

UNIVERZITET SINGIDUNUM
DEPARTMAN ZA POSLEDIPLOMSKE STUDIJE I MEĐUNARODNU
SARADNJU

Studijski program *Savremene informacione tehnologije*

ZAŠTITA DECE OD NEŽELJENIH INTERNET SADRŽAJA

Master rad

Mentor:
Prof. dr Gojko Grubor

Student:
Laslo Tot
Broj indeksa:
410534/2011

Beograd, mart 2013.

Zahvaljujem se svom mentoru, **Prof. dr Gojko Gruboru** jer je prihvatio da bude mentor kod izrade master rada koji predstavlja kontinuitet mog rada započetog izradom diplomskog rada pod njegovim rukovodstvom kao i na srsishodnoj saradnji i korisnim savetima.

Veliku zahvalnost dugujem **prof. dr Bošku Kovačeviću** u pregledavanju i korigovanju pitanja u anketi.

Želim se zahvaliti i **mr Silviji Tot** direktorici O.Š. „Majšanski put“ u Subotici i **Mariji Šifliš** oko pomoći kod podele anketnih listića.

“Today's parents and teachers want internet safety tools and skills. We must get more actively involved in our children's use of new media and in teaching them to use the internet safely.”

“Današnji roditelji i učitelji žele alatke i veštine za bezbednost na internetu. Moramo konstantno pratiti našu decu u korišćenju novog medija i podučavati ih da koriste internet bezbedno.”

Viviane Reding

SADRŽAJ

UVOD	- 7 -
Predmet istraživanja i obrazloženje rada	- 7 -
Ciljevi istraživanja	- 9 -
Hipotetički okvir	- 9 -
Metode istraživanja	- 9 -
Struktura rada	- 9 -
Kompjuterski Kriminali	- 10 -
1. BEZBEDNOST I ZAŠTITA DECE	- 11 -
1.1. Sajber zlostavljanje (Cyber bullying, Virtuelno zlostavljanje) .-	- 12 -
1.2. Dečja pornografija	- 13 -
1.3. Pedofilija	- 14 -
1.4. Internet zavisnost	- 15 -
1.5. Sporazum protiv internet-siledžija	- 16 -
1.6. Operacija Plava Orhideja	- 16 -
1.7. Operacija Delego	- 17 -
1.8. Ograničavanje dostupnih sadržaja	- 17 -
1.9. Zlatna pravila	- 19 -
2. TEORIJSKE OSNOVE	- 20 -
2.1. Content Control – Kontrola sadržaja	- 22 -
2.1.1. Terminologija	- 23 -
2.1.2 Pitanja	- 23 -
2.1.3. Istorija	- 24 -
2.1.4. Označavanje sadržaja	- 24 -
2.1.5. Korišćenje u javnim bibliotekama	- 25 -
2.1.6. Zaobilaženje filtera	- 25 -
2.1.7. Gateway baziran na rešenjima kontrole sadržaja	- 26 -
2.2. Internet Filter Review	- 26 -
3. ZAKONI	- 28 -
3.1. Pravilnik o kontroli interneta	- 28 -
3.2. Zakonska regulativa u Srbiji	- 29 -
4. TESTIRANJE RAZNIH PROGRAMA ZA FILTRIRANJE I NADGLEDANJE	- 30 -
4.1. Internet Filter Review	- 30 -

4.1.1.	Net Nanny	- 30 -
4.1.2.	CYBERsitter.....	- 31 -
4.1.3.	CyberPatrol.....	- 31 -
4.1.4.	MaxProtect	- 32 -
4.1.5.	FilterPak	- 32 -
4.1.6.	Netmop	- 32 -
4.1.7.	Safe Eyes	- 33 -
4.1.8.	WiseChoice.net	- 33 -
4.1.9.	Cyber Sentinel	- 34 -
4.1.10.	McAfee Parental Controls.....	- 34 -
4.2.	Access Control List (ACL) – Lista kontrole pristupa.....	- 34 -
4.2.1.	Bezbednosni modeli bazirani na ACL-u	- 34 -
4.3.	Proxy server	- 35 -
4.3.1.	Keširani (caching) Proxi server	- 35 -
4.3.2.	Mrežni (web) proxi.....	- 35 -
4.3.3.	Proxi za mrežu filtriranja sadržaja (Content Filtering Web Proxy) - 35 -	
4.3.4.	Anonimni (Anonymizing) proxi server – serveri za zaštitu privatnosti - 36 -	
4.3.5.	Neprijateljski (Hostile) proxi	- 36 -
4.3.6.	Sprečavani (Intercepting) proxi server.....	- 36 -
4.3.7.	Providni i neprovidni (Transparent and non-transparent) proxi server - 37 -	
4.3.8.	Prisiljeni (Forced) proxi	- 37 -
4.3.9.	Otvoreni (Open) proxi server	- 37 -
4.3.10.	Povratni (Reverse) proxi server.....	- 37 -
4.4.	Preskakač (Circumventor)	- 38 -
4.4.1.	U školama i kancelarijama	- 39 -
4.5.	Rizik prilikom korišćenja proxi servera za zaštitu privatnosti ..	- 39 -
4.5.1.	Proxi software-i	- 40 -
5.	REŠAVANJE PROBLEMA.....	- 42 -
5.1.	Proxy Plus.....	- 42 -
5.1.1.	Podešavanja za server računar:	- 43 -
5.1.2.	Podešavanja za klijent računar:	- 43 -
5.1.3.	Podešavanje programa (slika 4.):	- 44 -
5.2.	Webalizer – Log Analizator	- 52 -
5.3.	Crna lista (Blacklist).....	- 53 -
5.4.	Squid.....	- 53 -

5.5.	SquidGuard.....	- 54 -
5.6.	Network Guardian 2008	- 54 -
5.7.	Parental Lock Guard 1.1	- 55 -
6.	ISTRAŽIVAČKI RAD	- 56 -
6.1.	Rezultati istraživačkog rada.....	- 60 -
7.	VREDNOVANJE REZULTATA.....	- 72 -
7.1.	Zaključak	- 72 -
8.	LITERATURA	- 77 -

PREGLED SLIKA, GRAFIKONA I TABELA

Slike

<i>Slika 1</i> - Jedna od grupa: Svi koji mrze.....	12
<i>Slika 2</i> - Rezultat pretrage grupe „Svi koji mrze“.....	13
<i>Slika 3</i> - Prikaz gateway-a odnosno mrežne kapije	26
<i>Slika 4</i> – Ilustracija	28
<i>Slika 5</i> - Izgled programa Proxy+.....	42
<i>Slika 6</i> - Prikaz povezivanja dva računara na internet preko Proxy-a.....	43
<i>Slika 7</i> - Proxy+ Admin interface - Status info.....	44
<i>Slika 8</i> - Podešavanje programa.....	45
<i>Slika 9</i> - Non-ICP Parent Server.....	45
<i>Slika 10</i> - Cascading podešavanja.....	46
<i>Slika 11</i> - Sigurnosni interface.....	46
<i>Slika 12</i> - Sigurnosne klijente.....	47
<i>Slika 13</i> - Log fajlovi.....	47
<i>Slika 14</i> - Biranje formata log fajlova.....	48
<i>Slika 15</i> - NOD 32 plugin provera.....	48
<i>Slika 16</i> - www server podešavanje.....	49
<i>Slika 17</i> - Podešavanje lista pristupa.....	50
<i>Slika 18</i> - Objekti liste pristupa.....	50
<i>Slika 19</i> - Zabranjivanje pristup web stranici.....	51
<i>Slika 20</i> - Izgled zabranjenoj stranici.....	51
<i>Slika 21</i> - Webalizer – Log Analizator.....	52

UVOD

„Znaju li roditelji šta im deca rade na internetu, s kim se dopisuju, koje web stranice posećuju?

Decu najčešće upozoravamo da ne razgovaraju sa strancima, da budu oprezna kada im prilaze nepoznate osobe. Ali, kako im objasniti da se tako moraju ponašati i u svetu interneta. Od trenutka kada dete zakoračilo u virtuelni svet mora se znati kako ga zaštititi, jer uz tolike brojne prednosti, globalna mreža krije i mnoge opasnosti za najmlađe. Decu i maloletnike treba zaštititi od nasilnih i pornografskih sadržaja, neprimerenih poruka, od osoba koje pod zaštitom anonimnosti mogu zloupotребiti dečje poverenje, pokušati ih nagovoriti da odaju privatne podatke, razmenjuju slike, čak i da sami, bez pratnje roditelja, dođu upoznati online "prijatelja". Treba ih naučiti kako da sigurno i primereno koriste internet. Roditelji, nastavnici, institucije, stručnjaci, moraju preduzeti preventivne mere zaštite dece od nasilja i zlostavljanja putem interneta.“¹

Predmet istraživanja i obrazloženje rada

„ Ne postoji samo dobra ili samo loša tehnologija. U najvećem broju slučajeva, Internet se koristi za poslovanje, zabavu ili edukaciju, ali jednako nudi i neslućene mogućnosti za distribuiranje nelegalnog materijala ili sprovođenje nelegalnih aktivnosti. Upravo zbog internacionalnog karaktera ove mreže, efikasan način sprečavanja zloupotrebe zahteva zajednički angažman i odgovornost lokalnih vlada, policije, Internet industrije, školstva i roditelja, kao i njihovu blisku saradnju, kako na nacionalnom, tako i na internacionalnom nivou.

Ovo su reči Kalahana Kornaka, menadžera međunarodne organizacije Inhope (Internet Hotline Provides in Europe) za sprečavanje zloupotreba Interneta, koji je početkom juna 2010. gostovao u Beogradu.“²

U današnjem svetu Interneta, vreba mnogo opasnosti. Ljudi koji nemaju mnogo iskustva sa računarima i njegovim tajnama, mogu vrlo brzo i lako da postanu žrtve kiber(cyber) sveta. Nepromišljenim koracima, koji proizilaze iz neiskustva, mogu se naneti velike štete u razvoju svesti korisnika.

Internet kao servis sadržaja u mnogome doprinosi razvoju čovečanstva. Brzina širenja informacija je što je moguće najbrža. Brža je od svih medija današnjice. Lektorisanje sadržaja nije moguće kod svakog, zato se pored informacija, šire i

¹Zaštita dece na internetu, izvor: zena.hr (<http://www.poslovnazena.biz/porodica/zastita-dece-na-internetu-27-2785>)

²Aleksandar Arsenin, Sprečavanje zloupotrebe u Srbiji, referenca: www.netcentar.org (<http://www.internetservis.co.rs/zloupotreba/3.php?idtxt=134>)

dezinformacije. Pojedini slojevi korisnika interneta su jako osetljivi na kvalitet informacija. Javlja se potreba kontrolisanja pristupa sadržaju. Ova kontrola samo u retkim slučajevima može biti manualna. U današnje vreme su na raspolaganju automatizovane tehnike kontrole pristupa sadržajima. Ovaj rad obrađuje nekoliko tehnologija pristupa sadržaja.

„U Srbiji je 2009. proglašena za godinu zaštite dece na internetu, a nadležni kažu da roditelji treba više da razgovaraju sa decom o upotrebi interneta. Ministarka za telekomunikacije Jasna Matić je rekla da u Srbiji nema istraživanja koliko deca koriste internet, ali da iskustva Evropske unije pokazuju da tamo njih 90 odsto to čini svakodnevno, od kojih jedna trećina doživi neku vrstu internet zlostavljanja.

Matićeva kao glavni problem navodi što deca često ostavljaju na internetu lične podatke ili fotografije koji mogu biti zloupotrebljeni i da roditelji "moraju imati kontrolu gde njihova deca provode vreme i kome ostavljaju podatke".

"Nekad su roditelji deci pričali da se paze čike u parku koji nudi slatkiše, a danas čika može doći preko interneta", kaže ona.

"Internet deci dovodi ceo svet u sobu, ali i neke stvari koje nisu dobre, od kojih ih moramo zaštititi. Cilj ove godine je informisanje roditelja o novoj tehnologiji jer često znaju o internetu manje od svoje dece", istakla je Matićeva.

U tom cilju ministarstvo u saradnjom sa kompanijom Microsoft planira brojne edukativne akcije čiji je glavni cilj edukacija roditelja i nastavnika o opasnostima koje prete deci sa interneta.

Ambasadorka Češke Hana Hubačková istakla je da njena zemlja podržava kampanju srpskog ministarstva jer je tokom njihovog predsedavanja Evropskoj uniji jedan od prioriteta zaštita dece na internetu.

"Ovaj fenomen ne sme biti potcenjen. Internet nudi mnogo informacija do kojih možete doći sasvim slobodno, ali nedostaje dosta pravila", kaže ona.

"Potrebno je stoga da decu koja sve više vremena provode na internetu efikasno zaštitimo, a veliku ulogu imaju obrazovne institucije i roditelji", rekla je Hubačková.

Direktor za odnose sa javnim sektorom Microsofta Miloš Trkulja je istakao da njegova kompanija u svoje softverske pakete uključuje takozvanu "roditeljsku kontrolu" (parental control), odnosno opciju da roditelj određuje koliko vremenski njegovo dete može da pristupi internetu i kojim sadržajima. Promoter kampanje, muzičar Momčilo Bajagić Bajaga rekao je da se kao roditelj dvoje dece koja veliki deo slobodnog vremena provode na internetu sa zadovoljstvom priključio kampanji.

*"Tokom rada na projektu i pre toga postao sam svestan opasnosti koje internet može da pruži i pored dobri stvari. Ne puštajte svakog u svoju kuću i ne puštajte baš svakog na internet", rekao je Bajagić.*³

³ Kako zaštititi decu na internetu, izvor: BETA
(http://www.b92.net/info/vesti/index.php?yyyy=2009&mm=02&dd=10&nav_id=344237)

Ciljevi istraživanja

Cilj ovog pristupnog rada je da roditelji dobro zaštite svoj računar, kako bi njihova deca kao i razne informacije na računaru bile dovoljno zaštićene od zloupotrebe. Potrebno je, pre svega, opisati problematiku kontrole sadržaja na internetu. Prikazani su teoretski delovi zaštite računara, a u sledećem pristupnom radu će biti testirane i isprobane razne vrste ciljnih programa za zaštitu dece od neželjenih sadržaja. Pored toga, biće opisan i skup opcija i efekat različitih programa za filtriranje sadržaja.

Hipotetički okvir

Osnovna hipoteza ovog pristupnog rada, je da roditelji ne štite svoj računar i raznovrsne privatne inoformacije na adekvatan način od zloupotrebe. Kako bi sa tim istovremeno zaštitili svoju decu od štetnih virtuelnih sadržaja.

Podhipoteza je dokaz za osnovnu hipotezu, da roditelji nisu ni računarski dovoljno obučeni da bih znali zaštititi svoju maloletnu decu, a najveći problem je da nisu ni svesni kojim opasnostima su izložena današnja deca. Hipoteza će biti potvrđena ili odbačena u trećem pristupnom radu, odnosno u istraživačkom delu master rada.

Metode istraživanja

U ovom pristupnom radu korišćene su samo teorijske metode istraživanja

“Teorijski su oni metodi...

- kod kojih se primenjuju apstraktni teorijski principi i logička pravila, npr. silogizam u dedukciji, pravila definisanja, klasifikacije itd.;
- koji se uglavnom oslanjaju na postojeći kvantum saznanja i informacija
- kod kojih se vrši kvalitativno prekomponovanje saznanja, čime se stvaraju novi uvidi, osvetljavaju do tada manje poznati ili nepoznati delovi predmeta istraživanja

Teorijski metodi su:

- Definicija
- Klasifikacija
- Indukcija kao teorijski metod 1
- Dedukcija
- Analiza
- Sintez⁴

Struktura rada

Upotrebom odgovarajućih tehnologija, mogu se zaobići razne neprijatnosti i opasnosti iz sveta interneta. Opisane su opasnosti kojima su izlagana deca, operacije protiv pedofila, kontrola sadržaja sa interneta, ograničavanje dostupnih sadržaja, zakoni i zakonske regulative u Srbiji.

⁴ Prof. Dr Srbobran Branković-Uvod u metodologiju kvalitativni metodi istraživanja društvenih pojava (Beograd, mart 2007.)

Kompjuterski Kriminali

„Pod kompjuterskim kriminalom u najširem smislu podrazumevaju se krivična dela prema krivičnom zakonu nacionalne države, u koja su na bilo koji način uključeni računarski sistemi i mreže. U kompjuterskom i kibernetičkom kriminalu (cybercrime) računari se koriste kao predmet napada i krađe, izmene ili uništavanja podataka, kao alat za izvršavanje tradicionalnih oblika kriminala i za skladištenje kompromitujućeg materijala.

Glavni cilj istrage kompjuterskog kriminala je, kao i slučaju klasičnog kriminala, izgraditi za pravosudne organe neoboriv ili čvrst dokaz krivice, i/ili dokaz za oslobađanje osumnjičenog, i/ili pravedno sankcionisanje učinjenog dela. Ključnu metodologiju istrage i dokazivanja kompjuterskog kriminala obezbeđuje metodologija istrage klasičnog kriminala, sa specifičnostima istrage osteljivih, lako promenljivih i po svojoj prirodi posrednih digitalnih dokaza.“⁵

⁵ Milan Milosavljević, Gojko Grubor – Istraga Kompjuterskog Kriminala (Beograd, 2009)

1. BEZBEDNOST I ZAŠTITA DECE

„Deca su računarski pismenija od svojih roditelja i upravo su roditelji ti (prvenstveno) koji treba dodatno da se edukuju o opasnostima koja im prete na Internetu kao i prevencijama koje mogu da se sprovedu u cilju njihove zaštite“ ovo je zaključak nakon višemesečne obuke koja je sprovedena na teritoriji Vojvodine, na preko 200 tribina u 80 osnovnih škola.

POSITIVE se uključio u projekat „Elektronske droge – prevencija sajber zlostavljanja“ čiji je inicijator Centar za prevenciju devijantnog ponašanja „Target“ iz Novog Sada sa akcijom: „Bezbednost dece na internetu“ **u cilju edukacije i podizanja svesti roditelja i dece o načinima zaštite** dok surfuju internetom i istražuju web **kao i potencijalnim opasnostima** i psihološkim i fizičkim posledicama koje takve aktivnosti mogu da prouzrokuju.

Zajedno sa Biljanom Grujić kriminologom i Ljubicom Ristić psihologom uz podršku Pokrajinskog sekretarijata za obrazovanje i Gradske uprave za obrazovanje imali smo prilike da **u razgovoru sa decom, roditeljima i nastavnicima** podelimo svoja iskustva, posavetujemo ih, predložimo im konkretnim primerima koliko se naše ponašanje u stvarnom svetu oslikava i na ponašanje na Internetu.

Tribine su u vidu predavanja uz prezentaciju na projektoru oko 60 minuta sa opisima i screen shot-ovima a nakon toga pored klasičnih pitanja i odgovora pruža im se mogućnost da prenesu i svoja iskustva i zapažanja.

Roditelji: Prvo roditelji nisu svesni da fizičkim **odvajanjem deteta i računara u posebnu prostoriju** (njegovu sobu) **prave najveću grešku** jer na taj način deca se zatvore a roditelji slabo mogu da nadgledaju i umaju uvid koji su to web sajtovi koji posećuju, kako se ponašaju na Internetu i kakve su im aktivnosti.

Deca: Sa druge strane, deca svesna da se od roditelja bolje razumeju u računare i da nema načina na koji bi ih (neko) roditelji proveravao, **na internetu se ponašaju nekontrolisano** i često neprimereno što je za posledicu u Srbiji imalo **ekspanziju sajber zlostavljanja**.

Škole: Nastavnici informatike, bez obzira što tema bezbednost dece i ponašanje na internetu nije u nastavnom programu?! ipak **samoinicijativno skreću pažnju deci** na časovima informatike o tome.

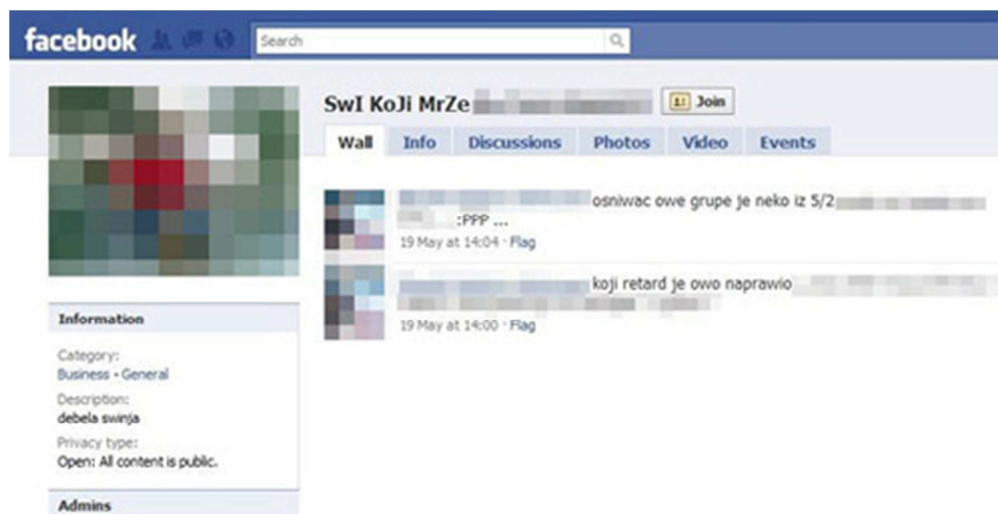
Opasnosti: Kada sam se početkom januara meseca uključila u projekat, tribine su održavane samo osnovcima od 5. do 8. razreda a za samo nekih mesec ipo dana moralo se proširiti i na decu od 1. do 4. razreda jer je glavni „krivac“ Facebook. Dovoljno je da samo jedno dete iz razreda otvori profil i lanac je krenuo... U Srbiji trenutno ima preko 2 miliona otvorenih naloga a većina su deca (a i sudeći po broju prijatelja koje imaju. Apsolutni rekorder je devojčica od 10 godina koja ima 3.200 prijatelja!).

Opasnosti koje najčešće prete deci na internetu, a čije primere smo mogli saznati i putem skoro svih medija proteklih godina su:

1. Sajber zlostavljanje
2. Dečja pornografija
3. Pedofilija
4. Internet zavisnost

1.1. Sajber zlostavljanje (Cyber bullying, Virtuelno zlostavljanje)

Najčešća pojava u Srbiji u poslednjih godina i to od strane dece. Na meti su druga deca i nastavnici (profesori). Najčešće se koristi **Facebook za otvaranje grupe** tipa: „**Ko mrzi tog i tog...**“ i snimanjem video sadržaja putem telefona da bi se namerno, svesno, neprijateljski ponašali i zlostavljali drugu decu, odnosno sa ciljem da naštetu pojedincu (ili grupi).



Slika 1. Jedna od grupa: Svi koji mrze...

Ovakvo ponašanje na Internetu je „**ničim izazvano**“ odnosno **grupe se otvaraju iz različitih (uglavnom dečjih) razloga**: debeo, mršav, kratka kosa, ružne patike, štreber, zato što neko ima plavu jaknu itd. Možete samo pretpostaviti kako je tom detetu koje dođe na Fejs i *sazna da postoji preko 100 druge dece koja ga mrzi*. **Deca nisu izgrađene ličnosti i njihove percepcije sveta (društva), pojava koje ih okružuju su potpuno različite od odraslih**. Neka deca naprosto puste da sve prođe, a druga dožive sve vrlo emotivno što za posledicu ima **promenu u ponašanju**: povlačenje u sebe, preispitivanje (sebe lično) svoje porodice, roditelja, škole, preispituje značaj prijateljstva, dobija loše ocene u školi, ne druži se, ne izlazi... Takođe otvaraju se i grupe gde đaci mrze svoje nastavnike i profesore: „**Ko mrzi nastavnicu biologije (ime i prezime) iz OŠ....**“ Na Facebook-u u trenutku kreiranja ovog posta je bilo 1.400 grupa koje su sadržale reči: svi koji mrze...



