ANALIZA OBRAZOVNOG SISTEMA U OBLASTI SAJBER BEZBJEDNOSTI U CRNOJ GORI
ANALYSES OF CYBER SECURITY EDUCATIONAL SYSTEM IN MONTENEGRO

Jelena Ljucović, Ivana Ognjanović, *Univerzitet Mediteran, Crna Gora*
Ramo Šendelj, *Univerzitet Donja Gorica, Crna Gora*

Sadržaj: *Jedan od glavnih izazova savremenog društva jeste efikasan razvoj sajber bezbjednosti na nacionalnom, regionalnom i globalnom nivou. U tom cilju, aktivnosti moraju da objedine raspoložive snage i obezbijede kako istraživačke aktivnosti usmjerene ka razvoju inovativnih alata i tehnika, tako i usklađene pravne okvire, visoko edukovane stručnjake i visok nivo svijesti građanstva u cjelini, što vodi ka povećanju opšte bezbjednosti na nacionalnom nivou. Crna Gora je u prethodnom periodu preuzela mnoge aktivnosti za implementaciju evropskih standarda i praksi, a u ovom radu se predstavlja analiza razvijenog sistema sajber bezbjednosti s posebnim naglaskom na sistem obrazovanja (formalnog i neformalnog) koji predstavlja jedan od ključnih preduslova za razvoj u ovoj oblasti.*

Abstract: *One of the main challenges of modern society is the efficient development of cyber security on the national, regional and global level. With this goal in mind, the activities need to consolidate the available strengths and provide both research activities aimed at developing innovative tools and techniques, as well as synchronized legal framework, highly educated experts and a high level of awareness of citizens in general, which leads towards the increase of the level of general security on the national level. Montenegro has undertaken various activities in the previous period on implementing European standards and practices, and in this paper the analysis of developed systems of cyber security is presented, with a special emphasis on the education system (formal and informal) which presents one of the key prerequisites in this area.*

1. UVOD

Jedan od glavnih izazova savremenog društva jeste efikasan razvoj sajber bezbjednosti na nacionalnom, regionalnom i globalnom nivou [3]. Potreba za kreiranjem visokog nivoa sigurnosti u upotrebi informaciono-komunikacionih tehnologija (engl. information-communication technology-ICT) je definisana u Digitalnoj Agendi Evrope (engl. Digital Agenda for Europe-DAE), u maju 2010.god [4]. DAE naglašava neophodnost ujedinjavanja svih raspoloživih snaga kako bi se osigurala sigurnost i otpornost ICT infrastrukture, i to istovremenim fokusiranjem na preventivne i reaktivne akcije i izazove, kao što su: (i) prevencija i upravljanje rizicima, i (ii) razvoj efekasnog i koordinisanog menahizma za odgovor na nove i sve više sofisticirane forme sajber napada i sajber kriminala.

S tim u cilju, Evropski Parlament (engl. Europpean Parlament) je preuzeo mnoge aktivnosti, kao što su: kreiranje Agencije za Informacionu bezbjednost i Evropsku mrežu (engl. Euroepan Network and Information Security Agency-ENISA) (regulativa br 460/2004), Strategija za sigurno informaciono društo Evrope (engl. Secure Information Society) [7] iz 2007.god, i mnoge druge. Takođe, zemlje članice Evropske Unije, kao i ostale razvijenije zemlje na globalnom nivou (kao što su Sjedinjene Američke Države, Rusija, Kina, itd.) su uspostavile pravne okvire za borbu sa izazovima sajber bezbjednosti. Ipak, borba u sajber prostoru zahtijeva sveobuhvatne pristupe i akcije, koji obuhvataju: razvoj i upotrebu sofisticiranih alata i tehnika, edukovane stručnjake koji mogu da uspostave odgovarajuće organizacione strukture na institucionalnom i državnom nivou, eksperte iz oblasti sajber bezbjednosti koji će kontinuirano raditi na poboljšanju i osavremenjavanju mehanizama, kao i edukovane građane u cjelini, koji će svojim svakodnevnim aktivnostima povećati nivo opšte bezbjednosti na nacionalnom nivou.

U ovom radu se analizira trenutni nivo sajber bezbjednosti u Crnoj Gori, s posebnim naglaskom na sistem obrazovanja (uključujući i formalno i neformalno obrazovanje), kao i poredbenoj analizi sa EU preporukama i praksom.

