4.4. Joint Bachelor's Program in Cyber Security

Joint Bachelor's Program in Cyber Security

www.cst.ge

Paata Saakadze street 1 Tbilisi, 0102, Georgia

2039 Kennedy Blvd Jersey City, New York, 07003, USA

Awarded Qualification: Caucasus University - Bachelor of Science in Computer Science; New Jersey City University - Bachelor of Science in Cyber Security (0613)	Program Admission Precondition: full secondary education and Results of Unified National Examinations; Passing the English Language as a foreign language at the Unified National Examinations is a mandatory requirement;
Language of Instruction: English	Possibility to Continue Studies: MA
Program Volume in Credits: 200 ECTS	duration of the program: 3 academic years

Program Objective: 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.

Program 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.

Areas of Employment: 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 tetsing 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, Consultant, Cyber security specialist, penetration tester, cryptographer etc.