



www.unvi.edu.ba



EDUK@TOR

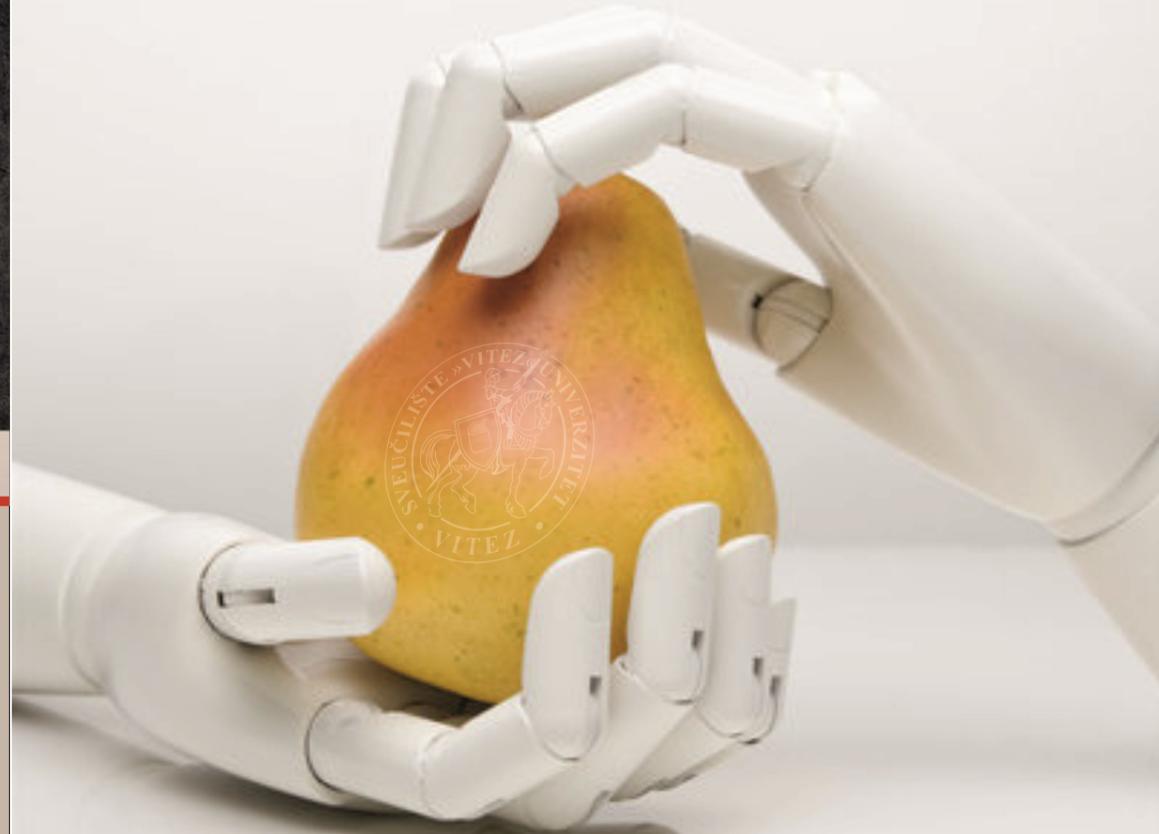
ISSN 2303-5564

Godina II, broj 3. juli 2015. godine

ISSN 2303-5560 / 2303-5584

NAUČNO-STRUČNI I INFORMATIVNI ČASOPIS FAKULTETA INFORMATIJSKIH TEHNOLOGIJA S/U VITEZ

Problematika kriminaliteta na području Srednjobosanskog kantona, sa posebnim osvrtom na razbojništva i razbojničke svade | Zaštita i kontola djece na internetu | Savjeti roditeljima
Savjeti nastavnicima | Savjeti učenicima | Antivirusna rješenja



ANDROID APLIKACIJE ZA ZAŠTITU DJECE

UVOĐENJE ASYCUDO PROGRAMA U BIH PRESTIGIO

MULTIBOARD ALL-IN-ONE PC RUDARENJEM DO ZDRAVLJA I PROSPEKTA

POVEZANOST POTROŠNJE ENERGIJE I EKONOMSKOG RASTA SA POSEBNIM OSVRTOM NA BIH

IMPRESSIUM

Gl.i odgovorni urednik **doc.dr Hadžib Salkić**

Tehnički urednik **mr.sc Almira Salkić**

Naslovnica **Mirsada Fuško, BA**

Redakcija: **doc.dr Hadžib Salkić, doc. dr Ibrahim Obhodaš, doc.dr Džemal Kulašin, doc.dr Jamila Jaganjac, mr.sc Almira Salkić, mr.sc Mahir Zajmović, mr.sc Adnan Pirić, Nermina Konjalić, BA, Dinka Šakić, BA, Senida Kakeš, BA.**

Recezentii: **prof.dr Lazo Roljić, prof.dr Branko Latinović, prof.dr Nedim Smailović, doc. dr Hadžib Salkić, doc. dr Ibrahim Obhodaš, doc.dr Džemal Kulašin, doc.dr Jamila Jaganjac**

SADRŽAJ

UVOĐENJE ASYCUDO PROGRAMA U BIH

Mr. Edin Hodžić

Uprava za indirektno oporezivanje
edin.hodzic@hotmail.com

-5-

ZAŠTITA DJECE NA INTERNETU – PRAVNI OKVIR

Mr.sc Adnan Pirić, Mr.sc Almira Salkić

Sveučilište/Univerzitet Vitez, Fakultet pravnih nauka
adnan.piric@unvi.edu.ba, almira.salkic@unvi.edu.ba

-10-

PRESTIGIO MULTIBOARD ALL-IN-ONE PC

Doc.dr Hadžib Salkić, Jasmin Kahrman

Sveučilište/Univerzitet Vitez
Dalcom d.o.o., Zenica, Bosna i Hercegovina
hadzib.salkic@unvi.edu.ba, jasmin.kahrman@dalcom.com.ba

-18-

DATA MINING

RUDARENJEM DO ZDRAVLJA I PROSPERITETA (BOINC)

Damir Emić, BA

Sveučilište/Univerzitet Vitez, BiH
damir.emic@outlook.com

-27-

ANTIVIRUSNA RJEŠENJA

Doc.dr Hadžib Salkić, Sandrino Vulović

Sveučilište/Univerzitet Vitez, Fakultet informacijskih tehnologija
hadzib.salkic@unvi.edu.ba, sandrino.vulovic@unvi.edu.ba

-35-

ZAŠTITA DJECE NA INTERNETU

SIGURNOSNI ASPEKAT

Inspektor Suzana Zec

MUP SBK/KSB TRAVNIK

-46-

ANDROID APLIKACIJE ZA ZAŠTITU DJECE

Dinka Šakić, BA, Denis Lovrinović, BA

Sveučilište / Univerzitet „Vitez“ Vitez
dinka.sakic@unvi.edu.ba, denis.lovrinovic@unvi.edu.ba

-49-

UTICAJ RODITELJA NA SIGURNOST DJECE NA INTERNETU

Senida Kakeš, BA, Amir Delić, BA

Sveučilište/Univerzitet Vitez, Fakultet informacijskih tehnologija
senida.kakes@unvi.edu.ba, amir.delic@unvi.edu.ba

-56-

SOFTVERI ZA ZAŠTITU I KONTROLU DJECE NA INTERNETU

Nehad Gaši, BA

Sveučilište/Univerzitet Vitez, Fakultet informacijskih tehnologija
nehad.gasi@unvi.edu.ba

-64-

**PROBLEMATIKA KRIMINALITETA NA PODRUČJU SREDNJOBOSANSKOG
KANTONA SA POSEBNIM OSVRTOM NA RAZBOJNIŠTVA I RAZBOJNIČKE
KRAĐE**

Mr. sc. Adnan Pirić

Sveučilište/Univerzitet „Vitez“ Vitez, Fakultet pravnih nauka piricadnan@unvi.edu.ba

-69-

**POVEZANOST POTROŠNJE ENERGIJE I EKONOMSKOG RASTA SA
POSEBNIM OSVRTOM NA BIH**

mr. Mirza Kulenović, dipl. ecc,

Visoka škola „CEPS-Centar za poslovne studije“ Kiseljak
mirza.visokaskola@gmail.com

-83-

**ANALIZA PROMETNOG SUSTAVA U SARAJEVU S CILJEM USMJERAVANJA
NJEGOVOG DALJEG RAZVOJA KA EVROPSKIM STANDARDIMA**

Palić Nermin, Mr. sc., Cinac Džemal, Mr. sc.

Visoka škola „CEPS-Centar za poslovne studije“ Kiseljak,
Sveučilište/Univerzitet "ITC - Interlogos centar" Kiseljak,
nermin.palic@yahoo.com, dcinac@yahoo.com

-96-

PROJEKAT „ZAŠTITA I KONTROLA DJECE NA INTERNETU“

Osvrt Marele Martinović

-116-

**SAVJETI RODITELJIMA, NASTAVNICIMA I DJECI
PROJEKAT „ZAŠTITA I KONTROLA DJECE NA INTERNETU“**

-119-

MICROSOFT FAMILY SAFETY

mr. sc. Mahir Zajmović, mr.sc Almira Salkić

Fakultet informacionih tehnologija, Sveučilište/Univerzitet „Vitez“ Vitez
mahir.zajmovic@unvi.edu.ba, almira.salkic@unvi.edu.ba

-136-

SOFTVER ZA PREPOZNAVANJE LICA

Nermina Konjalić, BA

Sveučilište/Univerzitet „Vitez“ u Vitezu, Bosna i Hercegovina
nermina.konjalic@gmail.com

-143-

UVOĐENJE ASYCUDO PROGRAMA U BIH

Mr.Edin Hodžić

Uprava za indirektno oporezivanje BiH

edin.hodzic@hotmail.com

SAŽETAK

Cilj rada je da pokaže doprinos programa ASCYDA efikasnom obavljanju svih potrebnih radnji vezanih za uvoz i izvoz dobara, odnosno za carinski postupak. Analiza će se odnositi na značaj programa ASCYDA u obavljanju poslova zaposlenih u Upravi za indirektno/neizravno oporezivanje Bosne i Hercegovine, prilikom carinskog postupka koji se sastoji u ubrzanju procesa carinjenja, a sve to omogućava olakšice i ubrzanje u kretanju roba i putnika.

Za analizu rada će se koristiti sekundarni podaci međunarodnih i domaćih organizacija koje su učestvovala u izradi programa kao i njegovom poboljšanju (nadogradnji) kao i podaci Uprave za indirektno oporezivanje.

Za potrebe ovog rada istražiti će se uloga države kao podsticajnog faktora u cilju implementacije nove verzije Asycuda program s ciljem da se omogući ubrzanje carinskog postupka a samim tim i efikasnosti postupka indirektnog oporezivanja.

UVOD

Uvođenje ASYCUDA programa u BiH koncipirano je i podržano na nivou međunarodne zajednice usmjereno na pomoć u stabilizaciji i razvoju, odnosno pod pokroviteljstvom CAFAO organizacije (Customs and Fiscal Assistance Office Programme).. Samo Uvođenje ASYCUDA programa prethodilo je Zakonu o PDV-u kojim je uspostavljena institucionalna i organizaciona osnova za jedinstveni sistem indirektnog oporezivanja u Bosni i Hercegovini, koja treba da podrži sveukupnu makroekonomsku stabilnost i fiskalnu održivost Bosne i Hercegovine kao i da pruži podršku funkcioniranju jedinstvene ekonomske teritorije u Bosni i Hercegovini.

U Bosni i Hercegovini koristi se "ASYCUDA++" ali u Upravi za indirektno oporezivanje Bosne i Hercegovine u toku su aktivnosti vezano za uvođenje nove carinske aplikacije „ASYCUDA World“ koja treba da ubrza protok roba kroz BiH prilikom izvoza i uvoza, osim toga i mnoge druge pogodnosti poput online podnošenja carinskih prijava, kvalitetniju kontrolu vrijednosti robe kroz online baze.

Osim nabrojanih prednosti koje donosi, uvođenje nove aplikacije „ASYCUDA World“ predstavlja i važan korak ka uspostavljanju novog kompjuteriziranog tranzitnog indirektno oporezivanje BiH započeo je 2013 godine, a finasira se dijelom iz budžeta UIO, a dijelom iz IPA fordova EU.

Država daje svoj doprinos unapređenju verzije ASYCUDA programa kao i kroz učešće u finansiranju uvođenja NCTS-a u Bosnu i Hercegovinu, gdje u ovom finansiranju učestvuje još i EU posredstvom IPA fordova. Na ovaj način odnosno

uvođenje NCTS-a u Bosnu i Hercegovinu doprinijet će efikasnosti carinskog postupka i uopšteno sistema indirektnog oporezivanja, što sa svoje strane utiče na stabilnost i povećanje prihoda od indirektnih poreza, a sve skupa utiče na bolje upravljanje državnim finansijama.

ASYCUDA program

ASYCUDA (Automated SYstem for CUstoms Data - automatizirani sistem za obradu carinskih podataka) je kompjuterski carinski upravljački sistem. Softver ASYCUDA je razvio UNCTAD (United Nations Conference on Trade and Development) u Ženevi na osnovu zahtjeva zemalja članica koje su željele obezbijediti odgovarajuće statističke podatke o uvozu/izvozu. Postoje tri verzije-generacije Asycude i to: ASYCUDA2.7, ASYCUDA++ i ASYCUDA World. Prilikom izrade verzija Asycude koriste se međunarodi standardi i kodovi razvijeni od strane međunarodnih organizacija kao što su: ISO (International Organisation for Standardisation), WCO (World Customs Organization) i UN (United Nations). S obzirom da se pri izradi verzija drži do propisanih i usaglašenih procedura kao i navedenih međunarodnih standarda i kodova ASYCUDA program omogućava generisanje podataka o trgovini (prometu dobara) koji se upotrebljavaju za statističke i ekonomske analize kao i izradu raznih izvještaja.

Primjena ASYCUDA programa omogućava:

- pouzdane informacije o spoljnoj trgovini.
- institucionalno jačanje carine kroz reformu i modernizaciju
- bolje upravljanje državnim finansijama

Sistem je instalisan u preko 90 zemalja, u svim regionima i kontinentima. Od evropskih zemalja ASYCUDA program se uglavnom koristi u tranzicijskim zemljama a neke od njih su: Albanija, Estonija, Jermenija, Makedonija, Slovačka.

Primjena ASYCUDA programa u BiH

U Bosni i Hercegovini koristi se "ASYCUDA++" koja predstavlja treću verziju sistema, s tim da ova verzija ima specifičnost da funkcioniše na principu upotrebe sva tri jezika (bosanski, hrvatski i srpski) i dva pisma (latinica i ćirilica). Sistem je operativan u unutrašnjim carinskim ispostavama i na graničnim prijelazima od 2002. godine, i mogu ga koristiti kako interni korisnici (službenici UIO) tako i eksterni korisnici (špediteri, kontrolni i inspeksijski organi). Vezano za ASYCUDA program u BiH isti se koristi od 2002. godine a uvođenje je bilo pod pokroviteljstvom CAFAO organizacije i Evropske unije.

ASYCUDA sistem čine dvije komponente i to: programski paket (koji je i srž sistema) i računarske komponente (konfiguracija i performanse su ostavljene na izbor korisniku sistema). U skladu sa tim konfiguracija ASYCUDA sistema

prilagođena je zahtjevima UIO BiH te obezbjeđuje primjenu važećih carinskih procedura, carinske tarife i ostalih zakonskih odredbi koje su neophodne za provedbu odgovarajućih carinskih postupaka. U zavisnosti od potreba u konfiguraciji sistema se obavljaju odgovarajuće izmjene. Službenici Sektora za informacione tehnologije obezbjeđuju pravovremenu tehničku i korisničku podršku svim korisnicima sistema.

Vežano za uvođenje nove carinske aplikacije „ASYCUDA World“ projektom je planirano da u toku 2015. godine slijedi instalisanje aplikacije na svim lokacijama, kao i obuka više od 3 hiljade korisnika, uključujući sve korisnike unutar UIO i poslovnu zajednicu koja će koristiti novu carinsku aplikaciju. Zajedno sa ovom aktivnošću raditi će se i na izradi softvera za nacionalni NCTS – Novi provozni kompjuterizovani sistem, koji koriste sve zemlje članice EU. Početak primjene nove carinske aplikacije planiran je za 01.01.2016. godine, nakon čega će se po isteku godinu dana rada nacionalnog provoznog sistema, Bosna i Hercegovina pridružiti međunarodnom provoznom sistemu –NCTS.

Nova carinska aplikacija ASYCUDA World ubrzaće protok roba prilikom izvoza i uvoza, osigraće mogućnost jedinstvene carinske garancije na cijelom području BiH, podnošenje carinske prijave online – putem interneta, te kvalitetniju kontrola vrijednosti robe kroz provjere online baza podataka sa vrijednostima robe i carinskim tarifama. Primjenom nove carinske aplikacije biće unapređeno i ubrzano provođenje i kontrola carinskih i poreskih propisa, kvalitetnija analiza rizika kao i sprečavanje prekograničnog krijumčarenja, povećane mogućnosti kontrole carinskih organa uz istovremeno smanjenje administrativnih troškova.

ASYCUDA World pružiće mogućnost on-line plaćanja carinskih dadžbina, poboljšanu evidenciju i kontrolu naplaćenih dažbina, ažurnije praćenje dinamike prikupljanja poreza, izvještavanje u realnom vremenu, te mogućnost bržeg i kvalitetnijeg donošenja strateških odluka i uočavanja aktuelnih trendova. Realizacijom cijelog projekta biće izvršena usaglašenost sa važećim carinskim propisima – u skladu sa evropskom legislativom i regulativama u carinskom poslovanju, te mogućnost povezivanja UIO sa evropskim i međunarodnim sistemima.

Rad u programu ASYCUDA

ASYCUDA sistem radi na principu klijent-server konfiguracije, pri čemu je kompjuter koji korisnici koriste ustvari klijent koji se povezuje na glavni računarski server. Da bi pristupili programu ASYCUDA odnosno prijavili se na server potrebno je da imamo lozinku od administratora. Na taj način svaki korisnik koji ima pristup klijentu povezan je sa serverom i čini lokalnu mrežu tzv. klijent/server konfiguracija.

Princip mreže kojom se ostvaruje veza između servera i klijenta, na kojem funkcioniše sistem je zatvorenog tipa (komunikacija se ostvaruje putem zakupljenih telefonskih linija koje su odvojene od ostatka telefonskog saobraćaja).

Rad u program omogućuje interakciju tako da se podaci sa kompjutera (klijenta) prenose na server za obradu i pohranjivanje, a isto tako klijent može da preuzima informacije koje su pohranjene na server, s tim da istovremeno pod jednim serverom može da radi veći broj klijenata.

Carinski postupak se pokreće, polazi kada podnosilac donese odštampanu deklaraciju sa pratećom dokumentacijom i istu preda carinskom službeniku na recepciji, koji treba da pokrene provjeru i procjenu te deklaracije. Ove operacije vrše se u modulu MODCBR.

Da bi proces carinjenja otpočeo potrebno je pokrenuti Procjenu deklaracije. Nakon procesa obrade deklaracije na recepciji, sistem određuje automatski carinike na prijemu i fizičkom pregledu robe. Za ove operacije takođe se koriste iste funkcije u modulu MODCBR.

Procjena deklaracije je pokrenuta čime je pokrenut i selektivitet u sistemu ASYCUDA. Sistem deklaraciji automatski dodjeljuje traku selektiviteta (crvena, žuta ili zelena traka selektiviteta) za daljnju obradu kao i službenike za pregled dokumenata i pregled robe.

Ako podaci iz JCI odgovaraju uslovima iz kriterija selektiviteta deklaracija se može usmjeriti na Crvenu traku, Žutu traku, Plavu traku ili Zelenu traku radi obrade.

- Crvena traka znači da je procjena deklaracije zaustavljena i da je neophodan pregled robe
 - fizički pregled (uz fizički pregled vrši se i pregled dokumenata).
- Žuta traka takođe znači da je procjena deklaracije zaustavljena i da je neophodan detaljniji pregled dokumenata - provjera dokumenata. Obično je ovo traka koja se odnosi na probleme koji se mogu ispraviti u kancelariji, a ako je neophodno nakon ovog pregleda može uslijediti fizički pregled robe.
- Plava traka znači da se može nastaviti sa procjenom deklaracije, ali je deklaracija označena za kontrolu nakon carinjenja.
- Zelena traka znači da se deklaracija odmah može procijeniti.

Zemlja korisnica ASYCUDA++ programa ne mora koristiti sve trake selektiviteta ili može neku traku selektiviteta koristiti za druge svrhe. Ono što je bitno da znate u ovom slučaju je da ASYCUDA zaustavlja procjenu deklaracije na Crvenoj traci i Žutoj traci, a procjena deklaracije se nastavlja na Plavoj traci i Zelenoj traci 12.

Sve korisničke grupe imaju pristup modulu MODTRS koji omogućava obradu tj. registraciju tranzitnih prijava, razduženje tranzitnih prijava i elektronski prenos podataka o tranzitu.

Modul MODACC je korisnički modul i namijenjen je računovodstvenom dijelu obrade JCI. Sve korisničke grupe u carinskim ispostavama imaju pristup modulu MODACC, a u okviru kog pristupaju izvještajima. Ostale operacije vezane za ovaj modul kao što su: Uplate/ Isplate po deklaracijama, unos garancija, otvaranje/zatvaranje Dnevne knjige i sl. obavljaju se u regionalnim centrima od strane ovlaštenih lica iz Sektora za poslovne usluge.

Važno je napomenuti da se sve uplate po deklaracijama elektronski prenose iz poslovnih banaka u UINO. Ovi podaci se zatim prosljeđuju na servere carinskih ispostava i plaćanje deklaracija se vrši automatski. UINO BiH je jedini korisnik ASYCUDA sistema, od oko 90 zemalja, koja posjeduje automatsko razduženje uplata u sistemu ASYCUDA.

Modul CHQ, je modul u kome se vrši unos i ažuriranje svih referentnih tabela u sistemu, pored ovih funkcija ovaj modul se koristi i za dobivanje nekih standardnih statističkih izvještaja. Pristup izradi statističkih i korisničkih izvještaja posjeduju sve korisničke grupe u carinskim ispostavama.

ZAKLJUČAK

Uvođenje ASYCUDA programa u Bosni i Hercegovini kao sastavni dio poboljšanja efikasnosti indirektnih poreza omogućilo je: podnošenje carinskih i tranzitnih prijava elektronskim putem, korištenje selektiviteta u uvoznim i izvoznim procedurama, elektronsko razduženje tranzitnih prijava, automatsko razduženje uplata carinskih dažbina, ažurne statističke podatke, ubrzanje procesa carinjenja, olakšice u kretanju roba i putnika.

U okviru napora za unapređenje i nadogradnju sistema ASYCUDA u toku su aktivnosti i radnje na uvođenju nove verzije i to "ASYCUDA World" a sve u cilju smanjenja trajanja provoznih carinskih procedura i olakšavanja prekograničnog prometa i protoka roba i putnika.

Osim nabrojanih prednosti koje donosi, uvođenje nove aplikacije „ASYCUDA World“ predstavlja i važan korak ka uspostavljanju novog kompjuteriziranog tranzitnog sistema (NTCS), koji u BiH treba da zaživi od 1. januara 2016. godine.

Realizacijom cijelog projekta uvođenje aplikacije ASYCUDA World kao i uspostavljanje novog kompjuteriziranog tranzitnog sistema (NTCS) biće izvršena odgovarajuća usaglašenost sa važećim carinskim propisima to jest u skladu sa evropskom legislativom i regulativama u carinskom poslovanju, te mogućnost povezivanja UIO sa evropskim i međunarodnim sistemima.

ZAŠTITA DJECE NA INTERNETU – PRAVNI OKVIR

Mr.sc Adnan Pirić, Mr.sc Almira Salkić

Sveučilište/Univerzitet Vitez, Fakultet pravnih nauka
adnan.piric@unvi.edu.ba, almira.salkic@unvi.edu.ba

SAŽETAK

Zaštita djece na internetu je jednako važna kao i njihova zaštita u realnom svijetu. Djeca pripadaju ranjivoj grupi korisnika interneta koja u biti, nisu svjesna svih opasnosti. Uporedo sa stalnim tehnološkim razvojem i porastom broja korisnika interneta i značaj zaštite djece u svijetu interneta je sve veći. Ovaj rad ima za cilj da predstavi kratak pregled aktivnosti koje su poduzete u cilju zaštite djece na internetu u Evropskoj uniji (EU), odnosno međunarodnim propisima, kao i da uakže na osvrt sličnih mjera, odnosno propise domaćeg zakonodavstva, tj. BiH. Shodno tome, predstavljene su neke od značajnijih zakonodavnih, regulatornih, samoregulatornih mjera i inicijativa s ciljem zaštite djece na internetu u međunarodnom i domaćem zakonodavstvu. Da bi se problem rizika koištenja informacionih i komunikacionih tehnologija sagledao i našla rješenja, koja obezbjeđuju i štite viši stepen sigurnosti djece pri korištenju moderne komunikacione tehnologije, potrebno je prvo izvršiti kvalitetnu analizu trenutnog stanja u ovoj oblasti, kako u smislu domaćeg i međunarodnog zakonodavstva u ovoj oblasti, tako i stvarno stanje u praksi. UN Konvencija o pravima djeteta jedinstven je međunarodni dokument u zaštiti prava i interesa djece. Posebnost konvencije, u odnosu na brojne dokumente o ljudskim pravima uopšte, ogleda se u činjenici, da jednim dokumentom uspostavlja sva prava za svako dijete, da sva prava uspostavlja kao jednako važna i osnovna, i da njima nema hijerarhije po njihovoj važnosti. Jedno od prava garantovanih konvencijom je pravo djeteta na zaštitu od svakog oblika nasilja, zlostavljanja, zanemarivanja i nemarnog postupanja.

Ključne riječi;

Dijete,internet, zaštita, pravo, međunarodni i domaći propisi.

UVOD

Zbog sve učestalijeg prisustva i ozbiljnosti pojave zloupotrebe djeteta na internetu u današnjem društvu, i zbog povezanosti ove pojave s kriminalnim aktivnostima, pitanje borbe protiv zloupotrebe djece putem informaciono komunikacionih tehnologija treba rješavati prvenstveno sa aspekta postojećih zakonskih propisa. Da bi se osigurala adekvatna zaštita djece od eksploatacije putem informaciono komunikacionih tehnologija, od presudne važnosti je napraviti moderan, sveobuhvatan i strog međunarodni i domaći pravni okvir. U tom smislu, da bi se učinkovito riješilo ovo pitanje iz perspektive prevencije i zaštite, potrebno je osigurati da se međunarodni standardi za zaštitu djece adekvatno primjenjuju u okviru domaćih pravnih propisa. U regionu je usvojen niz relevantnih, pravno obavezujućih akata i napravljen je niz formalnih obaveza sa potrošačima da bi se osigurala usklađenost s međunarodnim standardima vezanim za korištenje informaciono komunikacionih tehnologija. Međutim, međunarodni, regionalni i nacionalni normativni okviri u Jugoistočnoj Evropi još uvijek nisu u potpunosti

usklađeni i često ne mogu osigurati adekvatnu zaštitu prava djece koja koriste informaciono komunikacione tehnologije. Na temelju analiza koje su napravile institucije ombudsmana, kao i na temelju procjene koju je uradila organizacija Save the Children u saradnji s konsultantom, može se zaključiti da u nekim slučajevima nacionalni pravni okviri ne uključuju odgovarajuće norme o visokotehnoškom kriminalu (cyber crime), kojima bi se države mogle boriti protiv ove pojave na način kako to propisuju međunarodni standardi. U ovom radu ćemo dalje predstaviti određeni međunarodni i domaći pravni okvir, kada je ova problematika u pitanju.

MEĐUNARODNI PROPISI

UN Konvencija o pravima djeteta

Države članice su prema UN Konvenciji o pravima djeteta¹, između ostalog, obavezne na preduzimanje svih odgovarajućih zakonodavnih, administrativnih, socijalnih i obrazovnih mjera radi zaštite djeteta od fizičkog ili mentalnog nasilja, povreda ili zloupotreba, zanemarivanja ili nemarnog odnosa, maltretiranja ili eksploatacije, uključujući i seksualnu zloupotrebu, dok je na brizi kod roditelja, zakonitih staratelja ili nekog drugog lica kome je povjerena briga o djetetu. Takve zaštitne mjere treba da obuhvate, po potrebi, efikasne postupke za ustanovljavanje socijalnih programa za obezbjeđenje podrške neophodne djetetu i onima kojima je povjerena briga o djetetu, kao i ostale oblike sprečavanja, utvrđivanja, prijavljivanja, prosljeđivanja, istrage, postupanja i praćenja slučajeva ovdje navedenog zlostavljanja djeteta i, po potrebi, obraćanja sudu.² Države članice se obavezuju da zaštite dijete od svih oblika seksualnog izrabljivanja i seksualne zloupotrebe. U tom cilju, države članice posebno preduzimaju sve odgovarajuće nacionalne, bilateralne i multilateralne mjere za sprečavanje:

- navođenja ili prisiljavanja djeteta da učestvuje u nezakonitim seksualnim aktivnostima;
- eksploatatorskog korištenja djece u prostituciji ili drugim nezakonitim seksualnim radnjama;
- eksploatatorskog korištenja djece u pornografskim predstavama i časopisima.³

Ova konvencija takođe sadrži i fakultativni protokol;

Fakultativni Protokol uz Konvenciju o pravima djeteta o prodaji djece, dječijoj prostituciji i pornografiji.⁴

Evropska konvencija o kibernetičkom kriminalu

U smislu izraza Evropska konvencije o kibernetičkom kriminalu⁵ predstavlja;

- a) "kompjuterski sistem" označava svaki uređaj ili skup uređaja međusobno povezanih, koji osigurava ili čiji jedan ili više elemenata osiguravaju, prilikom izvršenja nekog programa, automatiziranu obradu podataka;

¹ Usvojena na Generalnoj skupštini UN 1989.godine (44/25 od 20.11.1989). Bosna i Hercegovina je preuzela UN Konvenciju o pravima djeteta notifikacijom o sukcesiji („Službeni list RBiH“, broj: 25/93).

² UN Konvencija o pravima djeteta, član 19.

³ UN Konvencija o pravima djeteta, član 34.

⁴ „Službeni glasnik Bosne i Hercegovine“, Međunarodni ugovori, broj: 5/02.

⁵ Savjet Evrope, 2001.godina; „Službeni glasnik Bosne i Hercegovine“, Međunarodni ugovori, broj: 6/06.

- b) "kompjuterski podaci" označavaju svako predstavljanje činjenica, informacija i koncepata u formi prilagođenoj za kompjutersku obradu, ubrajajući tu i program koji je takve prirode da kompjuterski sistem vrši svoju funkciju;
- c) "davalac usluge" označava:
 - svaki javni ili privatni organ koji nudi korisnicima svojih usluga mogućnost komunikacije putem kompjuterskog sistema;
 - svaki drugi organ koji obrađuje ili pohranjuje kompjuterske podatke za tu uslugu komunikacije ili za svoje korisnike;
- d) "promet podataka" označava sve kompjuterske podatke povezane sa komunikacijom i koji dolaze iz jednog kompjuterskog sistema i koje taj kompjuterski sistem proizvodi u svojstvu elementa u lancu komunikacije, označavajući porijeklo, odredište, putanju, vrijeme, datum, veličinu i trajanje komunikacije ili vrstu usluge.⁶

Ova Konvencija obavezuje države članice da svojim nacionalnim zakonodavstvom inkriminišu sljedeća ponašanja:

- proizvodnja dječije pornografije u cilju njene difuzije putem kompjuterskog sistema,
- nuđenje ili činjenje dostupnom dječije pornografije putem kompjuterskog sistema,
- distribucija i prenošenje dječije pornografije putem kompjuterskog sistema,
- pribavljanje za sebe ili drugoga dječije pornografije putem kompjuterskog sistema,
- posjedovanje dječije pornografije u kompjuterskom sistemu ili putem čuvanja kompjuterskih podataka.⁷

Konvencija o zaštiti djece od seksualnog iskorištavanja i seksualnog zlostavljanja (Savjet Evrope - CETS No201)

Konvencija o zaštiti djece od seksualnog iskorištavanja i seksualnog zlostavljanja (Savjet Evrope - CETS No201)⁸ Svrha Konvencije, prema članu 1. je:

- a) sprečavanje i borba protiv seksualne eksploatacije i seksualnog zlostavljanja djece,
- b) zaštita prava djece koja su bili žrtve seksualne eksploatacije i seksualnog zlostavljanja,
- c) unapređenje nacionalne i međunarodne saradnje u borbi protiv seksualne eksploatacije i seksualnog zlostavljanja djece.

Konvencija o zabrani i trenutnoj akciji na eliminaciji najtežih oblika rada djece (No.C182 (1999))

Konvencija o zabrani i trenutnoj akciji na eliminaciji najtežih oblika rada djece (No.C182 (1999))⁹, Svaka članica mora, nakon savjetovanja s organizacijama poslodavaca i radnika, uspostaviti ili odrediti odgovarajuće mehanizme za praćenje sprovođenja odredbi kojima se osigurava primjena ove Konvencije i kao prioritetni

⁶ Konvencija o kibernetičkom kriminalu, član 1.

⁷ PREVENCIJA EKSPLOATACIJE DJECE U JUGOISTOČNOJ EVROPI EKSPLOATACIJA DJECE NA INTERNETU Poseban izvještaj Ombudsmana za djecu Republike Srpske Banja Luka, 2013.p.17.

⁸ Savjet Evrope, 2007. godina. „Službeni glasnik Bosne i Hercegovine“, Međunarodni ugovori, broj: 11/12

⁹ Međunarodna organizacija rada (ILO), 1999.godine; „Službeni glasnik Bosne i Hercegovine“, Međunarodni ugovori, broj: 3/01.

zadatak, osmisliti i sprovoditi programe djelovanja kako bi ukinula najgore oblike dječjeg rada.¹⁰

UN Konvencija protiv transnacionalnog organizovanog kriminala

UN Konvencija protiv transnacionalnog organizovanog kriminala¹¹, Osnovni cilj ovog međunarodnog dokumenta je da predviđenim mjerama poveća efikasnost u borbi protiv transnacionalnog organizovanog kriminala i to naročito u oblasti trgovine ljudima, s posebnim naglaskom na djecu.¹² Ova konvencija sadrži i protokol: Protokol za prevenciju, suzbijanje i kažnjavanje trgovine ljudima, naročito ženama i djecom, koji dopunjava Konvenciju Ujedinjenih nacija protiv transnacionalnog organizovanog kriminala.¹³

Konvencija Savjeta Evrope o borbi protiv trgovine ljudima

Konvencija Savjeta Evrope o borbi protiv trgovine ljudima¹⁴, Ciljevi Konvencije su:
a) sprečavanje i suzbijanje trgovine ljudima, uz garantovanje ravnopravnosti polova;
b) zaštita ljudskih prava žrtava trgovine ljudima, osmišljavanje sveobuhvatnog okvira za pružanje zaštite i pomoći žrtvama i svjedocima, uz garantovanje ravnopravnosti polova, kao i obezbjeđivanje efikasne istrage i krivičnog gonjenja;
c) unapređenje međunarodne saradnje u suzbijanju trgovine ljudima.¹⁵

Evropska konvencija o obeštećenju žrtava krivičnih djela nasilja (1983.g.)

Evropska konvencija o obeštećenju žrtava krivičnih djela nasilja (1983.g.)¹⁶, Ovom konvencijom se uspostavlja standard u oblasti obeštećenja žrtava krivičnih djela nasilja. Implementaciju ove konvencije prate i dvije preporuke koje pružaju dodatna obrazloženja i zahtjeve za preduzimanje mjera od strane država ugovornica:

- Preporuka o poziciji žrtve u okviru krivičnog prava i postupaka (1985.) i
- Preporuka o pomoći žrtvama i prevenciji viktimizacije (1987.).¹⁷

Evropska konvencija o zaštiti ljudskih prava i osnovnih sloboda

Evropska konvencija o zaštiti ljudskih prava i osnovnih sloboda¹⁸, Evropska konvencija je međunarodni ugovor između država članica Savjeta Evrope i temeljni akt na kojem se zasniva zaštita osnovnih ljudskih prava i sloboda. Ova konvencija sadrži niz prava koja su na direktan ili indirektan način u kontekstu predmetnog

¹⁰ PREVENCIJA EKSPLOATACIJE DJECE U JUGOISTOČNOJ EVROPI EKSPLOATACIJA DJECE NA INTERNETU Poseban izvještaj Ombudsmana za djecu Republike Srpske Banja Luka, 2013.p.19.

¹¹ „Službeni glasnik Bosne i Hercegovine“, Međunarodni ugovori, broj: 3/02.

¹² PREVENCIJA EKSPLOATACIJE DJECE U JUGOISTOČNOJ EVROPI EKSPLOATACIJA DJECE NA INTERNETU Poseban izvještaj Ombudsmana za djecu Republike Srpske Banja Luka, 2013.p.20.

¹³ Palermo, 13.12.2000. godine; Ratifikovano u Bosni i Hercegovini 05.02.2002. godine; „Službeni glasnik Bosne i Hercegovine“, Međunarodni ugovori“, broj: 3/02.

¹⁴ Ratifikovana od strane Bosne i Hercegovine 2007. godine.

¹⁵ PREVENCIJA EKSPLOATACIJE DJECE U JUGOISTOČNOJ EVROPI EKSPLOATACIJA DJECE NA INTERNETU Poseban izvještaj Ombudsmana za djecu Republike Srpske Banja Luka, 2013.p.23.

¹⁶ Predsjedništvo Bosne i Hercegovine je ratifikovalo ovu konvenciju na 72. sjednici održanoj 22.03.2005. godine. Odluka o ratifikaciji konvencije objavljena je u „Službenom glasniku Bosne i Hercegovine“, broj 4/05. Stupila na snagu 14.04.2005. godine.

¹⁷ PREVENCIJA EKSPLOATACIJE DJECE U JUGOISTOČNOJ EVROPI EKSPLOATACIJA DJECE NA INTERNETU Poseban izvještaj Ombudsmana za djecu Republike Srpske Banja Luka, 2013.p.24.

¹⁸ U skladu sa Ustavom Bosne i Hercegovine, Evropska konvencija i njeni protokoli se direktno primjenjuju u pravnom sistemu Bosne i Hercegovine sa prioritonom nad svim drugim zakonima.

istraživanja, kao npr: pravo na život (član 2.), zabranu mučenja i podvrgavanja neljudskom ili ponižavajućem postupku (član 3.), zabranu držanja u ropstvu ili primoravanju na obavljanje prinudnog ili obaveznog rada (član 4.), pravna slobodu i sigurnost ličnosti (član 5.), pravo na poštivanje privatnog i porodičnog života (član 8.), zabranu diskriminacije po bilo kojem osnovu (član 14.), zabranu zloupotrebe prava (član 17.), itd.¹⁹

Domaći propisi

Pored međunarodnih akata i domaći propisi, počevši od Ustava pa do zakona i podzakonskih propisa takođe zahtijevaju od organa vlasti u Bosni i Hercegovini i njenim entitetima da osiguraju adekvatnu zaštitu prava i interesa djeteta.

Ustav Bosne i Hercegovine

Ustav Bosne i Hercegovine utvrđuju osnovna ljudska prava i slobode i garantuju da niko ne može biti podvrgnut mučenju, svirepom, nehumanom ili ponižavajućem postupanju, utvrđuju i garantuju nepovredivost ljudskog dostojanstva, tjelesnog i duhovnog integriteta, privatnosti i porodičnog života. Pored opštih principa koji se odnose na zaštitu prava i interesa čovjeka, pa time i djeteta, zaštita od iskorišćavanja i zloupotrebe putem savremenih komunikacionih tehnologija kao što su internet i mobilni telefoni, u Bosni i Hercegovini uspostavljena je kroz pravni okvir kojim je normirana oblast komunikacija.²⁰

Zakon o komunikacijama BiH

Zakon o komunikacijama²¹, Ovim zakonom regulisana je oblast komunikacija u Bosni i Hercegovini, te uspostavljanje i rad Regulatorne agencije za komunikacije Bosne i Hercegovine u skladu sa Ustavom Bosne i Hercegovine. Komunikacije uključuju telekomunikacije, radio, emitovanje i usluge i sredstva koja su s tim u vezi. Ovim zakonom su određene institucije i utvrđena nadležnost institucija Bosne i Hercegovine u oblasti Komunikacija.²²

Zakon o zaštiti ličnih podataka BiH

Zakon o zaštiti ličnih podataka²³, S obzirom na to da je upotreba, savremenih komunikacionih tehnologija, posebno mobilnih telefona i interneta veoma popularna i raširena, da se elektronska pošta danas koristi u mnogim oblastima poslovnog i društvenog života i djelovanja, da institucije državnog aparata koriste sredstva takvih tehnologija i da posjeduju baze podataka u koje pohranjuju razne informacije i podatke, ali i lične podatke građana, postoji realna mogućnost i za nedozvoljeno korišćenje i zloupotrebu tih podataka i svrhu vršenja krivičnih djela.²⁴

¹⁹ PREVENCIJA EKSPLOATACIJE DJECE U JUGOISTOČNOJ EVROPI EKSPLOATACIJA DJECE NA INTERNETU Poseban izvještaj Ombudsmana za djecu Republike Srpske Banja Luka, 2013.p.24.

²⁰ PREVENCIJA EKSPLOATACIJE DJECE U JUGOISTOČNOJ EVROPI EKSPLOATACIJA DJECE NA INTERNETU Poseban izvještaj Ombudsmana za djecu Republike Srpske Banja Luka, 2013.p.26.

²¹ Zakon o komunikacijama, „Službeni glasnik BiH“ broj 31/03, 35/06 i 32/10

²² PREVENCIJA EKSPLOATACIJE DJECE U JUGOISTOČNOJ EVROPI EKSPLOATACIJA DJECE NA INTERNETU Poseban izvještaj Ombudsmana za djecu Republike Srpske Banja Luka, 2013.p.26.

²³ Zakon o zaštiti ličnih podataka, „Službeni glasnik BiH“ broj 49/06 i 76/11

²⁴ PREVENCIJA EKSPLOATACIJE DJECE U JUGOISTOČNOJ EVROPI EKSPLOATACIJA DJECE NA INTERNETU Poseban izvještaj Ombudsmana za djecu Republike Srpske Banja Luka, 2013.p.27.

Krivični zakon Bosne i Hercegovin

Krivični zakon Bosne i Hercegovine²⁵, Krivično-pravnu zaštitu od nedozvoljenog korišćenja ličnih podataka na nivou Bosne i Hercegovine zakonodavac pruža i kroz Krivični zakon Bosne i Hercegovine i kao krivično djelo propisuje *Nedozvoljeno korišćenje ličnih podataka* i utvrđuje da će se svako službeno ili odgovorno lice u institucijama Bosne i Hercegovine koje bez pristanka pojedinca protivno uslovima propisanim u zakonu, prikuplja, obrađuje ili koristi njegove lične podatke ili te podatke koristi suprotno zakonom dozvoljenoj svrsi njihova prikupljanja, kazniti novčanom kaznom ili kaznom zatvora. Bitno je napomenuti da pomenutu problematiku regulišu i entitetski krivični zakoni, odnosno KZ FBiH, KZ RS, KZ BD.²⁶

Zakon o krivičnom postupku Bosne i Hercegovine

Zakon o krivičnom postupku Bosne i Hercegovine²⁷, sve veća opasnost od vršenja krivičnih djela putem savremenih komunikacionih tehnologija, zahtijeva i potrebu stalne borbe i angažovanja brojnih subjekata protiv kriminala te vrste, te je u tom kontekstu potrebno ukazati i na odredbe koje u sebi sadrži Zakon o krivičnom postupku Bosne i Hercegovine. Ovim zakonom utvrđena su pravila krivičnog postupka po kojima su dužni da postupaju sudovi, tužilac i drugi učesnici u krivičnom postupku kada postupaju u krivičnim stvarima radi dokazivanja određenog krivičnog djela. Bitno je napomenuti da pomenutu problematiku regulišu i entitetski zakoni o krivičnom postupku, odnosno ZKP FBiH, ZKP RS, ZKP BD.²⁸ Pored pomenutih zakona i podzakonskih akata, koji regulišu navedenu oblast, navodimo još nekoliko njih, koji su doneseni na nivo vlade SBK/KSB, a koji zantno utiču na navedenu problematiku, odnosno, propisi koji u mnogome doprinose zaštiti i kontroli djece, u ovom slučaju, kada je u pitanju sistem informacionih tehnologija i interneta.

- Zakon o osnovnom školstvu, Službene novine SBK/KSB, broj; 11/01, 11/04, 17/04,²⁹
- Zakon o srednjem školstvu, Službene novine SBK/KSB, broj; 11/01, 11/04, 17/04,³⁰
- Protokol o postupanju u slučaju, nasil, ja u školi, Vlada SBK/KSB Federacije Bosne i Hercegovine.³¹

²⁵ Krivični zakon Bosne i Hercegovine, „Službeni glasnik BiH“ br. 3/03, 32/03, 37/03, 54/04, 61/04, 30/05, 53/06, 55/06, 32/07

²⁶Službene novine Federacije Bosne i Hercegovine” br. 36/03, http://tuzilastvobih.gov.ba/files/docs/zakoni/ZKP_FBiH/ZKP_FBiH_35_03_bos.pdf, Službeni glasnik Republike Srpske” broj 49, od 25. juna 2003. Godine, http://univerzitetpim.com/wp-content/uploads/2013/03/Krivicni-zakon_RS.pdf, (Službeni glasnik Brčko distrikta BiH, brojevi 6/05, 21/10 i 9/13). <http://www.skupstinabd.ba/zakoni/2013/Krivicni%20zakon.%20preciscen%20tekst%20B.pdf>.

²⁷ Zakon o krivičnom postupku " Službeni glasnik ' ' , broj 36 , od 21 Novembar 2003

²⁸ Službene novine Federacije Bosne i Hercegovine” br. 35/03, http://tuzilastvobih.gov.ba/files/docs/zakoni/ZKP_FBiH/ZKP_FBiH_35_03_bos.pdf, Službeni glasnik Republike Srpske” br. 100/09,

http://www.tuzilastvobih.gov.ba/files/docs/Copy_of_Zakon_o_krivicnom_postupku_RS_precisceni_tekst_100_09_bos.pdf, (Službeni glasnik Brčko distrikta BiH, brojevi: 48/04, 6/05, 14/07, 19/07, 21/07, 2/08, 17/09 i 9/13). <http://www.skupstinabd.ba/zakoni/2013/Zakon%20o%20krivicnom%20postupku%20BDBiH,%20preciscen%20tekst%20B.pdf>.

²⁹ <http://hea.gov.ba/Dokumenti/Zakoni-propisi?id=4035>,

³⁰ <http://hea.gov.ba/Dokumenti/Zakoni-propisi?id=4035>,

³¹<http://www.mozksksb.ba/Dokumenti/OpciDokumenti/PROTOKOL%20O%20POSTUPANJU%20U%20SLUCAJU%20NASILJA%20OU%20SKOLI.pdf>.

Akcioni plan za djecu Bosne i Hercegovine 2011-2014.

OPĆI CILJ: Definiranje prioriternih ciljeva i mjera koje je neophodno poduzeti u periodu 2011. – 2014. godine, da bi se stvorili što povoljniji uvjeti za život djece i porodice, njihovo zdravo psiho-fizičko odrastanje i uključivanje u društvo i participaciju u odlučivanju, a u najboljem interesu djece.

Pravni okvir je izdvojen kao jedna cjelina, a posebni ciljevi i mjere u ovom dokumentu definirani su prema oblastima: zdravlje, obrazovanje, socijalna zaštita, djeca iz ranjivih grupa i drugi vidovi zaštite djece ili posebni oblici zaštite djece. Realizacijom predviđenih posebnih ciljeva i mjera u ovom Akcionom planu, može se očekivati znatno poboljšanje politika i praksi prema djeci i njihovim porodicama na svim nivoima vlasti u BiH.³²

ZAKLJUČAK

U zaključku možemo konstatovati da je BiH ratifikovala mnoge međunarodne konvencije i propise koje regulišu ovu oblast, zaštite djeteta uopšte, pa samim tim i na internetu. Isto tako jasno je da je BiH, usvojila mnoge domaće propise koji su svakako usklađeni s međunarodnim. Međutim, potrebno je osigurati jednaku pravnu zaštitu djece usklađivanjem zakona u praksi Bosne i Hercegovine, u skladu sa Konvencijom o pravima djeteta i, posebno, harmonizirati sve propise koji se odnose na segment zaštite prava djeteta, uključujući i harmonizaciju u ovoj oblasti unutar Bosne i Hercegovine, između propisa koje donosi Bosna i Hercegovina, Federacija Bosne i Hercegovine i kantoni, Republika Srpska i Distrikt Brčko Bosne i Hercegovine.

LITERATURA

1. Akcioni plan za djecu Bosne i Hercegovine 2011-2014,
2. Evropska konvencija o zaštiti ljudskih prava i osnovnih sloboda,
3. Evropska konvencija o obeštećenju žrtava krivičnih djela nasilja (1983.g.),
4. Evropska konvencija o kibernetičkom kriminalu,
5. Fakultativni protokol uz konvenciju o pravima djeteta, o prodaji djece, dječijoj prostituciji i pornografiji,
6. Konvencija o zaštiti djece od seksualnog iskorištavanja i seksualnog zlostavljanja (Savjet Evrope - CETS No201,
7. Konvencija o zabrani i trenutnoj akciji na eliminaciji najtežih oblika rada djece (No.C182 (1999)),
8. Konvencija Savjeta Evrope o borbi protiv trgovine ljudima,
9. Krivični zakon BiH, FBiH, RS, BD,
10. Okvini zakon o osnovnom i srednjem obrazovanju Bosne i Hercegovine,
11. PREVENCIJA EKSPLOATACIJE DJECE U JUGOISTOČNOJ EVROPI EKSPLOATACIJA DJECE NA INTERNETU Poseban izvještaj Ombudsmana za djecu Republike Srpske Banja Luka, 2013.
12. Protokol o postupanju u slučaju, nasil, ja u školi, Vlada SBK/KSB Federacije Bosne i Hercegovine,

³² http://www.mhrr.gov.ba/ljudska_prava/djeca_bih/Akcioni%20plan%20za%20djecu%202011%202014.pdf.

13. Protokol za prevenciju, suzbijanje i kažnjavanje trgovine ljudima, naročito ženama i djecom, koji dopunjava Konvenciju Ujedinjenih nacija protiv transnacionalnog organizovanog kriminala,
14. UN Konvencija o pravima djeteta,
15. UN Konvencija protiv transnacionalnog organizovanog kriminala,
16. Ustav Bosne i Hercegovine,
17. Zakon o komunikacijama BiH,
18. Zakon o zaštiti ličnih podataka BiH,
19. Zakon o krivičnom postupku BiH, FBiH, RS, BD,
20. Zakon o osnovnom školstvu, Službene novine SBK/KSB, broj; 11/01, 11/04, 17/04,
21. Zakon o srednjem školstvu, Službene novine SBK/KSB, broj; 11/01, 11/04, 17/04,
22. http://tuzilastvobih.gov.ba/files/docs/zakoni/ZKP_FBiH/ZKP_FBiH_35_03_bos.pdf
23. http://univerzitetpim.com/wp-content/uploads/2013/03/Krivicni-zakon_RS.pdf,
24. <http://www.skupstinabd.ba/zakoni/2013/Krivicni%20zakon,%20preciscen%20tekst%20B.pdf>.
25. http://tuzilastvobih.gov.ba/files/docs/zakoni/ZKP_FBiH/ZKP_FBiH_35_03_bos.pdf,
26. http://www.tuzilastvobih.gov.ba/files/docs/Copy_of_Zakon_o_krivicnom_postupku_RS_precisceni_tekst_100_09_bos.pdf
27. <http://www.skupstinabd.ba/zakoni/2013/Zakon%20o%20krivicnom%20postupku%20BDBiH,%20preciscen%20tekst%20B.pdf>.
28. <http://hea.gov.ba/Dokumenti/Zakoni-propisi/?id=4035>,
29. <http://hea.gov.ba/Dokumenti/Zakoni-propisi/?id=4035>,
30. [Http://www.mozksksb.ba/Dokumenti/OpciDokumenti/PROTOKOL%20O%20POSTUPANJU%20U%20SLUCAJU%20NASILJA%20U%20SKOLI.pdf](http://www.mozksksb.ba/Dokumenti/OpciDokumenti/PROTOKOL%20O%20POSTUPANJU%20U%20SLUCAJU%20NASILJA%20U%20SKOLI.pdf),
31. http://www.mhrr.gov.ba/ljudska_prava/djeca_bih/Akcioni%20plan%20za%20odjecu%202011%202014.pdf.

PRESTIGIO MULTIBOARD ALL-IN-ONE PC
doc.dr Hadžib Salkić, Jasmin Kahrman
Sveučilište/Univerzitet Vitez
Dalcom d.o.o., Zenica, Bosna i Hercegovina
hadzib.salkic@unvi.edu.ba, jasmin.kahrman@dalcom.com.ba

SAŽETAK

Prestigio MultiBoard All-in-One PC nudi sklop jedinstvene tehnologije koja ima za cilj povećati interakciju, kolaboraciju i produktivnost među korisnicima, te u jednom uređaju ponuditi kompletno rješenje u poređenju sa današnjim projektorima, interaktivnim Smart tablama i drugim sličnim proizvodima. Zamislite poslovni računar sa posljednjom Intel tehnologijom i preinstaliranim MS Windows 8.1 operativnim sistemom, na uistinu velikom ekranu osjetljivim na dodir i otpornim na udarce, koji ujedno možete koristiti i kao funkcionalan TV u najsavremenijoj HD rezoluciji. Dodatak svemu ovome je niz preinstaliranih interaktivnih aplikacija korisnih za edukaciju, vođenje poslovnih sastanaka, te konferencijske pozive sa partnerima i saradnicima na drugim lokacijama.

Ključne riječi: Prestigio Multiboard AIO PC, Prestigio Visconte, Edukacija.

SPECIFIKACIJA PRESTIGIO MULTIBOARD AIO PC

Prestigio Multiboard je digitalni Full HD ekran sa Multi-Touch tehnologijom, integrisanim Intel PC računarom, instaliranim Windows 8.1 operativnim sistemom i brojnim specijalno razvijenim aplikacijama, koji zajedno nude jedinstvena interaktivna rješenja za edukacijske, poslovne i privatne potrebe tokom višegodišnjeg korištenja. Prestigio Multiboard AIO PC je spoj hardware i software, pomoću kojega ćete raditi i informirati brže i učinkovitije nego dosad. Nema više monotonih ploča, papira, projektor, pratećeg PC-a. **Prestigio MultiBoard** donosi boju, sliku, zvuk, interakciju i dinamiku u jednom jedinom uređaju.



