Caucasus University

Caucasus School of Technology

Name of Educational Programme	კიბერუსაფრთხოება
Name of Educational Programme in English	Cybersecurity
Level of Higher Education	Doctoral
Type of Educational Programme	Academic
Language of Instruction	English
Awarded Qualification, Code	
In Georgian:	კიბერუსაფრთხოების დოქტორი, 0613
In English:	PhD of Cybersecurity, 0613
Date of Program Approval	Order #01/01-20, 18.03.2025
Date of Program Renewal	-
Program Coordinator/Co-Coordinator	**Coordinator:** Maksim Iavich, affiliated professor at Caucasus University, President of the Scientific Cybersecurity Association, +995 595 511 355, miavich@cu.edu.ge **Co-Coordinator:** Vladimir Svanadze, affiliated professor at Caucasus University, +995 577 155 168, vsvanadze@cu.edu.ge

Program Volume in Credits
The official duration of the program is 3 years (6 semesters). Maximum duration is 5 years (10 semesters). PhD in Cybersecurity program consists of the teaching component (60 ECTS credits) and a research component that comprises no less than 2 years (4 academic semesters). Teaching process is structured around semesters. Each teaching course/seminar lasts one semester. A semester consists of calendar weeks. 1 ECTS credit corresponds to 25 study hours that includes both contact hours (lectures, seminars,

examinations, etc.) and hours of independent study time.

Out of 60 ECTS of teaching component:

- 34 ECTS credits contribute to the mandatory seminars and methodology courses
- 6 ECTS credits contribute to the elective (optional) seminars (students can choose one of the elective seminars)
- 20 ECTS credits contribute to the mandatory teaching/assistanship module.

•To participate in the scientific conference in the direction of the dissertation topic;
•The doctoral student is obliged to publish at least two scientific articles (or to have consent for publication). Among them, one article should be published in a refereed (peer-reviewed) journal with a foreign international index corresponding to the specificity of the field. Published articles should be thematically related to the thesis topic;
•After registering on the research component, PhD student is obliged to present a report on the work completed at the end of each semester in accordance with pre-defined forms.

Program Admission Precondition

- ✓ Diploma certifying at least Master's degree or equivalent academic degree.
- ✓ Notarized copy of diploma supplement/mark sheet;
- ✓ Proof of English language proficiency on B2 level or Bachelor or Master Degree Diploma of a program taught in English Language; In case an applicant does not possess above mentioned documents, s/he will have to pass Caucasus School of Technology admission exam in English Language at B2 level;
- ✓ A research thesis in English that matches the candidate's research interests;
- ✓ Previous publications in the relevant field and participation in scientific research projects and events and at least 2 years of work experience in the relevant field;
- ✓ Two letters of recommendation (prepared in English);
- ✓ Resume (CV) in Georgian and English.
- ✓ The applicant is required to pass the Technology School's math admission exam.
- ✓ Interviews with the Caucasus Technology School's admissions committee.

* Terms and conditions of admission are approved by the Admissions Committee and published on the university's website.

Qualification Description of the Program

Program Objective	The Phd. Program in Cybersecurity reflects the mission, vision, and values of the Caucasus University, as well as of the Technology school. The program takes into account local labor market demands, successful experience from cybersecurity doctoral programs implemented by local and foreign universities, and the development trends in the cybersecurity field. The objectives of the program are: • To prepare doctoral students as qualified researchers in the cybersecurity field who can apply contemporary theories and research methodologies to solve complex problems in cybersecurity or related fields • Development of Research Competencies: Train students to independently plan and conduct original research using relevant quantitative and qualitative methods, ensuring the use of reliable data for impactful studies. • Advancement of Knowledge through Critical Analysis: Encourage students to critically analyze and evaluate research findings, enabling them to formulate original conclusions and develop theoretically and practically significant recommendations for innovative solutions to cybersecurity challenges. • Enhancement of Teaching Proficiency: Equip students with advanced pedagogical skills, ensuring they are prepared to effectively transfer knowledge in various academic and professional settings through the best teaching methods available. • Ethical Academic Practices: Instill high standards of academic integrity and ethical norms in students, ensuring that they conduct and disseminate research with integrity and respect for the scholarly community. • International Integration: Prepare students to actively participate and integrate into the international academic community, enhancing their regional perspective and networking capabilities in cybersecurity and related fields. These goals are crafted to ensure that graduates of the PhD program in Cybersecurity are not only experts in their field but also ethical, globally aware, and effective educators and communicators who can contribute significantly to both academic and business sectors in Georgia.
Program Learning Outcomes	Graduates of this program will: **Knowledge and Understanding:** 1. Critically evaluate and integrate advanced theories, concepts and models in cybersecurity related fields, covering both policy and strategic as well as technical directions. **Ability**: 2. Performs synthesis of recent achievements and theoretical knowledge in cybersecurity to identify complex problems related to cybersecurity or related fields. 3. Independently plans and conducts research using appropriate qualitative and quantitative methods to obtain reliable data and results.

	4. Conducts critical analysis and synthesis of new, complex, and sometimes contradictory ideas and approaches, formulates original conclusions, and develops innovative recommendations that facilitate the development of cybersecurity practice and theory. 5. Based on the latest knowledge and original research results, creates scientific products and effectively communicates-disseminates research results to both local and international scientific communities through scientific conferences, discussions, projects, or other forms of participation. **Responsibility and Autonomy:** 6. Consistently demonstrate ethical conduct in research and publication, adhering to principles of academic integrity, respecting diverse viewpoints, and maintaining accountability in all scholarly activities.
Areas of Employment	A graduate of the program will have employment opportunities in the following fields: ⇒ Educational institutions, ⇒ Scientific and research institutes, ⇒ Analytical research centers, ⇒ Consulting companies, ⇒ Analytical and research departments at state and private sectors, ⇒ Top management positions in private and public companies in the direction of cybersecurity.