Neretko smo imali prilike videti **na YouTube-u video snimke** (koje posle prenesu i ostali elektronski mediji, televizije uglavnom) o tome kako **deca u školi snimaju mobilnim telefonima međusobne tuče, zlostavljanja i maltretiranja druge dece i nastavnika**. Normalno je da u takvoj situaciji pokušate to da sprečite a ne da mirno gledate i tražite što bolji ugao da to snimate, pa brže bolje na YouTube da to okačite. Neverovatno je da tri starija dečaka tuku mlađeg a da oko njih stoji 20-tak drugih učenika koji to SAMO snimaju.

1.2. Dečja pornografija

⁶Bezbednost i zaštita dece na internetu – I deo: Sajber zlostavljanje (Cyber bullying, Virtuelno zlostavljanje) (<http://blog.positive.rs/2010/06/09/bezbednost-i-zastita-dece-na-internetu/>)

Dečja pornografija je među najrasprostranjenijim vidovima kriminala na internetu. Dečju pornografiju šire pedofili radi pravljenja lične kolekcije, razmene materijala sa ostalim pedofilima, ili pravljenja novog materijala i dečije prostitucije.

Naučnici i pravosuđe sve češće koriste izraz zlostavljanje dece, umesto pornografija, koji bi mogao pogrešno da implicira na pristanak na seksualne odnose, te samim tim prikriva pravu prirodu dečje pornografije, a to je zloupotreba. Termin dečja pornografija ostaje legalna definicija u raznim pravnim sistemima. Koji god izraz da se koristi, on upućuje na seksualnu eksploataciju dece i adolescenata u pornografiji, a sam materijal je evidencija počinjenog kriminala.

Od 1999. godine Interpolova stalna radna grupa za krivična dela protiv maloletnika koristi sledeću definiciju: Dečja pornografija je posledica eksploatacije, ili seksualnog zlostavljanja dece. Može se definisati kao bilo koji vid prikazivanja, ili promovisanja seksualnog zlostavljanja dece, uključujući i pisane i audio zapise, koji se odnose na seksualne odnose sa decom, ili drugi vid seksualnog iskorišćavanja dece.

Deca svih uzrasta su zloupotrebljena u dečjoj pornografiji i njihov broj je ogroman. Većina slika (83%) odnosi se na decu koja nisu dostigla pubertet, dok je u 80% slika zastupljen seksualni odnos. 21% slika sadrži scene nasilja, mučenja i sadizma. 39% materijala su video zapisi. 79% materijala su slike bez seksualnog odnosa, sa golom, ili polugolom decom.⁷

1.3. Pedofilija

„**Pedofilija** (grč*paidós* - dijete + *filéó* - volim, ljubim) je spoljna nastranost, tj. seksualna sklonost prema deci istog ili suprotnog spola.

Pedofili su blage i nežne osobe. Svom seksualnom objektu prilaze oprezno. Često se ponašaju onako kako se prema njima ponašalo u detinjstvu, nesvesno zaljubljeni u sebe-narcizam. Većina pedofila zadržava se na fantazijama. Najopasniji oblik pedofilije je pokušaj penetracije zato što ona izaziva oštećenja.

Pedofilija spada u najčešći oblik poremećaja ličnosti. Ovde dolazi do pogrešnog izbora seksualnog objekta, a to su deca. Može biti heteroseksualna (dva puta češća) i homoseksualna. Poremećaj se ređe javlja kod žena. Heteroseksualni pedofili biraju devojčice od 8 do 10 godina, dok homoseksualni pedofil bira stariji uzrast. Seksualno zlostavljanje dece predstavlja bilo koji vid eksploatacije dece mlađe od 16 godina u cilju seksualnog zadovoljavanja starije osobe. Ono obuhvata telefonske razgovore, pokazivanje skrivenih delova tela, milovanje, snimanje pornografskih fotografija, pokušaj izvršenja seksualnog odnosa, incest, silovanje, dečju prostituciju. Neka od njih su uvredljiva, mučna i neugodna. Mnogo više su traumatični i neugodni incest, silovanje i prostitucija. Najčešće počinje u detetovom dobu od 4 do 8 godina od maženja do silovanja. Devojčice su pet puta češće žrtve od dečaka. Većinom su zlostavljači muškarci i to deci poznate osobe. Retko koriste silu već nagovaranje i potkupljivanje. Silovanje je traumatski čin koji onemogućava normalan razvoj seksualnosti. Incest je seksualna eksploatacija od strane porodice. Predstavlja najveće traumatski čin koji onemogućava razvoj normalne psihoseksualnosti.⁸

⁷Dečja pornografija (http://sr.wikipedia.org/sr-el/Дечја_порнографија)

⁸Wikipedia-Pedofilija(<http://bs.wikipedia.org/wiki/Pedofilija>)

1.4. Internet zavisnost

„Šest sati neprekidnog korišćenja kompjutera granica posle koje neko može da bude klasifikovan kao "zavisnik" i upućen na lečenje. Širom sveta niču specijalizovani centri za lečenje internet zavisnika.“⁹

„ Da bismo se iole priblizili objasnjenju pojma Internet zavisnosti hajde da vidimo sta je uopste zavisnost?

Dare je u komentaru na prethodni post rekao vec nesto na ovu temu a ja cu da ponovim: zavisnost je uprosćenim recima – losa navika, ponasanje kojeg se ne mozemo osloboditi a koje se **odrazava negativno na vas zivot** i ugrozava vase svakodnevno funkcionisanje.

Kada je cyberokruzenje u pitanju, kao sto vec rekoh, misljenja razlicitih strucnjaka su jos uvek prilicno neuskладjena. Recimo Jonatan Bishop koji se bavi proučavanjem online zajednica ima zanimljivu tezu kako je Internet zavisnost kao fenomen nemoguća sama po sebi. Po njemu se “ne može biti zavistan od Interneta jer je Internet okruženje kao i RL, a niko ne govori o zavisnosti od RL”.

Bez obzira na takve i druge slicne stavove, sve je vise i vise evidentno da neki ljudi imaju ozbiljne probleme vezane sa upotrebom Interneta. Osnovno pitanje u svemu jeste šta je tu uzrok a šta posledica?

Alternativno objašnjenje je to da je povećana upotreba Interneta samo manifestacija drugih već postojećih problema, problema koje ne uzrokuje Internet i koji se manifestuju kroz povecan broj sati provedenih online.

Vrtimo se u krug, znam.

Kako uopšte da izmerimo šta je to povećana upotreba i u odnosu na šta?

U mnogim izvorima koji nude tekstove na ovu temu, pronaci cete broj sati provedenih za racunarom kao jedan od osnovnih kriterijuma zavisnosti od Interneta. Hm. Sta je ono sto je tu problematicno?

Cinjenica je da prosečno sve više vremena provodimo online. Istraživanje sprovedeno na Stanfordu 2005 pokazalo je da je tada prosečan amerikanac provodio oko 3.5 sati online. A ovaj broj je od 2005 u porastu.

Beba je u svom odlicnom postu na ovu temu navela citat iz jednog domaceg “istrazivanja” u kome se kaze izmedju ostalog i da *svako ko uz aktivnosti vezane za internet provede svakodnevno “svega” 4 sata, što je tek 28 sati nedeljno, duboko je zagazio u zavisnost*. Izvor ovih podataka je cini se nepoznat, ali je interesantan kriterijum zavisnosti .

Da, provodimo dosta vremena online. Ali – da li provodjenje vremena podrazumeva zavisnost? Ili samo kvalitativnu promenu u okruženju koja se odražava na način na koji naš svakodnevni život funkcioniše? Da li je to zapravo povezano sa promenama u nacinu života, komunikacija, načina na koji obavljamo posao, placamo račune, komuniciramo sa kolegama i prijateljima, stupamo u razlicite interakcije, zabavljamo se.....mnogo je stvari koje nas danas upućuju u sajberprostor.

Evo jedne ilustracije. Za mnoge od nas (uključujući i mene) proveravanje mejla je jedna od prvih stvari koje radimo kada ustanemo ujutro. Zavisnost ili potreba? Od toga sta vam se tog jutra naslo u inboxu moze vam zavisiti ceo dnevni plan pa se postavlja pitanje da li je u današnje vreme proveriti mejl rano ujutro stvar izbora ili *neophodnosti*?

Da se vratimo na pocetak – u cekanju da se najpsiholozi sveta dogovore oko toga ima li Internet zavisnosti, sta je, kakva je, kako je definisemo i kako je lecimo, kriterijum kojim se moramo voditi je jednak kao i za ostale bolesti zavisnosti – **ono što ugrozava nase životno funkcionisanje JESTE problem.**

Ako zbog Interneta ne obavljate svoje svakodnevne obaveze, zapostavljate porodicu, posao, školu, prijatelje – vreme je da se zabrinete i eventualno potrazite strucnu pomoc. Ali ako je Internet sastavni deo vasih zivotnih aktivnosti (posla, komunikacije sa prijateljima, obavljanja razlicitih stvari, informisanja itd) i ničim ne ugrozava vaše funkcionisanje, onda isklucivo broj sati koji ispred računara provodite ne moze biti jedino merilo zavisnosti od Interneta (jeste doduse jako problematičan za neka druga oboljenja pre svega vezano za repetitivne pokrete i previse sedenja).“¹⁰

1.5. Sporazum protiv internet-siledžija

Evropska unija je potpisala sporazum sa 17 internet mreža za druženje, uključujući Facebook, Myspace i Google, za poboljšanje zaštite tinejdžera od siledžijskog ponašanja na internetu. Portparol EU Martin Selmajr rekao je da internet stranice za društveno povezivanje sada koristi oko 42 miliona ljudi u EU i da mlade korisnike treba zaštititi od nasilničkog ponašanja. Sporazum, koji je danas objavljen, obavezuje vlasnike internet mreža da "ograniče rizik" od zloupotrebe omogućavajući "taster" za prijavu zlostavljanja.

To će omogućiti korisnicima da prijave "neprikladne kontakte ili ponašanje" drugih korisnika. Internet operateri takođe moraju da osiguraju da internet profili i kontakt liste maloletnih korisnika budu postavljeni uz najveću zaštitu privatnosti.

1.6. Operacija Plava Orhideja

„Operacija Plava Orhideja je bila udružena akcija Sjedinjenih Američkih Država i Rusije u rasturanju kriminalne organizacije koja se bavila dečjom pornografijom i čiji se sajt zvao *Plava orhideja*. Akcija je počela u maju 2000. godine, pošto je jedna informacija vezana za drugi slučaj dečje pornografije dovela do informacije o sajtu *Plava orhideja*. Sajt, na kome su se nalazile scene silovanja, takođe je imao video snimke zlostavljanja osmogodišnjih ruskih dečaka. Snimci su prodavani po ceni od oko 300 dolara. Istraga je uključivala kupovinu jednog snimka, od strane carinskih službenika SAD. Istraga je rezultirala hapšenjem četiri Amerikanca i pet Rusa uključujući kreatora i menadžera sajta, čije je ime Vsevolod Solnsteve-Elbe. Vođa akcije Čarls Vinvud je zbog uspešno obavljene akcije, ali i činjenice da je postojala međunarodna saradnja konstatovao da „**ne postoje granice kada je u pitanju zajednički interes zaštite dece**“.“¹¹

¹⁰ Internet zavisnost – deo drugi (<http://www.nikolinal.com/2010/04/internet-zavisnost-deo-drugi/>)

¹¹ Wikipedija- Operacija Plava Orhideja
(http://sr.wikipedia.org/sr-el/Операција_Плава_Орхидеја)

1.7. Operacija Delego

„**Operacija Delego** je međunarodna akcija sprovođenja zakona koju vodi FBI. Akcija obuhvata 14 zemalja, uključujući i SAD i Srbiju. U okviru te akcije uhapšene su 52 osobe optužene za internet dečiju pornografiju. Optuženi se terete za učešće u međunarodnoj mreži koja je distribuirala i reklamirala dečiju pornografiju preko privatnog foruma Drimbord. Njih 50 sumnjiči se i za proizvodnju dečije pornografije u koju su bila uključena deca uzrasta do 12 godina. Operacija Delego započeta je u decembru 2009. godine, a do sada (novembar 2011) su u tri faze uhapšene 72 osobe, dok je više od 500 ljudi ispitano.

Mreža pedofila funkcionisala je preko privatnog foruma Drimbord, koji je bio namenjen isključivo pedofilima. Bord foruma, koji su činila trojica uhapšenih, kontrolisao je snimke i slike koje su ostali članovi postavljali. Članovi su razmenili više desetina hiljada fotografija i snimaka zlostavljanja dece.

Otkriveno je 123 terabajta, koliko ima na 16.000 DVD sa dečijom pornografijom. Prema navodima optužnice, koja citira pravila Drimborda, „običan“ član morao je da postavi pornografiju bar jednom u pedeset dana. „Super VIP“ članovi su bile proverene osobe, ili one koje su pravile nove snimke zlostavljanja. Na forumu su postojale kategorije dečije pornografije, sve do super hardkora, koji je podrazumevao snimke silovanja male dece, fizičkog i psihičkog zlostavljanja. U Srbiji je privedeno pet osoba, a u SAD 13 je priznalo krivicu, dok su četiri osobe osuđene na 20 do 30 godina zatvora.“¹²

1.8. Ograničavanje dostupnih sadržaja

„Kod dece treba posvetiti pažnju i njima, informisati ih koje sve opasnosti vrebaju i koje benificije mogu imati koristeći internet i računar. Iako smatrate da je dete dok sedi u svojoj sobi bezbedno, ako ne vidite koje sadržaje posećuje to može da bude izuzetno opasno. Najbolje poređenje koje možete napraviti sa svim opasnostima koje vrebaju na internetu jeste da zamislite da putujete negde u nepoznato mesto. Gotovo ista pravila kojih se držimo prilikom posete mestu koje ne poznajemo, važe i kada je internet u pitanju. Mnogo lepih mesta, pametnih stvari i zanimljivih podataka možemo videti i naučiti, važno je samo da budemo svesni i obavešteni o ćorsokacima, mračnim ulicama i opasnim "krajevima grada" koje ne treba da posećujemo.

Ne postoji apsolutno sigurna zaštita deteta na internetu ali postoje programi (velika većina je besplatna i mogu se naći jednostavnom google pretragom) koji mogu da prate aktivnost deteta i da mu zabrane pristup ka neželjenim sadržajima. Sa sve većim širenjem interneta pojavio se i veliki broj provajdera koji sada već i sami u sklopu svojih paketa nude određenu mogućnost blokade nedozvoljenog materijala na kompjuteru koje dete koristi. Oni se baziraju na biranju liste sa neželjenim sadržajem, na osnovu čega softver dalje zabranjuje pristup određenom sajtu i ograničava slanje ličnih podataka sa računara na mrežu. Još jedan od korisnih načina da zaštitite dete je da tačno znate šta ono radi na internetu. Za tu svrhu postoje softvereri koji rade u pozadini (korisnik računara ne zna da se prate njegove aktivnosti) i beleže aktivnosti na mreži. Međutim, najbolje je ipak da razgovarate sa detetom i da vidite koja su

¹²Wikipedija-Operacija Delego (http://sr.wikipedia.org/sr-el/Операција_Делего)

njegova interesovanja i kakav utisak internet ostavlja na njega. Internet ne bi trebao da za meni prijatelje i igru, pa se zato treba potruditi da dete internet koristi u edukativne i praktične svrhe a ne samo za zabavu. Treba pratiti sadržaje koje koristi i blokirajte one neželjene.

Saveti za što veću bezbednost dece na internetu. Ukoliko računar budete držali na sigurnom mestu (tako da nije lako dostupan detetu), bićete upućeni u to na koji način i koliko dete koristi internet. Redovno pregledajte posećivane sajtove, pa možda čak i mejlove ako imate razloga za brigu u pogledu toga šta vaša deca rade na Internetu. Iako ovo deluje kao narušavanje privatnosti, deca nisu uvek u mogućnosti da spoznaju namere loših ljudi ili da uvek savesno izbegavaju spam.

Elektronska pošta je posle četa uživo najopasnija stvar za decu jer se u tim momentima njima može svašta sugerisati a njihova naivnost ih sprečava da budu oprezni. Iz istog razloga treba obratiti pažnju na korišćenje društvenih zajednica od strane dece. Sa druge strane, ukoliko detetu u programu za pretragu Interneta snimate omiljene sajtove (bookmark, favourites) i time mu možete olakšati pristup njima, manje su šanse da će "lutati" od sajta do sajta, tražeći ono što ga zanima. Mada, ovo se ne može u potpunosti izbeći tako da je najbolje da uz sve mere predostrožnosti ipak redovno pričate sa decom na ovu temu i razvijete kod njih osećaj odgovornosti kako bi oni razumeli vašu brigu, odnosno kako vaše mere zaštite ne bi tumačili samo kao kaznu ili bezrazložna ograničenja., pomoći će vam da upoznate njegov svet i interesovanja.“¹³

„Kompanija „Symantec“ (svetski lider u oblasti zaštite informacija i računarskih mreža) je objavila rezultate analize vezane za najtraženije pojmove na internetu među mladima, na uzorku od 3,5 miliona različitih internet upita. A to su:

1. YouTube
2. Google
3. Facebook
4. Sex
5. MySpace
6. Porn
7. Yahoo
8. Michael Jackson
9. Fred (YouTube zvezda)
10. eBay” ¹⁴

¹³Bezbednost prilikom upotrebe računara i interneta, autor: HERMES
(<http://serbianforum.org/obrazovanje/18037-bezbednost-prilikom-upotrebe-racunara-i-interneta.html>)

¹⁴Verat.net, Zaštita i edukacija dece na internetu
(<http://www.verat.net/sr/novosti/2010-08-02/zastita-i-edukacija-dece-na-internetu/>)

1.9. Zlatna pravila

1. „Nastojte da zaštitite decu od neprijatnih iskustava – pokažite im kako da zaštite sopstvenu privatnost i poštuju privatnost drugih.
2. Naučite decu da ne odgovaraju na uvredljive poruke.
3. Pomozite deci da shvate kakve poruke mogu da izazovu neprijatne osećaje.
4. Proverite umeju li deca da blokiraju prijem poruka od određenog pošaljioa.
5. Sačuvajte uvredljive poruke, mogu da vam posluže kao važan dokaz.
6. U suzbijanju klasičnog šikaniranja na Internetu sarađujte s učiteljima i drugim roditeljima.
7. Budite u kontaktu s ljudima iz okoline vašeg deteta – upoznajte se s njegovim drugovima, njihovim roditeljima, nastavnicima i uopšte okruženjem.
8. Naučite svoje dete da vas obaveštava o svakom iskustvu iz virtualnog / realnog sveta, koje ga zabrinjava. Ubedite ga da u vas može da se pouzda i kada neoprezno uradi nešto loše i da ćete zajedno potražiti rešenje!
9. Objasnite detetu da, ukoliko ga neko uznemirava, to nikad nije njegova krivica“ ¹⁵

¹⁵Infomreža, Zaštita dece na internetu (<http://www.infomreza.com/tehnologija/zastita-dece-na-internetu/>)

2. TEORIJSKE OSNOVE

Internet je krajem 20.veka, za samo nekih 10-12 godina postojanja, doneo globalnu promenu u načinu i brzini komunikacije. Uticao je mnogo na život "običnog čoveka" i na sva polja našeg životnog okruženja. Pored toga što čovek koristi internet za poslovnu komunikaciju, takođe ga upotrebljava da podesi klima-uređaj, rezerviše karte za pozorište, avion, da preuzme software za auto, gleda TV, komunicira. Sve je veća zavisnost od interneta. Međutim, problem je što su korisnici nedovoljno informisani o mogućnostima elektronskih servisa, pa tako nisu svesni opasnosti i rizika koje internet donosi. Edukacija rada na internetu se svodi na upotrebu računara, a ne i na bezbednost na internetu.

Danas oko 15 posto svetske populacije koristi svesno internet a nesvesno kroz razne uređaje, telefone, televiziju čak 25 posto. Polovina od toga je u uzrastu od 5 godina do adolescencije. Sadržaji koje deca koriste su uglavnom „zabavnog“ karaktera – slike, filmovi, chat i drugi sadržaji za „igru“ ili bolje „gubljenje dragocenog vremena“, dok je stav porodice (čast izuzecima): *„Neka deca uče sa kompjuterima, trebaće im ili neka se igraju. Bolje da ih ovde vidim nego da lutaju po ulicama!“*.

Odavno se pitamo gde je bezbednost dece veća, uz internet ili na ulici. Iz računara vrebaju skrivene zamke, a razni bolesni umovi svoju ciljnu grupu tj. vaše dete, našli su baš u tome. To naravno ne znači da je internet mračna strana sveta, ali nekontrolisana i besciljna upotreba interneta je velika opasnost za sve.

Prema definiciji Svetske zdravstvene organizacije (SZO), nasilje se definiše kao „namerna primena fizičke sile ili moći, sa ciljem zastrašivanja ili stvarna, nad samim sobom, drugom osobom, grupom ili zajednicom, a koja rezultira ili je velika verovatnoća da će rezultirati povređivanjem, smrću, osećanjem uskraćenosti, psihičkim poremećajima ili smetnjama u razvoju“. Prema podacima UNICEF-a, tokom 2001. godine ubijeno je dva miliona dece, šest miliona je teško ranjeno ili trajno onesposobljeno, a 12 miliona dece ostalo je bez svog doma.

Oni koji kreiraju sadržaje sa neadekvatnim informacijama i bave se distribucijom zakonski nedozvoljenog materijala (u blažoj varijanti muzika, film, teža varijanta nedozvoljeni sadržaj, dok su u istom rangu pedofilija i komunikacija sa ciljem iskorišćavanja, maltretiranja i zlostavljanja) takođe podležu ovoj definiciji, kao i iskorišćavanje interneta u bilo kom vidu prisiljavanja i ucene. Ali se zloupotreba interneta ne odnosi samo na najčešću asocijaciju – nedozvoljeni sadržaj. Sajtova sa „štetnom“ tematikom, poput samoubistava, anoreksije, otmica, abortusa, nacističkih sajtova, droge, ima na desetine hiljada u svetu. Takođe, sajтови sa raznim vrstama dijeta, vežbanja i drugih saveta veoma su opasni jer iako ne privlače toliku pažnju, ipak su, nažalost, uticajni, što dovodi do posledica od fizičkih povreda do bolesti, pa čak i smrti.

Osnovni problem je u tome što sadašnje društvo i roditelji nemaju jasnu sliku ove definicije i ne umeju da prepoznaju problem, a nažalost nisu svesni da jedan broj dece u uzrastu do 16 godina distribuira materijal nedozvoljenog sadržaja i spada u grupu prekršilaca, a da toga nisu ni svesni.

Web portali sa nelegalnim sadržajima funkcionišu ilegalno, ali javno i nude razne oblike mentalnog zlostavljanja (sekte, nacistički sadržaji, nedozvoljeni sadržaj...). Tim sadržajima posetioci pristupaju iz raznih pobuda, deca najčešće iz radoznalosti (po njihovoj prirodi ili zato što to rade njihovi vršnjaci). U svakom slučaju, ova vrsta „pasivnog” pristupa nudi razne bonuse i „zanimljivosti” vernim posetiocima – dugoročan i veoma siguran put za mentalno „trovanje” naivnog deteta. Naredna faza može biti lični kontakt, učlanjenje i sl.