Slika 1: Prestigio Multiboard All-In-One Solution

Prestigio Multiboard AIO PC karakteriše tanak LED ekran u različitim dimenzijama 55", 65", 70" i 84", od kojih 55", 65" i 70" dolaze u Full HD rezoluciji 1920x1080 piksela, i 84" model koji čak dolazi u UltraHD rezoluciji od 3840x2160 piksela. Široki ugao vidljivosti od 178 stepeni obezbeđuje kvalitetnu sliku bez uobičajenih sjenki pod bilo kakvim osvjetljenjem. Prestigio garantuje nesmetan rad LED ekrana na čak 80.000 radnih sati bez potrebe sa servisiranjem.

Compare models	MultiBoard 84" Series 5 PMB554H847	MultiBoard 70" Series 5 PMB554H707	MultiBoard 65" Series 5 PMB554H657	MultiBoard 55" Series 5 PMB554H557
				
	Top Quality for Real Productivity	Right Solution to Answer Real Needs	The Most Popular Design and Size	Designed for Meeting Rooms
Article	PMB554H847	PMB554H707	PMB554H657	PMB554H557
Series	5	5	5	5

Slika 2: Upoređivanje različitih modela Multiboard uređaja u zavisnosti od veličine ekrana

Radi se o Multi-Touch LED ekranu koji je u stanju podnijeti nepredviđene udarce, nepažljivo rukovanje ekranom ili često premještanje uređaja tokom svakodnevne upotrebe. Prestigio Multiboard AIO PC posjeduje ekran presvučen izuzetno izdržljivim Steel Glass materijalom predviđenim da izdrži okolnosti u industrijskoj upotrebi. Na Mohsovoj skali koja predstavlja niz od deset minerala poredanih po tvrdoći i izdržljivosti, Steel Glass zauzima sedmo mjesto, na kojem se nalaze minerali kao što je kremen ili kvarc, što je samo tri mjesta ispod jednog od najčvršćih materijala poznatog čovjeku, dijamanta. Važno je istaći da sigurnosni zaslon ekrana ne umanjuje kvalitet HD slike i veoma je jednostavan za održavanje, sve što zahtjeva je da se ekran povremeno obriše vlažnom krpom kako bi se uklonile masnoće i otisci prstiju. Ostatak Multiboard uređaja napravljen je od čvrste metalne konstrukcije sa posebnim otvorima za ventilaciju, koji upotpunjuju sigurnost uređaja uz minimalno zagrijavanje tokom duge upotrebe.



Slika 3: Izdržljivost i sigurnost na Prestigio način

Zahvaljujući unaprijeđenoj INFRA-RED Multi-Touch tehnologiji, LED ekran podržava do 6 dodirnih tačaka sa vremenom odziva manjim od 4 ms, što omogućava pisanje i upravljanje po ekranu sa čak 6 prstiju istovremeno.



Slika 4: Napredna Multi-Touch tehnologija sa podrškom 6 dodirnih tačaka

Postolja su posebno dizajnirana da podnesu težinu Multiboard uređaja i obezbijede sigurno korištenje uređaja. Svi stalci su izrađeni od nehrđajućih metala i dolaze na točkovima radi mobilnosti, koji se mogu zakočiti po potrebi radi dodatne sigurnosti.



Slika 5: Prestigio Multiboard AIO PC nam pruža veliki izbor indoor/outdoor postolja

Unutar kućišta Prestigio Multiboard AIO se nalazi integrisan računar malih dimenzija i visokih performansi, jednostavan za instalaciju, koji se može odvojiti od Multiboard ekrana. Modularni PC dolazi sa procesorom nove generacije Intel Core i3/i5/i7, 4 GB/8 GB DDR3 memorije, 500 GB/1 TB HDD, integrisanom VGA kartom HD 4000 i RealTek HighDefinition zvučnom karticom. U sklopu modularnog računara integrisana je WiFi kartica sa podrškom različitih standarda 802.11b/g/n. Različiti standardi nude različitu modulaciju signala, različitu propusnost i frekvencije rada. Unutar uređaja su ugrađena dva stereo zvučnika sa dva pojačala od 10W, čime obezbjeđuju kristalno čist i dinamičan zvuk optimalnog balansa sa tonovima visoke kvalitete. Multiboard AIO PC karakteriše izuzetno mala potrošnja električne energije kroz voltažu dometa 100-240V. Prilikom paljenja, operativni sistem na MultiBoard-u se veoma brzo pokreće i nema potrebe za dodatnim zagrijavanjem. U Standby modu troši manje od 0.5W. U sklopu LED ekrana i ugrađenog PC-a, MultiBoard nudi brojne priključke za eksterne periferije koji uključuju 6 x USB, 1xAV In, 1xAV Out, 1xCOAX, 2xVGA, 1xYPbPr, 1xMultimedia USB, 2xTouch Control USB, 2xHDMI, 2xPC Audio In, 1xPC Mic.



Slika 6: Prestigio Multiboard AIO dolazi sa integrisanim PC

Prestigio Multiboard AIO PC dolazi sa preinstaliran Windows 8.1 Pro operativnim sistemom i dodatnim aplikacijama EasiNote, EasiMeeting, EasiShow, EasiSign i PC WiFi Control. Aplikacije nude nova rješenja i mogućnosti tokom svakodnevnog rada uključujući komunikaciju, interakciju i kolaboraciju sa drugim učesnicima. Prestigio Multiboard AIO PC je jednostavan za instalaciju i upotrebu. Pored funkcije Windows 8.1 PC, Multiboard možemo koristiti i kao potpuno funkcionalan HD TV primjenik, te kao projektno platno ili interaktivna Smart tabla. Prestigio MultiBoard dolazi uz 2 godine fabričke garancije, koja se može produžiti na 3 ili 5 godina. Po specifikaciji, životni vijek uređaja je 80.000 radnih sati bez potrebe za redovnim servisom, što znači da se uređaj može koristiti 24 sata dnevno preko 10 godina bez dodatnih investicija za održavanje.

Tabela 1: Hardverska specifikacija Prestigio Multiboard AIO PC

Display	LED widescreen ekran (podržava milione boja) Rezolucija: 55“, 65“, 70“ – FullHD 1920x1080 piksela 84“ – UltraHD 3840x2160 piksela
PC	Modular Intel Intel Huron River Sandy Bridge i3/i5/i7 RAM 4GB / 8 GB DDR3 VGA HD 4000 Integrated HDD 500 GB / 1 TB NIC10/100/1000M Adaption WiFi 802.11b/g/n Integrated High Definition Audio Stereo USB(A) 6, Microphone, Earphone Out, VGA Out

Operativni sistem	Windows 7/8/8.1
Touch Frame	<p>Infra-red tehnologija</p> <p>MOHS 7 Steel Glass</p> <p>Vrijeme odziva na dodir manje od 4ms</p> <p>Podržano do 6 tačake dodira istovremeno</p> <p>Driver-free</p>
Audio	Ugrađena 2 stereo zvučnika sa 2 pojačala od 10W
Connections and Expansions	1xAV In; 1xAV Out; 1xCOAX; 2xVGA; 1xYPbPr; 1xMultimedia USB; 2xTouch Control USB; 2xHDMI; 2xPC Audio In; 1xPC Microphone
Power	<p>Podržana voltaža 100-240V AC</p> <p>Standby potrošnje struje < 0.5W</p>

PRIMJENA PRESTIGIO MULTIBOARD AIO PC

Obzirom na pomenutu specifikaciju i visoke performanse, Prestigio Multiboard AIO PC je fokusiran na obrazovne, zdravstvene i ostale institucije, ali također i na poslovne skupove te konferencije. Koristeći Prestigio Multiboard AIO PC i prateće aplikacije unutar obrazovnih institucija, poboljšavamo interaktivnost između profesora i studenata, te povećavamo angažman studenata na rješavanju određenog problema. Pored edukativne svrhe, Prestigio Multiboard AIO PC omogućava održavanje video konferencija, čime poboljšavamo produktivnost i smanjujemo troškove komunikacije. Prestigio Multiboard AIO PC možemo koristiti i kao sistem centralizovanog prenosa informacija, slika, videa, teksta i tona u realnom vremenu, Digital Signage (max 800 display-a). Koristeći Central Management Server upravljamo sadržajima dostupnim u javnosti.



Slika 7: Primjena Prestigio Multiboard AIO PC

Za razliku od interaktivnog displaya, čija je instalacija i puštanje u rad zahtjeva mnogo više uređaja (PC, projektor, pen, zvučnici, kablovi), a samim tim i više vremena, Prestigio Multiboard nam omogućava jednostavnu instalaciju i korištenje. Inovativan koncept Multiboard uređaja omogućava institucijama, kompletno poslovanje i edukaciju, u zavisnosti od krajnje namjene Multiboard AIO PC.



Slika 8: Interactive whiteboard vs. Prestigio Multiboard AIO PC

Prestigio Education Solution je interaktivna tehnologija usmjerena prema poboljšanju produktivnosti i interakcije među učiteljima i učenicima. Osmišljen je na način da pruži studentima i profesorima novo okruženje bez upotrebe table, krede i papira, kao primarnih metoda ostvarivanja komunikacije između profesora i učenika. U ovom slučaju studenti koriste Tablet PC, što omogućava profesorima potpunu kontrolu nastavnog procesa. Prestigio Multiboard i dodatne aplikacije, uključujući EasyNote aplikaciju nam pruža efikasno, efektivno i samim time produktivno okruženje, koje nam omogućava pisanje, crtanje grafikona, uređivanje sadržaja, i sve to koristeći touch screen.



Slika 8: Komunikacija nastavnika sa učenicima koristeći Prestigio Multiboard AIO PC

Elektronski sadržaj umjesto tradicionalnih knjiga obezbjeđuje manji broj potrebnog školskog pribora, jednostavniju pohranu podataka, 24/7 pristup edukativnim resursima i ECO društvenu sredinu. Prestigio edukacijska rješenja su pristupačna po povoljnim cijenama i jedostavnom implementacijom.



Slika 9: Elektronsko pristupanje edukativnim sadržajima

Implementacijom mrežnog okruženja između profesora i učenika, ostvarujemo centralizovano upravljanje i kontrolu sadržaja prikazanog na tabletima koje koriste studenti. Da bi interakcija između profesora i studenata bila funkcionalna Prestigio Solution nam nudi tri glavne komponente, koje uključuju Prestigio Multiboard AIO PC, Prestigio Multipad kao interfejs za eksterne učesnike, sa dodatnom opremom po zahtjevu klijenta: web kamera, mikروفon, tastatura/miš, i posebno dizajnirane aplikacije, kao ključni faktor rješavanja određenog problema. Multiboard AIO PC je elegantan spoj obrazovanja i tehnologije.



Slika 11: Šta nam je potrebno za uspostavljanje funkcionalnog okruženja?

Posebno dizajnirane aplikacije za Prestigio MultiBoard nude korisniku potpuno nova rješenja i mogućnosti. Različite aplikacije omogućavaju rješavanje različitih zahtjeva, što je prikazano u tabeli 2.

Tabela 2: Prestigio MultiBoard aplikacije i njihova namjena

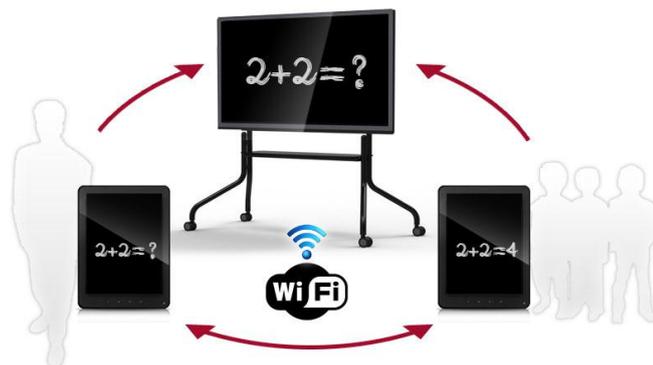
Naziv aplikacije	Namjena
Prestigio EasiNote	Pretvara MultiBoard ekran u interaktivnu elektronsku tablu koja registruje i prikazuje svaki dodir
Prestigio EasiMeeting	Posebno razvijena MultiBoard aplikacija nudi produktivna rješenja za poslovne prezentacije i sastanke
Prestigio EasiHow	Kreativna rješenja za prezentacije sa Multi-Touch tehnologijom i specijalnim animiranim efektima
Prestigio EasiSign	Inovativan signature software sa Camera Shot funkcijom za video sastanke i konferencije

Komunikaciju sa Multiboard AIO PC, studenti ostvaruju pomoću Prestigio Visconte uređaja. Naime, radi se o moćnom PC tabletu sa najnovijim Intel procesorom i Windows 8.1 operativnim sistemom, ali ujedno i istinskim mobilnim uređajem potpuno prilagođenom Prestigio MultiBoard rješenju. Prestigio Visconte podržava LOB (Line-of-Business aplikacije), te za zahtjevnije korisnike omogućava priključenje tastature, kao opcionalnog uređaja.



Slika 12: Prestigio Visconte

Primjer na osnovu kojeg radi Prestigio Multiboard AIO PC je predstavljen na Slici 13. Između Prestigio Multiboard AIO PC i Prestigio Multipad uređaja uspostavljena je bežična mreža koja omogućava komunikaciju između uređaja. Naime, radi se o jednostavnom matematičkom zadatku, gdje profesor postavlja zadatak koliko je $2+2=?$ Na svojim tablet uređajima, studenti dobiju navedeni zadatak, i odgovaraju.



Slika 13: Kako radi Prestigio Multiboard AIO PC?

U narednom periodu Prestigio će nuditi posebno razvijen software za edukaciju „Mythware Classroom Management“, koji predstavlja veoma interaktivnu aplikaciju koja funkcioniše po modelu Digitalne učionice za novo i poboljšano korisničko iskustvo sa profesore, učitelje i studente. Kroz ovo rješenje, profesor preko MultiBoard-a može voditi nastavu, prezentovati nastavni sadržaj i isti prenositi uživo na tablete studenata, imati interakciju i razmjenu podataka sa studentima preko njihovih tableta, kreirati testove i proslijediti ih studentima na tablete, te na kraju prikupiti sve testove i pojedinačno ili grupno ih ocjeniti i analizirati. Ono što je važno istaći je da tokom korištenja ove aplikacije profesor/učitelj ima potpunu kontrolu nad nastavom i tabletima koji se nalaze kod studenata. Mythware Classroom Management omogućava testiranje u trial verziji od 30 dana, uz prethodno implementirano mrežno okruženje. Prvi korak je kreiranje i aktiviranje korisničkog računa na <http://www.mythware.com/>, te preuzimanje Software u zavisnosti od OS platforme koju koristimo (Windows, Linux, Android). Zadovoljstvo mi je napomenuti da su Prestigio Multiboard All-in-One uređaji dostupni u prodaji na tržištu Bosne i Hercegovine.

Ekkluzivni distributer Prestigio uređaja na području Bosne i Hercegovine, je kompanija Asbis d.o.o., sa sjedištem u Sarajevu (www.asbis.ba; info@asbis.ba). Prva obrazovna institucija koja se odlučila za kupovinu i korištenje Prestigio Multiboard rješenja na području Bosne i Hercegovine je Sarajevo School of Science and Technology (SSST). Shodno pozitivnim komentarima korisnika koji su kupili Prestigio Multiboard uređaje, broj zainteresiranih korisnika je u porastu. Prestigio MultiBoard je rješenje koje možete opušteno koristiti i dozvoliti svojim poslovnim kolegama ili učenicima da neometano razvijaju svoje znanje, kreativnost i produktivnost tokom svakodnevnog korištenja istog.

"Prestigio je uvijek maksimalno posvećen svom primarnom cilju, a to je ponuda najmodernijih tehnoloških rješenja svim tržišnim segmentima. MultiBoard donosi novu dimenziju u poslovanju, edukaciji i oglašavanju. Kao i uvijek dosad, po vrlo prihvatljivoj cijeni." Sergei Kostevitch, ASBIS CEO

LITERATURA

[1] <http://www.prestigio.com/catalogue/MultiBoards> (09.04.2014.)

**DATA MINING
RUDARENJEM DO ZDRAVLJA I PROSPERITETA
(BOINC)**

Damir Emić, BA
SVEUČILIŠTE/UNIVERZITET „VITEZ“, Vitez, BiH,
damir.emic@outlook.com

SAŽETAK

Danas, kada su svuda oko nas informaciono komunikacione tehnologije (IKT), kada se oko nas kreću milioni frekvencija u različitim frekventnim opsezima, kada na jednog stanovnika zemlje postoje tri mobilna telefonska aparata, dok je jedan od njih „smartphone“, kada svako domaćinstvo posjeduje računar bio on stacionirani ili mobilan (računar, tablet, smartwatch...), koristio on operativni sistem na platformi Windowsa, Linuxa, Androida ili drugi, može se reći da su sve te IKT, bile one software-skog ili hardware-skog karaktera iskorištene u najboljem slučaju do 15%. Iz predhodnog zaključujemo da je 85% resursa IKT opreme pojedinca neiskorišteno dok se za iste troši energija, internet te ostali potrebni resursi. Dolazimo do zaključka zašto ne iskoristiti te neiskorištene resurse u data mining (rudarenje) koristeći „BOINC“ za napredak općeg zdravlja i prosperiteta (naučno istraživačke svrhe za opće dobro).

Ključne riječi: data, mining, rudarenje podataka, BOINC, IKT, zdravlje, prosperitet, naučno istraživački rad, opće dobro.

UVOD

Obzirom da se nalazimo u informatičkoj eri, gdje kao najvažniji resurs imamo „informaciju“, da se oko nas uz pomoć IKT-a kreću milijarde podataka, postavlja se pitanje kako doći do informacije iz mora tih podataka, kako iskoristiti te podatke i iz njihovih sekvenci ili pak cjelina izuzeti potrebne informacije, jer sam podatak kao takav je neiskoristiv sve onda do kad se skup tih podataka ne pretvori u jednu cjelinu koju nazivamo informacijom. Danas, svaki pojedinac, firma, udruženje posjeduje skup podataka, bili oni složeni strukturano ili nestrukturano, sa ili bez baza podataka, potrebno je iz tog skupa izdvojiti informacije koje su iskoristive za dobro pojedinca, firme ili dr. Tu nastupa „Data mining“, kod nas usvojen termin „rudarenje podataka“. Kako je navedeno u Apstraktu rada da je samo 15% resursa IKT opreme pojedinca iskorišteno, dok za ostalih 85% resursa opreme nije, a za iste se troši energija za napajanje i internet za komunikaciju BOINC platforma sa Univerziteta California, Berkeley došla na ideju kako da se ti isti resursi iskoriste u naučno istraživačke svrhe za napredak zdravlja, prosperiteta i općeg dobra.

POJAM DATA MINING (PODATAK, INFORMACIJA, ZNANJE)

Da bi se razumio pojam „Data mining-a“ potrebo je razumijeti razliku između podatka, informacije i znanja. Podatak je jednostavna neobrađena izolirana misaona činjenica koja ima neko značenje, dok je informacija rezultat analize i organizacije

podataka na način da daje novo znanje primatelju. Znanje je odgovarajuća zbirka informacija kojoj je namjera da bude korisna. [1]

Rudarenje podataka ili podatkovno rudarenje (eng. Data mining) je sortiranje, organiziranje ili grupisanje velikog broja podataka i izvlačenje relevantnih informacija. Sam termin mogli bismo objasniti kao proces pronalaženja korisnog znanja ili informacija, odnosno otkrivanje znanja iz velike količine podataka. Rudarenjem se poboljšava proces donošenja odluka na strateško-poslovnoj razini pružajući uvid u «skriven» podatke business intelligence (BI) metodologijom. Rudarenjem se također otkrivaju odnosi, logičnost, pravilnost te općenito bilo kakve strukture među podacima. Rudarenje podrazumijeva organiziranje baza čišćenjem podataka kako bi se pristupilo znanju i sticanju istog na temelju postojećih podataka u bazama. Razvoj tehnologije, računara, interneta bitno doprinosi lakšem organizovanju podataka, no da bi oni postali korisni, potrebno je njihovo pretvaranje u informacije i znanje. Termin rudarenja često se poistovjećuje sa 2 različita procesa: otkrivanje i predviđanje znanja. Proces otkrivanja znanja implicira korisnikovo razumijevanje eksplicitnih informacija za koje je bitno da su u čitljivom obliku. Predviđanje se odnosi na buduće događaje i u nekim pristupima može biti čitljivo i prozirno dok u drugim neprovidno.

Rudarenje je metoda kojom je U.S. Army uspjela identificirati vođu napada na Twin Towers, 11.9.2001., a tom se metodom također koriste CIA i Canadian Security Intelligence Service.

Data mining je proces u kojem se koriste sljedeće metode kako bi se otkrili skriveni uzorci, šablone podataka: neuronske mreže (virtualne mreže uređene po uzoru na ljudski mozak, u kojima različiti dijelovi mreže istovremeno procesuiraju informacije, te „proučavaju i pamte“ prošle šablone, uzorke podataka), grupisanje podataka, genetski algoritmi (kombinovanje određenih podataka kako bi se pronašlo rješenje za neki problem). Pretraživanje podataka bazirano na subjektu je metoda u kojoj se traže asocijacije između pojedinih podataka. Data mining se zasniva na poznavanju, odnosno predviđanju ponašanja varijabli koje čine svaki podatak u bazi podataka. Tačnije, zasniva se na poznavanju parametara varijabli (statistički podaci kao što su minimum, maksimum, standardna devijacija, itd.), te na znanju što svaka varijabla predstavlja u stvarnom svijetu, koje su varijable potencijalno korisne i kako se varijable u bazi podataka odnose međusobno. Jednomjerne, dvomjerne, višemjerne tehnike – i tablice i grafikoni – su tehnike koje se prvenstveno koriste. [2]

BOINC

O BOINC-u

BOINC platforma (eng: Berkley Open Infrastructure for Network Computing, Otvorena infrastruktura za mrežno računarstvo na Berkeleyju) je nekomercijalna računarska aplikacijska platforma za mrežno računarstvo. Nastala je 10. Aprila 2002. godine na Sveučilištu Kalifornije u Berkeleyju, gdje se i dalje razvija. Prvi projekt nosio je naziv Predictor@home.

BOINC platforma omogućava oslobađanje procesorsko-računarske snage više milijuna personalnih računara spojenih preko interneta ili intraneta. To se odvija u obliku datamining projekata koji su najčešće općekorisni i pod nadzorom univerziteta i drugih institucija diljem svijeta. Trenutno su računarski najintenzivniji oni projekti koji obrađuju matematički proračun trodimenzionalnog modela Mliječne staze, potragu za vanzemaljskom inteligencijom, izradu klimatskih modela te

predviđanje meteoroloških stanja, modeliranje i simulaciju savijanja proteina, računsku obradu gravitacijskih valova te istraživanje novih lijekova protiv aktuelnih opakih bolesti.

Same ideje se dosjetilo društvo okupljeno oko Davida Andersona u Space Sciences Laboratoryju na Kalifornijskom sveučilištu u Berkeleyju. Pri razvoju BOINC-a upotrijebljeno je iskustvo proizašlo iz rada sa SETI@home projektom koji se oslanjao na distribuirano računarstvo.

U BOINC platformu i projekte koji se realizuju kroz istu uključeni su: University California Berkeley, University of Wisconsin Milwaukee, National Science Foundation, Albert Einstein Institute Hannover, Max Planck Institut für Radioastronomie i drugi.

Glavni zadatak platforme jest odvojiti naučni sadržaj od upravljačkog. Korisnici BOINC platforme instaliraju na računar jednu aplikaciju pod nazivom BOINC klijent i mogu vlastitu slobodnu procesorsku snagu dodijeliti raznim projektima. To je velika prednost u odnosu na klijente koji su vezani isključivo za jedan određeni projekt, jer jedan projekt, koji se oslanja na distribuirano računarstvo, često nema dovoljno posla kako bi opskrba korisnika raznim djelićima projekata (zadatci, eng. tasks) bila osigurana. U projektima sudjeluju uglavnom entuzijasti amateri te znanstvenici i raduju se svakom malom napretku projekta u kojem sudjeluju.

SETI@home classic projekt je bio specifičan po načinu izdavanja radnih računalnih zadataka pa ih nikada nije manjkalo. Određeni su radni zadatci bili otvoreni BOINC klijentima čak i do dvanaest puta, iako su za osiguravanje točnosti i preciznosti, u naučnim proračunima, potrebna tri neovisna računarska ciklusa. Razvojem kasnijih i novijih generacija BOINC klijenata, koji su bili u stanju istovremeno sudjelovati u više projekata, iskorištavanje procesorske računarske snage postalo je efikasnije. Od 18. studenog 2003. godine BOINC podliježe GNU GP licenci. Cilj otvaranja izvornog programskog koda jest upravo brži daljnji razvoj BOINC-a, održavanje novih operacijskih sistema te povećanje sigurnosti. Veliku ulogu u razvoju BOINC-a imaju programeri okupljeni oko slobodno-softverske zajednice.

Kako BOINC radi

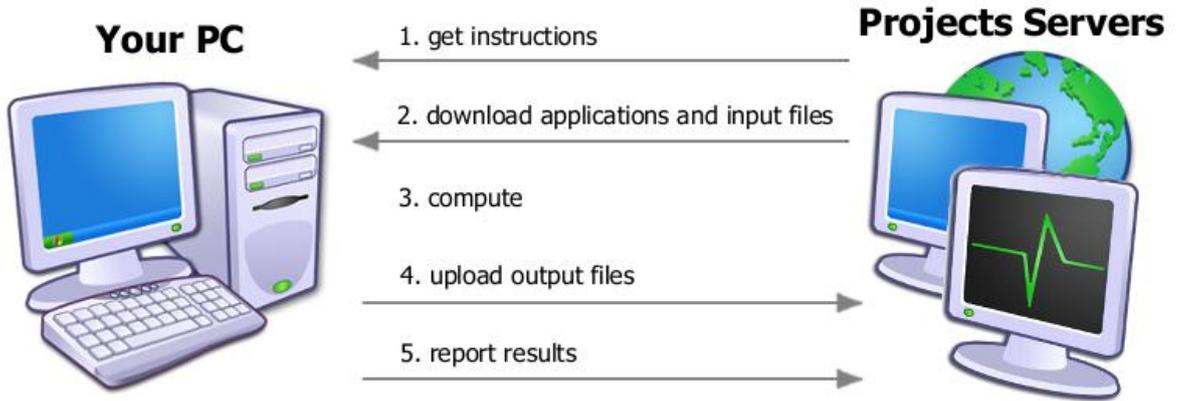
Da bi sudjelovali u BOINC-u potrebno je sa web stranice <http://boinc.berkeley.edu/> preuzeti paket instalacije i instalirati isti . Od stranekorisnika će se tražiti da odaberete projekat i unesite svoj account za koji ste predhodno izvršili registraciju na pomenutoj web adresi .

Kada pokrenete BOINC na vašem računaru, odvijaju se sljedeće radnje:

1. Korisnikov računar dobija niz instrukcija od strane servera projekta (poslužitelj podataka projekta). Količina i vrsta instrukcija koje će server dati klijentskom računaru prvenstveno će ovisi o hardware-skoj jačini računara, npr. Količina RAM memorije, jačina GPU-a, jačina CPU-a, kao i ostalih hardware-skih komponenti. Projekti mogu podržati nekoliko aplikacija, a server može poslati instrukcije iz bilo kojih aplikacija.
2. Korisnikov računar preuzimanja izvršne i ulazne datoteke sa poslužitelja podataka projekta. Ako se projektom proizvedu nove verzije aplikacija, izvršne datoteke se automatski preuzimaju na korisnikov računar.
3. Korisnikov računar pokreće programe, te na osnovu zadatih instrukcija od ulaznih datoteka proizvodi izlazne datoteke.
4. Korisnikov računar upload-a izlazne datoteke na poslužitelj podataka (Server).

- Kasnije (nakon nekog vremena, ovisno o performansama klijentskog računara) klijentski računar izvještava server o urađenom, te nakon toga dobija nove zadatke.

Ovaj ciklus se ponavlja u nedogled. BOINC to radi sve automatski, korisnik ne mora činiti ništa.

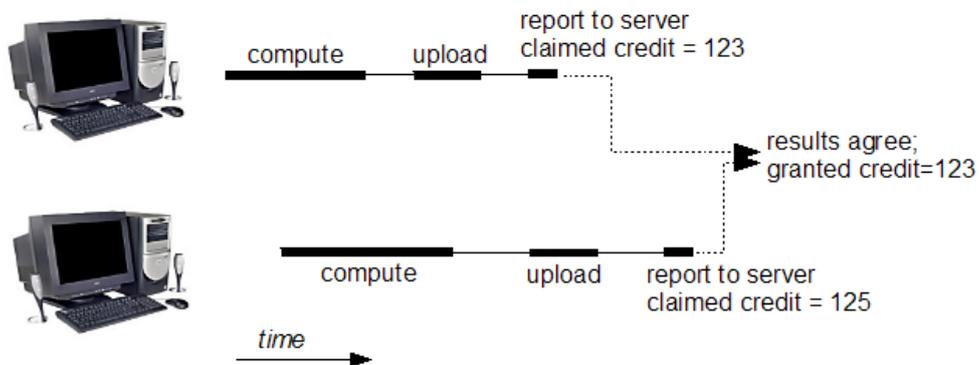


Slika 1. Opis rada BOINC-a, Klijent – Server mod.

Server vodi evidenciju o tome koliko posla je vaš računar uradio, te prikazuje rezultate o istom u vidu ostvarenog kredita. Da bi kredit bio odobren, većina BOINC projekata radi na sljedeći način:

- Svaki zadatak se mora poslati dva različita korisnička kompjutera.
- Nakon izvještavanja klijentskog računara serveru, utvrđuje se određena visina ostvarenog kredita, na temelju toga kolika je obrađena količina informacija, a ona će ovisiti o performansama korisničkog računara.
- Kada su dostavljena serveru najmanje dva rezultata od različitih klijenata, server ih uspoređuje, te ako se rezultati slažu, onda korisnici dobijaju kredit.

Tu može doći do kašnjenja od nekoliko dana, nakon izvještavanja klijentskog računara o urađenom serveru. [4]



Slika 2. Opis odobravanja ostvarenog kredita.

Projekti (Seti@home, Einstein@home, Worldcommunitygrid...)

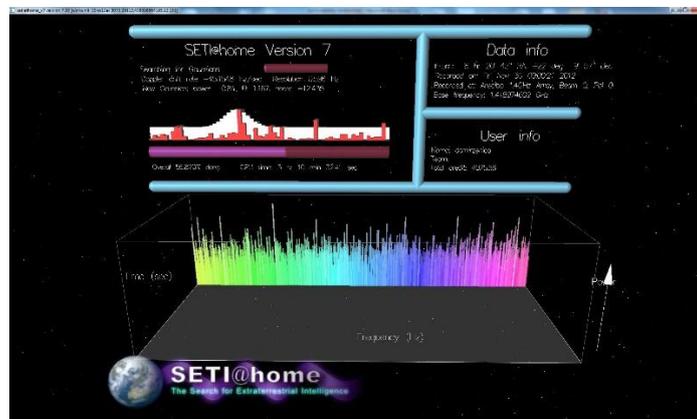
SETI @ home ("SETI kod kuće") je internet bazirani volonterski javni računarski projekat na Sveučilištu u Kaliforniji, Berkeley, u Sjedinjenim Američkim Državama. SETI je akronim za „Search for Extra-Terrestrial Intelligence“ (traženje izvanzemaljske inteligencije). Njegova je svrha analizirati radio signale, u potrazi za znakovima izvanzemaljske inteligencije, te je jedan od mnogih aktivnosti koje se poduzimaju u okviru SETI.

SETI @ Home je pušten u javnost 17. maja 1999. Uz MilkyWay@home i Einstein@home je treći veliki računarski projekat ove vrste koji je provodi istraživanje o pojavama u međuzvjezdanom prostoru kao svojoj osnovnoj namjeni.

Dva izvorna cilja SETI@home su:

1. Učiniti korisnim znanstveni rad podupirući istraživačke analize, te otkrivanje inteligentnog života izvan Zemlje,
2. Dokazati održivost i praktičnost koncepta „volonterskog računarstva“.

Drugi cilj se općenito smatra uspješnim u potpunosti. [5]



Slika 3. Seti grafički prikaz rada na projektu obrade radio signala.

Einstein@home koristi vrijeme neaktivnosti volonterskih računara u potrazi za slabim signalima astrofizičkih okretanja neutronskih zvijezda (također nazvanih pulsari) na temelju podataka iz „Ligo“ - Laser Interferometer Gravitational-Wave Observatory lasera koji detektuje gravitacijske valove (National Science Foundation - Pasadena), „Arecibo“ - radio teleskopa (National Science Foundation – Puerto Rico), i FGST - Fermi gama-zrakama satelita (U.S. Department of energy Office of Science). Einstein@home volonteri su već otkrili više od tri desetke novih neutronskih zvijezda, a praksa se i dalje nastavlja. Dugoročni cilj Einstein@home-a je da se prve izravne detekcije emisije gravitacijskih valova upotebe za prepoznavanje neutronskih zvijezda. Gravitacijske valove je predvidjeo Albert Einstein prije gotovo jednog stoljeća. [6]



Slika 4. Ligo - Laser Interferometer Gravitational-Wave Observatory.



Slika 5. FGST – Fermi gamma-ray space telescope.



Slika 6. Arecibo – Radio telescope.

World community grid - Svjetska zajednica Grid (WCG) uložila je truda kako bi stvorili najveću svjetsku javno računarsku mrežu koja sudjeluje u znanstvenoistraživačkim projektima koji su jako korisni za čovječanstvo. Pokrenuta 16. novembra 2004. godine, u koordinaciji sa IBM-ovim klijentskim softverom dostupnim na platformama za Windows , Linux , Mac OS X i Android operativnim sustavima.

Koristeći vrijeme neaktivnosti računara širom svijeta, svjetska zajednica Grid pokreće istraživačke projekte koji analiziraju aspekte ljudskog genoma, lijekove protiv HIV-a, denga, mišićne distrofije, raka, gripa, Ebole i dr. Od oktobra 2014. godine, organizaciji se pridružilo i 466 drugih tvrtki i organizacija za pomoć u svom radu, a danas ima više od 90.000 aktivnih registrovanih korisnika.

Od njegovog lansiranja najzujbudljivija otkrića World community grid-a su bila:

- U februaru 2014. godine u projektu „Pomoć u borbi protiv raka kod djece“ znanstvenici se objavili otkriće 7 spojeva koji uništavaju neuroblastomne stanice raka bez ikakvih vidljivih nuspojava.
- Iz projekta „Borba protiv malarije“ proizašlo je otkriće o nekoliko molekula koje su učinkovite protiv malarije i rezistentne tuberkuloze (uključujući TDR-TB, za koje ne postoji dostupan tretman).
- U projektu FightAIDS@ Home znanstvenici objavili da su otkrili dva spoja koji čine potpuno novu klasu lijekova za AIDS-borbu. Ovo otkriće postavlja temelj za razvoj nove klase anti-HIV lijekova kako bi se poboljšale postojeće terapije, liječenje lijekovima otpornim na bolesti, te usporavanje napredovanja opake bolesti. [7]

Tu su još i projekti: docking@home, FightMalaria@home, MindModelling@home, Radioactive@home, ClimatePrediction.net, ABC@home, Enigma@home, Asteroids@home, Cosmology@home i mnogi drugi.



Slika 7. Projekat borbe protiv HIV-a.



Slika 8. Projekat borbe raka kod djece.



Slika 9. Projekat borbe protiv Ebole.

ZAKLJUČAK

Nakon svega navedenog može se zaključiti sljedeće: Globalno gledajući, zajedničkim snagama, iskorištavajući neiskorištene hardware-ske i software-ske resurse pojedinca za koje se već troši energija i infrastruktura, te uključujući se u razne data mining volonterske projekte putem BOINC platforme, kao pojedinac možemo uveliko doprinjeti općem dobru kako ljudskoj rasi, tako i planeti zemlji. Obzirom da je veliki asortiman volonterskih data mining projekata, svako može naći sveru zanimanja i doprinjeti dobru za rješavanje nekih problema, bolesti, izračuna i sl. Pokazalo se da je ovakav način data mining-a na volonterskoj osnovi uveliko učinkovit jer su se u proteklih deset godina obradili proračuni, pronašle nove planete, otkrili novi hemijski elementi, pronađeni novi lijekovi za opake bolesti za koje se smatra da bi na institutima sa postojećim resursima superračunara trebalo nekoliko stotina godina. I na kraju, nakon istaživanja i uvida u navedeno smatram i predlažem prigodan slogan: „Rudarenjem do zdravlja i prosperiteta!“

LITERATURA

- [1] [http://hr.wikipedia.org/wiki/Podatak, informacija, znanje, mudrost](http://hr.wikipedia.org/wiki/Podatak,_informacija,_znanje,_mudrost) (17.03.2015)
- [2] [http://hr.wikipedia.org/wiki/Rudarenje podataka](http://hr.wikipedia.org/wiki/Rudarenje_podataka) (17.03.2015)
- [3] <http://hr.wikipedia.org/wiki/BOINC3> (18.03.2015)
- [4] http://boinc.berkeley.edu/wiki/How_BOINC_works (18.03.2015)
- [5] <http://en.wikipedia.org/wiki/SETI@home> (19.03.2015)
- [6] <http://www.einsteinathome.org/> (20.03.2015)
- [7] http://en.wikipedia.org/wiki/World_Community_Grid (20.03.2015)

ANTIVIRUSNA RJEŠENJA

Doc.dr Hadžib Salkić, Sandrino Vulović

Sveučilište/Univerzitet Vitez, Fakultet informacijskih tehnologija
hadzib.salkic@unvi.edu.ba, sandrino.vulovic@unvi.edu.ba

SAŽETAK

“Kompjuterski virus je kompjuterski program koji može inficirati druge kompjuterske programe modificirajući ih na taj način da to podrazumijeva stvaranje svoje vlastite kopije.”

Možemo naglasiti kako nije nužno da taj program mora učiniti nekakvu štetu (kao što je brisanje i oštećenje fajlova) kako bi ga se moglo svrstati u skupinu virusa. Postoji očita razlika između onog što Cohen smatra “virusom” i onog za što bi se većina složila da jest virus.

Da bi smo počeli obrađivati temu Antivirusnih rješenja u ovom uvodu upoznat ćemo se sa načinom na koji rade virusi. Svaki korisnički program (npr. Word ili Excel) napisan je u nekom programskom jeziku. Pisanjem programa nastaje takozvani izvorni kôd programa (eng. source code). Dakle, svaki program ima svoj izvorni kod. Kada prave virus, hakeri u stvari otvaraju izvorni kod programa i u njega ugrađuju svoj zlonamjerni kod, odnosno virus. U korisnički program, čija svrha nije da računaru pričinu štetu, hakeri praktično ugrađuju virus i time normalan korisnički program pretvaraju u nosioca računarskog virusa. Kada takav program, koji predstavlja nosioca računarskog virusa, dospe u računar dešava se sledeće: korisnik računara pokreće program, ne znajući da je on zapravo nosilac računarskog virusa. Pokretanjem programa, pokreće se i računarski virus koji je u njega ugrađen. Odmah zatim virus se učitava u radnu memoriju računara i tamo ostaje sve do isključivanja računara.

UVOD

Antivirusni softver ili antivirus (na engl. se često koristi akronim AV) je kompjuterski softver koji se koristi za prevenciju, otkrivanje i uklanjanje malware-a (zlonamjernog softvera).

Za razliku od prvobitnih antivirusnih softvera, koji su se bazirali isključivo na tretiranju kompjuterskih virusa, moderni antivirusni softveri štite od različitih malware-a, u koje osim "klasičnih" virusa spadaju i: crvi, trojanci, backdoor, rootkit, adware-i, spyware-i, dialer-i, keyloggeri... Mnogi današnji paketi nude zaštitu i od raznih vrsta socijalnog inženjeringa, poput fišinga (fishing).

Postoji više načina zaštite. Ona bazirana na potpisima uključuje otkrivanje i uklanjanje već poznatih napasti. No, problem je u tome što kompjuter može biti zaražen i nekim novim malware-om za koji još ne postoji potpis. Zbog toga antivirusi često koriste metodu heuristike. Jedna vrsta heuristike se zasniva na generičkim potpisima, koji mogu otkriti novi malware ili varijantu onog već poznatog, tako što u datoteci traže poznati maliciozni kod, ili njegove manje izmjene. Neki antivirusni softveri mogu predvidjeti djelovanje programa tako što će ga pokrenuti u sandboxu, i analizirati ga da provjere izvršava li kakve potencijalno zlonamjerne radnje. Sandbox je izolirano okruženje van kojeg program ne može prodrijeti i u slučaju da je maliciozan, ne može uraditi štetu stvarnom sistemu.

No, bez obzira koliko korisni mogu biti, antivirusi imaju i neke nedostatke. Oni utiču na korištenje sistemskih resursa, zbog čega može doći do smanjene brzine rada kompjutera (pada performansi). Neiskusni korisnici mogu također imati problema sa razumijevanjem obavijesti i odluka koje im antivirusni softver daje. Neispravna odluka, naime, može znatno oslabiti sigurnost sistema. Osim toga, ako se antivirus koristi heuristikom, te uspješnost te metode zavisi od balansa između lažno pozitivnih i lažno negativnih rezultata. Lažno pozitivni rezultati (kada je bezazlen program prepoznat kao prijetnja) mogu imati jednako loše posljedice kao i lažno negativni rezultati - npr. gubitak važnog.

HISTORIJA ANTIVIRUSA

Većina kompjuterskih virusa napisanih tokom ranih i sredinom 80-ih godina bili su ograničeni na širenje, te nisu činili značajnu štetu. No, to se počelo mijenjati kako su zlonamjerni korisnici postajali sve bolji u programiranju virusa, tako da su napravili viruse koji su mogli oštetiti ili izbrisati određenu količinu podataka na zaraženom kompjuteru.

Postoje proturječni navodi u vezi s prvim antivirusom. Vjerojatno je prvo javno dokumentirano uklanjanje virusa "u divljini" izvršio stručnjak za kompjutersku sigurnost Bernd Fix, 1987. godine. Poznato je i da su za platformu Atari, te iste godine, bila razvijena dva antivirusna softvera. Prvi je bio G Data (postoji i danas), a drugi UVK 2000.

Fred Cohen je 1984. godine izdao jedan od prvih akademskih papira o kompjuterskim virusima. 1987. godine ispravno je izjavio, da nijedan algoritam ne može otkriti sve moguće viruse, a 1988. godine počeo je razvijati strateške metode za antivirusne, koje su uskoro prihvatili i ugradili njihovih kasniji proizvođači.

Na mreži BITNET/EARN 1988. je godine nastala mail lista VIRUS-L na kojoj je se raspravljalo o novim virusima, te o mogućnostima njihove detekcije i uklanjanja. Neki su članovi spomenute liste, kao što su John McAfee i Eugene Kaspersky, kasnije osnovali antivirusne tvrtke koje su razvijale i prodavale komercijalne pakete. Prije velike dostupnosti interneta, virusi su se obično širili preko disketa. Antivirusni softver je u to vrijeme provjeravao izvršne datoteke i boot sektore na disketama i tvrdim diskovima, te je bio relativno rijetko osvježavan. Nakon što je internet postao raširen, i virusi su promijenili svoje glavno mjesto širenja, koje je se preselilo u spomenuto okruženje.

Tokom godina postalo je neophodno da antivirusni softver provjerava više tipova datoteka, a ne samo izvršne, zbog sljedećih potencijalnih prijetnji:

Moćni makroi, koji su bili korišteni u programima za obradu teksta, poput MS Worda. Pisci virusa su, naime, mogli koristiti makroe za stvaranje virusa koji bi bili ugrađeni u dokumente. Mogućnost ubacivanja izvršnih objekata u kod inače neizvršnih datoteka. Kasniji e-mail programi poput Microsoftovih Outlook Expressa i Outlooka, bili su ranjivi na viruse koji su bili ubačeni u samo tijelo poruke

METODE DETEKCIJE

Postoji više metoda otkrivanja malicioznog softvera, a većina antivirusa koristi kombinaciju više njih:

1. Detekcija bazirana na potpisima.
2. Detekcija štetnih aktivnosti,

3. Heuristička metoda,
4. Detekcija rootkita
5. Zaštita u realnom vremenu

DETEKCIJA BAZIRANA NA POTPISIMA

Otkrivanje malwarea dugo je vremena veoma ovisilo od ove metode detekcije. Ona može biti veoma učinkovita, ali ne može odbraniti kompjuter od malwarea ako ne postoje odgovarajući potpisi - pa nije pouzdana protiv novog, nepoznatog malicioznog softvera.

Kako novi virusi nastaju doslovno svaki dan, detekcija bazirana na potpisima zahtijeva česta osvježavanja rječnika potpisa. Neki antivirusi omogućavaju korisnicima slanje novih virusa ili njihovih varijanata antivirusnim tvrtkama, gdje se analiziraju i potom se u rječnik doda njihov potpis.

Još jedna potencijalna mana ove metode jest da neki autori virusa pokušavaju izbjeći sličnost sa postojećim potpisima te pribjegavaju morfičnim (oligomorfičnim, polimorfičnim i odnedavno metamorfičnim) virusima. Ta vrsta malicioznog softvera šifrira (enkriptira) dijelove svog koda, ili na druge načine izmjenjuje samog sebe, u svrhu prikrivanja, tj. da njegov potpis ne odgovara nekom u rječniku.

DETEKCIJA ŠTETNIH AKTIVNOSTI

Antivirusni softver nadgleda softver u okruženju sa kojim kompjuterski sistem komunicira. Ukoliko detektira sumnjive aktivnosti nekog softvera, dodatno ga detaljno provjerava koristeći neku od metoda detekcije. Ova metoda je pogodna za detekciju novih i nepoznatih virusa.

HEURISTIKA

Dosta antivirusa koristi metodu heuristike za identifikaciju nepoznatog malwarea ili novih varijanti postojećeg.

Mnogi virusi, naime, počnu na razini pojedinačnih infekcija. Preko kasnijih mutacija, tj. "poboljšavanja" njihovih svojstava (od strane samog autora ili nekih drugih napadača), on može imati više međusobno sličnih varijanti. Generička detekcija je detekcija i uklanjanje više malicioznih prijetnji korištenjem jednog odgovarajućeg potpisa.

Tako primjerice trojanac Vundo ima nekoliko porodica, ovisno o klasifikaciji proizvođača antivirusa; Symantec klasificira "članove" Vundo porodice u dvije kategorije: Trojan.Vundo i Trojan.Vundo. B.

Iako identificiranje specifičnog virusa ima svoje prednosti, brži je način stvaranje generičkog potpisa za porodicu. Istraživači virusa pokušavaju kod porodica naći jedinstvene zajedničke karakteristike, tako da za njih mogu stvoriti jedan generički potpis.

DETEKCIJA ROOTKITA

Antivirusni softver može pokušati skenirati kompjuter u potrazi za rootkitom. Riječ je o posebnoj vrsti malwarea dizajniranoj da si pridobije administratorske privilegije preko kompjuterskog sistema - a da pri tom, naravno, prođe nezapaženo što je duže moguće. Rootkit može promijeniti način funkcioniranja operativnog sistema, a

ponekad se i "uplesti" u rad antivirusnog softvera čineći ga nepouzdanim. Teško ga je ukloniti, a ponekad je jedino rješenje reinstalacija operativnog sistema.

Međutim, i na ovom polju ima nade obzirom da antivirusni program Avast ima licenciran GMER (program za detekciju rootkita) što znatno olakšava borbu protiv ove vrste malicioznog programa.

ZAŠTITA U STVARNOM VREMENU

Zaštita u stvarnom vremenu poznata je pod nazivima real-time protection, on-access scanning, background guard, resident shield i autoprotect. To je zaštita kakvu posjeduju skoro svi antivirusi, antispyware-i (često ne u besplatnoj verziji) i drugi programi za zaštitu kompjutera. Ona bilježi aktivnosti na sistemu i promatra događaju li se kakve sumnjive aktivnosti, i to u stvarnom vremenu. To je drugim riječima razdoblje kada su podaci učitani u memoriju kompjutera: kad korisnik stavlja CD, otvara e-mail poruku, ili surfa internetom; ili pak razdoblje kad je datoteka na kompjuteru već učitana ili izvršena

LAŽNO POZITIVNI REZULTATI

Lažno pozitivni rezultat označava dešavanje kada antivirus pogrešno detektira bezopasnu datoteku kao virus. Kada se ovo dogodi, mogu se javiti ozbiljni problemi. U slučaju da je antivirus konfiguriran da automatski briše zaražene datoteke ili da ih izolira u karantenu, lažno pozitivni rezultat kod neke važne datoteke može učiniti operativni sistem ili namjenski program nesposobnim za rad. U slučaju da Windowsi postanu nesposobni za rad, troškovi njihovog ponovnog popravljanja u servisima može prisiliti tvrtke u kojima se koriste na privremeno zatvaranje.

Navesti ćemo nekoliko slučajeva lažno pozitivnih rezultata:

U maju 2007. godine, loše napravljen Symantecov virusni potpis greškom je uklonio nekoliko esencijalnih sistemskih datoteka, zbog čega je tisuće kompjutera prestalo funkcionirati. Također u istom mjesecu iste godine, Norton AntiVirus (tvrtke Symantec) detektirao je izvršnu datoteku bitnu za rad Pegasus Maila kao trojanca, te ju automatski obrisao. To je, razumljivo, uzrokovalo nemogućnost pokretanja spomenutog mail klijenta. Da stvari budu još gore, Norton AntiVirus pogrešno je prepoznao čak tri izdanja Pegasus Maila kao malware, te bi obrisao njihovu pripadajuću instalacijsku datoteku. U tvrtki Pegasus Mail odgovorili su:

“Na osnovu činjenice da je Norton/Symantec detektirao svaki od tri posljednja izdanja Pegasus Maila kao malware, možemo samo osuditi pomenuti proizvod kao odviše loš za korištenje, i toplo preporučiti našim korisnicima da ga prestanu koristiti u korist alternativnog antivirusnog paketa sa manje bugova.”

U aprilu 2010. godine, McAfee je detektirao svchost.exe, bezazlenu Windows izvršnu datoteku, kao virus. To je se dogodilo na kompjuterima koji su pokretali Windows XP Service Pack 3, zbog čega bi korisnici izgubili vezu na internet ili bi se pak njihov kompjuter non-stop iznova pokretao.

U decembru iste godine, loše osvježanje AVG paketa oštetilo je 64-bitne verzije Windowsa 7 - zbog čega su se neprestano iznova pokretali te time postali onesposobljeni.

U oktobru 2011. Microsoft Security Essentials (MSE) je uklonio Google Chrome preglednik, konkurentan Microsoftovom Internet Exploreru, označivši ga kao boot trojanca.

SISTEMSKI PROBLEMI

Pokretanje više antivirusa istovremeno može ugroziti sistemske performanse i, još važnije, uzrokovati sukobe između antivirusa. Zbog toga će mnogi antivirusi odbiti da se instaliraju ako otkriju da na sistemu djeluje i neki drugi. Ipak, pomoću koncepta koji se naziva multiscanning nekoliko je firmi (uključujući G Data te Microsoft) uspjelo napraviti aplikacije koje istovremeno pokreću više engine-a.

Ponekad je neophodno privremeno isključiti antivirus, npr. tokom instalacije servisnih paketa za Windowse (što je i preporuka Microsofta) i osvježavanja drivera za grafičku karticu - iz razloga što antivirus može djelomično ili posve spriječiti ovakve znatne sistemske izmjene.

Na funkcionalnost nekoliko legitimnih aplikacija također mogu utjecati antivirusni programi. TrueCrypt, program otvorenog koda namijenjen enkripciji diskova, može se sukobiti s antivirusom, što dovodi ili do nemogućnosti funkcioniranja ili velike sporosti programa. I igre na Steam platformi mogu imati problema sa antivirusnim softverom, zbog čega će biti nestabilne ili spore.

POUZDANOST

Istraživanja provedena u decembru 2007. godine pokazala su da se pouzdanost antivirusnog softvera smanjila u odnosu na prethodnu godinu, posebno protiv nepoznatih prijetnji. Njemački kompjuterski magazin c't otkrio je da se njihova razina detekcije smanjila sa 40-50% (2006.) na 20-30% (2007.). Iznimka je bio NOD32, koji je u to vrijeme uspio ostvariti razinu od 68 posto.

Problem je dodatno uvećan zbog činjenice da je, za razliku od nekad, danas česta praksa da pisce malicioznog softvera financiraju kriminalne organizacije. Nije rijetkost da kriminalne organizacije bez dovoljno tehničkog znanja za pisanje malwarea čak kupuju maliciozne pakete od programera, kojima cijene variraju obično ovisno od kompleksnosti i broja opcija, a kreću se od tristotinjak pa sve do preko hiljadu eura. Pakete je moguće zasebno podesiti da se izbace ili uvedu neke druge opcije, po želji kriminalaca, a onda ukupna cijena ovisi o komponentama koje su izabrane.

Nezavisna testiranja antivirusa u februaru 2010. pokazala su da najbolja razina detekcije iznosi 99,6, a najmanja samo 81,8%. Svi antivirusi na testiranju imali su određen broj lažno pozitivnih rezultata, neki više, neki manje. Iako se metodologije razlikuju, neke istaknute nezavisne kompanije za testiranje uključuju AV-Comparatives, ICSA Labs, West Coast Labs, Virus Bulletin, AV-TEST i ostale članice Anti-Malware Testing Standards Organization-a. Valja spomenuti da je testiranje antivirusnih programa vrlo složeno te da varira o mnogim faktorima.

NOVI VIRUSI

Antivirusni programi mogu biti nepouzdana protiv novih virusa, čak i kada koriste metode detekcije koje se ne baziraju na potpisima. Razlog za ovo je što pisci virusa testiraju svoja "djela" na najpoznatijim antivirusima kako bi bili sigurni da nisu prepoznati, prije nego što su pušteni "u divljinu".

Određeni maliciozni softver, nadasve ransomware (koji zaključava pristup sistemu te prikazuje lažnu poruku korisniku da uplati određen iznos novca za njegovo otključavanje), koristi polimorfični kod kako bi onemogućila i izbjegla detekciju antivirusa. Sigurnosni analitičar Jerome Segura ovako je objasnio ovu pojavu:

“ To je nešto što im promakne mnogo puta zato što ovaj tip virusa, ransomware, dolazi sa internetskih stranica koje koriste polimorfizam, što znači da te stranice praktični randomiziraju datoteku koju vam pošalju, a koja vrlo jednostavno bude propuštena pokraj poznatih antivirusnih proizvoda. Imao sam prilike vidjeti ljude sa zaraženim sistemima, sa puno skočnih prozora, a opet oni imaju instaliran antivirusni softver koji ništa ne detektira. Zapravo može biti dosta teško riješiti se toga, a i tada niste sigurni je li zaista nestalo. Kada vidimo nešto ovako, obično savjetujemo reinstalaciju operativnog sistema ili sigurnosne kopije podataka.”

