FBIM Transactions
DOI 10.12709/fbim.07.07.01.13

INFORMACIONO-BEZBEDNOSNA KULTURA MLADIH U SRBIJI

INFORMATION-SECURITY CULTURE OF YOUTH IN SERBIA

Zoran Milanović
Kriminalističko-policijska akademija, Beograd, Srbija

JEL Kategorija rada: **L86**

Rezime

Mlađe populacije su najčešći korisnici interneta, a posebno društvenih mreža i kao takve su najugroženija ciljna grupa većine pojavnih oblika zloupotrebe. Zato je sprovedeno istraživanje korišćenjem upitnika, a sa ciljem utvrđivanja njihovih trenutnih znanja i ponašanja na internetu i njihove informaciono-bezbednosne kulture. Rezultati istraživanje treba da imaju za posledicu podizanje svesti krajnjih korisnika o potrebi zaštite podataka, informacija i znanja. Istraživanje je pokazalo postojanje nedoslednosti između stečenih znanja (svesti) o informaciono-bezbednosnim rizicima i ponašanju (informaciono-bezbednosne kulture) ispitanika. Uzroke ovih nedoslednosti autor vidi u nedostatku praktičnih (primenjivačkih) znanja i smatra da mlade treba podsticati da budu aktivniji u sticanju većeg opsega znanja, razumevanja i mogućnosti da se suoče sa problemima.

Ključne reči: *mladi, znanje, ponašanje, svest, informaciono-bezbednosna kultura.*

Abstract:

Younger populations are the most common Internet users, especially social networks, and as such are the most vulnerable target group for most forms of abuse. Therefore, a survey was conducted using a questionnaire, with the aim of determining their current knowledge and behavior on the Internet and their information and security culture. The research results should have the effect of raising the awareness of the end users about the need to protect data, information and knowledge.The research has shown the existence of inconsistencies between the acquired knowledge (awareness) of the information-security risks and behavior (information-security culture) of the respondents. The author believes that the causes of these inconsistencies lack of practical (applicable) knowledge and thinks that young people should be encouraged to be more active in acquiring a greater scope of knowledge, understanding and ability to cope with problems.

Keywords: *youth, knowledge, behavior, awareness, information-security culture**.***

Adresa autora:
Zoran Milanović
zoran.milanovic@yahoo.com

1. UVOD

Vreme u kome živimo odlikuje se primenom naprednih informaciono-komunikacionim tehno-

logijama (IKT) u svim sferama života i rada, unapređujući ih kako u kvalitativnom tako i u kvantitativnom smislu. Ova činjenica je, između ostalog, nametnula i novu društvenu vrednost: informaciono-bezbednosnu kulturu i kao takva postala je predmet interesovanja mnogih istraživača. Obzirom da je posmatrana sa različitih aspekata i da su se fokusi istraživača međusobno razlikovali, nastale su i različite definicije informaciono-bezbednosne kulture. Jednu od najopštijih definicija dao je Roer (2015) u knjizi "Izgradnja bezbednosne kulture", ističe: Bezbednosna kultura pomaže i olakšava ljudima da koriste informacione tehnologije na zadovoljavajući način, bez opasnosti i pretnji. Na sličan način su definisali informaciono-bezbednosnu kulturu i Kizist i Ilvonen (2003), Vrum i Solms (2004) i Tomson i ostali (2006). Roer (2015), takođe, navodi da je jedan od ključnih faktora izgradnje informaciono-bezbednosne kulture promena ponašanja pojedinaca podizanjem svesti o informaciono-bezbednosnim rizicima i mogućim posledicama.

S druge strane, najranjiviji deo svakog društva su deca i mladi. Njihova ranjivost u informaciono-bezbednosnom smislu potiče pre svega zbog njihovog neiskustva i naivnosti, te njihovog rizičnog ponašanja kao posledice nedostatka svesti o mogućim posledicama. Prema Mišelu Sen Lou (2015), direktoru UNICEF-a u Srbiji, „sve više dece koristi digitalne alatke za učenje, društveno angažovanje i druženje. Međutim, putem njih se izlažu i novim rizicima – nasilju, neprikladnom sadržaju, nepoznatim ljudima, a rizik za njihov razvoj predstavlja i prekomerna upotreba digitalnih sadržaja". Naime, mladi imaju probleme koje ne mogu uvek da prepoznaju i objasne, susreću se sa različitim pojavama i pretnjama bez prethodne psihološke zaštite. Probleme uglavnom ne mogu sami da reše i/ili ne znaju kome da se obrate za pomoć.

