



Co-funded by the  
Erasmus+ Programme  
of the European Union



ISSES – Information Security Services  
Education in Serbia

Supported by the Erasmus+ Capacity Building in  
the field of Higher Education (CBHE) grant  
N° 586474-EPP-1-2017-1-RS-EPPKA2-CBHE-JP

# Serbian Cybersecurity Challenge 2020 – From zero to hero

## Opis projekta v1.2 / Project Description v1.2

<b>Autori/organizacije:</b>	<b>Authors/organizations:</b>
Imre Lendak / UNS Igor Tartalja, Žarko Stanisavljević, Pavle Vuletić / ETF Viktor Varga / UT	Imre Lendak / UNS Igor Tartalja, Žarko Stanisavljević, Pavle Vuletić / ETF Viktor Varga / UT
<b>Datum objavljivanja:</b>	<b>Release date</b>
TBD	TBD
<b>Relevantni Erasmus+ radni paketi:</b>	<b>Relevant Erasmus+ Work Packages:</b>
WP6 – Dissemination & Exploitation	WP6 – Dissemination & Exploitation
<b>Kratak opis:</b>	<b>Short description:</b>
Opis programa I projekta Serbian Cybersecurity Challenge 2020	Serbian Cybersecurity Challenge 2020 project and program description
<b>Ključne reči:</b>	
Cybersecurity challenge, sajber izazov, hakaton, Srbija, 2020	Cybersecurity challenge, hackathon, Serbia, 2020

*The European Commission support for the production of this publication does not constitute endorsement of the contents which reflects the views only of the authors, and the Commission cannot be held responsible for any use which may be made of the information contained therein.*



Co-funded by the  
Erasmus+ Programme  
of the European Union



ISSES – Information Security Services  
Education in Serbia

Supported by the Erasmus+ Capacity Building in  
the field of Higher Education (CBHE) grant  
N° 586474-EPP-1-2017-1-RS-EPPKA2-CBHE-JP

<b>Verzije dokumenta / Document versions:</b>				
<b>Version</b>	<b>Date</b>	<b>Author(s)</b>	<b>Status</b>	<b>Opis / Description</b>
V1.0	Dec 13, 2019	Imre Lendak	Draft	Opis projekta, partneri i plan / Project, partner and plan descriptions
V1.1	Feb 5, 2020	Imre Lendak	Release	English translation added. Minor clarifications and updates.
V1.2	Feb 6, 2020	Igor Tartalja	Release	Clarifications in sections 2 and 4



Co-funded by the  
Erasmus+ Programme  
of the European Union



ISSES – Information Security Services  
Education in Serbia

Supported by the Erasmus+ Capacity Building in  
the field of Higher Education (CBHE) grant  
N° 586474-EPP-1-2017-1-RS-EPPKA2-CBHE-JP

## CONTENTS

1	Uvod / Introduction .....	4
2	Plan projekta i implementacije / Project plan and implementation .....	5
2.1	Opšti ciljevi / Project goals .....	5
2.2	Ciljne grupe učesnika / Target stakeholder groups.....	5
2.3	Faze implementacije / Implementation phases .....	6
2.4	Metodologija i sadržaj treninga / Training methodology and content .....	7
2.5	Nagrade i rodna ravnopravnost / Prizes and gender equality .....	8
3	Ključni partneri programa / Key project partners .....	<u>10</u>
4	Detaljan plan projekta / Detailed project plan.....	<u>12</u>

Deleted:

Deleted:



Co-funded by the  
Erasmus+ Programme  
of the European Union



ISSES – Information Security Services  
Education in Serbia

Supported by the Erasmus+ Capacity Building in  
the field of Higher Education (CBHE) grant  
N° 586474-EPP-1-2017-1-RS-EPPKA2-CBHE-JP

## 1 Uvod / Introduction

Ovaj dokument sadrži opis događaja Serbian Cybersecurity Challenge 2020 (SCC 2020) sa podnaslovom “From zero to hero”. Ovaj projekat je element programa čija je održivost planirana za duži niz godina, tj. sam projekat neće biti ograničen na 2020. godinu.

Uvođenje ovakvog programa je od izuzetnog značaja za jačanje kompetentnosti R. Srbije na polju sajber bezbednosti, kao i smanjivanja postojećeg manjka kvalifikovane radne snage u ovoj oblasti. Veličina manjka te radne snage se procenjuje na ~290,000 na teritoriji Evrope.