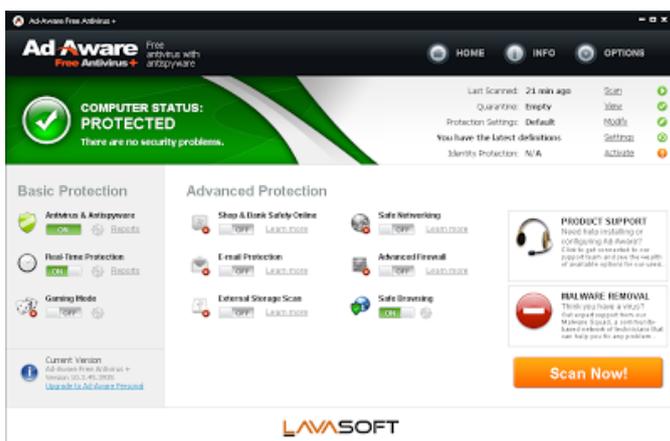
ROOTKIT

Detekcija rootkita predstavlja veliki izazov za antivirusne - s obzirom na to da rootkiti imaju potpuni administratorski pristup kompjuteru, te su nevidljivi korisniku na popisu procesa u Task Manageru; također mogu izmijeniti unutrašnje funkcije sistema kao i antivirusa.

BESPLATNI ANTIVIRUSNI PROGRAMI

Ad-Aware Free Antivirus +

Instalacija je jednostavna ali zavisi od Internet konekcije jer se instalacijske datoteke preuzimaju sa Interneta. Nakon uspješne instalacije potrebno je ponovo pokrenuti računar kako bi program ispravno radio. Nakon toga pojavit će se prozor u kojem trebate izvršiti besplatnu registraciju.



Programski interfejs je veoma praktičan. Na prvi pogled i ne nudi baš mnogo opcija, ali klikom na svaku osnovnu mogućnost prikazuju se detaljnije opcije.

Zaštite koje program nudi su antivirusna zaštita, zaštita od špijunskih programa te nadgledanje poveznica i web adresa s ciljem sigurnog

pretraživanja. Dodatna opcija je *Gaming Mode* koja onemogućava iskakanja bilo kakvih obavijesti od strane Ad-Aware programa.

Minus: Tokom instalacije program mijenja zadanu web pretraživač u *Blecko* te početnu web adresu u *Ad-Aware Safe Search*. Također se instalira i *Ad-Aware Safe Browser* dodatak za Internet Explorer i Firefox koji služi za sigurno surfanje Internetom. Sve ovo moguće je onemogućiti tokom instalacije.

Ocjena: Ad-Aware Free Antivirus+ je solidan antivirusni program sa osnovnom zaštitom od virusa i špijunskih programa.

Avast! Free Antivirus

Instalacija programa relativno je jednostavna i brza, u svega nekoliko klikova. Prije završetka instalacije Avast! će brzo skenirati računar. Nakon uspješne instalacije korisnik nema nikakve potrebe za dodatnim podešavanjima već je najbolje da sve ostane onako kako jeste, kao što to proizvođač i preporučuje.



Interfejs je veoma jednostavan i podijeljen je u kartice koje se nalaze na lijevoj strani programa. Zavisno od kartica u njima se nalaze detaljne informacije o trenutnom statusu zaštite, verziji programa i virusnih definicija, načinima skeniranja računara i privremenih medija uključenih u računar, spremnik za sumnjive i zaražene datoteke, sve vrste podrške - od čestih pitanja, foruma, tehničke podrške, uputstava, korištenja

udaljene pomoći te pomoći o programu. Zaštite koje Avast! Free Antivirus nudi su: *Zaštita datoteka*, *Mail zaštita*, *Web zaštita*, *P2P zaštita*, *IM zaštita*, *Mrežna zaštita*, *Zaštita skripti* te *Zaštita ponašanja*.

Dodatne opcije su *AutoSandbox* - opcija za pokretanje sumnjivih programa u izoliranom okruženju, zaštita web pretraživač, opcija za slanje ili primanje udaljene pomoći te opcija za blokiranje web stranica.

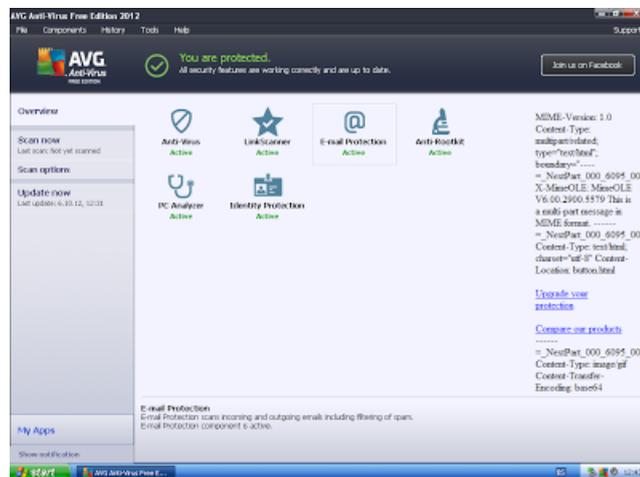
Minus: Tokom instalacije instalirat će se *Google Chrome* te će se postaviti kao zadani web preglednik. Ovo je moguće promijeniti na samom početku instalacije.

Ocjena: Avast! Free Antivirus jedan je od najboljih besplatnih antivirusnih programa sa sistemom zaštite i brojem detekcija kakve se mogu postići i neke komercijalne verzije. Jednostavnog je interfejsa, ne troši mnogo sistemskih resursa, posjeduje mnogo opcija i dodataka, kako za početnike tako i za napredne korisnike.

AVG Anti-Virus Free

Instalacija programa je jednostavna ali ne baš tako brza. Nakon odabira jezika i prihvatanja pravila ugovora, nastavit će se sa instalacijom programa. Po uspješnom završetku instalacije dočekat će nas vrlo jednostavan interfejs.

Zaštite koje AVG nudi su: *Anti-Virus*; *Link skener* - zaštita od prijetnji sa Interneta, također prati i mrežni saobraćaj; *E-mail zaštita*; *Anti-Rootkit* - pronalazi



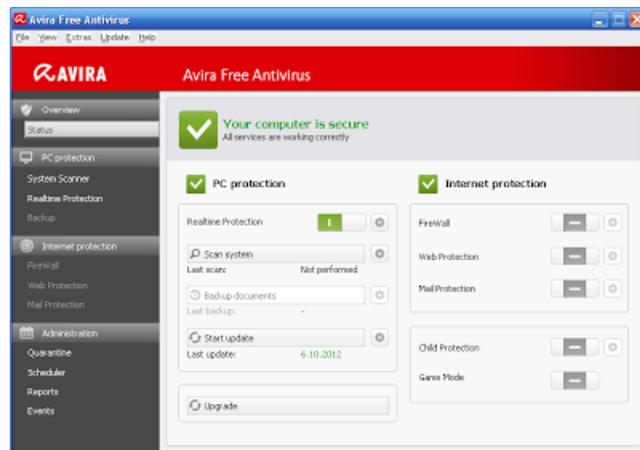
rootkit programe skrivene u operativnom sistemu; *PC Analyzer* - analizira računar i pronalazi greške u registarskoj bazi, neželjene datoteke, oštećene prečace te provjerava fragmentaciju; te *Zaštita identiteta* - zaštita od krađe identiteta i ugrožavanja privatnosti.

Minus: Tokom instalacije program mijenja zadanu web pretraživač u *AVG Secure Search* te instalira *AVG Security Toolbar*. Ovu opciju moguće je promijeniti tokom instalacije. Također se na kraju instalacije korisniku nameće mogućnost sudjelovanja u procesu poboljšanja proizvoda, iako ovaj korak nije presudan za uspješnu instalaciju programa.

Ocjena: AVG Anti-Virus Free jedan je od najboljih besplatnih antivirusnih programa. Jednostavnog je interfejsa iza kojeg se krije mnogo opcija koje će znati iskoristiti napredniji korisnici.

Avira Free Antivirus

Postoje dva načina instalacije, preporučeni i napredni način. Ako odaberete preporučeni način onda će instalacija proći veoma jednostavno i brzo. Ako ipak odaberete napredni način onda ćete po završetku instalacije morati proći nekoliko koraka na podešavanju programa. Međutim, ako u oba slučaja tokom instalacije odaberete da ne želite instalirati *Avira SearchFree Toolbar* i *Avira SearchFree Updater* onda nećete imati web zaštitu.



Interfejs je krajnje jednostavan i jedina zaštita koja se nudi je ona od virusa. Međutim, ni ova zaštita neće ispravno raditi ukoliko nemate pristup Internetu kako bi se preuzela ažuriranja.

Minus: Tokom instalacije program mijenja zadanu web tražilicu i početnu web adresu u *Avira SearchFree*. Također za aktivnu web zaštitu potrebno je instalirati *Avira SearchFree Toolbar* i *Avira SearchFree Updater*. Sve ovo moguće je onemogućiti tokom instalacije. Dalje, za aktivnu zaštitu računara potrebno je ažurirati program što je malo problematično za računare koji nemaju vezu sa Internetom.

Ocjena: Avira Free Antivirus je prosječan antivirusni program budući da nudi solidnu zaštitu od virusa, ali ne i zaštitu od prijetnji sa Interneta, niti ima bilo kakvu dodatnu mogućnost.

Comodo Internet Security

Instalacija programa je jednostavna ali traje nešto duže. Po zadanim postavkama instalirat će se osnovna zaštita, firewall i program za udaljeno upravljanje (*GeekBuddy*). Nakon uspješne instalacije potrebno je ponovo pokrenuti računar kako bi program ispravno radio.

Interfejs je jednostavan i podijeljen je u kartice koje se nalaze u gornjem dijelu



programa. Zavisno od odabrane kartice u njima se nalaze osnovne informacije o trenutnom statusu zaštite, detaljne informacije i mogućnosti za antivirusni program, firewall i sigurnost računara (Defense+), te sve ostale dodatne mogućnosti.

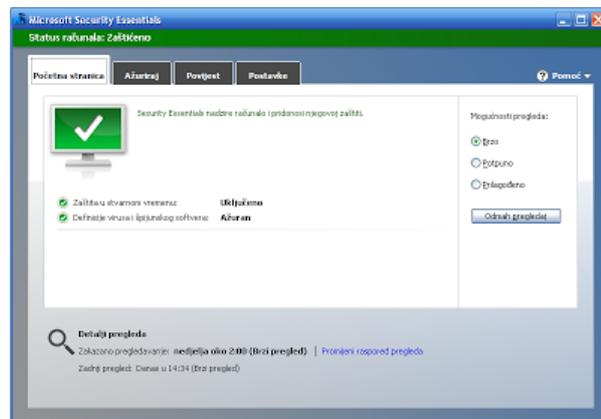
Pored osnovne antivirusne zaštite, Comodo Internet Security nudi i firewall. Također tu je i Sandbox - mogućnost pokretanja sumnjivih

programa u izoliranom okruženju, zatim dijagnostika računara u svrhu pronalaženja registarskih grešaka i nekompatibilnih programa.

Ocjena: Comodo Internet Security jednostavnog je interfejsa sa mnogo opcija koje će dobro doći naprednijim korisnicima. Pored osnovne zaštite tu je i firewall te dodatni alati za sigurnost računara. Međutim, kompanija Comodo malo je paranoična pa njihova antivirusna rješenja u odnosu na konkurenciju imaju najviše *false positive* tj. pogrešno prepoznatih datoteka kao potencijalne prijetnje.

Microsoft Security Essentials

Instalacija programa je jednostavna i brza, a jedini uslov za uspješnu instalaciju je da imate licenciran Windows operativni sistem. Po završetku instalacije program će se pokušati povezati sa Internetom kako bi preuzeo ažuriranja koja su potrebna za ispravan rad programa. Interfejs je krajnje jednostavan i podijeljen je u kartice u kojima se nalaze osnovne informacije, informacije o ažuriranjima, povijest dešavanja te postavke.



Zaštita koju Microsoft Security Essentials nudi je osnovna zaštita od virusa, trojanca i zlonamjernih programa.

Minus: Nakon instalacije potrebna je veza sa Internetom kako bi se program ažurirao da bi mogao štiti računar.

Ocjena: Microsoft Security Essentials nudi solidnu zaštitu od virusa i špijunskih programa. Ne bih ga preporučivao korisnicima, a oni koji ga imaju neka ga zamijene za neko bolje antivirusno rješenje.

ZoneAlarm Free Antivirus

Instalacione datoteke se preuzimaju sa Interneta pa instalacija najviše zavisi od brzine Internet konekcije. Nakon uspješne instalacije potrebno je ponovo pokrenuti računar kako bi program ispravno radio. Interfejs je jednostavan i veoma praktičan. Na početnom ekranu nalaze se tri velika dugmeta za antivirusnu komponentu,



firewall te zaštitu identiteta i podataka. Klikom na svako dugme dolazimo do detaljnijeg uvida u trenutnu zaštitu te opcija koje se tamo nalaze.

Zaštite koje program nudi je antivirusna zaštita, firewall te zaštita identiteta i podataka. Dodatna mogućnost je *Game Mode* odnosno sprječavanje prikazivanja poruka.

Postoje dva načina rada *Game Mode* i to blokiranjem svih akcija koje zahtijevaju korisnikovu interakciju, ili odobravanjem svih akcija. Nijedan način nije dobar jer prilikom blokiranja svih akcija mogu se blokirati one legitimne, a odobravanjem svih akcija može se dopustiti izvršavanje onih zlonamjernih.

Minus: Program mijenja zadanu web pretraživač i početnu web adresu u *Zone Alarm* te instalira *Zone Alarm* alatnu traku. Sve ovo je moguće onemogućiti tokom instalacije.

Ocjena: ZoneAlarm Free Antivirus je solidan antivirusnih programa. Jedna od boljih mogućnosti ovog programa je besplatan vatrozid.

Pored dobrog antivirusnog programa za bolju zaštitu računara potrebno je da imate i dobar firewall te program za pronalaženje zlonamjernih programa (*malware*).

Malwarebytes Anti-Malware

Instalacija programa veoma je jednostavna i brza. Nakon uspješne instalacije program će pokušati preuzeti ažuriranja sa Interneta.

Interfejs je jednostavan i podijeljen u kartice u kojima se nalaze detaljne informacije o dostupnim provjerama, zaštiti (probni period na 30 dana), nadogradnjama, karanteni, izvještajima, zanemarenim postavkama te podešavanjima.

Malwarebytes Anti-Malware jedan je od najboljih programa za pronalaženje, uništavanje i blokiranje zlonamjernih programa koje mnogi drugi antivirusni programi nisu u stanju pronaći.

Ocjena: Malwarebytes Anti-Malware je program kojeg morate imati.



ZAKLJUČAK

Iz ovog seminarskog rada možemo zaključiti da je u današnje vrijeme je gotovo nezamisliv rad na kompjuteru bez zaštite od virusa koje možemo dobiti otvaranjem bilo koje stranice na internetu. Potrebno je imati dobre antivirusne programe kako se ne bi doveli u situaciju da pokupimo raznorazne viruse koji bi obrisali važne datoteke ili nam srušili sistem. Danas se sva poslovanja vode preko kompjutera i nedopustiv je

rizik da se dovedemo u situaciju prekida poslovanja na određeno vrijeme. To nam ne dopušta današnji način života. Potrebno je redovito obnavljati antivirusne programe jer svakog dana nastaju milijuni novih virusa.

Na nama samima je da odlučimo da li ćemo uložiti određenu sumu novca za kupovinu antivirusnih rješenja ili ćemo koristiti besplatna koja su dostupna na internetu putem besplatnog preuzimanja ali koja nemaju sve module zaštite.

LITERATURA

1. <http://sh.wikipedia.org/wiki/Antivirus>
2. <http://pc-savjeti.blogspot.com/2012/10/9-besplatnih-antivirusnih-programa.html>
3. <http://www.netlab.ba/index.php/style-2/2012-06-23-10-46-59/2012-06-24-22-21-55>

ZAŠTITA DJECE NA INTERNETU
SIGURNOSNI ASPEKAT
Inspektor Suzana Zec
MUP SBK/KSB TRAVNIK

SAŽETAK

Ne želeći umanjiti sve prednosti, mogućnosti i neophodnost korištenja interneta, kao i njegovu važnost za intelektualni razvoj, kako djece tako i cjelokupnog društva, zbog negativnih iskustava od izuzetne važnosti je ukazati i na negativne strane korištenja interneta, osobito za djecu, odnosno mladu populaciju.

Internet je odličan izvor informacija i zabave kako za djecu tako i za odrasle. Želimo li uživati u internetu i svim sadržajima koje pruža, potrebno je da nučimo našu djecu odgovornom i pametnom korištenju interneta.

U cilju smanjenja mogućnosti pojave negativnih iskustava na internetu za djecu i roditelje naš cilj je da upoznamo roditelja o potrebi kontrole onog sta njihova djeca rade na internetu, koje stranice otvaraju, sa kim se dopisuju i sl.

Također, bitno je naglasiti da su za sigurnost djece pored policije i nastavnog osoblja, upravo roditelji ti čija je uloga u zaštiti djece primarna i nezamjenjiva, odnosno samo kao tim (roditelji, školstvo i policija) možemo smanjiti mogućnost da naša djeca postanu žrtve bilo kakvog oblika nasilja na internetu.

**NEKI OD NAJČEŠĆIH OBLIKA ZLOSTAVLJANJA NA INTERNETU-
LOŠE STRANE INERNETA:**

- Hakovanje

Hakovanje je oblik uznemiravanja mladih na internetu. Hakeri koriste svoje napredno kompjutersko znanje i vještine da bi neovlašteno ušli u tuđe kompjuterske sisteme i time napravili štetu, ali ponekad i dobit za sebe.

Jedan od načina odbrane od hakera je praviti dobre šifre, kje se ne mogu lako otkriti. Preporučuje se kombinacija slova i brojeva, upotreba malih i velikih slova. Važno je šifru čuvati samo za sebe i ne dijeliti je ni sa prijateljima.

- Vršnjačko nasilje- „Sajber buling- oblik vršnjačkog nasilja u virtualnom svijetu“

Jedan od vrlo prisutnih načina zlostavljanja djece na internetu jeste upravo vršnjačko nasilje. Za razliku os nasilja koje se dešava u školi ili na ulici, vršnjačko nasilje na internetu traje 24 sata svih sedam dana u nedjelji, dakle djeca doživljavaju neprijatnosti u svojoj kući, dok roditelji misle da su njihova djeca na sigurnom mjestu. Ono se osobito odnosi na korištenje društvenih mreža (Facebook, Twitter, Skype Viber, Messenger...), koje djeca koriste da bi se međusobno vrijeđali, ponižavali i sl. To kod određenog broja djece može da izazove niz negativnih pojava, kao što je pretjerana izolovanost, depresija, strah, sram, razvijanje pogrešne slike o spolnosti, oblikovanje pogrešnih stavova, poticanje na nasilje i u najgorem slučaju djeca se zbog takvih vrijeđanja mogu

odlučiti na suicid. Zbog toga je neophodno da roditelji imaju otvoren odnos sa djecom, zasnovan na redovnoj komunikaciji i povjerenju.

- **Trgovina djecom i mladima**

Na internetu postoji mogućnost nezakonite trgovine djecom i mladima. Svrha trgovine je ilegalno iskorištavanje mladih u različite svrhe: radno iskorištavanje, trgovina organima, seksualno iskorištavanje i sl. Postoje Zakoni kojima je regulisano navedeno pitanje, pa je neophodno da se roditelji o tome informišu, kako njihova djeca ne bi postala žrtva ove trgovine. Ukoliko na internetu slučajno nađete na sadržaje koji izazivaju sumnju u tom smislu, odmah i obavezno pozvati policiju ili neku drugu instituciju u koju imate povjerenja. To se može uraditi i anonimno.

- **Seksualno zlostavljanje**

Seksualna zlostavljanja i pornografija su nažalost česti oblici nasilja na koje mlada osoba može naići na internetu. Seksualna zlostavljanja podrazumjeva: seksualno uznemiravanje riječima, primoravanje na kontakte i seksualne aktivnosti, kao i izrada pornografskih sadržaja sa žrtvom. Ako primjetite da neko pokušava da uznemirava i ili na neki način ugrozi Vaše dijete na ovaj način, ili Vam se dijete samo povjeri, treba da znate da problem nije u Vama niti u Vašem djetetu, jer niko nema pravo da nekoga seksualno uznemirava. Sa djecom treba da razgovarate otvoreno o ovom problemu i uvijek imajte na umu da problem može da se riješi. U tom slučaju obavezno događaj, bez ustručavanja prijaviti policiji.

- **Krađa identiteta i prevare prilikom kupovine putem interneta**

Također su jako česte negativne pojave na internetu. Potrebno je da ste upoznati sa tim kolika je opasnost davanja ličnih podataka na internetu, odnosno da na taj način ugrožavate ličnu privatnost i sigurnost. Dakle moramo biti oprezni na internetu i ne vjerovati svakoj reklami, osobi i sl. U svakom slučaju nije dobro ići na stranice na kojima se dolazi u kontakt sa nepoznatim osobama i nikad ne ostavljati svoje lične podatke.

- **Stranice koje promovišu loše navike u ishrani (anoreksija)...**

Web stranice koje promovišu nepravilne navike u ishrani, kao što su bulimija i anoreksija, mogu biti oblici uznemiravanja mladih na internetu. Takvi sadržaji mogu motivirati mlade ljude na identifikaciju sa zdravstveno neispravnim modelima i podsticati mladu osobu da se nepravilno hrani i samopovređuje na taj način. Ako primjetite da Vaše dijete privlače takvi sadržaji, bilo bi dobro da o tome razgovarate sa nekim stručnim licem.

ŠTA MI KAO RODITELJI MOŽEMO URADITI DA SPRIJEČIMO, ODNOSNO SMANJIMO MOGUĆNOST NASTAJANJA BILO KOJEG OD NAVEDENIH OBLIKA NASILJA

- **Otvoreno razgovarati sa djecom- s ciljem stjecanja njihovog povjerenja, iako tinejdžeri traže privatnost to ne znači da nemate pravo znati sa kom se dijete druži, kako u stvarnom životu, tako i u virtualnom.**
- **Stalno pratiti kakve fotografije objavljuju na internetu, s kim se dopisuju i sl., dakle ukoliko imaju FB profil, potrebno je da budete njihovi prijatelji na Facebook-u.**

- Ukazati na opasnost postavljanja ličnih podataka na internet (tačnu adresu, naziv škole koju pohađaju i sl., ne najavljivati odlazak na godišnji odmor na FB..).
- Ne kriviti djecu ako postanu žrtvom nasilja na internetu, odnosno objasniti im da oni nisu krivi za to što se desilo.
- Svi aparati koji imaju pristup internetu trebali bi biti na mjestu koje roditelj može stalno nadgledati bar do 12 godine djeteta, dakle dijete do 12 godine ne bi trebalo bez roditeljskog nadzora surfati internetom.
- Educirajte se, jer djeca danas odrastaju sa računarima. Razumljivo je da u Vašoj mladosti nije bilo računara, stoga je neophodno da se educirate o opasnostima koje vrebaju kako bi Vaše dijete bez opasnosti moglo iskusiti sve dobrobiti interneta.
- Prilikom prodaje ličnih računara, laptopa, tableta, smartfona iz koji se teško brišu Vaši nekada uneseni podaci ili fotografije- savjetujemo da navedene aparate odnesete stručnim licima kako bi iste vratili na fabričke postavke, čime će se izbjeći mogućnost ponovnog vraćanja Vaših već „izbrisanih“ podataka, i tek nakon toga vršiti prodaju ili poklanjanje aparata.

ŠTA AKO SE DESI DA DIJETE IPAK POSTANE ŽRTVA BILO KOG OBLIKA NASILJA NA INTERNETU

- Kontaktirajte policiju. Kada se stvari otmu kontroli, primjerice saznate da je dijete nekome slalo svoje nage fotografije, ne ustručavajte se obratite se policiji, posao policije je da Vam pomogne.
- Ne brišite poruke poslone od strane nasilnika iste fotografišite svojim telefonom ili drugim aparatima, jer će iste u daljnjem postupku, koji poduzima policija, predstavljati materijalni dokaz na sudu.
- Ne odgovarati na nasilne poruke.

Ne gurajte glavu u pijesak i djelujte proaktivno. Nemojte misliti da se to Vama ne može desiti. Pedofili i nasilnici ne biraju žrtve. Minimalna edukacija Vas i Vašeg djeteta odagnat će većinu opasnosti.

ANDROID APLIKACIJE ZA ZAŠTITU DJECE
Dinka Šakić, BA, Denis Lovrinović, BA
Sveučilište / Univerzitet „Vitez“ Vitez
dinka.sakic@unvi.edu.ba, denis.lovrinovic@unvi.edu.ba

SAŽETAK

Informacione tehnologije postale su neizostavni dio života. Svaki napredak u razvoju istih je od velikog značaja kako za pojedinca koji je pridonio tom napretku, tako i onima koji će se koristiti tim. Također, neizostavan dio svakodnevnog upotrebe su i smartphone (pametni telefoni) ili tablete kao jedan od načina komunikacije. Nerijetko je da djeca gledajući kako se roditelji koriste mobitelima, požele da se i oni koriste istim. Međutim, sada se postavlja pitanje da li je dovoljno samo dati tek tako djetetu mobitel ili je prije tog koraka neophodno učiniti nešto kako bi zaštitili vlastito dijete od mogućih opasnosti? Pošto živimo u digitalnom dobu gdje nam je većina stvari lako dostupno, tako se mogu pronaći niz aplikacija koje su napravljene za zaštitu kako same djece, tako i smartphone – a.

Ključne riječi: Opasnost, djeca, smartphone, android, aplikacije

MALIŠANI I ANDROIDI

Mališani su sami po sebi radoznali i kao takvima neće im trebati puno vremena da primjete stvari koje vi kao roditelj svakodnevno koristite, a oni nemaju pristup istim. Neko vrijeme će biti moguće da se igraju sa igračkama kao što su mobitel ili tableti, ali tokom vremena će tražiti da koriste upravo isti kao što vi koristite. Kako se sve ranije mališani upoznaju sa tehnologijom, tako će sve teže biti onemogućiti im pristup istim. Nebitno o kojim tehnologijama da se radi prije nego što vaše dijete dođe u dodir sa smartphone – om ili tabletom potrebno je učiniti par jednostavnih koraka kako bi i vi i vaše dijete se osjećalo sigurnijim, kako bi ste spriječili neželjeno brisanje podataka, pristupanje pozivima, instaliranje aplikacija itd. Ovo je najlakše uraditi tako što ćete zaključati Trgovinu Play, odnosno staviti uređaj u sandbox okruženje (ograničeni način rada).

Pošto je kod nas više zastupljeno korištenje smartphone – a sa androidom, kao i tableta tako će se u okviru ovog rada moći pronaći par aplikacija koje već postoje i koje su jednostavne za korištenje, odnosno trebat će vam samo par minuta kako bi ih instalirali

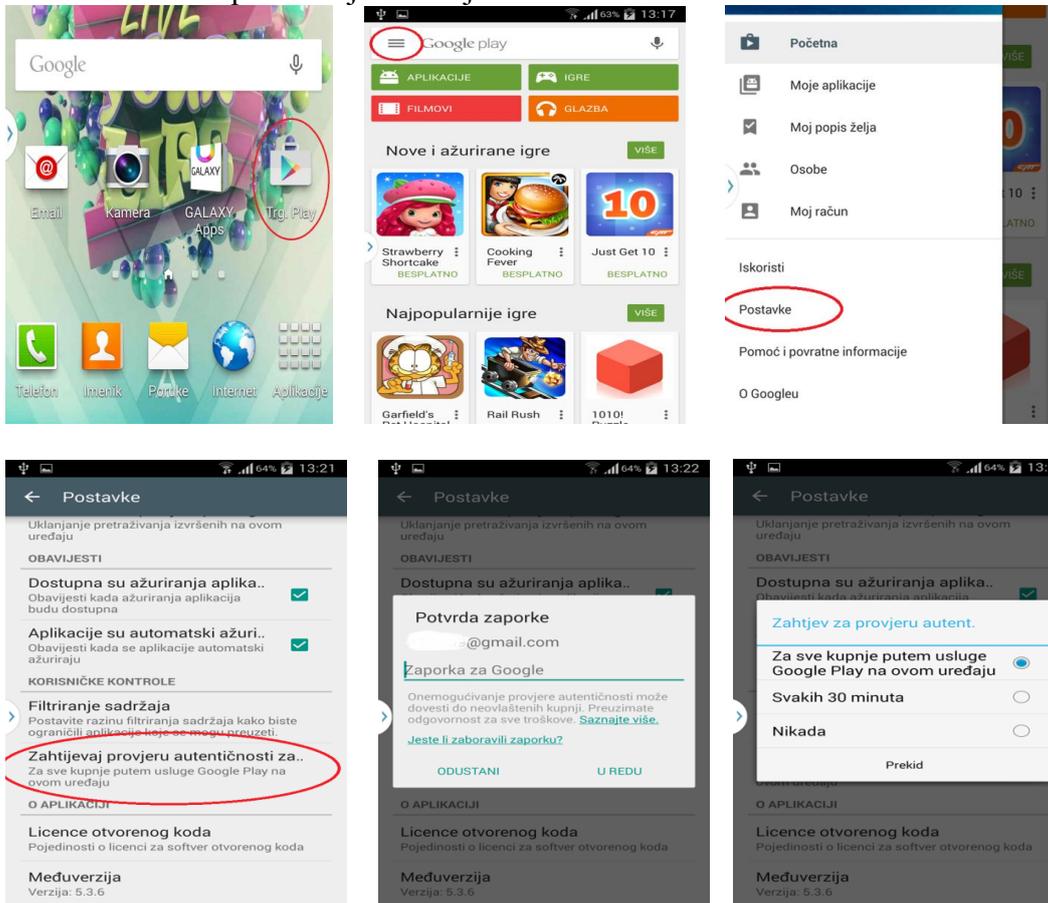
Zaključavanje Trgovina play i filtriranje sadržaja

Jedan od načina jeste zaključavanje Google Play trgovine, kako se ne bi mogle preuzimati i instalirati neželjene ili potencijalno opasne aplikacije. Ovo se može učiniti na sljedeći način:

- Otvori se aplikacija Trgovina Play,
- Dodirnemo  kako bi pristupili meniju,
- Zatim odaberemo opciju postavke,
- Pronađemo red gdje se nalazi „Zahtijevaj provjeru autentičnosti za svaku kupnju“ i odaberemo,
- Nakon toga, pojavi nam se da odaberemo kada želimo to da činimo,

- Zatim je potrebno da postavimo password.

Svi ovi koraci su predstavljeni na sljedećim slikama:



Ukoliko želite da imate dodatnu zaštitu, onda u ovom slučaju može se raditi filtriranje sadržaja, odnosno opcija koja se nalazi odmah iznad „Zahtijevaj provjeru autentičnosti za svaku kupnju“. U tom dijelu odaberemo za koju starosnu grupu želimo filtriranje tako što označimo pored navedenih, kao na sljedećoj slici.



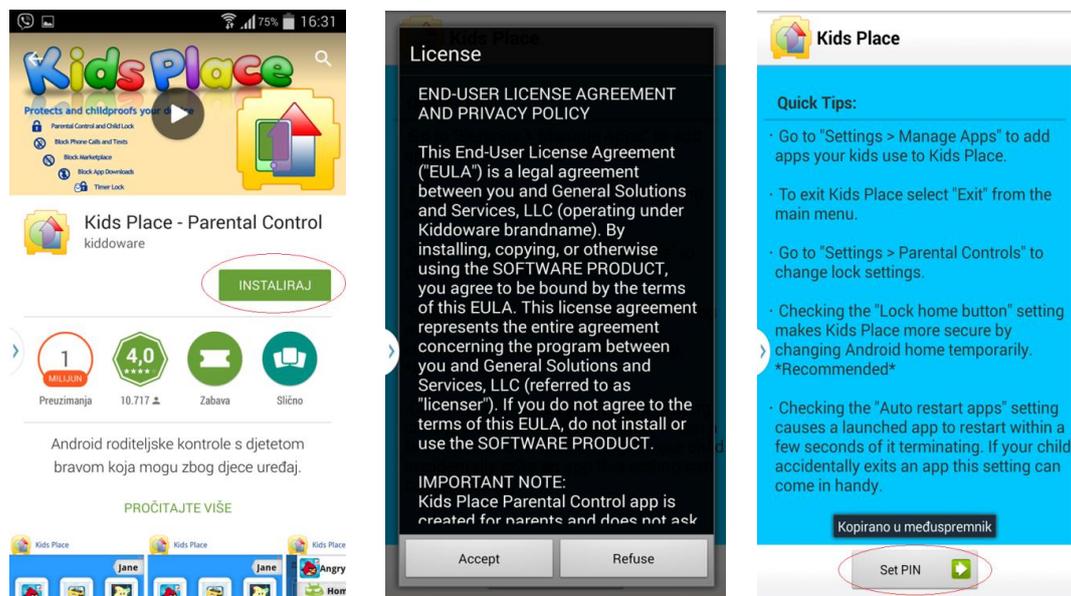
Dodatni korisnički računi

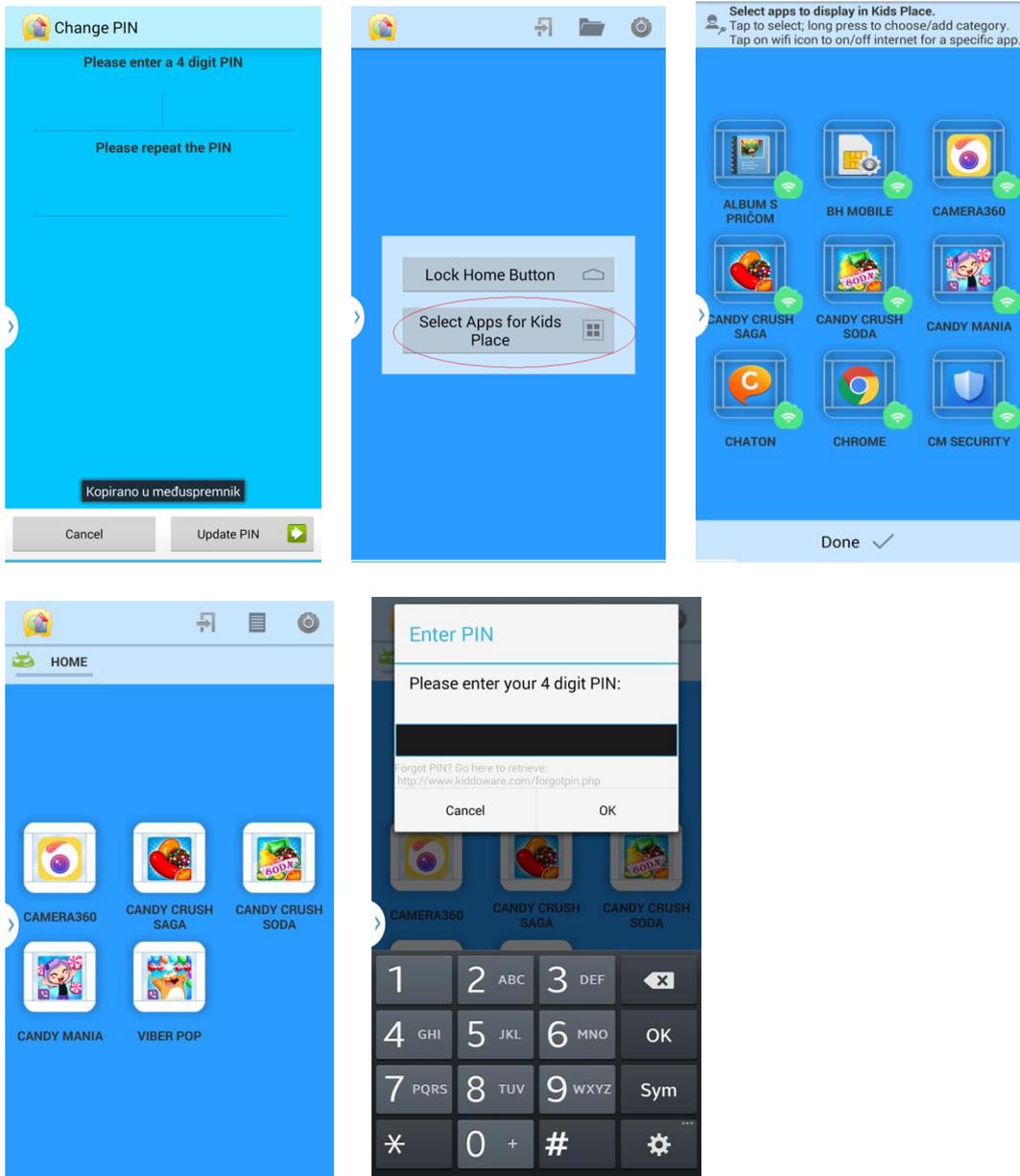
Korisnici Android uređaja koji imaju instaliran najmanje Android 4.2. mogu na svojim uređajima postaviti dodatni korisnički račun. Ovo je jako dobra opcija za sve one koji imaju npr. samo jedan tablet u porodici, a kojim se koristi više članova. Možete postaviti korisnički račun za djecu i u okviru tog računa postaviti ograničenja koja su na raspolaganju.

Stvaranje sandbox okruženja

Kako bi omogućili sandbox način rada, morate instalirati dodatne aplikacije specijalizirane za **roditeljsku zaštitu Androida**. Na svu sreću, ima ih dosta i većina je besplatna. Neke od osobina koje su poželjne: timer koji će automatski ugasiti uređaj nakon vremena koje postavite, blokiranje/dopuštanje pokretanja određenih aplikacija, blokiranje pristupa internetu, blokiranje pristupa pozivima, porukama i imeniku, i slično.

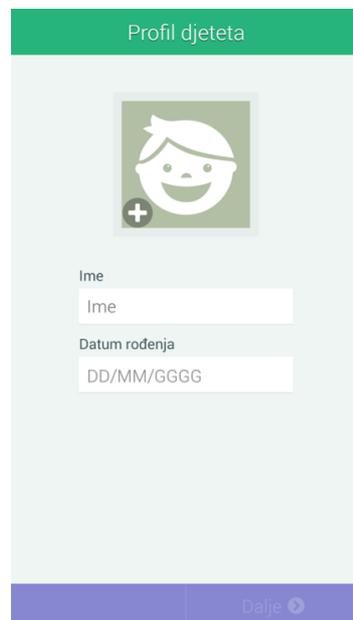
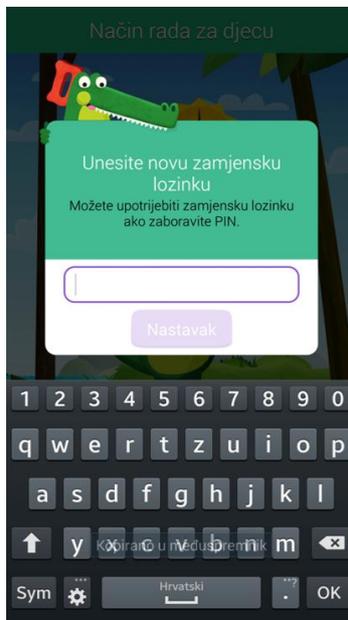
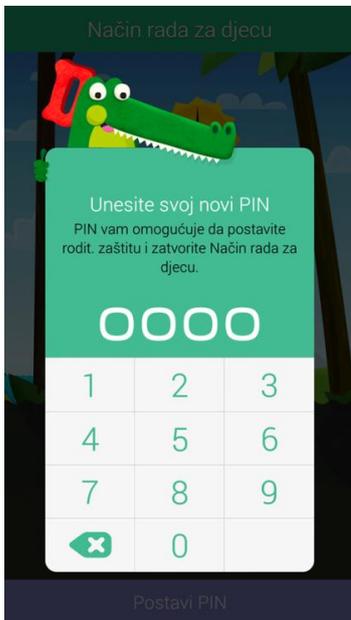
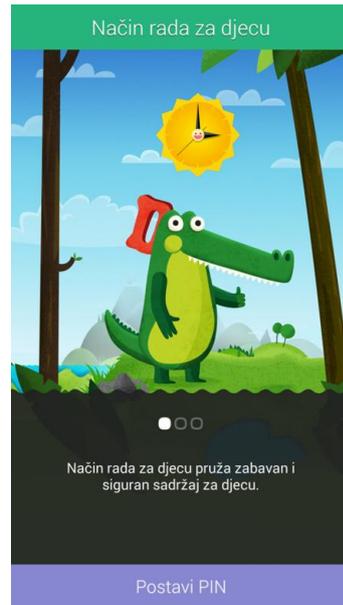
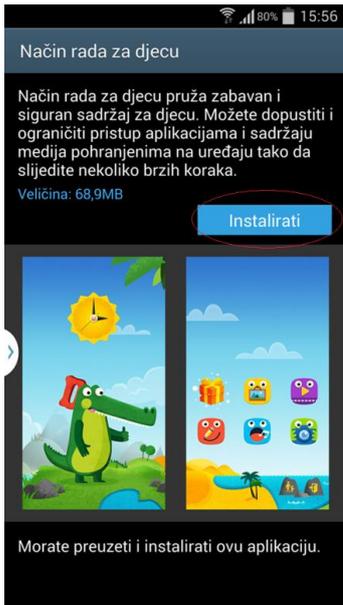
Jedna od takvih aplikacija jeste Kids Place koja je na Google – ovom Play Store ocijenjena sa 4 zvjezdice. Sve što je potrebno da uradite kako bi ste koristili ovu aplikaciju predstavljeno je na sljedećim slikama:

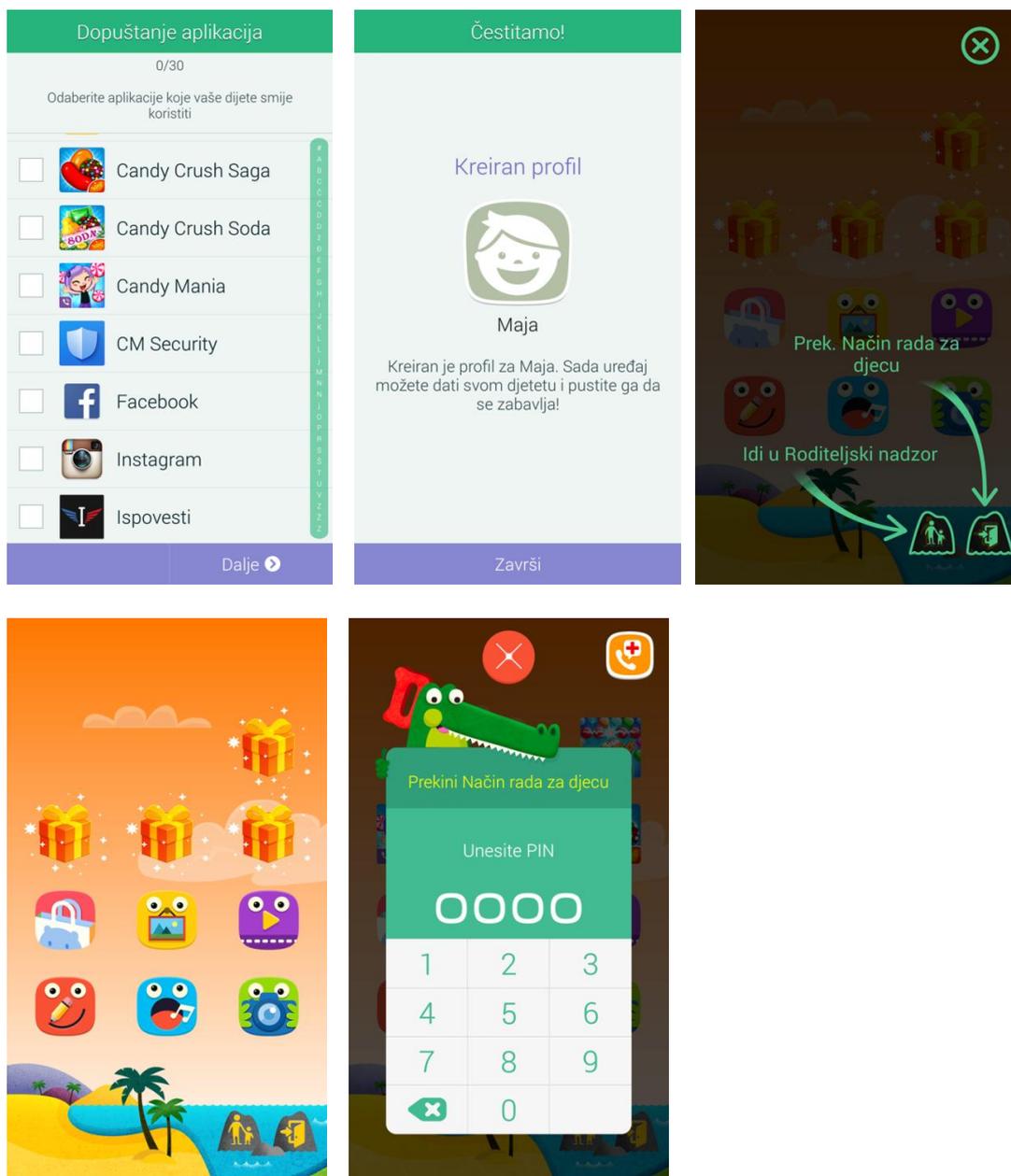




Način rada za djecu

U okviru Android uređaja također je moguće pronaći aplikacije koje su namjenjene baš za zaštitu djece. Jedan od takvih jeste „Način rada za djecu“. Kako instalirati i koristiti ovu aplikaciju moguće je vidjeti na sljedećim slikama:





Također, u okviru aplikacije moguće je dodavati video i audio sadržaje sa različitih servisa kao što su npr. You Tube itd.

IGRE ZA DJECU

Neke od igrica koje se preporučuju za djecu zavisno od uzrasta su:

- Toddler Lock – Ova aplikacija namijenjena je najmlađima (1-3) a zaključava cijeli mobilni telefon i dopušta tek crtanje šarenih linija po ekranu, pri tome puštajući ugodne zvukove. Igra je odlična za djecu koja se prvi put susreću s tabletom ili mobilnim telefonom, a može ih zaokupirati na duže vrijeme.
- Kids Piano Lite – Simpatična muzička aplikacija koja će vašem mališanu pružiti sate i sate zabave. Ima nekoliko načina rada, od jednostavnog “nabijanja” po tipkama do sviranja pjesama ili igranja mini-igrica.

- Zebra Paint Coloring App – Digitalna bojanka čiji ćete potencijal najviše iskoristiti ukoliko imate tablet sa stylusom. Naravno, može se bojati i s prstom, ali onda niste toliko precizni.
- Animal Games for Kids: Puzzles – Ako vaši mališani obožavaju životinje, ovo je prava aplikacija za njih. S lijeve strane nalaze se životinje, a na slici su prazne siluete koje morate popuniti s onom odgovarajućom. Igra je namijenjena djeci od 1-6 godina.
- LEGO Duplo Zoo – Lego igrice su uvijek privlačne mlađim korisnicima, a ni ova nije izuzetak. Namijenjena je djeci od 2-6 godina, a u njoj gradite razne stvari te učite i istražujete.
- LEGO Juniors Create & Cruise – Oni malo stariji (4-7) mogu uživati u ovoj igrici sklapajući LEGO automobile i mini-figure, te na taj način razvijati maštu i kreativnost (nemojte se začuditi ako i sami zaigrate, jer igra je vrlo privlačna i starijoj publici koja se ne boji djeteta u sebi).

ZAKLJUČAK

Nemoguće je opisati koliko je opasnosti koje „vrebaju“ na internetu, neke od njih znamo, ali većinu ne. Svaki roditelj ima za cilj da zaštiti svoje dijete kako bi imalo sretno i sigurno djetinstvo. To je potrebno da čini svakodnevno, ali danas u digitalnom dobu potrebno je da to čini na malo drugačiji način u odnosu na prije. Iz ovog rada je vidljivo da postoji dosta načina koji su jednostavni za korištenje, ali koji su jako efikasni. Za korištenje bilo koje navedene aplikacije potrebno je jako malo vremena kako bi se instalirale i počele da se koriste, ali rezultati korištenja istog su nemjerljivi. Od svega najvažnije je da su djeca koja koriste tehnologiju zaštićeni od svih potencijalnih opasnosti.

UTICAJ RODITELJA NA SIGURNOST DJECE NA INTERNETU

Senida Kakeš, BA, Amir Delić, BA

Sveučilište/Univerzitet Vitez, Fakultet informacijskih tehnologija

senida.kakes@unvi.edu.ba, amir.delic@unvi.edu.ba

SAŽETAK

Roditelji su pokretači svega u životu djeteta. Koliko god mislili da je internet bezopasan, postoji i 8754 druga strana interneta gdje se odvija čitava drama. Cyberkriminal, zlostavljanje djece na internetu i slične kriminalne radnje su česta pojava na zapadu, a u posljednje vrijeme pristižu i u Europu, te na Balkan. Potpuna sigurnost na Internetu je nemoguća, ali ipak bi roditelji trebali uticati na svoju djecu o tome gdje postavljaju svoje informacije i sa kim ih treba dijeliti. Ali prije toga je bitno da su roditelji svjesni takvih radnji na Internetu kako bi znali da se pravilno edukuju i pravovremeno utiču i spriječe neželjene posljedice.

Ključne riječi: Cyberkriminal, Cyberbullying

UVOD

Zapanjujuća je činjenica da je dvije trećine djece na internetu imalo neko loše iskustvo. To podrazumijeva i omalovažavanje na internetu, zlostavljanje, dječija pornografija, zloupotreba informacija, krađa identiteta, krađa facebook, twitter i ostalih računa, i slične aktivnosti. Sve ovo nabrojano treba da uzruja roditelje širom svijeta i nagna ih na razmišljanja. Međutim, uvijek se otvara debato pitanje: Da li je potpuna kontrola roditelja nad svojom djecom na internetu narušavanje njihove privatnosti? U dvije trećine djece koja su osjetila nesigurnost na internetu spada i 41% onih koji su se izjasnili da ih je neko “dodao” za prijatelja na nekoj od društvenih mreža koga ne poznaju, 33% njih je “skinulo” viruse na svoj račun, 10% njih je imalo iskustva sa osobama koje su ih objeđivale na upoznavanje uživo. U takvim situacijama kod djece se javlja ogromno emocionalno uznemiravanje koje opisuju kao pribojavanje, strah, sram, gađenje i zbunjivanje. Međutim, pogrešno je reći da su djeca mlađa od 18 godina sama odgovorna za svoje ponašanje na internetu. Odrasli trebaju da osjećaju odgovornost za njihovo ponašanje. A takvu vrstu odgovornosti mogu ponuditi osim roditelja i školske i obrazovne institucije. Odrasli ljudi, koji su prošli neko informatičko obrazovanje, često steknu iskustvo koje su stranice na internetu sigurne za posjećivanje, dok se djeca mnogo slobodnije ponašaju i u internetu ne vide nikakvu prijetnju niti opasnost. Dakle, prvo su roditelji ti koji trebaju da se edukuju o tome koliko opasnosti postoji na internetu kako bi to mogli prenijeti svojoj djeci. Međutim, u sadašnjem društvu je jako bitno da djeca imaju slobodu da se obrate roditeljima ili nekim nadležnim institucijama (policiji, socijalnim institucijama, obrazovnim institucijama) kada imaju neki problem vezan za njihovu sigurnost na internetu, a bez da budu napadani ili osuđivani. Ukoliko djeca osjete da će biti osuđeni ili odgurnuti sa strane na takva ili slična pitanja, to ih često može dovesti do nepovjerenja ili pogrešnih aktivnosti pokušavajući da se izvuku iz krize u koju su zapali. Međutim, dobra vijest je da djeca vole da budu uključena u obiteljske aktivnosti i često će (ukoliko roditelj pozitivno utječe na dijete) poštovati obiteljska pravila. Nikako ne vole da se osjećaju odbačeno ili

istrgnuto iz nekih važnih odluka roditelja. Naravno, upravo su to stvari koje roditelji trebaju da iskoriste kako bi zajedno sudjelovali u prevenciji loših iskustava djece na internetu i eventualno ih pokušali navesti na prave primjere ponašanja na internetu. Ono što bi svaki roditelj trebao da kaže svome djetetu prije stupanja u kontakt sa internetom su osnove ponašanja na internetu, kao naprimjer: Ne zlostavljati nikoga psihički na internetu, obratiti se roditeljima za bilo koji problem sa kojim se suoče, ne maltretirati niti uznemiravati druge ljude, ne postavljati neadekvatne fotografije na društvene mreže, ne nasjedati na "spam" poruke, ne odavati nikome privatne informacije, ne odgovarati na poruke nepoznatim osobama.