2. PRAVNI I INSTITUCIONALNI OKVIRI SAJBER BEZBJEDNOSTI U CRNOJ GORI

Od 2005. godine, Crna Gora je kroz reformu krivičnog zakonodavstva počela sa kreiranjem institucionalnih i pravnih okvira, koji sprečavaju bilo kakvu vrstu slučajnog ili namjernog ometanja i onesposobljavanja informacionog sistema [16]. Usvajanje novih i unapređenje postojećih zakona i podzakonskih akata, predstavlja ključni element za postojanje informacione bezbjednosti u Crnoj Gori.

Pravni akti, koji predstavljaju osnovu za funkcionisanje i dalji razvoj savremenog koncepta informacione bezbjednosti u Crnoj Gori su: Krivični zakonik [5]; Zakon o krivičnom postupku [6]; Zakon o informacionoj bezbjednosti [8]; Zakon o Agenciji za nacionalnu bezbjednost [9]; Zakon o tajnosti podataka [10]; Zakon o elektronskom potpisu [11]; Zakon o elektronskim komunikacijama [12]; Zakon o elektronskoj trgovini [13]; Strategija sajber bezbjednosti Crne Gore 2013-2017 [14] i Pravilnik sa detaljnim uslovima i načinima sprovođenja mjera IT zaštite tajnih podataka [15].

"*Strategija sajber bezbjednost Crne Gore od 2013. do 2017. god*" usvojena je 12. septembra 2013. godine i predstavlja krucijalni dokument za sprovođenje sajber

bezbijednosti na nacionalnom nivou. Ova strategija definiše sedam ključnih oblasti sajber bezbjednosti za Crnu Goru: (1) Definisanje institucionalne i organizacione strukture u oblasti sajber bezbjednosti u zemlji; (2) Zaštita kritične informacione infrastrukture u Crnoj Gori; (3) Jačanje kapaciteta policijskih organa; (4) Reakcija na incidente; (5) Uloga Ministarstva odbrane Crne Gore u sajber prostoru; (6) Javno-privatna partnerstva; (7) Podizanje svijesti ljudi i zaštita pri korišćenju Interneta.

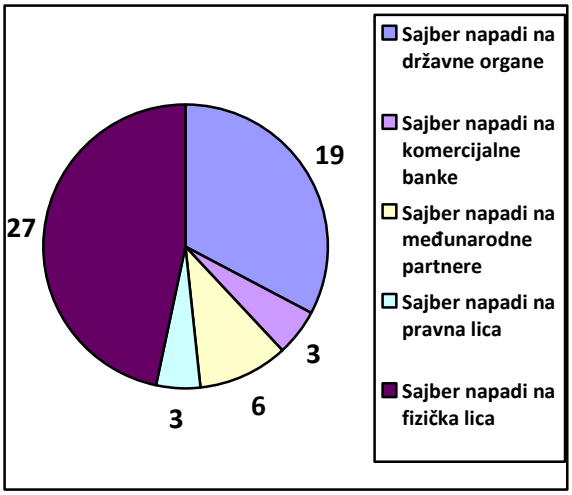
Da bi se na najefikasniji i dugoročno održiv način osiguralo pravilno upravljanje informacionom bezbjednošću u Crnoj Gori unutar javne uprave, neophodna je jasno definisana organizaciona hijerarhija, koja u Crnoj Gori obuhvata odgovornosti sljedećih institucija: (i) Ministarstvo informacionog društva i telekomunikacija (Nacionalni CIRT); (ii) Ministarstvo odbrane; (iii) Ministarstvo unutrašnjih poslova; (iv) Ministarstvo pravde; (v) Agencija za nacionalnu bezbjednost; (vi) Policijski organi; (vii) Direkcija za zaštitu tajnih podataka; (viii) Univerziteti u Crnoj Gori.