This document contains the description of the Serbian Cybersecurity Challenge 2020 (SCC 2020), with subtitle „From zero to hero“. The 2020 event is planned to initiate a sustainable sequence of similar events, i.e. the event is not limited for execution in 2020 only.

The introduction of this event is of utmost importance towards improving the cybersecurity capabilities of the Republic of Serbia, as well as in the process of answering the existing lack of skilled cybersecurity professionals. The extent of that missing workforce is estimated to be ~290,000 in Europe.



## 2 Plan projekta i implementacije / Project plan and implementation

### 2.1 Opšti ciljevi / Project goals

<p>Strateški ciljevi projekta SCC 2020 su (1) promocija oblasti sajber bezbednosti, odnosno (2) identifikacija, privlačenje, edukacija i zadržavanje mladih talenata sa ciljem smanjenja tržišnog manjka eksperata u oblasti sajber bezbednosti.</p>	<p>The strategic goals of SCC 2020 are (1) the promotion of cybersecurity and (2) identification, inclusion, education and retention of young talents with the ultimate goal of lowering the cybersecurity workforce shortage in Serbia, in the government, non-government and private sectors.</p>
<p>Operativni ciljevi u 2020. godini su uključivanje barem 50 talentovanih studenata osnovnih i master akademskih, odnosno strukovnih studija u edukativni i takmičarski deo programa. Ovaj broj je minimalno potreban na godišnjem nivou za popunjavanje nepopunjenih pozicija iz oblasti sajber bezbednosti na tržištu rada u sledećim sektorima: privatni, državni, nevladin i akademsko-istraživački. Konkretni ciljevi su sledeći:</p> <ul style="list-style-type: none"> <li>• Stimulisanje interesovanja za užu oblast sajber bezbednosti, odnosno širu oblast računarstva;</li> <li>• Identifikacija mladih talenata i njihov trening sa ciljem opšteg unapređenja kapaciteta u sajber bezbednosti na teritoriji Republike Srbije.</li> <li>• Podizanje svesti uključenih studenata i drugih učesnika o trenutnom manjku eksperata u oblasti sajber bezbednosti i značaju edukacije i pozitivnom uticaju uvođenja novih i unapređenja postojećih edukativnih programa u ovoj oblasti;</li> <li>• Povezivanje mladih talenata sa potencijalnim poslodavcima;</li> </ul>	<p>The operational goals of SCC 2020 are the inclusion of at least 50 talented Bachelor and Master-level students in the training and competition parts of the event. This number (i.e. 50) is estimated to be the minimum number of necessary new experts entering the cybersecurity workforce in the R. of Serbia in the following sectors: private, government, non-government (NGO) and academic/research. The specific operational goals are the following:</p> <ul style="list-style-type: none"> <li>• Stimulate interest for the fields of cybersecurity and computer science in general;</li> <li>• Identification of young talents and their training towards capacity building in the field of cybersecurity in Serbia;</li> <li>• Awareness raising campaign for students and other participants about the current workforce shortage in the field of cybersecurity and the importance of education and introduction of novel courses and training programs in this novel and very competitive field;</li> <li>• Connecting young talent with potential employers;</li> </ul>
<p>Učešće u programu SCC 2020 je besplatno za studente. Organizaciju potrebnih treninga, odnosno sprovođenje sajber izazova se realizuje uz pomoć sponzora iz privatnog i državnog sektora, odnosno uz podršku Erasmus+ projekta “Information Security Services Education in Serbia (ISSES)”.</p>	<p>Participation in the SCC 2020 program is free for students. The organization of trainings and implementation of cyber challenges (i.e. hackathons) will be supported by sponsors from the private and government sectors, as well as through the “Information Security Services Education in Serbia (ISSES)” Erasmus+ project.</p>

### 2.2 Ciljne grupe učesnika / Target stakeholder groups

<p>Planom projekta je predviđeno da se u program sajber izazova uključe studenti osnovnih i master akademskih,</p>	<p>The program will be open to Bachelor and Master-level students who study at either state-funded or privately-</p>
--	--