Zbog prava na slobodu mišljenja i govora, zakonske norme nemaju uticaja, a globalni uticaj na roditelje i društvo je lagano navikavanje na postojanje ovih sadržaja. Nijedan posetilac nije prisiljen na korišćenje (ne)legalnih sadržaja, već se sam odlučuje i sa tim se skida odgovornost sa autora web portala.

Kanali komunikacije i uticaji na određenu grupu se vrše aktivnom metodom najčešće e-mail porukama, chat servisima i mobilnom telefonijom (poslednjih godinu dana su učestale e-mail poruke sa ličnim obraćanjem i pozivom da pogledate slike navodne drugarice sa mora ili izlaska) ili pasivnom metodom putem web portala sa nelegalnim sadržajima (na domaćem Internetu ćete naći sajtove sa raznolikim sadržajem za široku populaciju i zabavu uz dodatak glasanja za razne slike nedozvoljenog sadržaja).

Način pristupa deci je najčešće oblik lažnog predstavljanja, kao u navedenom primeru i „tešenja” (uglavnom je to dobar virtuelni drug vršnjak – pun razumevanja). Nakon što dete stekne poverenje, naredna faza je slanje fotografija, upućivanje na web portale ili zakazivanje „druženja” i lični kontakti. U ovoj poslednjoj fazi, dolazi do prisiljavanja deteta putem ucene ili prostim sistemom sile na željenu aktivnost. Ovo se odnosi i na vrste iskorišćavanja kao što su krađe, prevare, itd.

Mobilni telefoni su sve rizičnija kategorija uređaja koji neometano prenose nelegalne sadržaje, a pružaju i velike mogućnosti samog kreiranja takvog sadržaja. Često se snimaju filmovi mobilnim telefonom čiji su ciljevi ismevanje, ucena, itd. Tako su sada nemoralni materijali prisutni na GSM mreži i javno reklamirani u medijima. U proseku svako drugo dete ima svoj mobilni telefon, a samo je mali broj u kontrolisanim uslovima, pa je opasnost od mobilnog pristupa deci i zlostavljanja sve veća. Takođe je zabrinjavajući podatak da je u 2006. godini na Internetu sa područja Srbije i Hrvatske uklonjeno na desetine fajlova video-materijala u režiji dece od 12 do 16 godina. Deca u školama sama postaju zlostavljači i ucenjivači (vršnjačko nasilje preko Interneta i mobilnih uređaja), dok odgovorna lica nisu sigurna šta mogu da učine da bi se to sprečilo. Dva skorašnja primera iz Hrvatske pokazuju na šta su deca spremna. Na stranicama sajta YouTube, na kojem se razmenjuju slike, muzika i video snimci, zabranjena je lokacija sa video-materijalom snimljenim mobilnim telefonom gde nekoliko učenika zlostavlja svoju školsku drugaricu, kao i fizičko nasilje maturanata nad svojim profesorom.

Najpopularnije i istovremeno najopasnije područje interneta je chat prostorija (room). Ovaj servis omogućava deci da se putuje u bilo koji deo sveta, da se razgovara i razmenjuju poruke sa bilo kim, bez obzira što ne znaju ništa o njima i koji su za njih potpuni stranci. Deca ne znaju sa kim pričaju, a sa druge strane mogu biti i odrasli a da se predstavljaju kao da su deca. Oni su naivni i imaju želju da upoznaju vršnjake iz drugih krajeva i zemalja, pa daju informacije o sebi kao što su godine, uzrast, pol, mesto boravka, škola, itd. Pedofili na ovaj način mogu da saznaju sve o

deci koja ih zanima – kuda se kreće, šta voli, kakav mu je raspored, u kakvim je odnosima sa roditeljima, itd. Da bi saznali sve ove podatke, ne trebaju čak ni da se aktivno uključe u razgovor. Dovoljno je da skriveno prate razgovor među decom i tako da prikupe informacije koje ih zanimaju. Sada je lakše nego ikad da se sazna nešto o detetu preko interneta. Ranijih godina, pedofili su odlazili na igrališta i tamo su posmatrali decu, pratili ih, pričali sa njima. Ali sa tim su se izlagali riziku. Međutim, preko interneta je lako kroz uključivanje u igru i zabavu a ako osete opasnost od otkrivanja, jednostavno beže u anonimnost interneta.

Američka istraživanja pokazuju da 19 posto dece koja se služe internetom biva izloženo raznim vrstama nedozvoljenih poruka. Riziku su najviše izložena deca od 12 do 17 godina koja koriste chat-prostorije i, naravno, koja razgovaraju sa strancima.

Roditelji i vaspitači imaju najveću odgovornost u vaspitanju i obrazovanju deteta, a najbolji interesi deteta moraju biti njihova osnovna briga. Pojedinačne mere borbe protiv zlostavljanja nisu davale željene rezultate na globalnom nivou, ali mogu spasti vaše dete ili njegovog drugara ili drugaricu.

2.1. Content Control – Kontrola sadržaja

Content-control software, takođe poznat kao censorware ili web filtering software, je termin za software koji je dizajniran i optimizovan za kontrolu sadržaja koji je dozvoljen čitaču, naročito kada je korišćen da bi ograničio dostavljen materijal preko web-a. Software za kontrolu sadržaja odlučuje koji će sadržaj biti dostupan na određenom računaru ili mreži; povod za ovo je sprečavanje osoba da vide sadržaj koji vlasnici računara ili drugi autoriteti možda smatraju nepoželjnim; kada je nametnut bez dozvole korisnika, kontrola sadržaja može predstavljati cenzuru. Obični slučajevi koji se koriste kod takvih programa uključuju roditelje koji žele da ograniče na koje web stranice mogu njihova deca da idu sa kućnih računara, škole koje rade to isto sa računarima po školama i zaposlene ograničavajući ih koje sadržaje mogu da vide dok su na poslu.

Uobičajeni predmeti software-a za kontrolu sadržaja sadrže web stranice koje u zavisnosti od kompanije održavaju kontrolu:

- Uključuju nelegalni sadržaj sa referencom legalnog domena dostavljenog od strane te kompanije.
- Promovišu, omogućavaju, ili raspravljaju o padu sistema, softverskoj pirateriji, zločinskim veštinama, ili drugim potencijalnim nelegalnim činovima.
- Sadrže nedozvoljeni sadržaj, i diskusije o nedozvoljenim temama.
- Promovišu, omogućavaju, ili raspravljaju o raznim prirodnim opredeljenjima van braka ili drugim stilovima života koje se čine nemoralnim.
- Sadrže nasilje ili druge oblike grafičkog ili ekstremnog sadržaja.
- Promovišu, omogućavaju, ili raspravljaju o fanatizmu (slepoj privrženosti) ili govorima mržnje.

- Promovišu, omogućavaju, ili raspravljaju o kockanju, rekreativnom korišćenju droge, alkohola ili drugih aktivnosti koje se često smatraju porocima.
- Koji verovatno nisu u vezi sa naukama studenata, sa funkcijom posla zaposlenog, ili drugih zadataka za koje je računar potreban, naročito ako je uključena široko pojasna potrošnja.
- Koje su suprotne interesovanjima autoriteta, kao što su organizovane laboratorije za promociju web stranica ili kritikovanje određene kompanije ili industrije.
- Promovišu ili raspravljaju o politici, religiji, zdravlju ili drugim temama.
- Sprečavaju umišljene ljude (hipohondere) od gledanja web stranica vezanih za zdravlje.
- Uključuju mogućnosti socijalnog umreženja koji bi mogli da otkriju decu lovcima.

Software za kontrolu sadržaja takođe može da se koristi da bi u potpunosti blokirao pristup internetu.

2.1.1. Terminologija

Kompanije koje prave proizvode koje posmatraju i selektivno blokiraju web stranice, ne odnose se na proizvode kao što su censorware, i više koriste termine kao što su "Internet filter" ili "URL Filter"; takođe je u upotrebi specijalno dizajniran software, koji bi dozvolio roditeljima da nadgledaju i ograniče pristup svojoj deci, "parental control software". Neki proizvodi loguju sve web stranice kojima korisnik pristupa i raspoređuju ih na osnovu tipa sadržaja za izveštavanje odgovornom partneru ili odabiru osobe, i koristi se termin accountability software. Internet filteri, parental control software, i/ili accountability software može takođe da bude povezan u jedan proizvod.

Seth Finkelstein, advokat za anti-censorware i vlasnik EFF Pioneer Award-a, opisao je termin censorware: "Mislim da su najbolji odnosi sa javnošću, koji su censorware kompanije uradile je što su dodale reč "filter" svojim proizvodima. Kada pomislite na spam filter, na primer, odmah vas to asocira na nešto što ne želite da vidite. Ali, censorware nije kao spam filter. To je autoritet koji želi da zaštiti neki subjekat pod svojom kontrolom, od gledanja materijala koji mu zabranjuje."

2.1.2 Pitanja

Filteri mogu biti realizovani na različite načine: software-skim programom na osobnom računaru ili putem servera koji provajderi omogućuju pristupom internetu. Birajući provajder (internet service provider - ISP) koji blokira nepoželjni materijal pre ulaska u kuću, može da pomogne roditeljima koji brinu za svoju decu gledajući nepoželjan sadržaj.

Oni koji veruju da je software za kontrolu sadržaja koristan, možda se još uvek ne slažu sa određenim načinima na koji je korišten, ili sa obaveznim uopštenim pravilom informacija. Na primer, mnogi ne odobravaju neke poglede fitracije na

moralnoj ili političkoj osnovi, slagajući se sa tim da to može postati podrška za propagandu. Mnogi bi smatrali neprihvatljivim da provajderi, bez obzira da li zakonom ili svojim ličnim izborom, razvije takav software bez da dozvoli korisnicima da onemoguće filtriranje za svoje veze.

2.1.3. Istorija

Kako se www (world wide web) sve više razvijao, roditelji, vođeni pričama iz masovne medije, počeli su da se brinu da dopuštanjem svoje dece da koriste mrežu, mogli bi da ih izlože nemoralnom materijalu. Američki kongres zabranjuje nemoralnost na internetu. Neke grupe koje se bave pravima građana, izjavljuju da roditelji koji žele da blokiraju web stranice, mogu da koriste svoj lični software za filtriranje sadržaja, sa tim da je neophodno uključiti vladu.

Kritike su tvrdile da software za filtriranje sadržaja možda čini cenzuru vlade manje verovatnom, to bi možda činilo ako bi manjim kompanijama bilo dozvoljeno da cenzurišu što žele. Oni su dalje tvrdili da bi vladino ohrabrenje filtriranja sadržaja, ili legalnih zahteva za software označavanja sadržaja, odgovaralo cenzuri. Iako pri ozbiljnim rizicima od optužbe za falsifikovanje, tajnu trgovinu nasilja, ili kršenja licencnih ugovora, grupe kao što su Cenzorware Project počele su sa analiziranjem software-a za kontrolu sadržaja i sa dešifrovanjem crnih listi da bi odredili kakve vrste web stranica software blokira. Otkrili su da takve alatke rutinski blokiraju besprekorne web stranice a opet ne uspevaju da blokiraju one na koje ciljaju. Primer ciljanih je filtriranje svih web stranica koje sadrže reč "grudi", pod pretpostavkom da jedino ova reč može biti spomenuta u seksualnom kontekstu. Ovaj pristup je imao, kao posledicu blokiranja web stranice koje sadrže rasprave o raku dojke, ženskom stilu oblačenja, i čak recepte piletine.

Mnoge vrste software-a za kontrolu sadržaja su blokirale web stranice koje se baziraju na religijskim i političkim temama vlasnika kompanija. Primeri uključuju blokiranje nekoliko religijskih web stranica (uključujući web stranice Vatikana), mnogo političkih web stranica, i web stranice o homoseksualcima.

Iako se većina software-a za kontrolu sadržaja prodaje organizacijama i roditeljima, takođe se reklamira i za kućnu upotrebu kao cenzura za one koji se muče sa zavisnošću sa internetom. Ljudi koji provode opsesivno vreme na posjećivanju nedozvoljenog sadržaja, kockanja, chat prostorija ili interneta uopšte, možda samovoljno žele da uklone ili ograniče pristup sadržajima interneta. Mnogi proizvodi koji se prodaju za kućnu upotrebu ili software za obavezu, promovišu se u crkvama ili kroz religijske medije.

2.1.4. Označavanje sadržaja

Označavanje sadržaja može da razmatra drugačiji oblik software-a za kontrolu sadržaja. Asocijacija za vrednovanje internet sadržaja (ICRA-Internet Content Rating Association) koji je sada deo institucije online bezbednosti porodice (Family Online Safety Institute), 1994. godine razvio je sistem vrednovanja sadržaja za provajdere online sadržaja. Korišćenjem online upitnika, webmaster opisuje prirodu sadržaja svoje web stranice. To je jedan mali fajl koji sadrži kratki opis koji može da koristi software za filtriranje sadržaja za blokiranje ili dozvolu te web stranice.

ICRA oznake postoje u različitim formatima. Ovi uključuju okvir opisa izvora konzorcije svetske mreže (World Wide Web Consortium's Resource Description

Framework - RDF) i PICS oznake koji definiše generalni format za oznake (Platform for Internet Content Selection - PICS) korišćene od strane savetnika sadržaja Microsoft-ovog Internet Explorera (Microsoft's Internet Explorer Content Advisor).

2.1.5. Korišćenje u javnim bibliotekama

SAD

Korišćenje internet filtera ili software-a za kontrolu sadržaja brzo se menja u javnim bibliotekama u SAD, otkad postoji primena interneta od strane bibliotekarske uprave. Mnogo biblioteka je usvojilo internet filtere nakon što je kongres uslovio račun univerzalnih servisnih popusta na korišćenje internet filtera kroz akt dečije bezbednosti na internetu (Children's Internet Protection Act - CIPA). Druge biblioteke ne instaliraju software za kontrolu sadržaja, jer veruju da prihvatljive primene načina rada i edukativni naponi čine ishod da deca gledaju neprikladan sadržaj za svoje godine uskraćujući odraslim korisnicima time pravo da slobodno dolaze do informacija. Neke biblioteke koriste internet filtere samo na računarima na koje deca koriste. Neke biblioteke koje koriste software za kontrolu sadržaja dozvoljavaju da software bude deaktiviran u zavisnosti od slučaja na osnovu aplikacije ili bibliotekara; biblioteke koje su podvrgnute CIPA-i, treba da imaju politiku koja dozvoljava odraslima da zahtevaju da se filter onesposobi bez da moraju dati razlog za svoj zahtev.

Australija

Australijski savetnik za bezbednost na internetu (The Australian Internet Safety Advisory) ima informaciju o “praktičnim savetima za bezbednost na internetu, roditeljsku kontrolu i filtere za zaštitu dece, studenata i porodica” koji takođe sadrže javne biblioteke.

NetAlert, software koji je bio besplatan od strane australijske vlade, kreovan je od strane jednog studenta od 16 godina, Tom Wood-a, koji je to uspeo za manje od nedelju dana nakon izdavanja u avgustu 2007. Wood je izbegao filter u vrednosti od 84 miliona funti za otprilike pola sata da bi obelodanio probleme sa vladinim pristupom ka filtriranju internet sadržaja.

Danska

U Danskoj postoji stav po kome se sprečava pristup dece na neprikladne web stranice širom biblioteka u Danskoj. Bitno je da svaka biblioteka u državi ima mogućnost da zaštiti decu od nedozvoljenog materijala kada koriste računare u biblioteci.

2.1.6. Zaobilazanje filtera

Neki software-i se uspešno zaobilaze korišćenjem opcionih protokola kao što su FTP, telnet ili HTTPS (Hypertext Transfer Protocol over Secure Socket Layer), upravljajući pretragama na različitim jezicima, koristeći proxy server ili zaobilaznik kao što je Psiphon (web proxy dizajniran tako da pomaže korisnicima interneta koji su zaraženi internet cenzurom bezbedno zaobilazivši sisteme filtriranja sadržaja). Takođe

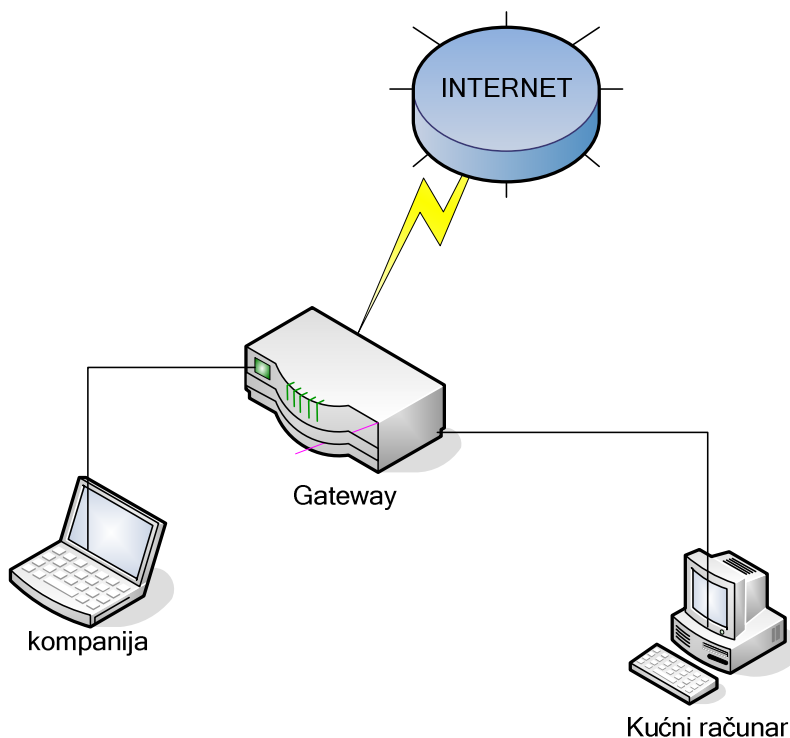
keširane web stranice koje vraća Google ili drugi pretraživači, mogu zaobići neke kontrole. Neki Web servisi mogu snabdeti opcione putanje za sadržaje. Neki od siromašnije dizajniranih programa kogu biti isključeni, prekidajući njihove procese: na primer, u Microsoft Windows-u kroz Windows Task Manager, ili u Mac OS X koristeći Activity Monitor.

Mnogi filteri sadržaja imaju opciju koja dozvoljava autorizovanim ljudima da zaobiđu filter sadržaja. Ovo je naročito korisno u okruženjima gde se računar nadgleda i filter blokira web stranice kojima se želi pristupiti.

2.1.7. Gateway baziran na rešenjima kontrole sadržaja

Kompanije koje žele da primene rešenja kontrole sadržaja, sve više primenjuju bezbednosne alate na mrežnoj kapiji, npr. web proxy za filtriranje sadržaja SafeSquid. Untangle je opcija otvorenog izvora (open source) za filtriranje web sadržaja na kapiji.

Za gateway koji je baziran na rešenjima kontrole sadržaja se često smatra da je teže zaobići nego rešenja desktop software-a, s obzirom da se ne mogu lako deinstalirati ili onemogućiti od strane lokalnog korisnika. (slika 2.1.)



Slika3. Prikaz gateway-a odnosno mrežne kapije

2.2. Internet Filter Review

Internet je jedan od najvećih pronalazaka svih vremena. Kako ga naše porodice koriste sve više, sve više je aktivna uloga da se moraju zaštititi najbliži od internetskog nedozvoljenog sadržaja. Iako ništa ne može da zameni dobro informisanog roditelja koji učestvuje u aktivnom delu života svog deteta, software za

filtriranje interneta dodaje jak, dodatan sloj odbrane – dajući roditeljima dodatnu meru kontrole i daljeg unutrašnjeg mira.

Software za filtriranje interneta daje mogućnost da se kontroliše prikazani sadržaj, blokiraju web stranice i postavljaju lozinke. Moćni servisi kao što su email filtriranje, popup blokiranje i nadgledanje chat prostorije su samo od nekih alata koje su raspoloživi sa današnjim software-om za filtriranje interneta – svaki dizajniran tako da spreči i zaštiti protiv taktika agresivnih online kompanija nedozvoljenih sadržaja.

Iako ne postoji savršen filter interneta na današnjem tržištu, postoji veliki broj rešenja u zavisnosti od potrebe porodice. Najvažnije osobine jednog software-a su:

- Lakoća korišćenja (Ease of Use) – je najvažnija osobina programa za filtriranje interneta koja može da se ponudi je dizajn lakoće korišćenja, koja omogućava ljudima sa različitim nivoima znanja korišćenja računara, da lako instaliraju i koriste filter u potpunosti.
- Efektivnost pri filtriranju (Effective at filtering) – software za filtriranje interneta nudi dobar balans između filtriranja nepoželjnog materijala i ne filtriranja previše sadržaja. Druga bitna osobina je sposobnost da se prilagodi osetljivost filtera za svakog člana porodice.
- Algoritam filtriranja (Filtering algorithm) – Najbolji programi za filtriranje koriste kombinaciju tehnika filtriranja, uključujući URL filtriranje, filtriranje ključnih reči i dinamičko filtriranje.
- Izveštavanje aktivnosti (Activity reporting) – Najkorisnija osobina software-a za filtriranje interneta nudi izveštaje o tome šta svaki član porodice radi na računaru, koje uključuje posećene web stranice, aktivnosti u chat prostorijama, itd.
- Na temelju klijent – server (Client-Server based) – Dobri programi za filtriranje dozvoljavaju korisnicima da odluče da li će njihovo optimalno rešenje filtriranja da bude na temelju klijenta (kućni računar), na temelju server (proxy ili provajder) ili kombinacija oba.
- Filtriranje stranog jezika (Foreign language filtering) – Efektivni software-i za filtriranje interneta nude sposobnost da filtriraju ključne reči na više jezika. Jedan od trikova koja su otkrila deca da zaobiđu internet filtere je da ukucaju na stranom jeziku isto od ključnih reči.
- Filtriranje portova i blokiranje (Port filtering and blocking) – Programi za filtriranje bi trebali da blokiraju ili filtriraju sve važnije internet protokole, uključujući web pristup, chat prostorije, email, peer-to-peer mreže, bulletin board-ovi i popup prozori.

3. ZAKONI

3.1. Pravilnik o kontroli interneta



Slika 4. Ilustracija

“Novi izmenjenipravilnik o kontroli internet stupio nasnagu. Javnost oštro kritikovala prva verziju tog dokumenta koju je predložio Ratel.

U 2009.godini ponovo je stupio na snagu Pravilnik o tehničkim uslovima za nadzor internet komunikacije. Prva verzija tog dokumenta je promenjena i iz njega su izbačene pojedine odredbe koje su izazvale negodovanje javnosti.

Nova verzija Tehničkih uslova, koji su stupili na snagu 8. januara, propisuje da hardver i softver za elektronski nadzor moraju da omoguće stvaranje neizbrisive baze podataka o prisluškivanju i nadgledanju internet komunikacije i internet aktivnosti.

Ta baza, kako se navodi u dokumentu Tehničkih uslova, mora da sadrži podatak o tome ko je obavio nadzor, o pravnom osnovu za nadzor internet aktivnosti, kao i podatke o tome koje aktivnosti su nadzirane i datum i vreme nadzora.

Iz novog pravilnika izbačena je odredba da internet operater mora da imenuje osobu za komunikaciju sa "nadležnim državnim organima" uz saglasnost državnih organa, što je jedna od odredbi koje su izazvale oštre reakcije javnosti.

Taj podzakonski document propisuje da internet operateri moraju o svom trošku da omoguće državnim organima da nadziru internet aktivnosti korisnika, kao i da im dostave podatke o korisnicima i servisima.

U saopštenju koje je povodom ponovnog stupanja na snagu Tehničkih uslova izdao Ratel, navodi se da je to podzakonski dokument i da se sprovodi u skladu sa Zakonom o telekomunikacijama, Ustavom, kao i sa Zakonom o zaštiti podataka o ličnosti koji je nedavno usvojen.