Opasnosti i pretnje kojima je mlađa populacija korisnika interneta svakodnevno izložena su brojne i raznovrsne, a posebno sa ekspanzivnim razvojem društvenih mreža i on-line igrica. One danas predstavljaju sadržaje koji su popularni i kao takvi veoma uticajni na mlađu populaciju korisnika interneta.

Mladi su najugroženija ciljna grupa većine pojavnih oblika zloupotrebe, a posebno nastajanju, razvoju i širenju dečije pornografije. Ciljana edukacija, kao i razgovori sa roditeljima igraju najznačajniju ulogu u prevenciji i rešavanju ovog problema. Tako mnoge zemlje u svetu uvode obavezno obrazovanje, a poslednji primer uvođenja edukacije na svim obrazovnim nivoima je Indija. Ona se na ovaj korak odlučila zbog širenja velikog broja lažnih vesti putem interneta, a koji su za posledicu imali više od 25 ubistava (BBC, 2018). Adekvatna bezbednosna kultura svih korisnika, a naročito mladih, imperativ je savremenog društva (Bjelajac, 2014).

U tom smislu nastao je i ovaj rad, kao želja autora da skrene pažnju javnosti na trenutno stanje i nivo informaciono-bezbednosne kulture mladih kao i da ukaže na hitnost preduzimanja sveobuhvatnih mera kako bi se podigla svest i bezbednosni nivo ovog najosetljivijeg i najizloženijeg, a pre svega najvažnijeg dela našeg društva.

U radu su prezentovani rezultati i zaključci anonimnog upitnika kao istraživačkog instrumenta koji je doveo u korelaciju nivo znanja, kao merila svesti o mogućim informaciono-bezbednosnim rizicima i ponašanje kao merila informaciono-bezbednosne kulture.

2. ISTRAŽIVANJE

Cilj istraživanja je utvrđivanje postojećeg znanja i ponašanja korisnika IKT-a, ali i njihova edukacija, kao i posredno i neposredno unapređenje njihove bezbednosne kulture i podizanja svesti o narastajućim bezbednosnim problemima, pretnjama i rizicima, i moguća rešenja za zaštitu.

Prva faza se odnosi na kreiranje anonimnog upitnika, tj. strukturu pitanja i istraživačke oblasti – konstrukte. Pitanja za intervju koji je obavljen „licem u lice" i elektronski veb upitnik su kreirani na osnovu značajnog teorijskog i praktičnog iskustva autora, kroz njegov dvadesetogodišnji rad na održavanju i zaštiti digitalnih sistema, kao i pregleda velikog broja elektronskih publikacija i veb sajtova iz oblasti informacione bezbednosti.

Po formiranju upitnika koji je imao 35 pitanja, izvršeno je preliminarno testiranje na kontrolnoj grupi od 18 korisnika IKT-a, oba pola od 18 do 27 godina. Cilj probnog testiranja je provera konzistentnosti postavljenih pitanja unutar dve varijable: znanja i ponašanja.

Broj i redosled pitanja je isti kod upitnika za intervju i elekronski.

Konačan izgled upitnika (Tabela 1) je 34 pitanja, od kojih se na 31 pitanje odgovara sa DA ili NE.

2.1. Metod anketiranja i distribucije podataka

Za potrebe elektronskog upitnika dizajnirana je klijentska veb orjentisana aplikacija (*www.mzt.in.rs/Anketa.php*), kao i *MySQL* baza u koju se slivaju svi prikupljeni podaci. Ovaj automatizovani način anketiranja u mnogome je olakšao proces popunjavanja i slanja odgovora. Sa jedne strane, korisnici IKT-a koji su se anketirali nisu bili vezani ni za mesto ni za vreme popunjavanja, a sa druge strane, administratoru baze podataka koji je istovremeno sa popunjavanjem upitnika imao i ažuriran tabelarni prikaz rezultata.

