



The University Of Georgia

Program name:	Cybersecurity (Eng)
Study Level:	Graduate
Program leader:	Sulkhan Sulkhanishvili kakha chkhartishvili Kim Tracy
Study language:	English
Qualification:	Master of Cybersecurity
Program capacity:	120
Program permission:	Admission to the second cycle of academic higher education (Master's programs) is carried out cumulatively based on the following: • Based on the Unified Master's Examinations or in accordance with the Order of the Minister of Education and Science of Georgia No. 224/N (December 29, 2011); • Confirmation of English language proficiency at the B2 level (confirmed through one of the following international certificates: TOEFL iBT – minimum score 80; IELTS – minimum score 6.5; PTE General – minimum level B2; FCE – minimum level B; CPE – passing is sufficient; CAE – passing is sufficient. Applicants without an international certificate may take the university's internal English language test at the B2 level, where a minimum score of 70% is considered sufficient); • Successful completion of an oral and practical examination in the specialty; • Completion of administrative registration and issuance of a presidential decree by the university.
Program goals:	The objective of the program is to prepare highly qualified and competitive cybersecurity specialists equipped with knowledge and skills that meet international standards and labor market demands, both locally and globally. The program provides students with a solid and systematic understanding of both theoretical foundations and practical applications in cybersecurity, enabling graduates to independently and effectively address the challenges and issues in the modern technological world related to cybersecurity. Upon successful completion of the program, graduates will be qualified to work in various roles, including but not limited to: security auditor, analyst, cloud security specialist, cybersecurity operations specialist, software security engineer, penetration testing expert, and other related positions.
Methods for Attaining Learning Outcomes:	• Lecture-seminar • Interactive lectures • Explanatory method • Demonstration method • Practical work • Critical analysis • Teamwork / Group work • Problem-oriented exercises • Case study and analysis • Literature review • Working with textbooks • Searching for relevant materials in electronic format or library • Written work method • Verbal (oral) method • Discussions / Debates • Simulation • Role-playing • Induction, deduction, analysis and synthesis • Presentation
Learning outcomes:	Knowledge and understanding • Describes the requirements of software and cloud security, as well as the methods of threat modeling within relevant cybersecurity contexts. • Discusses the role, functions, and risk assessment methods of auditing. • Describes the core principles of systems theory and the systems approach, explains the processes involved in assessing the operability and reliability of complex systems. Skills • Develops security requirements for software systems in accordance with cybersecurity standards and best practices; • Ensures the security of cloud-based solutions, including network configuration, identity and access management, infrastructure protection, and data security; • Plans and conducts audits of information systems to evaluate compliance, performance, and risk; • Identifies cybersecurity threats and responds appropriately to related incidents. Responsibility and autonomy • Independently addresses security-related issues and develops appropriate problem-solving strategies;

	- Ensures compliance with organizational governance structures, IT and information security policies, procedures and standards; - Adheres to security protocols and safeguards the security of cloud-based solutions, networks and infrastructure.
--	---

Date of approval:	02-28-2025
Approval protocol number:	3PCD6067-01

Date of program update:	
Update protocol number:	

Program details:	
Teaching Process Characteristics:	The program consists of 120 ECTS credits, with 102 ECTS allocated to core subjects and 18 ECTS to elective subjects. The total number of elective subjects amounts to 102 ECTS, from which the student must choose 18 ECTS. In the core part of the program, the student is required to complete a Master's thesis (30 ECTS).

Program Core

Code	Subject	ECTS	Semester
CYBR5005E	Information Security Management - Governance, Risk and Compliance	6	1
CYBR5006E	Cyber threat analysis, research and education	6	1
CYBR5016E	Cybersecurity in Computing	6	1
CYBR5018E	Physical Security	6	1
CYBR5001E	Application security	6	2
CYBR5017E	Network Security	6	2
INFO6340E	Structural analysis of systems	6	2
MATH3345E	Mathematical statistics	6	2
CYBR5002E	Cloud security	6	3
CYBR5004E	Offensive Cybersecurity	6	3
CYBR5014E	Cyber Threat Intelligence	6	3
CYBR5019E	Manual Testing and Automation of Software	6	3
CYBR0007E	Master's project	30	4
	Total ECTS to be taken:	102	

Program Elective

Code	Subject	ECTS	
CYBR5008E	Cybersecurity Architecture and Management in the Microsoft Ecosystem	6	
CYBR5009E	AWS Cloud Infrastructure Security	6	
CYBR5010E	IAC (Infrastructure as Code) Terraform	6	
CYBR5011E	IAC (Infrastructure as Code) Bicep	6	
CYBR5020E	Operation System Linux	6	
MATH4119E	Cryptology	6	
INFO5226E	Flask	6	
INFO5249E	Agile-Software Development Project Management	6	
INFO5254E	IT Service Strategy and Design	6	
INFO5256E	Transition of IT Services	6	
INFO6212E	Personal data protection in the digital age	6	
INFO6260E	IT Project Management	6	
BLCH5145E	Security Methods in Blockchain and Cryptocurrency Systems სილაბუსი	6	

CYBR5012E	Incident response and forensics	6	
CYBR5015E	Logging and Monitoring	6	
INFO6263E	Big Data Systems	6	
INFO6270E	Artificial Intelligence Based Machine Learning Algorithms	6	
	Total ECTS to be taken:	18	

[Matrix Of Privequisites](#)

Point	GPA	The university assessment	The general assessment in Georgia	
97-100	4,00	A+	A	Excellent
94-96	3,75	A		
91-93	3,50	A-		
87-90	3,25	B+	B	Very good
84-86	3,00	B		
81-83	2,75	B-		
77-80	2,50	C+	C	good
74-76	2,25	C		
71-73	2,00	C-		
67-70	1,75	D+	D	Satisfactory
64-66	1,50	D		
61-63	1,25	D-		
51-60	1,00	E	E	Sufficient
Not passed				
41-50		FX	FX	Insufficient
<40		F	F	Failed