Caucasus University

New Jersey City University

Joint Bachelor's Degree Program in Cyber Security

Caucasus University
Caucasus School of Technology

Program Name		
Joint Program in Cyber Security		
Program Name In Georgian		
კიბერუსაფრთხოების ერთობლივი პროგრამა		
Degree level		
Bachelor's Degree		
Type of the educational program		
Academic		
Instruction Language		
English		
Expected Qualification		
Caucasus University	In English - Bachelor of Science in Computer Science	0613
	In Georgian - მეცნიერების ბაკალავრი კომპიუტერულ მეცნიერებაში	0613
New Jersey City University	In English - Bachelor of Science in Cyber Security	
	In Georgian - მეცნიერების ბაკალავრი კიბერუსაფრთხოებაში	
Date of Program Approval		
07 Oct. 2021		
Academic head of the Program		
Maksim Iavich, PhD., Affiliated Porfessor at Caucasus University		
Program Volume in Credit Hours		

200 ECTS (120 US credits) credits are envisaged to achieve the results of the Joint Bachelor's Program in Cybersecurity and the standard duration of the Program is 3 (three) academic years, the first two years (150 ECTS / 75 ECTS a year) at Caucasus University and the last 3rd year (50 ECTS / 30 US credits) at New Jersey City University (NJCU).

A credit is a unit for volume of work that is required from the students in terms of time spent. 1 ECTS credit is worth of 25 hours of student's academic workload (which includes class hours and time spent on independent work, midterm and final examinations, as well as homework assignments).

The program envisages learning courses of a narrow sphere and of free components:

Learning courses of a narrow sphere (185 ECTS credits):

- Mandatory learning courses -170 ECTS credits;
- Optional learning courses - 15 ECTS credits

Learning courses of free component (15 ECTS credits):

- University Mandatory learning courses - 10 ECTS credits;
- University Optional learning couses - 5 ECTS credits;

In case a foreign student attests the level of general English language proficiency defined by the program, he / she will be exempted from passing English language courses and will study the courses form the program's elective learning courses of free component.

Program Description

Admission Requirements

- Any person having a secondary education is entitled to enroll in the Undergraduate Program in Cybersecurity. The precondition for admission to the program is to pass the Unified National Examination. Any exceptions to the Law on Enrolment at Higher Education Institutions are allowed only in the cases prescribed by Law.
- Passing the English Language as a foreign language exam in the Unified National Examinations is a mandatory requirement for program enrollment.
- Prospective students eligible for the program without having passed the Unified National Examinations must confirm English language B2 level proficiency (IELTS-6.0; TOEFL-78; or other relevant international certificate confirming B2 level proficiency) or he/she has to pass an English language B2 level exam administered by the Caucasus University
- Mobility to the program is allowed in accordance with procedures set by the relevant law.

Program Objectives

The objectives of the Program in Cybersecurity are to:

- Provide the student with an in-depth knowledge of the theoretical aspects of higher education disciplines, which prepares the person for further study at the Master's degree program or work with a qualification.
- Provide students with the necessary knowledge, skills, and professional training to pursue careers in the rapidly growing field of Cybersecurity.
- Prepare high-level, competitive specialists with the broad theoretical knowledge and practice-oriented, transferable skills necessary for professional development in modern ICT field with the focus on security.
- To satisfy the demand of Cybersecurity workforce in the government and private industry.

Learning Outcomes

Upon completion of the Bachelor's degree program in Cybersecurity, the graduate will acquire the following competencies:

- Describes security design principles and identifies the security mechanisms to implement desired security principles.
- Analyzes complex computational problems and selects the appropriate algorithm for their solution.
- Applies the principles of programming, computer systems, the latest approaches and technological tools in practice.
- Evaluates the architecture of a typical, complex system and identifies potential risks, vulnerabilities , and points at which specific security technologies/ methods should be employed.
- Identifies which cryptographic protocols, tools and techniques are appropriate for a given situation.
- Identifies malicious activities and attacks in the system and recommends appropriate response capabilities.
- Executes incident response activities and helps to solve cyber-crime investigations.
- Appreciates and shares technology-related values, ethical and social responsibilities with others.

Building a Career

Program graduates will have an opportunity to work in a variety of environments such as industry, government, private and business organizations. As a rule, the work of graduates involves the following types of activities: analyzing problems for solutions, formulating and testing, working in teams for product development, penetration testing and protecting the organizations against cyber attacks . Examples of job titles of program graduates may include: System and Security Administrator, Software Developer, Computer Communications Specialist, Cyber security specialist, penetration tester, cryptographer etc.

Study Continuation Opportunities

The program graduates can continue their studies at any of Master's Degree programs in Georgia or abroad, in accordance with the regulation required by the law.