Evaluation System of Student's Knowledge

The aim of the evaluation is to assess to what extent the learning outcomes prescribed by the syllabus are reached. The student's evaluation consists of multiple components and evaluates the course goals and learning outcomes by applying measurable criteria and appropriate rubrics. The student's evaluation is based on four major principles: objectivity, trustworthiness, validity and transparency.

The students are evaluated according to two sets of evaluation: summative and formative. The aim of the summative assessment is to accurately evaluate the student's performance. It monitors quality of learning and the level of the student's achievement in relation to the goals set by the course. The formative assessment is oriented on the student's development. It gives students appropriate feedback on their achievements.

The evaluation system includes 100 points and envisages:

a) Five types of positive grades:

a.a) (A) Excellent – 91-100 points of assessment;

a.b) (B) Very good – 81-90 points of maximal assessment;

a.c) (C) Good – 71-80 points of maximal assessment;

a.d) (D) Satisfactory – 61-70 points of maximal assessment;

a.e) (E) Sufficient – 51-60 points of maximal assessment;

b) two negative grades:

b.a) (FX) Did not pass – 41-50 points of maximal assessment, which means the student needs to work harder and is allowed to retake the exam one more time after working independently;

b.b) (F) Fail – 40 points or less of maximal assessment, which means the student's work is insufficient and he/she has to retake the course.

Students are awarded credits on the basis of the final evaluation comprising the scores of the interim and final exam assessments.

The attainment of student's learning outcomes considers the interim and final evaluations, for which relative proportions out of the total score (100 points) and a minimum competence level are allocated. Namely, out of 100 points, the interim results are allocated 70 points, while the final exam results are 30 points. In interim evaluations the minimum competency barrier to be reached is 59%. The interim evaluation includes assessment methods, the total of which is 70 points. For each assessment method, the evaluation is based on the pre-determined learning goals, task-oriented clear criteria and the learning rubrics drawn on their basis. In the interim results the student has to accumulate at least 59% of the 70 points to be allowed to take the final exam. The student's final examination is passed, if he/she gets at least 60% of the total 30 points.

In case the student fails to overcome the minimum competency barrier of the final exam, he/she is allowed to retake the final examination. The student shall retake the final exam within the period prescribed by the academic calendar no later than 5 days after announcement of the results of the final exam.

In case the student totally scores 0-50 points or fails to overcome the minimum competency barrier set for any component of the evaluation (Interim/Final exam), he/she shall be given a grade of "F-0".

Accumulated points of additional exam are not added to points of final assessment. Evaluation received in additional exam is the final exam evaluation and is reflected in the final assessment of learning component of the learning program.
The scientific-research component is evaluated in accordance with the one-time evaluation principle according to the following scheme:
a) summa cum laude – excellent work;
b) very good (magna cum laude) – a result that exceeds the requirements in every way;
c) good (cum laude) – a result that exceeds the requirements;
d) average (bene) – an average-level paper that meets the basic requirements;
e) Satisfactory (rite) - a result that, despite the shortcomings, still meets the requirements satisfies;
f) Insufficient – work of an unsatisfactory level that cannot meet the requirements;
g) completely unsatisfactory (sub omni canone) – a result that does not fully meet the requirements.
Dissertation evaluation criteria, procedures, and rubrics are detailed in the Technology School Doctoral Regulations and Dissertation Syllabus.

Teaching and Learning Methods

- Verbal method;
- Method of written work;

Program Curriculum

(With the indication of modules, courses, relevant credits)

№	Course Code	Prerequisite	Course\ Module	Study Year								ECTS Credits
				I		II		III				
				ECTS Credits								
				I Semester	II Semester	III Semester	IV Semester	VSemester	VI Semester			
1.	SIWR 7111C	N/A	Research Methods	2								
2.	SEM 7112C	N/A	Seminar on Artificial Intelligence Cybersecurity	6								
3.	REME 7114C	N/A	Quantitative Research Methods	6								
4.	TEME 7112C	N/A	Teaching Methods	4								
5.	REME 7214C	N/A	Qualitative Research Methods		4							
6.	SEM 7213C	N/A	Seminar on Cyber Diplomacy and Technologies		6							
7.	SEM 7214C	N/A	Seminar in post-quantum cryptography									
8.	TEAS 7001C	TEME 7112C	Teaching Assistantship: Syllabus and Content Development		2							
9.	REDE 7121C	SIWR 7111C	Research Design		6							
10.	REME 7125C	REME 7114C	Multivariate Data Analysis		6							
11.	TEAS 7002C	TEME 7112C REDE 7121C	Teaching-Assistantship			6						
12.	TEAS 7003C	TEME 7112C REDE 7121C	Teaching-Assistantship				6					
13.	REAS 7002C	REME 7114C REME 7214C REDE 7121C	Research Assistantship									
14.	REAS 7001C	REME 7114C REME 7214C REDE 7121C	Research Assistantship					6				
15.	DISS 7321C		Dissertation			X	X	X	X			
		ECTS Credits	Per Semester	18	24	6	6	6				
			Per Year	42		12		6				

Remark :