<p>odnosno strukovnih studija koji imaju aktivan studentski status u državnim, odnosno privatnim visoko-školskim institucijama akreditovanim na teritoriji Republike Srbije.</p>	<p>owned Higher Education Institutions (both universities and colleges) on the territory of Serbia.</p>
<p>U 2020. godini jezgro grupe učesnika će činiti profesori-treneri i studenti sledećih institucija partnera u okviru Erasmus+ projekta Information Security Services Education in Serbia (ISSES):</p> <ul style="list-style-type: none"> <li>• Elektrotehnički fakultet (ETF), Univerzitet u Beogradu;</li> <li>• Fakultet organizacionih nauka (FON), Univerzitet u Beogradu;</li> <li>• Elektronski fakultet (EF), Univerzitet u Nišu;</li> <li>• Visoka tehnička škola strukovnih studija Subotica (VTŠ);</li> <li>• Fakultet tehničkih nauka (FTN), Univerzitet u Novom Sadu.</li> </ul>	<p>In 2020 the core group of participants will consist of professors-trainers and students coming from the partner institutions which are members of the Information Security Services Education in Serbia (ISSES) Erasmus+ project, namely:</p> <ul style="list-style-type: none"> <li>• School of Electrical Engineering (ETF), University of Belgrade;</li> <li>• Faculty of Organizations Sciences (FON), University of Belgrade;</li> <li>• Faculty of Electronic Engineering (EF), University of Nis;</li> <li>• Subotica Tech – College of Applied Sciences (VTS);</li> <li>• Faculty of Technical Sciences (FTN), University of Novi Sad;</li> </ul>
<p>Pored jezgra projekta planom projekta je predviđeno da se u program po pozivu uključe profesori i studenti sledećih dodatnih visoko-školskih institucija:</p> <ul style="list-style-type: none"> <li>• Kriminalističko-policijska univerzitet (KPU), Beograd;</li> <li>• Fakultet tehničkih nauka, Univerzitet u Kragujevcu;</li> <li>• Fakultet bezbednosti, Univerzitet u Beogradu;</li> <li>• Univerzitet odbrane, Beograd;</li> <li>• Belgrade Metropolitan Univerzitet, Beograd;</li> </ul>	<p>Besides the institutions forming the core team of the program, it is envisaged that the professors and students of the following Serbian HEIs will be invited as well:</p> <ul style="list-style-type: none"> <li>• The Academy of Criminalistic and Police Studies (KPA), Belgrade;</li> <li>• Faculty of Technical Sciences (UKG), University of Kragujevac;</li> <li>• Faculty of Security Studies, University of Belgrade;</li> <li>• University of Defense, Belgrade;</li> <li>• Belgrade Metropolitan University, Beograd;</li> </ul>
<p>Učešće u programu će biti omogućeno svim zainteresovanim studentima. Organizatori zadržavaju pravo da izvrše pred-selekciju kandidata preko posebno dizajniranih upitnika ukoliko broj prijavljenih kandidata premaši kapacitet infrastrukture na kojoj će se program realizovati.</p> <p>Srednjeročni plan razvoja programa predviđa uključenje talentovanih učenika srednjih škola u kasnijim godinama, najranije počevši od kalendarske 2021. godine.</p>	<p>All interested students will be able to participate in the event. The organizers retain the rights to perform a pre-selection process via purpose-built questionnaires or other means, should the number of applied candidates surpass the capacity of the infrastructure used to implement the program.</p> <p>The mid-term plan of the program is to include talented high-school pupils in the following events, but not earlier than in year 2021.</p>