Tabela 1 – Upitnik

	PITANJE
1.	Pol:
2.	Koje od ponuđenih digitalnih uređaja koristite:
3.	Da li znate koji je operativni sistem se nalazi na njima?
4.	Da li znate za pristup operativnom sistemu koji nalog koristite (admin ili korisnički)?
5.	Da li znate koji zaštitni softver se nalazi na njima?
6.	Da li bi prepoznali nasilje na internetu (govor mržnje, uznemiravanje...)?
7.	Da li bi prijavili problem nasilja na internetu?
8.	Da li imate nalog na nekoj od društvenih mreža?
9.	Da li ostavljate lične podatke na internetu (ime, datum i mesto rođenja, šta studirate, slike)?
10.	Da li ste upoznati sa problemom krađe identiteta na internetu?
11.	Da li igrate on-line igrice?
12.	Da li skidate filmove, serije i muziku sa interneta?
13.	Da li gledate filmove ili slušate muziku on-line?
14.	Da li ste nekada povredili nečija autorska prava?
15.	Da li menjate lozinke (bar jednom u tri meseca) na svojim internet nalozima?
16.	Da li koristite istu lozinku za dva različita naloga (servisa, računara)?
17.	Da li znate nečiju pristupnu lozinku za: mail nalog ili društvenu mrežu?
18.	Da li neko zna Vašu pristupnu lozinku?
19.	Da li redovno pravite rezervne kopije svojih podataka?
20.	Na čemu pravite kopije podataka (DVD, flash, cloud, drugo)?
21.	Da li Vam se desilo da izgubite ili da Vam je ukraden neki od mobilnih uređaja (telefon, tablet, laptop)?
22.	Da li ste se susreli sa nekim oblikom malicioznog softvera (virus, trojanac...) na računaru ili telefonu?
23.	Da li znate šta je enkripcija?
24.	Da li znate šta je bitkoin?
25.	Da li znate šta je rensomver (*Ransomware*)?
26.	Da li znate šta je DDoS?
27.	Da li znate šta je fišing?
28.	Da li znate šta je ZiroDej (*Zero Day*)?
29.	Da li znate čime se bavi digitalna forenzika?
30.	Da li znate čime se bavi digitalna anti-forenzika?
31.	Da li znate neki od standarda koji se bave informacionom bezbednošću?
32.	Da li znate šta je ISO 27000 i NIST 800?
33.	Da li ste učestvovali na predavanjima, seminarima ili kursevima gde se govorilo o informacionoj bezbednosti, zaštiti korisnika na internetu, o društvenim mrežama itd?
34.	Da li na internetu čitate tekstove koji se bave zaštitom korisničkih podataka i informacija?

2.2. Obrazloženje pitanja iz upitnika

U obrazloženju je dato šta sve korisnici IKT-a treba da znaju kako bi bili bezbedni tj. kako bi što

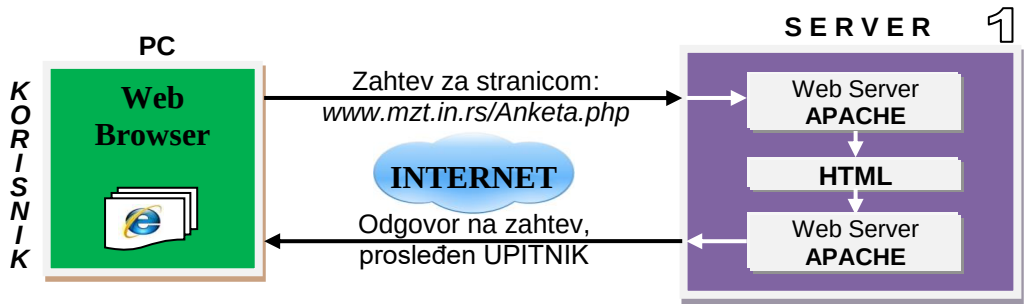
bolje zaštitili svoju privatnost i podatke na internetu.

