master's Program

Curriculum
Name of education program
Cyber and Information Security
Higher ecademic education level
Master's
Qualifications to be granted
Master of Cybersecurity
Head of the program
Heads of the program – Anastasia Bajiashvili, Akaki Shekeladze Detailed information about the qualifications and scientific and teaching activities of the program headს is provided in the attached files.
Program structure
The Master's Program is built on the basis of the ECTS system. To obtain a qualification, a Master student must accumulate 120 credits within the framework of the Master educational program, which is the sum of the credits of the core and elective educational components, with content corresponding to the main field of study, and free credits. Educational components are presented in the amount of 120 credits, including: - Core components of the main field of study - 75 credits; - Elective components of the main field of study - 25 credits; - Research component - 20 credits. During the year, a student accumulates 60 credits, i.e. 30 credits per semester, although depending on the student's individual workload, the number of credits per year may be less or more than 60 credits, but no more than 75 credits. The program includes 10 free credits, which the student may earn within the elective course framework. These credits can be obtained through courses offered within the current program, from other academic programs of the same level at the School of Informatics and Engineering or Georgian-American University, from accredited academic programs of the same level at other higher education institutions in Georgia, or from academic programs of the same level at foreign higher education institutions, provided that the credits are recognized in accordance with Georgian legislation.

Language of instruction

English

The Goals of the program

The aim of the master's program is to prepare a highly responsible specialist aligned with modern requirements, who:

1. Describes the fundamental concepts, theories, methods, and tools in cybersecurity within ICTs, as well as technological solutions and international practices used in the field;
2. Based on the analysis, synthesis, and evaluation of information, is capable of practically conducting activities in the field of cybersecurity within ICTs — including maintaining the resilience of information security, identifying cyber risks, and effectively planning and managing resources in a multidisciplinary context;
3. Independently conducts scientific-research activities in the field of cybersecurity within ICTs using relevant research methods, and engages in public discourse with reasoned arguments while upholding academic integrity and ethical norms; evaluates the professional development needs of themselves and their teams and contributes to the development of the field;
4. Makes independent decisions in addressing problems in cybersecurity within ICTs, based on the principles of confidentiality, integrity, and availability.

Prerequisite for addmition to the program

The master's program is intended for individuals who have already obtained higher education in a relevant field related to Information and Communication Technologies (ICTs) and wish to deepen their knowledge in the area of cyber and information security. Accordingly, the necessary prerequisites for enrollment in the Master's Program are:

- Bachelor's degree or equivalent academic degree;
- Successfully passing the unified masters exams;
- Passing the internal university procedure, which consists of the following stages:
    - Documentation analysis - at this stage, the general application form developed by the university is filled out, which includes an assessment of the applicant's professional biography;
    - Passing the exam in English (B2 level) - applicants who present a certificate confirming the relevant qualification (TOEFEL, IELTS) or have completed a bachelor's or postgraduate educational program in English will be exempted from the exam;
    - Interview/exam in the specialty* - the purpose of which is to assess the applicant's knowledge in the IT field.

* Exam questions in the specialty will be posted in advance on the university website.

Field of employment

A master's degree holder can successfully find employment in all local or international organizations whose activities are related to ensuring and managing cyber and information security.

A Master in Cybersecurity may be employed in the following positions:

- Cybersecurity Analyst;
- Information Security Manager;
- Network Security Engineer;

- Data Protection Officer (DPO);
- Security Auditor;
- Ethical Hacker;
- Security Consultant;
- Security Software Architect;
- and others.

Opportunity to continue studies

A graduate of the Master's Program in Cyber and Informaiton Security is eligible to continue their studies at the doctoral level at a higher education institution in Georgia or abroad, provided that the doctoral program does not require a master's degree in a different specific field as a prerequisite.

Learning outcomes

Upon successful completion of the program, graduate**:**

1. Provides in-depth explanations of cybersecurity concepts, theories, methods, tools, techniques, and international practices within ICTs; monitors and implements industry developments.
2. Develops strategic and operational cybersecurity documentation; identifies information security management system challenges and communicates with senior management;
3. Designs technological solutions for cybersecurity resilience, defines implementation, monitoring, and evaluation mechanisms, and manages workgroups effectively, considering risk factors and efficient use of resources;
4. Independently conducts research in cybersecurity with academic integrity; presents well-supported conclusions to both academic and professional communities, contributing to the field's advancement within a multidisciplinary framework.
5. Makes independent decisions in addressing cybersecurity challenges, considering principles of confidentiality, integrity, availability, and ethical/professional standards;
6. Evaluates and defines both personal and team members' professional and career development needs

Teaching-learning methods and relevant activities

- Lecture
- Seminar (Group work),
- Practical Work,
- Homework /Abstract;
- Teaching with electronic resources,
- Master Thesis and others.