## 2.3 Faze implementacije / Implementation phases



<p>Program se implementira u sledećim fazama:</p> <ul style="list-style-type: none"> <li>• Faza I: Uključivanje partnera i sponzora iz državnog, privatnog, nevladinog i akademsko-istraživačkog sektora. Potpisivanje memoranduma o saradnji i ugovora o sponzorstvu.</li> <li>• Faza II: Razvoj trening materijala i izvođenje treninga kao pripreme za sajber izazove. Izbor izazova i/ili njihova priprema od strane profesora i predstavnika ostalih uključenih sektora, npr. privatnih kompanija. Izbor timova za polu-finale.</li> <li>• Faza III: Polu-finale sajber izazova organizovan na Avatao cloud-baziranoj platformi, koja omogućava studentima učesnicima udaljen pristup i rešavanje izazova u periodu od 1 do 7 dana. Polu-finale omogućava izbor najtalentovanijih učesnika. Ova faza se održava u paraleli u većem broju gradova na teritoriji R. Srbije. Predviđen datum ovog dela programa je 28-29. mart 2020. godine.</li> <li>• Faza IV: Priprema infrastrukture i izazova za finale projekta SCC 2020. Dodatni treninzi za pojedince i timove studenata.</li> <li>• Faza V: Finale sajber izazova. Biće organizovano u posebno pripremljenim učionicama. Umesto cloud-baziranih izazova će se koristiti IKT infrastruktura posebno pripremljena za potrebe vežbe. Studenti će pored samostalnih izazova biti u prilici da rešavaju timske izazove, npr. Red vs Blue Team vežbe. Predviđen datum ovog dela programa je 21-25. septembar 2020. godine.</li> </ul>	<p>The program is implemented in the following phases:</p> <ul style="list-style-type: none"> <li>• Phase I: Partnership and sponsor agreements with entities in the government, private, non-government and academic-research sectors. Collection of signed memorandums of understanding and sponsorship contracts.</li> <li>• Phase II: Development of training materials. Training the teams in the Higher Education Institutions. Choosing and/or preparing the challenges by professors and other parties, e.g. representatives of the private sector. Choosing teams for the semi-final.</li> <li>• Phase III: Hackathon semi-final on the Avatao cloud-based platform. This platform allows students remote access and parallel work on the challenges in a pre-defined period of 1 to 7 days. The semi-final allows the organizers to select the most talented participants. This phase will be carried out simultaneously in multiple cities in Serbia. The planned dates of the semi-final are March 28-29, 2020.</li> <li>• Phase IV: Infrastructure design and implementation for the SCC 2020 hackathon finals. Additional trainings for individuals and teams of students.</li> <li>• Phase V: SCC 2020 hackathon finals and debriefing. This phase will be implemented on-site and supported by a purpose-built infrastructure. It is envisaged that the students will be able to participate in individual, capture-the-flag (CTF) and Red team vs Blue team exercises. The planned dates of the finals are September 21-25, 2020.</li> </ul>
--	---

## 2.4 Metodologija i sadržaj treninga / Training methodology and content

<p>Razvoj trening materijala je zajednička akcija profesora i instruktora uključenih u program. Planirani format izvođenja treninga će biti u učionicama u okviru visoko-školskih institucija i to u sledećim koracima:</p> <ol style="list-style-type: none"> <li>1. 30-45 minuta predavanja o određenoj temi,</li> </ol>	<p>The training materials will be developed jointly by the professors and instructors involved in the program. The trainings will be delivered in the lecture rooms of the higher education institutions in the following steps:</p> <ol style="list-style-type: none"> <li>1. 30-45 minutes of lectures on a specific topic,</li> </ol>
--	--



<p>npr. kriptografija, veb, reverzni inženjering, rad sa memorijom.</p> <ol style="list-style-type: none"> <li>2. Prikaz rešenja jednog ili više lakših izazova koji studenti pasivno prate.</li> <li>3. Studenti samostalno rešavaju još barem 2-3 scenarija. Ukoliko ne stignu da ih reše tokom vremena odvojenog za rešavanje izazova, onda nastavljaju rešavanje kod kuće.</li> </ol> <p>Visoko-školske institucije koje učestvuju u programu imaju potpunu slobodu da prilagode ovu metodologiju sopstvenim mogućnostima i potrebama, odnosno nivou znanja studenata.</p>	<p>e.g. cryptography, web, reverse engineering, memory corruption.</p> <ol style="list-style-type: none"> <li>2. Demonstration of one or more easier challenges and their solution by the professors and/or instructors which is passively followed by students.</li> <li>3. The students solve at least 2-3 additional scenarios on their own. If they do not succeed to solve these challenges in the allotted time, then the students solve them individually at home,</li> </ol> <p>The Serbian HEIs involved in the program are free to streamline the above methodology and align it with their needs and capabilities, as well as with the skill and knowledge of their students.</p>
--	--