Zbog moguće zloupotrebe odbačena prva verzija pravilnika

Prva verzija pravilnika stupila je na snagu u julu 2008. godine, a protiv tog pravilnika su se izjasnili poverenik za informacije od javnog značaja Rodoljub Šabić, zaštitnik građana Saša Janković, nevladine organizacije i stručnjaci, a internet provajderi su ukazali da bi im primena tehničkog uputstva nametnula velike troškove.

Šabić je ukazao da bi primenatog pravilnika mogla da dovede do zloupotreba jer Srbija još nema zakon o zaštiti podataka o ličnosti ni funkcionalne mehanizme zaštite prava na tajnost podataka.

Ratel je Tehničke uslove stavio van snage krajem avgusta, posle konsultacija sa Zaštitnikom građana, a 22. decembra donet je novi tekst, u koji su unete izmene i na koji je "zelenosvetlo" dalo i Ministarstvo za telekomunikacije, pa je on stupio na snagu 8. januara.

U međuvremenu je usvojen i Zakon o zaštiti podataka o ličnosti, koji se primenjuje od 1. januara 2009. godine.”¹⁶

3.2. Zakonska regulativa u Srbiji

„Zloupotreba maloletnih lica (dečja pornografija) se sankcioniše u Republici Srbiji. Republika Srbija je potpisala Konvenciju o sajber kriminalu, dok se u Skupštini Srbije nalazi Nacrt zakona o ratifikovanju Sajber konvencije.

Prema rečima Zorana Kostić, na Naučnom skupu Sinergija 2009:

„U Srbiji ne postoji zvanična baza podataka o broju dece žrtava nasilja, a ni jedinstvena baza podataka o počiniocima seksualnih delikata. Članom 185 Krivičnog Zakonika Srbije sankcionisana su tri moguća načina izvršenja krivičnog dela proizvodnje i prikazivanja pornografskog materijala koji uključuju decu.“

To su prikazivanje i distribucija, koji se sankcionišu novčano, ili kaznom zatvora do dve godine i proizvodnja koja se kažnjava kaznom od šest meseci do pet godina zatvora. Samo posedovanje pornografskog materijala, ukoliko nije bilo distribucije, se ne kažnjava.“⁵

¹⁶<http://www.rts.rs/page/stories/sr/story/125/Dru%C5%A1tvo/38276/Pravilnik+o+kontroli+interneta+stupio+na+snagu.html>

⁵Dečja pornografija (http://sr.wikipedia.org/sr-el/Дечја_порнографија)

4. TESTIRANJE RAZNIH PROGRAMA ZA FILTRIRANJE I NADGLEDANJE

4.1. Internet Filter Review

Sa software-om za filtriranje interneta i pravilnim nadgledanjem, roditelji mogu da zaštite svoju porodicu od uvek prisutnog problema online nedozvoljenog sadržaja.

Opisani su:

- Skup opcija (Feature Set)
- Efekat filtriranja (Filtering Effectiveness)

■■■■■	Odlično
■■■■□	Vrlo dobro
■■■□□	Dobro
■■□□□	Slabije
□□□□□	Slabo

4.1.1. Net Nanny

Skup opcija: ■■■■■

Istaknute osobine u Net Nanny-u uključuju funkcije udaljenog upravljanja i udaljenog izveštavanja. ContentWatch je bio jedini proizvod koji je nudio ovakve povoljne osobine i sada su raspoložive pod imenom Net Nanny. Udaljene funkcije vam omogućuju da, kao administrator, budete bilo gde u svetu sa računarom i da budete povezani sa internetom, da dođete do access activity logova i pravite konfiguracijske promene. Možete biti povezani sa internetom dok ste kući, na poslu ili na odmoru. Net Nanny koristi Dynamic Contextual Analysis za filtriranje web sadržaja. Drugim rečima, CNN.com može biti blokiran ujutro zbog neke veoma nasilne nove vesti. Međutim, sat vremena kasnije, kada se sadržaj web stranice menja, sajt će ponovo biti pristupačan. Ovaj software takođe ima opciju “upozorenja” koji funkcioniše suprotno od funkcije “blokiranja”. Korisnik prima upozorenje nepoželjnog materijala, ali onda je dopušten da se prosledi bez zaustavljanja ili ograničenja. Net Nanny može redovno da obaveštava roditelje putem email-a ako deca pokušavaju da pristupe nepoželjnom materijalu. Druga praktična osobina je sposobnost da se brzo pređu blokirane web stranice pomoću lozinke.

„Porodična podešavanja”, kako se identifikuju u *Net Nanny* kontrolama, omogućavaju dodavanje izuzetaka po pitanju dozvoljenih sadržaja. U okviru istih regulativa nalaze se i usluge pristupa nadgledanim nalogima sa udaljenog računara, pa i blagovremeno slanje izveštaja o aktivnostima dece željne gledanja obnaženih devojaka. Ponovo kršenje prava na privatnost prilikom beleženja *IM* konverzacija i

temeljni listing svega što je pokrenuto ili posećeno na računaru zaokružuju ovaj, prema rečima autora, najbolji alat na tržištu.“¹⁷

Efekat filtriranja: ■■■■□

Software je testiran na preblokiranje (web stranice koje ne bi trebale da budu blokirane) i podblokiranje (web stranice koje bi trebale da budu blokirane, ali nisu). Net Nanny je prošao ovaj test uspešno ali ne savršeno. Preblokiranje se pojavilo s vremena na vreme ali odmah sa funkcijom prelaska preko toga, to nije bio veliki problem. Samo se par slučajeva podblokiranja pojavilo, čak sa web stranicama na stranim jezicima. To je prijatno iznenađenje s obzirom da većina programa za filtriranje internet imaju problem sa otkrivanjem nedozvoljenog sadržaja sa web stranica na stranim jezicima.

4.1.2. CYBERsitter

Skup opcija: ■■■■

Jedna korisna funkcija koja je raspoloživa a koju nijedan drugi proizvod nema, je sposobnost da skenira hard drive za nepoželjan materijal. Takođe će pronaći svakakve vrste špijunskih programa koje su se možda instalirale na računar, bilo da je bez reklame ili sa namerom. CYBERsitter je jedini proizvod koji sadrži osnovnu osobinu filtriranja email-a, iako ova osobina ne može da zameni tipičan proizvod za filtriranje spam-a.

Efekat filtriranja: ■■■■□

Preblokiranje (web stranice koje ne bi trebale da budu blokirane) i podblokiranje (web stranice koje bi trebale da budu blokirane, ali nisu) rade odlično u većini slučajeva.

4.1.3. CyberPatrol

Skup opcija: ■■■□□

Pravljenje profila za pojedinačne članove porodice moglo je imati još nekoliko osobina ali nije dozvoljeno da se pravi profil za web stranice i ključne reči. Kada se uporedi sa nekih drugim proizvodima, ima mnogo osobina koje nedostaju. Izveštavanje o aktivnosti na internetu je bila jedna od važnih osobina koja nedostaje.

Efekat filtriranja: ■■■■□

Podblokiranje (web stranice koje bi trebale da budu blokirane, ali nisu) je išlo bez problema u većini slučajeva. Prilikom filtriranja, program nije dozvoljavao puno nepoželjnih web stranica na stranim jezicima. Problem je da kada se jedna web stranica dozvoli, bilo koji link na toj web stranici koja vodi drugim web stranicama je takođe dozvoljen, iako bi trebao da bude blokiran. Preblokiranje (web stranice koje ne bi trebale da budu blokirane) je radilo odlično.

¹⁷ Džordž Orvel, Filtriranje internet sadržaja (<http://www.sk.rs/2009/02/sktr08.html>)

4.1.4. MaxProtect

Skup opcija: 

MaxProtect pokriva sve aspekte računara i to je alatka koja će zaštititi decu i smiriti roditelje. Neke osobine vredne spomena jesu funkcija kontrole vremena koja je laka za korišćenje i funkcija koja dozvoljava administratoru da blokira određene aplikacije. Obe su lake za instaliranje i podešavanje za svakog korisnika. U administratorskoj kontroli, može se dodati ili ukloniti web stranice ili ključne reči sa crne liste (blacklist) i izveštaji pristupa (access reports). Izveštaji uključuju Chat View, Site View i Capture View. Capture View snima ekran kada se pristupa nekoj zabranjenoj stranici.

Efekat filtriranja: 

Max Control odmah prepoznaje ključne reči sa crne liste, daje upozorenje i isključuje program. Na primer, nije se moglo ispisati reč “playboy” u polje za pretraživanje i morao se onesposobiti filter da bi se napisao izveštaj. Software je bio sposoban da napravi razliku između ključnih reči “breast” i “chicken breast” i da ispiše važne informacije. Međutim, i dalje se moglo pristupiti slikama ljudi pretraživanjem nedozvoljenih stranica koje nisu nedozvoljenog sadržaja. Takođe se moglo pristupiti nekim stranicama za odrasle koje se bave upoznavanjem, pažljivo birajući ključne reči. MaxProtect je testiran na neke poznate strane nedozvoljenih web stranica i uvek je blokirao pristup njima. Neka se filter preblokira. Drugim rečima, filtriranje se bazira na ključnim rečima, ne na sadržaju. Na primer, na CNN.com-u, kada se traže vesti vezane za “Playboy”, sve pretrage se blokiraju.

4.1.5. FilterPak

Skup opcija: 

Skup osobina je ograničen s obzirom na ostale proizvode. Nema funkcije izveštavanja i porodični profili su takođe slabiji.

Efekat filtriranja: 

Podblokiranje i preblokiranje dobro rade, čak i na stranim jezicima. Ima funkciju da pređe odmah preko blokirane web stranice ali se slabo primenjuje. Kada se prikazuje prelazak, ima problema sa upotrebom petlje za blokiranu poruku. Pojavljuje se više puta iznova. Da bi se došlo do zahtevane stranice, put može biti komplikovan sa neprijatnim dugmetom za prelazak.

4.1.6. Netmop

Skup opcija: 

Netmop ima ograničene osobine što se tiče ukupne roditeljske kontrole. Ne nudi se prelazak preko blokade, koja može biti dobra stvar, i ovaj software nema nikakvih kontrola vremena. Postoji mogućnost da se naprave podešavanja za svakog korisnika. Može se udaljeno pristupiti stranici sa podešavanjima sa bilo kojeg računara sa pretraživačem. Neka podešavanja koja se odnose na nedozvoljeni sadržaj, ne mogu da se menjaju, oni su stalno uključeni.

Efekat filtriranja: ■■■□

Netmop koristi istu mašinu za filtriranje kao i WiseChoise, koja je S4F (Server-Side Sub-System Filtering). Dobro blokira ključne reči stranica i one stranice koje se nalaze na crnoj listi. Ali ima nedostatka - na jednoj stranici je blokiralo i nakon klika na "ok", dopušta ulazak na tu stranicu.

4.1.7. Safe Eyes

Skup opcija: ■■■□

Osobina za upravljanje vremenom je laka za podešavanje. Jednostavno treba da se selektuje vreme u toku dana kada je dozvoljen pristup internetu. Može da se podesi raspored za svakog korisnika i da se ograniči ukupno vreme koje korisnik provede na internetu. Safe Eyes loguje posećene web stranice. Mogu se skladištiti web logovi za svakog korisnika na kućnom računaru ili na Safe Eyes serveru. Fajlovima na Safe Eyes serveru mogu se pristupiti sa bilo kojeg internet pretraživača. I mogu se deliti logovi sa prijateljima, tako da oni mogu da provere šta vi, kao administrator, gledate. Mogu se primiti korisna upozorenja putem email-a, tekstualna poruka ili telefonski pozivi kada neko pokuša da pristupi zabranjenoj web stranici. Ovaj software nema neke osobine kao što su udaljeno upravljanje, upozorenje umesto blokiranja i direktan prelazak preko blokiranog, pa administrator može lako da pređe filter sa lozinkom.

Efekat filtriranja: ■■■□

Safe Eyes je znao da napravi razliku između sličnih ključnih reči "breast" i "chicken breast". Prilikom pretraživanja, rezultati su bili prikazani ali klikom na neke od linkova, bili su blokirani i pretraživač se zatvorio dosta često. Mogle su se posetiti nedozvoljene slike bez mnogo napora- ako nije bilo očiglednih ključnih reči, stranica je prešla preko filtera. Safe Eyes je blokirao nepoželjne strane web stranice i rizične kao što je playboy.com.

4.1.8. WiseChoice.net

Skup opcija: ■■■□

Ovaj software je lak i nema nekih naprednih osobina. Jedine opcije su selekcija posebnih kategorija za blokiranje. Takođe se može birati da se blokira chat, email i peer-to-peer deljenje fajlova. Može se podesiti kriterijum filtriranja korisnika, tako da mlađa deca mogu imati drugačija podešavanja nego adolescent ili odrasli u porodici. WiseChoise osobine nude kontrolu vremena i širokog izveštaja.

Efekat filtriranja: ■■■□

WiseChoise je znao da napravi razliku između sličnih ključnih reči "breast" i "chicken breast" i čak je blokirao sumnjivu vest. Takođe je blokirao nepoželjne strane web stranica i rizične kao što je playboy.com. Ali ima nedostatka - na jednoj stranici je blokiralo i nakon klika na "ok", dopušta ulazak na tu stranicu.

4.1.9. Cyber Sentinel

Skup opcija: ■■■□

Ovde nema profila tako da ne treba da se bira da se podesi aplikacija drugačije za roditelje za razliku od dece. Nema funkcije izveštavanja. Ali postoji sposobnost da se prave slike monitora i tako vide blokirane stranice.

Efekat filtriranja: ■■■□

Preblokiranje/podblokiranje je dobro ali ne savršeno. Dopušta ulaz na mnoge stranice na koje ne bi smelo, naročito na stranom jeziku.

4.1.10. McAfee Parental Controls

Skup opcija: ■■■□

Postoji veoma puno opcija i pojedinačnih podešavanja ali su teški za razumevanje.

Efekat filtriranja: ■■■□

Preblokiranje/podblokiranje je odlično ali kada se javi blokirana strana i prikaže funkcija prelaza, postoji upotreba petlji kod opcije prelaska.

4.2. Access Control List (ACL) – Lista kontrole pristupa

U računarskoj bezbednosti, lista kontrole pristupa (access control list – ACL) je lista dozvola pripojenih jednom objektu (slika, URL, tekst). Lista opisuje kome ili čemu je dozvoljeno da pristupi objektu i koje operacije su dozvoljene da se izvedu na objektu. U tipičnom ACL-u, svaki unos na listu opisuje jedan subjekat i operaciju: na primer, unos (Alice, delete) na ACL-u za fajl XYZ daje Alice dozvolu za brisanje fajla XYZ.¹⁸

4.2.1. Bezbednosni modeli bazirani na ACL-u

Na jednom bezbednosnom modelu koji se bazira na ACL-u, kada subjekat zahteva da izvede operaciju na jednom objektu, sistem prvo proverava listu za primenjiv unos da bi odlučio da li da izvede operaciju ili ne. Ključno pitanje u definisanju bilo kojeg bezbednosnog modela koji se bazira na ACL-u je na koji način je ACL uređen. Za svaki objekat (svojstva, karakteristika); ko može da menja ACL na objektu i koje promene su dozvoljene.

Sistemi koji koriste ACL, mogu biti podeljeni u dve kategorije: voljna i obavezna (discretionary and mandatory). Za sistem se kaže da ima voljnu kontrolu (discretionary access control) ako vlasnik objekta može u potpunosti da kontroliše pristup objektu, uključujući, na primer, menjanje ACL-a objekta da bi omogućio pristup bilo kome drugom. Za sistem se kaže da ima obaveznu kontrolu (mandatory access control ili non-discretionary access control) u bezbednosnoj literaturi, ako ga prisiljava na ograničenja širokog kruga sistema koja prelaze preko dozvola napomenutih u ACL-u.

¹⁸ Access Control List - <http://c2.com/cgi/wiki?AccessControlList>

Tradicionalni ACL sistemi određuju dozvole za pojedinačne korisnike, koji mogu da postanu nespretni u sistemu sa velikim brojem korisnika. U novijem pristupu zvanim kontrola pristupa na bazi funkcije (role-based access control), dozvole su određene funkcijama, a funkcije su određene korisnicima.

4.3. Proxy server

Proxy server je server (kompjuterski sistem ili aplikacioni program) koji uslužuje zahteve svojih klijenata prosleđivanjem zahteva drugim serverima. Klijent se povezuje na proxy server, zahteva neke servise, kao što su fajl, konekcija, web stranica, ili drugi resurs, raspoloživ sa drugačijeg servera. Proxy server pruža resurs povezivanjem na poseban server i zahtevanjem servisa u ime klijenta. Proxy server može opcijski da menja klijentov zahtev ili serverov odgovor, i ponekad može da servira zahtev bez kontaktiranja posebnog servera. U ovom slučaju, keširao bi se prvi zahtev na udaljenom računaru, tako da bi zadržao informaciju za kasnije, čineći time bržu uslugu.

Proxy server koji propušta sve zahteve i odgovara nepromenjeno se obično naziva gateway ili ponekad tunneling proxy.

Proxy server može da bude smešten u lokalnom korisnikovom računaru ili na posebnim ključnim tačkama između korisnika i odredišnih servera ili na internetu.

4.3.1. Keširani (caching) Proxi server

Proxi server može da preda zahteve bez kontaktiranja posebnog servera, vraćanjem sadržaja koji je sačuvan od prošlog zahteva, koji je podneo isti ili drugi klijent. Ovo se zove keširanje. Keširani proxi čuva lokalne kopije trenutno zahtevanih resursa, dozvoljavajući velikim organizacijama da značajno smanje svoje korišćenje i cenu, i usput značajno povećavaju radni učinak. Postoje definisani zakoni za keširanje. Neki loše odrađeni keširani proxi serveri imaju loše strane (npr. nesposobnost da koriste korisnikovu autorizaciju).

4.3.2. Mrežni (web) proxi

Proxi koji se fokusira na www saobraćaj, zove se mrežni proxi. Mrežni proxi se najviše koristi kao mrežni keš. Većina proxi programa (npr. Squid, Ncncache) uslužuje način da zabrani pristup određenim web stranicama na crnoj listi, time uslužujući filtriranje sadržaja. Ovo se obično koristi u kolektivoj sredini, iako sa sve više korišćenim Linuxom u malim poslovima i kućnim upotrebama, ova funkcija više nije ograničena velikim kolektivima. Neki mrežni proxi serveri preformatiraju web stranice za posebne svrhe ili publiku (npr. mobilni telefoni).

4.3.3. Proxi za mrežu filtriranja sadržaja (Content Filtering Web Proxy)

Filtriranjem sadržaja, mrežni proxi server uslužuje administrativnu kontrolu nad sadržajem koji može biti položen kroz proxy. Obično se koristi u komercijalnim i

nekomercijalnim organizacijama (naročito u školama) kako bi osiguralo da korišćenje interneta odgovara prihvatljivoj politici korišćenja.

Metode koje se obično koriste za filtriranje sadržaja sadrže: URL (Uniform Resource Locator) ili DNS crne liste, URL regex (regular expression) filtriranje, MIME (Multi-purpose Internet Mail Extension) filtriranje, ili filtriranje ključne reči sadržaja. Neki proizvodi su poznati po tome što upotrebljavaju tehnike analiziranja sadržaja koji traže osobine koje se obično koriste od strane određene vrste dobavljača sadržaja.

Proxy za filtriranje sadržaja će često da podrži sigurnost korisnika, da bi kontrolisao pristup mreži. Takođe često pravi logove, da bi davao detaljne informacije o URL-u kojima su pristupili posebni korisnici, ili da nadgleda statistike širine opsega korišćenja. Takođe mogu da komuniciraju sa antivirus programom koji se baziraju na daemon-u ili ICAP-u (Internet Content Adaptation Protocol) da bi obezbedili sigurnost protiv virusa ili drugog malware-a (malicious-logic software) skeniranjem ulazećeg sadržaja u realnom vremenu pre nego što uđe na mrežu.

4.3.4. Anonimni (Anonymizing) proxy server – serveri za zaštitu privatnosti

Anonimni proxy server (ponekad zvani mrežni proxy) ustvari pokušava da anonimizira mrežno surfovanje. Oni lako mogu da budu podređeni administratorima web stranica i tako postanu beskorisni u nekim slučajevima. Postoji nekoliko vrsta anonimizatora.

Kontrola pristupa: neki proxy serveri izvršavaju zahtev prijave. U velikim organizacijama, autorizovani korisnici moraju da se uloguju da bi postigli pristup mreži. Organizacija može s toga da prati pojedinačno korišćenje.

4.3.5. Neprijateljski (Hostile) proxy

Proxy serveri mogu biti instalirani od strane online kriminala, da bi špijunirali tok podataka između klijentovog računara i mreže. Sve pristupačne web stranice, isto kao i sve podnešene forme, mogu biti uhvaćene i analizirane putem proxy operatora. Zbog ovog, lozinke za online servise (kao što su webmail i bankarstvo) bi trebalo da se promene ako se otkrije neki nepoznati proxy.

4.3.6. Sprečavani (Intercepting) proxy server

Sprečavani proxy (takođe poznat i kao “providni proxy”) spaja proxy server sa gateway-om. Konekcije putem pretraživača kroz gateway su preusmerene kroz proxy bez klijent-strana u konfiguraciji.

Sprečavani proxy serveri su obično korišćeni u poslovanju da bi sprečili izbegavanje prihvatljive politike korišćenja, i da bi se olakšao administrativni teret, s obzirom da nisu zahtevane konfiguracije pretraživača.

Često je moguće otkriti korišćenje sprečavanog proxy servera upoređivanjem externe IP adrese sa adresom koja je viđena na nekom externom mrežnom serveru, ili isprobavajući HTTP naslove na strani servera.

4.3.7. Providni i neprovidni (Transparent and non-transparent) proxy server

Termin “providni proxy” se najčešće koristi neispravno da znači “sprečavani proxy” (zato što klijent ne treba da konfiguriše proxy i ne može direktno da otkrije da mu zahtevi idu preko proxija).

Međutim, postoje razne definicije koje nudi RFC 2616 (Hypertext Transfer Protocol -- HTTP/1.1):

“Providni proxy je proxy koji ne modifikuje zahtev ili odgovor izuzev što je zahtevano za proxy provere i identifikacije”.

“Neprovidni proxy je proxy koji modifikuje zahtev ili odgovor da bi obezbedio neke dodatne servise korisnikovom agentu, kao što su servisi grupne napomene, transformacije medije, ograničenog protokola ili filtriranja anonimnosti”.

4.3.8. Prisiljeni (Forced) proxy

Termin “prisiljeni proxy” je dvosmislen. Znači i “sprečavani proxy” (zato što filtrira sav saobraćaj na jedinom raspoloživom gateway-u na internetu) i njegovu tačnu suprotnost “nesprečavani proxy” (zato što je korisnik prisiljen da konfiguriše proxy da bi pristupio internetu).

Operacija prisiljenog proxija je ponekad neophodna zbog problema sa sprečavanjem TCP konekcije i HTTP-a. Na primer, sprečavanje HTTP zahteva može da deluje na korišćenje proxy keša, i može veoma da deluje na određene sigurnosne mehanizme. Ovo je prvenstveno zbog toga što klijent misli da se on obraća serveru, i tako su naslovi zahtevani od strane proxija nesposobni da budu različiti od naslova koji mogu biti zahtevani od strane uzvodnog servera (naročito sigurnosni naslovi). Takođe HTTP specifikacija zabranjuje keširanje odgovora tamo gde zahtev sadrži autorizovani naslov.