Nacionalni CIRT[1] predstavlja centralno tijelo u Crnoj Gori za koordinaciju i razmjenu podataka, odbranu od sajber napada i uklanjanje posljedica sajber napada. CIRT u okviru svog djelovanja sprovodi proaktivne i reaktivne mjere. Proaktivnim mjerama se djeluje prije incidenata i drugih događaja koji mogu ugroziti sigurnost informacionih sistema, a u cilju sprječavanja ili ublažavanja mogućih šteta. Dok, reaktivnim mjerama pruža pomoć u otkrivanju počinioca i vraćanju sistema u funkcionalno stanje. Glavne usluge koje CIRT pruža svojim korisnicima su: identifikacija incidenata, odgovor na njih i koordinacija. Da bi se na incidente odgovorilo na najefikasniji način, CIRT ima dobru saradnju i razmjenu informacija sa ključnim institucijama u oblasti sajber bezbjednosti. To se prije svega odnosi na saradnju državnih institucija sa institucijama u privatnom sektoru (Internet provajderima, agentima ".me" domena, mobilnim operaterima, bankarskim sektorom, Elektrodistribucijom, Poštom, itd.). Statistički pregled prijavljenih sajber incidenata u 2014. Godini je prikazan na Slici 1.

Ministarstvo odbrane. Imajući u vidu da ICT igra veliku ulogu u vojnim operacijama, potrebno je razviti objekte povezane sa vojskom u cilju zaštite sajber prostora Crne Gore. Svi moderni vojni objekti današnjice širom svijeta su priključeni na sajber prostor. Na primjer, prema izveštajima NATO-a [14], oko 120 zemalja ima usko povezanu vojsku sa sajber prostorom. S obzirom da strateški cilj Crne Gore predstavlja Evroatlansku integraciju, njime Crna Gora usvaja politku sajber zaštite u skladu sa NATO standardima.

Ministarstvo unutrašnjih poslova. Osnovni cilj Ministarstva unutrašnjih poslova u oblasti sajber bezbjednosti je osposobljavanje specijalizovanih jedinica u okviru Uprave policije, koje bi mogle da se bore sa bilo kojom vrstom sajber kriminala, omogućavanje nesmetanog procesuiranja krivičnih napada na kompjuterske podatake i sisteme, kao i druge protivzakonite radnje koje se mogu uraditi uz pomoć računara.

Policijski organi. Stalno unapređenje nivoa sofisticiranosti sajber prijetnji i napada, kao i njihovih metoda i tehnika zahtijeva kontinuirano jačanje kapaciteta policijskih organa u cilju efikasnijeg odgovora na širok spektar sajber prijetnji. Policijski organi i tužioci treba da budu u stanju da sprovedu istragu i krivično procesuiraju napade na kompjuterske sisteme, kao i na prekršaje načinjene uz pomoć računara, te da postoji elektronska evidencija prekršaja. Ovo podrazumijeva: poboljšanje kvaliteta digitalne forenzike, jačanje kapaciteta Agencije za nacionalnu bezbjednost u oblasti prikupljanja, evidentiranja, analiziranja, čuvanja i razmjene podataka u sajber prostoru, kao i usvajanje kompletnih i djelotvornih pravnih rješenja u oblasti sajber kriminala, koji su u skladu sa ljudskim pravima i vladavinom prava.



Slika 1. Statistički pregled sajber incidenata prijavljenih u 2014.god

Univerziteti u Crnoj Gori. U obrazovnim institucijama, poseban fokus treba da bude usmjeren na nove generacije, kao i na krajnje korisnike Interneta, čime se podrazumijeva da obrazovne institucije treba konstantno da predstavljaju nove programe o bezbjednosti informacija na svim nivoima obrazovanja, u cilju korišćenja naprednih informacionih sistema. Neophodno je stvoriti bezbjednije Internet okruženje za građane Crne Gore, te da se korisnici Interneta edukuju podizanjem svijesti o potrebi daljeg usavršavanja i informisanja u ovoj oblasti. Konkretno, univerziteti u Crnoj Gori, kao agenti u procesu visokog obrazovanja, treba da rade na organizovanju posebnih studijskih programa u oblasti sajber bezbjednosti, u cilju stvaranja specijalizovanog i stručnog kadra iz ove oblasti, a u saradnji sa ostalim relevantnim institucijama da rade na organizaciji obuka i treninga za razne starosne kategorije građana koji koriste i/ili imaju svoje poslovne aktivnosti na Internetu

3. OBRAZOVNI SISTEM U OBLASTI SAJBER BEZBJEDNOSTI U CRNOJ GORI

Obrazovanje se generalno može podijeliti na formalno i neformalno obrazovanje. Oba vida informisanja i podučavanja ljudi imaju značajnu ulogu u razvoju jedne zemlje. Formalno obrazovanje obuhvata sistematski strukturirano obrazovanje koje se sprovodi po nastavnim listama i planovima u državnim ili privatnim obrazovnim

[1] Nacionalni CIRT: www.cirt.me

institucijama. S druge strane, neformalno obrazovanje se može definisati kao preduzimljivost osobe u cilju sticanja znanja (obično izvan tradicionalnih školskih sistema putem kurseva i obuka) gde je sadržaj prilagođen jedinstvenim potrebama pojedinca [2]. U Tabeli 1 je prikazano stanje u crnogorskom obrazovnom sistemu u poređenju sa evropskim praksama za obrazovanje o sajber bezbjednosti.