Tabela 2 – Obrazloženje pitanja iz upitnika

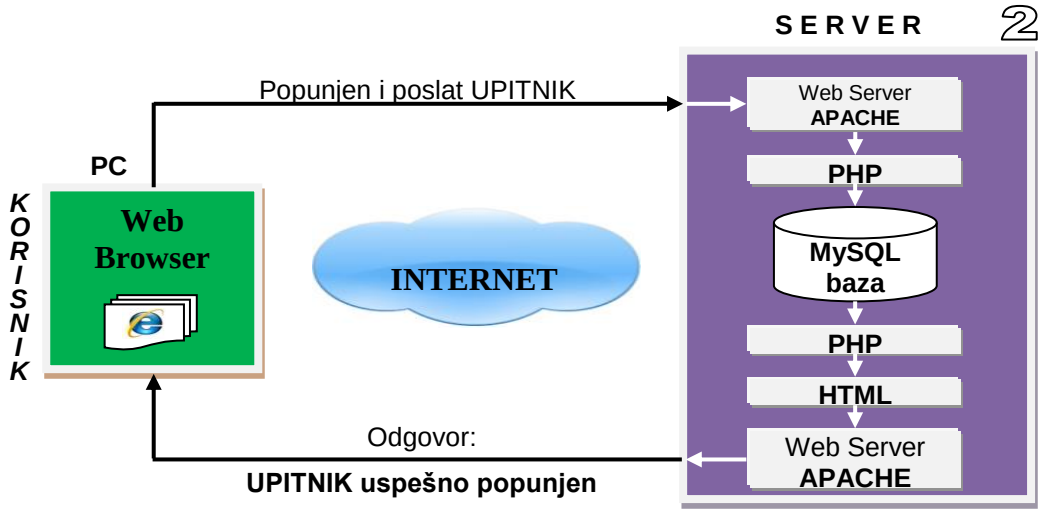
	OBRAZLOŽENJE
1.	Muško, Žensko, Nije važno
2.	Računar, laptop, pametni telefon, tablet.
3.	Korisnici treba da znaju koji OS koriste i da ni jedan od OS (*Windows OS, Mac OS, Linux*…) nije apsolutno bezbedan, kao i da novije verzije OS imaju manje bezbednosnih propusta. Novi OS imaju najnoviju i najbolju zaštitu, kao i podršku proizvođača.
4.	Korisnici treba da znaju da li pristupaju sa administratorskim nalogom, koji zlonamernim korisnicima pruža mnogo više privilegija za preuzimanje sistema, nego kada se koristi nalog sa ograničenim funkcijama.
5.	Korisnici treba da znaju da li imaju i da li je ažuriran antivirusni softver ili neki drugi program za zaštitu od malicioznog softvera.
6.	Korisnici treba da prepoznaju nasilje na internetu, ali i da prijave nadležnim organima, jer posledice mogu biti katastrofalne.
7.	Korisnici treba da prijave probleme koje imaju na internetu, jer tako mogu zaštititi i pomoći velikom broju korisnika koji su potencijalne žrtve.
8.	Korisnici treba da znaju da društvene mreže predstavljaju potrebu, ali i opasnost, jer se na njima odvija veliki broj kriminalnih radnji.
9.	Korisnici treba da budu svesni da društvene mreže prikupljaju veliku količinu informacija koje su za nas naizgled nevažne, ali koje spadaju u kategoriju ličnih podataka i koje kriminalni korisnici (Zdnet, 2016), a i velike tehnološke kompanije mogu zloupotrebiti. (Engadget, 2018a)
10.	Korisnici treba da budu upoznati sa svim vidovima nasilja i mogućih metoda iskorišćavanja njihovih ličnih podataka. Krađa identiteta je među pet najobimnijih vrsta internet kriminala (Business reporter, 2016).
11.	Najčešći korisnici su deca i mladi koji predstavljaju najosetljiviju grupu za informacionu bezbednost, jer što su duže u on-line komunikaciji veće su šanse i da budu napadnuti ili zloupotrebljeni.
12.	Korisnici treba da budu svesni da skoro svako skidanje i striming datoteka sa interneta povlači za sobom i mogućnost nesvesnog dovlačenja i aktiviranja malicioznog softvera, aki i narušavanje nečijih autorskih prava.
13.	Korisnici treba da budu svesni da gledanjem i slušanjem, tj. njihovim traženjem i izborom mogu ugroziti svoju bezbednost.
14.	Korisnici treba da budu svesni da gledanjem i slušanjem mogu da ugroze nečija autorska prava, što je veoma čest slučaj.
15.	Korisnici treba da razmišljaju o važnosti i potrebi ne samo kvalitetnih (jakih) lozinki, već i o njihovoj redovnoj zameni, kao i da ih ne ponavljaju na više servisa.
16.	Korisnici treba da znaju da je čest slučaj u praksi da zlonamerni korisnici upotrebljavaju otkrivene korisničke lozinke na drugim servisima u potrazi za još nekim nalogom sa koga će slati neželjenu elektronsku poštu, ali i krađu identiteta.
17.	Korisnici treba da znaju značaj jedinstvenih lozinki i da svako zna svoju, a ne i tuđu. Nije dobro deliti pristupne lozinke sa porodicom i prijateljima, jer u svim slučajevima one mogu, svesno ili nesvesno biti zloupotrebljene.
18.	Nije dobra praksa da svako svakome zna lozinku, jer kada dođe do bezbednosnog incidenta nikad se ne zna ko je kriv i gde je nastao problem. Sve ovo otežava rešenje problema.
19.	Pravilno i redovno pravljenje rezervnih kopija je sigurno jedan od najvažnijih elemenata zaštite.
20.	Rezervne kopije treba praviti izvan izvornog digitalnog uređaja, na uređajima ili medijumima koji su fizički odvojeni. Preporuke su, zbog dostupnosti, da to bude negde na mreži, ali da se isključi svaka mogućnost automatskog ažuriranja.
21.	Veliki broj digitalnih uređaja se izgubi ili bude ukraden, a sa njima i važni podaci i informacije. Ovaj segment predstavlja veliki problem za bezbednost.
22.	Danas nema korisnika IT-a koji se nisu susreli sa nekim vidom malicioznog softvera. Jedino se može postaviti pitanje da li su toga svesni i da li su u stanju da prepoznaju oblike savremenog kriminaliteta.

