PROJECT SUMMARY

Project ID	**CARYS-19-121**
Project Title	Cyber incident response platform for 5G cellular networks
Research sub direction / sub directions	2.2 Electrical engineering, electronic engineering
Host institution	Caucasus University
Web	www.cu.edu.ge
Name of the co-funding organization	-
Web	-
Co-funding	-
Project budget (Lari)	204330 GEL
Contribution of the foundation	204330 GEL
Contribution of the co-funding	-
Project duration (in month)	12

Personnel

N	Key Personnel Name , Surname	Position in the project	Academic Degree	Date of birth
1	Maksim Iavich	Principal Investigator	Doctoral/PhD, Ed.D or other equivalent	26.04.1985
2	Avtandil Gagnidze	Researcher	Doctoral/PhD, Ed.D or other equivalent	01.02.1959
3	Sergiy Gnatyuk	Researcher	Doctoral/PhD, Ed.D or other equivalent	11.01.1985
4	Roman Odarchenko	Researcher	Doctoral/PhD, Ed.D or other equivalent	02.05.1988
5	Giorgi Iashvili	Researcher	PhD student	04.06.1990
6	Shalva Khukhashvili	Researcher	Master student	06.02.1997

Project Summary

The telecoms industry is undergoing a major transformation towards 5G networks in order to fulfill the needs of existing and emerging use cases. Novel networking, service deployment, storage and processing technologies will be used to provide the necessary services envisioned by 5G. These technologies should bring a lot of new challenges for the 5G cybersecurity systems and its functionality. Therefore, it is highly important to investigate most important security challenges in 5G networks and propose the potential solutions that could lead to secure 5G systems. In these conditions, it is necessary immediately to define new architecture for the 5G and future 6G networks in order to provide novel AI/ML based algorithms which should give great opportunities to provide the highest cybersecurity level and to ensure mobile subscribers, industry, government etc. in overall safety of all processes and lives. That is why the main goal of the project is to develop novel 5G cybersecurity platform with new relevant for the modern and future society trust models, cryptographic algorithms, enhanced critical information infrastructure security etc. This platform will integrate User, Application, and Network Operator-provided preferences, rules, and parameter values to provide the best Cyber Security Level for the user while not compromising network and application providers' interests. The platform will also contribute to a higher quality of experience (QoE), reduces user and operator burden for different network devices security management, and keeps the device optimally securely connected. It allows users to define preferences and/or permissions for automatic management of connections and services, and allow application/service providers to better adjust application-level QoS to network conditions to result in higher QoE for their users. It also allows operators to retain control of the subscriber's use of the network and to give the best service possible at a specified price points.