Tabela 1. Poredbena analiza EU praksi i CG obrazovanja [1]

Formalno obrazovanje u oblasti sajber bezbjednosti	
Osnovno i srednjoškolsko obrazovanje	U osnovnom i srednjoškolskom obrazovanju postoji po jedan (dva) opšta obavezna IT predmeta, međutim njime nije obuhvaćena oblast koja se bavi temom sajber bezbijednosti. Niti postoji ijedan od izbornih predmeta koji izučava ovu oblast.
Bachelor studijski programi	U Crnoj Gori trenutno ne postoji ni jedan Bachelor studijski program u oblasti sajber bezbjednosti. Ipak, EU iskustva i praksa pokazuju da kompletan bachelor program posvećen sajber bezbjednosti nije toliko neophodan, ukoliko u okviru postojećih studijskih programa postoje predmeti koji obrađuju ovu temu. Na crnogorskim univerzitetima trenutno postoji samo nekoliko predmeta koji obuhvataju teme sajber bezbjednosti a izučavaju se samo na fakultetima tehničkog usmjerenja gdje se analiziraju tehnički aspekti bezbejdnosti računarskih sistema i na fakultetima pravnog usmjerenja gdje se analiziraju pravni aspketi bezbjednosti i zaštite.
Master studijski programi	Samo jedan od univerziteti u Crnoj Gori (Univerzitet Donja Gorica) ima posebne master programe o sajber zaštiti, sa multidisciplinarnim pristupom i različitim profilima stručnjaka u ovoj oblasti. Na Univerzitetu Donja Gorica osnovana su dva postdiplomska studijska programa: • "Sajber bezbjednost"- master program koji se izučava na Humanističkim studijama; • "Zaštita podataka i sigurnost informacionih sistema" – specijalističke i master studije na Fakultetu za informacione sisteme i tehnologije.
Doktorski studijski programi	Ne postoji posebni doktorski program u oblasti sajber bezbjednosti. Zaseban doktorski program nije toliko potreban ukoliko drugi doktorski programi obrađuju ovu oblast i edukuju stručnjake o njoj.
Neformalno obrazovanje u oblasti sajber bezbjednosti	
Profesionalno usavršavanje	Postoji nekoliko inicijativa ili generalno profesionalnih obuka na institucionalnom (obično u organizaciji banaka, telekomunikacionih provajdera, isl) i nacionalnom nivou koje se organizuju za širok spektar ICT kadra. Ne postoji podatak da li se neke privatne kompanije bave pružanjem profesionalnih obuka u ovoj oblasti, kao ni koliko su dostupni i rasprostranjeni drugi strani programi.
Obuke zaposlenih	U Crnoj Gori, kompanije, posebno mala i srednja preduzeća ne praktitkuju organizovanje obuka u oblasti sajber zaštite za svoje zaposlene. U posljednje vrijeme, primijećen je rastući trend organizovanja ovih obuka od strane velikih kompanija (obično banke, ICT kompanije, telekomunikacioni provajderi isl).
Obrazovanje šire javnosti u oblasti sajber bezbjednosti	
Kampanje za podizanje svijesti	Efektivne kampanje za podizanje svijesti šire javnosti ne postoje. Ministarstvo za informaciono društvo i telekomunikacije planira da organizuje obuke za širu javnost, gdje će posebna pažnja biti posvećena djeci i mladima, i kontinuiranom uvođenju novih programa iz oblasti sajber bezbjednosti na svim nivoima obrazovanja. Međutim konkretne akcije još nisu evidentirane.
Informativne kampanje o sajber bezbjednosti	Efektivne kampanje namijenjene široj javnosti ne postoje osim za učenike osnovnih i srednjih škola (organizovano od starne Ministarstva prosvjete u saradnji sa Telenor Crna Gora) gdje su đaci informisani o savjesnom korišćenju ICT-a i Interneta, sa aspekta bezbjednosti. Potrebno je organizovati inicijative između univerziteta, privatnih kompanija i škola.