Program Curriculum

№	Course Code	Prerequisite	Course	Year						ECTS
				I		II		III		
				Semester						
				I	II	III	IV	V	VI	
Required Specialization Courses										
Mandatory learning courses - 170 ECTS										
1.	MATH 0003E		Calculus I	x						5
2.	DM 1140		Discrete Mathematics	x						5
3.	CARC 1140		Computer Architecture	x						5
4.	CSC 1140		Fundamentals of Computer Science I	x						5
5.	CSC 1142		Operating Systems & their Security Principles	x						5
6.	CSC 1143		Basics of practical Cyber Security	x						5
7.	MATH 0004E	MATH 0003E	Calculus II		x					5
8.	CSC 1241	CSC 1140	Fundamentals of Computer Science II		x					5
9.	PYTH 1240	CSC 1140	Python Programming I		x					5
10.	CSEC 1240		Computer Security I		x					5
11.	IDB 1240		Introduction to Database Systems		x					5
12.	SCMP 2140	MATH 0004E	Scientific Computing			x				5
13.	PST 2140	MATH 0003E	Probability & Statistics			x				5
14.	NTW 2140		Principles of Networking			x				5
15.	ALG 2140	CSC 1241	Algorithms & Data Structures			x				5
16.	CSEC 2141	CSEC 1240	Computer Security II			x				5
17.	CSEC 2142		Ethics in National Cyber Security			x				5
18.	SE 2140	CSC 1241	Software Engineering I			x				5
19.	CRPT 2241	SCMP 2140	Cryptography				x			5
20.	CSEC 2242	CSEC 1240	Hacking and forensic investigation				x			5

№	Course Code	Prerequisite	Course	Year						ECTS
				I		II		III		
				Semester						
				I	II	III	IV	V	VI	
21.	CSEC 2243	NTW 2140	Network Security				x			5
22.	AI 2241	ALG 2140	Artificial Inteligence				x			5
23.	PRP 2240	CSC 1241	Programming Paradigms				x			5
24.	CMP 2240	CSC 1241	Compilers				x			5
25.	SECU 345	CSEC 1240	Computer Forensics					x		5 (3 US cr.)
26.	SECU 460		Security and Privacy					x		5 (3 US cr.)
27.	SECU 422	CSEC 2141	Computer Security III					x		5 (3 US cr.)
28.	SECU TBD9	CSEC 2141	Cyber Incident Handling					x		5 (3 US cr.)
29.	SECU 400		Cybersecurity & Event Management					x		5 (3 US cr.)
30.	SECU 220		Contemporary International Security						x	5 (3 US cr.)
31.	SECU 323		Risk Management						x	5 (3 US cr.)
32.	SECU 340	CSEC 1240	Ethical Hacking						x	5 (3 US cr.)
33.	SECU 415	SECU 422	Intrusion Detection & Prevention						x	5 (3 US cr.)
34.	SECU 655		Computer Security Topics						x	5 (3 US cr.)
Optional learning courses - 15 ECTS										
35.	CSEC 1242		Ethical hacking of web systems I		x					5
36.	CSEC 1243		Intro to Intelligence							5
37.	CSEC 1244	CSC 1142	Intro to Linux administration							5
38.	PAR 2140		Principles of Parallel Programming			x				5
39.	CSEC 2143	CSEC 1242	Ethical hacking of web systems II							5
40.	PYTH 2140	PYTH 1240	Python Programming II							5
41.	WEB 2141	CSC 1140	Web Technologies I							5
42.	JAVA 2140	CSC 1241	Java Programming I							5
43.	NET 2141	CSC 1241	.NET Technologies I							5
44.	ITPM 2140		IT Project Management							5

№	Course Code	Prerequisite	Course	Year						ECTS
				I		II		III		
				Semester						
				I	II	III	IV	V	VI	
45.	SE 2240	SE 2140	Software Engineering II				x			5
46.	WEB 2241	WEB 2141	Web Technologies II							5
47.	DSY 2240	ALG 2140	Distributed Systems							5
48.	JAVA 2240	JAVA 2140	Java Programming II							5
49.	NET 2241	NET 2141	.NET Technologies II							5
50.	ML 2241	PST 2140	Machine Learning							5
Learning courses of free component										
University Mandatory learning courses - 10 ECTS										
51.	ENGL 0009E		General English C1.0	x						5
52.	ENGL 0010E	ENGL 0009E	General English C1		x					5
University Optional learning couses - 5 ECTS										
53.	ENTP 0009E		Entrepreneurship		x					5
			ECTS Credits Per Year	75		75		50		
			Courses Per Year	15		15		10		