## 2.5 Nagrade i rodna ravnopravnost / Prizes and gender equality

<p>U cilju motivisanja što većeg broja studenata da se uključe u program, predviđene su sledeće mere:</p> <ul style="list-style-type: none"> <li>• Nagrade za najbolje plasirane učesnike u finalu. Nagrade obezbeđuju sponzori programa. Potencijalni vidovi nagrada: sitna računarska oprema (tablet, mobilni telefon, monitori), stipendije za treninge iz sajber bezbednosti u lokalnim trening centrima, stipendije za odlazak na kratkotrajne posete, odnosno master studije kod (inostranih) partnera.</li> <li>• Najbolje plasirani studenti koji učestvuju u programu će moći da dobiju dodatne bodove za predmete iz oblasti informacione bezbednosti.</li> <li>• Gemifikacija uvođenjem dešbordova na kojima se prikazuju najbolje plasirani studenti, bedževi za učesnike koji se iskažu u određenim oblastima (npr. najbolji kripto ili veb hakeri), međusobno takmičenje između visoko-školskih institucija.</li> <li>• Mogućnost formiranja timova i odlaska na slične događaje u susednim državama, npr. Severna Makedonija.</li> </ul>	<p>The following dissemination and motivation techniques are envisaged with the final goal to motivate the largest possible number of students to participate in the program:</p> <ul style="list-style-type: none"> <li>• Prizes for the best-performing students in the finals. The prizes will be provided by the partners and sponsors. Potential types of prizes: small computing equipment (tablets, mobile phones, monitors), scholarships for trainings in the field of cybersecurity provided by local training providers, scholarships for short-term stays at (international) partners or for attending Master programs abroad.</li> <li>• Best performing students participating in the program will be able to receive additional credit in cybersecurity courses delivered at the partner HEIs.</li> <li>• Gamification through dashboards, which show the highest-ranking students, badges for participants who perform particularly well in certain fields (e.g. best in crypto or web hacking), inter-HEI competition.</li> <li>• Possibility to form teams and attend similar events abroad, e.g. in North Macedonia.</li> </ul>
<p>Organizatori programa će implementirati dodatne mere</p>	<p>The program organizers will implement additional</p>



Co-funded by the  
Erasmus+ Programme  
of the European Union



**ISSES** – Information Security Services  
Education in Serbia

*Supported by the Erasmus+ Capacity Building in  
the field of Higher Education (CBHE) grant  
N° 586474-EPP-1-2017-1-RS-EPPKA2-CBHE-JP*

<p>za uključivanje što većeg broja studentkinja. Predviđene su posebne, garantovane nagrade za sve učesnice, nagrade za timove koji uključuju članice, odnosno vredne nagrade za najbolje plasirane učesnice.</p>	<p>measures for the inclusion of the highest possible female participants. The organizers plan to award guaranteed prizes to female participants, as well as valuable prizes for the best-performing female participants.</p>
---	---



### 3 Ključni partneri programa / Key project partners

<p>U cilju postizanja ciljeva programa SCC 2020, predviđeno je uključivanje sledećih ključnih partnera:</p> <ul style="list-style-type: none"> <li>• Ministarstvo trgovine, turizma i telekomunikacija (MTT) – nadležno ministarstvo za oblast sajber bezbednosti, sa sledećim organizacionim jedinicama:             <ul style="list-style-type: none"> <li>○ Regulatorna agencija za elektronske komunikacije i poštanske usluge (RATEL);</li> <li>○ Nacionalni CERT;</li> </ul> </li> <li>• Ministarstvo prosvete i nauke (MPN) – nadležno ministarstvo za oblast visokog školstva;</li> <li>• Ministarstvo unutrašnjih poslova (MUP);</li> <li>• Ministarstvo odbrane (MOD);</li> <li>• Visoko-školske institucije akreditovane na teritoriji R. Srbije;</li> <li>• Inostrani partneri, npr. Makedonski nacionalni CERT;</li> <li>• Javno-privatno partnerstvo u oblasti sajber bezbednost „Petnička grupa“ i predstavnici nevladinog sektora (npr. DCAF);</li> <li>• Fondacija Sajber heroj (FSH).</li> </ul>	<p>The following group of core partners will be invited to support SCC 2020 and thereby ensure that its goals are reached:</p> <ul style="list-style-type: none"> <li>• Ministry of Trade, Tourism and Telecommunications, the competent ministry for the field of cybersecurity, with its following units:             <ul style="list-style-type: none"> <li>○ Regulatorna agencija za elektronske komunikacije i poštanske usluge (RATEL);</li> <li>○ National CERT;</li> </ul> </li> <li>• Ministry of Education, Science and Technological Development – competent ministry for the field of higher education;</li> <li>• Ministry of Internal Affairs;</li> <li>• Ministry of Defence;</li> <li>• Higher Education Institutions accredited in Serbia;</li> <li>• International organizations, e.g. the National CERT of North Macedonia;</li> <li>• „Petnička grupa“ public-private partnership and representatives of other relevant NGOs;</li> <li>• Foundation “Cyber Hero”.</li> </ul>
<p>Ministarstva i državna tela potpisuju sporazume podrške i uključuju program SCC 2020 u njihove marketing aktivnosti u skladu sa mogućnostima. Po potrebi obezbeđuju fizički prostor (npr. sale, učionice) za implementaciju programa.</p>	<p>The Ministries and other government institutions sign memorandums of support/understanding and incorporate SCC 2020 into their marketing activities where applicable. If able, they provide physical space (e.g. rooms, halls) for the implementation of the program.</p>
<p>Visoko-školske institucije (VŠI) takođe potpisuju sporazum podrške i uključuju program SCC 2020 u njihove marketing aktivnosti. Omogućavaju profesorima izvođenje potrebnih treninga i pružaju neophodnu, ne-finansijsku podršku. Profesori i ostali treneri učestvuju u izradi izazova i pripremi potrebne IKT infrastrukture. VŠI učestvuju u realizaciji programa i sa finansijske strane uključivanjem programa u planove diseminacije, eksploatacije i održivosti njihovih kako nacionalnih, tako i internacionalnih programa u oblasti sajber bezbednosti.</p>	<p>Higher education institutions (HEI) sign memorandums of support/understanding and incorporate SCC 2020 into their marketing activities where applicable. They allow their professors to carry out the necessary trainings and provide any needed, but non-financial support. Professors and other trainers participate in challenge and infrastructure preparation. HEIs might provide financial support to the program by including it in their dissemination, exploitation and sustainability plans in the fields of both national and international programs in the field of cybersecurity. One example of</p>