Čak iako Crna Gora znatno razvija domaću radnu snagu koja će vjerovatno biti u stanju da vodi računa o pomenutim obavezama u narednom periodu, od suštinskog značaja je subvencionisanje saradnje sa javnim i privatnim organizacijama iz zemalja EU, kako bi se moglo početi sa opsežnim kursevima i treninzima iz oblasti sajber bezbijednosti, kao i uspostavljanje obrazovnih programa vezanih za sajber bezbjednost..

4. POREDBENA ANALIZA EU PRAKSI SA TRENUTNIM PRAKSAMA U CRNOJ GORI

Kada se uporedi trenutna situacija u vezi sa sajber bezbjednošću u Crnoj Gori sa EU praksama, evidentno je da postoji jaz koji treba prevazići. Crnogorsko društvo se nalazi u periodu tranzicije, i sve javne i privatne organizacije ulažu značajan napor kako bi brzo ispunile EU standarde u pogledu podizanja svijesti stanovništva o rizicima, i konstituisanju radne snage koja je u stanju da sprovede u praksu odgovarajuće mjere.

Prethodnih godina, Crna Gora je uložila značajan napor kako bi dostigla EU standarde u oblasti sajber bezbjednosti i formalno, iz ove perspektive Crna Gora je već dostigla najuobičajnije standarde. Međutim, jaz između plana i akcija je ono što je evidentno i što treba u najkraćem roku prevazići. Pravni okvir je dobro strukturiran i razrađen, međutim, nije jasno u kojoj mjeri je to u skladu sa propisima i na koji način se sprovode vezane EU direktive.

Naime, identifikovani su sljedeći koraci koje treba sprovesti u cilju poboljšanja. Potrebno je:

• **Razjasniti ulogu Vojske u (nacionalnoj) sajber bezbjednosti:** iako je Crna Gora identifikovala da Vojska

mora posjedovati kapacitete za sajber bezbjednost, ovi kapaciteti nijesu dobro definisani i ne postoje adekvatni resursi za izgradnju tih kapaciteta.

• **Definisati međusektorski organ zadužen za koordinaciju aktivnosti različitih državnih organa:** među glavnim ciljevima Nacionalne strategije o sajber bezbjednosti je "*Definisanje institucionalne i organizacione strukture u oblasti sajber bezbjednosti u zemlji, koja obuhvata osnivanje Nacionalnog savjeta za sajber bezbjednost i stvaranje lokalnih CIRT timova*". Međutim, ništa slično još uvijek nije formirano, i različiti ministri i državni organi su dobili dužnosti u vezi sa sajber bezbjednošću koji se često preklapaju. Fundamentalno je identifikovati smjernice za raspodjelu odgovornosti i obim posla.

• **Poboljšati saradnju između javnih i privatnih institucija:** značaj postizanja dugoročnih i dobro utvrđenih sporazuma između privatnog sektora i javnih institucija je od vitalnog značaja za garanciju najvišeg nivoa zaštite od stalno promjenjivih sajber napada.

Mnogi univerziteti u EU su već kreirali (ili su u procesu kreiranja) nastavnog programa u oblasti sajber bezbjednosti. Često, ovi nastavni planovi su interdisciplinarni, kao što je slučaj i u Crnoj Gori. Ovo posebno važi za manje zemlje, gdje se očekuje da jedan studijski program ponudi obrazovanje za buduće menadžere sajber sigurnosti, kao i tehničke eksperte. Kada se uspostave jasni, specijalizovani doktorski i master programi u oblasti sajber bezbjednosti, obrazovanje u toj oblasti će se regularno i nesmetano sprovoditi i na nižim nivoima i drugim oblastima obrazovanja.

Identifikovanjem najvažnijih problema formalnog obrazovanja u Crnoj Gori, i najrelevantnijih razlika sa EU praksama, dolazi se do sljedećih zaključaka. Evidentan je:

• *Nedostatak stručnjaka:* generalno, u Crnoj Gori nedostaje grupa iskusnih profesionalaca i predavača, koji mogu da definišu kako novi nastavni plan i program u oblasti sajber bezbjednosti, tako i da prenesu svoje znanje.

• *Nedostatak specijalizovanih kurseva:* iako je prihvatljivo da nema nijedan nastavni plan u ovoj oblasti, neophodno je početi sa realizacijom specijalističkih kurseva u oblasti sajber bezbjednosti koji će obezbijediti multidisciplinarna znanja u ovoj oblasti.