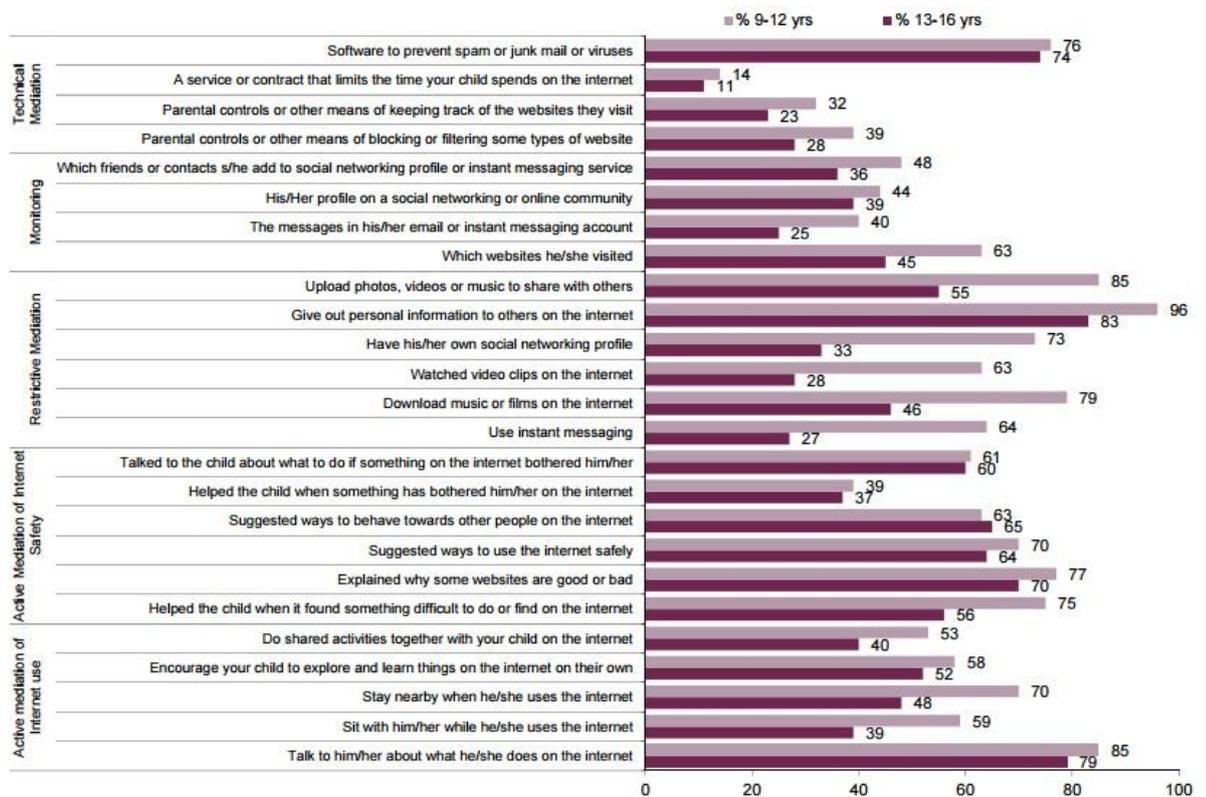
PODRŽAVANJE DJEČIJE SIGURNOSTI

U podržavanju dječije sigurnosti na internetu treba da učestvuju razne institucije uključujući vladu, nastavno osoblje i obrazovne ustanove, internet provajdere i servise, agencije za sigurnost i zaštitu djece, roditelje i samu djecu. U podržavanju dječije sigurnosti se treba uticati na više pozitivnije načine, dakle umjesto zabranjivanja i restrikcija, roditelji bi trebali prenijeti pozitivna iskustva korištenja interneta. Dakle, umjesto društvenih mreža približiti im internet za druge aktivnosti, kao naprimjer čitanja knjiga, gledanje dokumentaraca, istraživanja na internetu, slušanje muzike i tako dalje, kako bi djeca počela da koriste internet na sigurniji način, a ujedno bi bili i odvojeni od direktne komunikacije sa drugim osobama putem interneta i tako smanjili mogućnost nasilja. Danas je izlaganje sebe i privatnih informacija online jedna od svakodnevnih aktivnosti (objavljivanje slika, statusa, pjesama, aktivnosti itd.). Zapanjujuća je činjenica da djeca u Europi u prosjeku provedu 88 minuta online na dan, od kojih djeca između 9-10 godina provedu u prosjeku jedan sat online a djeca između 15-16 godina u prosjeku dva sata. Skoro polovina djece idu online u svojim sobama, dok jedna trećina imaju pristup internetu na mobilnim i drugim lako prenosivim uređajima (tableti, laptopi). Dakle, iz godine u godinu djeca sve mlađa i mlađa imaju pristup internetu, a u novije vrijeme i roditelji dobrovoljno objavljuju fotografije svoje djece na društvenim mrežama te ih tako nesvjesno izlažu internetu i široj javnosti. Dakle, umjesto što bi trebalo da bude obrnuto, roditelji su često nezainteresovani ili nedovoljno obaviješteni i edukovani da kontrolu uzmu u svoje ruke i tako zaštite svoju djecu. Ali sa druge strane, strogim restrikcijama i zabranama, roditelji djeci oduzimaju mogućnosti šireg učenja i obrazovanja, komunikacije sa prijateljima, učestovanju u zabavi i slično.

Šta roditelji rade dok su djeca online?

Osim što su roditelji nezainteresovani za aktivnosti svoje djece na internetu, postoje i drugi razlozi zbog kojih roditelji obavljaju neke druge aktivnosti dok su njihova djeca izložena rizicima. U anketi koju je objavila britanska agencija "EU Kids Online" ispitano je 25, 142 učesnika, u dobi između 9- 16 godina, kako bi utvrdili koje su sposobnosti i strategije roditelja koje mogu spriječiti rizike njihove djece na internetu. U toj anketi su ispitani i roditelji, dakle koje su to aktivnosti koje oni obavljaju dok su njihova djeca online. 89% njih postavljaju pravila o tome da li njihova djeca smiju odavati privatne informacije o sebi, 82% njih razgovaraju sa svojom djecom, pogotovo kćerkama, o tome šta rade na internetu a 59% njih ostaju u blizini svoje djece dok su na internetu. Međutim, provjeravanje šta su njihova djeca radila na internetu je manje popularno, jer to odaje manjak povjerenja sa obje strane. Tri četvrtine njih koriste neki oblik softverskih rješenja (antivirusne programe) kako

bi spriječili eventualne napade virusa ili spam-a, a trećina ih koristi filtere iz sigurnosnih razloga. Od njih deset, otprilike jedno koristi neke posrednike koji su napomenuti u anketi (Slika 1.). Roditelji koriste te posrednike (programe i razna softverska rješenja), međutim sve manje kako djeca postaju starija. Ali svakako savjetuju svoju djecu o sigurnosti na internetu. Korištenje tih posrednih rješenja je manje u porodicama sa nižim obrazovanjem, malim finansijskim prihodima, manjim korištenjem interneta. Neki od njih čak misle da isključivanje računara iz napajanja pomaže u sigurnosti. Međutim, te informacije se ne brišu isključivanjem iz računara već samo duže ostaju dostupne. Oko 15% roditelja se izjasnilo da su promijenili pogled na sigurnost na internetu ako su njihova djeca doživjela neke neugodne posljedice interneta. Jedna četvrtina njih (23%) misli da je prilično sigurno da će njihovo dijete doživjeti neki oblik neugodnosti u sljedećih šest mjeseci, dok su njih 5% sigurni u to da će njihovo dijete doživjeti neugodnost. Polovina njih misli da je neophodno da se više uključe u to šta njihova djeca rade na internetu te u slične aktivnosti. Nake studije pokazuju da ukoliko su roditelji pokretači određenih aktivnosti na internetu (edukativne prirode) smanjuje rizik štete. Međutim, uglavnom ni sami roditelji nisu svjesni širine internetskih mogućnosti i količine dostupnih informacija. U sljedećoj anketi su postavljena sljedeća pitanja: Koje od sljedećih aktivnosti radite sa svojom djecom? Jeste li ikada neke od sljedećih aktivnosti radili sa svojom djecom? Da li je vašem djetetu dopušteno ili zabranjeno da stalno radi/ ne radi neke od ovih aktivnosti? Da li ste ikada provjeravali šta su vaša djeca radila na internetu? Anketa je obrađena na način- jedan roditelj od svakog ispitanika koje koristi internet.



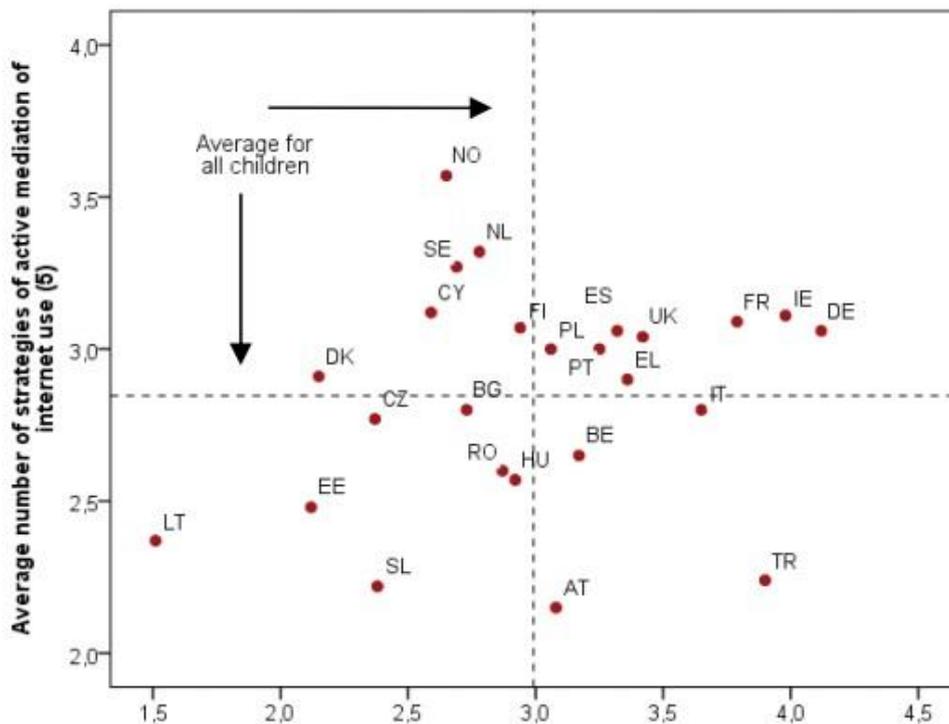
Slika 1: Rezultati ankete

Mitovi i problemi sa kojima se suočavaju roditelji

Postoji problem koji je opšte poznat na internetu, a to je da sve što se postavi online može se iskoristiti bez ikakvih odobrenja onoga ko je to postavio. Taj problem je pogotovo izražen u državama i okruženjima koje nemaju regulisan sistem za zaštitu informacija na internetu (nemaju regulisana autorska prava i korisnici interneta se nemaju kome obratiti ukoliko ista budu narušena). Međutim, kada su roditelji u pitanju, onda oni imaju drugačija razmišljanja. Prema anketi, četiri petine roditelja su uvjereni da mogu pomoći svojoj djeci ukoliko se iznađe neki problem (to je pogotovo slučaj sa roditeljima koji imaju mlađu djecu), a nekolicina njih je prilično sigurna da njihova djeca mogu sama savladati neke od problema. Roditelji koji upotrebljavaju restriktivne metode kako bi zaštitili svoju djecu, imaju djecu koji se manje suočavaju sa rizicima i štetama (međutim, pošto ova djeca imaju manje pristupa internetu također imaju manje i digitalnih vještina). Dok je obratna situacija kod roditelja koji upotrebljavaju druge metode kao što je praćenje i nadgledanje šta njihova djeca rade na internetu. Međutim, iako roditelji tvrde da uglavnom ne znaju i nisu sigurni u aktivnosti njihove djece na internetu, djeca ispitanih roditelja tvrde suprotno. Dvije trećine djece (32%) tvrdi da njihovi roditelji znaju šta oni rade online, ali ipak polovina njih tvrdi da njihovi roditelji vrše restrikcije i zabrane i tako ih spriječava u obavljanju određenih aktivnosti online koje bi oni željeli da rade. I povrh toga, trćina ispitanika ignoriše to što njihovi roditelji kažu o njihovom korištenju interneta. Oko 5% njih se izjasnilo da bi voljeli da se njihovi roditelji više zainteresiraju o tome, dok njih 10% ne bi volelo da roditelji imaju neki veliki interes za njihove aktivnosti na internetu. Ali svakako bi rezultati sigurnosti i zaštite djece na internetu bili bolji kada bi roditelji posvetili pažnju tome. Međutim, da li djeca koriste više ili manje internet zavisi i od navika njihovih roditelja, te drugih faktora kao što je kultura i okruženje u kojem žive ili finansijsko stanje porodice.

Različitosti po državama

Koje metode koriste roditelji i sa kojeg stanovišta i načina posmatraju ovu temu zavisi i od kulture i države. Na individualnom pogledu, što su roditelji više upoznati sa informacijama o tome šta njihova djeca rade na internetu to je više zastupljena metoda restrikcije. Međutim sve ovisi od države do države. Zemlje Sjeverne Europe kao što su Norveška, Švedska, Danska, Finska i Nizozemska praktiraju više učešće u aktivnostima svoje djece na internetu ali manje su zastupljene metode restrikcije. Međutim, zemlje Istočne Europe kao što su Litvanija, Estonija i Rumunska su karakteristične po ispodprosječnom restriktivnom učešću. Osebito u Turskoj, ali i u Austriji, Italiji i Belgiji, roditelji preferiraju metode zabrane i to iznadprosječnosti od ostatka Europe. Visoko učešće u aktivnostima i zaštiti neke vrste, svoje djece na internetu ali i visokim restriktivnim metodama karakteriziraju se države Južne Europe kao što su Portugal, Španija i Grčka, ali ovaj način je zastupljen i u nekim drugim zemljama (Francuska, Njemačka i Velika Britanija). (Slika 2.)



Slika 2: Prosječan broj restriktivnih strategija u posredovanju aktivnosti svoje djece

OPASNOSTI INTERNETA

Većina roditelja nisu u mogućnosti prepoznati simptome ili opasnosti internet svijeta. Nisu u mogućnosti prepoznati opasnosti jer nisu u dovoljnoj mjeri edukovani o svim trenutno postojećim opasnostima, a samim tim onda ne znaju prepoznati ni simptome ukoliko se ta opasnost i dogodi, jer veći broj djece (pogotovo u tinejdžerskoj dobi) se boji priznati da je žrtva nekog vida nasilja. Uglavnom iz osjećaja sramote, osuđivanja ili pak straha. Roditeljima se apeluje da utiču na svoju djecu tako što će i oni da se edukuju i koriste internet na siguran način. A neke od opasnosti koje su prijetnja za njihovu djecu su:

- Krađa identiteta,
- Internet predatori,
- Veliki opseg dostupnih stranica (od kojih su neke lažne),
- Nemogućnost privatnosti informacija,
- Djeca preuzimaju kontrolu na internetu

Mogući simptomi

Ono što roditelji često ne znaju jeste da su upravo djeca i tinejdžeri uglavnom meta internet predatora. Mnogi od njih također nisu svjesni da se takav proces ne dešava preko noći. Dakle, internet predatori se uglavnom predstavljaju da su starosne dobi kao i njihove mete te na taj način pokušavaju da zadobiju povjerenje djece. Takav proces može potrajati danima i sedmicama. Kako bi roditelj na vrijeme reagovao na ovakvu vrstu prijetnji potrebno je da prati ponašanje svoga djeteta na internetu. A jedan od simptoma jeste ako dijete ulazi na internet u isto vrijeme svaki dan. Ovo je znak da su ostvarili svakodnevni vid komunikacije sa nekim ko nema čiste namjere. Također pod takvim ponašanjem se podrazumijeva i ako se dijete ponaša tajnovito

kada koristi računar. A pod takvim ponašanjem se smatra da krije historiju posjećenih stranica na web pregledniku, ukoliko automatski gase računar ili prebace svoj interes na drugu aktivnost kada roditelj uđe u prostoriju i slično. Ovakvi i slični simptomi mogu ukazivati da dijete ne želi da roditelj vidi ono što on radi na internetu, dakle ili je ostvarilo neki vid komunikacije sa nepoznatim licem koji može biti dječiji predator ili jednostavno radi i posjećuje stranice koje nebi trebalo. Također, ukoliko je dijete odviše sretno kad napusti internet i ugasi računar, velika je mogućnost da su na putu ka nevoljama.

Kako reagovati?

Međutim, ovakve vrste simptoma mogu biti pomalo zagonetne. Postoji mogućnost da su završili neki školski projekat pa osjećaju sreću, ali u svakom slučaju ako se patern ovakvog ponašanja događa duže on nekoliko dana, potrebno je da roditelj to uprati i reaguje. Također, suptorno ovom simptomu može se javiti i simptom da je dijete depresivno Pogotovo kada se odjavi sa interneta. Moguće je da su postali meta uznemiravanja ili zlostavljanja. U ovakvim slučajevima djeca obično teže ne razgovarati ni sa svojim prijateljima i zatvaraju se u sebe. Na ovakve simptome pod hitno treba reagovati. Ali opet se postavlja pitanje: Kako roditelji mogu reagovati a da ne naruše povjerenje svoje djece? Ukoliko roditelj primijeti ovakvo ponašanje kod svoga djeteta, treba prvo sačekati da se dijete obrati roditelju za pomoć. Međutim, da bi se dijete obratilo za pomoć potrebno je da roditelja smatra dovoljno zrelim da može riješiti djetetov problem. U drugu ruku potrebno je da je roditelj jako blizak sa svojim djetetom da bi dijete steklo njegovo potpuno povjerenje. Međutim, ako se dijete obrati sa problemom roditelj treba da istraži problem, a potom da sa interneta ukloni što više informacija o porodici ili djetetu. Zatim da promijeni broj telefona djeteta, ili kućni broj. Također da izmijeni e-mail adrese. Također je potrebno da se preduzmu dodatne sigurnosne mjere, kao što su bolje praćenje okoline, zaključavanje doma i auta, i po mogućnosti kontaktiranje nadležnih organa (policije ili socijalnih i zdravstvenih ustanova). Također treba imati u vidu da mlađa djeca i tinejdžeri pokušavaju da se uklope u svoje društvo i pokušavaju da izgledaju "cool" pred drugom djecom, i često iz tih razloga postavljaju videe i slike na društvene mreže o sebi i svojim aktivnostima.

Prevenција i smanjivanje rizika od internet opasnosti

Prevenција je češće potrebna u ovakvim situacijama nego reakcija. Potrebno je preuzeti mjere opreza kako nebi došlo do izlaganja djece opasnostima interneta. Neki stručnjaci smatraju da neke od sljedećih preventivnih koraka može umanjiti rizike:

- Prije svega važno je računar s pristupom internetu postaviti u dnevnu sobu ili prostoriju u kojoj češće borave roditelji. Na taj način nadgledanje sadržaja s kojima se dijete susreće postaje lakše te roditelji mogu upoznati djetetove on-line prijatelje. Dijete će teže ući u potencijalno rizičan razgovor s strancem u chat-roomu ili tražiti pristup eksplicitnim seksualnim sadržajima ako roditelj može usput pogledati što dijete radi na kompjuteru.
- Važno je da roditelji nauče osnovne stvari i terminologiju u korištenju interneta i u tome mogu potražiti dječju pomoć, što nudi mogućnost za uspostavu komunikacije, pokazivanje interesa za ono što dijete radi i odnosa povjerenja. Pokazujući interes i pažljivo nadgledajući djetetove aktivnosti na

internetu, ipak mogu zaštititi djecu od rizika, što je u svakom slučaju bolje nego jednostavno upotrebljavati restriktivne metode.

- Bitno je postaviti određen skup pravila o korištenju interneta, vremenu koje dijete provodi, stranicama koje posjećuje te dogovorene posljedice ponašanja. Djeca će uglavnom ta pravila prihvatiti i na to će odlično reagirati, jer im je jasno da su roditelji tu, da se brinu i da se imaju kome obratiti u slučaju potrebe. Važno je da roditelji uključe i dijete u proces dogovaranja pravila, čime povećavamo djetetovu odgovornost za poštivanje dogovorenih pravila.
- Odrasli, i nastavnici i roditelji, mogu se educirati kako provjeriti koje stranice dijete posjećuje. Pri tome je važno otvoreno komunicirati s djetetom, kako ovaj način provjeravanja ne bi dugoročno narušio odnos roditelja ili nastavnika s djetetom.
- Važno je objasniti zašto provjeravati sadržaje koje dijete posjećuje. Naprimjer to se može uraditi riječima: "Brine me to što na nekim web stranicama postoje sadržaji koji su neprikladni za djecu" ili "Moja je odgovornost i obveza kao odraslog da vodim računa na to koliko vremena i kako provodiš na internetu". Preuzimanje odgovornosti odraslog u ovom slučaju je isto kao i u situacijama kad je odrasla osoba odgovorna koliko mladi provode vremena u gledanju televizije, čitanju časopisa i stripova, igranju video-igara itd.
- Dobro je s djetetom razgovarati o tajnama i o tome kakve tajne roditelj čuva. Također, važno je djeci reći da, ako se osjećaju neugodno ili zbunjeno zbog nečeg što su doživjela, uvijek mogu razgovarati s roditeljima ili odraslom osobom kojoj vjeruju.
- Moguće je da će dijete htjeti upoznati svog online prijatelja ili prijateljicu. Važno je da na prvi susret dijete odlazi u pratnji roditelja ili odrasle osobe kako bi i roditelji upoznali novog prijatelja svoga djeteta. Djetetu objasniti da prijatelj koji im stvarno želi biti prijatelj i ima poštene namjere neće imati ništa protiv da upozna roditelje, kao što bi bilo dobro da online prijatelj dođe sa svojim roditeljima.

Također je bitno da osim preventivnih metoda, roditelj uvijek bude u pripravnosti. Ukoliko su djeca mlađa izuzetno je važno edukovati se o softverskim alatima i mogućnostima koje postoje za prevenciju ulaska na nedozvoljene sadržaje i eksplicitne web stranice. Neki od najpoznatijih alata a dosad najpouzdaniji jeste "Family Safety" iz porodice Microsofta, gdje roditelj neće zabraniti djetetu korištenje interneta ali ga stavlja pod nadzor.

ZAKLJUČAK

Internet je danas najveći i najbrži izvor informacija. Međutim, tim informacijama je bitno raspolagati na prave načine. Djeca su nevina i naivna bića, i sve što rade to vide iz okruženja ili od svojih uzora. Tako je jako bitno da roditelj bude uzor svome djetetu. Glavni uzrok zašto se dešavaju dječija zlostavljanja na internetu je često nedovoljna edukacija roditelja i obrazovnih ustanova. Svi danas imaju mišljenje da njihova djeca postaju pametnija od prethodnih generacija, samo zato što znaju koristiti tehnologiju i moderne uređaje. Međutim, nijedno dijete se nije rodilo naučeno, i sve što nauči, nauči od roditelja i okoline. Stoga svaki roditelj treba da bude spreman na nove izazove. Na nova učenja. Čak i ako se nikada nije susretao sa tehnologijama, mora biti svjestan da njegovo dijete hoće u nekoj fazi svog života. A

studije pokazuju da i sami roditelji prave česte greške, pa postavljaju slike svoje male djece na svoje facebook profile. Naravno da to oni rade nesvjesno, ali kada bi se posvetili malo više ovom problemu, postali bi više oprezniji. Dakle, nikada dijete neće biti pametnije od svoga roditelja ukoliko je roditelj spreman da uči. Pogotovo sada kada je ovo nova informatička paradigma, i sve što je važno prije dvadeset godina sada ne važi. Nažalost, činjenica je da djeca imaju i po pet stotina prijatelja na društvenim mrežama, međutim roditelj se mora zapitati: Je li moguće da moje dijete poznaje 500 ljudi? Naravno da nije moguće, i to je jedan od znakova da su i neznancima dostupne informacije koje dijete slučajno ili namjerno podijeli na društvenim mrežama. Postoje mjere sigurnosti na društvenim mrežama, i takve mjere roditelji treba da iskoriste. Da uključe što manju vidljivost i izloženost slika i sadržaja nepoznatim ljudima, da komuniciraju na internetu sa samo poznatim licima i tako dalje. Generalni je problem što roditelji danas nemaju vremena za neke druge aktivnosti sa svojom djecom, i kupujući djetetu računar rješavaju se muka. U redu je da se dijete upozna sa takvim uređajima kako bi stekli neke druge prednosti i vještine digitalnog doba, ali potrebno je da je roditelj uvijek u kontroli, pa makar i nesvjesno. Potrebno je da roditelji budu uzor svojoj djeci a ne glumci ili pjevači.

LITERATURA

- [1] http://www.childalert.co.uk/article.php?articles_id=352 (25.03.2015)
- [2] <http://www.lse.ac.uk/media@lse/research/EUKidsOnline/EU%20Kids%20III/Reports/ParentalMediation.pdf> (25.03.2015)
- [3] <http://childdevelopmentinfo.com/family-living/kids-media-safety/children-teens-web-internet-safety/> (26.03.2015)
- [4] http://www.cnzd.org/site2/index.php?option=com_content&view=article&id=103%3Astvari-koje-roditelji-i-odrasli-trebaju-znati-o-djeci-i-internetu&catid=38%3Aroditelji&Itemid=82 (26.03.2015)

SOFTVERI ZA ZAŠTITU I KONTROLU DJECE NA INTERNETU

Nehad Gaši, BA

Sveučilište/Univerzitet Vitez, Fakultet informacijskih tehnologija

nehad.gasi@unvi.edu.ba

SAŽETAK

U ovom radu opisano je kako uz ličnu zaštitu možemo zaštititi i kontrolisati djecu na internetu uz pomoć određenih softvera, odnosno kako da spriječimo da dijete bude žrtva internet kriminalaca, to jest osoba koje nastoje da zloupotrijebe slike i ostale privatne stvari koje djeca postavljaju na internet. Također je opisano i to kako da kontrolišemo djecu uz pomoć navedenih softvera koji nam omogućavaju da pratimo šta djeca rade za računarom i koje stranice, video zapise ili podatke pretražuju po internetu.

Ključne riječi : softver, zaštita, kontrola, internet, napad, netnanny, k9Web, kidZui

UVOD

Internet i njegovi brojni servisi poput e-maila, youtube-a, raznih stranica sa online igrama su za milijone ljudi danas postali svakodnevnica. Upotreba interneta proširila se skoro na svaku školu ili kuću, tako da je među korisnicima sve više djece koje su osnovno školskog uzrasta. Prema rezultatima istraživanja, više od pedeset posto djece svakodnevno koristi internet, a 27 posto ih je bilo izloženo porukama seksualnog sadržaja ili nekom drugom obliku internetskih prijetnji. U većini slučajeva roditelji nisu bili prisutni prilikom surfanja njihovog djeteta ili ne znaju kako da osjete potencijalne opasnosti za svoje dijete i za sebe. Dosta roditelja nije informisano o opasnostima koje mogu nastati zbog nekontrolisanog korištenja interneta, a velika većina djece internetom surfa bez cilja u potrazi za zanimljivim sadržajem. Zbog rastućih problema ovog tipa stvorena je potreba za efikasnom edukacijom djece i roditelja o opasnostima prilikom korištenja interneta. Iako je internet sjajan izum koji je u mnogo čemu poboljšao kvalitet života ljudi i dosta pomogao u širenju mnogih znanja, nemoguće je njegovo korištenje bez problema i opasnosti koje nastaju upotrebom interneta. Na Internetu se neke stvari jednostavno ne rade s oprezom i na tačno određen način na koji bi se trebale raditi, a kada su djeca u pitanju nameću se i dodatna logična ograničenja s obzirom na njihove godine. Internet je danas izvor svega i svačega, pa tako i materijala koji je prilično opasan za one najmlađe. Tu je uvijek i rizik od upadanja u zamku različitih trolova, perverznojaka i sl. što znači da je nadzor roditelja od velikog značaja. Internet trol označava osobu koja dolazi na internet zajednice kao što su internet forum, soba za razgovor (chat room), tematske grupe (newsgrupe), blogovi, i to s jedinim ciljem da na njih šalje uvredljive poruke ili poruke koje nisu tema da bi namjerno dosađivala ostalim učesnicima, stvarala zavade, odnosno remetila red rasprave na tim određenim stranicama na kojima taj trol upada. Pored same roditeljske zaštite, potrebna je i softverska zaštita koja može dosta pomoći da dijete bude sigurno dok se koristi internetom i njegovim sadržajem. Najbolja zaštita jeste da svaki roditelj u bilo kojem trenutku zna šta njegovo dijete radi za računarom i na internetu, to jest da sjedi blizu svog djeteta i tako ima pristup svemu što dijete koristi, ali je svima poznato da je to nešto što je nemoguće u današnjem vremenu i da nijedan roditelj nije u stanju da sjedi pored djeteta i prati njegov rad na internetu, tako da se softverska zaštita

pokazala kao jedna odlična zamjena za to i kao odlična zaštita i kontrola djeteta na internetu. Mnoge kompanije su se odlučile na kreiranje raznih softverskih alata za kontrolu i filtriranje internet sadržaja, kao i kreiranje raznih web browsera koji su namjenjeni baš mlađoj populaciji, odnosno djeci između 3 do 12 godina koji su najčešće mete napada na internetu.

SOFTVERI I BROWSERI ZA KONTROLU INTERNET SADRŽAJA

Softveri za kontrolu internet sadržaja

- NetNanny
- SentryPC
- KidsWatch
- WebWatcher
- SafeEyes
- TimeSherif
- TimeBoss
- K9 Web protection

K9 Web protection

K9 Web protection je besplatni internet filter i program veličine dva do tri MB za kontrolu aktivnosti na internetu. Ovaj navedeni softver omogućava blokiranje web stranica prema kategorijama, uključujući pornografiju, zloupotrebu droga, društvenih stranica, stranica na temu mržnje, nasilja, rasizma. Također posjeduje unaprijed postavljene razine zaštite, ovisno o dobi vaše djece. SafeSearch ili sigurno pretraživanje omogućuje pročišćene rezultate pretraživanja u svim pretraživačima. Vremenska ograničenja ili Time restrictions djeci onemogućuju pristup internetu u odabrano vrijeme. Tu je i mogućnost odabira stranica koje će se uvijek dopustiti (always allow) i onih koje će se uvijek blokirati (always block). K9 posjeduje i mogućnost deblokiranja sadržaja uz upis šifre (koja je poznata samo roditelju). Ovaj način je dovoljno čvrsta zaštita koju ni spretniji učenici ne mogu probiti, a posjeduje i mogućnost izvještavanja o aktivnostima djece na internetu (koje stranice posjećuju). Program koristi tri vrste lista i to : Black List (crna lista) koja sadrži stranice koje su zabranjene, odnosno koje je roditelj zabranio da njegovo dijete posjećuje, White List (bijela lista) koja sadrži stranice koje je roditelj dozvolio da njegovo dijete koristi i Neutral List (neutralna lista).



Slika 1.: Izgled K9 Web protection-a

NetNanny

Net Dadija je brand sadržaja kontrolnog softvera, koji je prvenstveno kreiran za roditelje da im omogući kontrolu djeteta i aktivnosti djeteta na računaru i internetu. Vodeći proizvođač omogućuje vlasniku računara blokiranje i filtriranje internet sadržaja, vremenske rokove za korištenje računara i blokadu PC igrica. Net Nanny (Net Dadija) je najučinkovitiji i najfleksibilniji plaćeni internet filter koji je dostupan danas. Cijena Net Nanny-a iznosi 30 \$ za PC verziju. Net Nanny posjeduje dinamično filtriranje koje osigurava da članovi vaše obitelji neće biti izloženi pornografiji i drugim uvredljivim sadržajima. Net Nanny je jedini obiteljski orijentirani filter koji vam omogućuje da pratite i upravljate željenim računarom pomoću korištenje interneta s bilo kojeg mjesta u bilo koje vrijeme. Pored Windows platforme, Net Nanny je dostupan i za: Mac, iOS, Android i za socijalne mreže.



Slika 2.: Prikaz interface-a NetNanny zaštite

Web browseri za sigurno surfanje djece

- Buddy Browser
- PikLuk
- My Kids browser
- KidRocket
- KidZui
- Zac Broswer
- Shrek Browser
- McGruff Kid Safe

KidZui browser za djecu

KidZui je web preglednik koji omogućava pristup na preko 500.000 web stranica koji sadrže tekst, slike i video zapise, a posebnost programa je što su svi sadržaji i stranice pregledani su od strane učitelja i roditelja. Preko 250 kompetentnih osoba pregledava i odobrava stranice, video sadržaje i slike, koristeći se rigoroznim procesima selekcije, a oni ne samo da odobravaju sadržaj, već ga i kategoriziraju prema dobnoj primjerenosti. Preglednik je namijenjen uzrastu od 3-12 godina.

KidZui ne stvara sadržaje, on ih prikuplja iz svih kutaka interneta, a baza prijateljskih web stranica svakodnevno raste. Uz sve to, mogu se i dodavati web mjesta: kao što su škola, obiteljski blogovi... Uslugu pruža tvrtka, iz San Diega, istog imena, a unutar softvera koji se je razvijao tri godine, tvrtka je pokušala stvoriti zabavan i veseo svijet. Tako svako dijete može biti zastupljeno svojim "Zui," avатарom koji ga

predstavlja prijateljima i drugim korisnicima, može se prilagođavati kosa, odjeća i druge značajke. Ima također puno zvučnih efekata, a svaki prijatelj mora biti odobren od strane roditelja.³³

Starija djeca mogu također pretraživati stranice po ključnim riječima koristeći okvir za pretraživanje. Ako dijete zatraži ili pokuša samostalno upisati URL neke stranice koja se ne nalazi u bazi sigurnih, sustav se blokira dok čeka pregled od strane uredničkog tima. Ekipa KidZuia tvrdi da će se pregled s njihove strane dogoditi u roku od tri sata. Glavna stranica Google i Yahoo pretraživača ne mogu biti pozvane. Kao najbolja stvar vi kao roditelj primati ćete sedmične e-maileve koje će vas obavještavati o sedmičnim aktivnostima vašeg djeteta kada je online.

KidZui-u se ne može pristupiti putem web preglednika. Umjesto toga, mora se preuzeti poseban KidZui browser, bilo da se radi na Windows ili Macintosh platformi. KidZui je besplatan za korištenje sa ograničenim mogućnostima (osnovnim) za svu djecu. Međutim, nudi se i opcija članstvo, koja omogućava djeci i roditelja mnogo dodatnih mogućnosti. Pretplaćena usluga iznosi \$ 9.95 mjesečno ili 99,95 dolara godišnje, što za dječju sigurnost u online svijetu doista nije mnogo.³⁴



Slika 3.: Izgled KidZui browsera za djecu

³³ <http://www.bswireless.hr/lifestyle/563-kidzui--internet-za-djecu>

³⁴ Ibidem

**PROBLEMATIKA KRIMINALITETA NA PODRUČJU
SREDNJOBOSANSKOG KANTONA SA POSEBNIM OSVRTOM NA
RAZBOJNIŠTVA I RAZBOJNIČKE KRAĐE**

Mr. sc. Adnan Pirić

piricadnan@unvi.edu.ba

Sveučilište/Univerzitet „Vitez“ Vitez, Fakultet pravnih nauka

SAŽETAK

Razbojništva i razbojničke krađe, specifična vrsta imovinskog kriminaliteta, oduvijek su predmet interesovanja građana i stručne javnosti. Kroz istraživanje koje će se provesti u ovom radu, nastojaće se ukazati na rasprostranjenost ovih krivičnih djela, njihovu društvenu i individualnu opasnost. Na kraju će se istraživanjem na određenom području, odnosno na području Srednjobosanskog kantona SBK/KSB sagledati stanje kriminaliteta sa posebnim aspektom na imovinske delikte, odnosno razbojništva i razbojničke krađe, i indirektno ukazati na mogućnosti kvalitetnije prevencije i aktuelne modele preventivnog djelovanja prema ovim, ali i drugim potencijalnim učiniteljima krivičnih djela. Razlika koja postoji između krivičnog djela razbojništva i krivičnog djela razbojničke krađe je u tome što kod razbojničke krađe pri zatjecanju razbojnika u krađi isti upotrebljava silu i prijetnju da zadrži već oduzetu stvar, dok kod krivičnog djela razbojništva razbojnik upotrebljava silu i prijetnju radi oduzimanja neke stvari.

Ključne riječi: *razbojništvo, razbojnička krađa, kriminalistika, kriminologija, otkrivanje, razjašnjavanje.*

UVOD

Da bi se moglo pristupiti obradi teme ovog rada, neophodno je istražiti temeljne kriminološko – kriminalističke aspekte o nastanku kriminaliteta uopšte, te problematici istog kao i načinu suzbijanja krivičnih djela, a posebno onih koji su predmet ovog rada, odnosno krivičnim djelima imovinskog kriminaliteta, razbojništvima i razbojničkim krađama. Potrebno je u prvom djelu, **uvodu** posebnu pažnju posvetiti metodološkim tematskim jedinicama: 1) problem, predmet i objekt istraživanja, 2) glavna hipoteza i pomoćne hipoteza, 3) svrha i ciljevi istraživanja, 4) naučne metode i 5) struktura rada.

Problem, predmet i objekt istraživanja

Objašnjavanje o osnovnim pojmovima nastanka kriminaliteta uopšte, a samim tim na području srednjobosanskog kantona, a potom otkrivanja i razjašnjavanje svih vrsta krivičnih djela, a posebno ovdje za nas interesantnih razbojništava i razbojničkih krađa, uz pomoć teorijskih i praktičnih doprinosa kriminologije i kriminalistike kao nauka u najkonkretnijim vezama sa uzrocima, fenomenima i tehnologijama otkrivanja i razjašnjavanja kriminaliteta, kao i praktično utemeljenih saznanja i informacija od izuzetnog su značaja za cijelu društvenu zajednicu. Tako postavljen **problem** istraživanja determinira i **predmet** istraživanja: Istražiti i naučno

utemeljeno prezentovati činjenice o problemima i nastanku kriminaliteta na području srednjobosanskog kantona, postojanju krivičnih djela uopšte, a potom posebno krivičnih djela imovinskog kriminaliteta sa posebnim osvrtom na razbojništava i razbojničke krađe. S obzirom na problem i predmet istraživanja, **objekti** istraživanja su kriminalistika (otkrivanje, razjašnjavanje)³⁵ i kriminologija³⁶ u svim svojim sadržajima, a u vezi sa predmetom istraživanja.

Radna i pomoćne hipoteze

U skladu sa problemom, predmetom i objektom istraživanja postavljena je **radna hipoteza**: Istraživanjem osnovnih pojmova o kriminalitetu, a posebno o imovinskom, razbojništvima i razbojničkim krađama, te njihovim uzrocima, moguće je ukazati na probleme ovih krivičnih djela, na području srednjobosanskog kriminaliteta pa i šire, načine izvršenja, mogućnost i načine otkrivanja i razjašnjavanja krivičnih djela značajnih za sigurnost cjelokupne društvene zajednice. Tako postavljena radna hipoteza implicira **pomoćne hipoteze (kraće: P.H.)**:

P.H. 1 : Definisanjem kriminaliteta sa aspekta kriminologije, odnosno objašnjavanjem etiološke dimenzije o nasilničkom – razbojničkom kriminalitetu, te objašnjavanjem kriminoloških teorija moguće je ukazati na mnoštvo faktora o samom nastanku i razvoju kriminaliteta uopšte.

P.H 4 : Uspostavljena interakcija kriminološke i kriminalističke istražne sadržine doprinijeće efikasnijem suzbijanju nasilničkih delikata, a time i razbojništava, što ukazuje na neophodnost naučnog i stručnog pristupa u suzbijanju kriminaliteta uopšte.

Svrha i ciljevi istraživanja

U vezi sa problemom i predmetom istraživanja, te postavljenom radnom i pomoćnim hipotezama, određena je i **svrha istraživanja**: Prezentovati i objasniti pojam, historijski razvoj kriminaliteta, nastanak i pojmove krivičnih djela razbojništava i razbojničkih krađa, te ukazati na njihovu veliku rasprostranjenost i opasnost, kako na kantonu tako i šire. **Cilj istraživanja**: je istražiti relevantne karakteristike, pojmove i elemente krivičnih djela na području srednjobosanskog kantona, sa posebnim osvrtom na razbojništava i razbojničke krađa, odnosno značaj i poteškoće razjašnjavanja i otkrivanja pomenutih krivičnih djela. Primjereno i na jednostavan način teorijski i praktički predstaviti rezultate istraživanja.

³⁵ Kriminalistika je nauka koja se bavi proučavanjem, usavršavanjem i primjenom onih naučnih metoda kao i sredstava koja su najpogodnija za otkrivanje, krivičnih djela, pronalaženje počinitelja krivičnih djela, obezbjeđivanje dokaza, fiksiranje dokaza. Kriminalistika ima također i zadatak sprečavanje učinjenja krivičnih djela. Kriminalistika se dijeli na tri velike grane: kriminalistička taktika, kriminalistička tehnika, kriminalistička metodika.

³⁶ Kriminologija ("Crimen" latinski=zločin "logos" grčki=nauka) uopćeno je sintetička i samostalna nauka koja se bavi izučavanjem kriminaliteta kao društvene pojave, odnosno nauka koja izučava oblike ponašanja koji su inkriminirani i sankcionisani pozitivnim pravom u datom društvu.

Dva osnovna područja ove nauke su kriminalna etiologija, koja se bavi izučavanjem uzroka kriminaliteta i kriminalna fenomenologija, koja proučava pojavne oblike krivičnih djela. Kriminologija se prilikom proučavanja problema kriminaliteta, kao i druge nauke koristi različitim metodama, ali dvije osnovne metode su metod proučavanja individualnih slučajeva i metod proučavanja kriminaliteta kao masovne pojave.

Naučne metode

Prilikom istraživanja koristiće se relevantne naučno istraživačke metode i tehnike, koje mogu dati najkvalitetnije rezultate u oblasti istraživanja kriminogenih pojava. Isto tako treba afirmisati istraživanja u cilju mjerenja kvaliteta i efikasnosti istrage nasilničkih delikata kroz dobijanje validnih rezultata u istražnoj praksi. U tom cilju afirmisaće se standardne, ali i neke specifične metode, primjenljive za oblast istraživanja, kao što su: Kvalitativni pristup, kvalitativna metoda, fokus grupe, analiza scenarija, kompilacija, deskripcija, analiza i sinteza, anketa, intervju, statistička metoda, metoda izučavanja individualnih slučajeva, indicijalna metoda otkrivanja KD-a i metodologija primjene kriminalističkih verzija.

POJAM I KRIMINALNA ETIOLOGIJA

Kriminalitet je posebna društvena i individualna pojava, koja se odvija prema posebnim zakonitostima, a njom se bavi posebna naučno istraživačka disciplina, koju neki nazivaju kriminologija, a u svijetu se upotrebljavaju i druga imena, kao npr. nauka o kriminalitu (*science criminelle*). Veliku ulogu u čovjekovom ponašanju zauzima sredina u kojoj čovjek boravi, odnosno okolina u kojoj se kreće i živi i gdje je sve navedeno međusobno uslovljeno. Opšte je poznato da čovjek živi u “društvu” i razvija se u interakciji sa svojom užom ili širom okolinom, koja utiče na formiranje ličnosti i ponašanje čovjeka uopšte. Ljudska radnja, ponašanje, pa samim tim i krivično djela, rezultat su zajedničkog djelovanja nasljednih, bioloških, konstitucionalnih, psiholoških i društvenih faktora koji se međusobno uslovljavaju.³⁷

Pojam kriminaliteta

Oksfordski riječnik definira kriminalitet kao zbir krivičnih djela po zakonu, tj. Djela, koja su zabranjena zakonom i štetna su ljudima i društvenom blagostanju. Kriminalitet je zlo, oštećenje, prekršaj, grijeh.³⁸ Kriminalitet je negativna društvena pojava vršenja krivičnih djela od strane pojedinaca. Kriminalitet predstavlja pojedinačni akt i društveni fenomen. Postoji veliki broj različitih definicija kriminaliteta i zločina, ali u zavisnosti od njihovog karaktera sve one se mogu sistematizovati u dvije osnovne, a to su: zakonska ili pravna i sociološka definicija. Pojam kriminaliteta podrazumjeva pojavu svih vrsta krivičnih djela na određenom prostoru u određeno vrijeme. Od kada postoji društvo postoji i kriminalitet. Do sada nije poznato nijedno društvo kao ni određeni period bez kriminaliteta. Razvojem društva samo su se mijenjale njegove forme i oblici. U vidu treba imati niz faktora koji utiču na razvoj kriminaliteta uopšte, a to su; kultura, tradicija, ideologija, religija, socijalni, ekonomski i drugi uslovi, geografsko-klimatski faktori, odanost jednog naroda vladavini prava i poštovanju njegovih normi, njegova prosvjećenost, pravni i društveni sistem u jednoj državnoj zajednici i dr.³⁹ Svugdje se od napada štite najvrednija dobra čovjeka i društva kao što je: čovjekov život, tijelo, imovina, bezbjednost države i slično. Razlika se sastoji samo u načinu zaštite tih vrijednosti. Kriminalitet je veliko društveno zlo, odnosno negativna društvena pojava.

³⁷ Opširnije v. Singer M.,: Kriminologija, Globus, Zagreb, 1994., p. 106-108.

³⁸ V. Petrović. B. Meško. G. „Kriminologija“, op.cit.p.14.

³⁹ Marković, I. : op.cit., p. 16.

Pravno definisanje kriminaliteta

Pravna definicija kriminaliteta temelji se na normama materijalnog krivičnog zakonodavstva. Nekada se smatralo da predmet kriminologije i pojam kriminaliteta nije moguće odrediti bez krivičnog prava. Međutim, danas se kriminalitet isključivo tretira kao krivičnopravna kategorija i ograničava na ona protivpravna ponašanja koja su inkrimisana u normama važećeg krivičnog zakonodavstva. Postoje i uža i šira shvatanja pojma kriminaliteta, prema užim shvatanjima kriminalitetom se smatraju samo radnje koje predstavljaju krivična djela određena u zakonodavstvu. Krivičnopravna - definicija zasniva se na principu zakonitosti, koji je uvela klasična krivičnopravna škola (*nullum crimen sine lege*) i omogućava sigurnost u pogledu obima i sadržaja učinjene protivpravne radnje. U krivičnopravnoj literaturi preovlađuje uža pristup, jer se smatra da ukoliko nešto nije krivično djelo, onda nije ni zločin, a to bi značilo da nije ni kriminalitet. "Uže ili restriktivno definisanje kriminaliteta često je zastupljeno u literaturi i njegovi sljedbenici su kategorični u tome da predmet kriminologije ne treba proširivati izvan krivičnog prava. Ovakve definicije kriminaliteta imaju svoj osnov u načelu legaliteta klasične škole prema kojem svako krivično djelo mora biti jasno i precizno određeno (*lex certa*), što isključuje mogućnost arbitriranja u pogledu širine koju zahvata jedno protivpravno ponašanje.

Sociološko definisanje kriminaliteta

Sociološka definicija je u definisanju kriminaliteta šireg pristupa. Ona je sadržajnije i ne posmatra samo djelo, već proučava i učinitelja, društvene uzroke, uslove i posljedice kriminaliteta. Sociološka definicija kriminalitet definiše kao društvene pojave kojima se ugrožavaju osnovne društvene vrijednosti. Kriminološka definicija postavlja vezu između pravnih i socioloških tumačenja. Ovu vezu su popunili kriminolozi i kriminološka shvatanja koja polaze od inkriminiranih djela i društvenih uslova. Sociološka definicija⁴⁰ kriminaliteta koja za razliku od pravne limitirana zakonskim normama na koju se nadovezuju kažnjive radnje, odnosno pravne sankcije ovaj pojam proširuju i na ponašanja koja ne podpadaju pod pojam kriminaliteta. Ovo shvatanje kreće od stava da je kriminalitet društveni fenomen koji obuhvata sva devijantna i asocijalna ponašanja koja predstavljaju odstupanje od društveno prihvatljivi normi ponašanja.

Neposredni sociološki faktori kriminaliteta

Uticaj socioloških faktora na nastanak i razvoj kriminaliteta kao negativne društvene pojave u savremenoj kriminološkoj literaturi je nesporan. Autori, uglavnom, prihvataju tvrdnju koju je još sedamdesetih godina prošlog vijeka u svojim udžbenicima iz kriminologije postavio prof. Milutinović, da "društveno – materijalni uslovi života, ekonomske, klasne i druge osnovne strukture i protivriječnosti, koje se rađaju i razvijaju iz tih uslova, predstavljaju osnovnu snagu koja determiniše pojavu kriminalne djelatnosti u krajnjoj instanci. Međutim, ti krajnji uzroci kriminaliteta ostvaruju se preko neposrednih uzoraka i uslova tj. preko kriminogenih faktora koji stoje, sudeći po karakteru svoga dejstva, u neposrednijem odnosu prema kriminalnoj

⁴⁰ Marković. I.op, cit, p.21

aktivnosti.”⁴¹ U zavisnosti od toga koji su to uzroci možemo konstatovati i zbog čega se pojedine osobe bave određenom vrstom kriminaliteta, odnosno da li će to biti krvni delikti, kriminalitet bijelog okovratnika ili imovinski kriminalitet, tj. Krivična djela protiv imovine. Neposredni sociološki faktori kriminaliteta dijele se na: društveno - ekonomske, političko - idejne, mikrogrupne i socijalno - patološke. U literaturi postoje i drugačije klasifikacije kriminogenih faktora,⁴² ali mi ćemo prihvatiti navedenu podjelu jer je ona dominantna među autorima sa prostora Bosne i Hercegovine.⁴³

IMOVINSKI KRIMINALITET (KRIVIČNA DJELA PROTIV IMOVINE)

Krivična djela protiv imovine (imovinski kriminalitet) veoma su rasprostranjena i u ukupnoj masi kriminaliteta zastupljena su u znatnom postupku – prema nekim procjenama kod nas i u svijetu – čak i preko 50%. Gledajući statistički, prema ukupnom broju prijavljenog i otkrivenog kriminaliteta, imovinski delikti čine ponekad 70% od ukupne mase kriminaliteta, jer su mnogi pojavni oblici ostalih grupacija krivičnih djela prikriveni, neuočljivi, tako da nisu ni otkriveni ni registrirani, za razliku od imovinskih delikata, koji su po pravilu lako uočljivi i odmah poznati, samo što su izvršioc i takvih djela nepoznati.⁴⁴ Stvari koje čine imovinu mogu se, po pravilu, izraziti u novcu. Imovina čini ekonomski osnov svakog društva. Ona služi za zadovoljavanje opštih, zajedničkih i pojedinačnih potreba. Zbog posebnog značaja imovine za čovjeka i društvenu zajednicu u cjelini regulišu se oblici vlasništva, znači sticanja vlasništva nad stvarima i drugih imovinskih prava, kao i način raspolaganja s njim. Otuda neophodnost krivično-pravne zaštite imovine i imovinskih prava i interesa. Krivično-pravna zaštita imovine ne ostvaruje se samo krivičnim djelima iz predhodno navedene glave (poglavlja XXV KZ FBiH), već i nizom drugih krivičnih djela: protiv privrede i jedinstva tržišta, protiv službene dužnosti, protiv opšte sigurnosti ljudi i imovine ili bezbjednosti javnog saobraćaja. Razlika između ovih krivičnih djela je u tome što se kod krivičnih djela protiv imovine, imovina pojavljuje kao osnovni, jedini ili pretežniji objekat zaštite, dok se kod drugih krivičnih djela pojavljuje kao zaštitni objekat zajedno s nekim drugim objektom, pri čemu taj drugi objekt ima primarni značaj. To znači, da krivična djela iz ove glave predstavljaju klasična imovinska krivična djela koja imaju, zajedno s krivičnim djelima protiv života i tijela i političkim krivičnim djelima, najdužu istoriju. Mijenjali su se načini i sredstva izvršenja djela i pojavni oblici, ali je njihova suština ostala ista. Imovina kao zaštitni objekt kod većeg broja krivičnih djela iz ove glave pojavljuje se u vidu pokretne stvari. Pokretna stvar je objekt napada kod krađe, razbojništva, utaje i oduzimanja tuđe stvari. Osnovni motiv izvršenja većeg broja krivičnih djela protiv imovine je pribavljanje imovinske koristi za sebe ili nekog drugog. Krivična djela protiv imovine su dosta heterogena po neposrednom predmetu napada i vrijednosnom iznosu štete.⁴⁵

⁴¹ Milutinović M.: , op. cit. p. 321.

⁴² Tako npr. Ignjatović. Đ. i . Bošković. M, vrše podjelu na spoljne ili ambijentalne i unutrašnje ili individualne faktore, te u okviru spoljnih faktora obrađuju i problematiku neposrednih socijalnih faktora. Međutim, kada je u pitanju određivanje pojedinačnih socijalnih faktora, tu nema veće razlike među autorima.

⁴³ U tom smislu podjelu vrši Mladenović - Kupčević R. , a u novijoj literaturi tu klasifikaciju nalazimo u udžbeniku katora B. Petrović i G. Meško.

⁴⁴ V. Korajlić. N., „Kriminalistička metodika“, Fakultet kriminalističkih nauka Sarajevo, 2008.godine. p. 299.

⁴⁵ V. Korajlić. N., op. cit. p. 300-301.

RAZBOJNIŠTVA I RAZBOJNIČKE KRAĐE, POJAM, OTKRIVANJE, RAZJAŠNJAVANJE

Pojam i krivično pravno određenje

Razbojništvo⁴⁶ je složeno krivično djelo: u njemu je uvijek sadržan element nasilja i element oduzimanja tuđe pokretne stvari (novca, nakita i drugih pokretnih stvari). Element nasilja javlja se kao sredstvo izvršenja djela – razbojnik primjenjuje silu ili prijetnju da će neposredno napasti na život i tijelo žrtve u namjeri da na taj način od nje oduzme stvari koje želi prisvojiti. Razbojništvo spada u najteže imovinske delikte, jer razbojnik ne preza da žrtvu rani ili čak liši života.⁴⁷ Veoma opasan i razbojništvu srodan imovinski delikt jeste razbojnička krađa.⁴⁸ Razlika je između razbojničke krađe i razbojništva, u tome što izvršilac razbojničke krađe pri zatjecanju na krađi upotrebljava silu ili prijetnju u namjeri da zadrži već ukradenu stvar, a izvršilac razbojništva upotrebljava silu ili prijetnju radi oduzimanja (otimanja) stvari. Prema tome, u razbojništvu sila ili prijetnja prethodi protupravnom oduzimanju, a u razbojničkoj krađi sila ili prijetnja dolazi poslije protupravnog oduzimanja stvari. U suštini razbojništvo je brutalni akt nasilja iz koristoljublja. Zbog toga razbojništvo predstavlja najteža krivična djela protiv imovine. Prema načinu izvršenja, objektu napada, broju učesnika, mjestu izvršenja i drugima elementima razbojništva se mogu podijeliti na nekoliko karakterističnih grupacija, što treba imati na umu pri operativno – preventivnom postavljanju i provođenju operativne kontrole.⁴⁹

Otkrivanje i razjašnjavanje

Pojam „otkrivanja“ otkrivanje kaznenih djela i njihovih učinitelja je svojevrsni stvaralački heuristički proces, izrazito dinamičke prirode, koji proizilazi kroz više razina. Ta dinamička djelatnost se sastoji u pronalaženju i prikupljanju latentnih i potencijonalnih informacija o kaznenom djelu i njegovom učinitelju i svim pratećim okolnostima djela njihovom kriminalističkom interpretiranju u vidu svojevrsnog „dešifriranja“ (dekodiranja). Ova djelatnost okarakterizirana je primjenom algoritma kriminalističke znanosti, osobno u sferi interpretiranja informacija. Po prirodi stvari, otkrivanje kaznenih djela je primarno u integraciji policije. Pojam otkrivanje primarno se odnosi na postupke kojima se zahvaća u tzv. „tamni pojas“ kriminaliteta, bilo da se radi o otkrivanju još neotkrivenih kaznenih djela ili nepoznatih učinitelja poznatih kaznenih djela. Kada je riječ o tzv. „svjetlom pojasu“ kriminaliteta, tada kriminalni slučaj treba samo razjašnjavati, a iznimno u postupku razjašnjavanja neke činjenice i okolnosti i otkrivati. Riječ je o heurističkoj djelatnosti čiji je cilj, pretvaranje nekog oblika sumnji niže kategorije u „osnovanu sumnju“. Ukoliko „osnovana sumnja“ postoji od samog početka, tad u pravilu nema potrebe za postupkom otkrivanja, nego kriminalnog razjašnjavanja slučaja. Riječ je specifičnom retrospektivnom procesu.⁵⁰ U kriminalističkoj teoriji su razrađene tri metode za

⁴⁶ Čl. 289. KZ FBiH, čl. 283. KZ BDBiH I čl. 233. KZ RS. V. Petrović. B., Jovašević. D. op. cit. p. 252.