Academic and invited staff may use one or more methods listed above or any other method based on tasks of a specific course. Specific teaching-learning methods are indicated in the syllabus* of the relevant course.

* Syllabuses include consultation time that will be individually agreed with each teacher by the program head and communicated to students.

Assessment system

Receiving/accumulating credits in the relevant educational component by the student assumes active participation in the teaching process and is based on the principle of continuous evaluation of acquired knowledge.

The level of achievement of learning outcomes is assessed in accordance with the assessment system approved by the Order No. 3 of the Minister of Education and Science of Georgia of January 5, 2007, "About the Rules for Calculating Credits in Higher Education Programs."

Assessment of the level of achievement of learning outcomes includes assessment forms - intermediate and final assessment, the sum of which represents the final assessment - 100 points.

Assessment forms include an assessment component/components that determine the way to assess the student's knowledge/awareness and/or ability and/or autonomy/responsibility (verbal/written exam, verbal/written quiz, practical/theoretical work, homework, etc.). Assessment components combine assessment methods (test, presentation, etc.). The assessment method is measured by assessment criteria.

Each form and component of the assessment has a specific share of the total assessment score (100), which is reflected in the specific syllabus.

Each assessment form has a minimum competence threshold - at least 25 points for the intermediate assessment, at least 16 points for the final assessment.

A minimum competency threshold may also be set for the assessment component(s), which will be detailed in the course syllabus.

Credit cannot be awarded using only one form of assessment. Credit is awarded to the student in case of a positive assessment.

Program's educational components' assessment system:

A. The system has 5 types of Positive Assessment:

- **a)** Excellent – 91-100 points
- **b)** Very Good – 81-90 points
- **c)** Good – 71-80 points
- **d)** Satisfactory – 61-70 points
- **e)** Sufficient – 51-60 points

B. 2 types of Negative Assessment:

- **a)** (FX) Did not pass - 41-50 points, which means that the student needs more work in order to pass and, with independent work, is given the right to take the additional exam once
- **b)** (F) Failed - 40 points and less, which means that the work done by the student is insufficient, and they have to retake the course/subject.

To determine a student's final ranking and to encourage them, a cumulative grade point average (GPA) is calculated at the end of the learning process. The cumulative grade point average is calculated as follows: the quantitative indicator of the grade received by the student in each course of study is multiplied by the number of credits allocated for that course of study, and then the total sum of these numbers is divided by the number of credits accumulated by the student.

The research component of the Master's degree program (the completion and defense of the master thesis) must be assessed in the same or the following semester in which the student completes the work. The research

component includes research and practical aspects, this component is completed in the field of Constratction engineering and is assessed once (with a final assessment).

Resources available for program implementation

Material resources:

- Space requiredby legislation (teaching and auxiliary);
- Classes equipped with appropriate equipment, conference rooms, academic staff work rooms, and space for administration;
- Uninterrupted electricity supply system;
- Bathrooms;
- Natural lighting;
- Heating facilities;
- Fire safety mechanisms and fire-fighting equipment;
- Evacuation plan;
- Medical assistance mechanisms (medical office);
- Mechanisms for maintaining order (university protection);
- Adequate number of computers and access to the Internet;
- A library equipped with textbooks appropriate to the educational programs and modern information and communication technologies;

Human Resources:

- Academic staff is selected in accordance with Georgian legislation and taking into account their qualifications.
- People with appropriate qualifications, practical experience and scientific degrees are invited to the university as researchers and lecturers.

Map of the goals and outcomes of the Master's Program in Cyber and Inforamtion Security