	OBRAZLOŽENJE
23.	Enkripcija, pored pravljenja rezervnih kopija, predstavlja drugi najvažniji element zaštite. Sva nova IKT rešenja poseduju neki vid enkripcije, da li u procesu komunikacije ili u zaštiti intelektualne svojine.
24.	Digitalni novac predstavlja sadašnjost i budućnost razmene vrednosnih sredstava. Veliki značaj ima primena savremenih tehnologija gde je skoro nemoguće ispratiti transakciju tj. tok (ko uplaćuje i kome).
25.	Vrsta malicioznog softvera koja je napravila do sada najveću štetu, kako organizacijama, tako i običnim korisnicima. (Business reporter, 2016)
26.	DDoS su postali sve veći, kompleksniji ali i učestaliji metod hakerskih napada, koji se koristi za zatrpavanje i obaranje servera, slanjem miliona upita. (Digital attack map)
27.	Glavni hakerski napad, gde se od najivnih i lakomislenih korisnika očekuje da ostave svoje poverljive podatke. (Deloitte, 2014)

	OBRAZLOŽENJE
28.	Ranjivost u sistemu (hardver, softver, mreža, servis…) za koje ni njihovi proizvođači ne znaju da postoje, a koji su čest uzrok napada. (Norton)
29.	Korisnici treba da imaju osnovna saznanja o forenzici i šta uraditi kada se desi bezbednosni incident.
30.	Korisnici treba da budu svesni da se većina digitalnog kriminala prikriva i da je primena ovih metoda usporila njihovo razjašnjavanje.
31.	Korisnici treba da su bar čuli da postoje propisani bezbednosni standardi.
32.	Osnov za holistički pristup informacionoj bezbednosti od koga treba početi. Sa sadržajima ove familije standarda treba upoznati i edukovati korisnike, jed pored bezbednosne terminologije tu se nalaze i osnovne mere zaštite.
33.	Ovo je neophodni korak u edukaciji svakog korisnika digitalnih uređaja.
34.	Korisnici treba da prate preporuke bezbednosnih stručnjaka i da u nekim posebnim situacijama postupaju po njihovim preporukama.



Slika 1 – Blok dijagram povezivanja zahteva krisnika sa odgovorom servera



Slika 2 – Blok dijagram povezivanja poslatog upitnika sa bazom podataka

Blok dijagram (slika 1) pokazuje vezu između principa rada servera i računara korisnika tj. povezivanja zahteva korisnika sa odgovorom servera. Korisnik koji pristupa anketiranju, preko svog Web Browser-a šalje zahtev serveru tako što unosi već naznačenu URL adresu. Server odgovara na zahtev i prosleđuje upitnik.
Korisnik popunjava i šalje upitnik serveru (slika 2) na kome se nalazi ***APACHE Web*** server koji skladišti primljene podatke u ***MySQL*** bazu i prosleđuje odgovor klijentu da je anketiranje uspešno obavljeno.
Na kraju, kada administrator baze podataka želi da pregleda i preuzme tabelu sa prikupljenim podacima, takođe, preko Web Browser-a šalje zahtev serveru, tako što unosi određenu URL adresu: *http://mzt.in.rs/preuzmipodatke.php.* Zatim, prostim selektovanjem i kopiranjem tabele, prebacuje podatke u alat za statističku analizu.

2.3. Analiza rezultata istraživanja

Analiza upitnika obuhvata 34 pitanja, od kojih su 3 opšta, a ostalih 31-no pitanje su razvrstani u dve varijable: znanje (15 pitanja) i ponašanje (16 pitanja) korisnika IT-a. Pitanja koja ukazuju na znanje su: 3, 4, 5, 6, 10, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32, a ponašanje: 7, 8, 9, 11, 12, 13, 14, 15, 16, 17, 18, 19, 21, 22, 33 i 34.