4.3.9. Otvoreni (Open) proxy server

Iz razloga što proxy serveri mogu biti korišćeni za zloupotrebu, sistem administratori su razvili više načina da odbace servis da bi otvorili proxy servere. Mnoge IRC mreže automatski testiraju klijent sisteme na poznatim vrstama otvorenog proxija. Takođe, email server može biti konfigurisan da automatski testira email sender-e za otvorene proxy servere.

Etika automatskog testiranja klijenata za otvorene proxy servere su sporna. Neki eksperti smatraju da je takvo testiranje isto kao i skeniranje portova napadača na klijentovom serveru. Drugi smatraju da klijent traži skeniranje povezivanjem na server čiji servis uključuje testiranje.

4.3.10. Povratni (Reverse) proxy server

Povratni proxy je proxy server koji je instaliran u susedstvu jednog ili više mrežnih servera. Sav saobraćaj koji dolazi sa interneta i sa odredišta jednog od mrežnih servera prolazi kroz proxy server. Postoji nekoliko razloga za instaliranje povratnog proxy servera:

- Šifriranje/SSL (secure socket layer) ubrzavanje: kada su sigurnosne web stranice napravljene, SSL šifriranje često nije odrađeno sa strane samog web servera, nego sa strane povratnog proxija koji je opremljen sa SSL ubrzavanjem
- Balansiranje tereta: povratni proxy može da raspodeli teret na nekoliko web servera, svaki web server nudeći svoje područje aplikacija. U takvom slučaju, povratni proxy možda treba da prepíše svaki URL na svakoj web stranici (prevod od eksterno znanih URL-ova na internet lokacije).
- Servis/keš statični sadržaj: Povratni proxy može da se reši web server keširanjem statičnog sadržaja kao što su slike i drugi statičko grafički sadržaj.
- Kompresija: proxy server može da optimizuje i kompresuje sadržaj da bi ubrzao vreme load-ovanja.
- Dostavljanje odgovora (spoon feeds) : Ograničava korišćenje resursa prouzrokovanjem sporih klijenata na web serverima keširanjem sadržaja koji web server šalje i polako dostavlja odgovore klijentu.
- Bezbednost: proxy server je dodatni sloj odbrane i može da štiti protiv nekih operativnih sistema i posebnih napada web servera.
- Ekstranet objavljivanje: povratni proxy server suočavajući se sa internetom, može da se koristi za komunikaciju sa firewall-nim serverom unutar neke organizacije, pružajući ekstranet pristup nekim funkcijama dok servere drže u pozadini firewall-ova. Ako se koristi u ovom slučaju, mere bezbednosti bi mogle da se primene da bi se zaštitio ostatak infrastructure u slučaju da je ovaj server nagođen, pošto je njegova web aplikacija izložena napadu sa interneta.¹⁹

4.4. Preskakač (Circumventor)

Preskakač je metod poražavanja blokiranih načina rada koji se izvršavaju koristeći proxy servere. Većina preskakača su takođe proxy serveri, različitog stepena profinjenosti, koji je efektivno izvršio “način rada sa preskakivanjem”.

Preskakivač je stranica koja se bazira na mreži. On uzima stranicu koja je blokirana i “preskakuje” je do neblokirane web stranice, dozvoljavajući korisniku da vidi blokirane stranice. Poznat primer je “elgooG”, koji dozvoljava korisnicima u Kini da koriste Google nakon što je tamo blokirano. elgooG se razlikuje od većine preskakača u tome da preskače samo jedan blok.

¹⁹ Proxy Server - <http://www.publicproxyservers.com>

Studenti su u mogućnosti da pristupe blokiranim stranicama (igrice, chat prostorije, messenger, uvredljiv materijal, nedozvoljeni sadržaj na internetu, društveno umreženje, itd.) kroz preskakač. Dok software za filtriranje blokira preskakače, drugi ih propuštaju. Međutim, u nekim slučajevima filter ipak može da spreči saobraćaj do preskakača, iako osoba koja upravlja filterom može da vidi stranice koje su posećene.

Preskakače takođe koriste ljudi koji su blokirani sa web stranice.

Jedan drugi način korišćenja preskakača je da se dozvoli pristup servisima određenih zemalja, tako da korisnici interneta iz drugih zemalja takođe mogu da imaju koristi od njih. Primer za to je razmnožavanje medija i prenos vesti kroz mrežu (webcast) za zemlje ograničenja.

Korišćenje preskakača je obično bezbedno sa izuzetkom da se preskakačka stranica koja se koristi sa nepouzdanе treće strane, može biti korišćena sa skrivenim namerama, kao što su sakupljanje ličnih podataka, i kao rezultat korisnici su obično savetovani da kroz preskakač ne koriste lične podatke kao što su broj kreditne kartice ili lozinka.

4.4.1. U školama i kancelarijama

Mnoga radna mesta i škole ograničuju web stranice i online servise koje su raspoložive u njihovim zgradama. Pošto su preskakači korišćeni za zaobilazjenje cenzura u računarima, društvena umreženja i druge stranice smatraju gubljenjem vremena ili resursi postaju mete masovnog zabranjivanja.

Vlasnici proxy web servera su postali sve veštiji, dozvoljavajući korisnicima da šifruju linkove i bilo kakve podatke koji idu i dolaze od drugih web servera. Ovo omogućava korisniku da pristupi web stranicama koje bi inače bile blokirane.

Posebna vrsta web proxy servera su "CGI proxy serveri". To su web stranice koje dozvoljavaju korisniku da pristupe stranici kroz njih. Oni obično koriste PHP ili CGI da bi izvršili funkciju proxija. Ove vrste proxy servera su privremeno korišćene da steknu pristup web stranim koje su blokirane kolektivnim ili školskim serverima. Pošto oni takođe sakrivaju korisnikovu IP adresu od web stranica kojima pristupaju kroz proxy, oni su ponekad korišćeni da steknu stepen anonimnosti, zvanog "izbegavanje proxija".

4.5. Rizik prilikom korišćenja proxy servera za zaštitu privatnosti

Korišćenjem proxy servera (npr. proxy za zaštitu privatnosti), svi podaci poslati servisu koji su korišćeni (npr. HTTP server u web stranici) moraju proći kroz proxy server pre nego što budu poslani servisu, većinom u nekodiranoj formi. Moguće je, kako je već predstavljeno, za zloćudan proxy server da zabeleži sve što je poslato proxiju: uključujući nekodirane prijave i lozinke. Međutim, ako se koristi HTTP proxy kao što je LinkItTo, ta informacija će se kodirati time ga čineći težim za lopove da ukradu informacije.

Ulančavanjem proxy servera koji ne otkrivaju podatke o originalnom podnosiocu zahteva, moguće je zamračiti aktivnosti od očiju korisnikovog cilja. Međutim, više tragova će ostati na prelaznim skokovima, koji bi mogli da se koriste

ili da se ponude sve do tragova korisnikovih aktivnosti. Ako su način rada i uprava ovih drugih proxy servera nepoznati, korisnik može da postane žrtva lažnog osećaja bezbednosti samo zato što su ti detalji nevidljivi.

Donja linija ovoga je biti pažljiv kada se koriste proxy serveri, i samo koristiti proxy servere koji su poznatog integriteta (npr. vlasnik je poznat i pouzdan, ima čist tajni način rada, itd.), i nikad ne koristiti proxy servere nepoznatog integriteta. Ako baš moraju da se koriste nepoznati proxy serveri, ne prenositi nikakvu ličnu informaciju (ako nije pravilno kodovana) kroz proxy.

4.5.1. Proxy software-i

- AlchemyPoint je proxy server koji može i korisnik da programira. Služi da bi prepisao web stranice, email-ove, instant messenger poruke, i druge mrežne prenose na putu.
- Apache HTTP Server može da se konfiguriše tako da se ponaša kao proxy server.
- Blue Coat-ov (ranije Cacheflow-ov) izgrađen SGOS su proxy serveri 15 protokola uključujući HTTPS/SSL, ima široku politiku i pokreće se na širokom opsegu uređaja od ispostave do preduzeća.
- EZproxy je URL prepisujući web proxy koji je dizajniran prvenstveno za snabdevanje udaljenog pristupa sajtovima koji overavaju korisnike po IP broju.
- JAP je lokalni proxy, software za anonimiziranje web-a koji se povezuje na lance proxy servera različitih organizacija.
- Microsoft Internet Security i Acceleration Server je proizvod koji se pokreće na Windows 2000/2003 serverima i sastavljaju funkcije i proxy servera i firewall-a.
- Nginx je web i povratni proxy server koji može da se ponaša kao POP3 proxy server.
- Privoxy je besplatan, open source web proxy sa osobinama poverljivosti i blokiranja reklama.
- Proxomitron – je web proxy koji može i korisnik da konfiguriše. Služi da bi prepisao web stranice na putu. Većina je poznata po blokiranju reklama, ali ima i mnoge druge korisne osobine.
- SafeSquid pravljen je u Linux okruženju, kompletan proxy za filtriranje sadržaja HTTP1.1, dozvoljava raspodelu “profilne” pristupe internetu.

- SSH je sigurnosni oklop (Secure Shell) koji može biti konfigurisan tako da zastupa (proxify) vezu, postavljanjem SOCKS proxija na klijenta, i kanalisanjem saobraćaja kroz SSH konekciju.
- Sun Java System Web Proxy Server je keširani proxy server koji se pokreće na Solaris-u, Linux-u i Windows serverima koji podržavaju HTTP/S, NSAPI I/O filtere, dinamičku rekonfiguraciju, SOCKSv5 i povratni proxy.
- Squid cache je popularan HTTP proxy server u UNIX/Linux svetu.
- inproxy je brz i lak HTTP proxy koji je idealan za ugrađeno korišćenje na POSIX operativnim sistemima.
- Tor je sistem na bazi proxija koji služi za anonimizaciju internet veze.
- Varnish je dizajniran da bude kvalitetno izvršen keširani povratni proxy.
- WinGate je više-protokolni proxy server i NAT rešenje koji može da se koristi da preusmeri bilo koju vrstu saobraćaja na Microsoft Windows serveru.
- WWWOFFLE postoji od 1990-ih godina, i razvijen je za skladištenje online podataka za offline korišćenje.
- yProxy je NNTP proxy server koji pretvara yEnc dodatke u obliku kodiranih poruka u UU Kodovanje, kompletan sa SSL podrškom klijenta.
- Ziproxy je nekeširani proxy za svrhu ubrzanja. Ponovo smanjuje slike i optimizira HTML kod.

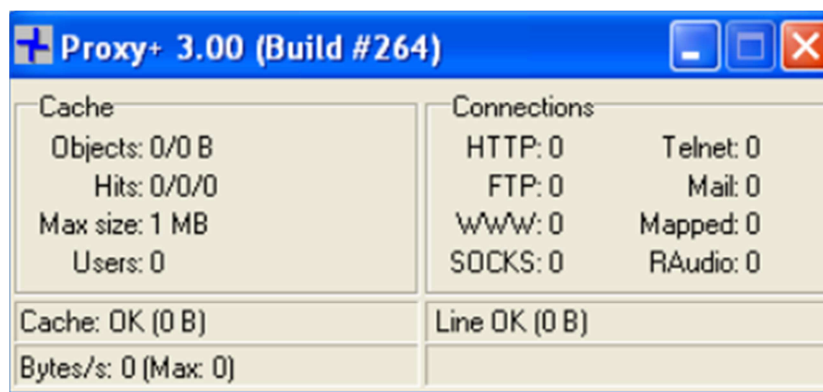
5. REŠAVANJE PROBLEMA

5.1. Proxy Plus

Proxy+ (slika 1.) je program koji se može pokrenuti na radnoj stanici ili na server sa MS Windows9x, Windows NT, Windows ME, Windows 2000, Windows XP ili Windows 7 i veza za internet. Proxy+ radi kao firewall proxy server i kao mail server. Sve radne stanice mogu koristiti Proxy+ servise putem TCP/IP protokola.

Osnovne karakteristike su:

- Firewall povećava bezbednost izdvajanjem LAN-a sa interneta
- Disk keš sa naprednim upravljanjem
- Mail server sa intranet mail sposobnošću
- Automatsko razvrstavanje ulaznih poruka
- Automatsko biranje/prekidanje prekidača telefonske linije
- Podrška istovremene (sinhronizovane) i neusklađene (asinhronizovane) namenske linije
- WWW server za intranet
- Upravljanje svim funkcijama putem WWW interface-a
- Doživotna besplatna dogradnja (upgrade), besplatna email podrška
- Potpuna funkcija 3 korisnika besplatna verzija, 31 dan neograničene besplatne probne verzije

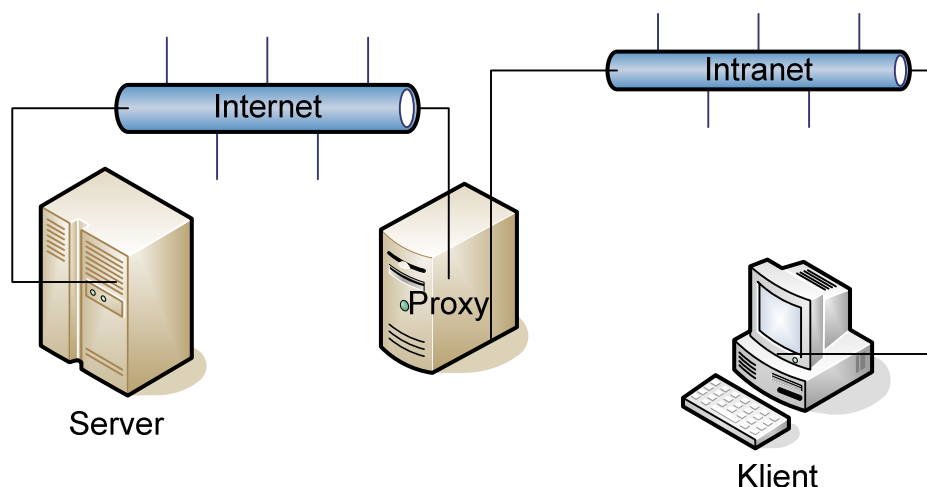


Slika 5. Izgled programa Proxy+

Potrebno je isključiti proxy u pretraživaču jer se proxy posmatra (npr. Mozilla Firefox) – tools – options – advanced – settings – manual proxy configuration - HTTP proxy: localhost; port: 8080; no proxy for: localhost.

Sva podešavanja programa su dostupna korišćenjem www pretraživača. Adresa interface-a je `http://x.x.x.x:4400`, gde je x.x.x.x ime ili IP adresa računara sa Proxy+ -em.

Proces povezivanja dva računara u Ethernet mreži. Prvi računar je server i on se povezuje na internet sa unutrašnjom IP adresom. Drugi računar je klijent i on je povezan na gateway prvog računara (slika 2.).



Slika 6. Prikaz povezivanja dva računara na internet preko Proxy-a

5.1.1. Podešavanja za server računar:

IP adresa 192.168.125.124

Subnet mask: 255.255.255.0

5.1.2. Podešavanja za klijent računar:

IP adresa: 192.168.125.190

Subnet mask: 255.255.255.0

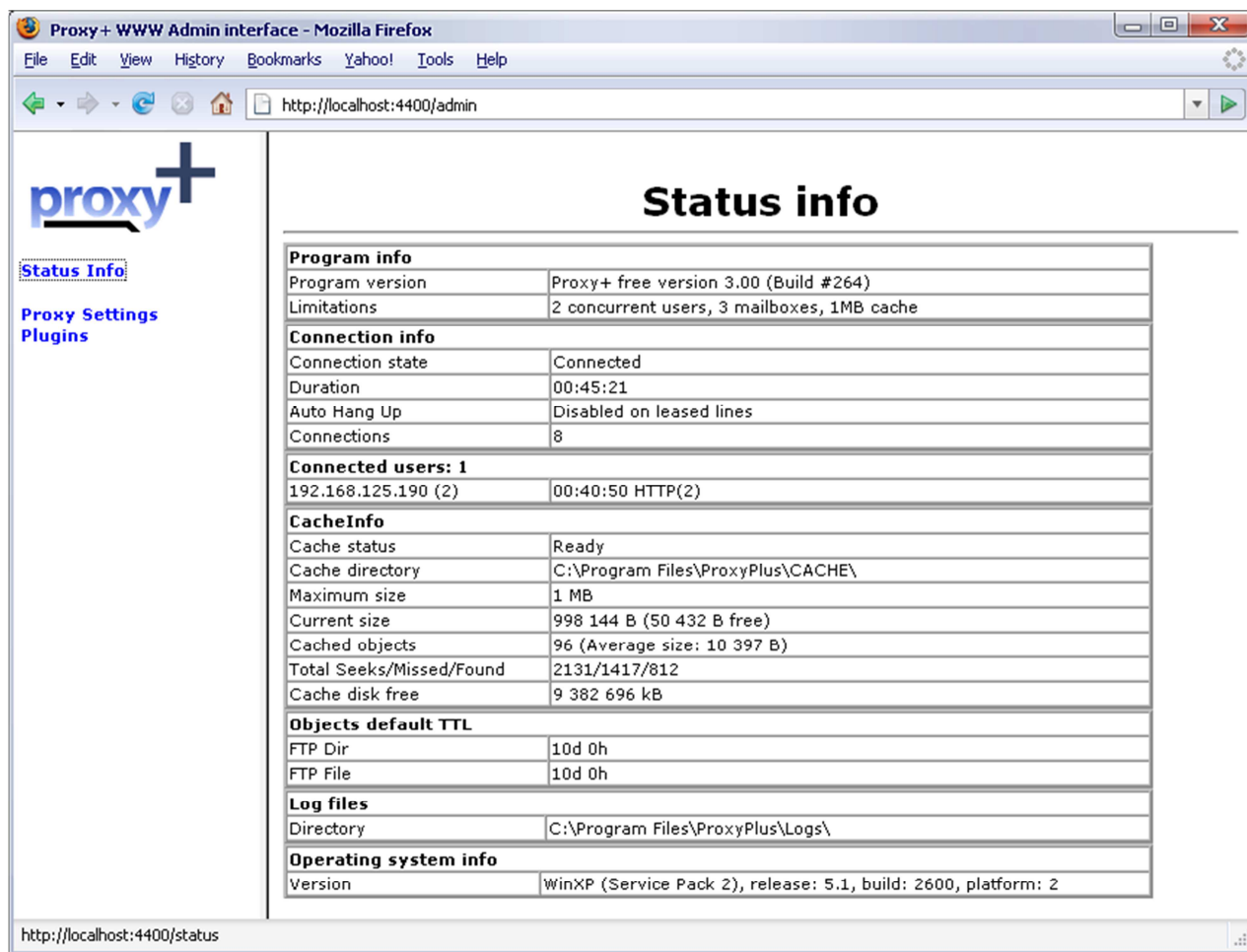
Default gateway: 192.168.125.124

Preferred DNS server: 192.168.125.124

Opcije programa: Status Info (slika 3.), Proxy Settings, Plugins

Proxy Settings:

Dial-up settings, Proxies Setup, Cascading General Setting, Cache General Setup, DNS Cache General Setup, General Account Settings, General Mail Settings, General Alarm Settings, Antivirus General Settings, Filter General Settings, General Security Settings, Access List General Settings, WWW Server Settings, Log Files, Utilities, Administrator General Settings.



Slika 7. Proxy+ Admin interface - Status info

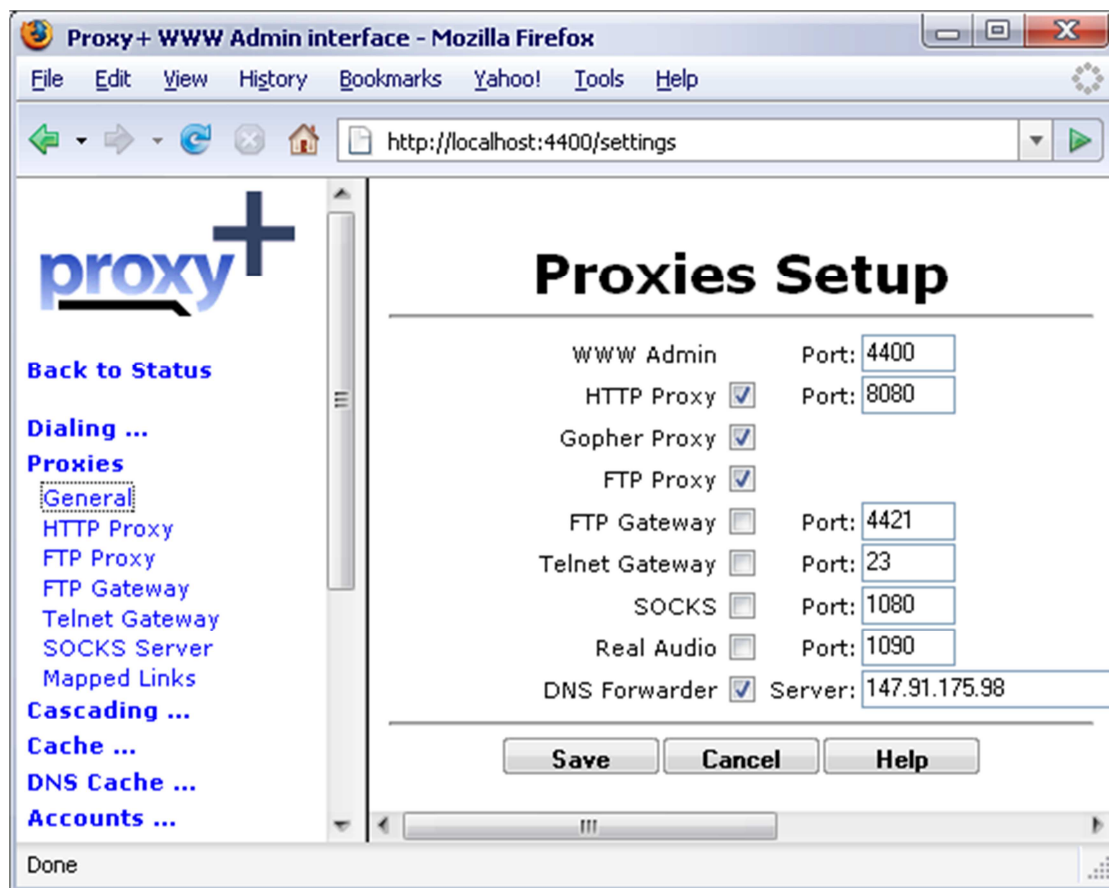
5.1.3. Podešavanje programa (slika 4.):

Sva podešavanja idu kroz pretraživač.

Proxies General - http proxy port 8080

Kada se želi otvoriti neka web stranica, ide DNS upit. Kada pretraživač dobije odgovor, (npr. `www.subotica.com`), dobija IP broj te web stranice, i vuče sadržaj sa te adrese.