⁴⁷ V. Korajlić. N. op. cit. p. 355.

⁴⁸ Čl. 288. KZ FBiH, čl. 282. KZ BDBiH I čl. 234. KZ RS. V. Petrović. B., Jovašević. D. op. cit. p. 250.

⁴⁹ Ib.

⁵⁰ Modly. D. op. cit. p. 47.

otkrivanje nepoznatih učinilaca na osnovu **indicija**⁵¹: 1) metoda eliminacije ili isključivanja, određenih osumnjičenih sužavanjem kruga osumnjičenih lica, pri otkrivanju učinioaca određenog krivičnog djela; 2) metoda otkrivanja nepoznatog učinioaca po načinu izvršenja u slučajevima ponavljanja krivičnih djela (korišćenje MOS metode) i 3) metoda sastavljanja lista indicija za više krivičnih djela i osumnjičenih lica kako bi se pronašao stvarni izvršilac.

EMPIRIJSKO ISTRAŽIVANJE NA PODRUČJU SREDJOBOSANSKOG KANTONA U PERIODU OD 2007 - 2011 GODINE (analiza kriminaliteta sa posebnim osvrtom na razbojništva)

U CILJU PROVJERAVANJA I ANAIZIRANJA TEORIJSKIH SADRŽAJA. U OKVIRU IZRADE NAUČNOG RADA, IZVREŠNO JE EMPIRIJSKO ISTRAŽIVANJE PO PREDMETNOJ TEMI, PROBLEMATICI

Empirija potječe od grčke riječi „*empeiria*“, a znači iskustvo, znanje, dok pridjev empirijski ima značenje: iskustven, iskustvenog porijekla, koji se osniva samo na iskustvu. U filozofiji empirizam je spoznajno teorijsko stajalište koje drži da je iskustvo temeljni izvor sveukupne spoznaje. Iskustvo je znanje stečeno praksom i izravnim doživljavanjem, poznavanje stvari, pojava, vještina, umješnosti, ono je naučeno životnom praksom, to je znanje stečeno ljudskim radom(...).⁵² Empirijska istraživanja nisu jednosmislen pojam jer se pod tim pojmom najčešće razumjeva.⁵³ primjena iskustva u spoznavanju istine i primjena istraživanja u rješavanju praktičnih problema. U empirijskim se istraživanjima ne primjenjuju znanstvene metode, jer se sudovi donose na osnovi iskustava. Međutim, primjena takvih istraživanja u rješavanju praktičnih problema ima karakteristike znanstvenog istraživanja. Takvo stajalište ne negira i ne umanjuje važnost empirijske metode.⁵⁴

Ukupno stanje kriminaliteta za pet (5) godina na području MUP-a Srednjobosanskog Kantona, pregled 2007 – 2011.godina

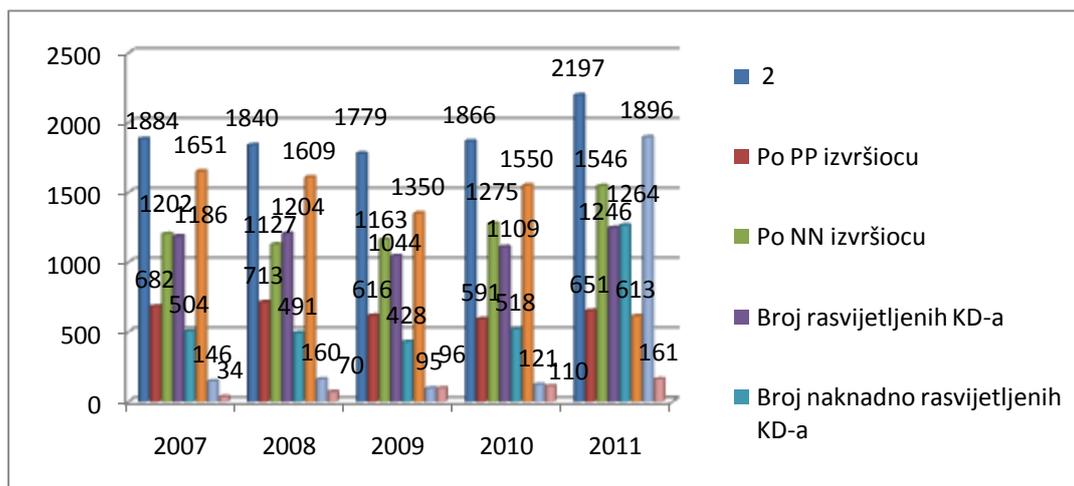
Pregledom ukupnog stanja kriminaliteta na određenom području, u ovom slučaju na području MUP-a Srednjobosanskog Kantona, pokušat će se pregledom statističkih podataka u pet godina ukazati na problematiku kriminaliteta uopšte, a naročito na problematiku teških krivičnih djela razbojništava i razbojničkih krađa. Budući da na navedenom području nisu rađena naučna istraživanja o navedenoj temi i problematici, mi će mo se u ovom slučaju osloniti na statističke podatke Ministarstva Unutrašnjih poslova. U grafikonu koji slijedi, dat je prikaz ukupnog broja krivičnih djela na području srednje Bosne za svaku godinu pojedinačno.

⁵¹ Ove metode je prvi u svijetu prikazao Vajngart u knjizi: kriminalistička taktika, Beograd, 1905, p. 106-112. U domaćoj kriminalističkoj literaturi tim pitanjem bavio se Vladimir Vodinić, Kriminalistika, Kragujevac, 2004. p. 310. Uporedi sa Simonović, B., Kriminalistika, Kragujevac, 2004. Str. 83-89.

⁵² Cf. ANIĆ, V.: Natuknica iskustvo, riječnik hrvatskog jezika, Novi Liber, Zagreb, 1991., p. 212. R. Zelenika.: metodologija i tehnologija izrade znanstvenog i stručnog djela, četvrto izdanje. Ekonomski fakultet u Rijeci, Rijeka, 2000.god, p. 113.

⁵³ Cf. BABAN, LJ. Et al.: primjena metodologije znanstvenog istraživanja, Ekonomski Fakultet Sveučilište Josipa Jurija Strossmayera u Osijeku, Osijek, 1993., p. 7. R. Zelenika.: op. cit. p. 113.

⁵⁴ O tome cf.: infra točku 4.23. empirijska metoda. R. Zelenika.: op. cit. p. 113.



Prethodni grafikon oslikava ukupno stanje kriminaliteta za svaku godinu pojednačno. Kao što se može vidjeti, stanje kriminaliteta, kao i rasvijetljenost krivičnih djela, odnosno broj prijavljenih i pritvorenih lica varira iz godine u godinu. Najveći broj krivičnih djela, kao što se može i vidjeti iz predhodnog grafikona učinjen je u 2011 godini, što nam na jedan način oslikava realno stanje, odnosno povećanje kriminaliteta iz godine u godinu.

Stanje imovinskih delikata u periodu od 2007 – 2011. Godine

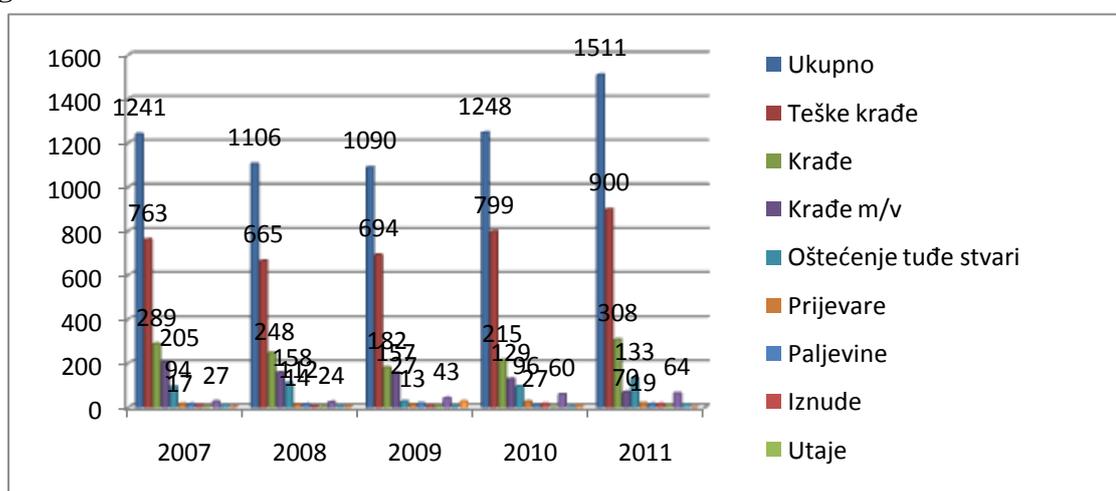
Krivična djela protiv imovine (imovinski kriminalitet) veoma su rasprostranjena i u ukupnoj masi kriminaliteta zastupljena su u znatnom postupku – prema nekim procjenama kod nas i u svijetu – čak i preko 50%. Gledajući statistički, prema ukupnom broju prijavljenog i otkrivenog kriminaliteta, imovinski delikti čine ponekad 70% od ukupne mase kriminaliteta, jer su mnogi pojavni oblici ostalih grupacija krivičnih djela prikriveni, neuočljivi, tako da nisu ni otkriveni ni registrirani, za razliku od imovinskih delikata, koji su po pravilu lako uočljivi i odmah poznati, samo što su izvršiocu takvih djela nepoznati.⁵⁵ Inkriminacijama iz glave zakona **imovinski kriminalitet (krivična djela protiv imovine, poglavlje XXV KZ FBiH, ČLAN. 286-302)**⁵⁶ štiti se imovina koja se sastoji od stvari (predmeta) i imovinskih prava i interesa vezanih za stvari. Imovina podrazumjeva vlasništvo, tj. oblik prisvajanja stvari i vrijednosti u kojima i preko kojih se one izražavaju. Imovina može biti pokretna i nepokretna. Imovina je oduvijek bila predmetom zaštite. U uslovima neorganiziranog društva tu suzaštitu osiguravali su pripadnici zajednice sami, a sa nastankom i razvojem organiziranih ljudskih društava tu je ulogu preuzimao kolektiv. Dakako da su se sa razvojem društva mijenjali i oblici protuzakonitih ponašanja protiv imovine, tako da danas značajan segment imovinskog kriminaliteta čine krađe motornih vozila, kojim se u statistikama organa formalne socijalne kontrole posvećuje posebna pozornost. Neka bitna opšta obilježja imovinskog kriminaliteta danas su: masovnost (u ukupnom kriminalitetu imovinski sudjeluje u velikom procentu); recidivizam i profesionalizam (ni kod jedne druge vrste kriminaliteta su specijalizacija i povrat toliko prezentni kao kod imovinskog); organiziranost (vrlo često- ipak ne u pravilu- su počinitelji krivičnih djela imovinskog

⁵⁵ V. Korajlić. N prikrivanje.op, cit. p. 299.

⁵⁶ XXV KZ FBiH, člutažaan. 286-302, poglavlje.

kriminaliteta organizirani u slabije ili čvršće vezane zločinačke skupine); i, velika tamna brojka (počinjena, a neopažena ili neprijavljena krivična djela). Sem toga, oblast maloljetničke delinkvencije koja najčešće vodi u tzv. kriminalne karijere (zbog visokog stepena povratništva) u najvećem broju slučajeva utilitaristički je motivirana i usmjerena protiv imovine (Singer, 1994).⁵⁷ Učešće imovinskog kriminaliteta u ukupno registriranom kriminalitetu je izuzetno visoko, i zapravo predstavlja osnovu svakodnevnog istražiteljskog rada policije. Na području Srednjobosanskog kantona (kantona Središnja Bosna 2007- 2011 godina, imovinski kriminalitet je u prosjeku činio većinu registriranog kriminaliteta. U strukturi prijavljenih krivičnih djela dominiraju krivična djela teške krađe, krađe, razbojništva, oštećenja tuđe stvari, itd. Objekti napada pri vršenju krivičnih djela protiv imovine najčešće su bili automobili, zatim stambeni objekti, te prodavnice i poslovni objekti, pri čemu su otuđivana motorna vozila, novac, zlatni nakit, tehnička roba, cigarete, auto-dijelovi, itd.

Pregled značajnijih krivičnih djela protiv imovine u periodu 2007 – 2011 godine.



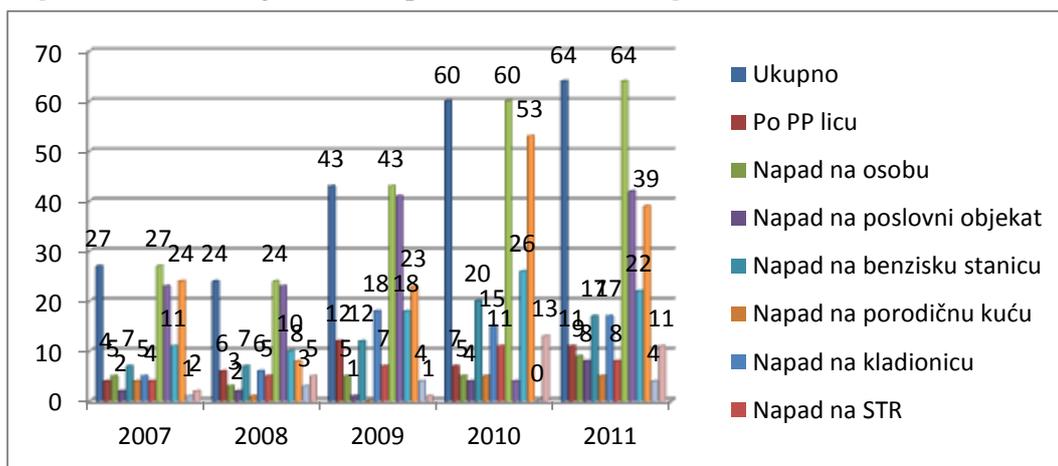
Za 2007 godinu počinjeno je 1241 krivično djela imovinskih delikta. Imovinski delikti su najzastupljeni u ukupnoj strukturi krivičnih djela sa visokih 66%. Broj krivičnih djela protiv imovine veći je za 5 ili 1%, u odnosu na 2006 godinu. Najviše evidentiranih krivičnih djela po nepoznatom počiniocu sa 1080 ili 90%. Od ukupnog broja krivičnih djela po NN izvršiocu, rasvijetljeno je 416 ili 39 %. Prijavljeno je 907 lica, od 117 maloljetnika i 394 povratnika. Za 2008 godinu registrovano je 1106 imovinskih delikata, što čini 60%, u ukupnoj strukturi krivičnih djela. U odnosu na 2007 godinu, broj krivičnih djela protiv imovine manji je za 135 ili 11%. Evidentirano je 969 krivičnih djela po nepoznatom počiniocu, a rasvijetljeno je 381 i iz ranijeg perioda 28. Prijavljeno je 819 lica, od toga 135 maloljetnika i 392 povratnika. Za 2009 godinu ukupno je registrovano 1090 imovinskih delikata, što čini 61% u ukupnoj strukturi krivičnih djela. U odnosu na 2008 godinu, broj krivičnih djela protiv imovine manji je za 16 ili 1%. Evidentirano je 969 krivičnih djela po nepoznatom počiniocu, a rasvijetljeno je 312 i iz ranijeg perioda- 22. Prijavljena su 653 lica, od toga 74 maloljetnika, i 339 povratnika. U 2010 godini ukupno je registrovano 1248 imovinskih delikata, što čini 67% u ukupnoj strukturi

⁵⁷ Udruženje Centar za Novi grad Sarajevo, 2011.godina.

krivičnih djela. U odnosu na prethodnu godinu, broj krivičnih djela protiv imovine veći je za 158 ili 14%. Evidentirana su 1123 krivična djela po nepoznatom počiniocu, a rasvijetljena su 424 iz ranijeg perioda- 23. Prijavljeno je 890 lica, od toga 93 maloljetnika i 471 povratnik. Dominiraju teške krađe sa 64% zastupljenosti u imovinskim deliktima. U odnosu na prethodni godinu teške krađe su povećane za 105 ili 15%. U 2011 godini ukupno je registrovano 1517 imovinskih delikata, što čini 69% u ukupnoj strukturi krivičnih djela. U odnosu na 2010 godinu, broj krivičnih djela protiv imovine veći je za 269 ili 22%.

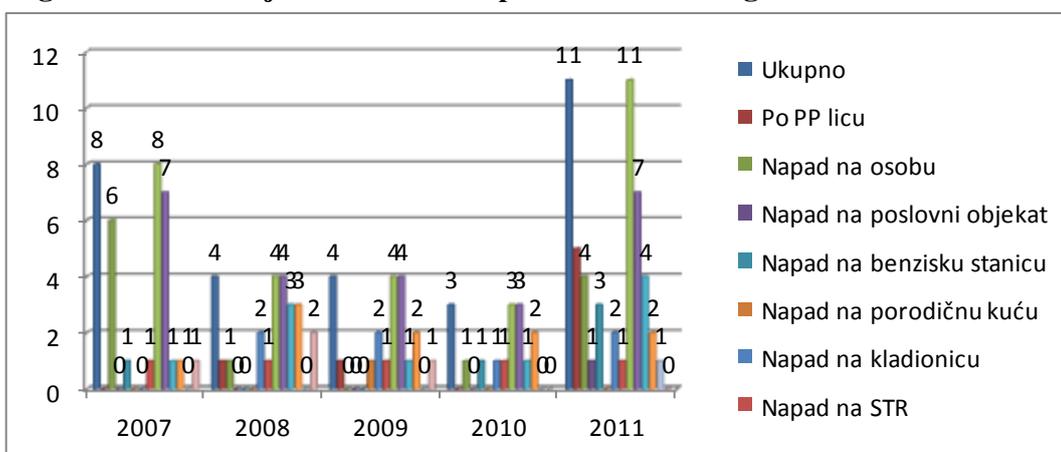
Stanje razbojništava i razbojničkih krađa u periodu 2007 - 2011 godine.

Pregled KD-a razbojništava u periodu 2007-2011 godine



Iz predhofnog grafikona uočljivo je da je ukupan broj krivičnih djela razbojništava krađa povećavan iz godine u godinu. Aa da je najviše napada na osobu, zatim napadi na porodičnu kuću, napadi na poslovni objekat i sl. Najveći broj ovih krivičnih djela je po nepoznatom izvršiocu odnosno po NN licu. Veći broj ovih krivičnih djela ostao je nerazjašnjen, manji broj lica je prijavljen, među kojima se česti bili maloljetnici, a naročito povratnici (recidivisti) u činenju krivičnih djela.

Pregled KD-a razbojničkih krađa za period 2007-2011 godine



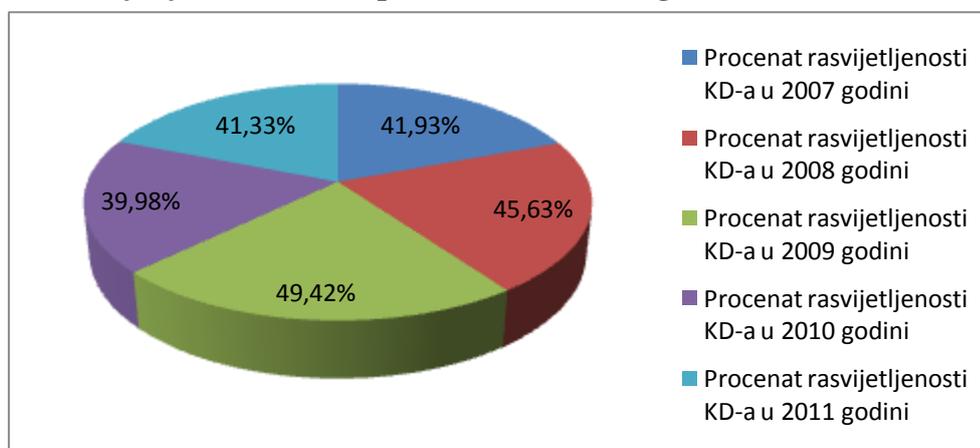
Prethodni grafikoni pokazuju nam stanje razbojništava i razbojničkih krađa u periodu od 2007 godine pa do 2011 godine. Iz pomenutih grafikona vidljivo je da je mnogo

veći procenat razbojništava u odnosu na razbojničke krađe. Najveći broj ovih krivičnih djela je po nepoznatom izvršiocu odnosno po NN licu. Najčešće objekti napada bili su benzinske stanice, poslovni objekti, trgovački centri, osobe is sl.. najčešći period napada uglavnom je od sedamnaest do dvanaest sati iza ponoći. Veći broj ovih krivičnih djela ostao je nerazjašnjen, manji broj lica je prijavljen, među kojima se česti bili maloljetnici, a naročito povratnici (recidivisti) u činenju krivičnih djela. Razloge, zbog čega je najveći broj ovih krivičnih djela upravo po nepoznatom počiniocu, odnosno NN licu, možemo tražiti pored ostalog u specifičnosti, samog vremena izvršnja ovih krivičnih djela. Naime najveći broj ovih krivičnih djela dešava se u noćnim satima, odnosno u periodu pred zatvaranje obilakata, kada je riječ o poslovnim objektima. Međutim kada je riječ o porodičnim kućama, najveći broj ovih krivičnih djela izvršen je u periodu kada nema nikoga kod kuće. Pored navedenih konstatacija, takođe jedan od razloga, zašto je ovaj broj krivičnih djela najveći po NN je i taj što, u slučaju samog krivičnog djela žrtva bude u stanju šoka i straha, te tako veoma rijetko može pomoći policiji prilikom identifikacije samog počinioca.

Procenti rasvijetljenosti krivičnih djela, NN, otkriveni i sl..

U 2007 godini registrovana su 1202 krivična djela po nepoznatom počiniocu, rasvijetljena su 504 ili 42% krivičnih djela, što je u odnosu na 2006 godinu nešto manji broj i procenat rasvijetljenih, kada je rasvijetljenost iznosila 548 ili 45%. Ukupna rasvijetljenost krivičnih djela iznosila je 1186 ili 63%.

Procenat rasvijetljenosti KD-a u periodu 2007- 2011 godine



Ukupan broj rasvijetljenih krivičnih djela imovinskih delikata čini 416 ili 83% ukupne rasvijetljenosti. Otkriveno je 208 teških krađa, zatim 136 krađa, 40 oštećenja tuđe stvari, 12 krađa motornih vozila, 11 razbojništava itd. U 2007 godini ukupno je registrovano 1127 krivičnih djela po nepoznatom počiniocu. Naknadnim radom rasvijetljeno je 491 ili 41,93% djela, što je nešto lošiji procenat rasvijetljenosti u odnosu na pedhodnu godinu, kada je rasvijetljenost iznosila 504 ili 42%. Rasvijetljeno je i 28 krivičnih djela iz ranijeg perioda, što znači da je rasvijetljeno 519 ili 46%. Ukupna riješenost krivičnih djela iznosi 1204 ili 65%. U 2008 godini registrovana su 1100 krivična djela po nepoznatom počiniocu, rasvijetljena su 402 ili 41% krivičnih djela, što je u odnosu na 2007 godinu nešto manji broj i procenat rasvijetljenih, kada je rasvijetljenost iznosila 504 ili 42%. Ukupna rasvijetljenost

krivičnih djela iznosila je 1186 ili 63%. Ukupan broj rasvijetljenih krivičnih djela imovinskih delikta čini 312 ili 79% ukupne rasvijetljenosti. Otkriveno je 190 teških krađa, zatim 100 krađa, 55 oštećenja tuđe stvari, 15 krađa motornih vozila, 10 razbojništava itd. U 2008 godini ukupno je registrovano 952 krivična djela po nepoznatom počiniocu. Naknadnim radom rasvijetljeno je 488 ili 52% djela, što je nešto bolji procenat rasvijetljenosti u odnosu na pedhodnu godinu, kada je rasvijetljenost iznosila 504 ili 42%. Rasvijetljeno je i 27 krivičnih djela iz ranijeg perioda, što znači da je rasvijetljeno 515 ili 46%. U 2009 godini ukupno je registrovano 1163 krivična djela po nepozntom NN počiniocu. Naknadnim radom rasvijetljeno je 428 ili 37% krivičnih djela, što je slabiji procenat rasvijetljenosti u odnosu na prošlu godinu, kada je rasvijetljenost iznosila 491 ili 44%. Rasvijetljeno je i 25 krivičnih djela iz ranijih godina, što znači da je rasvijetljeno 453 ili 39%. Ukupna riješenost krivičnih djela iznosi 1044 ili 59%. Najviše rasvijetljenih krivičnih djela protiv imovine 312 i iz ranijeg perioda- 22, od toga 192 teške krađe, 80 krađa, 20 razbojništava itd. U 2010 godini ukupno je registrovano 1275 krivičnih djela po NN počiniocu. Naknadnim radom rasvijetljeno je 518 ili 41% krivičnih djela, što je veći procenat rasvijetljenosti u odnosu na prošlu godinu, kada je rasvijetljenost iznosila 428 ili 37%. Ukupna riješenost krivičnih djela iznosi 1109 ili 59%. Rasvijetljeno je i 29 krivičnih djela iz ranijeg perioda, što znači da je rasvijetljeno 547 ili 43%. U 2011 godini ukupno je registrovano 1546 krivičnih djela po NN počiniocu. Naknadnim radom rasvijetljeno je 613 ili 40%, što je manje za 1% u odnosu na prošlu godinu, kada je rasvijetljenost iznosila 518 ili 41%. Ukupna riješenost krivičnih djela iznosi 1264 ili 58%. Rasvijetljeno je i 59 krivičnih djela iz ranijeg perioda. Izdvajamo da su rasvijetljena sljedeća krivična djela: 516 krivičnih djela protiv imovine i 54 krivična djela iz ranijeg period.

ZAKLJUČAK

Nakon provedenog istraživanja na temu „Problematika kriminaliteta na području srednjobosanskog kantona sa posebnim osvrtom na razbojništva i razbojničke krađe“, i prezentiranja teme kroz pet cjelina, neophodno je izložiti i rezimirati ostvarene rezultate sveukupnog istraživanja. U tom kontekstu posebno će se istaći ključni stavovi i mišljenja u vezi sa definisanim hipotezama. Definisanje kriminaliteta sa aspekta kriminologije kao nauke koja izučava pojave kriminaliteta i njihove uzroke, odnosno objašnjavanjem etiološke dimenzije o nasilničkom – razbojničkom kriminalitetu, o kriminalitetu uopšte, te objašnjavanjem teorija koje ukazuju na mnoštvo faktora o njegovom nastanku i razvoju uopšte, a posebno o nastanku i razvoju krivičnih djela imovinskog kriminaliteta, je početno pitanje na koje se u radu nastojao dati naučno utemeljen odgovor, skladno raspoloživoj domaćoj i inostranoj literaturi. U okviru šireg definisanja i analiziranja kriminaliteta, a posebno nasilničkog, u radu je dat prikaz i krivično prvnog aspekta ove oblasti kriminaliteta, u potrebnom obimu bez detaljnijeg izučavanja krivično pravnog obilježja, s obzirom da to nije centralno pitanje rada. Izučavajući kriminološke karakteristike kriminaliteta, posebno u svijetlu etiologije (uzroka, uslova i povoda) kriminaliteta, data je optimalna dimenzija shvatanja u okviru teorije i prakse kriminološkog učenja, u funkciji otkrivanja i razjašnjavanja krivičnih djela imovinskog – nasilničkog kriminaliteta. Iz ovog se izvodi nedvosmislen zaključak da pomoću kriminologije kao nauke o etiologiji i fenomenologiji kriminaliteta (uzroci i karakteristike), je moguće objasniti pojam i razvoj kriminaliteta, nastanka i pojave razbojničkih delikata. Ova tvrdnja je posebno značajna zbog potrebe aktualiziranja nedovoljno

afirmisanih shvatanja, i konkretnog dokazivanja da se pomoću kriminološkog učenja o delinkventnoj ličnosti, može uspješnije doprinijeti otkrivanju i razjašnjavanju ovih, a i svih ostalih oblika imovinskog kriminaliteta. Centralno pitanje u radu je da se kroz teorijsko empirijsko istraživanje funkcionalno uvežu kriminološko kriminalistička znanja i učenja o nasilničkom kriminalitetu, u cilju unapređenja kriminalističko istražnih tehnologija otkrivanja, razjašnjavanja i dokazivanja krivičnih djela i učinilaca. Rukovodeći se tim zahtjevom u radu se nastojao dati odgovor u smislu potvrda ili negiranja takve potrebe i shvatanja. U radu se ravnopravno tretira doprinos i značaj, kako kriminologije, tako i kriminalistike kao nauke o metodama otkrivanja, razjašnjavanja krivičnog djela i učinioca. Uspostavljenije svojevrstne interakcije između kriminološke i kriminalističke istražne sadržine, sigurno mnogo doprinosi efikasnijem suzbijanju nasilničkih delikata, a time i razbojništava, što ukazuje na neophodnost naučnog i stručnog pristupa u suzbijanju kriminaliteta uopšte. U okviru realizovanog empirijskog istraživanja nedosmisleno se pokazalo shvatanje o potrebi posjedovanja kriminološko - kriminalističkog znanja o kriminogenosti u ličnosti potencijalnog – stvarnog učinioca. U tom kontekstu, posebno je potrebno istaći shvatanje praktičara – kriminalista da je kriminalistička istraga nepotpuna, nefikasna bez primjene kvalitetno pripremljenih metoda i sredstava kriminologije i kriminalistike u svakoj, kao i u predmetnoj oblasti (imovinski kriminalitet). Rezultati empirijskog istraživanja takođe ukazuju na potrebu stalnog unapređenja kriminalističko istražne prakse, koja se ne smije pretvoriti u puki praktikizam. Naprotiv stalnim inoviranjem istražnih metoda i sredstava, njihovom primjenom i potvrđivanjem u praksi, na konkretan način se dokazuje neophodnost stručnog i naučnog unapređenja kriminološko kriminalističkih metoda otkrivanja i razjašnjavanja krivičnih djela i učinilaca, što doprinosi efikasnijem suzbijanju kriminaliteta. Koliko će policijski službenici - kriminalistički istražitelji, biti efikasni prilikom otkrivanja, razjašnjavanja razbojništava – razbojničkih krađa zavisi u svakom slučaju od poštivanja i primjene pravila kriminalističko – kriminološke nauke. Zbog toga je potrebno posebno naglasiti i istaći neophodnost stvaranja neospornog integriteta kriminaliste – koji u svome stručnom obrazovanju izučava, a u praksi verifikuje stečena učenja i znanja. Problematika kriminaliteta bilo koje vrste ista je svugdje u svijetu, pa i u Bosni i Hercegovini, a samim tim i u srednjobosanskom kantonu, kao i svakom drugom. Razlike nema, kriminalitet je jednako opasan štetan za sve građane Bosne i Hercegovine, i u svakom slučaju predstavlja problem jednake prirode svima...

LITERATURA

1) Knjige

1. Ignjatović. Đ. „Kriminološko naslijeđe“, Beograd, 1997. god.
2. Korajlić. N, „Kriminalistička metodika“, Fakultet kriminalističkih nauka Sarajevo, 2008.god.
3. Marković. I, „Osnovi kriminologije“, Banja Luka, 2007.god.
4. Milutinović. M. „Kriminologija IV dopunjeno izdanje, Beograd 1981. god.
5. Mladenović – Kupčević. R. „Kriminologija“, Sarajevo 1977. god
6. Mladenović-Kupčević. R, „Kriminologija“, Fakultet kriminalističkih nauka, Sarajevo 1997.god.
7. Modly. D, Petrović. B, Korajlić. N, „Uvod u kriminalistiku“, Fakultet Kriminalističkih Nauka, Sarajevo, 2004.god.

8. Modly. D, Korajlić. N, „Kriminalistički riječnik“, Centar za kulturu i obrazovanje, Tešanj, 2002.god.
9. Modly. D, Šuperina. M, Korajlić. N, „Riječnik Kriminalistike“, Zagreb, 2008.god.
10. Modly. D, „Metodika istraživanja razbojništava“, Fakultet Kriminalističkih Nauka, Sarajevo, 1999.god.
11. Modly. D, „Kriminalistička metodika“, Fakultet Kriminalističkih Nauka, Sarajevo, 1998.god.
12. Petrović. B, Gorzad. M, „Kriminologija“, Pravni fakultet Sarajevo, 2004.god.
13. Petrović. B, Gorzad. M, „Kriminologija“, Pravni fakultet Sarajevo, 2008.god.
14. Petrović. B, Jovašević. D, „Krivično pravo I, opšti dio“, Pravni fakultet Sarajevo, 2005.god.
15. Petrović. B, Jovašević. D, „Krivično pravo II, posebni dio“, Pravni fakultet Sarajevo, 2005.god.
16. Simonović. B. „Kriminalistika“, Pravni fakultet u Kragujevcu 2004. god.
17. Singer. M, „Kriminologija“, Globus, Zagreb, 1994.god.
18. Vodinelić. V. „Kriminalistika V izdanje“, Beograd 1984. god.
19. Vodinelić. V, „Kriminalistika“, Beograd, 1996.god.
20. Vodinelić V, Kriminalistika, otkrivanje, dokazivanje, Tom 1,2, Fakultet bezbednosti i DSZ, Skopje, 1985. god.
21. Zelenika. R. „Metodologija i tehnologija izrade znanstvenog i stručnog djela“, Rijeka, 2000. god.

Članci referati studije i rasprave

Osatali izvori

1. Komentar krivičnih zakona SR Srbije, SAP Kosova i SAP Vojvodine, 1986., Beograd;, Savremena administracija Beograd.
2. Službeni glasnik BiH br 3/07.
3. Udruženje Centar za Novi grad Sarajevo, 2011.godina.
4. Zakonski tekstovi važećih krivičnih zakona u BiH (KZ BiH, KZ FBiH, KZ RSBiH, KZBDBiH).
5. XXV FBiH čl. 286-302. KZ FBiH čl. 287, 288, 289, KZ RS-a 233, 234, KZ BD-a .

POVEZANOST POTROŠNJE ENERGIJE I EKONOMSKOG RASTA SA POSEBNIM OSVRTOM NA BIH

mr. Mirza Kulenović, dipl. ecc,

Visoka škola „CEPS-Centar za poslovne studije“ Kiseljak
mirza.visokaskola@gmail.com

SAŽETAK

Posljedice prvog i drugog naftnog šoka plasiraju energiju, te energetske sektor kao jedan od najznačajnijih sektora svake ekonomije, pri čemu ekonomisti posebnu pažnju posvećuju povezanost potrošnje energije i ekonomskog rasta zemlje. U zavisnosti od uzročnosti ove dvije varijable zemlje mogu planirati svoju strategiju vezanu za potrošnju energije. U radu se prvo pristupa analizi makroekonomskih efekata energetske sektora, te detaljnoj razradi najznačajnijih. Iako postoji dosta rasprava da li energetske sektor utiče na GDP, detaljnom analizom OECD i ne-OECD zemalja, zemalja Balkana, Republike Hrvatske, te Bosne i Hercegovine, dolazimo do zaključka da potrošnja energije utiče na GDP, naravno, različito na svaku od zemalja. Korištenjem jednostavne korelacije između varijabli od interesa izvršena je analiza povezanosti potrošnje električne energije i GDP-a u Bosni i Hercegovini.

Ključne riječi: ekonomija energetske sektora; makroekonomski efekti energetske sektora; povezanost potrošnje energije i GDP-a; energetske sektor Bosne i Hercegovine;

UVOD

Energija, te energetske sektor jedan je od najvažnijih sektora svake ekonomije. Energiji, kao jednom od ključnih faktora razvoja nije se posvećivalo mnogo pažnje, no nakon naftnih šokova⁵⁸ ekonomisti sve više pažnje posvećuju ovome faktoru i njegovom uticaju na cijelu ekonomiju. Danas energija ima jako važnu ulogu u ekonomiji svake države, te svake godine se povećava broj radova na ovu temu. Najviše pažnje se posvećuje analiziranju uzročnosti između potrošnje energije i GDP-a, što je jako važno za buduće politike svake zemlje. Kao što će biti rečeno u nastavku rada, ukoliko uzročnost se kreće od potrošnje energije ka dohotku, to dokazuje da je zemlja energetske zavisna i da stoga energija je stimulant razvoju zemlje, što u slučaju manjka resursa, zemlju može dovesti u jako nezahvalnu situaciju. Ukoliko se pokaže da uzročnost ide od dohotka ka potrošnji energije, to znači da je zemlja energetske nezavisna, te energetske politike mogu biti implementirane bez učinka na razvoj i zaposlenost.

⁵⁸ "Prvi naftni šok se desio 1973/74. godine - približno četverostruko povećanje cijena nafte izazvan je bojkotom - dakle, političkom redukcijom ponude. Drugi naftni šok, 1979/80., uz otprilike dvostruko povećanje cijena, pratio je redukciju ponude koja je bila izazvana iranskom revolucijom, tj. ponovno političkim događanjem." (Benac, Slosar i Žuvić, 2008, str. 72)

Makroekonomski efekti energetskega sektora

Energetski sektor je izuzetno važan iz više razloga. Ključna uloga energetskega sektora u ekonomskim aktivnostima ogleda se u međusobnoj ovisnosti između ekonomskih djelatnosti i energije. Na primjer, energetski sektor koristi inpute iz raznih drugih sektora (industrija, promet, domaćinstva, itd.), a također je ključni input za većinu sektora. Ovi međusobni odnosi utiču na tražnju za energijom, mogućnosti zamjene unutar energije i drugih resursa (kapital, zemlja, rad i materijal), opskrba energijom i drugim robama i uslugama, investicijske odluke i makroekonomske varijable zemlje (ekonomski output, vanjska trgovina, inflacija, kamatna stopa, itd.). Također, institucije na nacionalnoj razini (uključujući pravila i organizacije kao što je vlada, sudstvo, itd.) utiču i pod uticajem su tih interakcija (Bhattacharyya, 2011).

Može se reći da dva najvažnija makroekonomska efekta energetskega sektora predstavljaju naftni šokovi i zagađenje okoliša. Energetski šokovi imaju uticaj na cijelu ekonomiju, a najznačajnije se ogleda u najvažnijim ekonomskim varijablama, a to su: GDP, cijene u zemlji, plate, nezaposlenost, preraspodjela dohotka zemlje i potrošače (Vlahinić-Dizdarević i Živković, 2011).

Uslijed visoke uvozne ovisnosti zemlje o energentima, stalni porast cijena i visoka volatilnost cijena na tržištima energenata, rast cijena nafte i ostalih energenata će uticati na pad potrošnje energije ovisno o cjenovnoj elastičnosti tražnje, te će uticati na smanjenje stope rasta GDP-a i proizvodnje. Porast cijene nafte i ostalih energenata kratkoročno dovodi i do porasta nivoa cijena u zemlji jer su preduzeća prisiljena povećavati cijene svojih proizvoda/usluga, što u krajnjem slučaju se prevlađuje na same potrošače (ukoliko je neelastična cjenovna tražnja za naftom i ostalim energetima). U slučaju cjenovno elastične potražnje, troškove rasta cijena snosili bi proizvođači koji zbog konkurencije ne mogu više troškove prevaliti na krajnje potrošače. Rast cijena nafte i ostalih energenata utiče i na plate, te povećava prirodnu stopu nezaposlenosti. „Rast prirodne stope nezaposlenosti utiče na smanjenje prirodne stope zaposlenosti, što dovodi do istovjetnog smanjenja prirodnog nivoa domaćeg proizvoda“ (Vlahinić-Dizdarević i Živković, 2011, str.14). Također, rast cijena utiče na kontrakciju energetski intenzivnih sektora i ekspanziju energetski efikasnih sektora, što dovodi do rasta nezaposlenosti i suboptimalne alokacije resursa. U slučaju preraspodjele dohotka, energetski šokovi utiču da se dohodak preraspoređuje od zemalja uvoznica prema zemljama izvoznicama energije. „Veličina ovog učinka zavisi od energetske intenzivnosti i energetske ovisnosti zemlje uvoznice, kao i sposobnosti krajnjih korisnika da racionaliziraju svoju potrošnju energije“ (Vlahinić-Dizdarević i Živković, 2011, str.15). Ukoliko je zemlja manje ovisna, ovaj efekat će biti manji, dok u suprotnom slučaju će imati negativne efekte na zemlju uvoznicu energenata.

Povezanost potrošnje energije i ekonomskog rasta

Iako mnogi ekonomisti smatraju povezanost ekonomskog rasta i potrošnje energije kao opšteprihvaćenu tezu, još uvijek ne postoji konsenzus o smjeru te kauzalnosti. Neki autori su dokazali da je energija ključan proizvodni input, dok drugi smatraju da je energija limitirajući faktor ekonomskog rasta, to jeste ima neutralan efekat na ekonomski rast.

U sljedećem dijelu ćemo pokazati neke od rezultata povezanosti potrošnje energije i ekonomskog rasta. Kakar, Khijli i Khan (2011) su analizirali povezanost energetske

potrošnje i ekonomskog razvoja i finansijskog razvoja u Pakistanu za godine od 1980.-2009. Oni su dokazali da postoji kauzalnost između finansijskog razvoja, energetske potrošnje i ekonomskog razvoja u dužem vremenskom periodu, dok u kratkom vremenskom periodu ne postoji. Chontanawat, Hunt i Pierse (2006) su također analizirali povezanost između energetske potrošnje i GDP-a u 30 OECD i 78 ne-OECD zemalja. Dokazali su da postoji veza između GDP-a i energetske potrošnje s vezom u 70 % OECD zemalja, dok samo 46 % u ne-OECD zemljama. Također su dokazali da postoji smjer kauzalnosti od GDP ka energetske potrošnji od 69 % u visoko razvijenim zemljama, 42 % u srednje razvijenim zemljama, te 35 % u nisko razvijenim zemljama. O ovome će biti više govora u sljedećem naslovu.

Autori Hossain i Saeki (2011) su analizirali da li postoji veza između potrošnje električne energije i ekonomskog rasta u zemljama južne Azije. Dokazali su da u kratkom roku postoji kauzalnost od potrošnje električne energije ka ekonomskom rastu u Bagladešu, dok u Pakistanu, Indiji i Nepal u taj smjer je obrnut u kratkom roku. U dugom roku, postoji kauzalnost od ekonomskog razvoja ka potrošnji električne energije u Šri Lanki i Bangladešu, dok Iran ima negativnu kauzalnost u dugom roku. Janosi i Grayson (2002) su dokazivali povezanost između potrošnje energije i ekonomskog rasta u 30 zemalja svijeta, te su dokazali da postoji kauzalnost od ekonomskog rasta ka potrošnji energije, međutim, rezultati su se jako puno razlikovali između sličnih zemalja.

Syotas i Sari (2002) su također dokazivali kauzalnost između energetske potrošnje i GDP-a za najrazvijenije zemlje svijeta, to jeste G-7 zemlje, bez Kine, za koju nisu bili dostupni podaci. Dokazali su da postoji smjer veze od GDP-a ka potrošnji energije u Italiji i Južnoj Koreji, dok je smjer obrnut za Tursku, Francusku, Njemačku i Japan. Lise i Montfort (2005) su također dokazivali uticaj između potrošnje energije i GDP-a u Turskoj, gdje su došli do rezultata da postoji ko-integracija. Georgantopoulos i Tsamis (2011) su analizirali relaciju između energetske potrošnje i GDP-a za određene zemlje Balkana, to jeste, Grčku, Bugarsku, Rumuniju i Albaniju. Dokazali su da postoji smjer kauzalnosti od potrošnje energije ka GDP-u u Bugarskoj, Rumuniji i Grčkoj, dok u Albaniji nije pronađen pravac uticaja između ove dvije varijable.

Posljednje istraživanje su uradili Vlahinić-Dizdarević i Živković (2011) koji su analizirali povezanost energije i ekonomskog rasta u Republici Hrvatskoj za područje od 1993.-2006. godine. Dokazali su da postoji smjer kauzalnosti od GDP-a prema potrošnji nafte, potrošnji energije u domaćinstvima i industriji, proizvodnji primarne energije te uvoza energije. Ovu analizu ćemo detaljnije objasniti u narednim naslovima.

Povezanost potrošnje energije i ekonomskog rasta u različitim zemljama

Chontanawat, Hunt i Pierse (2006) su empirijski istraživali vezu između potrošnje energije i ekonomskog rasta za 30 OECD i 78 ne-OECD zemalja. Testovi koje su koristi su nedavno razvijene metode. Prvo je korištena metodologija koja je razvijena od strane Granger-a i Sims-a⁵⁹. Nakon toga je korištena metoda korekcije greške

⁵⁹ „Grangerova uzročnost“ implicira kauzalnost u predviđanje razuma radije nego u strukturnom smislu. Počinje sa pretpostavkom „budućnost ne može uzrokovati prošlost“; ako događaj A se javlja nakon događaja B, onda A ne može izazvati B (Granger, 1969).

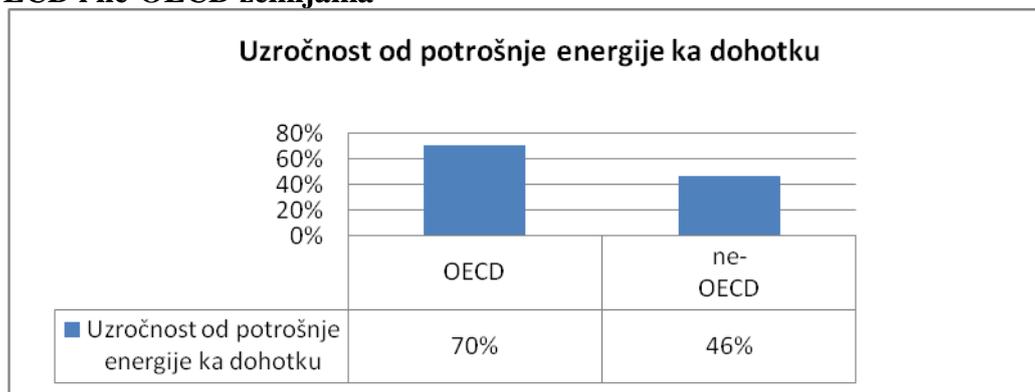
(Error Correction Model⁶⁰), koji je također razvijen od strane Granger-a. Treća metoda koja se koristila jeste Hsiao tehnika⁶¹ koja poboljšava Grangerovu prvobitnu metodologiju sa korištenjem kriterija završne greške predviđanja (FPE). Autori su podatke uzeli iz međunarodne energetske agencije (IEA) za 2002. godinu.

Rezultati ovih istraživanja su bili jako važni, jer ukoliko se pokaže da uzročnost ide od potrošnje energije ka dohotku, to dokazuje da je zemlja energetska zavisna i da stoga energija je stimulant razvoju zemlje, što u slučaju manjka ovog resursa, zemlju može dovesti u jako nezahvalnu situaciju. Ukoliko se pokaže da uzročnost ide od dohotka ka potrošnji energije to znači da je zemlja energetska nezavisna, te energetske politike mogu biti implementirane bez efekata na razvoj i zaposlenost.

Prvo su rađeni rezultati Grangerove uzročnosti za OECD i ne-OECD zemlje. Dokazali su da 26 OECD zemalja (87 %) pokazuje određenu uzročnost između potrošnje energije i ekonomskog rasta, dok samo 51 ne-OECD zemlja (65 %) . Također, dokazali su da 38 visoko razvijenih zemalja ima određenu uzročnost (84 % od ukupno), 29 srednje razvijenih zemalja (67 %) i samo 8 nerazvijenih zemalja, odnosno (47 %).

Postotak OECD zemalja i ne-OECD zemalja o uzročnosti koja vodi od energetske potrošnje ka dohotku pokazuje da 21 OECD zemlja, odnosno 70 % pokazuje takvu vrstu uzročnosti, dok samo 36 ne-OECD zemalja dokazuje isto, što je grafički prikazano na Grafikonu 1.

Grafikon 1: Dokaz Grangerove uzročnosti od potrošnje energije ka dohotku u OECD i ne-OECD zemljama



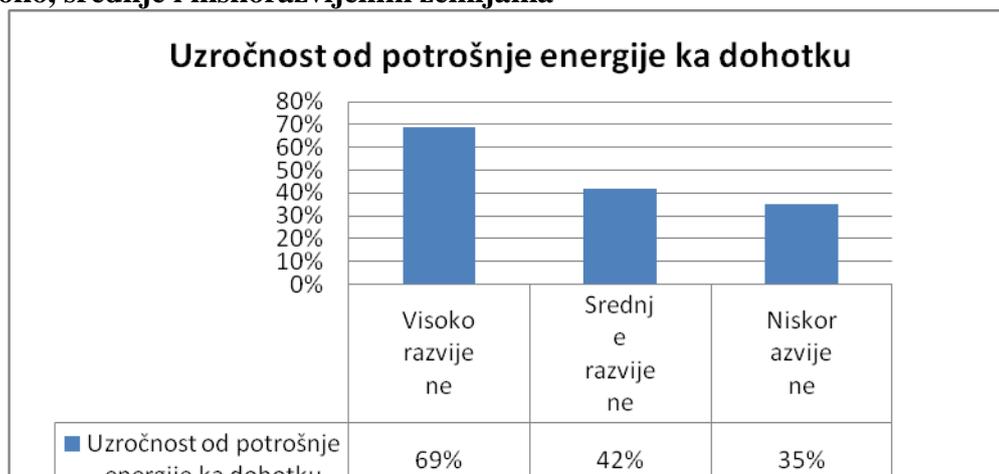
Izvor: Chontanawat, Hunt i Pierse, 2006

Na Grafikonu 2 je analizirana uzročnost od potrošnje energije ka dohotku za visoko, srednje i niskorazvijene zemlje. Kao što je očekivano, najveću uzročnost pokazuju upravo visokorazvijene zemlje, to jeste 31 od 45 zemalja, njih oko 69 %. Osamnaest od 43 srednje razvijene zemlje pokazuje ovu istu uzročnost, što je oko 42 %, dok samo 6 od 17 niskorazvijenih zemalja pokazuje uzročnost od energije ka dohotku, to jeste samo 35 % zemalja.

⁶⁰ Formula : $Y_t^* = \gamma_1 + \gamma_2 X_t + u_t$, EC model ima karakteristike da devijacija trenutnog stanja iz odnosa dužeg roka će biti korištena u kratkom roku. EC model nije model koji ispravlja greške u drugom modelu.

⁶¹ Koristi se kao dodatak Grangerovom modelu uzročnosti kako bi se dokazao smjer i postojanje određene veze.

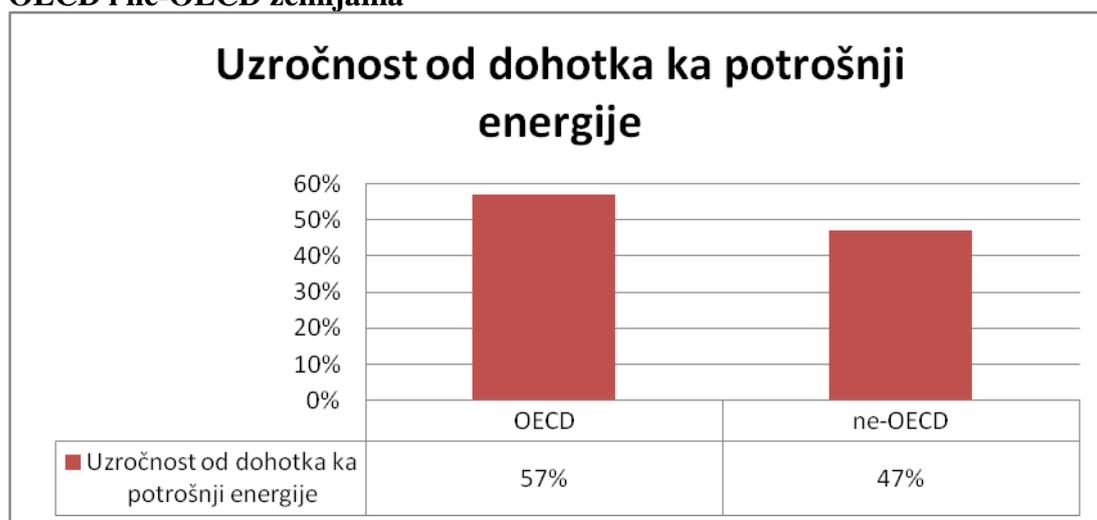
Grafikon 2: Dokaz Grangerove uzročnosti od potrošnje energije ka dohotku u visoko, srednje i niskorazvijenim zemljama



Izvor: Chontanawat, Hunt i Pierse, 2006

U suprotnom pravcu, to jeste uzročnost od dohotka ka potrošnji energije pokazuje da 17 od 30 OECD zemalja ima određeni dokaz ove uzročnosti, što je oko 57 %, dok samo 37 od 78 ne-OECD zemalja pokazuje isto, to jeste 47 %. To je prikazano na Grafikonu 3.

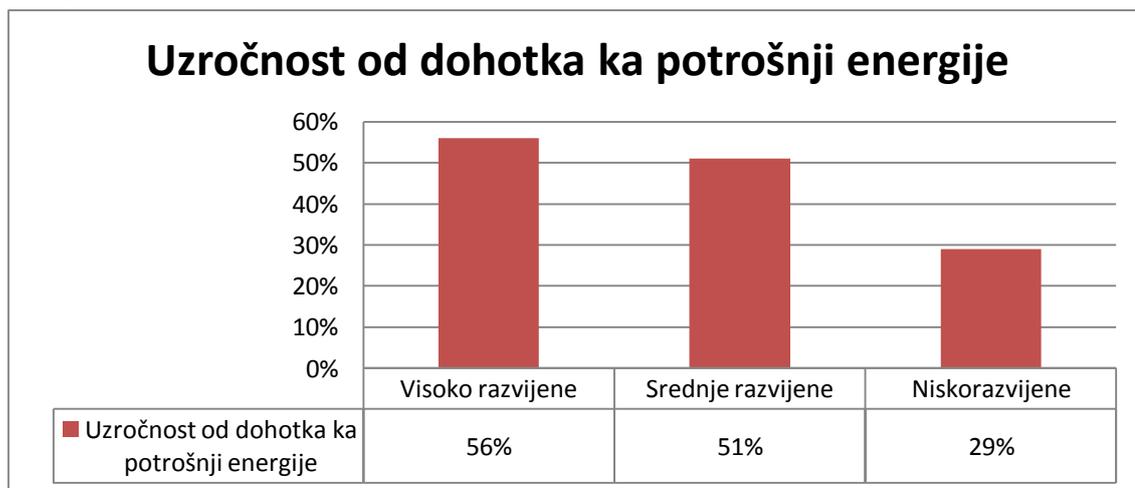
Grafikon 3: Dokaz Grangerove uzročnosti od dohotka ka potrošnji energije u OECD i ne-OECD zemljama



Izvor: Chontanawat, Hunt i Pierse, 2006

Ovi autori su također pokazali uzročnost od dohotka ka potrošnji energije i za visoko, srednje i niskorazvijene zemlje. Dokazali su da 25 od 45 visoko razvijenih zemalja (56 %), 22 od 43 srednje razvijene zemlje (51 %) i 5 od 17 niskorazvijenih zemalja (29 %) ima određene dokaze uzročnosti koja ide od dohotka ka potrošnji energije. Grafički je prikazano na Grafikonu 4.