Na osnovu ove dve varijable izabrana je statistička metoda za analizu prikupljenih podataka – χ^2 (Hi) kvadrat test nezavisnosti, koji testira povezanost između dva obeležja jednog skupa (Mann, 2009).

Prikupljeni zbirni rezultati upitnika su analizirani u SPSS (Analyze-Descriptive statistics-Crosstabs) programu za statističku obradu podataka.

Dihotomne[1] varijable – znanje i ponašanje, odn. njihove binarne vrednosti, u upitniku su kodirane sa: 1 (jedan) – za odgovor DA i 0 (nula) – za odgovor NE. Njihove ukupne i zbirne vrednosti, kao i uzajamni odnosi, prikazani su u tabeli 3.

U varijabli znanje, odgovori kodirani 1 pokazuje da postoji znanje, a 0 kada na postavljeno pitanje ne postoji znanje tj. odgovor nije tačan. Analogno tome, u varijabli ponašanje, oznakom 1 je ocenjeno pozitivno ponašanje u određenoj situaciji, odnosno oznakom 0 negativno ponašanje. Kod ove varijable je izvršeno rekodiranje, jer su neki odgovora u upitniku koji su označeni sa 1 mogli ukazivati na pozitivno odn. negativno ponašanjem.

Tabela 3 – Dihotomne varijable – znanje i ponašanje

			PONAŠANJE		Zbir
			1 – DA	0 – NE	
ZNANJE	1 – DA	**Ukupno**	**222**	**396**	**618**
		% znanje	35,9%	64,1%	100,0%
		% ponašanje	34,5%	43,9%	40,0%
		% od ukupnog	14,4%	25,6%	40,0%
	0 – NE	**Ukupno**	**421**	**506**	**927**
		% znanje	45,4%	54,6%	100,0%
		% ponašanje	65,5%	56,1%	60,0%
		% od ukupnog	27,2%	32,8%	60,0%
Zbir		**Ukupno**	**643**	**902**	**1545**
		% znanje	41,6%	58,4%	100,0%
		% ponašanje	100,0%	100,0%	100,0%
		% od ukupnog	41,6%	58,4%	100,0%

2.4. Diskusija rezultata

Iz tabele 3, iz pojedinačnih i unakrsnih rezultata može se zaključiti sledeće:

- 35,9% onih koji su pokazali viši nivo znanja (svesti) je istovremeno iskazao i viši nivo bezbednosne kulture, dok je njih 64,1%, naprotiv pokazao niži nivo bezbednosne kulture;
- 45,4% onih koji su pokazali niži nivo bezbednosnog znanja (svesti) je pokazao viši nivo bezbednosne kulture, dok je njih 54,6% pokazao istovremeno i niži nivo bezbednosne kulture.
- Od ukupnog broja ispitanika 40,0% je pokazalo viši nivo znanja, a nasuprot tome 60,0% niži nivo znanja ili bolje reći neznanja pojedinih termina ili pojava u oblasti informacione bezbednosti;
- Sa druge strane 41,6% je pokazalo pozitivno ponašanje u određenim bezbednosnim

[1] „Uglavnom zavisna varijabla sa dve moguće vrednosti, često označene nulom i jedinicom.“ (Metodologija)

situacijama, tj. viši nivo bezbednosne kulture, dok je 58,4% pokazalo niži nivo bezbednosne kulture.

Generalno ove zaključke potvrđuju neke druge studije (Kaspersky, 2014): „i pored straha, korisnici i dalje imaju tendenciju da budu nebezbedni u svojim ponašanjima, jer mnogi ne samo da nemaju instalirana bezbednosna rešenja na svojim uređajima, već ih i ne štite lozinkama, a samo mali broj korisnika su svesni i mogu se suočiti sa pretnjama na netu."

Takođe, korisnici na društvenim mrežama, bez obzira na to što su upoznati sa činjenicom da su im lični podaci zloupotrebljeni (The Guardian, 2018), nisu značajno promenili svoja ponašanja, kao ni postavke privatnosti (Engadget, 2018b).

Dok se iz tabele 4 može konstatovati da su ispunjene osnovne predpostavke Hi kvadrat testa, jer je očekivana učestalost u svim ćelijama veća je od 5, tj. u ovom konkretnom slučaju je 257,20.