DNS Forwarder je omogućen, Server ima IP adresu: 147.91.175.98



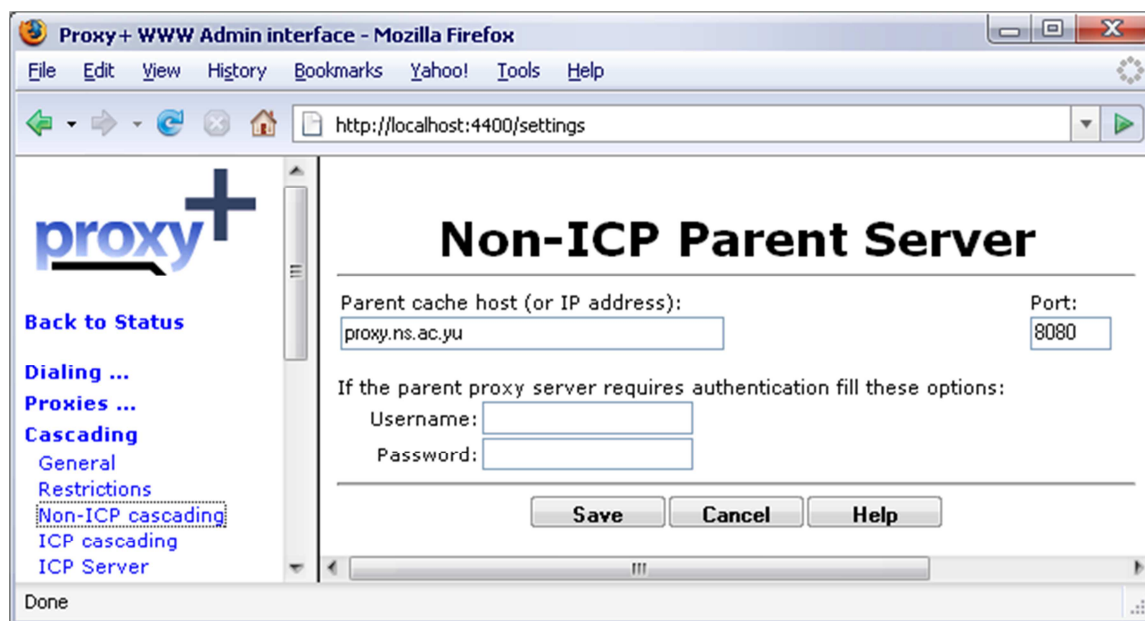
Slika 8. Podešavanje programa

Cascading-Non-ICP cascading (ICP – internet cache protocol)

Parent cache host (or IP address): proxy.ns.ac.yu

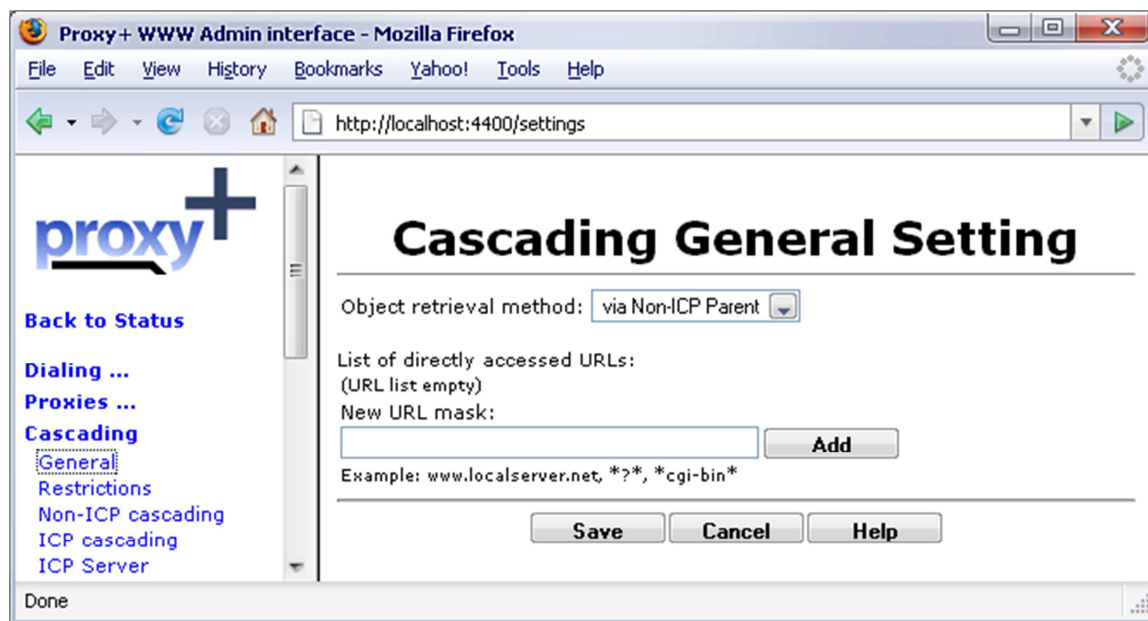
Port: 8080

Zbog akademske mreže, proxy server se obraća ovom hostu (slika 5.).



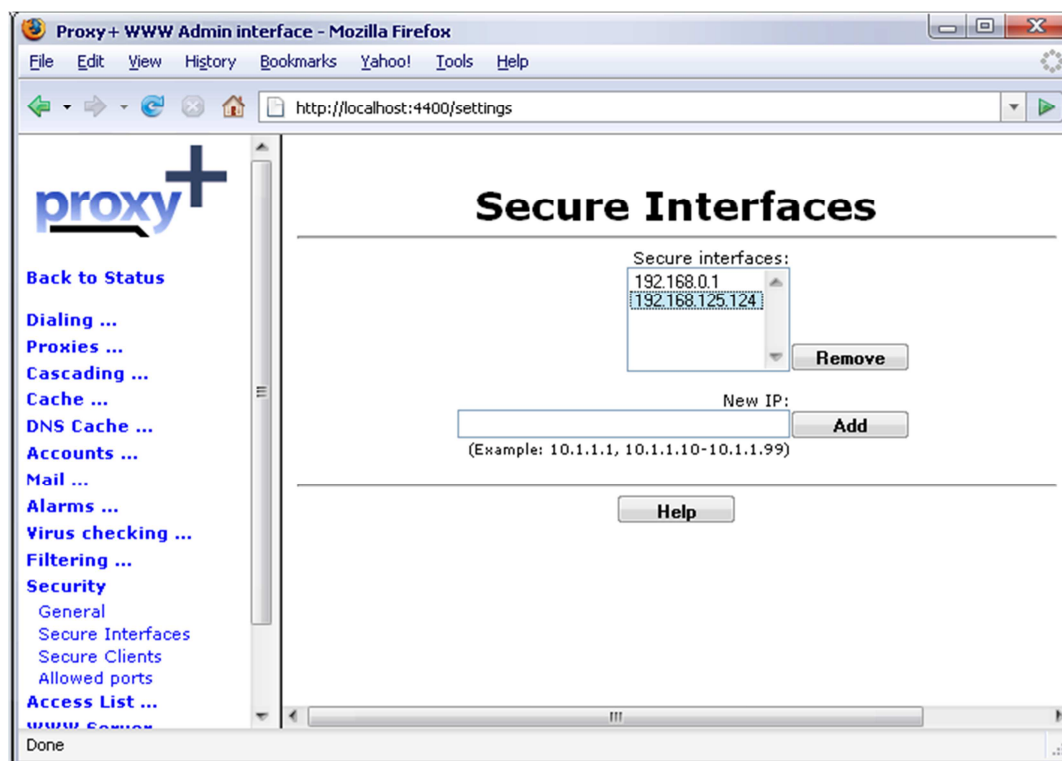
Slika 9. Non-ICP Parent Server

U podešavanjima Cascading-a, za objekat metode pretraživanja biramo: via non-ICP parent (slika 6.).



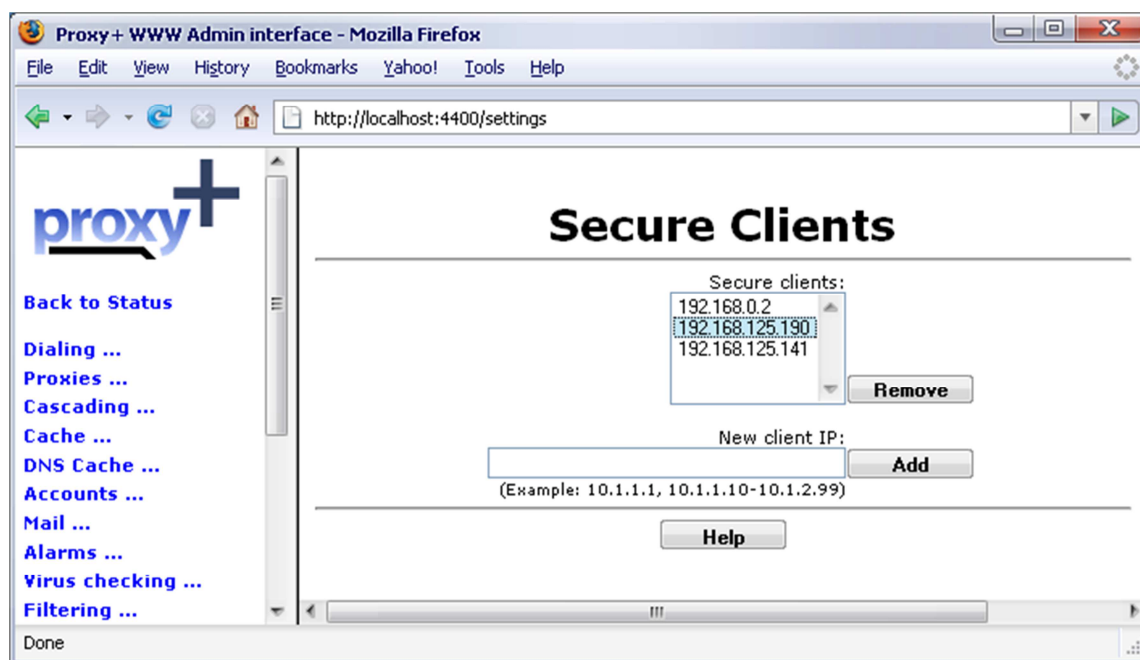
Slika 10. Cascading podešavanja

Biramo sigurnosne interface-e (slika 7.):
192.168.125.124



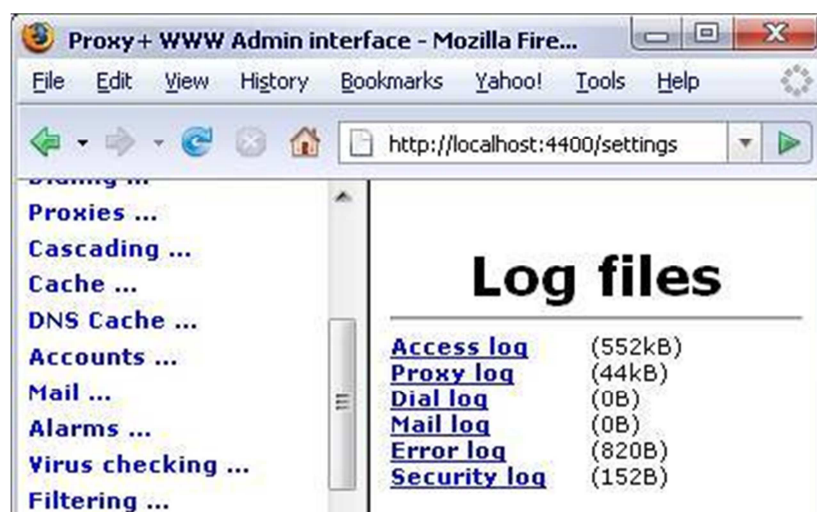
Slika 11. Sigurnosni interface

Biramo sigurnosne klijente: 192.168.125.190
Klijent ima izlaz samo na pretraživač (slika 8.).



Slika 12. Sigurnosne klijente

Log fajlovi: Access log, Proxy log, Dial log, Mail log, Error log, Security log.
Smeštamo ih u direktorijum za log fajlove. C:\ProgramFiles\ProxyPlus\Log\ (slika 9.)

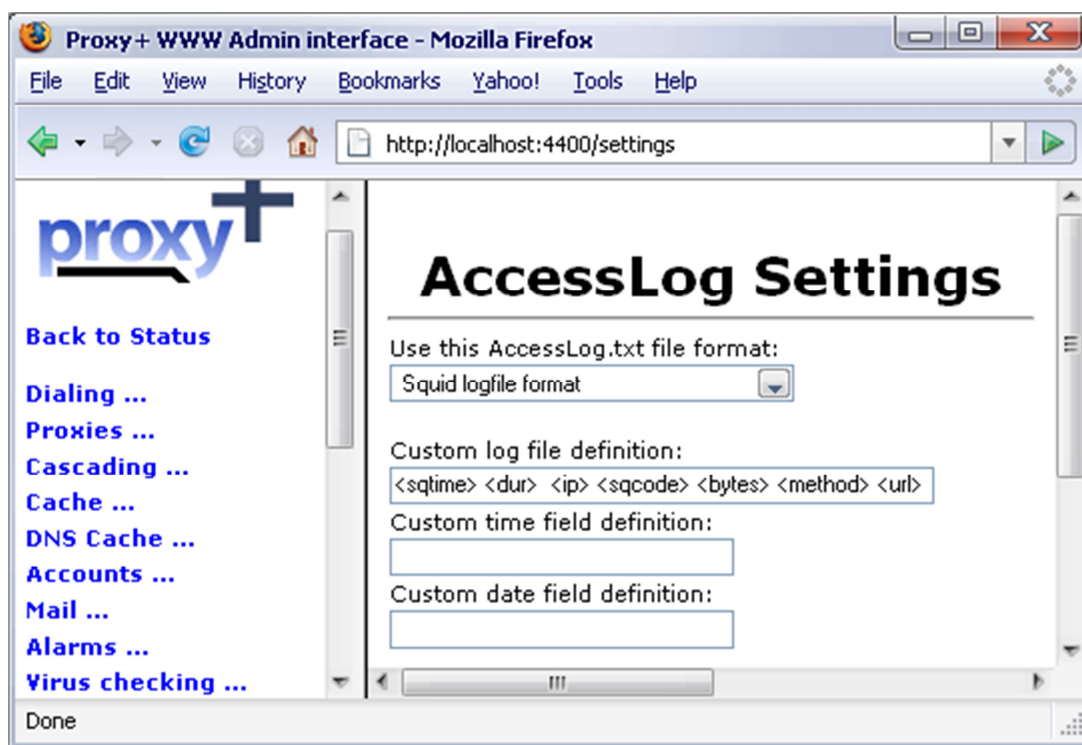


Slika 13. Log fajlovi

Biramo u kom formatu želimo da primamo log fajlove (slika 10.). Log files - Use this AccessLog.txt file format (squid logfile format).

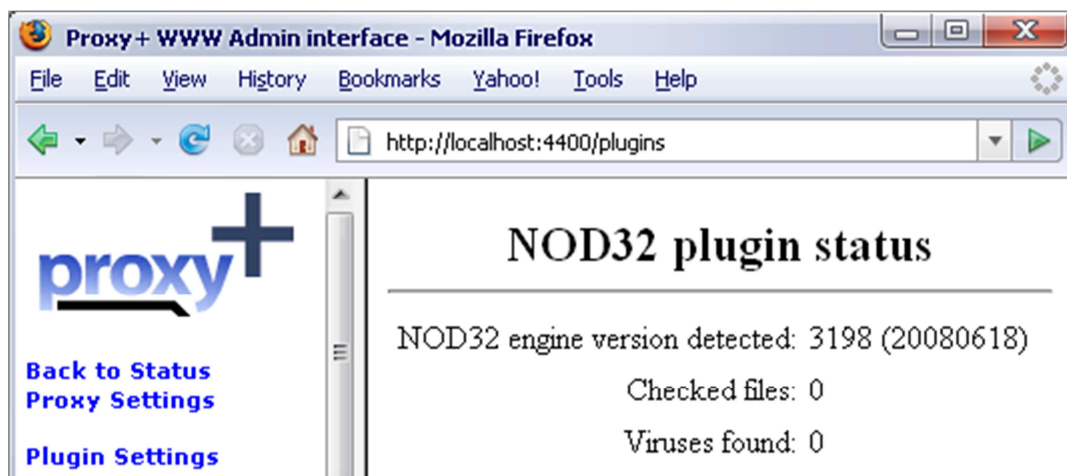
Prilagodimo definiciju log fajla. Custom log file definition:

<sqtime> <dur> <ip> <sqcode> <bytes> <method> <url> - <sqhcode>
<ctype>



Slika 14. Biranje formata log fajlova

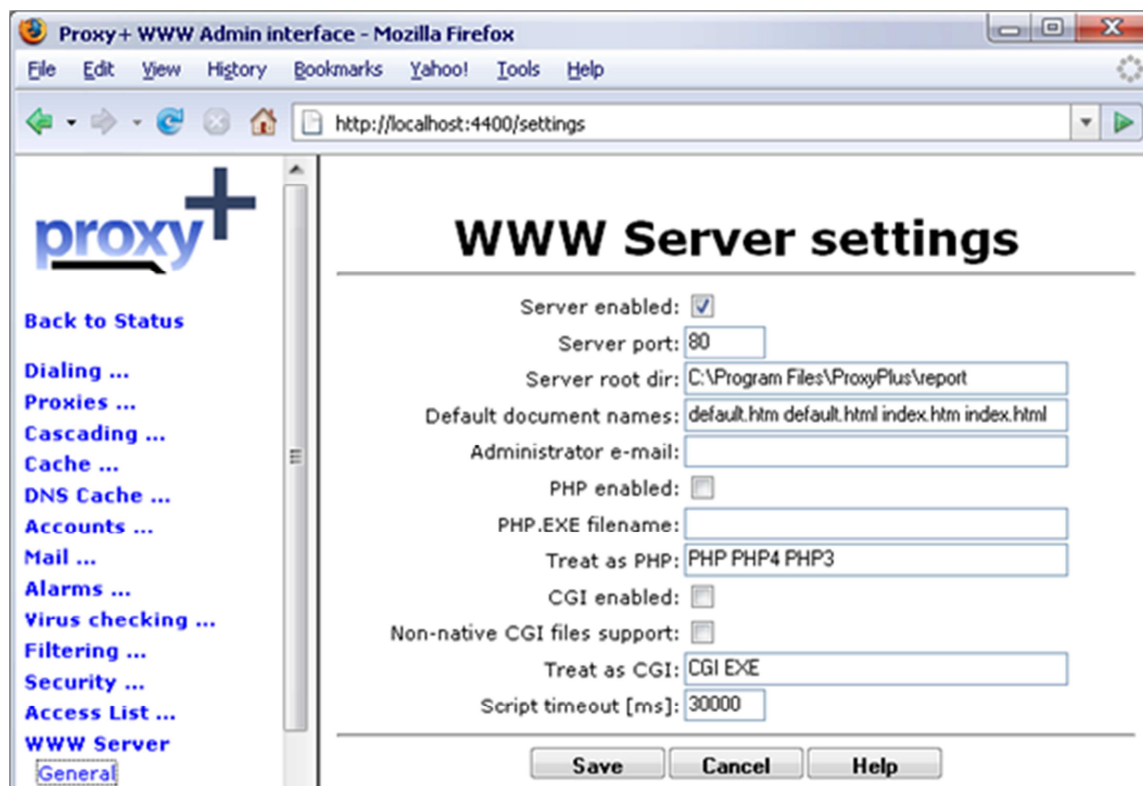
Treba omogućiti plugins i izabrati NOD32. Ovim smo podesili opciju da prilikom prolaska nekog fajla kroz proxy plus, anti virus program (u ovom slučaju NOD32) proverava da li taj fajl sadrži neki virus (slika 11).



Slika 15. NOD 32 plugin provera

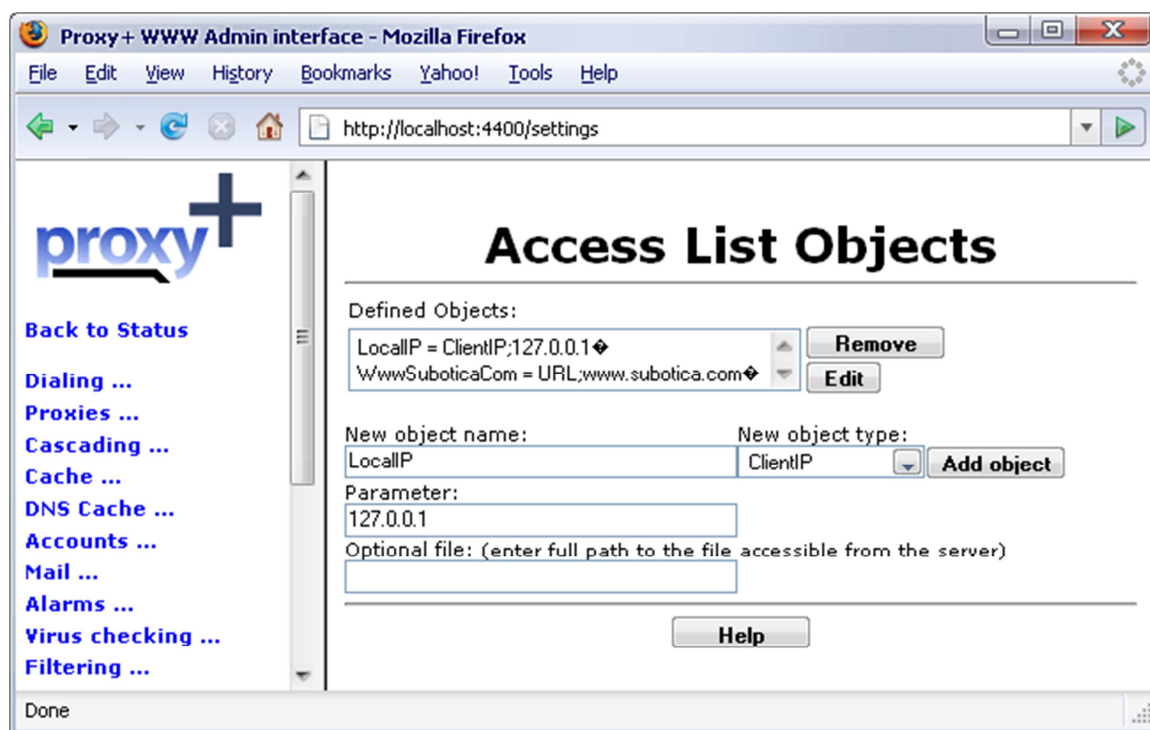
U podešavanjima www servera omogućujemo server i na taj način možemo stavljati neku web stranicu. Server root dir pokazuje putanju gde su smešteni fajlovi

koji generišu izveštaj. Pokretanjem localhost-a u pretraživaču, ispisuje se u html formatu (slika 12.).



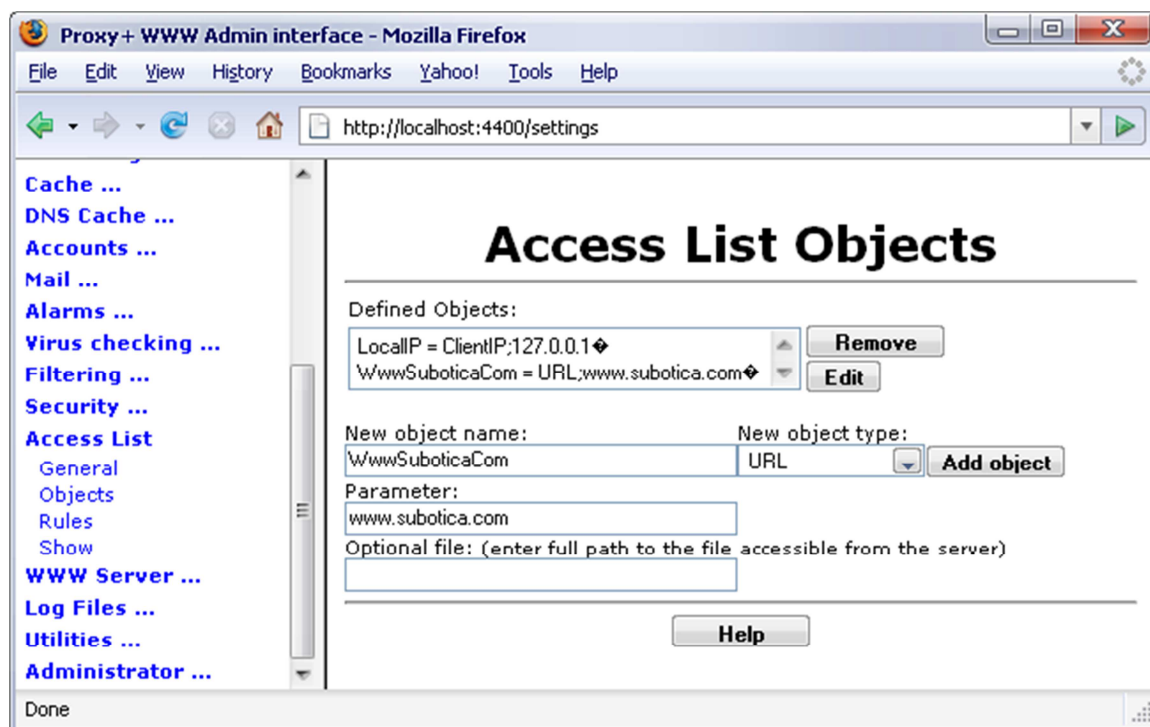
Slika 16. www server podešavanje

Podešavanja za listu pristupa treba omogućiti. Objekti liste pristupa za klijenta (slika 13.).