Grafikon 4: Dokaz Grangerove uzročnosti dohotka ka potrošnji energije u visoko, srednje i niskorazvijenim zemljama



Izvor: Chontanawat, Hunt i Pierse, 2006

Analiza uzročnosti od dohotka ka potrošnji energije ustvari pokazuje da je mnogo veći u OECD/razvijenim zemljama, nego u ne-OECD/zemljama u razvoju. To sugerira da samo u vrlo siromašnim zemljama kauzalnost ide od dohotka ka potrošnji energije vjerovatno odražavajući da mnoge od tih zemalja imaju ekonomije temeljene na poljoprivredi, a time, s obzirom na njihov stepen razvoja, manje energetske ovisne, te potrošnja energije u tim zemljama nema velikog efekta.

Što se tiče uzročnosti od potrošnje energije ka dohotku, također je pokazano da više prevladava u OECD zemljama u odnosu na ne-OECD zemlje, s tim da je razlika dosta veća od uzročnosti od dohotka ka energetske potrošnji. Rezultati upućuju na zaključak da stepen uzročnosti od potrošnje energije ka dohotku općenito manji u zemljama u razvoju nego u razvijenim zemljama (ili alternativno uzročnosti od potrošnje energije ka dohotku se povećava na višim fazama razvoja). Rezultati podupiru stav da je energija uglavnom neutralna s obzirom na njen uticaj na ekonomski razvoj u zemljama u razvoju, što znači da efekat očuvanja energetske politika u borbi protiv globalnog zagrijavanja bi imao veći štetan učinak u OECD zemljama, nego u ne-OECD zemljama.

Povezanost potrošnje energije i ekonomskog rasta zemalja Balkana

Georgantopoulos i Tsamis (2011) su radili istraživanje uzročnosti između potrošnje energije i ekonomskog rasta u četiri zemlje Balkana (Grčka, Bugarska, Rumunija i Albanija). Ovo istraživanje je važno i za našu zemlju, jer su ovo zemlje koje se nalaze u našoj neposrednoj blizini, to jeste, na Balkanu.

Analiza je rađena za period od 1980.-2009. godine, a osnovne varijable koje su korištene su GDP u američkim dolarima i potrošnja energije (u kilotonama) za ove četiri zemlje. Podaci potrošnje energije su uzeti sa stranice međunarodne energetske agencije (IEA).

Grangerov test uzročnosti je korišten u analizi, ali i model vektorske autoregresije (VAR) i model korekcije greške (EC).

Rezultati koji su dobiveni u ovom istraživanju su prikazani u nastavku. Za Grčku, uzročnost se kreće od ekonomskog rasta (GDP) ka potrošnji energije. To znači da

povećanje ekonomskog rasta zahtjeva veliku potrošnju ukupne energije i energetske politike ne utiču na ekonomski rast.

Rezultati dobiveni za Bugarsku i Rumuniju su suprotni, to jeste, uzročnost ide od potrošnje energije ka GDP-u. U ovom slučaju, potrošnja energije se može posmatrati kao vodeći pokazatelj ekonomskog rasta tih dvaju balkanskih zemalja, što znači da će politike uštede energije vjerovatno uticati na ekonomski rast ovih zemalja.

Empirijski rezultati u Albaniji ukazuju da su potrošnja energije i GDP nezavisni, što pogoduje neutralnoj hipotezi. Stoga, energetska politika zaštite ne može uticati na ekonomski rast.

Tabela 1: Rezultati empirijske analize povezanosti potrošnje energije i ekonomskog rasta u zemljama Bakana

Zemlja	Uzročnost
Grčka	GDP → EC
Bugarska	EC → GDP
Rumunija	EC → GDP
Albanija	EC ≠ GDP

Izvor: autor

Povezanost potrošnje energije i ekonomskog rasta u Republici Hrvatskoj

Vlahinić-Dizdarević i Živković (2011) su analizirali povezanost potrošnje energije i ekonomskog rasta u Republici Hrvatskoj. Smatramo da je ovo istraživanje jako važno, jer je Hrvatska, iako dosta različita od BiH, naš prvi zapadni komšija.

Varijable koje su korištene u ovoj analizi su: realni bruto domaći proizvod (u miliona američkih dolara) na godišnjoj razini, konačna potrošnja energije u industriji i domaćinstvima, primarna proizvodnja energije, neto uvoz energije i potrošnja nafte u hiljadama barela dnevno. Vremenski niz koji je korišten se odnosi na razdoblje od 1993.-2006. godine. Korišten je Grangerov test uzročnosti, zajedno sa vektorskim modelom autoregresije (VAR) i model korekcije greške (EC), uz dodatne modele koji su bili potrebi pri izračunima (Akaike informacijski kriterij AIC, Schwarzov informacijski kriterij SIC, ADF metoda testiranja, Johansenova metoda testiranja postojanja kointegracije⁶²).

Rezultati koji su dobiveni su prikazani u Tablici 2. U Republici Hrvatskoj, uzročnost se keće od GDP-a ka potrošnji energije u industriji i domaćinstvima, primarno proizvodnji energije, neto uvozu energije i potrošnji nafte.

Tabela 2: Uzročnost između GDP-a i energetske varijabli u Republici Hrvatskoj

Varijabla	Kauzalnost	Varijabla
GDP	→	OIL
GDP	→	PEP
GDP	→	NIE
GDP	→	FEC_H
GDP	→	FEC_I

Izvor: Vlahinić-Dizdarević i Živković, 2011

Ovi rezultati ukazuju da je kratkoročno smjer uzročnosti uvijek isti i kreće se od realnog GDP-a prema energetskim varijablama. Ovi rezultati razlikuju se od većine

⁶² Cijeli proces izračuna može se naći u knjizi: Vlahinić-Dizdarević i Živković (2011) „Ekonomija energetskog sektora – izabrane teme“ str. 26-35

studija koje istražuju zemlje u razvoju kod kojih kauzalnost ima obrnuti smjer: od potrošnje energije ka ekonomskom rastu. Rezultati koje su autori dobili za Hrvatsku su specifični za razvijene, postindustrijske zemlje s razvijenim uslužnim sektorom. Iako je Hrvatska tranzicijska zemlja, njena ekonomska struktura je slična razvijenim zemljama u kojima uslužni sektor čini preko 60 % udjela u bruto domaćem proizvodu. Međutim, problemi privatizacije, to jeste privlačenje *brown-field* investicija u uslužni sektor, posebice telekomunikacije i finansije, restrukturiranje teške industrije koja je bila veliki potrošač energije, te nekonkurencije na EU tržištu i gubitak ex-jugoslavenskog tržišta su uticali na značajno smanjenje potrošnje energije u industrijskom sektoru.

Hrvatska ima sličnu strukturu razvijenim zemljama, međutim, samo što se tiče uslužnog sektora, dok je industrija daleko od nivoa industrija razvijenih zemalja.

Povezanost potrošnje energije i ekonomskog rasta u Bosni i Hercegovini

Kao što smo napomenuli u prvom poglavlju, jedna od najvažnijih analiza ekonomije energetskega sektora jeste analiziranje povezanosti (veze) potrošnje energije i ekonomskog rasta. Ova analiza je rađena u većini zemalja i jako je važna iz razloga što ova analiza jer mnogo pomaže pri kreiranju budućih energetskega strategija. Tako npr. ukoliko uzročnost se kreće od potrošnje energije ka dohotku, to dokazuje da je zemlja energetskega zavisna i da stoga energija je stimulant razvoju zemlje, što u slučaju manjka resursa, zemlju može dovesti u jako nezahvalnu situaciju. Ukoliko se pokaže da uzročnost ide od dohotka ka potrošnji energije, to znači da je zemlja energetskega nezavisna, te energetskega politike mogu biti implementirane bez učinka na razvoj i zaposlenost. Također, treba napomenuti da mnogo toga zavisi i od razvijenosti zemlje, jer se ne mogu isto tumačiti rezultati za razvijene i nerazvijene zemlje. Kao što smo prethodno napisali, skoro svaka zemlja je uradila ovu analizu, čak i susjedne zemlje, kao što je Hrvatska, dok u Bosni i Hercegovini još uvijek takva jedna analiza nije urađena.

Nažalost, nemam dovoljno podataka da radimo modeliranje, jer se radi o jako kratkom vremenskom periodu dostupnosti podataka, to jeste od 2000. – 2005. godine, a razlog tome jeste primarno nedostupnost energetskega podataka i to finalne potrošnje energije, finalne potrošnje energije u kućanstvima i industriji. Ono što se moglo napraviti jeste izračunati jednostavnu korelaciju između varijabli od interesa. U ovu analizu sam uključio GDP (milijunima KM) , GDP per capita, realni GDP⁶³, te energetskega podatke koje obuhvataju finalna potrošnja energije (PJ), finalna potrošnja energije u kućanstvima i industriji (PJ)⁶⁴, primarna potrošnja energije (kvadrilijon btu)⁶⁵ i ukupna potrošnja električne energije⁶⁶.

Nakon urađene analize, dobili smo slijedeće koeficijente korelacije.

⁶³ Preuzeto iz statističke publikacije Centralne banke Bosne i Hercegovine

⁶⁴ Preuzeto iz „Studja energetskega sektora Bosne i Hercegovine“

⁶⁵ Preuzeto sa internet stranice:

http://www.tititodorancea.com/z/ies_bosnia_and_herzegovina_total_primary_energy_consumption.htm

⁶⁶ Preuzeto iz statističke publikacije DERK-a

Tabela 1: Rezultati analize uzročnosti potrošnje energije i ekonomskog rasta u Bosni i Hercegovini za razdoblje od 2000. – 20005. godine

Korelacija	gdp	gdppc	gdprgr	Fconsnat	fconshos	fconsind	primen	Totalelec
gdp	1.000							
gdppc (p-value)	1.000 <i>0.000</i>	1.000						
gdprgr (p-value)	-0.4060 <i>0.2154</i>	-0.4080 <i>0.2129</i>	1.000					
fconsnat (p-value)	0.8167 <i>0.0473</i>	0.8245 <i>0.0435</i>	-0.0332 <i>0.9502</i>	1.000				
fconshos (p-value)	0.8726 <i>0.0233</i>	0.8769 <i>0.0218</i>	-0.3695 <i>0.4710</i>	0.8859 <i>0.0188</i>	1.000			
fconsind (p-value)	0.6527 <i>0.1600</i>	0.6623 <i>0.1518</i>	0.1649 <i>0.7550</i>	0.9347 <i>0.0063</i>	0.6757 <i>0.1407</i>	1.000		
primen (p-value)	0.9033 <i>0.0021</i>	0.9020 <i>0.0022</i>	0.5860 <i>0.1268</i>	0.9294 <i>0.0073</i>	0.8201 <i>0.0457</i>	0.8873 <i>0.0183</i>	1.000	
totalelec (p-value)	0.9253 <i>0.0000</i>	0.9242 <i>0.0000</i>	-0.3357 <i>0.2861</i>	0.9596 <i>0.0024</i>	0.9115 <i>0.0114</i>	0.9310 <i>0.0404</i>	0.9432 <i>0.0004</i>	1.0000

Izvor: autor

Rezultati koje smo dobili su sljedeći: GDP i GDPpc su povezani sa finalnom potrošnjom energije, finalnom potrošnjom energije u kućanstvima, primarnom potrošnjom energije i ukupnom potrošnjom električne energije na jako velikom nivou oko 0.8 pa na više (čak 0.92 sa potrošnjom električne energije za obje varijable). Koeficijenti korelacije su statistički signifikantni. Na manjem nivou GDP i GDPpc su povezani sa finalnom potrošnjom energije u industriji u visini od 0.65 i 0.66. Također, potrošnja električne energije je korelirana na jako visokom nivou sa finalnom potrošnjom energije i finalnom potrošnjom energije u kućanstvima (0.96 i 0.91), dok u manjem iznosu sa finalnom potrošnjom energije u industriji (0.83). Uočavamo da najveću potrošnju energije u BiH (naročito električnu energiju) troše kućanstva, zatim transport, pa tek onda industrija. Prema tome, ovi podaci impliciraju da je Bosna i Hercegovina nerazvijena zemlja u kojoj industrija ne troši mnogo energije iz razloga što je na jako niskom nivou, a ne iz razloga što je energetska efikasna. Konačni zaključak može biti da bi prema ovim rezultatima BiH mogla provoditi politike zaštite okoliša, te smanjenja potrošnje energije, međutim, naš glavni prioritet bi možda trebao biti razvoj industrije, pa tek onda stimulisanje ovih politika.

ZAKLJUČAK

Nakon prvog, odnosno drugog naftnog šoka, ekonomisti počinju pridodavati dosta pažnje energiji i energetskom sektoru. Detaljnim analizama se dolazi do zaključka da energija ima više nego jasne makroekonomske efekte, gledajući njen uticaj na GDP, cijene u zemlji, plate, nezaposlenost, preraspodjela dohotka zemlje i potrošače. Analiza koja najviše pažnje privlači jeste računanje povezanosti između potrošnje energije i ekonomskog rasta. Na osnovu radova koje smo istakli u ovome

radu može se zaključiti da ova veza postoji, te su dobiveni različiti rezultati od strane različitih autora. U analizi Bosne i Hercegovine možemo zaključiti da postoje inicijalne indicije o statistički značajnoj korelaciji između ekonomskog rasta i potrošnje električne energije. Dobiveni podaci za BiH upućuju da je zemlja energetska efikasna, gdje industrija troši malo energije, međutim, razlozi su nerazvijenost, a ne energetska efikasnost. Naravno, ovo pitanje je potrebno dalje analizirati kroz naprednije modele, ali trenutno za takve analize nisam mogao obezbjediti relevantne podatke.

LITERATURA

Knjige i udžbenici:

- Beggs, C., (2009), “Energy – Management, supply and conversation”, Elsevier, UK
- Bhattacharyya, S.C., (2011), “Energy Economics- Concepts, Issues, Markets and Governance”, Springer-Verlag London Limited, UK
- Chandler, W., (2000), “Energy and environment in the transition economies”, Westview press, USA
- Conkling, R.L., (2011), “Energy Pricing- Economics and principles”, Springer- Verlag Berlin Heidelberg
- Dabrowski, M., Maliszewska, M., (2011), “EU Eastern neighborhood- Economic potential and future development”, Springer- Verlag Berlin Heidelberg
- Ekspertna grupa za izradu SPP, (2008), “Strateški plan i program razvoja energetskog sektora Federacije BiH”, Sarajevo
- Energetski institut "Hrvoje Požar", Ekonomski institut Banjaluka, (2011), “Strategija razvoja energetike Republike Srpske do 2030. Godine”, Banjaluka
- Evans, J. i Hunt, L., (2009), “International Handbook on the Economics of Energy”, MPG Books Group, UK
- International Energy Agency, (2008), “Energy in the Western Balkans- The path to reform and reconstruction”, OECD/IEA
- International Energy Agency, (2010), “World Energy Insight 2010”, OECD/IEA
- International Energy Agency, (2010), “World Energy Outlook 2010”, OECD/IEA
- Pollitt, M. i Jamasb, T., (2005), “Electricity Market Reform in the European Union: Review of Progress toward Liberalization & Integration”, The Energy Journal, 26(Special Issue): 11-41
- Salzmann, O., (2006), “Corporate Sustainability Management in the Energy Sector”, Galber Edition Wissenschaft, Berlin
- Sionshansi, F. i Pfaffenberger, W., (2006), “Electricity Market Reform – An international perspective”, Elsevier Global Energy Policy and Economics Series, Oxford, UK
- Turner, W.C. i Doty, S., (2006), “Energy management handbook- sixth edition”, The Fairmont Press Inc. , New York
- Turner, W.C., (2005), “Energy management handbook- fifth edition”, The Fairmont Press Inc. , New York

- Vlahinić – Dizdarević, N. i Živković, S., (2011), “Ekonomija energetskeg sektora – izabrane teme”, Rijeka
- Zenfora, A. L. , (2010), “Encyclopedia of Energy Research and Policy”, Nova Science Publisher Inc. , New York

Članci:

- Alam, M. S., (2006) "Economic Growth with Energy," MPRA Paper 1260, University Library of Munich, Germany
- Alam, M.S., (2006), “Economic growth with energy”, Northeastern University, Boston
- Auty, R., (1993) “Sustaining Development in Mineral Economies: The Resource Curse Thesis”, London: Routledge
- Auty, R., (2001) “Resource Abundance and Economic Development”, New York: Oxford University Press
- Ayres, R. i van den Bergh, J., (2002), “The role of material/energy resources and dematerialization in economic growth theories”, Department of Spatial Economics Free University Amsterdam
- Bojnec, Š. i Papler, D., (2011), “Economic efficiency, energy consumption and sustainable development”, Journal of Business Economics and Management. Volumen 12
- CEIP: Centre on Emission Inventories and Projections Report, 2007
- Centar za politike i upravljanje, (2010), “Izvještaj o politikama energetskeg sektora u Bosni i Hercegovini”
- Chontanawat, J., Hunt, L., Pierse, R., (2006), “Causality between energy consumption and GDP: Evidence from 30 OECD and 78 Non-OECD Countries”, University of Surrey ,Energy Economics Centre
- Choucri, N., Heye, C., Lynch, M., (1990), “Analyzing oil production in developing countries: A case study of Egypt”, The Energy journal. Volumen 11. Broj 3
- Dekanić, I., Kolundžić, S., i Slipac, G. (2006), “Croatia's Energy Future and Gas Supply / Energija – Journal of Energy” , Zagreb, 55, 382/415
- European Commission, (2010), “Energy 2020: A strategy for competitive, sustainable and secure energy”, Brussels
- European Commission, (2011), “Energy Roadmap 2050”, Brussels
- Georgantopoulos, A.G. i Tsamis, A.D., (2011), “The relationship between energy consumption and GDP: A causality analysis on Balkan countries”, European journal of scientific research
- Hossain, S. i Saeki, C., (2011), “Does electricity consumption panel Granger cause economic growth in South Asia? Evidence from Bangladesh, India, Iran, Nepal, Pakistan and Sri-Lanka”, European journal of Social Science. Volumen 25. Broj 3
- Imran, K. i Siddiqui, M.M., (2010), “Energy consumption and economic growth: A Case Study of Three SAARC Countries”, European journal of Social Science. Volumen 16. Broj 2
- Jakovac, P., (2010), “Važnost električne energije i osvrt na reform elektroenergetskog sektora u Europskoj Uniji i republici Hrvatskoj”, Ekonomski fakultet u Rijeci
- Janosi, P., Grayson, L., (2002), “Patterns of energy consumption and economic growth and structure”, Journal of development studies

- Jelavić, B., Željko, M., Statham, B., (2008), “Energetska budućnost kroz studije WEC-a”, Energija. Volumen 57
- Jorgenson, D.W., (2001), “Economic effects of the rise in energy prices: what have we learned in ten years?”, The energy journal
- Kakar, Z.K. i Khilji, B.A., (2011), “Energy consumption and economic growth in Pakistan”, Journal of International Academic Research. Volumen 11. Broj 1
- Karanfil, F., (2008), “Energy consumption and economic growth revisited: Does the size of unrecorded economy matter?”, Energy policy. Volumen 36
- Kennedy, D., (2003), “Power sector regulatory reform in transition economies: Progress and lessons learned”, European Bank for Reconstruction and Development
- Kristian Benac, Teo Slosar, Marko Žuvić, (2008), “Svjetsko tržište nafte”, Pomorski zbornik 45
- Lise, W. i Van Montfort, K., (2005), “Energy consumption and gdp in Turkey: is there a co-integration relationship?”, Energy research Centre of the Netherlands
- MOFTER, Energija 21. vijeka – preduslov industrijskog, ekonomskog i društvenog ravoja, Međunarodni Poslovni Forum perspective, Tuzla 5-6. 05.2009.
- Rodrik, D., (2006), "Goodbye Washington Consensus, Hello Washington Confusion? A Review of the World Bank's Economic Growth in the 1990s: Learning from a Decade of Reform.", Journal of Economic Literature, 44(4): 973–987
- Sauter, R. i Awerbuch, S., (2003), “Oil price Volatility and economic activity: A survey and literature review”, IEA Research paper
- Smajević, I., Bašić, A., Vućina S., Ninković, N., Knežević, A., Petrović, S., Čizmić, E., Kazagić, A., Hadžiomerović-Šutović, M., (2008), “Strateški plan i program razvoja energetskog sektora Federacije BiH”
- Soytaş, U. i Sari, R., (2003), “Energy consumption and GDP: causality relationship in G-7 countries and emerging markets”, Energy economics 25
- Stern, D.I. i Cleveland, D.J., (2004), “Energy and economic growth”, Rensselaer working papers in economics
- Stern, D.I., (2001), “The role of energy in economic growth”, Annals of the New York academy of science
- Stern, D.I., (2003), “Energy and economic growth”, Rensselaer Polytechnic Institute, New York
- Svjetska Banka, (2008), “Energetska studija za BiH”, Ministarstvo vanjske trgovine i ekonomskih odnosa, Sarajevo, BiH
- Tabata, S., (2008), “Influence of the oil price increase on the Russian Economy: Comparison with Saudi Arabia”, Hokkaido University
- Vasconcelos, J., (2004), “Services of General Interest and Regulation in the EU Energy Market, Council of European Energy Regulators (CEER)”, Presentation at XVI CEEP Congress 17 June 2004, Leipzig
- Vlahinić – Dizdarević, N. i Galović, T., (2007), “Macroeconomic context of economic reforms in electricity sector of transition countries”, Ekonomski fakultet u Rijeci
- Vlahinić – Dizdarević, N. i Živković, S., (2010), “The role of energy in economic growth: the case of Croatia”, Ekonomski fakultet u Rijeci

- Vlahinić – Dizdarević, N., (2009), “Preconditions and impacts of regional electricity market in Southeast Europe”, Ekonomski fakultet u Rijeci
- Vlahinić – Dizdarević, N., Host, A., Galović, T., (2009), “The genesis of EU electricity market opening: Liberalization effects and obstacles”, Ekonomski fakultet u Rijeci

Ostali izvori, Internet :

- www.europa.eu
- www.wikipedia.org
- www.iea.org
- <http://www.news.balkanenergy.com/>
- <http://www.mvteo.gov.ba>
- <http://www.indexmundi.com>
- <http://www.rzs.rs.ba>
- www.fzs.ba
- www.ebrd.com
- www.derk.ba
- www.bitno.ba

ANALIZA PROMETNOG SUSTAVA U SARAJEVU S CILJEM USMJERAVANJA NJEGOVOG DALJEG RAZVOJA KA EVROPSKIM STANDARDIMA

Palić Nermin, Mr. sc., Cinac Džemal, Mr. sc.

Visoka škola „CEPS-Centar za poslovne studije“ Kiseljak,
Sveučilište/Univerzitet "ITC - Interlogos centar" Kiseljak,
nermin.palic@yahoo.com, dcinac@yahoo.com

SAŽETAK

Sarajevo je grad koji trenutno nema detaljno razrađenu strategiju razvoja prometnog sustava sukladno s propisima EU. U ovom radu iznesene su neke osnovne značajke te primjenom prikupljenih podataka urađena je detaljna analiza prometnog sustava. Svrha ove analize je ustanovljavanje stvarnog stanja prometnog sustava u Sarajevu, te na primjerima drugih razvijenih gradova pronaći adekvatna i provjerena rješenja za saniranje prometne problematike grada. Prilikom analize prometnog sustava u Sarajevu bazirat ćemo se na analizu stupnja motorizacije i intenziteta korištenja osobnih automobila, analizi broja javnih garaža u centru grada, mogućnosti implementacije Park & Ride sustava, analizu masovnog javnog gradskog prijevoza, analizi taksi prijevoza i duljini biciklističkih staza. Gradovi, na osnovu kojih ćemo vršiti usporedbu prometnog sustava Sarajeva su Brisel, Beč, Štokholm, Amsterdam, Prag i Edinburg.

Ključne riječi: Sarajevo, prometni sustav, gradski prijevoz.

UVOD

Posmatrajući prikupljene podatke u periodu od 2008. – 2012. godine u Sarajevu je zabilježen blagi, ali konstantan porast broja motornih vozila. U ovih 5 godina broj registriranih motornih vozila se povećao sa 119.081 na 141.461, tj. za 15%, što znači da je taj porast godišnje iznosio oko 4.245 vozila⁶⁷.

S navedenom količinom motornih vozila promet je u Sarajevu već dugi niz godina najveći izvor zagađenja zraka što je potvrdio i Registar emisija u zrak za područje Kantona Sarajevo.⁶⁸ Shodno tome, važno je navesti da Europska Zelena knjiga o gradskom prometu navodi da se zbog prometnih gužvi i oboljenja uzrokovanih ispušnim plinovima prometa godišnje gubi gotovo 100 milijardi eura, tj. 1% europskog BDP-a.⁶⁹ EU donijela je Akcijski plan koji propisuje konkretne mjere za uspostavu održivog gradskog prometa i rokove za njihovu implementaciju. Za Sarajevo trenutno ne postoji detaljno razrađena strategija razvoja prometa sukladno s propisima EU.

⁶⁷ Bosanskohercegovački auto – moto klub. Informacija o ukupnom broju registriranih i prodatih novih motornih vozila u BiH 2008. – 2012. http://bihamk.ba/index.php?option=com_content&view=article&id=10&Itemid=147

⁶⁸ <http://mpz.ks.gov.ba/sites/mpz.ks.gov.ba/files/Skraceni%20REGISTAR%20KS.pdf> (pristupljeno 21. avgust 2014. g.)

⁶⁹ Green paper. 2007. Towards a new culture for urban mobility. European Commission (pristupljeno 21. avgust 2014. g.) http://ec.europa.eu/transport/clean/green_paper_urban_transport/doc/2007_09_25_gp_urban_mobility_en.pdf (pristupljeno 21. avgust 2014. g.)

Najveći problem predstavljaju putovanja na posao i sa posla. Odredište mnogih putovanja automobilom je centar grada, koji je prostorno i prometno dobrim dijelom već izgrađen i definiran. U tim periodima stvaraju se ogromne gužve pri čemu neizbježno dolazi do znatnih poteškoća u odvijanju prometnog sustava na području cijelog grada, a osobito u središtu čije ulice ne uspijevaju izdržati toliki pritisak.

CILJ ANALIZE

Cilj ove analize je ustanovljavanje stvarnog stanja prometnog sustava u Sarajevu, te na primjerima drugih razvijenih gradova pronaći adekvatna i provjerena rješenja za saniranje prometne problematike grada. Prometne slabosti grada jasno su navedene u Strategiji razvoja grada Sarajeva 2012-2020 godine, a u koje spadaju: preopterećenje prometom kako centralnih tako i perifernih dijelova grada, neadekvatna rješenja za promet u mirovanju, izrazito visoko zagađenje zraka i saobraćajna buka.⁷⁰

Shodno tome, prilikom analize prometnog sustava u Sarajevu bazirat ćemo se na analizu stupnja motorizacije i intenziteta korištenja osobnih automobila, analizi broja javnih garaža u centru grada, mogućnosti implementacije Park & Ride sustava, analizu masovnog javnog gradskog prijevoza, analizi taksi prijevoza i duljini biciklističkih staza. Gradovi (i razlozi za usporedbu) na osnovu kojih ćemo vršiti usporedbu prometnog sustava Sarajeva su: Amsterdam – dobro razvijen biciklistički promet; Beč – idealno uređen centar grada, a konkretno ako se u obzir uzme broj garaža u centru grada; Brisel – Administrativno središte Europske unije, preuzimanja primjera dobre prakse; Edinburg – Pokušava ograničiti ulazak automobila u samo jezgro grada; Prag – svojom konstrukcijom u mnogome sličan Sarajevu, zanimljivo primijetiti sličnosti i razlike u karakteristikama prometnog sustava; Štokholm – jedan od najboljih primjera pravilnog prometnog i prostornog planiranja.

Podaci su prikupljeni istraživanjem provjerenih internet portala, pribavljene literature i kataloga iz raznih statističkih i drugih zavoda, te slanjem upita firmama i gradskim upravama o statističkim podacima neophodnim za ovo istraživanje. U određenim kategorijama nismo uspjeli da prikupimo tražene informacije za sve navedene gradove, što nije bitno uticalo na samo istraživanje. U tabeli 1 prikazan je broj stanovnika u gradovima koji su predmet analize:

Tabela 1: Broj stanovnika po gradovima

Grad	Broj stanovnika
Sarajevo ⁷¹	438.443
Amsterdam ⁷²	820.654
Beč ⁷³	1.766.746

⁷⁰ Služba za lokalno poslovanje i razvoj. 2012. Strategija razvoja Grada Sarajeva 2012-2020. Sarajevo

⁷¹ <http://dnevni-list.ba/web1/2013/11/06/u-bih-zive-3791-622-osobe-sarajevo-ima-291-422-banja-luka-199-191-a-mostar-113-169-stanovnika/> (pristupljeno 25. avgust 2014. g.)

⁷² <http://www.amsterdam.info/basics/> (pristupljeno 25. avgust 2014. g.)

⁷³ <https://www.wien.gv.at/statistik/pdf/viennainfigures.pdf> (pristupljeno 25. avgust 2014. g.)

Brisel ⁷⁴	1.154.635
Edinburg ⁷⁵	487.500
Prag ⁷⁶	1.243.201
Štokholm ⁷⁷	905.184

ANALIZA PROMETNOG SUSTAVA S REZULTATIMA ISTRAŽIVANJA

Analiza stupnja motorizacije i intenziteta korištenja osobnih automobila

Stupanj motorizacije predstavlja broj motornih vozila na 1000 stanovnika. Pod motornim vozilom podrazumjevaju se sva motorna vozila, osim motocikla, namijenjena za prijevoz putnika i dizajnirana tako da nemaju više od 9 sjedišta uključujući vozača.⁷⁸ Stupanj motorizacije predstavlja jedan od osnovnih pokazatelja prilikom predviđanja prijevozne potražnje. U tabeli 2 i na slici 1 prikazana je promjena stupnja motorizacije u Sarajevu, Beču i Briselu.

Tabela 2: Broj motornih vozila na 1000 stanovnika

Godina	Gradovi		
	<i>Sarajevo</i> ⁷⁹	<i>Beč</i> ⁸⁰	<i>Brisel</i> ⁸¹
2007.	-	392,5	478,1
2008.	282,7	389,5	477
2009.	282,4	390,8	470
2010.	288,8	390,4	468
2011.	304,5	389,6	-
2012.	321	390,2	442 ⁽¹⁾

(1) proračunato na osnovu broja stanovnika i broja motornih vozila za odgovarajuću godinu

⁷⁴ http://www.statistics.irisnet.be/files/publications/minibru/mini_bru_2014_EN.pdf (pristupljeno 25. avgust 2014. g.)

⁷⁵ <http://www.gro-scotland.gov.uk/files2/stats/council-area-data-sheets/city-of-edinburgh-factsheet.pdf> (pristupljeno 25. avgust 2014. g.)

⁷⁶ <http://www.citypopulation.de/php/czechrep-praguecity.php?cid=PR161> (pristupljeno 25. avgust 2014. g.)

⁷⁷ http://en.wikipedia.org/wiki/Stockholm#cite_note-StockholmUrbanArea-4 (pristupljeno 25. avgust 2014. g.)

⁷⁸ http://epp.eurostat.ec.europa.eu/cache/ITY_SDDS/DE/tsdpc340_esmsip.htm#meta_update1401955299169 (pristupljeno 25. avgust 2014. g.)

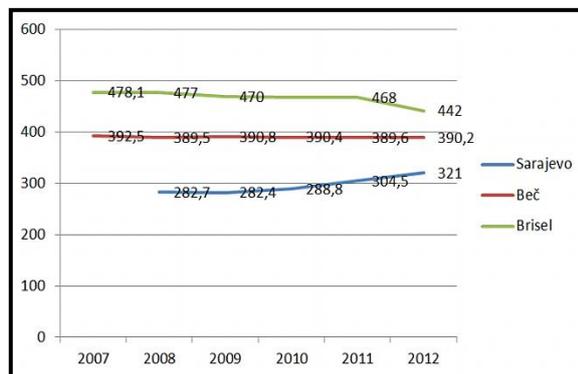
⁷⁹ Stupanj motorizacije proračunat na osnovu podataka iz BiHAMK-ovih kataloga o broju registriranih motornih vozila, Demografske analize Kantona Sarajevo po općinama u periodu 2003 – 2010. godine (Zavod za planiranje razvoja Kantona Sarajevo) i publikacije Federalni zavod za statistiku. 2013. „Kanton Sarajevo u brojkama 2013.“

<http://www.fzs.ba/Podaci/09.pdf> (pristupljeno 26. avgusta 2014. g.)

⁸⁰ <http://www.wien.gv.at/statistik/pdf/viennainfigures.pdf> (pristupljeno 26. avgust 2014. g.)

⁸¹ <http://knoema.com/atlas/Belgium/R%C3%A9gion-de-Bruxelles-Capitale-Brussels-Hoofdstedelijk-Gewest-BE1/Motorisation-rate> (pristupljeno 26. avgust 2014. g.)

Na osnovu grafičkog prikaza možemo ustanoviti tri različita trenda. Dok se u Sarajevu stupanj motorizacije počeo povećavati, posebno u posljednjoj godini analize i to za 16,5 vozila u odnosu na prethodnu godinu (u prosjeku 7,6 vozila godišnje), u Beču stupanj motorizacije ostaje ujednačen (u prosjeku oko 390 vozila na 1000 stanovnika), dok u Briselu taj stupanj iz godine u godinu konstantno opada, za prosječno 7,2 vozila. Prije 5 godina Brisel je na 1000 stanovnika



Slika 1: Grafički prikaz promjene stupnja motorizacije

imao skoro 200 motornih vozila više nego Sarajevo, dok se ta razlika u 2012. godini znatno smanjila (121 motornih vozila na 1000 stanovnika više ima Brisel). Stupanj motorizacije u Sarajevu je još uvijek zadovoljavajući, međutim, ukoliko bi se nastavila ovakva kretanja, Sarajevo bi za par godina moglo prestići i Brisel i Beč.

Klimatske promjene koje smo već počeli osjećati, uzročnici su razornih posljedica, pa se iz tog razloga sve više ulažu naponi za smanjenje emisija stakleničkih plinova. Cilj EU je da do 2020. smanji emisiju stakleničkih plinova za 20%, a do 2050. za 50% u odnosu na 1990. godinu. Mnogi stručnjaci iz ovih oblasti mišljenja su da se taj proces smanjenja emisija mora još ubrzati. Kao što je mnogo puta ustanovljeno, promet je jedan od najvećih uzročnika velike emisije stakleničkih plinova. 2004. godine, na razini EU promet je sudjelovao sa 24% u ukupnoj emisiji stakleničkih plinova.⁸² Iste godine je ukupna emisija CO₂ u odnosu na 1990. porasla za 30%.⁸³

Najbolji način za redukciju emisije stakleničkih plinova je unaprijeđenje masovnog javnog gradskog prijevoza putnika. Pored toga, postoje i drugi alternativni pokušaji, koji postaju sve popularniji, međutim nemaju zadovoljavajuću brzinu i efekt na smanjenje. Neki od tih pokušaja su proizvodnja motornih vozila s manjom potrošnjom goriva. Uz stopu porasta broja automobila u svijetu od prosječno preko 4% količina stakleničkih i ostalih plinova iz prometa neće se uspjeti niti zadržati na trenutnoj razini, a pogotovo smanjiti, usprkos smanjenu pojedinačne emisije ispušnih plinova iz automobila. Zbog toga je smanjenje broja motornih vozila, kao i smanjenje njihovog korištenja najučinkovitija mjera za smanjenje emisija štetnih i stakleničkih plinova iz prometa, a glavni način za postizanje tog cilja je naveden na samom početku – javni gradski prijevoz putnika uz promociju i poticanje biciklističkog prometa.

Analiza broja javnih garaža i parkirališta u centru grada

Najčešće odredište putovanja najvećeg broja građana često je sam centar grada. To često predstavlja problem u prometu. S jedne strane postoji ograničena propusna moć starih i uskih ulica, a s druge strane veliki broj građana koji putuju u gradsko središte. Taj problem moguće je riješiti poticanjem ljudi da prilikom putovanja u centar ne

⁸² European Federation for Transport & Environment. 2004. „Greenhouse gas emissions from transport in the EU25“. UNFCCC

⁸³ Preparation of a Green Paper on Urban Transport. 2007. „Report on Urban Transport in Europe“

koriste automobil već javni prijevoz ili bicikl. Ovaj trend bi imao smisla tek kada bi gradska uprava alternativne vidove prijevoza učinila maksimalno kvalitetnima i atraktivnima što većem broju građana.

Jedan od čestih problema prilikom ulaska osobnim vozilom u samo jezgro grada je pronalazak slobodnog parking prostora. Svi veliki gradovi imaju garaže u svojim središtima. Međutim, njihov broj tj. broj parking mjesta u garažama je potrebno optimizirati jer preveliki broj parking mjesta uzrokuje probleme u normalnom odvijanju prometnog toka. Kako to postići? Zbog različitih politika određenih gradova postoje i različite strategije. Ako je prometna strategija nekog grada maksimalno poticanje korištenja automobila, onda je jasno da će gradska uprava nastojati izgraditi veliki broj parking mjesta u garažama. Sigurno je da će tako velika orijentiranost na privatni individualni cestovni promet rezultirati prometnim čepovima te da je takav princip dugoročno neodrživ. Međutim, ako grad odluči da je s aspekta prometa najvažnije osigurati građanima kvalitetan sustav prijevoza, sigurno je da će uložiti znatne napore u razvitak javnog prometa i biciklizma. Zbog toga će Uprava takvog grada isticati da je u gradskom središtu potrebno znatno manje parking mjesta, nego što će to biti slučaj s predstavnicima grada koji sastav prijevoza temelji na osobnim automobilima.

Iznimno je bitna lokacija svake javne garaže; ako se ona gradi u nekoj rezidencijalnoj četvrti gdje ne postoji mnogo kulturnih i/ili komercijalnih sadržaja, takvu garažu bi uglavnom koristili stanari i njihovi posjetitelji pa je vjerojatno da ta garaža ne bi stvorila probleme u odvijanju prometa. S druge strane, ako se javna garaža izgradi u centru grada, vjerojatno je da će broj automobila u pristupnim ulicama još više porasti. Generalno se može reći da u središtima gradova treba pokušati maksimalno smanjiti intenzitet prometa, a preveliki broj garaža će sasvim sigurno uzrokovati dijametralno suprotan učinak.

Kako postići optimalan broj parking mjesta u garažama pokušali smo pronaći u usporedbi s drugim gradovima. U Sarajevu postoji ukupno ukupno 1.750 parking mjesta. Da bi se mogao usporediti broj parking mjesta u garažama između više gradova, potrebno ih je dovesti u vezu s brojem stanovnika svakog grada. Koristit ćemo se pretpostavkom: Što neki grad ima više stanovnika, to će broj putovanja u centar biti veći te će zbog toga uvjetno rečeno biti “potreban” veći broj parking mjesta nego kod grada s manjim brojem stanovnika.

Tabela 3: Broj parking mjesta u javnim garažama u centru grada

	Sarajevo ⁸⁴	Amsterdam ⁸⁵	Beč ⁸⁶	Štokholm ⁸⁷
Br.garaž. u centr grada	-	7	23	8
Br. park. mj. u javnim garaž. u	1750	2758	6960	1363

⁸⁴ <http://novovrijeme.ba/u-sarajevu-u-narednih-pet-godina-3-250-novih-parking-mjesta/> (pristupljeno 26. avgusta 2014. g.)

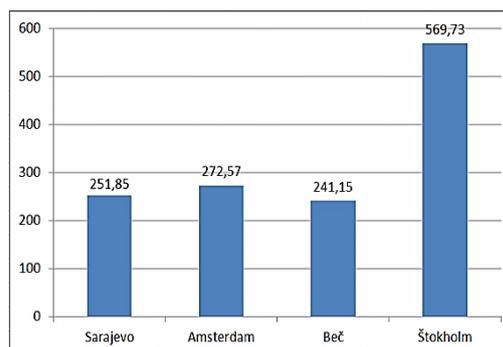
⁸⁵ http://www.bereikbaaramsterdam.nl/live/main.asp?display_framework=garaže&mode=overzicht01&selected_balkitem_id=860 (pristupljeno 26. avgusta 2014. g.)v

⁸⁶ Ivčić, B.: *Usporedba zagrebačkog prometnog sustava s prometnim sustavima europskih gradova*, Zelena akcija/FoE, Zagreb, 2008.

⁸⁷ Isto

centru				
Br.stanovn./parking mj. u centru grada	251,85	272,57	241,15	569,73

Kao što se može vidjeti na slici 2 i tabeli 3, u odnosu na broj stanovnika, **Sarajevo ima 56% više parking mjesta od Štokholma, 7,6% više od Amsterdama, a 4,2% manje od Beča.** Kada bi Amsterdam htio imati jednak omjer stanovnika i parking mjesta u garažama kao i Sarajevo, bilo bi mu potrebno da izgradi ukupno 210 parking mjesta. Kada bi Sarajevo težilo manjem broju parking mjesta po stanovniku, oslanjajući se na praksu iz Beča, onda bi trebalo da smanje broj parkinga za 74 mjesta. U nastavku ćemo težiti smanjenju broja parking mjesta u Sarajevu, primjenom odgovarajućih alternativnih rješenja oslanjajući se na iskustva drugih gradova.



Slika 2: Grafički prikaz broja stanovnika po jednom mjestu u javnim garažama u centru

Potrebno je istaći da se ne treba protiviti novim javnim garažama gdje one mogu pomoći u eliminiranju velikog broja vožnji automobilom u strogi centar Sarajeva. U planovima razvoja grada najavljena je gradnja novih javnih garaža sa dodatnih 3250 parking mjesta.⁸⁸ U tom slučaju Sarajevo bi imalo 5000 parking mjesta, odnosno 89 parking mjesta na jednog stanovnika.

Mogućnosti implementacije Park & Ride sustava

Park & Ride (P&R) sustav predstavlja jedan od najjednostavnijih načina smanjenja broja vozila koja dolaze u središte grada. Princip funkcionisanja je sljedeći: uz terminale javnog prijevoza, kao i uz njihova glavna stajališta izgradi se parkiralište na kojem vozači, dolazeći iz okolice grada ili iz perifernih naselja, parkiraju svoje automobile te javnim prijevozom nastavljaju put do središta grada. Na taj način se direktno utječe na smanjenje broja automobila u centru grada te se samim time rješava i problem mogućeg nedostatka parking mjesta u gradskim jezgrama. P&R parkirališta bi trebala da budu besplatna. Da bi ovaj sustav funkcionirao na zadovoljavajući način, potrebno je unaprijediti kvalitetu javnog prijevoza, a prvenstveno povećati prosječnu brzinu vožnje i frekventnost prijevoznih sredstava. U tu svrhu najefikasnije bi bilo onemogućiti osobnim automobilima da voze unutar žute trake namijenjene isključivo za vozila javnog gradskog prijevoza, jer time usporavaju javni prijevoz. To se vrlo jednostavno postiže gradnjom fizičke barijere koja se proteže po žutoj traci, što se u mnogim europskim gradovima pokazalo vrlo uspješnim.

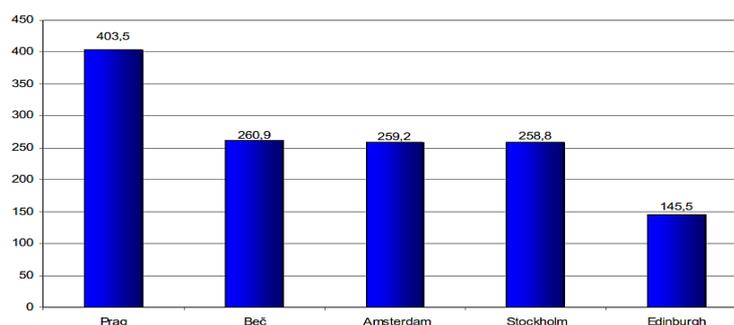
⁸⁸ <http://novovrijeme.ba/u-sarajevu-u-narednih-pet-godina-3-250-novih-parking-mjesta/> (pristupljeno 26. avgusta 2014. g.)

Za usporedbu broja parking mjesta na takvim parkiralištima u različitim gradovima, najrelevantniji način bi bio dovesti ih u vezu s brojem stanovnika koji žive u perifernim naseljima i okolnim mjestima jer to su ljudi koji su potencijalni korisnici P&R parkirališta. Međutim, takve podatke je skoro nemoguće dobiti pa u ovoj analizi uspoređujemo gradove s brojem parking mjesta u odnosu na broj stanovnika u samim gradovima. Što neki grad ima više stanovnika, u pravilu ima i razvijenije gospodarstvo i veće gravitacijsko područje, tako da je i usporedba gradova prema tom omjeru sasvim mjerodavna.

Tabela 4: P&R parkirališta

	Sarajevo	Amsterdam ⁸⁹	Edinburg ⁹¹	Štokholm ⁹³
Broj P&R parkinga	-	4	5	23
Broj parking mjesta na P&R parking.	-	2900	3146	3000
Br. stanovnika po jednom P&R mjes.	-	259,2	145,5	258,8

Slika 3: Broj stanovnika po jednom parking mjestu na P&R parkiralištu



⁸⁹ <http://www.edinburgh.gov.uk/internet/Attachments/Internet/Transport/Parking/EdinburghAreaP&R MapRevised 4.4.06-sr.pdf> (pristupljeno 27. avgust 2014. g.)

⁹⁰ Ivčić, B. 2008. *Usporedba zagrebačkog prometnog sustava s prometnim sustavima europskih gradova*, Zagreb: Zelena akcija/FoE

⁹¹ <http://www.midlothian.gov.uk/Article.aspx?TopicId=0&ArticleId=21552> (pristupljeno 27. avgust 2014. g.)
<http://www.edinburgh.gov.uk/internet/Attachments/Internet/Transport/Parking/EdinburghAreaP&R MapRevised4.4.06-sr.pdf>

⁹² <http://www.tsk-praha.cz/web/doprava/parkovistePRstav/> (pristupljeno 27. avgust 2014. g.)

⁹³ Ivčić, B. 2008. *Usporedba zagrebačkog prometnog sustava s prometnim sustavima europskih gradova*, Zagreb: Zelena akcija/FoE

Iz tabele 4 i slike 3 vidljivo je da svi analizirani gradovi, za razliku od Sarajeva, imaju razvijen Park & Ride sustav. Zanimljivo je primijetiti da Beč i Amsterdam imaju približno jednak iznos omjera iz tabele 3 i tabele 4 pa bismo na taj način mogli zaključiti da je u Sarajevu potrebno oko 1700 parking mjesta na P&R parkiralištima. Sasvim je jasno da je takva organizacija prometa neophodna kako bi se smanjio pritisak automobila na prometnice šireg centra svakog velikog grada.

Analiza masovnog javnog gradskog prijevoza

Javni gradski prijevoz putnika predstavlja jednu od najvažnijih funkcija savremenog grada, prevazilazeći čisto komunikacijski značaj. On treba da je dio politike razvoja grada i osnova zdravog življenja u gradu. Masovni javni prijevoz predstavlja glavnu alternativu velikom korištenju automobila. Javni gradski prijevoz putnika u Sarajevu se odvija autobusima, tramvajima i trolejbusima, a vrše ga firme CENTROTRANS (autobus) i GRAS (tramvaj, trolejbus, autobus).

Tabela 5: Tramvaj

	Sarajevo ⁹⁴	Amsterdam ⁹⁵	Beč ⁹⁶	Brisel ⁹⁷	Prag ⁹⁸	Štokholm ⁹⁹
Broj linija	6	15	29	19	30	9
Duljina linija (km)	22,9	200	221,5	203	142,4	113
Broj stanovnika po jednom metru duljine linije	19,1	4,1	8	5,7	8,7	8
Broj stajališta	30	500	1056	2124	606	108
Broj putovanja (mil./god.)	47,19	271	295,1	123,5	324,2	277
Broj putovanja po jednom	107,63	330,22	167	107	260,78	306,01

⁹⁴ http://bs.wikipedia.org/wiki/Sarajevski_tramvaji (pristupljeno 28. avgust 2014. g.) i publikacija: Federalni zavod za statistiku. 2013. „Kanton Sarajevo u brojkama 2013.“

⁹⁵ <http://en.gvb.nl/overgvb/bedrijfsprofiel/MaterieelEnCijfers/Pages/Netwerk.aspx> (pristupljeno 28. avgust 2014. g.) i brošura: <http://en.gvb.nl/overgvb/bedrijfsprofiel/jaarverslag/Documents/GVB-HOLDING2013-FINAL-LR.pdf> (pristupljeno 28. avgust 2014. g.) http://www.emta.com/article.php3?id_article=14

⁹⁶ <http://www.wien.gv.at/statistik/pdf/viennainfigures.pdf> (pristupljeno 28. avgust 2014. g.)

⁹⁷ http://en.wikipedia.org/wiki/Trams_in_Brussels (pristupljeno 28. avgust 2014. g.)

<http://www.stib-mivb.be/figures.html?l=en>

http://www.stib-mivb.be/iri/go/km/docs/resource/RA_2013/EN/sources/index.htm

⁹⁸ http://en.wikipedia.org/wiki/Trams_in_Prague (pristupljeno 28. avgust 2014. g.)

<http://www.dpp.cz/en/company-profile/>

www.dpp.cz/download-file/6145/annual_report_2012_en.pdf

⁹⁹ http://www.emta.com/article.php3?id_article=91 (pristupljeno 28. avgust 2014. g.) – zajednički podaci za lokalne vozove i tramvaje

stanovniku (god.)						
----------------------	--	--	--	--	--	--

Iz tabele 5 možemo vidjeti da najdužu tramvajsku mrežu ima Beč s 221,5 km, a najkraću Sarajevo s 22,9 km. Po broju tramvajskih linija predvodi Prag s 30 linija, a ponovno na zadnjem mjestu se nalazi Sarajevo. Po broju stanovnika po jednom metru duljine linije Sarajevo je ubjedljivo na posljednjem mjestu s 19,1 stanovnika po jednom metru tramvajske pruge, dok najgušću mrežu tramvajskih linija ima Amsterdam s 4,1 stanovnika po jednom metru. Kada gledamo broj stajališta Sarajevo je ponovo na posljednjem mjestu, dok Brisel ima enormnih 71 puta više stajališta od Sarajeva. Promatrajući prosječan broj putovanja koje jedan stanovnik grada obavi tramvajem u godini dana, uočava se da građani Sarajeva koriste tramvaj jednako često kao i građani Brisela, a manje od svih ostalih gradova. Šta nam ovaj podatak govori? Unatoč slabije razvijenoj tramvajskoj infrastrukturi (kraća mreža linija, manji broj linija, manje stajališta) tramvaj se u Sarajevu koristi isto kao i u Briselu. Taj podatak nam dovoljno govori o lošim uvjetima putovanja u sarajevskim tramvajima, to znači da je udobnost korištenja tramvaja u Sarajevu mnogo manja nego u Briselu. To nas navodi na zaključak da je potrebno obnoviti i modernizovati vozni park. Važno za napomenuti je da Sarajevo ovu tramvajsku mrežu i broj tramvajskih linija dobrim dijelom nadopunjuje prijevozom putnika trolejbusima. Mreža trolejbuskog prometa sastoji se od 33 stajališta, sa ukupno 6 linija.¹⁰⁰ Duljina linija iznosi 22,4 km, tako da imamo 19,6 stanovnika po jednom metru duljine. Ovim vidom masovnog prijevoza putnika se u Sarajevu preveze oko 18,4 miliona putnika godišnje, što znači da po jednom stanovniku godišnje imamo 42 putovanja.

Tabela 6: Autobus

	Sarajevo ¹⁰¹	Amsterdam ¹⁰²	Beč ¹⁰³	Brisel ¹⁰⁴	Prag ¹⁰⁵	Štokholm ¹⁰⁶
Broj linija	31	137 ⁽¹⁾	98	61	169	27
Duljina linija (km)	-	4032 ⁽¹⁾	717,3	470	769	10032
Broj stanovnika po jednom metru duljine	-	0,39 ⁽¹⁾	2,46	2,46	1,62	0,09

¹⁰⁰ http://bs.wikipedia.org/wiki/Sarajevski_trolejbusi#Linije (pristupljeno 29. avgust 2014. g.)

¹⁰¹ www.gras.ba/bs/ (pristupljeno 29. avgust 2014. g.)

¹⁰² <http://en.gvb.nl/overgvb/bedrijfsprofiel/jaarverslag/Pages/Jaarverslag-2013.aspx> (pristupljeno 29. avgust 2014. g.)

http://www.emta.com/IMG/pdf/barometer_report_2012_data_2009_.pdf

http://en.wikipedia.org/wiki/Amsterdam#Metro.2C_tram.2C_bus

¹⁰³ <http://www.wien.gv.at/statistik/pdf/viennainfigures.pdf> (pristupljeno 29. avgust 2014. g.)

¹⁰⁴ <http://www.emta.com/spip.php?article88> (pristupljeno 29. avgust 2014. g.)

<http://www.stib-mivb.be/figures.html?l=en#>

¹⁰⁵ <http://www.emta.com/spip.php?article83> (pristupljeno 29. avgust 2014. g.)

<http://www.dpp.cz/en/company-profile/>

http://www.dpp.cz/download-file/6145/annual_report_2012_en.pdf

¹⁰⁶ http://www.emta.com/article.php3?id_article=91 (pristupljeno 29. avgust 2014. g.)

http://app.lta.gov.sg/Itaacademy/doc/13Sep105-Pan_KeyTransportStatistics.pdf

linije						
Broj stajališta	-	3325 ⁽¹⁾	3626	-	1250	6000
Broj putovanja (mil./god.)	42,51	55 ⁽²⁾	167.1	87,6	310	297,1
Broj putovanja po jednom stanovniku (god.)	97	67 ⁽²⁾	94,6	75,9	249,4	328,2

(1) za metropolitansko područje (br. stanovnika 1.575.263)

(2) za gradsko područje (br. stanovnika 820.654)

Iz tabele 6 možemo vidjeti da Sarajevo ima ubjedljivo najmanji broj gradskih autobusnih linija. Zbog nemogućnosti pronalaska podataka o ukupnoj duljini gradskih autobusnih linija nećemo moći porediti ove podatke sa ostalim gradovima, a nećemo moći ni izračunati kolika je gustoća mreže autobusnih linija u Sarajevu. Jedini podatak koji je bio dostupan je broj pređeni kilometara godišnje, koji iznosi 8.469.000 km/god.¹⁰⁷ Međutim, možemo ustanoviti da najgušću mrežu autobusnih linija ima Štokholm i to s nevjerovatnih 0,09 stanovnika po jednom metru autobusne linije. Sarajevo se može pohvaliti brojem putovanja po jednom stanovniku jer se po ovoj karakteristici nalazi ispred Amsterdama, Beča i Brisela.