Tabela 4 – Hi kvadrat test

	Value	df	Exact Sig. (2-sided)	Exact Sig. (1-sided)
Pearson Chi-Square	13,753[a]	1		
Continuity Correction[b]	13,365	1		
Likelihood Ratio	13,840	1		
Fisher's Exact Test			0,000	0,000
Linear-by-Linear Association	13,744	1		
N of Valid Cases	1545			
a. 0 cells (,0%) have expected count less than 5. The minimum expected count is **257,20**.				
b. Computed only for a 2x2 table				

Takođe, iz tabele 4 se može konstatovati da je značajna vrednost Hi kvadrata, tj. njegova korigovana vrednost (*Continuiti correctionb*), s obzirom da postoje samo dve kategorije: znanje i ponašanje.

Korigovana vrednost Hi kvadrata je 13,365 sa statističkom značajnošću p=0,0001, što je manje od 0,05 (Mann, 2009). Ova vrednost Hi kvadrata pokazuje statistički značajne razlike između znanja i ponašanja ispitanika.

Tabela 5 – Fi koeficijent korelacije

		Value	Asymp. Std. Error[a]	Approx. T[b]
Nominal by Nominal	Phi	-0,094		
	Cramer's V	0,094		
Interval by Interval	Pearson's R	-0,094	0,025	-3,723
Ordinal by Ordinal	Spearman Correlation	-0,094	0,025	-3,723
N of Valid Cases		1545		
a. Not assuming the null hypothesis.				
b. Using the asymptotic standard error assuming the null hypothesis.				

Ovo je potvrđeno i Fi koeficijentom (Tabela 5) koji predstavlja koeficijent korelacije između dve dihotomne varijable.

Naime vrednost od -0,094 ukazuje na neznatnu i to negativnu korelaciju.

Ovako nizak i to negativan koeficijent korelacije može se tumačiti na sledeći način:

- Ispitanici koji su pokazali viši nivo znanja, a nasuprot tome niži nivo bezbednosne kulture, zapravo to znanje nisu suštinski usvojili i pretvorili ga u svest o potrebi zaštite i potencijalnim opasnostima u digitalnom svetu;
- Ispitanici koji su pokazali niži nivo znanja i pri tome imaju ocenjen viši nivo bezbednosne kulture, zapravo slabije koriste IT, pa time i nisu u prilici da iskažu negativno ponašanje tj. niži nivo bezbednosne kulture;
- Naposletku, može se reći da su ovakvi rezultati i posledica metode ocenjivanja tj. njene ograničenosti obzirom da ona ocenjuje prisustvo, odnosno odsustvo obeležja koje se istražuje bez daljih kvalifikacija.

3. ZAKLJUČAK

I pored svih ograničenja, ovo istraživanje je pokazalo postojanje nedoslednosti između stečenih znanja (svesti) o informaciono-bezbednosnim rizicima i ponašanju ispitanika što

generalno ukazuje na probleme u srpskom obrazovnom kontekstu tj. da se stečena saznanja ne pretvaraju u praktična znanja koja bi vodila podizanju svesti i time uticala na ponašanja odn. na bezbednosnu kulturu i kulturu u najopštijem smislu.

U tom smislu autor se slaže sa Ejdusom i ostalima (2009) da decu i mlade treba podsticati da postanu aktivniji, sa većim opsegom znanja, razumevanja i mogućnosti da se suoče sa problemima, kao i da neguju ona ponašanja koja će značajno podići njihov nivo bezbednosne kulture. Da bi se ovaj cilj postigao neophodno je da informaciono-bezbednosna kultura postane sastavni deo planova i programa svih nivoa obrazovanja i vaspitanja. Prihvatanjem osnovnih načela informaciono-bezbednosne kulture stvorio bi se preduslov za uspostavljanje bezbednog ambijenta u kome bi mladi neometano mogli da koriste sve prednosti i blagodeti informacionih tehnologija i tako ostvare svoja prava na kvalitetno obrazovanje, informisanje i lični razvoj.