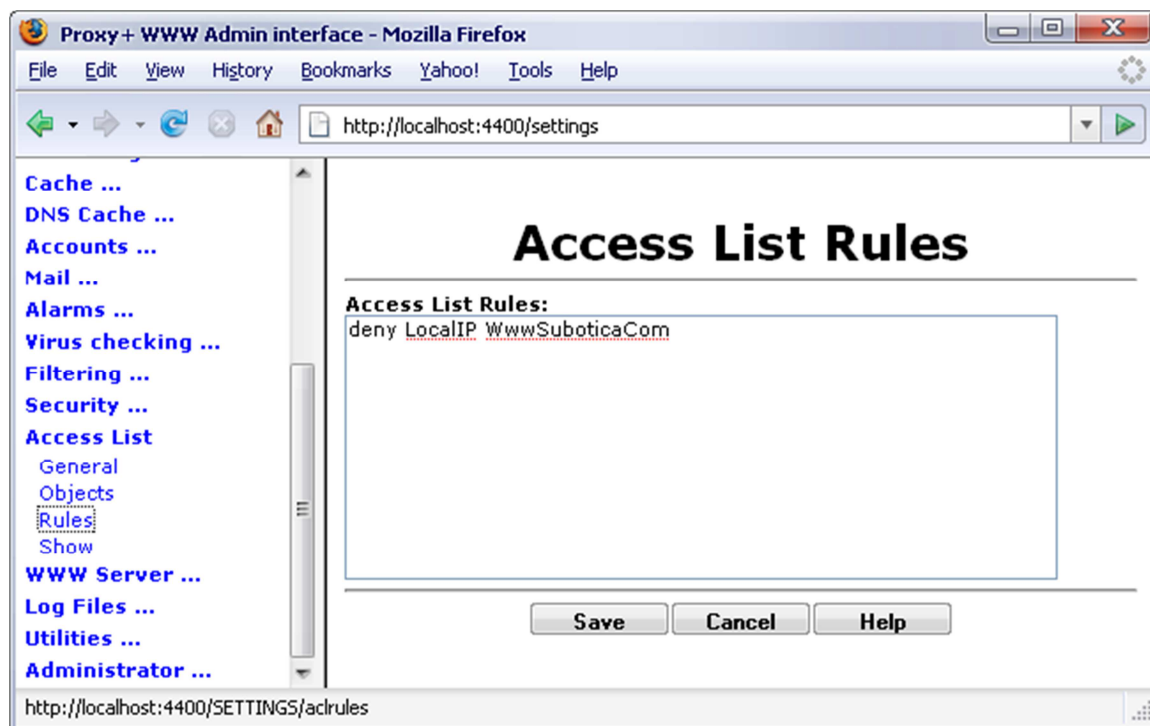
Slika 17. Podešavanje lista pristupa

Objekti liste pristupa za web stranicu www.subotica.com (slika 14.).



Slika 18. Objekti liste pristupa

Sa pravilima liste pristupa zabranjujemo pristup web stranici www.subotica.com (slika 15.).



Slika 19. Zabranjivanje pristup web stranici

Pristup je zabranjen za ovu stranicu.

Opis: pristup nije dozvoljen zbog podešavanja liste pristupa u Proxy+ (slika 16.).²⁰



Slika 20. Izgled zabranjenoj stranici

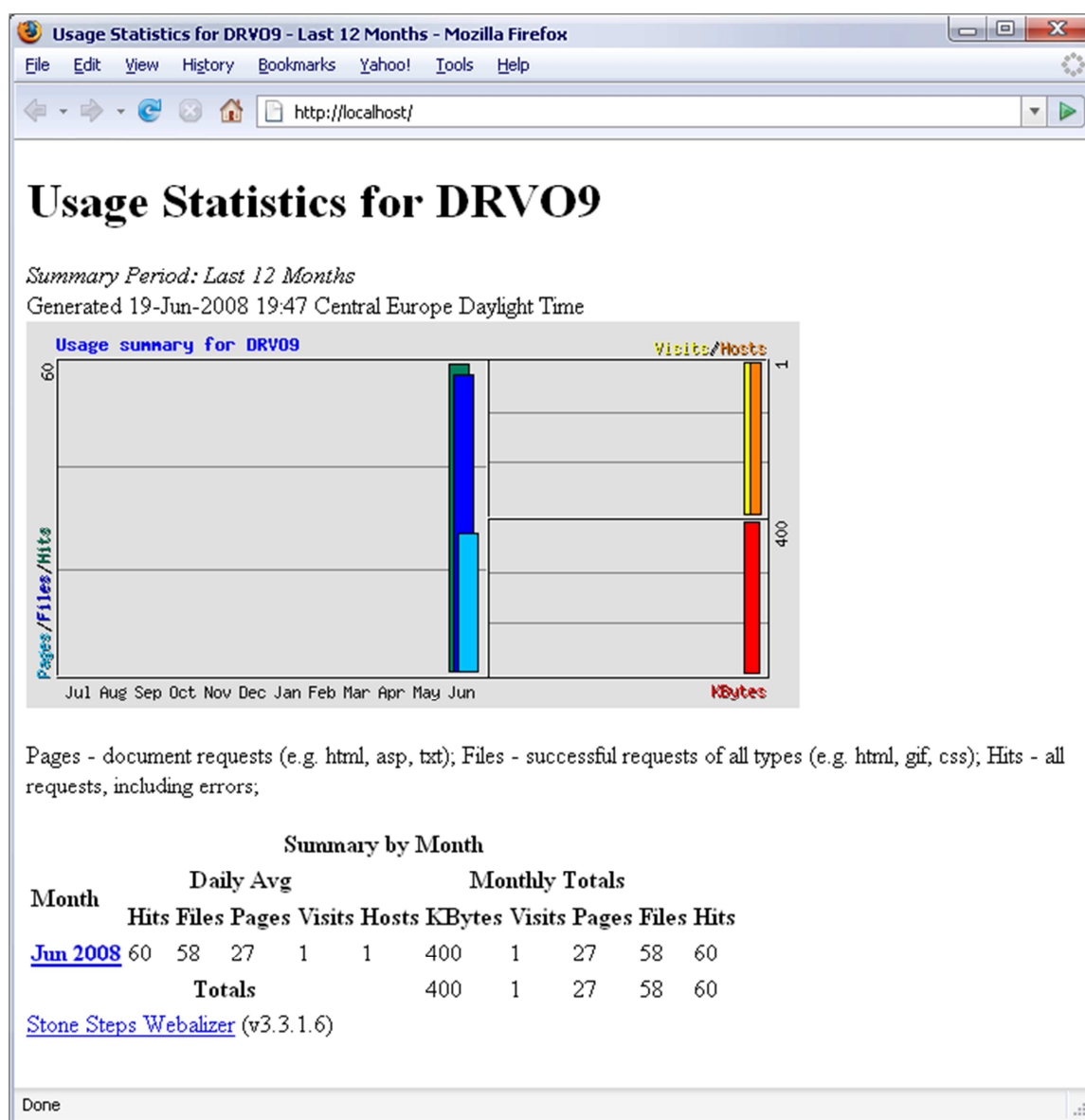
²⁰ Proxy Plus - <http://www.proxyplus.net>

5.2. Webalizer – Log Analizator

Webalizer je aplikacija koja generiše analizu web stranica, na osnovu logova pristupa i korišćenja. On zapisuje log fajlove koji prođu kroz proxy plus. Služi da bi napravio statistiku korišćenja određenog računara.

Pri instaliranju ovog programa treba da se pokrene fajl vcredist_x86.exe. Zatim u webalizer_win_3_3_1_6 direktorijumu, treba da se napravi (prepiše-rewrite sample.conf fajl) webalizer.conf fajl i da se edituje: Log File, Log Type, Output Dir. (LogFile c:\program files\proxyplus\logs\accesslog.txt; LogType squid; OutputDir c:\program files\proxyplus\report)

Pokretanjem localhost-a u pretraživaču, ispisuje se izveštaj u html formatu (slika 17.).²¹



Slika 21. Webalizer – Log Analizator

²¹ Webalizer - <http://www.snapfiles.com/get/webalizerwin32.html>

5.3. Crna lista (Blacklist)

Crna lista (blacklist) je osnovni mehanizam kontrole pristupa koji dozvoljava svaki pristup, osim za članove crne liste (npr. lista zabranjenih pristupa). Suprotno od ovog je bela lista (whitelist), koji znači dozvolu nikog drugog sem onih koji su članovi bele liste. Neka vrsta srednjeg tla, siva lista (greylist) sadrži unose koji su privremeno blokirani ili privremeno dozvoljeni. Stavke sive liste mogu biti pregledane ili dalje testirane za uključivanje u crnu listu ili belu listu.

Organizacije mogu da zadrže crnu listu software-a ili web stranica u svom računarskom sistemu. Naslovi na listi bi bili zabranjeni i sve ostalo bi bilo dozvoljeno. Na primer, škola može da stavi KaZaA i ICQ na crnu listu; ostali internet servisi bi i dalje bili dozvoljeni.

Primeri

- Software za kontrolu sadržaja kao što je DansGuardian i SquidGuard mogu da rade sa crnom listom da bi blokirali neke URL-ove web stranica koje smatraju neprikladnim za posao ili obrazovno okruženje.
- Filteri email spam-a mogu da zadrže crnu listu adresa, bilo koji mail od kojeg bi bili sprečeni da dođu do nameravanog odredišta. Popularna tehnika za izvršavanje crne liste je DNS blacklisting (DNSBL).
- Mnoge šeme kopiranja sprečavanja sadrže software blacklisting.
- Članovi web stranica za online aukcije mogu dodati druge članove ličnoj crnoj listi. Ovo znači da ne mogu da ponude cenu ili pitaju pitanja o vašim aukcijama, niti mogu koristiti “buy it now” (kupite sada) funkciju na vašim stavkama.
- Još jedan oblik liste je žuta lista. To je lista IP adresa email servera koja većinom šalje dobre mail-ove ali takođe šalje i neke spam-ove. Primeri su Yahoo, Hotmail i Gmail. Server žute liste je server koji ne bi trebao biti stavljen nikad na crnu listu. Žuta lista se prvo proverava i ako se nalazi tamo, testovi crne liste se ignorišu.²²

5.4. Squid

Squid je keširani proxy za web podršku HTTP, HTTPS, FTP. On ograničava širinu opsega i poboljšava vreme odgovora keširanjem i ponovnim korišćenjem često zahtevanih web stranica. Squid ima široke kontrole pristupa i pravi veliko ubrzanje servera. Pokreće se na Unix i Windows platformi.

²² Blacklist - <http://www.sharewareconnection.com/602lan-suite-content-filter.htm>

Squid je korišćen od strane stotine internet provajdera širom sveta da bi snabdeo svoje korisnike sa najboljim mogućim pristupom internetu. On optimizuje tok podataka između klijenta i servera da bi poboljšao izvršavanje i keš sadržaja koji je često korišćen da bi sačuvao širinu opsega. Squid takođe može da rutira zahteve sadržaja serverima na različite načine da bi sagradio hijerarhiju keš servera koja optimizuje prolaz kroz mrežu.

Hiljade web stranica koristi Squid da bi drastično povećali dostavu svojih sadržaja. On može da ograniči teret servera i poboljša brzine dostava klijentima. Squid takođe može da se koristi za dostavu sadržaja širom sveta – kopirajući samo sadržaj koji se koristi, pre nego neuspešno kopirajući sve. Najzad, napredna konfiguracija rutiranja sadržaja dozvoljava da se grade grupe (klasteri) za rutiranje i učitavaju zahtevi balansiranja putem mnogih web servera.

Stvaraoci HTTP protokola su rano primetili da će biti naglo povećanje sadržaja i zbog toga su dodali ovaj moćni keš mehanizam.

Ovi mehanizmi omogućavaju stvaraocima sadržaja i distributerima da označe serverima i korisnicima kako bi sadržaj trebalo potvrditi, ponovo potvrditi, i keširati. Ovo je imalo efekat drastičnog ograničenja širine opsega zahtevane da se servira sadržaj i poboljšanja vremena odgovora korisnika.

Squid je jedan od projekata koji su iznikli iz prvobitne distribucije i keširanja sredinom devedesetih. Sadrži posebne osobine kao što su moćna kontrola pristupa, autorizacija, logovanje, distribucija/podela sadržaja, upravljanje saobraćajem, oblikovanje, itd.²³

5.5. SquidGuard

SquidGuard je URL preusmerivač koji koristi crne liste sa Squid proxy software-om. Sadrži konfiguracione logove, bar (crta) napretka prilikom sastavljanja crne liste, blokira URL-ove sa host imenima. Preusmerivač je program koji se povezuje sa Squid-om i dozvoljava da se prevedu URL-ovi pre nego što se pošalju Squid procesu za: ograničene pristupe, za raspremanje banera da bi se ubrzalo korišćenje mreže, za preusmerenje URL-ova na lokalnoj kopiji (npr. Netscape Navigator downloading).

Crna lista je najbitniji deo svakog URL filtera.

Primeri crnih lista: MESD blacklists, Shalla's Blacklists, Université Toulouse blacklist collection, URLBlacklist.com.²⁴

5.6. Network Guardian 2008

Network Guardian je inteligentna opcija koja dinamički analizira, razume i kategoriše svaku web stranicu koja postoji.

URL filtriranje nije dovoljno. Potrebna je inteligencija da se pročita i razume svaka zahtevana web stranica sa kontrolom koja se bazira na ono što stranica zaista sadrži a ne samo obično blokiranje unapred kategorizovanog URL filtera. Dinamička analiza sadržaja je ključna tehnologija koja Guardian čini efektivnijim od drugih proizvoda za filtriranje. Filter dinamičke analize sadržaja skenira svaku web stranicu, svaku reč i fraze iz brojnih kategorija nepoželjnih sadržaja, uključujući nedozvoljen

²³ Squid - <http://www.squid-cache.org>

²⁴ SquidGuard – <http://www.squidguard.org/>

sadržaj, nasilje, droge, rasne mržnje i kockanje. Bilo koja stranica koja sadrži neodgovarajući sadržaj, biće blokirana, čak i ako dolazi iz uglednog izvora kao što je važna stranica vesti ili pretraživač.²⁵

5.7. Parental Lock Guard 1.1

„Sa aktiviranjem Parental Lock Guard-a možete u potpunosti zaštititi svoj računar – zabraniti pristup određenim folderima, programima i Internet adresama pa čak i automatski ugasiti računar ukoliko neko neovlašćen pokuša da radi na njemu. Drugim rečima, puna kontrola nad računarom je samo u vašim rukama i niko drugi neće moći da ga koristi u većoj meri nego što ste mu dozvolili. O tome da je u pitanju dobra ideja i odlična realizacija govori i činjenica da je Parental Lock Guard dobio brojna priznanja na mnogim download sajtovima. Aktiviranje i isključivanje zaštite vrši se samo jednim dugmetom. Administrator (vlasnik programa) može da proveri koliko je dugo i šta je koji korisnik radio za računarom, koliko puta je Windows restartovan itd.

Ukoliko pokušate da prevarite program ručnom izmenom vremena u Windowsu (vraćanjem vremena za nekoliko sati ili promenom datuma), Parental Lock Guard će odmah otkriti vašu prevaru i kazniće vas trenutnim gašenjem računara.

Deo koji se odnosi na nadgledanje rada na Internetu nosi (logičan) naziv Internet špijun. On sakuplja informacije o Internet adresama koje korisnik posećuje i proverava da li se adresa upisana u browser nalazi na tzv. „crnoj listi”. Ova lista, pored kompletnih adresa, može da sadrži i samo neke njihove delove (ključne reči), što je, čini nam se, mnogo efikasniji način zaštite. Interesantan je način manifestovanja ove zaštite. Ukoliko korisnik ukuca adresu ili reč koja se nalazi na crnoj listi, Parental Lock Guard će istog trenutka automatski ugasiti browser. Na raspolaganju vam je i sigurno brisanje programa koje zahteva njihovo prethodno uklanjanje korišćenjem standardne opcije Add/Remove Programs iz Control Panela. Zaključavanje foldera onemogućuje pristup podacima koji se u njemu nalaze. Zbog preventive i eventualne moguće nestabilnosti sistema, folderi Root i Windows se ne mogu zaključati na ovaj način.

Zaključavanje programa je veoma korisna opcija. Njom, recimo, možete onemogućiti pristup igrama instaliranim na računaru dok se nalazite na poslu kako se vaše dete ne bi igralo umesto da uči. Slično kao kod pokušaja pristupa zaštićenim Internet stranicama, zaštićeni program će se odmah nakon pokušaja startovanja ugasiti.”²⁶

²⁵ Network Guardian 2008 - <http://www.smoothwall.net/products/networkguardian2008/>

²⁶ Branislav Bubanja, Parental Lock Guard, Sveobuhvatna zaštita računara (<http://www.sk.rs/2004/07/skpd01.html>)

6. ISTRAŽIVAČKI RAD

ANKETA – KÉRDŐÍV

Poštovani Roditelji!

Ovaj upitnik je sastavni deo istraživanja koje se bavi sagledavanjem Vaših iskustava, mišljenja i predloga šta je potrebno i moguće učiniti u razvijanju efikasnije strategije u zaštiti dece od neželjenih internet sadržaja.

Molimo Vas da odvojite nekoliko minuta za ovu anketu i svojim odgovorima pomognete u proceni koliko su učenici zaštićeni na internetu.

Učešće u ovom istraživanju je dobrovoljno i anonimno, što znači ne treba da napišete svoje ime i prezime. Ako imate bilo kakva pitanja, molimo Vas obratite se anketaru. Takođe Vas molimo da pažljivo pročitate pitanja i da na svako iskreno odgovorite.

ZAHVALJUJEMO SE NA RAZUMEVANJU I SARADNJI!

Tisztelt Szülők!

A kérdőív része annak a kutatásnak, melynek célja, hogy feltárjuk hogyan tudjuk leghatékonyabban megvédeni az interneten előforduló esetleges káros tartalmaktól a gyerekeket.

Szeretnénk megkérni, hogy szánjon a kérdőív kitöltésére néhány percet, így segítve a gyerekek biztonságos internet használatát. Kérjük figyelmesen olvassa el a kérdéseket mielőtt megválaszolná őket. Mivel a kérdőív anonim, nem kell feltüntetnie a nevét.

KÖSZÖNJÜK MEGÉRTÉSÜKET ÉS EGYÜTTMŰKÖDÉSÜKET!

Vaša godina starosti _____

1. Az Ön életkora _____

Vaša školska sprema

2. Az Ön iskola végzettsége
(**Zaokružite samo jedan odgovor,
Egy választ karikázzon be**)

1. Nezavršena osnovna škola
Befejezetlen általános iskola
2. Osnovna škola
Általános iskola
3. Trogodišnja srednja stručna sprema
Hároméves középiskola
4. Četvorogodišnja srednja škola
Négyéves középiskola
5. Viša škola
Főiskola
6. Fakultet
Egyetem

3. Koliko dece imate?
Hány gyereke van?

1. Jedan
Egy
2. Dve
Kettő
3. Tri
Három
4. Više. Koliko? _____
Több. Hány? _____

4.	Da li imate računar? Van-e számítógépük? (Zaokružite samo jedan odgovor, Egy választ karikázzon be)	1. Da Igen, van 2. Ne Nem, nincs
5.	Vaše znanje korišćenja računara Mennyire tudja használni a számítógépet? (Zaokružite samo jedan odgovor, Egy választ karikázzon be)	1. Ne znam da koristim Nem tudom használni 2. Najosnovnije stvari znam Az alapokat tudom 3. Korisnički nivo Felhasználói szinten tudom 4. Dobro Jól 5. Professionalno Professzionálisan
6.	Koliko Vaše dete koristi računar? Mennyi időt tölt gyermeke számítógép előtt? (Zaokružite samo jedan odgovor, Egy választ karikázzon be)	1. Nedeljno do 2 sati Heti 2 órát 2. Nedeljno 2 dana 2 napot hetente 3. Dnevno do 2 sata Napi 2 órát 4. Dnevno do 4 sati Napi 4 órát 5. Dnevno više od 5 sati Naponta több mint 5 órát
7.	Da li Vaše dete ima svoj računar? Gyermekeének van-e saját számítógépe? (Zaokružite samo jedan odgovor, Egy választ karikázzon be)	1. Da Igen 2. Ne Nem
8.	Ima li Vaše dete smart telefon? Van-e gyerekének okostelefonja? (Zaokružite samo jedan odgovor, Egy választ karikázzon be)	1. Da Igen 2. Ne Nem
9.	Imate li internet pristup u kući? Van-e internet hozzáférése otthon? (Zaokružite samo jedan odgovor, Egy választ karikázzon be)	1. Imam Van 2. Nemam Nincs
10.	Kakvu zaštitu ima Vaš računar? Milyen védelme van a számítógépének? (Možete zaokružiti više odgovora, Több választ is bekarikázhat)	1. Antivirus 2. Firewall 3. Anti spyware / anti-malware 4. Pored ovih još: _____ Ezek mellett még: _____
11.	Za šta koristi Vaše dete računar? Mire használja gyereke a számítógépet? (Možete zaokružiti više odgovora, Több választ is bekarikázhat)	1. Za pretraživanje Keresésre 2. Za druženje Barátkozásra 3. Za društvene mreže (facebook, twitter, itd.) Közösségi hálókra (facebook, twitter, stb.) 4. Za gledanje filmova / muzike (youtube) Film nézésre / zenehallgatásra (youtube)

Zaštita dece od neželjenih internet sadržaja

12.	Da li neko iz porodice prati aktivnosti Vašeg deteta na internetu? Követi-e valaki a családból gyereke aktivitásait az interneten? (Zaokružite samo jedan odgovor, Egy választ karikázzon be)	1. Da Igen 2. Ne Nem
13.	Ako je na 12. pitanje odgovor DA, onda kako? Ha a 12. kérdésre a válasz IGEN, akkor hogyan? (Možete zaokružiti više odgovora, Több választ is bekarikázhat)	1. Puno pričamo o opasnostima na internetu Sokat beszélgetünk az internet veszélyeiről Kontrolom računara (e-mailova, pregledavanjem facebook aktivnosti, chat poruka, itd.) 2. A számítógép átnézésével (e-mailek, facebook beszélgetések, chat üzenetek, stb.) 3. Ograničavanjem korišćenja računara A számítógép használatának korlátozásával 4. Pomoću nekih programa Különbféle programok segítségével 5. Verujem svom detetu, i ne treba da ga/je kontrolišem Hiszek a gyerekemnek és nem kell, hogy ellenőrizsem
14.	Da li ste Vi upoznati sa opasnostima interneta? Ismeri-e Ön az internet veszélyeit? (Zaokružite samo jedan odgovor, Egy választ karikázzon be)	1. Da Igen 2. Ne Nem
15.	Koliko se brinete za bezbednost Vašeg deteta kada koristi internet? Mennyire aggódik gyermeke biztonságáért, amikor az internetet használja? (Zaokružite samo jedan odgovor, Egy választ karikázzon be)	1. Izuzetno se brinem Rendkívül aggódom 2. Jako se brinem Nagyon aggódom 3. Malo se brinem Kissé aggódom 4. Ne brinem se baš puno Nem nagyon aggódom 5. Uopšte se ne brinem Egyáltalán nem aggódom
16.	Zbog čega se najviše brinete ? Mi az, amitől leginkább félti a gyermekét? (Možete zaokružiti najviše tri odgovora, Legtöbb három választ karikázhat be)	1. Da će izdati svoje lične podatke Hogy kiadja személyes adatait 2. Da će upoznati nemoralne (opscene) sadržaje Hogy szeméremsértő (obszcén) tartalmakat ismer meg 3. Da će naći agresivne sadržaje Hogy agresszív tartalmakat talál majd 4. Da će ga/je neko online terorizirati Hogy valaki online terrorizálja majd 5. Da će do njega/nje dospeti neki sadržaji koji sugerišu samopovređivanje (samoubistvo, anorexia, itd.) Hogy önkárosításra ösztönző tartalmat vagy tájékoztatásokat talál (öngyilkosság, anorexia, stb.) 6. Da će postati usamljen Hogy magányossá válik 7. Ne brinem se Nem féltém