Tabela 7: Metro

	Sarajevo	Amsterdam ¹⁰⁸	Beč ¹⁰⁹	Brisel ¹¹⁰	Prag ¹¹¹	Štokholm ¹¹²
Broj linija	-	4	5	4	3 (+1)	7

¹⁰⁷ Federalni zavod za statistiku. 2013. „Kanton Sarajevo u brojkama 2013.“

¹⁰⁸ http://en.wikipedia.org/wiki/Amsterdam_Metro (pristupljeno 30. avgust 2014. g.)

<http://www.amsterdam.nl/gemeente/organisatie-diensten/dienst-metro/metro-tramnetwork/>

<http://www.noordzuidlijnkennis.net/wp-content/uploads/2013/05/metronetstudie.pdf>

¹⁰⁹ <http://www.wien.gv.at/statistik/pdf/viennainfigures.pdf> (pristupljeno 30. avgust 2014. g.)

¹¹⁰ (pristupljeno 30. avgust 2014. g.) <http://www.brussels.irisnet.be/about-the-region/regional-bodies/societe-des-transport-intercommunaux-de-bruxelles-stib>

http://www.mivb.be/iri/go/km/docs/STIB-MIVB/INTERNET/attachments/Bilan_2011/STIB_FiguresStatistics_2011.pdf

<http://www.stib-mivb.be/figures.html?l=en>

¹¹¹ <http://www.dpp.cz/en/company-profile/> (pristupljeno 30. avgust 2014. g.)

<http://www.dpp.cz/en/annual-reports/>

¹¹² http://sl.se/globalassets/rapporter-etc/sl_arsberattelse2013.pdf (pristupljeno 30. avgust 2014. g.)

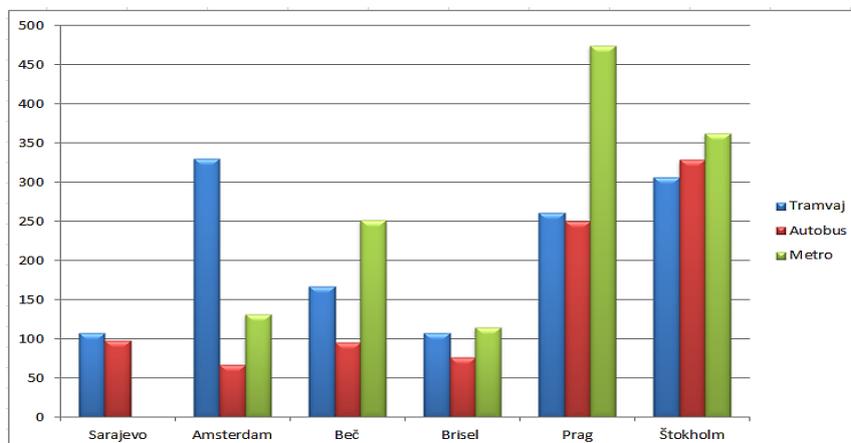
http://en.wikipedia.org/wiki/Stockholm_metro

<https://web.archive.org/web/20070927003006/http://www.sl.se/upload/rapporter/uploads/arsredovisning%20eng%202006.pdf>

Duljina linija (km)	-	117	74,2	39,9	59,4	105,7
Broj stanovnika po jednom metru duljine linije	-	7,01	23,81	28,94	20,93	8,56
Broj stajališta	-	52	101	59	57	100
Broj putovanja (mil./god.)	-	107,7	444,4	132,4	589,2	328
Broj putovanja po jednom stanovniku (god.)	-	131,2	251,5	114,7	473,9	362,4

Iz tabele 7 možemo vidjeti da je Sarajevo jedini grad koji nema metro ili sličan sustav javnog prijevoza (lightrail i sl.). U Pragu se, u odnosu na broj stanovnika, na 3 (+1 odobrena) metro linije preveze skoro duplo više putnika (473,9), nego u Sarajevu s tramvajem, trolejbusom i autobusom zajedno (246,63 putovanja). Ta činjenica se mora uzeti u obzir prilikom usporedbe korištenja tramvaja i autobusa, jer pojedini gradovi relativno slabije korištenje autobusa ili tramvaja kompenziraju s intenzivnijim korištenjem metro sustava. Međutim, u praksi je opravdano da samo višemilionski gradovi imaju osnovu za izgradnju metro sustava, tako da Sarajevo još uvijek nema potrebu za ovim vidom masovnog prijevoza. Sarajevo treba da radi na optimizaciji postojećih vidova javnog masovnog prijevoza (tramvaj i trolejbus), što bi bilo dovoljno za povećanje broja prevezenih putnika u godini.

Slika 4: Prosječan godišnji broj putovanja tramvajem, autobusom i metroom po jednom stanovniku.



Na slici 4 možemo vidjeti da Amsterdam ima najveći broj godišnjih putovanja tramvajem, dok Štokholm ima najviše godišnjih putovanja autobusom, a Prag metroom. Sarajevo ima isto godišnjih putovanja tramvajem kao Brisel, a više godišnjih putovanja autobusom od Amsterdama, Beča i Brisela.

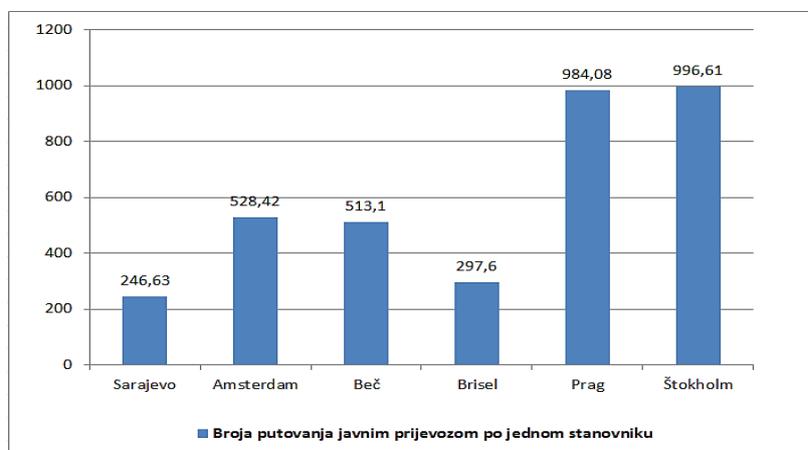
Da bismo dobili što vjerodostojnu usporedbu korištenja javnog prijevoza, dat je prikaz ukupnog broja putovanja svim sustavima javnog prijevoza (tabela 8 i slika 5).

Tabela 8: Ukupan prosječan broj putovanja sredstvima javnog prijevoza

	Ukupan br. putovanja javn. prijevoz. (mil.)	Br. putovanja javn. prijevoz. po jednom stanovniku
Sarajevo ⁽¹⁾	108,1	246,63
Amsterdam	433,7	528,42
Beč	906,6	513,1
Brisel	343,5	297,6
Prag	1223,4	984,08
Štokholm	902,1	996,61

(1) Sarajevu smo dodali i vrijednosti za trolebuski prijevoz

Slika 5: Grafički prikaz ukupnog prosječnog broja putovanja sredstvima javnog prijevoza



Na slici 5 možemo jasno vidjeti da građani Sarajeva najmanje koriste javni prijevoz u usporedbi sa ostalim gradovima u ovom istraživanju. Da bi se u Sarajevu povećao broj korisnika javnog putničkog prijevoza potrebno je povećati kvalitet prijevoza, a tu se prvenstveno misli na izgradnju nove tramvajske pruge, uvođenje žute razdjelne trake namijenjene samo za kretanje gradskih autobusa, uvođenje prednosti za tramvaje sinhronizacijom semaforских sustava na raskrižjima, poboljšanje informacionog sistema na stajalištima, te uvođenje lakošinskih tramvaja u gradski promet.

Potpuniju sliku o korištenju javnog prijevoza dobili bismo prikazom broja putničkih kilometara koje naprave stanovnici promatranih gradova, kao i njihovim udjelom u ukupnom broju putničkih kilometara ostvarenih svim vidovima prometa. Na žalost, nismo uspjeli dobiti uvid u te podatke, ali vjerojatno je da bi i oni dali slične rezultate.

Analiza taksi prijevoza

Taksi prijevoz je individualni javni prijevoz lica u vanlinijskom cestovnom prijevozu za koji je cijena prijevoza unaprijed određena, ili iznos za izvršenu uslugu utvrđuje se taksimetrom po cjeniku usluga. U pojedinim gradovima ima nezanemarlivu važnost u sustavu gradskog prijevoza i time direktno utječe na smanjenje korištenja osobnih vozila. Korištenjem taksi vozila stvaraju se jednake emisije ispušnih plinova kao i prilikom korištenja osobnih vozila, međutim, prednost korištenja taksija je smanjenje potrebe za parkirališnim mjestima. Dobro implementiran, uređen i jeftin taksi prijevoz može eliminisati potrebu za kupovinom osobnog automobila kod pojedinih građana, čime se opet smanjuje potreba za parkirališnim mjestima te problem zbrinjavanja osobnih automobila nakon isteka vijeka trajanja, kao i utrošak energije kod proizvodnje automobila.

Ključni i odlučujući faktor pri odluci o korištenju taksi prijevoza je cijena prijevoza. Cijena prijevoza se sastoji od cijene starta, cijene po prijeđenoj udaljenosti, te cijene čekanja. U sljedećoj tabeli prikazane su cijene taksi usluga u gradovima koji su dio ove analize.

Tabela 9: Cijene taksi usluga (KM)¹¹³

	Sarajevo ¹¹⁴	Amsterdama ¹¹⁵	Beč ¹¹⁶	Brisel ¹¹⁷	Edinbur ^g ¹¹⁸	Prag ¹¹⁹	Štokhol ^m ¹²⁰
Cijena starta	1,50	5,69	7,49	4,93	6,15	2,80	9,45
Cijena/km	1	4,18	2,8	3,55	3,99	1,82	2,52
Čekanje/h	10	78,31	54,77	59,10	55,35	25,2	95,97

Najbolji način za usporedbu taksi usluga je da ih dovedemo u vezu sa standardom građana u svakoj pojedinoj državi. Podaci o nacionalnom dohotku po glavi stanovnika nalaze se u tabeli 10. Na osnovu toga izračunati su indexi pomoću kojih je napravljena tabela 11. Dakle, ako je u državi „A“ nacionalni dohodak po glavi stanovnika veći nekoliko puta za određeni iznos, nego u državi „B“, tada cijene države „A“ možemo podijeliti s tim indexom kako bismo dobili ekvivalentan iznos za standard države „B“.

Tabela 10: Nacionalni dohodak po glavi stanovnika

	Holandija	Austrija	Belgija	V. Britanija	Češka	Švedska
Nacionalni dohodak (US\$) ¹²¹	43.750	43.850	40.680	35.620	25.480	43.960
Index (BiH=1)	4,53	4,54	4,22	3,69	2,64	4,55

¹¹³ Navedeni iznosi odnose se na dnevnu vožnju. U mnogim gradovima cijena vožnje po kilometru opada s povećanjem duljine vožnje. U tabeli su navedeni podaci za početnu vožnju, kada je cijena najviša. U Sarajevu je cijena po kilometru konstantna bez obzira na udaljenost. Cijene su u BAM, a proračuni su izvršeni na: <http://coinmill.com/> (1SEK = 0,21 KM; 1 EUR = 1,97 KM; 1 CZK = 0,07 KM; 1 GBP = 2,46 KM)

¹¹⁴ <http://www.sarajevotaxi.com.ba/> (pristupljeno 01. septembar 2014. g.)

¹¹⁵ <http://www.taxiamsterdam.nl/html/rates.html> (pristupljeno 01. septembar 2014. g.)

¹¹⁶ http://www.numbeo.com/taxi-fare/city_result.jsp?country=Austria&city=Vienna (pristupljeno 01. septembar 2014. g.)

¹¹⁷ http://www.numbeo.com/taxi-fare/city_result.jsp?country=Belgium&city=Brussels (pristupljeno 01. septembar 2014. g.)

¹¹⁸ http://www.numbeo.com/taxi-fare/city_result.jsp?country=United+Kingdom&city=Edinburgh (pristupljeno 01. septembar 2014. g.)

¹¹⁹ http://www.numbeo.com/taxi-fare/city_result.jsp?country=Czech+Republic&city=Prague (pristupljeno 01. septembar 2014. g.)

¹²⁰ http://www.numbeo.com/taxi-fare/city_result.jsp?country=Sweden&city=Stockholm (pristupljeno 02. septembar 2014. g.)

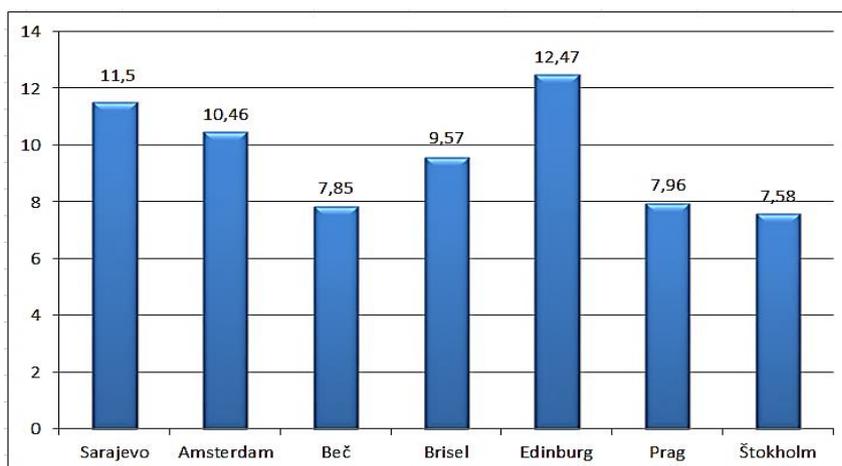
¹²¹ <http://data.worldbank.org/indicator/NY.GNP.PCAP.PP.CD> (pristupljeno 02. septembar 2014. g.)

Tabela 11: Cijene taksi usluga, uzevši u obzir nacionalni dohodak po glavi stanovnika [KM]

	Sarajevo	Amsterdam	Beč	Brisel	Edinburg	Prag	Štokholm
Cijena starta	1,50	1,26	1,65	1,17	1,67	1,06	2,08
Cijena/km	1	0,92	0,62	0,84	1,08	0,69	0,55
Čekanje/h	10	17,29	12,06	14	15	9,54	21,09

Iz tabele 11 možemo vidjeti da je cijena starta u Sarajevu skuplja od one u Amsterdamu, Briselu i Pragu, a skoro jednaka cijenama u Beču i Edinburgu. Najskuplji start je u Štokholmu. Cijena starta je jeftinija minimalno za 16% (Amsterdam) do maksimalnih 29,33% (Prag). U Štokholmu je cijena starta skuplja za 27,88%. U Sarajevu je cijena vožnje po kilometru skuplja u odnosu na sve gradove, osim za Edinburg, pa stoga imamo da je cijena vožnje po kilometru jeftinija minimalno za 8% (Amsterdam) do maksimalnih 45% (Štokholm), a u Edinburgu skuplja za 7,4%. Cijena čekanja po satu u Sarajevu je jeftinija za sve gradove osim za Prag, gdje je čekanje po satu za 4,6% jeftinije. U Beču je čekanje po satu skuplje za 17,08%, a u Štokholmu čak za 52,58% u odnosu na cijene u Sarajevu. Pošto se usluge čekanja često i ne koriste one stoga i nemaju veliki utjecaj na prosječnu ukupnu cijenu vožnje taksijem. Na slici 6 prikazane su cijene vožnje taksijem na udaljenosti 10 km (KM).

Slika 6: Cijena vožnje taksijem na udaljenosti 10 km [KM]



Možemo vidjeti da je ukupna cijena korištenja taksi usluga mnogo povoljnija u skoro svim analiziranim gradovima u odnosu na Sarajevo (samo je u Edinburgu skuplje). Najjeftinija cijena korištenja taksi usluge je u Štokholmu (za 34% jeftinije od Sarajeva).

Spuštanjem cijene taksi usluga, kao npr. onoj u Štokholmu, Beču i Pragu, građanima koji žele doći u centar grada automobilom u slučaju duljeg zadržavanja bilo bi jeftinije koristiti taksi nego osobni automobil jer ne bi morali plaćati parkiranje. Povećano korištenje taksi usluga donosi brojne prednosti, a neke od njih su: povećanje sigurnosti na cestama (posebno u kasnim noćnim satima jer bi alkoholizirane osobe više koristile taksi nego osobni automobil); smanjenje bespotrebnih gužvi u samom centru grada; smanjenje emisije otrovnih i zagađujućih plinova; ušteda na gorivu i dr.

Analiza biciklističkog prometa i duljine biciklističkih staza

Prilikom planiranja grada i gradskog uređenja često se zanemaruje u te planove ukomponirati promet, a posebno ovdje ispašta biciklistički promet koji je u mnogim gradovima Europe (npr. Holandija – Amsterdam) istinska alternativa korištenju osobnih vozila i gdje nije rijetkost vidjeti poslovne ljude koji idu na posao biciklom. Najzaslužnija za to je dobro razvijena biciklistička infrastruktura.

U tabeli 12 su prikazani podaci koji dovode u vezu duljinu biciklističkih staza i broj potencijalnih korisnika, odnosno broj stanovnika. Dakle, što je u nekom gradu taj omjer manji, razvijenost biciklističkih staza je veća.

Tabela 12: Duljina biciklističkih staza

	Sarajevo ¹²²	Amsterdam ¹²³	Beč ¹²⁴	Edinburg ¹²⁵	Prag ¹²⁶
Ukupna duljina (km)	16	400	1223	150	199
Broj stanovnika na jedan metar bic. staze	27,4	2,05	1,44	3,25	6,24

Zbog pretežno ravničarske konfiguracije terena, biciklistički promet u Sarajevu ima izrazito visok potencijal. Upravo zbog toga je najavljen i značajniji razvoj biciklističke infrastrukture od strane Gradonačelnika Sarajeva i direktora Direkcije za puteve Kantona Sarajevo. Posebno veliku ulogu u razvoju biciklističkog prometa ima i ponuda parking mjesta za bicikle. Kao što parkirališna mjesta potiču automobilistički promet, tako i parkirališta za bicikle potiču biciklistički promet. U centru Sarajeva postoji samo jedan parking za bicikle (ispred BBI centra) koji može da primi 20 bicikala, dok su pojedini gradovi odlučili mnogo jače poticati građane na korištenje bicikala, tako da Beč ima 233 parkirališta s ukupno 3.194 parking

¹²² <http://girodisarajevo.ba/giro-di-sarajevo/> (pristupljeno 03. septembar 2014. g.)

<http://www.klix.ba/vijesti/bih/uskoro-biciklisticka-staza-od-nedzarica-do-skenderije/131105062>

¹²³ <http://www.amsterdamtips.com/tips/cycling-in-amsterdam.php> (pristupljeno 03. septembar 2014. g.)

¹²⁴ <http://www.wien.gv.at/statistik/pdf/viennainfigures.pdf> (pristupljeno 03. septembar 2014. g.)

¹²⁵ http://download.edinburgh.gov.uk/transport/LTS_Ch6_8.pdf (pristupljeno 03. septembar 2014. g.)

¹²⁶ [http://doprava.praha-mesto.cz/\(l023c2qtb1wt435tidv5j55\)/zdroj.aspx?typ=2&id=68860&sh=1185842776](http://doprava.praha-mesto.cz/(l023c2qtb1wt435tidv5j55)/zdroj.aspx?typ=2&id=68860&sh=1185842776) (pristupljeno 03. septembar 2014. g.)

mjesta, dok je u Pragu moguće besplatno parkirati bicikl na svakom P&R parkiralištu.¹²⁷

ZAKLJUČAK

Iz svega navedenog dolazimo do saznanja da je promet osobnim automobilima u Sarajevu intenzivniji nego u ostalim gradovima koji su bili dio ove analize (Amsterdam, Beč, Brisel, Edinburg, Prag i Štokholm). To proizilazi iz činjenice da je razvijenost alternativnih vidova prijevoza (javni prijevoz, taksi prijevoz, biciklistički promet i Park&Ride sustav) znatno slabija nego u većini analiziranih gradova.

Svaki grad koji je bio predmet ove analize je okarakteriziran po svojim najboljim prometnim značajkama, a prilikom usporedbe uvidjeli smo da Sarajevo zaostaje u svakoj od njih.

U ovoj analizi vidjeli smo da svi europski gradovi poklanjaju veliku pozornost kvaliteti javnog prijevoza putnika i izgradnji biciklističke infrastrukture, te da je to smjer razvitka prometa kojeg treba slijediti Sarajevo. Ova analiza potkrepljuje naše tvrdnje iz kojih proizilazi da je potrebno uraditi sljedeće:

- unapređenje sustava javnog gradskog prijevoza,
- uvođenje Park&Ride sustava na perifernim dijelovima grada,
- smanjenje broja izgrađenih javnih garaža u centru grada i usmjeravanje njihove gradnje na obodu gradskog jezgra,
- izgradnja biciklističke staze i uvođenje većeg broja biciklističkih parkirališta u samom centru grada i
- izrada detaljne strategije razvoja prometnog sustava Sarajeva koja će se temeljiti na pozitivnoj praksi i iskustvima evropskih gradova i smjernica koje nudi Evropska Zelena knjiga o gradskom prometu.

LITERATURA

Mehanović, M.: *Planiranje ponude usluga u gradskom prometu putnika*, Fakultet za saobraćaj i komunikacije, Sarajevo, 2011

Green paper: *Towards a new culture for urban mobility*, European Commission, 2007.

European Federation for Transport & Environmen: „Greenhouse gas emissions from transport in the EU25“, UNFCCC, 2004.

Služba za lokalno poslovanje i razvoj: *Strategija razvoja Grada Sarajeva 2012-2020*, Sarajevo, 2012.

Bosanskohercegovački auto – moto klub: „Informacija o ukupnom broju registrovanih i prodatih novih motornih vozila u BiH“ BIHAMK, (pristupljeno 26. avgusa 2014. godine)

¹²⁷ <http://www.udi-praha.cz/rocniky/Yearbk03/texts/dttcha07.htm> (pristupljeno 03. septembar 2014. g.)

http://bihamk.ba/index.php?option=com_content&view=article&id=10&Itemid=147

Ministarstvo prostornog uređenja i zaštite okoliša KS: Registar emisija u zrak za područje Kantona Sarajevo za 2010. godinu – CETEOR d.o.o., Sarajevo, 2010.

<http://mpz.ks.gov.ba/sites/mpz.ks.gov.ba/files/Skraceni%20REGISTAR%20KS.pdf>
(pristupljeno 28. avgusta 2014. g)

Federalni zavod za statistiku: „Kanton Sarajevo u brojkama 2013.“ (pristupljeno 27. avgusta 2014. g.) <http://www.fzs.ba/Podaci/09.pdf>

Vienna City Administration: „Vienna in Figures 2014“. Vienna: Statistical analyses on the City of Vienna. (pristupljeno 29. avgusta 2014. g.) <http://www.wien.gv.at/statistik/pdf/viennainfigures.pdf>

**PROJEKAT
„ZAŠTITA I KONTROLA DJECE NA
INTERNETU“**

PROJEKAT „ZAŠTITA I KONTROLA DJECE NA INTERNETU“

Mart – Juni 2015.godine

Marela Martinovic

marela.martinovic@unvi.edu.ba

Na Sveučilištu/Univerzitetu 'VITEZ' održana je press konferencija na kojoj je javnost upoznata s rezultatima kampanje 'Zaštita i kontrola djece na internetu', koja je započela prije tri mjeseca u organizaciji naših Fakulteta informacijskih tehnologija i Fakulteta pravnih nauka.

Glavni koordinator projekta, doc.dr. Hadžib Salkić izrazio je veliko zadovoljstvo odzivom nastavnoga osoblja koje su naši edukatori u protekla tri mjeseca upoznavali s opasnostima koje sa sobom nosi korištenje interneta te s načinima izbjegavanja takvih opasnosti.

'U proteklom je periodu educirano oko 200 nastavnika, pedagoga, predstavnika Vijeća roditelja osnovnih i srednjih škola u bugojanskoj i travničkoj regiji' izjavio je doc. dr. Hadžib Salkić izražavajući, pri tome, razočaranje izuzetno slabim odzivom na edukaciju u kiseljačkoj regiji. 'Ovo je jako važan projekt koji je, prije svega usmjeren na roditelje djece i mladih školskog uzrasta. Namjera nam je bila da realizacijom ovih aktivnosti usmjerimo pažnju na prisutnost problema zloupotrebe interneta te da ih educiramo kako zaštititi i kontrolirati djecu koja koriste internet', dodao je glavni koordinator projekta.

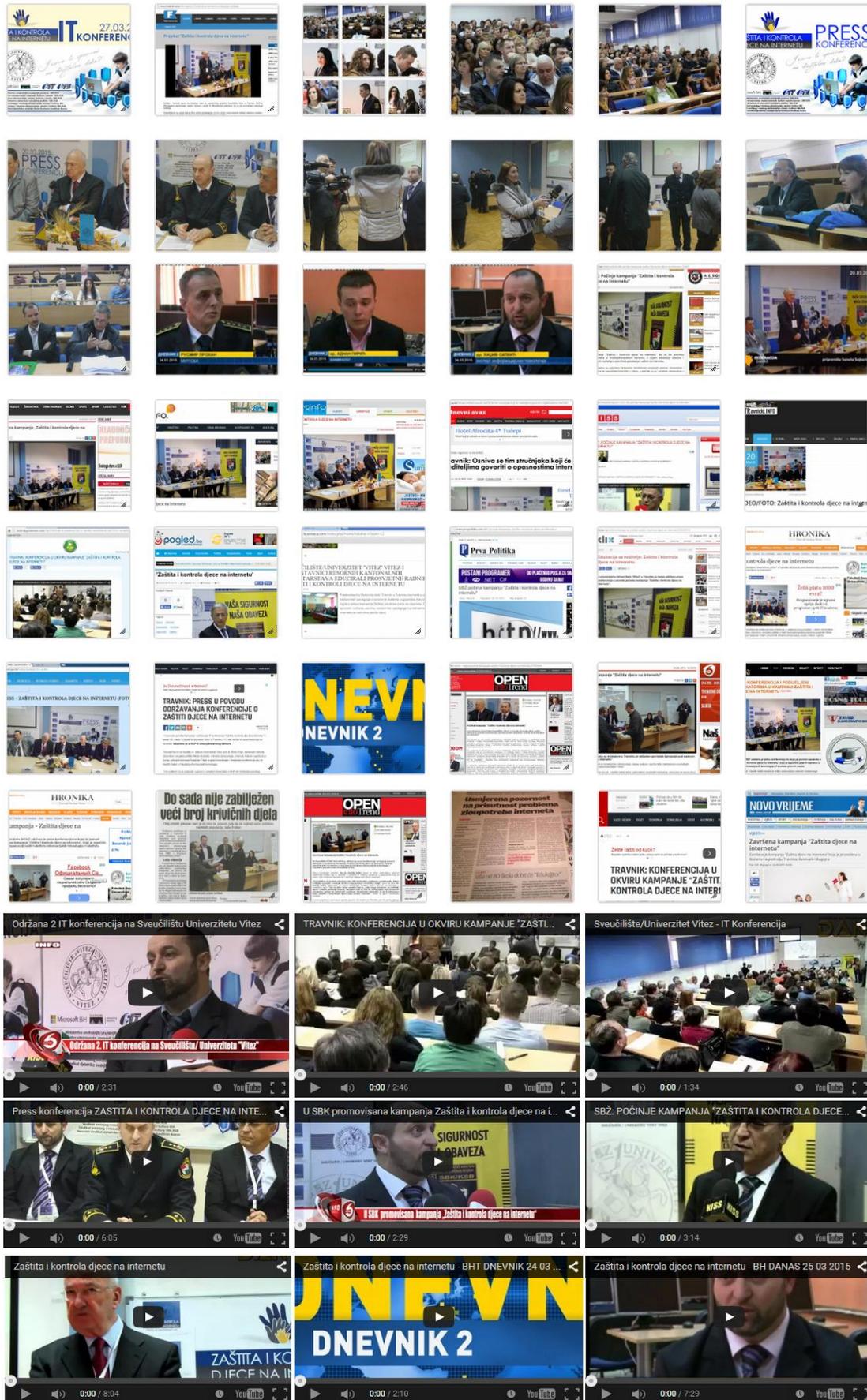
O ovom problemu s pravnog je aspekta govorio viši asistent na Fakultetu pravnih nauka, mr.sc. Adnan Pirić koji je u ovom projektu bio jedan od glavnih edukatora ispred Sveučilišta/Univerziteta. 'Ni o jednom problemu nikada nije ni prerano niti je o njemu previše govoriti, jer na taj način se bavimo prevencijom, a ne posljedicama što je uglavnom slučaj', poručio je prof. Šerif Šuvalić ispred Centra za mentalno zdravlje i Ministarstva zdravstva i socijalne politike SBK/KSB. Dodao je kako je ovom kampanjom zadan 'početni udarac' i ukazano na načine izbjegavanja opasnosti koje vrebaju pri korištenju interneta.

Zahvaljujući se predstavnicima osnovnih i srednjih škola na suradnji u projektu i pozivajući ih da kroz nastavni proces prenose stečena znanja o zaštiti i kontroli djece na internetu, na press konferenciji se obratila i Suzana Zec, inspektorica MUP-a SBK/KSB. Naglasila je kako će predstavnici MUP-a prisustvovati i roditeljskim sastancima na kojima se bude govorilo o ovoj temi, no, na raspolaganju su im i za bilo koju drugu temu koja zahtijeva uključenost policije, poručila je inspektorica.

Podsjetimo, kampanju 'Zaštita i kontrola djece na internetu' organiziralo je Sveučilište/Univerzitet 'VITEZ', a u suradnji s partnerima u projektu - kantonalnim Ministarstvom obrazovanja, znanosti, kulture i sporta, Ministarstvom zdravstva i socijalne politike, MUP-om SBK/KSB te poduzećem Microsoft BiH, KimTec Vitez i Baglama BiH.

Svi materijali vezani za ovu kampanju tiskati će se u časopisu "Eduk@tor", koji će biti podijeljen u više od 80 osnovnih i srednjih škola, a bit će dostupni i na web portalu www.unvi.edu.ba kao i www.fit.co.ba na kojem možete preuzeti i instalirati program za zaštitu djece na internetu.

Na kraju press konferencije edukatorima su uručeni certifikati kao potvrda završene obuke u sklopu spomenute kampanje.



SAVJETI

PRIJE NEGO ŠTO SVOM DJETETU DOZVOLITE DA IDE NA INTERNET (ONLINE) BEZ VAŠEG NADZORA, POBRINITE SE DA STE UTVRDILI GRUPU PRAVILA OKO KOJIH SE SVI MOŽETE SLOŽITI.

AKO NISTE SIGURNI ODAKLE DA POČNETE, EVO NEKIH PRIJEDLOGA O ČEMU DA RAZGOVARATE SA SVOJOM DJECOM KAKO BISTE IH NAUČILI DA NA SIGURNIJI NAČIN KORISTE INTERNET.

Podstičite svoju djecu da sa Vama podijele svoja iskustva sa interneta. Uživajte u internetu zajedno sa svojom djecom.

Naučite djecu da vjeruju svojim instinktima. Ako su uznemireni ili nervozni zbog bilo čega na internetu, trebaju Vam to reći.

Ako Vaša djeca koriste internet usluge za koje je potrebno ime za prijavu kako bi se identifikovali, pomozite im da odaberu to ime i pobrinite se da ono ne otkriva nikakav lični podatak o njima.

Insistirajte na tome da Vaša djeca nikada ne otkrivaju Vašu adresu, broj telefona ili druge lične podatke, uključujući i to gdje idu u školu ili gdje se vole igrati.

Naučite svoju djecu da je razlika između toga šta je dobro, a šta loše ista na internetu kao i u stvarnom životu.

Pokažite svojoj djeci kako da poštuju druge na internetu. Pobrinite se da znaju da se pravila dobrog ponašanja ne mijenjaju samo zbog toga što su za računom.

Insistirajte da Vaša djeca poštuju imovinu drugih na internetu. Objasnite im da je ilegalno kopiranje rada i djela drugih ljudi (muzike, video igara i ostalih programa) jednako kao da su ih ukrali iz prodavnice.

Recite svojoj djeci da se nikada ne trebaju sastajati uživo sa osobama koje su upoznali na internetu. Objasnite im da njihov prijatelj kojeg su upoznali na internetu možda nije ona osoba za koju se izdaje.

Naučite djecu da nije istina sve što pročitaju ili vide na internetu. Podstičite ih da Vas pitaju ako nisu sigurna.

Kontrolišite aktivnost svoje djece na internetu pomoću naprednog internet softvera. Roditeljska kontrola može Vam pomoći da uklonite štetne sadržaje, da pratite sajtove (sites) koje posjećuju Vaša djeca i da saznate šta tamo rade.

Tekst brošure predstavlja adaptaciju i lokalizaciju originalnog teksta na engleskom jeziku objavljenog na: . Ilustraciju teksta razvila . <http://www.microsoft.com/protect/LUNA/TBWA/SARAJEVO>

Smjernice za korištenje interneta za djecu različitog uzrasta

AKO VAŠA DJECA
KORISTE INTERNET KOD KUĆE,
VI VEĆ ZNATE KOLIKO JE VAŽNA
NJIHOVA ZAŠTITA OD
NEPRIMJERENIH SADRŽAJA
I KONTAKATA.

DJECA MLADA OD DESET GODINA

Alati poput **Windows Live Family Safety** (<https://fss.live.com/safety/default.aspx>) i **Roditeljski nadzor** (<http://www.microsoft.com/windows/windows-vista/features/parental-controls.aspx>) predstavljaju sastavni dio operativnih sistema Windows 7 i Windows Vista i mogu Vam pomoći u kreiranju sigurnijeg internetskog okruženja za Vašu djecu.

Djecu ovog uzrasta morate držati pod stalnim nadzorom. Možete koristiti alate za sigurnost na internetu kako biste im ograničili pristup pojedinim sadržajima, web stranicama i aktivnostima, kao i aktivno kontrolisati korištenje interneta od strane Vašeg djeteta, ali @man Vam preporučuje da, kada se radi o djeci ovog uzrasta, sjedite uz njih dok se služe internetom. Ovdje su navedeni neki od savjeta za kontrolu korištenja interneta za djecu uzrasta između dvije i deset godina:

1. Nikada nije prerano za uspostavljanje otvorene i pozitivne komunikacije s djecom. Preporučljivo je s djecom razgovarati o računarima i biti susretljiv prema njihovim pitanjima i radoznalosti.
2. Budite uz djecu ovog uzrasta sve dok ona provode vrijeme na internetu.
3. Postavite jasna pravila za korištenje interneta.
4. Zabranite djeci da osobama koje upoznaju na internetu ostavljaju lične podatke na internetu, poput pravog imena, adrese, broja telefona ili lozinki (password).
5. Ako se na nekoj web stranici traži unošenje imena radi prilagođavanja web sadržaja pojedincu, pomozite djeci da kreiraju nadimke u kojima neće biti sadržani njihovi lični podaci.
6. Koristite alate za porodičnu sigurnost kako biste kreirali odgovarajuće profile za svakog člana i tako olakšali filtriranje internet sadržaja.

**SVI ČLANOVI PORODICE
TREBAJU POSLUŽITI KAO
UZOR DJECI MLADEG
UZRASTA KOJA TEK
POČINJU KORISTITI
INTERNET.**

Više informacija o ovim alatima potražite na:

<https://fss.live.com/safety/default.aspx> (Porodična sigurnost na servisu Windows Live),

<http://www.microsoft.com/windows/windows-7/features/parental-controls.aspx>

(Roditeljski nadzor u okviru operativnog sistema Windows 7)

<http://www.microsoft.com/windows/windows-vista/features/parental-controls.aspx>

(Roditeljski nadzor u okviru operativnog sistema Windows Vista).

Zaštite djecu od agresivnih pop-up (skočnih) prozora uz pomoć alata za njihovo blokiranje koji je sastavni dio pretraživača Internet Explorera: <http://www.microsoft.com/windows/internet-explorer/default.aspx>

Smjernice za korištenje interneta za djecu različitog uzrasta

1. Preporučljivo je uspostaviti otvorenu i pozitivnu komunikaciju s djecom. Razgovarajte s djecom o računarima i budite susretljivi prema njihovim pitanjima i radoznalosti.
2. Postavite jasna pravila za korištenje interneta.
3. Zabranite djeci da osobama koje upoznaju na internetu ostavljaju lične podatke, poput pravog imena, adrese, broja telefona ili lozinki.
4. Ako se na nekoj web stranici traži unošenje imena radi prilagođavanja web sadržaja pojedincu, pomozite djeci da kreiraju nadimke u kojima neće biti sadržani njihovi lični podaci.
5. Koristite alate za porodičnu sigurnost kako biste kreirali odgovarajuće profile za svakog člana i tako olakšali filtriranje internet sadržaja. Više informacija o ovim alatima potražite na:
 - a. Windows Live Family Safety (<https://fss.live.com/safety/default.aspx>),
 - b. Windows 7 Parental Controls (<http://www.microsoft.com/windows/windows-7/features/parental-controls.aspx>),
 - c. Windows Vista Parental Controls (<http://www.microsoft.com/windows/windows-vista/features/parental-controls.aspx>).
6. Podesite postavke alata za porodičnu sigurnost na srednji nivo zaštite koji djelimično ograničava pristup nekim sadržajima, web stranicama i aktivnostima.
7. Računare koji su spojeni na internet postavite na vidljiva mjesta s kojih možete lako pratiti aktivnosti Vaše djece.
8. Zaštitite djecu od agresivnih pop-up (skočnih) prozora uz pomoć alata za njihovo blokiranje koji je sastavni dio Internet Explorera:
<http://www.microsoft.com/windows/internet-explorer/default.aspx>.

Podstičite djecu da Vam kažu ako ih nešto ili neko uznemirava ili im prijete. Sačuvajte prisebnost i objasnite djeci da neće imati problema zato što su vas obavijestili o tome. Pohvalite ih i posavjetujte ih da urade isto ako dožive nešto slično.

TINEJDŽERI IZRASTA OD 15 DO 18 GODINA

OVDJE SU NAVEDENI
NEKI OD SAVJETA ZA KONTROLU
KORIŠTENJA INTERNETA
OD STRANE TINEJDŽERA:

Tinejdžeri bi trebali imati gotovo neograničen pristup sadržajima, web stranicama i aktivnostima koje se nude na internetu. Oni već znaju dosta toga o internetu, ali ih roditelji i dalje moraju podsjećati o smjernicama za njegovo sigurno korištenje. Roditelji moraju biti u mogućnosti da pomognu svojoj djeci ovog uzrasta da shvate šta su neprimjerene poruke i da izbjegavaju rizične situacije. Preporučljivo je da roditelji podsjećaju tinejdžere na to koje lične podatke ne bi smjeli ostavljati na internetu.

1. Nastavite održavati otvorenu i pozitivnu komunikaciju koja se tiče upotrebe računara i interneta. Razgovarajte o njihovim virtuelnim životima, prijateljima i aktivnostima, na isti način kao i o drugim vrstama prijatelja i aktivnosti. Podstičite ih da Vam kažu ako ih nešto ili neko uznemirava ili im prijete. Također im recite da, ako im se čini da na internetu nešto nije u redu s nečim ili nekom osobom, obavijeste druge o tome.
2. Kreirajte listu kućnih pravila za korištenje interneta. Navedite koje web stranice su zabranjene, vrijeme kada se internet smije koristiti, informacije koje se ne smiju ostavljati na internetu, kao i uputstva o komunikaciji s drugim korisnicima interneta, uključujući i društvene mreže.
3. Računare koji su spojeni na internet postavite na vidljivo mjesto, a ne u dječju sobu.
4. Probajte i alate za kontrolu pristupa internetu (kao što su Windows Live Family Safety (<https://fss.live.com/safety/default.aspx>), Windows 7 Parental Controls (<http://www.microsoft.com/windows/windows-7/features/parental-controls.aspx>), Windows Vista Parental Controls (<http://www.microsoft.com/windows/windows-vista/features/parental-controls.aspx>) kao potencijalnu pomoć u roditeljskom nadzoru.
5. Zaštitite djecu od agresivnih pop-up (skočnih) prozora uz pomoć alata za njihovo blokiranje koji je sastavni dio Internet Explorera:
<http://www.microsoft.com/windows/internet-explorer/default.aspx>.
6. Saznajte koje web stranice posjećuju Vaša djeca, kao i s kim razgovaraju. Savjetujte ih da koriste chat sobe koje se nadziru, kao i da ne napuštaju javne chat sobe.

Vodič o sigurnosti na internetu za nastavnike

Glavne napomene

Internet je izvanredan alat koji djeca mogu koristiti za istraživanje i učenje o svijetu koji ih okružuje. Nastavnici također moraju imati na umu da je "tehnološka pismenost" učenika jedan od preduslova za njihovo buduće uspješno nošenje sa zahtjevima današnje umrežene ekonomije. Program [No Child Left Behind](#) predviđa da škola pomogne svakom učeniku u "prevazilaženju digitalnog jaza" i osigura "tehnološko opismenjavanje svakog učenika do završetka osmog razreda".

Iako internet našoj djeci nudi nevjerojatne mogućnosti za učenje, on ih istovremeno izlaže izvjesnim opasnostima i problemima, poput krađe identiteta, neprimjerenih sadržaja i seksualnih ponuda, zlostavljanja i uznemiravanja. Jasno je da obrazovanje koje vodi tehnološkom opismenjavanju mora uključiti i poduku o takvim opasnostima i zaštiti od njih, kao i razvijanje dobrih navika jednog građanina interneta (pojam kojim se označava član internetske zajednice), poput poštovanja privatnog vlasništva i prihvatanja osnovnih normi prihvatljivog oblika ponašanja u ophođenju s drugima.

Sigurnost na internetu - Seksualne ponude i ostale opasnosti

Prema studiji koju su proveli Nacionalni centar za nestalu i izrabljivanu djecu i Univerzitet u New Hampshireu, svako sedmo dijete je tokom korištenja interneta dobilo neku vrstu seksualnih ponuda. Iako su roditelji i nastavnici uglavnom svjesni ovog problema, djeca često ne shvataju ozbiljnost spomenute opasnosti. U istoj studiji se navodi da djeca vjeruju da 43% ovih ponuda dolazi od drugih tinejdžera, dok 66% djece ovakve ponude nisu uplašile niti uznemirile.

Jasno je da edukacija o sigurnosti na internetu mora uključiti savjete o "sigurnom ponašanju" koje može pomoći u zaštiti djece od neželjenih vidova komunikacije i ponuda i podučiti ih o primjerenim "strategijama reagiranja" u ovim slučajevima, od čega je najvažnija ona koja se tiče obavještanja odraslih o situacijama neugodnim po djecu. Osim toga, djeca moraju biti svjesna važnosti zaštite ličnih podataka, poput imena, koliko imaju godina i koja im je adresa, te im se mora pomoći u razvijanju navika koje će umanjiti rizik koji sa sobom nose različite aktivnosti na internetu, poput pisanja blogova, uključivanja u društvene mreže itd.

Vodič o sigurnosti na internetu za nastavnike

Sigurnost na internetu - Zaštita od krađe identiteta i drugih finansijskih prevara

Učenici mogu biti i žrtve krađe identiteta i internetskih prevara. Prema podacima Savezne trgovinske komisije SAD-a, 5% žrtava krađe identiteta u 2006. godini bili su korisnici mlađi od 18 godina, dok su u najbrojnijoj skupini žrtava krađe identiteta u istoj godini bili korisnici starosne dobi od 18 do 29 godina.

Djecu je potrebno podučiti o važnosti opreznog korištenja ličnih podataka na internetu, posebno onih najvažnijih, poput matičnog broja građana i broja kreditnih kartica. Ona moraju shvatiti značaj posjedovanja kvalitetne lozinke (password), opasnosti koju predstavljaju virusi i načina prepoznavanja phishing prevara (lažnih poruka u kojim se korisnik navodi na otkrivanje ličnih podataka) i pharming napada (preusmjerenje konekcije s legitimne web stranice na neku lažnu web stranicu). Djecu treba obučiti da u virtualnom svijetu postanu snalažljivi, skeptični i osviješteni korisnici, a ne naivne žrtve osoba s kojima dolaze u kontakt putem interneta.

Internetska zajednica (internet citizenship) - Podsticanje odgovornog ponašanja tokom korištenja interneta

Prema studiji koju su proveli Nacionalni centar za nestalu i izrabljivanu djecu i Univerzitet u New Hampshireu, broj slučajeva uznemiravanja preko interneta porastao je za 50% između 2000. i 2006., a u 44 % njih, žrtve su uznemiravane od strane svojih vršnjaka. Studija organizacije PEW pokazala je da je trećina svih tinejdžera koji koriste internet bila žrtva nasilja preko interneta (cyber-bullying). Još neki od problema su: virtualne zajednice u kojima se podstiče antisocijalno ponašanje poput korištenja narkotika, kockanja i kladenja preko interneta, kao i rašireno nepoštovanje privatnog vlasništva.

Učenicima je potrebno objasniti da se pravila koja postoje u nevirtuelnom tj. "realnom" svijetu jednako tako uvažavaju i na internetu. Tu spada i poštovanje osjećaja i ličnog integriteta drugih korisnika interneta. Nasilje i uznemiravanje na internetu jednako su neprihvatljivi kao i isti vidovi ponašanja u školskom dvorištu i mogli bi biti i kažnjivi zakonom. Učenici koji su žrtve takvog ponašanja moraju znati kako da prijave takve slučajeve odraslima. Istovjetno, krađa je uvijek krađa, bilo da se radi o nezakonitom skidanju materijala s interneta ili krađi CD-a ili DVD-a iz dućana. Djeci i naročito tinejdžerima mora se skrenuti pažnja na važnost njihovog ličnog integriteta, kao i na činjenicu da se informacije koje iznose u sobama za chat i na društvenim mrežama nalaze u javnoj domeni i da mogu imati potencijalno negativan učinak na njih u kasnijim fazama života.

Korisni izvori informacija

Dodatne materijale o sigurnosti na internetu možete dobiti besplatno ili po simboličnim cijenama putem organizacija specijalizovanim za tu oblast:

i-SAFE www.isafe.org/channels/?ch=ed

WiredSafety www.wiredsafety.org/educators.html

NetSmartz www.netsmartz.org/overview/statepartnerships.htm

Dodatne informacije o edukaciji o sigurnosti na internetu možete pronaći na web stranici američke organizacije National Cyber Security Alliance <http://www.staysafeonline.info/>

Ovako će Vaše dijete
sigurno surfati na internetu



www.sigurnodijete.ba

Savjeti za roditelje
mlađe djece (do 10 godina)
za korištenje interneta



Sigurnodijete savjeti za roditelje mlađe djece (do 10 godina)

Na pitanje „Da li si ikada bio na internetu?” danas većina djece odgovara brzim „da”. Već osmogodišnjaci surfaju na internetu. Što su djeca i mladi stariji, to više vremena provode online.

Posebno roditelji mlađe djece postavljaju sebi pitanje: Kako mogu surfanje na internetu, chatanje i komunikaciju elektronskom poštom učiniti sigurnijim za moju djecu? Generalno je bitno da pratite Vaše dijete prilikom njegovih prvih posjeta internetu i da se nakon toga interesirate za aktivnosti Vašeg djeteta u mreži.

Pomoć i praktična uputstva u vezi sa savjetima možete pronaći na www.sigurnodijete.ba. Osim toga imate mogućnost da djelujete protiv problematičnih sadržaja tako što ih prijavite odgovornim organizacijama za pritužbe.

Preventivnu zaštitu nude sljedeći savjeti:

www.sigurnodijete.ba



1. Podržite djecu dok rastu uz svijet medija

Djeca moraju naučiti pravilan odnos prema internetu. Neophodna im je podrška roditelja i pedagoga kako bi mogli rasti uz svijet medija. Za osnovce je dovoljna pregledna ponuda stranica za igru i učenje koje mogu stalno posjećivati.

2. Uređivanje korisničkog računa i početne stranice

Uredite Vašem djetetu poseban korisnički račun sa ograničenim pristupom koristeći programske i sistemske postavke. Tamo možete podesiti postavke za tražilicu (browser) kako bi odgovarao potrebama djeteta. Kao početnu stranicu izaberite neku tražilicu za djecu ili omiljenu stranicu Vašeg djeteta.

3. Sastavite listu omiljenih stranica i pozitivnu listu

Za mlađu djecu obavezno morate ograničiti broj stranica koje dijete može posjećivati. U tražilici možete ili dodati odabrane stranice na listu favorita ili sami sastaviti tzv. „pozitivne liste“.

Time se mogu izbjeći greške pri unosu koje mogu dovesti do neželjenih rezultata. Pri tome birajte samo one stranice koje odgovaraju uzrastu Vašeg djeteta. Ukoliko zajedno sa Vašim djetetom skupljate zanimljive linkove, onda izbor postaje veći, a Vaše dijete malim koracima uči kako da se koristi internetom.



4. Zamijenite tražilicu

Djeca koja još idu u osnovnu školu ne bi se trebala sama koristiti uobičajenom tražilicom, već je neophodno da je zamijenite specijalnom dječijom tražilicom. Na taj način djeca mogu da steknu rutinu pretraživanja interneta, a da pri tome ne dođu u dodir sa problematičnim rezultatima. Dječije tražilice nude mnogo više od preporučenih linkova. Osim aktuelnih vijesti, igara ili recepata nude se specijalne informacije za djecu. Na nekim internetskim preglednicima moguće je pomoću samo nekoliko koraka podesiti tražilicu.

Uputstva možete naći na www.sigurnodijete.ba.

5. Obratiti pažnju na reklame

Iako se Vaša djeca interesiraju za heroje iz TV serija, za zvijezde ili skupljaju sličice: obratite pažnju da reklame i različite ponude ne zauzmu previše prostora. Odaberite uvijek stranice bez reklama ili one na kojima su reklame jasno označene. Ovo je posebno bitno uzimajući u obzir da djeca ne mogu razlikovati redakcijski sadržaj od reklama.

www.sigurnodijete.ba

6. Pažljivo postupati sa ličnim podacima

Često se na internetu traže lične informacije kao što su ime, hobi, adresa, navike korištenja interneta itd. Ozbiljno shvatite problem o zaštiti podataka i pojasnite svom djetetu da je veoma bitno da ne iznosi sve podatke o sebi. Ni u „stvarnom životu“ dijete ne bi podijelilo takve stvari sa strancem samo zato što je pitao.

Stoga morate insistirati na tome da se Vaše dijete dogovori s Vama u slučaju da se od njega traže lični podaci.

7. Sigurnije urediti komunikaciju na chatu

Mlađa djeca bi s drugima smjela komunicirati samo na moderiranim forumima. Takvi se chat forumi nadziru kako ne bi bili objavljeni diskriminirajući i uvredljivi prilozima. Tu djeca mogu naći vršnjake za razgovor koji imaju ista interesiranja. Zajedno sa svojim djetetom odaberite jednu takvu chat sobu i razgovarajte o tome šta se dešava na chatu.

www.sigurnodijete.ba

Postanite aktivni!

www.sigurnodijete.ba

Postanite aktivni i prijavite problematične internetske ponude kod nadležnih institucija ili organizacija! Kontrola je otežana s obzirom na raznovrsnost sadržaja na internetu i na mnoštvo ponuda koje su relevantne za zaštitu mladih. Stoga se sljedeće institucije angažuju za zaštitu djece i omladine na internetu i prate napomene korisnika.

www.sigurnodijete.ba

Šta mogu prijaviti instituciji?

Sadržaje na internetu koji predstavljaju opasnost za mlade. U takve sadržaje se ubrajaju interaktivne i komunikacione ponude kao npr. chat, instant messaging, tzv. berze za razmjenu podataka i dr. Pritužbe možete iznijeti putem formulara na www.sigurnodijete.ba

Šta mogu prijaviti udruženju?

Nelegalne i štetne sadržaje sljedećih internetskih usluga: world wide web, e-mail, spam, berze za razmjenu podataka, sadržaje za mobitel itd.

Pritužbe možete iznijeti putem formulara na www.sigurnodijete.ba

www.sigurnodijete.ba



NA WEBU SE MOŽEŠ
ZABAVITI NA RAZNE NAČINE. MOŽEŠ
RAZGOVARATI. MOŽEŠ SLUŠATI MUZIKU.
MOŽEŠ UPOZNATI NOVE PRIJATELJE IZ
CIJELOG SVIJETA. DA BI TI NA WEBU I
DALJE BILO ZABAVNO, PRIDRŽAVAJ SE
SLJEDEĆIH PET PRAVILA:

PRAVILO 1:
NE OTKRIVAJ SVOJE LIČNE PODATKE.

PRAVILO 2:
LJUDI MOŽDA NISU ONO ZA ŠTA SE
PREDSTAVLJAJU.

PRAVILO 3:
NE OTVARAJ PRILOGE (ATTACHMENTE)
KOJE SI DOBIO/LA OD NEPOZNATIH
OSOBA.

PRAVILO 4:
AKO NA INTERNETU IMA NEŠTO ZBOG
ČEGA SE OSJEĆAŠ NEUGODNO, RECI TO
ODRASLOJ OSOBI U KOJU IMAŠ
POVJERENJA.

PRAVILO 5:
OPASNO JE SASTAJATI SE SAM/A SA
NEPOZNATIM OSOBAMA KOJE SI
UPOZNAO/LA NA INTERNETU.

PRAVILO 1: NE OTKRIVAJ SVOJE LIČNE PODATKE

Postoje ljudi koji svoj život posvete tome da prikupljaju djeliće tvojih ličnih informacija. A to može biti opasno.

- Ne koristi svoje pravo ime na internetu. Budi kreativan/na i izmisli neko ime. Neka ti i tvoji roditelji pomognu.
- Nikada, ni po koju cijenu, nemoj odavati informacije o svojoj porodici ili sebi. Nikada nikome na internetu ne otkrivaj svoje ime, broj telefona, adresu, u koju školu ideš, ili gdje se voliš igrati, niti svoje lozinke (passworde) ili ostale privatne podatke.
- Nemoj na internetu s nepoznatim osobama razmjenjivati fotografije na kojima si ti ili članovi tvoje porodice.
- Ako održavaš web log (ili blog), onda ga održavaj anonimno. Nemoj praviti link sa svog bloga na bilo koje druge podatke ili stvari koje imaš na internetu.