CITIRANI RADOVI

BBC (2018.), preuzeto 20. 8. 2018., sa https://www.bbc.com/news/world-asia-india-45140158

Bjelajac, Ž., Zirojević M., (2014), BEZBEDNOSNA KULTURA U ERI GLOBALIZACIJE, Institut za međunarodnu politiku i privredu Beograd. Preuzeto 20.8.2018., sa http://kpolisa.com/KP23/kp23-II-3-BjelajacZirojevic.pdf

Business reporter (2016), preuzeto 20.8.2018., sa http://business-reporter.co.uk/2016/05/26/5-costly-types-cyber-crime-2015/?getcat=2

Business reporter (2016), preuzeto 20.8.2018., sa http://business-reporter.co.uk/2016/05/26/two-five-consumers-unaware-ransomware-threat-survey-finds/?getcat=2

Deloitte (2014), preuzeto 20.8.2018., sa http://www2.deloitte.com/content/dam/Deloitte/nl/Documents/risk/deloitte-nl-phishing-awareness.pdf

Digital attack map, preuzeto 20.8.2018., sa https://www.digitalattackmap.com/understanding-ddos/

Ejdus, F., Unijat, J., Milošević M., (2009), Istraživanje i podizanje nivoa bezbednosne kulture mladih, preuzeto 20.8.2018., sa http://www.bezbednost.org/Svi-projekti/700/Istrazivanje-i-podizanje-nivoa-bezbednosne.shtml#sthash.IRucHXPn.dpuf

Engadget (2018a), preuzeto 20.8.2018., sa https://www.engadget.com/2018/06/30/facebook-shared-user-data-with-52-tech-companies/

Engadget (2018b), preuzeto 20.8.2018., sa https://www.engadget.com/2018/04/13/facebook-users-aren-t-changing-privacy-settings/

Kaspersky, Consumer security risks survey 2014: multi-device threats in a multi-device world. Preuzeto 20.8.2018., sa http://media.kaspersky.com/en/kaspersky_lab_consumer_security_risks_survey_2014_eng.pdf

Kuusisto, T., Ilvonen, I. (2003), Information security culture in small and medium size enterprises. Frontiers of E-business Research.

Lo, S., M, (2015), Preuzeto 20.8.2018., sa http://www.mpn.gov.rs/prvo-razmisli-borba-protiv-digital/

Mann S. P., (2009) Увод у статистику, Шесто издање, Економски факултет, Београд.

Metodologija sa statistikom, Fakultet za specijalnu edukaciju i rehabilitaciju, Univerzitet u Beogradu, preuzeto 20.8.2018., sa http://metodologija.org/doktorske/tipovi-varijabli/

Norton, preuzeto 20.8.2018., sa http://www.pctools.com/security-news/zero-day-vulnerability/

Roer K., (2015), Build a Security Culture, IT Governance Publishing, United Kingdom, pp.14.

The Guardian, (2018), preuzeto 20.8.2018., sa https://www.theguardian.com/news/2018/mar/17/cambridge-analytica-facebook-influence-us-election

Thomson, K., Solms, R., Louw, L. (2006), Cultivating an organizational information security culture. Computer Fraud & Security. 10:7-11.

Vroom, C., Solms, R., (2004), Towards information security behavioral compliance. Computers & Security, 23(3): 191-198.

Zdnet, (2016), preuzeto 20.8.2018., sa http://www.zdnet.com/article/its-2016-and-we-dont-know-who-has-our-personal-data/

Datum prve prijave: 28.08.2018.
Datum prijema korigovanog članka: 19.03.2019.
Datum prihvatanja članka: 27.03.2019.

Kako citirati ovaj rad? / How to cite this article?

*Style – **APA** Sixth Edition:*

Milanović, Z. (2019, 04 15). Informaciono-bezbednosna kultura mladih u Srbiji. (Z. Čekerevac, Ur.) *FBIM Transactions, 7*(1), 110-118. doi:10.12709/fbim.07.07.01.13

*Style – **Chicago** Sixteenth Edition:*

Milanović, Zoran. 2019. „Informaciono-bezbednosna kultura mladih u Srbiji.“ Urednik Zoran Čekerevac. *FBIM Transactions* (MESTE) 7 (1): 110-118. doi:10.12709/fbim.07.07.01.13.

*Style – **GOST** Name Sort:*

Milanović Zoran Informaciono-bezbednosna kultura mladih u Srbiji [Časopis] // FBIM Transactions / ur. Čekerevac Zoran. - Beograd : MESTE, 15 04 2019. - 1 : T. 7. - str. 110-118.

*Style – **Harvard** Anglia:*

Milanović, Z., 2019. Informaciono-bezbednosna kultura mladih u Srbiji. *FBIM Transactions,* 15 04, 7(1), pp. 110-118.

Style – **ISO 690** Numerical Reference:

Informaciono-bezbednosna kultura mladih u Srbiji. **Milanović, Zoran.** [ur.] Zoran Čekerevac. 1, Beograd : MESTE, 15 04 2019, FBIM Transactions, T. 7, str. 110-118.