• *Nedostatak osnovnog znanja:* iako generalno gledajući, u obrazovnom sistemu Crne Gore postoje dva specifična studijska programa za edukaciju stručnjaka u oblasti sajber bezbjednosti, čini se da se ne pridaje dovoljno značaja osnovnim i fundamentalnim znanjima. Nastavni planovi i programi su više usmjerena ka pravnom i tehnološkom aspektu, ali postoji čitav niz znanja koje je neophodno posjedovati da bi se razumjela suština mnogih sajber bezbjednosnih prijetnji, od osnova ICTa, preko osnova bezbjednosti, matematike itd.

Neformalne obuke u okviru preduzeća i javne kampanje Vlade su ohrabrujuće, ali interesovanje privatnog sektora za trenzizima u oblasti sajber bezbjednosti primjetno izostaje. Kampanje za podizanje svijesti stanovništva najčešće ne zahtijevaju angažovanje stručnjaka sa naprednim tehnološkim vještinama.

5. ZAKLJUČAK

Kada se uporedi trenutna situacija u vezi sa sajber bezbjednošću u Crnoj Gori sa EU praksama, evidentno je da su preduzeti inicijalni koraci i da se na nacionalnom nivou počelo sa aktivnostima koji vode ka kreiranju sajber bezbjedonosnog okvira. Čitav ICT prostor je i dalje izložen visokom riziku narušavanja informacione bezbjednosti, zbog činjenice da se razvijaju i implementiraju kratkoročne mjere za eliminaciju napada na sigurnost IT sistema, umjesto dugoročnog planiranja i koordiniranih akcija. Ipak, mnoge aktivnosti u pogledu obrazovanja je neophdono implementirati, kako bi se obezbijedili edukovani stručnjaci spsobni da odgovore savremenim izazovima sajber bezbjednosti, kao i edukovanu naciju koja će svojim svakodnevnim aktivnostima na Internetu povećati nivo lične i opšte sajber bezbjednosti na nacionalnom nivou.

Zahvalnost. U ovom radu su predstavljeni rezultati Tempus projekta 'Unapređenje obrazovnog sistema u oblasti sajber bezbjednosti u Crnoj Gori- ECESM', br. 544088-TEMPUS-1-2013-1-SI-TEMPUS-JPHES.

LITERATURA

[1] *EU practice for cyber security education*, ECESM Report, 2014 (dostupno na: http://ecesm.net/publications-0)
[2] M. Mušanović, "*Pedagogija profesionalnog obrazovanja"*, Graftrade Rijeka, 2001
[3] R.Milašinović, S.Mijalković, G.Amidžić, "*Bezbednost i internet"*, 2012
[4] European Commission, *A Digital Agenda for Europe,* Brussels, COM(2010) 245
[5] *Krivični zakon*, Sl. list Crne Gore, br. 40/2008, 25/2010, 32/2011, 40/2013 i 56/2013
[6] *Zakonik o krivičnom postupku*, Sl. list Crne Gore, broj 57/09
[7] European Commission, *A strategy for a Secure Information Society – "Dialogue, partnership and empowerment"*, Brussels COM(2006) 251
[8] *Zakon o informacionoj bezbjednosti*, Sl. list CG, br.14 od 17.mart 2010
[9] *Zakon o Agenciji za nacionalnu bezbjednost*, Sl. list Crne Gore, br. 86/09, 20/11
[10] *Zakon o tajnosti podataka*, Sl. list Crne Gore, br. 79/08, 70/09, 44/12
[11] *Zakon o elektronskom potpisu*, Sl. list RCG,br: 55/03 i 31/05
[12] *Zakon o elektronskim komunikacijama*, Sl. list Crne Gore, broj 40/2013
[13] *Zakon o elektronskoj trgovini*, Sl.list RCG,br.80/04
[14] *Strategija sajber bezbjednosti Crne Gore* 2013-2017, Podgorica jun 2013.
[15] Direkcije za zaštitu tajnih podataka, *Vodič za pristup informacijama u posjedu Direkcije za zaštitu tajnih podataka*, 2013
[16] R.Šendelj, F.Lombardi, I.Ognjanović, S.Guarino, "*Cyber Security in Montenegro: Practice, Framework and Challenges*", INFOFEST 2014