PRAVILO 2: LJUDI MOŽDA NISU ONO ZA ŠTO SE PREDSTAVLJAJU

Postoje dvije osnovne vrste ljudi na internetu koje treba izbjegavati. Najlakši način da se riješiš ovih ljudi je da im kažeš da čuvaš sve svoje razgovore na računaru i da ćeš ih prijaviti.

- **Zlostavljač koji ne bira žrtvu** – Ova osoba može biti muško ili žensko. On ili ona ti se u život uvuče kroz chat sobe, koristi pogrdne izraze, govori o stvarima koje imaju seksualno značenje, i uopšteno je jeziv/a i ljigav/a i tjera te da se osjećaš loše i neugodno. Ne brini; ovi ljudi su uglavnom dosadni, glupi i nemaštoviti, jednostavno ne obraćaj pažnju na njih.

Ako ne odu, **prijavi ih**.

- **Pervertit** – Ovo je osoba koje se tvoji roditelji najviše plaše. On ili ona želi znati sve o tebi i pretvara se da ti je prijatelj. On ili ona će sačuvati svaku informaciju koju mu/njoj daš o sebi. Pervertit želi tvoj broj telefona, tvoju adresu, tvoju fotografiju – a iznad svega, želi da se sastane sa tobom. Moguće je da policija već traga za njim/njom, pa zato ovu osobu odmah prijavi.

Fotografije na kojima se nalaziš ti ili članovi tvoje porodice ne razmjenjuj s nepoznatim osobama na internetu.

PRAVILO 3: NE OTVARAJ PRILOGE (ATTACHMENTE) KOJE SI DOBIO/LA OD NEPOZNATIH OSOBA

Ako otvoriš datoteke, linkove ili priloge od nepoznatih osoba, može se desiti da otvoriš i virus, ili da na računar prebaciš (download) štetan softver, fotografiju čiji sadržaj će te uznemiriti, ili nešto drugo što bi ti moglo pokvariti dan. Čak i ako prilog dobiješ od nekoga koga znaš, još jednom provjeri s tom osobom da ti je ona to zaista poslala, kako bi bio/la potpuno siguran/na prije nego što otvoriš prilog.

PRAVILO 4: AKO NA INTERNETU IMA NEŠTO ZBOG ČEGA SE OSJEĆAŠ NEUGODNO, RECI TO ODRASLOJ OSOBI U KOJU IMAŠ POVJERENJA.

Osjetiš li strah ili bojazan na internetu, uvijek to reci roditeljima, učitelju, nastavniku ili onoj odrasloj osobi kojoj vjeruješ. Ako neko, s kim razgovaraš na internetu, učini da se osjećaš nelagodno ili te uznemiri, nikada nemoj odgovoriti toj osobi. Ako se uplašiš, ti ili tvoji roditelji definitivno trebate pozvati policiju. I zapamti, ako na internetu vidiš nešto zbog čega se osjećaš neugodno, uvijek možeš jednostavno ugasiti računar.

PRAVILO 5: OPASNO JE SASTAJATI SE SAM/A SA NEPOZNATIM OSOBAMA KOJE SI UPOZNAO/LA NA INTERNETU

Ljudi koje nisi upoznao/la u stvarnom životu za tebe su stranci. Oni mogu biti divni ljudi. Mogu biti i dosadni. Mogu biti i zabavni, ili čak ljudi, loši ili ona vrsta ljudi koje je opasno poznavati. Nije dobra ideja sastajati se uživo s nekim koga si upoznao/la na internetu.

Međutim, ako zaista želiš uživo upoznati prijatelja sa interneta:

- Uvijek imaj na umu da neko koga si upoznao/la na internetu možda nije onaj ko se čini da jeste, ili ona osoba za koju se predstavlja. Zapamti da neko koga si upoznao/la u chat sobi možda uopće nije dijete, već je u stvari starija odrasla osoba.
- Jedan od tvojih roditelja ili tvoj odrasli rođak treba da ide sa tobom i da sa tobom ostane sve vrijeme.
- Sastani se sa tom osobom na javnom mjestu, gdje ima puno ljudi i ostanite tu. Nemoj sa tim strancem ići nigdje sam/a.
- Ne dopusti da te nepoznata osoba nagovori da uradiš bilo što kod tebe izaziva i najmanji osjećaj nelagode.



Ovako možeš sigurno surfati!



Savjeti za mlade za sigurno surfanje na internetu

Sigurnodijete savjeti za mlade

Sigurnodijete savjeti za mlade

Smatraš da je internet „prokleta“ dobra stvar, ali nekada ne znaš kako da se snađeš u mnoštvu informacija i mogućnosti koje nudi WWW? Osim toga često si nesiguran/-a u vezi sa količinom podataka o sebi koje smiješ objaviti u forumima i tokom chata? Ili si vidio/-la na internetu stvari koje su te uznemirile? Skupili smo nekoliko savjeta o ovim i drugim temama koji će od tebe napraviti eksperta za internet!

1.

Nemoj se nikada sam sastajati s drugim ljudima

koje si upoznao/-la na chat-u, na društvenim mrežama ili putem jednog od instant messenger-a, a koje nikada nisi vidio/-la. Jednostavno, ne možeš znati ko je osoba iza monitora s kojom razgovaraš. Trinaestogodišnja Ena može u stvarnosti biti 60-godišnji Emir ili 17-godišnji Dario. Ukoliko želiš da upoznaš drugu osobu, onda povedi sa sobom odraslu osobu. Više informacija možeš naći na www.sigurnodijete.ba !

2.

Ponašaj se fer na internetu

Nije uredu nekoga vrijeđati ili širiti ružne informacije o nekoj osobi na forumima, na chatu ili putem SMS-a. Neugodni ili brutalni snimci koji se postavljaju na videoportalima poput Youtube-a nisu nimalo smiješni. Ukoliko si sam nešto slično doživio/-la ili primijetio/-la stručni naziv za to je „cyberbullying“ onda se usudi i razgovaraj s nekim o tome (npr. sa roditeljima, nastavnicima,...). Postoji i mogućnost da nekoga prijaviš, jer je kažnjivo ciljano maltretirati druge ljude. Sve informacije o cyberbullying-u možeš pronaći na www.sigurnodijete.ba !

3.

Nemoj odavati lične podatke na internetu (ime, adresu, broj telefona, fotografije ili lozinke)

Često se ne zna šta će se desiti sa tim podacima. Ukoliko ipak želiš da kreiraš profil u jednoj od društvenih mreža, kao što je facebook, onda podesi postavke na profilu tako da ga samo tvoji prijatelji mogu vidjeti. Važno: Uvijek vodi računa o tome koje informacije o sebi odaješ na internetu. Trebao/la bi ujedno informisati roditelje o tome da si član neke društvene mreže. Naime, na takvim portalima postoje informativne stranice za tvoje roditelje.

4.

Budi skeptičan/-na prema informacijama koje nađeš na internetu

Na internetu svako može objaviti nešto što ne mora nužno biti tačno. Često se ne zna izvor informacija i ko ih je postavio na internet. Najveća i najpopularnija online-enciklopedija www.wikipedia.org nudi mnoge zanimljive informacije, ali budi kritičan/-na prema njima. Često ti može pomoći ukoliko informacije sa interneta porediš sa knjigama koje se bave istom tematikom. Tek tada možeš biti siguran/-na da su informacije tačne i da ih možeš koristiti, npr. za školu. Korisne tražilice i linkove možeš naći na www.sigurnodijete.ba .

5.

Ponude na internetu koje se čine zanimljivim i besplatnim mogu koštati veoma mnogo novca

Zamisli da si na internetu otkrio/-la stranicu sa zanimljivim muzičkim hitovima, slikama i melodijama za mobitel. Odjednom moraš napisati svoj broj telefona. Ovdje budi veoma oprezan/-na: Cijena se često ne vidi jer je napisana negdje sitnim slovima. I prilikom prijavljivanja na stranice za pomoć pri izradi domaćih zadataka moraš biti izuzetno oprezan/-na i najbolje je da pri tome zatražiš pomoć roditelja.

6.

Nikada ne otvaraj mailove ili priloge uz mail
ukoliko ne znaš ko ih je poslao i šta sadrže

Najbolje je da ih odmah izbrišeš. Takozvani spam mailovi koje ti šalju nepoznate osobe jer su tvoju adresu pronašli negdje na internetu mogu biti problematičnog sadržaja: pozivaju te na kupovinu nekog proizvoda, žele doći do tvojih ličnih podataka ili sadržavaju viruse koji štete tvom računaru.



7.

Besplatno preuzimanje muzike i
filmova često nije dozvoljeno

U prodavnici CD-ova također moraš platiti najnovija izdanja, a legalni portali za preuzimanje kao npr. itunes, musicload itd. na internetu nisu besplatni. Ukoliko naiđeš na besplatnu ponudu, budi isprva skeptičan/-na, jer je kažnjivo posjedovati nelegalno preuzetu muziku, filmove itd.

8.

Ukoliko želiš da u društvenim mrežama ili
na videoportalima objaviš slike ili videozapise
na kojima se vide drugi ljudi, pitaj ih prethodno
da li smiješ



Svaki čovjek zadržava prava za svoju sliku, što znači da se njegova slika smije objavljivati samo uz njegovo odobrenje. Isto važi za „zaštićene“ sadržaje (tačnije: djela drugih, muziku, filmove, tekstove, grafike i dr.). Njihovo nedozvoljeno korištenje može te koštati.

9.

Ukoliko ti prilikom surfanja
internetom nešto zasmeta

npr. naiđeš na stranicu sa slikama ili tekstovima koji kod tebe izazivaju strah ili nelagodu onda razgovaraj sa odraslom osobom u koju imaš povjerenja i pokaži joj takve stranice. Ona može dalje djelovati i prijaviti stranice organizacijama koje primaju takve pritužbe na www.sigurnodijete.ba.

Kome se obratiti za pomoć?

- Ministarstvo sigurnosti BiH
Odsjek za borbu protiv trgovine
ljudima i ilegalne migracije ☎ 033/492-454
- Lokalni centar za socijalni rad
• Save the Children Norway ☎ 033/550-531
- NVO MFS-EMMAUS ☎ 033/263-385
- www.sigurnodijete.ba

Kome prijaviti?

- Lokalna policijska stanica ☎ 122
- Federalna uprava policije ☎ ☎ ☎ 033/261-300
033/261-301
- Uprava policije Republike Srpske ☎ ☎ ☎ 051/331-164
- Policija Brčko Distrikta ☎ ☎ ☎ 049/233-200
- Krimolovci ☎ ☎ ☎ 080/020-505
- www.sigurnodijete.ba



Surfaj sigurno!

Pridružite nam se u borbi protiv
dječije pornografije i pedofilije!
Zaštite svoje dijete i posjetite
www.sigurnodijete.ba

Savjeti za mlade za
sigurno surfanje na internetu



 **MINISTARSTVO
SIGURNOSTI**
www.msb.gov.ba

 **FEDERALNA
UPRAVA POLICIJE**
www.fup.gov.ba

 **POLICIJA
REPUBLIKE SRPSKE**
www.mup.vladars.net

 **POLICIJA
BRČKO DISTRIKTA**
www.policijabdbih.gov.ba

 **MEDUNARODNI FORUM
SOLIDARNOSTI - EMMAUS**
BOSNA I HERCEGOVINA
www.mfs-emmaus.ba

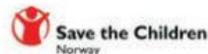
 **METABH**



 **Microsoft**

 **klicksafe.de**

 **OAK
FOUNDATION**

 **Save the Children
Norway**

MICROSOFT FAMILY SAFETY

mr. sc. Mahir Zajmović¹, mr.sc Almira Salkić²

Fakultet informacionih tehnologija, Sveučilište/Univerzitet „Vitez“ Vitez

mahir.zajmovic@unvi.edu.ba, almira.salkic@unvi.edu.ba

SAŽETAK

Family Safety predstavlja uslugu roditeljskog nadzora koja omogućava roditeljima da odrede sadržaj koji njihova djeca mogu da vide na mreži i kontakte sa kojima ona mogu da komuniciraju korištenjem usluga Windows usluga za chat (Messenger).

UVOD

Kao roditelj sigurno znate mnogo više od svog djeteta o stvarima s kojima se ono prvi put susreće u životu. Računari su jedan od primjera gdje gotovo sigurno nije tako. Čak i ako su računari vaša struka, vaše će dijete i dalje biti u prednosti zbog specifičnog načina na koji se njime koristi i područja interesa koje vjerojatno s njime ne dijelite. Zato uvijek preporučujemo korištenje softvera za roditeljsku kontrolu. Najrasprostranjeniji operativni sistem Windows od verzije Vista ima vlastiti softver namijenjen zaštiti djece na Internetu.

Usluga Family Safety obuhvata:

- a) Filtriranje sadržaja
Roditelji mogu da preciziraju Web lokacije koje njihova djeca mogu da pregledaju, i po kategorijama sadržaja, i po URL adresi.
- b) Izvještavanje o aktivnostima
Roditelji mogu da biraju da li žele da (na mreži ili putem e-pošte) pregledaju izvještaje o Web lokacijama koje su njihova djeca posjetila ili pokušala da posjete.
- c) Ograničenje korištenja aplikacija
Roditelji mogu da izaberu da li njihova djeca mogu da koriste određene usluge na mreži.
- d) Upravljanje kontaktima
Ukoliko je djeci dozvoljeno da koriste Windows Live usluge, roditelji mogu da izaberu kontakte s kojima djeca smiju da komuniciraju korištenjem ovih usluga.

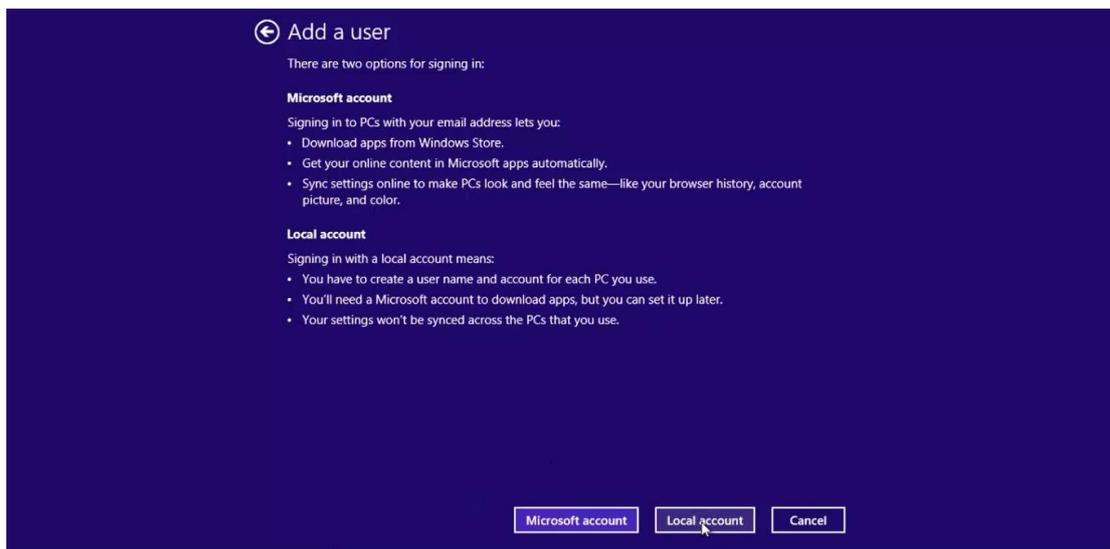
Djeca mogu da traže od svojih roditelja da im dozvole pristup blokiranim web lokacijama ili kontaktima. Usluga Family Safety ne dijeli podatke o aktivnostima djeteta na mreži sa drugim proizvodima ili uslugama. Roditelji i djeca će primati e-mailove u sklopu uobičajenog načina funkcionisanja usluge.

SISTEMSKI ZAHTJEVI

- Operativni sistem: Windows Vista SP2, Windows 7, Windows 8, Windows 8.1, Windows Server 2008 R2
- Web preglednik: Internet Explorer 6, Chrome 2, Firefox 2.0, Opera 10, Safari 3.0

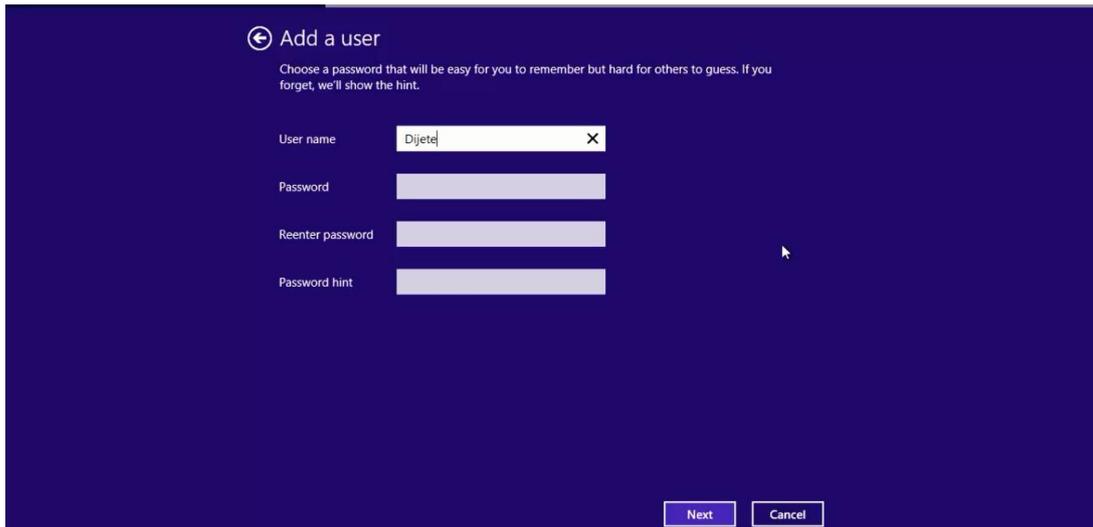
FAMILY SAFETY – KORAK PO KORAK

Prvi korak koji je potrebno uraditi jeste da kreiramo ograničeni korisnički račun (npr. „Dijete“). Potrebno je da pokrenemo Control Panel te izaberemo opciju User Accounts. Windows 8 dozvoljava kreiranje korisničkog računa na osnovu Microsoft-ovog računa. To je račun koji koristimo za prijavu na Microsoft-ove servise (OneDrive, Hotmail, Office 365 itd.). Ukoliko ne želimo da na ovaj način kreiramo korisnički račun, potrebno je da kliknemo na „Local account“ te unesemo podatke za korisnički račun.



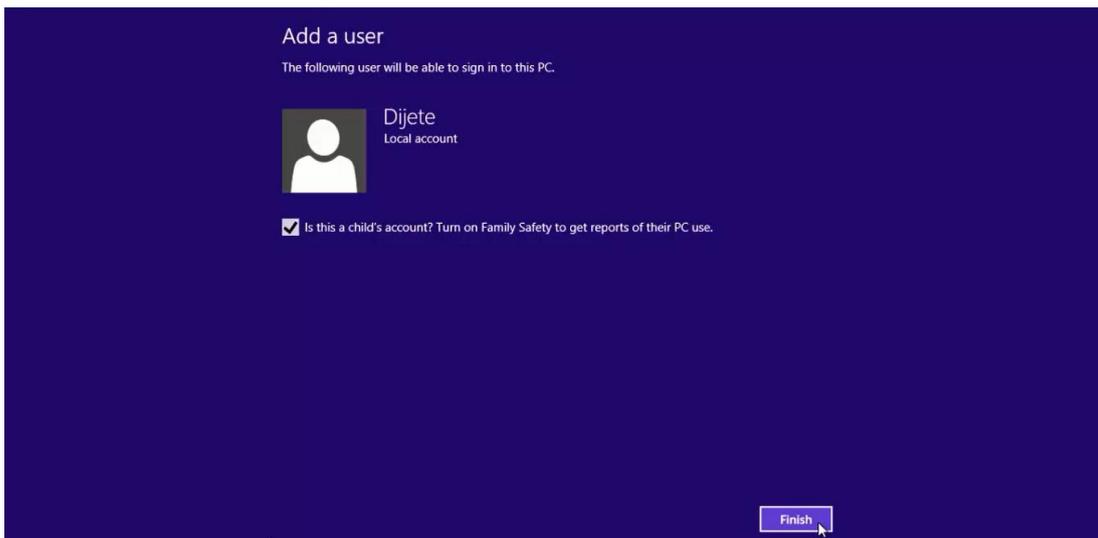
Slika 1. Kreiranje novog korisničkog računa

Kreiramo korisnički račun pod nazivom „Dijete“. Lozinku možemo unijeti ali ista nije obavezna kod kreiranja korisničkog računa.



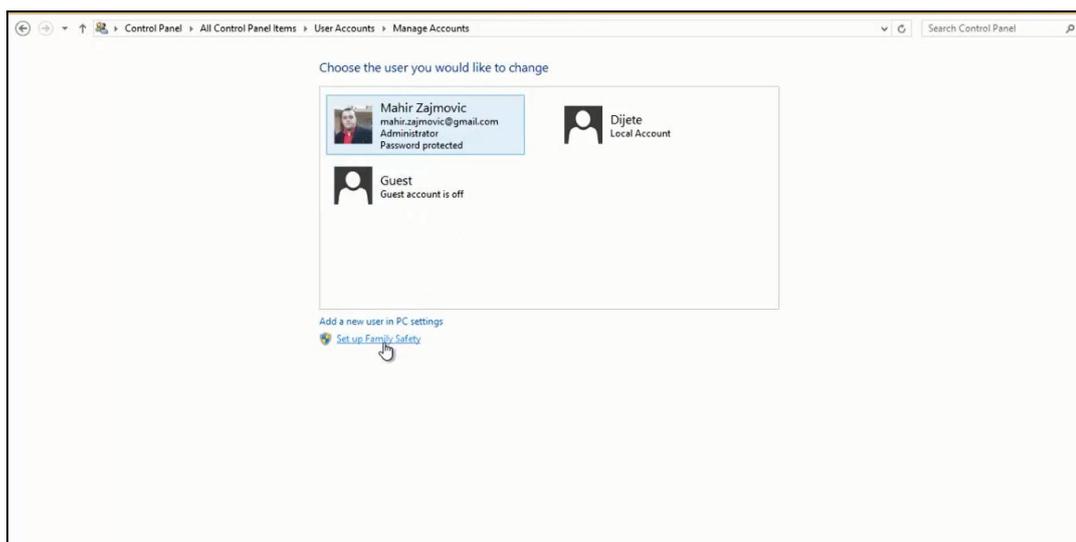
Slika 2. Kreiranje novog korisničkog računa

Nakon što smo kreirali korisnički račun „Dijete“ potrebno je za isti označiti da se radi o „child“ account-u.



Slika 3. Kreiranje novog korisničkog računa

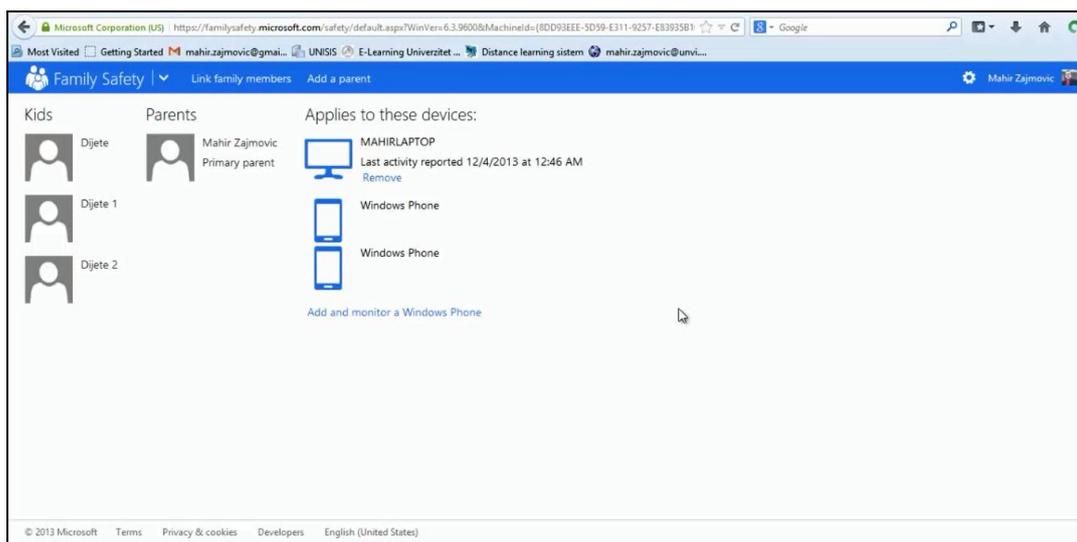
Potrebno je kliknuti na gumb „Finish“ kako bismo završili sa kreiranjem novog korisničkog računa. Dobijemo potvrdu da je korisnički račun kreiran. Zatim biramo opciju „Set up Family Safety“ kako bismo po odredili sadržaj koji ovaj korisnički račun može otvarati.



Slika 4. Family Safety – podešavanje

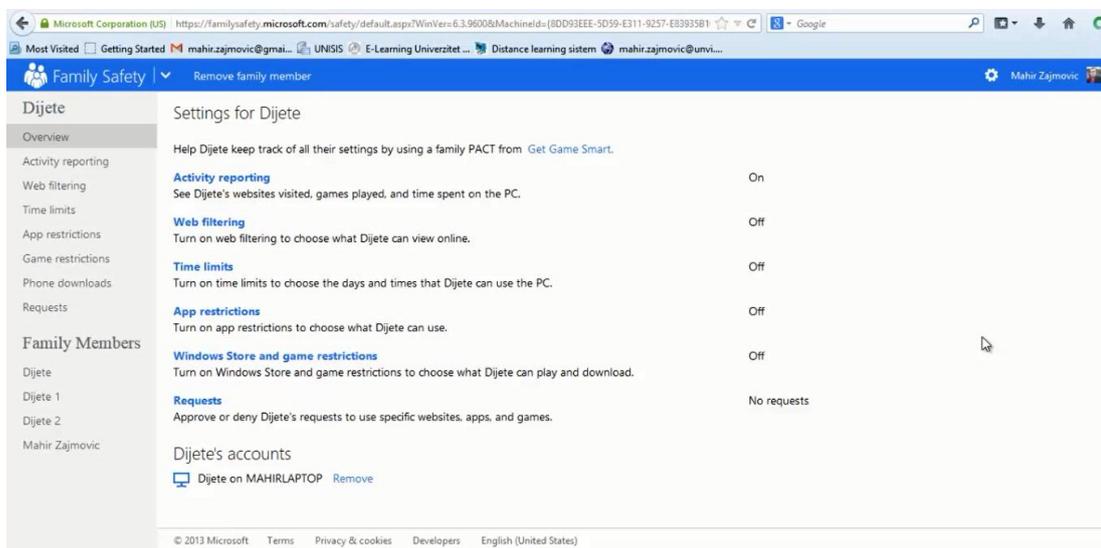


Slika 5. Family Safety – podešavanje



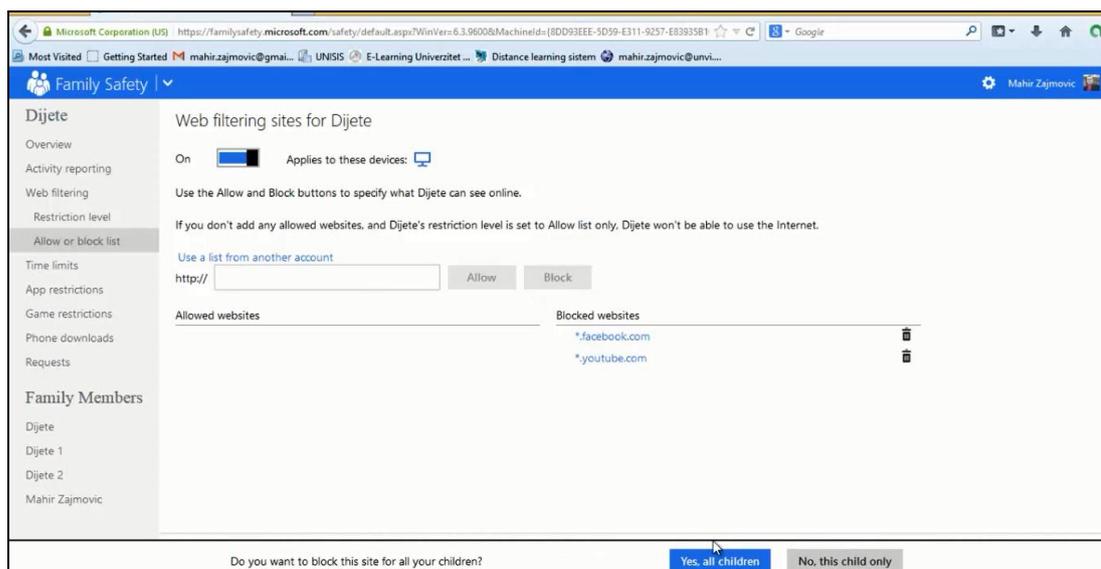
Slika 6. Family Safety - Web aplikacija

Slika 6 prikazuje sve „kids“ account-e: Dijete, Dijete 1 i Dijete 2, te „parent“ account: Mahir Zajmovic. Također možemo vidjeti sve urađaje na kojima je bio prijavljen (ulogovan) „parent“ account. Ovdje izaberemo „child“ account Dijete na nastavljamo sa unosom ograničenja za ovaj korisnički račun.



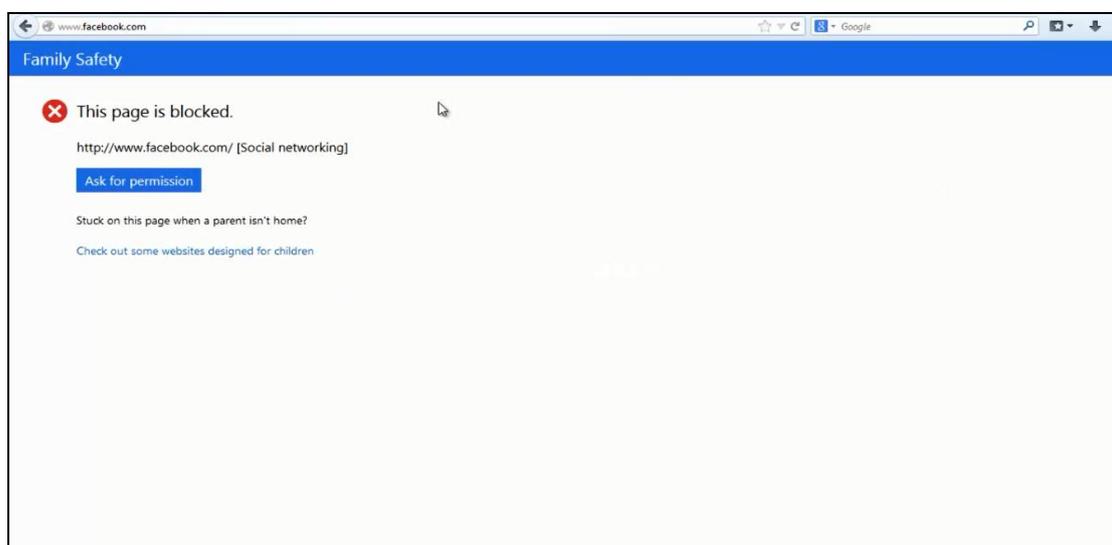
Slika 7. Family Safety - Web aplikacija

Ono što ćemo uraditi jeste da ćemo ovom korisničkom računu onemogućiti korištenje web stranica: facebook.com i youtube.com. Sve stranice koje želimo onemogućiti stavljamo u „block“ listu.



Slika 8. Family Safety - Web aplikacija

Ukoliko korisnički račun „Dijete“, nakon što smo uradili ove restrikcije, pokuša da otvori neku od web stranica koja je u „block“ listi dobit će poruku kao na slici 9.



Slika 9. Family Safety - blokirana web stranica

ZAKLJUČAK

Korištenjem usluge Family Safety možemo da vršimo „monitoring“ nad svim korisničkim računima za koje smatramo da to trebamo i uraditi. Ovo se posebno odnosi na roditelje i djecu, jer na ovaj način svojoj djeci možemo da onemogućimo korištenje nepoželjnih web stranica ili pak da im ograničimo korištenje istih na način da kažemo kako dijete može koristiti npr. facebook smo vikendom. Osim onemogućavanja web stranica mi također možemo i onemogućiti korištenje određenih aplikacija koje su instalirane na računaru. Djeca mogu da traže od svojih roditelja da im dozvole pristup blokiranim web stranicama ili aplikacijama, a mi kao roditelji tu dozvolu možemo izdati da fizički ne budemo uz računar koji dijete koristi već jednostavno odaberemo opciju „Allow“ koristeći smartphone uređaj.

LITERATURA

- [1] <https://www.youtube.com/watch?v=skMjubdAUEY>
- [2] <http://windows.microsoft.com/hr-hr/windows/set-up-family-safety#set-up-family-safety=windows-8>
- [3] http://en.wikipedia.org/wiki/Microsoft_Family_Safety
- [4] <https://www.lol.ba/files/dokumenti/Zastita.pdf>
- [5] <http://www.microsoft.com/bih/family-safety/>

SOFTVER ZA PREPOZNAVANJE LICA

Nermina Konjalić, BA

Sveučilište/Univerzitet „Vitez“ u Vitezu, Bosna i Hercegovina

nermina.konjalic@gmail.com

SAŽETAK

Sistemi za prepoznavanje lica postali su jedan od najvažnijih i najrasprostranjenijih biometrijskih mjera sigurnosti u posljednjih nekoliko godina u svijetu. Dva primarna razloga zašto je baš ova tehnologija u centru pažnje je prvo zbog mogućnost primjene ove tehnologije u različitim okruženjima i sistemima, bilo da se radi o sistemima za obradu video sadržaja, sistemi za lakše provođenje zakona i za uspostavljanje jačih i boljih sigurnosnih mjera. Tađer, jaka potreba za snažnim automatski sistemom je očita zbog raširene upotrebe foto-ID (Photo identification) za osobnu identifikaciju i sigurnosne mjere. Drugi razlog - Iako postoje pouzdane biometrijske metode identifikacije, kao što je skeniranje otiska prsta i skeniranje rožnjače, ipak se tehnika prepoznavanja lica pokazala mnogo učinkovitijom zbog činjenice što je jednostavnija i pogodnija za različite korisnike (user-friendly). Sam sistem od svojih korisnika ne zahtijeva da učine išta – njegovo rukovanje ne zahtjeva kontakt.

Ključne riječi: *Face recognition software, biometrija, biometrijske sigurnosne mjere zaštite, privatnost*

UVOD

„Biometrija (grč. bios – život, metron – mjera) predstavlja skup automatiziranih metoda za jedinstveno prepoznavanje ljudi temeljeno na jednoj ili većem broju njihovih fizičkih i ponašajnih karakteristika.

U informatičkoj tehnologiji se biometrijska autentikacija odnosi na tehnologije koje mjere i analiziraju fizičke (otisci prstiju, rožnica oka, prepoznavanje lica i sl.) i ponašajne karakteristike (rukopis, tipkanje, hod i sl.) čovjeka. Iako se biometrija prvenstveno koristi za potrebe autentikacije, ista se primjenjuje i u drugim područjima kao što je prepoznavanje korisnikovog govora u svrhu bržeg pisanja.¹²⁸

Dr Joseph J. Atick se smatra pionikom za ove tehnologije.

U zavisnosti od pristupa analizi biometrije postoje i razne podjele koje se u osnovi mogu svesti na dvije kategorije i to :

- fizička biometrija

¹²⁸ Croatian academic and research network & LSS (2006) „Biometrija“

- biometrija ponašanja

U tipove fizičke biometrije, a ujedno ono u čemu ćemo se baviti u ovom radu, spadaju:

- lice
- otisak prsta
- geometrija dlana
- šarenica
- mrežnica
- termogram lica i tijela
- DNK
- miris
- uho

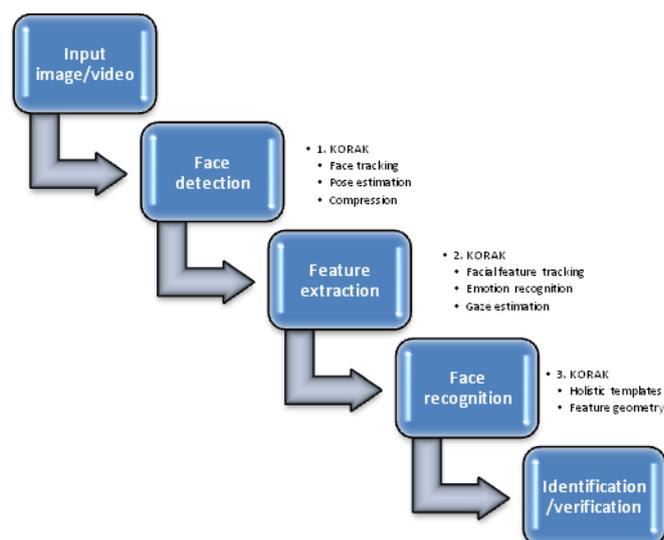
Fizički izgled je prvo što primjećujemo na osobama i na osnovu čega ih prepoznavamo u svakodnevnom životu. U ovom slučaju, pored ostalih tjelesnih karakteristika, primarnu ulogu ima izgled lica.

Klasični postupci identifikacije osoba prvenstveno se odnose na prepoznatljive lica. Postoji nekoliko načina dohvata fotografije neke osobe, a najčešći su korištenje kamere za snimanje u vidljivom spektru ili kamere koja pomoću infracrvenih zraka pravi uzorke lica. Sistem koji radi na principu vidljivog spektra pomoću kamere uzima fotografiju osobe i poredi je sa uzorcima spremljenim u neku od baza. Zanimljivo je da oni uzorci koji su promjenljive prirode poput izraza lica ili frizure. Također, postoje sistemi koji uzimaju uzorke u pokretu i analiziraju ih. Prepoznavanje osobe preko lica, kao biometrijske karakteristike, spada u tzv. nenametljive tehnike.

PRINCIP RADA

Ljudski mozak, već milionima godina evolucije i napretka, radi na procesu identifikacije i raspoznavanja lica. Za ljude, taj proces je relativno olakšan, dok za računare predstavlja izazov. Računari su projektovani da „vide“ i obrađuju informacije na različit način nego što to radi ljudski mozak. Da bi računar „vidio“ odnosno raspoznao lice, potrebno mu je da pređe nekoliko koraka, a svaki od njih sa sobom nosi jedinstvene i izazovne prepreke koje moraju uspješno biti pređene da bi proces bio korektno završen. Pogreške na svakom etapi se mogu akumulirati, te u konačnici smanjiti pouzdanost konačnog rezultata.

Glavni problem računara, kod procesa prepoznavanja lica, može se definisati na slijedeći način: datu mirnu fotografiju ili video identifikuj ili provjeri jednu ili više osoba u sceni koristeći spremljenu bazu lica.



Slika 10. Proces prepoznavanja lica

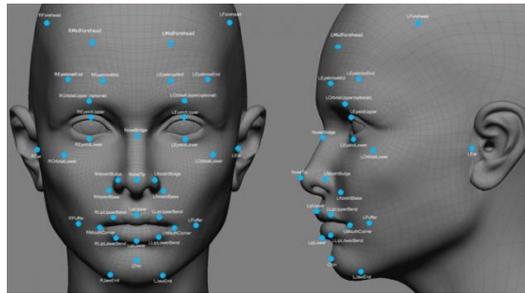
Princip rada svakog softvera za prepoznavanje lica, temelji se na nekoliko osnovnih koraka:

- 1) Pronalazak tj lociranje lica
- 2) Normalizacija fotografije
- 3) Pretraživanje baze podataka
- 4) Prikaz lica sa najslučajnijim karakteristikama

Kada je u pitanju prvi korak, sistemi procesiraju brojeve stoga prva etapa u prepoznavanju i autentikaciji lica je naučiti računar kako da pronađe lice u fotografiji, što je mnogo teži zadatak nego što se čini. Tamna pigmentacija, loša rasvjeta, niska rezolucija, različita lica i uglovi kamere mogu da numerički „sakriju“ lice. Gdje osoba vidi lice, računar može da vidi samo brojeve koje ne može razlikovati od pozadine osim ukoliko se ne koriste sofisticirani algoritmi. Pronalazak lica također znači izdvajanje lica od ostatka fotografije, a u slučaju videa, znači praćenje lica u pokretu kroz kadrove. Stoga, korištenje softvera koji u sebi imaju ukomponovane komplikovane i napredne algoritme, omogućava sofisticirano lociranje lica bez obzira na ugao fotografije/video, osvjetljenje i slično. Također, softver može izolirati nekoliko fotografija i izabirati najbolju kao uzorak za kasnije pretraživanje.

Prije nego se počne s procesom pretrage i podudaranja, lice ponajprije mora biti prilagođeno prema unaprijed utvrđenim pravilima, odnosno skupu podataka, postavljenim od strane Nacionalnog instituta standarda i tehnologija (National Institute of Standards and Technology – NIST). Posmatraču, ovaj skup podataka izgleda kao ravna, dobro osvijetljena fotografija lica gdje su oba oka otvorena i gdje lice nije izobličeno usljed neke facijalne ekspresije. Budući da većina fotografija lica nisu savršena, sam softver mora da normalizuje fotografiju.

Lice, čak i nakon normalizacije, je samo gomila podataka, ali svi ti podaci nisu neophodni da bi se ispravno izvršila podudarnost lica na fotografiji. Prikupljanje najvažnijih obilježja lica je matematička obrada signala koji koriste algoritmi. Upotrebljavaju ih kako bi pronašli i izolirali najkorisnije brojčane informacije ljudskog lica, informacije koje nude najveće razlike za varijacije među licima. Nakon što su sve fotografije, uključujući i fotografije u bazi podataka, prošle kroz ove prve tri etape, sistem je spreman da pronađe odgovarajuća lica.



Slika 11. Prepoznavanje specifičnosti lica

"Prepoznavanje" je posljednji korak automatskog prepoznavanja lica što podrazumijeva uspoređivanje novo dobijenih podataka nepoznatog lica s ranije poznatim podacima poznatih lica. Dalje, pojedinačni podaci lica se uspoređuju, identificiraju se razlike u podacima, a kada su podaci slični, vjerojatnost (rezultat) se prikazuje konačnom korisniku. Sofisticiranost i točnost ranijih algoritama su ključni za pružanje tačnih i usporedivih podataka.



Slika 12. „Face recognition“ sistem

BIOMETRIJA I SIGURNOST

Sigurnost danas postaje važno pitanje u našim životima, više nego ikada prije. Bilo da se radi o državnoj sigurnosti (nadzor granice) ili sigurnosti velikih kompanija i poduzeća, glavnu ulogu ima verifikacija identiteta.

Tragedije u cijelom svijetu, uključujući tragediju u Sjedinjenim Američkim Državama 2004. godine, razna bombardiranja i ono što mediji karakterišu kao teroristički napadima, su promijenili svijet i pokazali koliko su i najrazvijenija

društva ranjiva. Države i njihove vlade su u stanju visoke pripravnosti, pa na razne načine pokušavaju pronaći solucije kako spriječiti da se slične katastrofe od ponove.

Korporacije primjenjuju vrhunske sigurnosne mjere u svojim objektima. Fotografije terorista i drugih kriminalaca su lako dostupne i brzo se distribuiraju.

Danas, biometrija predstavlja rješenje za pojačavanje sigurnosnih mjera i svijesti, te se koristi da suzbija zločince i terorističke aktivnosti. Biometrija se koristi putem računara da bi se raspoznale fizičke i osobine ponašanja osoba. Ta obilježja se čuvaju putem računara i koriste kako dva oblika autentikacije; jedan-na-jedan i jedan-na-mnogi u odnosu na jedinstvene osobine. Popularni oblici biometrija su ruke, oči, glas i prepoznavanje lica. Svaki ima jedinstven obilježja koja ne mogu biti genetski umnožena. Međutim, svi oblici biometrija nisu usavršeni u smislu tačnosti.

Prepoznavanje lica se smatralo jednom od nižih formi biometrije, međutim vratilo se kao jedna goruća tema o sigurnosti. Od početka vremena, ljudi su se oslanjali na prepoznavanje lica kao način da se uspostavi i provjeri identitet druge osobe.

Tehnologija prepoznavanja lica nije mnogo drugačija. Korištenje softvera, računar je u stanju locirati ljudska lica na fotografijama, a zatim uskladiti ukupne uzorke lica u evidenciji pohranjenih u bazi podataka. Većina zemalja, zračnih luka, vlada i drugih javnih objekata je u potrazi za načinom povećanja sigurnosti, dodavanjem sistema za prepoznavanje lica kako bi se lakše i brže mogli identificirati teroristi, kriminalci, te drugi sumnjivi pojedinci. Ova tehnologija poboljšava uz korištenje odgovarajućih algoritama i različitim metodama kao što su neuronske mreže i princip analize komponente.



Slika 13. IDTECK Facial Recognition & Access Controller

PRIMJERI U PRAKSI

Kao prvi primjer može se navesti nedavni slučaj pokušaja otmice koji se dogodio u Beogradu. Korištenjem softvera za prepoznavanje lica pronađena je djevojčica i to preko društvene mreže Facebook. Budući da je djevojčica bila stara svega 2 godine, nije posjedovala svoj profil, nego su otmičari locirali djevojčicu preko fotografija koje su postavljali njeni roditelji. Stoga, u cilju očuvanja privatnosti i sigurnosti, potrebno je obratiti pažnju na sadržaj koji dijelimo na internetu.

„Troje otmičara iz Francuske je priznalo da su djevojčicu pronašli preko Facebooka, uz pomoć softwera za prepoznavanje lica, a plan im je bio njen DNK podmetnuti na sudu kako bi dokazali da bivši suprug jedne od otmičarki nije otac njezine kćeri. Upravo je Maša, od svih djevojčica koje su otkrili na društvenim mrežama, najviše sličila otmičarkinoj kćerki. Sumnja se da su planirali Mašu, nakon sudskog postupka, prodati pedofilima za 100 tisuća eura.“¹²⁹

Drugi primjer je prijava od strane Googlea o tome da jedan od njihovih korisnika na svom Gmail računu posjeduje dječiju pornografiju. Sama prijava od strane Googlea je zaista pohvalna i to je bilo neophodno uraditi, ali se postavlja pitanje privatnosti. Da li je onda istina da je privatnost na Internetu postala mit, da je privatnost koju smo nekada imali sada samo utopijska priča.

Kao treći primjer se može navesti Facebook-ov sistem za raspoznavanje lica „DeepFace“ za koji tvrde da ima tačnost podudarnosti od 97.25%. Za sada, ovaj projekat je i dalje u procesu istraživanja. Sistem radi na principu neuronske mreže, što znači da „uči“ kao i sam ljudski mozak. Na primjer, jedan neuron može da postavi pitanje: „Da li lice koje tražite ima tanke usne?“ – ukoliko je odgovor pozitivan, signal putuje jednom sinapsom, a ukoliko je odgovor negativan, signal traži drugu rutu. Međutim, ovaj razvoj tehnologije, iako vrlo ambiciozan i jako iskoristiv, može da sa sobom donese određene probleme. Vlada Njemačke je već izrazila svoju zabrinutost uvođenjem ove tehnologije i značajem koji će imati na njene korisnike. Smatraju da je to u suprotnosti sa europskim propisima vezanim za zaštitu podataka. „Johannes Caspar navodi da propisi Europske Unije koji se tiču privatnosti zahtijevaju da korisnici daju svoj pristanak prije nego što njihovi podaci budu pohranjeni, uključujući i podatke koji se koriste kako bi se omogućilo označavanje.“¹³⁰ Johannes Caspar je izjavio: „Potpuno je jasno je da svatko, čiji podaci će biti pohranjeni, mora dati svoj izričit pristanak.“ Ukoliko Facebook u potpunosti implementira „DeepFace“ da li to znači da će sve podatke svojih korisnika iskoristiti u jednom trenutku u komercijalne svrhe, što se ujedno može lako nadovezati na sljedeći primjer.

Ovaj primjer predstavlja novu etapu inovativnosti, a stiže iz kompanije Intel. Naime, koristeći Core i7 procesor za „multiperson“ upotrebu, ovaj stakleni holografski digitalni displej se aktivira nakon što mu priđe kupac. Iza displeja se nalazi radnja u kojoj se prodaju određeni artikli, a ti isti artikli se smjenjuju na staklenom displeju. Nakon što kupac priđe, kamera na vrhu displeja, uz pomoć senzora, registruje osobu kojeg je spola i visine i počene da prikazuje artikle namjenski za taj spol u visini koja im odgovara. Sistem posjeduje i meni da se promijeni spol ili da se određeni artikli putem bluetooth veze prebace na Vaš pametni telefon. Na taj način možete otići direktno do kase i pokazati koji su to artikli koje želite kupiti.

¹²⁹<http://dnevnik.hr/vijesti/svijet/beograd-otmicari-htjeli-malu-masu-prodati-pedofilima-za-100-000-eura---376475.html>

¹³⁰<http://onlinetrziste.com/2011/08/njemacka-postavila-pitanje-zakovitosti-facebook-ove-znacajke-za-prepoznavanje-lica/>



Slika 14. Intelov stakleni holografski digitalni displej

Slične tehnologije koriste i druge kompanije, ali s tim da Vam memorišu u bazi podataka, pa naredni put kada dođete u tu trgovinu biva Vam prezentovano nešto drugo iz ponude. U Americi, za trgovinske lance koji ovo koriste, što je poprilično rijetko zbog cijene, nema nekog posebnog zakona, dok vlada i vojska strogo moraju paziti kako prikupljaju informacije i ukoliko Vas i snime na sličan način, ponajprije moraju tražiti Vašu suglasnost.

ZAKLJUČAK

U budućnosti, tehnologije prepoznavanja lica će biti popularane i vrlo zahtijevne. Neuronske mreže i druge tehnologije će neprestano povećavati tačnost. Prenosni računari će omogućiti da ova tehnologija bude sveprisutna, pa čak i učinkovitija u velikim gužvama. Osim toga, ova tehnologija će biti ujedinjena s drugim oblicima biometrije kao što su glas i termalno skeniranje. U konačnici, osoba će moći kupiti stvari samo što se smiješi u kameru.

Također, ova tehnologija će se sve češće koristiti za sigurnosni pristup zgradama i računarima. Prepoznavanje lica će se koristiti za pristup automobilima i domovima. Jednako tako, prepoznavanje lica će raditi s bankomatima za autentifikaciju korisnika bankovnih računa, podudaranjem lica i prespajanjem na njihove bankovne kartice i pametne kartice. U sljedećih nekoliko godina, ova fenomenalna tehnologija će se pojaviti u važan aspekt matematike, nauke i tehnologije. Digitalne fotografije će pojačati jasnoću, pa će se srazmjerno tome kontinuirano povećavati tačnost.

Biometrijska tehnologija sa sobom donosi promjene u ekonomskom, društvenom, političkom i kulturnom polju. Korištenje ove tehnologije ima mnoge prednosti, ponajviše u kontekstu uspostavljanja sigurnosti i očuvanja iste, ali isto tako postoje određene mane koje mogu ozbiljno poljuljati dalji razvoj i upotrebu ove tehnologije.

Svjedoci smo kako u trenutnom okruženju, putem medija, saznajemo da kompanije ili vlade određenih zemalja na razne načine dolaze u posjed privatnih podataka, pa iste dijele dalje bez našeg znanja i odobrenja. Stoga se nameću određena pitanja

etičke prirode i treba se voditi briga da se u svakom trenutku primjenjuju moralni i pravni standardi.

Da li se korištenjem ove tehnologije krše zakonski zaštićena prava na privatnost? Ovaj problem se pojavljuje zbog zloupotrebe ove tehnologije što predstavlja direktno kršenje privatnosti. U kontekstu provedbe zakona, korištenje tehnologije biometrijskog prepoznavanja lica u svrhu praćenje na javnim mjestima, ne predstavlja se kao problem, ponajviše što još uvijek ne postoji zakon ili propis u vezi s tim.

REFERENCE

[1] FingerTec Worldwide Sdn. Bhd (2009). " Face Recognition Technology White Paper".

[2] Croatian academic and research network & LSS (2006) „Biometrija“

[3] Setiawan Hadi, Iping Supriana Suwardi, and Farid Wazdi:“Technology of Face Recognition for Security System“, 2006.

[4] <http://www.extremetech.com/extreme/178777-facebooks-facial-recognition-software-is-now-as-accurate-as-the-human-brain-but-what-now>

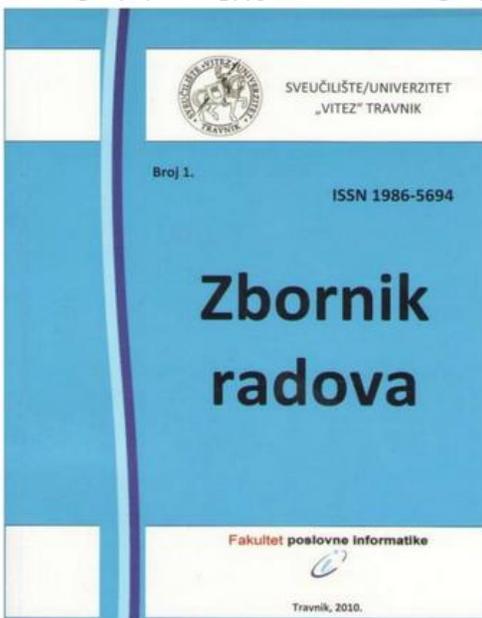
[5] <http://www.edge-group.info/hr-edge-group/sto-je-zaista-biometrija/2>
(26.03.2015.)

[6]<http://dnevnik.hr/vijesti/svijet/beograd-otmicari-htjeli-malu-masu-prodati-pedofilima-za-100-000-eura---376475.html> (26.03.2015.)

[7]<http://onlinetrziste.com/2011/08/njemacka-postavila-pitanje-zakonnosti-facebook-ove-znacajke-za-prepoznavanje-lica/> (26.03.2015.)

[8]<http://www.zdnet.com/article/ces-2010-intel-ceo-otellini-shows-off-holographic-glass-display-multipoint-smartphone-videoconferencing/>

PRETHODNA IZDANJA FIT-a S/U VITEZ



Univerzitet/Sveučilište Vitez
 Školska 23, 72270 Travnik
 Telefon: +387 (0) 30 509 754
 Fax: +387 (0) 30 509 758
 Mob.: +387 (0) 61 792 779
 E-mail: urednik@casopisedukator.info

Izdavač: Univerzitet/Sveučilište Vitez i
 Asocijacija za informacione tehnologije @zIT