<p>Kao konkretan primer ovakve podrške, predviđeno je da Erasmus projekat ISSES<sup>1</sup> podrži program sa marketinške strane i isplatom dela honorara trenera/profesora, odnosno troškova putovanja članova projektnog tima potrebna za realizaciju ovog programa.</p>	<p>such support for the program will be implemented as part of the ISSES Erasmus+ project, which will support the dissemination activities as far as provide partial financial coverage for the trainers/professors involved in the training activities, as well as their travel costs incurred as part of the program.</p>
<p>Privatne kompanije potpisuju ugovore o sponzorstvu i/ili memorandume o saradnji sa Fondacijom Sajber heroj. Učestvuju u izgradnji potrebne IKT infrastrukture preko njihovih kontakata sa pružaocima usluga i proizvođačima opreme. Učestvuju u izradi samih izazova.</p>	<p>Private companies sign sponsorship contracts and/or memorandums of understandings with Foundation “Cyber Hero”. They take part in implementing the necessary IT infrastructure via relying on their partners and equipment vendors. They participate in the development of challenges as well.</p>
<p>Inostrani partneri učestvuju u programu u svojstvu posmatrača. Omogućavaju učešće odabranih timova studenata iz R. Srbije učešće u njihovim sličnim programima, npr. sajber izazov koji organizuje makedonski nacionalni CERT u 2020. godini, odnosno ITU vežba koja je planirana za jun 2020. godine u Skoplju.</p>	<p>International partners participate in the program as spectators. They also allow chosen student teams from Serbia to participate in similar programs organized by them, e.g. the hackathon organized by the CERT of North Macedonia in 2020, or the exercise organized by ITU in June 2020, also in North Macedonia.</p>
<p>Predstavnici „Petničke grupe“ javnog-privatnog i nevladinog sektora pružaju finansijsku i medijsku podršku programu. Imaju aktivnu ulogu u internacionalizaciji događaja i povezivanja sa sličnim inicijativama u regionu, Evropi i u svetu. Dodatno, oni učestvuju i u izradi samih izazova.</p>	<p>The representatives of the „Petnička grupa“ public-private partnership and other non-government organizations offer financial and support via mass media. They have an active role in the internationalization of the program in the region, Europe and worldwide. Additionally, they participate in challenge preparation.</p>
<p>Fondacija Sajber heroj je koordinator programa SCC 2020. Potpisuje sporazume o saradnji sa ministarstvima i državnim telima i ugovore o sponzorstvu programa sa privatnim kompanijama, nevladinim sektorom i državnim institucijama. Kroz sponzorstva obezbeđuje potrebna sredstva za zakup potrebne cloud-bazirane ili <i>onsite</i> infrastrukture i servisa za implementaciju programa, usluge marketinga, nagrade za studente, predviđena službena putovanja i honorare trenera i administratora programa.</p>	<p>SCC 2020 is coordinated by Foundation “Cyber Hero”. It signs memorandums of understandings with Ministries and other government institutions, as well as sponsorship agreements with private companies, NGOs and government institutions. The sponsorships allow it to finance the necessary cloud-based or on-site IT infrastructure and services necessary for program implementation, marketing services, prizes for the students, necessary travel and salaries for the trainers and program organizers/administrators.</p>

<sup>1</sup> <https://isses.etf.bg.ac.rs>