მიზნები/შედეგები Goals/Outcomes	შედეგი Outcome 1	შედეგი Outcome 2	შედეგი Outcome 3	შედეგი Outcome 4	შედეგი Outcome 5	შედეგი Outcome 6
1. მოამზადოს თანამედროვე მოთხოვნების შესაბამისი, მაღალი პასუხისმგებლობის მქონე სპეციალისტი, რომელიც აღწერს ICTs-ში კიბერუსაფრთხოების მიმართულებით ძირითად კონცეფციებს, თეორიებს, მეთოდებს, ასევე ამ სფეროში გამოყენებულ ინსტრუმენტებს, ტექნოლოგიურ გადაწყვეტილებებსა და საერთაშორისო პრაქტიკებს; 1. To prepare a highly responsible specialist aligned with modern requirements, who describes the fundamental concepts, theories, methods, and tools in cybersecurity within ICTs, as well as technological solutions and international practices used in the field;	x					x
2. მოამზადოს თანამედროვე მოთხოვნების შესაბამისი, მაღალი პასუხისმგებლობის მქონე სპეციალისტი, რომელიც ინფორმაციის ანალიზის, სინთეზისა და შეფასების საფუძველზე შეძლებს ICTs-ში კიბერუსაფრთხოების მიმართულებით საქმიანობის პრაქტიკულად წარმართვას, მათ შორის, ინფორმაციული უსაფრთხოების მდგრადობის შენარჩუნებას, კიბერ-რისკების იდენტიფიცირებას, რესურსების ეფექტურ დაგეგმვასა და მართვას მულდტისიტსიპლინურ კონტექსტში; 2. To prepare a highly responsible specialist aligned with modern requirements, who based on the analysis, synthesis, and evaluation of information, is capable of practically conducting activities in the field of cybersecurity within ICTs — including maintaining the resilience of information security, identifying cyber risks, and effectively planning and managing resources in a multidisciplinary context;	x	x	x			
3. მოამზადოს თანამედროვე მოთხოვნების შესაბამისი, მაღალი პასუხისმგებლობის მქონე სპეციალისტი, რომელიც დამოუკიდებლად შეძლებს ICTs-ში კიბერუსაფრთხოების მიმართულებით სამეცნიერო-კვლევითი საქმიანობის განხორციელებას დარგის შესაბამისი კვლევის მეთოდების გამოყენებით, არგუმენტირებულად და აკადემიური კეთილსინდისიერებისა და ეთიკური ნორმების დაცვით იმსჯელებს საზოგადოების წინაშე; შეაფასებს საკუთარი და გუნდის პროფესიული განვითარების საჭიროებებს და წვლილს შეიტანს დარგის განვითარებაში; 3. To prepare a highly responsible specialist aligned with modern requirements, who independently conducts scientific-research activities in the field of cybersecurity within ICTs using relevant research methods, and engages in public discourse with reasoned arguments while upholding academic integrity and ethical norms; evaluates the professional development needs of themselves and their teams and contributes to the development of the field;	x			x	x	x

4. მოამზადოს თანამედროვე მოთხოვნების შესაბამისი, მაღალი პასუხისმგებლობის მქონე სპეციალისტი, რომელიც ICTs-ში კიბერუსაფრთხოების მიმართულებით პრობლემების გადაჭრისას, იღებს დამოუკიდებელ გადაწყვეტილებებს ინფორმაციის კონფიდენციალობის, მთლიანობისა და ხელმისაწვდომობის პრინციპების გათვალისწინებით; 4. To prepare a highly responsible specialist aligned with modern requirements, who makes independent decisions in addressing problems in cybersecurity within ICTs, based on the principles of confidentiality, integrity, and availability.			x		x	

Below each core course for passing the Master's Program is presented in relation to the program outcomes, showing which course leads to which outcome with indication of the corresponding level.

The Courses are broken down into three levels:

a) Inroduction Courses (I-Introduction)
b) Development Courses (D -Development)
c) Mastering Courses (M - Mastering).

An indicator of one of the levels is specified in the intersection of the course and the outcome - I, D or M.

#	Core Components ძირითადი სასწავლო კომპონენტები	შედეგი Outcome 1	შედეგი Outcome 2	შედეგი Outcome 3	შედეგი Outcome 4	შედეგი Outcome 5	შედეგი Outcome 6
I სემესტრი/ Semester							
1	Network Defense/ ქსელის უსაფრთხოება	I		I			
2	Operation System Security/ ოპერაციული სისტემის უსაფრთხოება	I		I		I	
3	Digital Project Management/ ციფრული პროექტების მართვა		I	I	I		I
4	Principles of Cyber Security/ კიბერუსაფრთხოების პრინციპები	I				I	
5	Math in Cybersecurity/ მატემატიკა კიბერუსაფრთხოებაში	I			I		
II სემესტრი/ Semester							
6	Management Systems and Operational Risks/ მართვის სტანდარტები და ოპერაციული რისკები		I	I		I	
7	DevSecOps/დევსეკოპსი		I	I			D
8	Cloud and AI Security Practices/ ღრუბლოვანი და ხელოვნური ინტელექტის უსაფრთხოების პრაქტიკები	I	I		I		
9	Ethical Hacking and Penetration Testing/ ეთიკური ჰაკინგი და შეღწევადობის ტესტირება	I	I			D	

10	Algorithms and Data Structures / ალგორითმები და მონაცემთა სტრუქტურები		I	I			
	III სემესტრი/ Semester						
11	Threat Hunting and Cyber Threat Intelligence/ კიბერ საფრთხეების ანალიტიკა	I	I				
12	Security Operations / უსაფრთხოების ოპერაციები	D		D	D		
13	Incident Response and Digital Forensics/ ინციდენტებზე რეაგირება და ციფრული ექსპერტიზა		D	M	M		D
14	Python in Cybersecurity/ პითონი კიბერუსაფრთხოებაში	D	D				
	IV სემესტრი/ Semester						
15	Cybersecurity Law and Compliance/ კიბერ სამართალი და შესაბამისობა		M	M	M		M
16	Master Thesis / სამაგისტრო ნაშრომი	M	M	M	M	M	M

Annex 1: Program Academic Plan

Annex 2: CV-s of Heads of Program