Zaštita dece od neželjenih internet sadržaja

17.	Koristite li program za praćenje ili program za filtriranje sadržaja? Használ-e követő és tartalomszűrő programot? (Zaokružite samo jedan odgovor, Egy választ karikázzon be)	1. Da, program za filtriranje sadržaja i program za praćenje Igen, szűrő és követő (monitoring) szoftvert 2. Samo program za filtriranje Csak szűrő programot 3. Samo program za praćenje (monitoring) Csak felügyeleti (monitoring) programot 4. Ne Nem
18.	Ako je na 17. pitanje odgovor NE, zašto? Ha a 17. kérdésre a válasz NEM, miért? (Zaokružite samo jedan odgovor, Egy választ karikázzon be)	1. Ne, jer ne znam gde mogu naći tako nešto Nem, mert nem tudom hol lehet hozzájutni 2. Ne, jer mislim da nije korisno Nem, mert nem hiszem hogy hasznos 3. Ne, jer verujem svom detetu Nem, mert hiszek a gyerekemnek 4. Drugo: _____ Más: _____
19.	Znate li šta treba da radite u slučaju opasnosti? Tudja-e mit kell tennie veszély esetén? (Zaokružite samo jedan odgovor, Egy választ karikázzon be)	1. Da Igen 2. Ne Nem
20.	Da li je Vaše dete tražio/tražila pomoć? Kért-e már a gyereke segítséget? (Možete zaokružiti najviše dva odgovora, Legtöbb két választ karikázhat be)	1. Da, jer mu/joj je neko provalio profil na društvenoj mreži Igen, mert a közösségi hálón valaki feltörte a profilját 2. Da, jer ga/ju je neko uznemiravao preko interneta Igen, mert valaki zaklatta az interneten keresztül 3. Da, jer ga/ju je neko pozvao na susret Igen, mert valaki találkozóra hívta 4. Nije još tražio/la pomoć Még nem kért segítséget
21.	Po Vašem mišljenju kako bi roditelji mogli bolje da zaštite svoju decu? Ön szerint hogyan védhetnék meg jobban a szülők a gyerekeiket? (Možete zaokružiti najviše tri odgovora, Legtöbb három választ karikázhat be)	1. Raznovrsnim aktivnostima roditeljima u školama Különbféle iskolai foglalkozásokkal szülőknek 2. Redovnim medijskim kampanjama Több figyelmeztető kampánnyal a médiában 3. Edukacijom roditelja A szülők felvilágosításával 4. Strožijim zakonima koji regulišu online sadržaje Szigorúbb törvényi szabályozással az online tartalmakkal szemben 5. Aktivnostima gde su roditelji i deca zajedno Közös (szülő-gyermek) felvilágosító programokkal 6. Lakše dostupnim monitoring softverima Monitoring szoftverek könnyebb, egyszerűbb elérhetőségével

Prema Vašem mišljenju, ima li potrebe za firmom ili civilnom organizacijom koja bi instalirala monitoring softvere i davala pomoć roditeljima?

22. Ön szerint, szükség van-e olyan cégre, civil szervezetre amely monitoring szoftvereket telepítene és segítséget nyújtana a szülőknek?

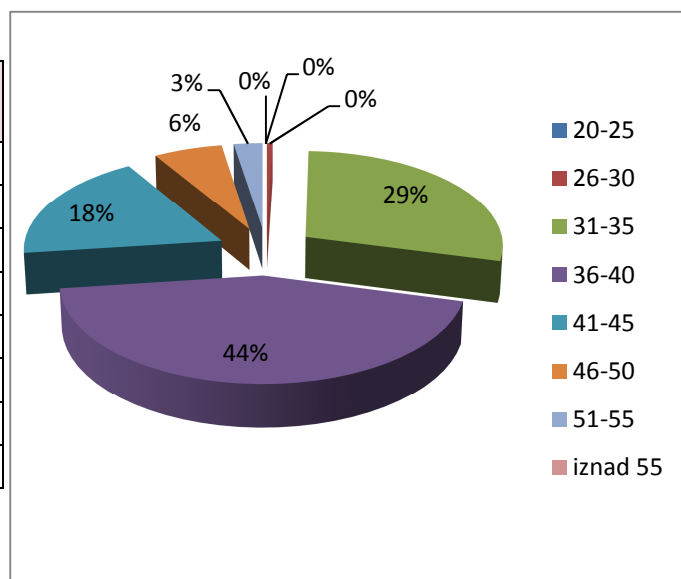
(Zaokružite samo jedan odgovor,
Egy választ karikázzon be)

1. Da, ima potrebe
Igen, szükség van rá
2. Nema potrebe
Nincs rá szükség

**HVALA NA SARADNJI!
KÖSZÖNJÜK A KÖZREMŰKÖDÉST!**

6.1. Rezultati istraživačkog rada

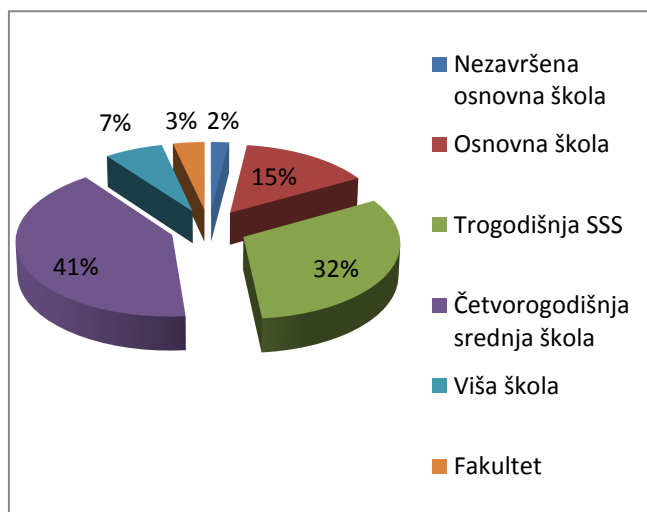
1. Vaša godina starosti	196	100%
1. 20-25	0	0%
2. 26-30	1	1%
3. 31-35	56	29%
4. 36-40	86	44%
5. 41-45	36	18%
6. 46-50	12	6%
7. 51-55	5	3%
8. iznad 55	0	0%



Analiza prikazanih rezultata:

Najveći prosek godina starosti roditelja je između 36 i 40 godina sa 44% , a posle toga sledi između 31 i 35 godina sa 29%.

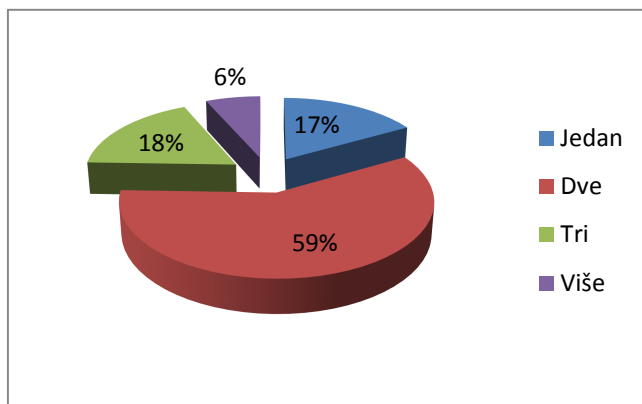
2. Vaša školska sprema		196	100%
1.	Nezavršena osnovna škola	4	2%
2.	Osnovna škola	29	15%
3.	Trogodišnja SSS	62	32%
4.	Četvorogodišnja srednja škola	81	41%
5.	Viša škola	13	7%
6.	Fakultet	7	4%



Analiza prikazanih rezultata:

Najveći prosek školske spreme roditelji imaju završenu četvorogodišnju srednju školu sa 41%, a toga sledi trogodišnja srednja stručna sprema za 32%, dok 15% ima završenu osnovnu školu i samo 4% ima završen fakultet.

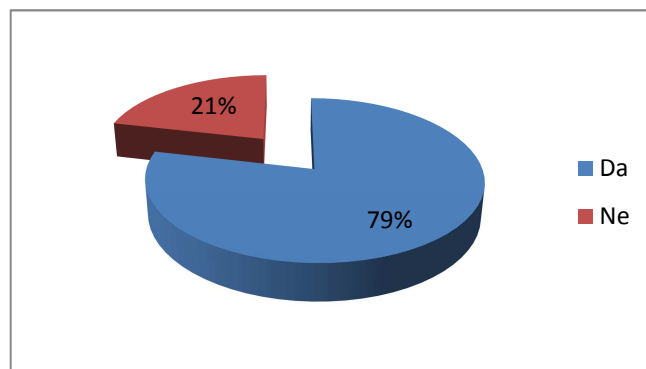
3. Koliko dece imate?		196	100%
1.	Jedan	33	17%
2.	Dve	115	59%
3.	Tri	35	18%
4.	Više	13	7%



Analiza prikazanih rezultata:

Od ukupnog broja ispitanika 59% ima dvoje dece, dok 18% tri dece, i samo 17% ima samo jednu.

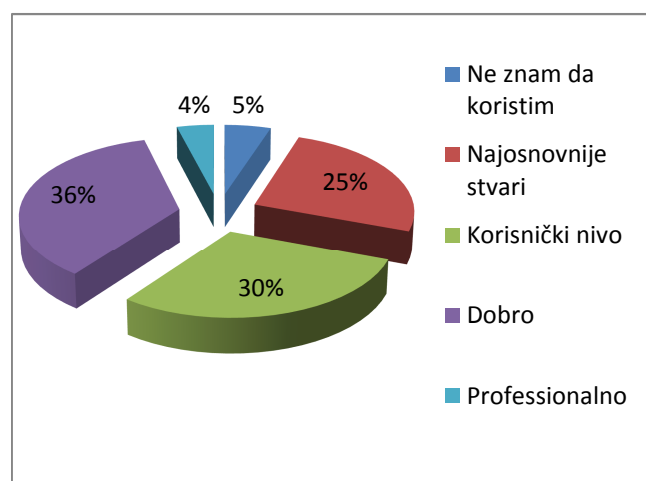
4. Da li imate računar?	196	100%
1. Da	154	79%
2. Ne	42	21%



Analiza prikazanih rezultata:

Od ukupnog broja ispitanika 79% ima računar, koji je dobar broj naspram stepena obrazovanja.

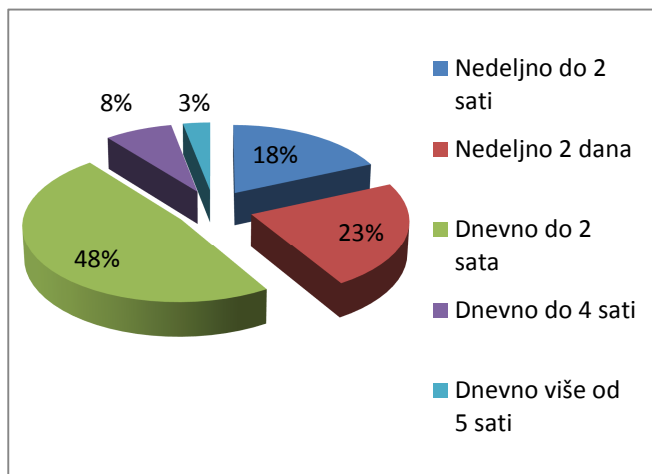
5. Vaše znanje korišćenja računara	196	100%
1. Ne znam da koristim	10	5%
2. Najosnovnije stvari	50	26%
3. Korisnički nivo	58	30%
4. Dobro	70	36%
5. Profesionalno	8	4%



Analiza prikazanih rezultata:

Samo 36% od ukupno broja ispitanika zna da koristi računar na dobrom nivou, a samo 4% na profesionalni nivo. Ostali ne znaju da koriste, samo najosnovnije stvari znaju ili samo na korisnički nivo zna da koristi računar.

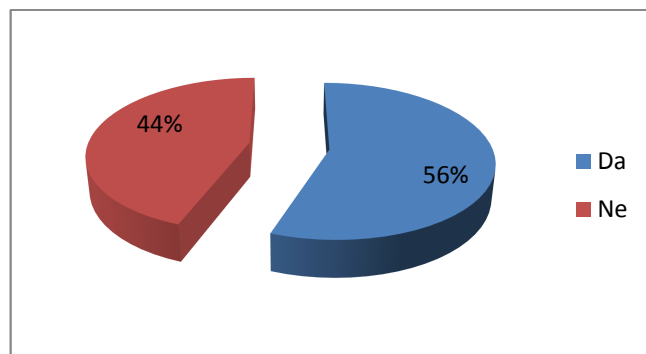
6. Koliko Vaše dete koristi računar?	196	100%
1. Nedeljno do 2 sati	36	18%
2. Nedeljno 2 dana	45	23%
3. Dnevno do 2 sata	94	48%
4. Dnevno do 4 sati	15	8%
5. Dnevno više od 5 sati	6	3%



Analiza prikazanih rezultata:

Dete od ukupnog broja ispitanika skoro pola, 48% sprovede dnevno do 2 sata ispred svog računara, dok samo 3% koristi više od 5 sati dnevno.

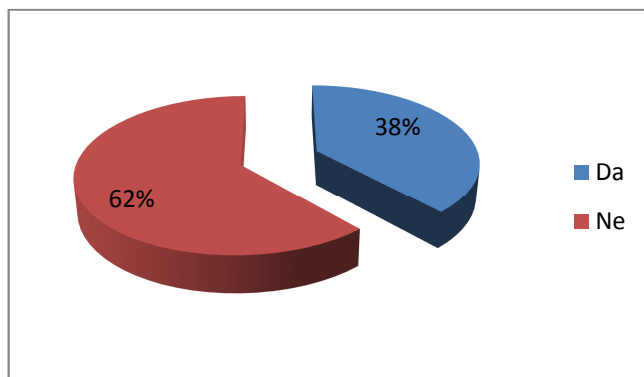
7. Da li Vaše dete ima svoj računar?	196	100%
1. Da	109	56%
2. Ne	87	44%



Analiza prikazanih rezultata:

Od ukupnog broja ispitanika 56% kaže da deca imaju svoj računar, a 44% koriste računar od roditelja.

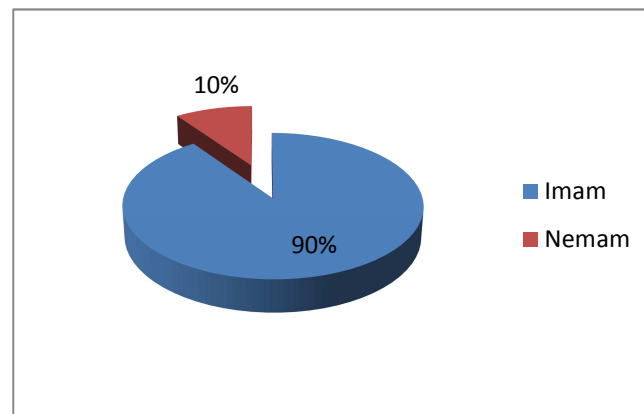
8. Ima li Vaše dete smart telefon?	196	100%
1. Da	75	38%
2. Ne	121	62%



Analiza prikazanih rezultata:

Samo 33% dete od ukupnog broja ispitanika ima smart (pametni) telefon, koji je značajno manji broj od očekivanog.

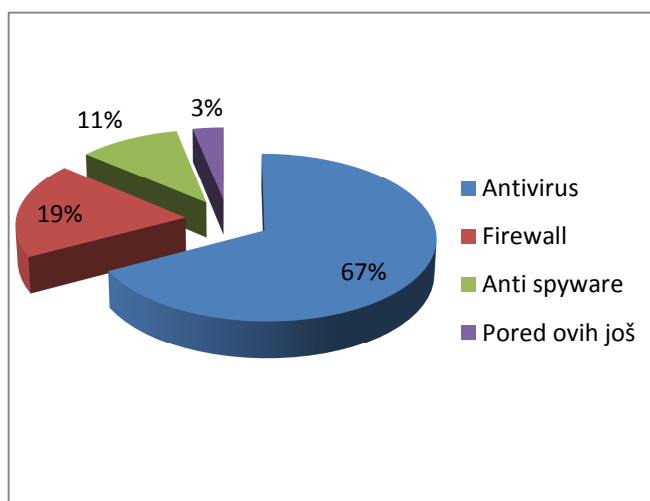
9. Imate li internet pristup u kući?	196	100%
1. Imam	177	90%
2. Nemam	19	10%



Analiza prikazanih rezultata:

Od ukupnog broja ispitanika 90% ima internet pristup kući, koji je značajno veći broj od očekivanog, i samo 10% nema internet pristup.

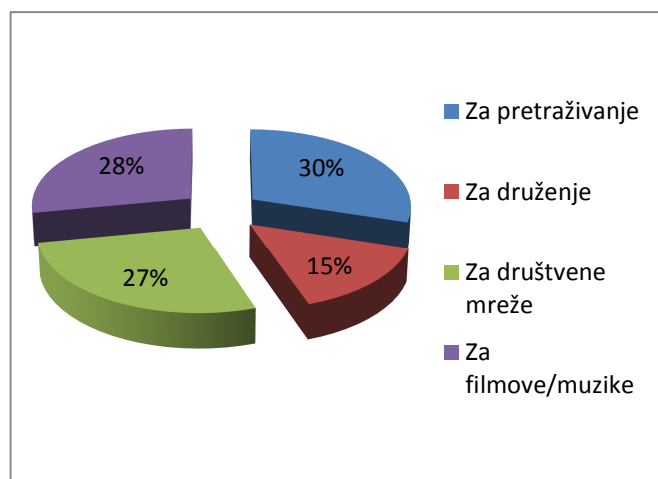
10. Kakvu zaštitu ima Vaš računar?	217	100%
1. Antivirus	146	67%
2. Firewall	41	19%
3. Anti spyware	23	11%
4. Pored ovih još nešto	7	3%



Analiza prikazanih rezultata:

Pošto kod ovog pitanja ispitanici su mogli više odgovora da zaokruže, od ukupnog broja ispitanika samo 67% ima najosnovniju zaštitu računara a to je Antivirus, a samo 19% ima Firewall zaštitu, koji je veoma ispod očekivanog broja.

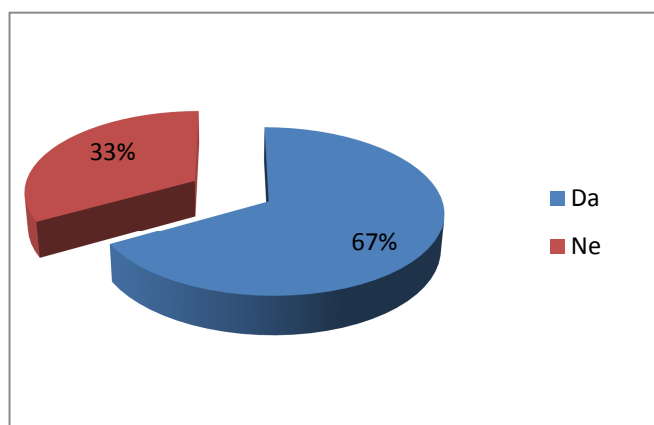
11. Za šta koristi Vaše dete računar?	275	100%
1. Za pretraživanje	82	30%
2. Za druženje	41	15%
3. Za društvene mreže	75	27%
4. Za filmove/muzike	77	28%



Analiza prikazanih rezultata:

I kod ove pitanje ispitanici su mogli više odgovora za zaokruže, i vidimo da 30% od ukupnog ispitanika koristi za pretraživanje, 28% koristi za filmove/muzike, 27% za društvene mreže. Od ovih brojeva lepo se vidi da nema velika rastojanja između odgovora, znači deca uglavnom ravnomerno koriste sve ponuđene opcije.

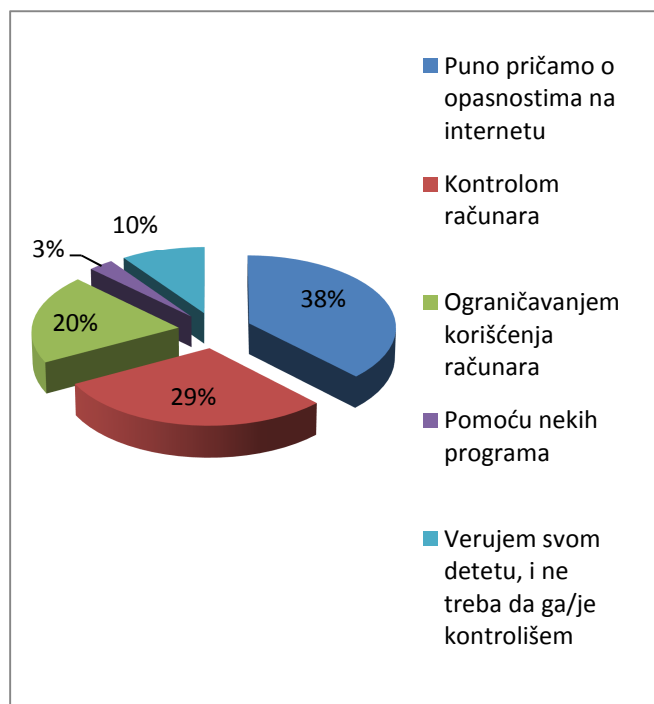
12. Da li neko iz porodice prati aktivnosti Vašeg deteta na internetu?	196	100%
1. Da	131	67%
2. Ne	65	33%



Analiza prikazanih rezultata:

Od ukupnog broja ispitanika samo 67% prati aktivnosti deteta na internetu, koji je značajno manji broj od očekivanog. Avaj broj lepo pokazuje da roditelji ni ne znaju za opasnostima kojima su izričena deca na virtuelnom svetu.

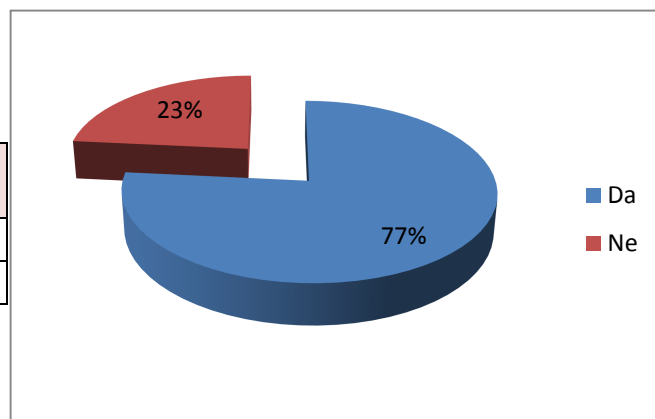
13. Ako je na 12. pitanje odgovor DA, onda kako?	204	100%
1. Puno pričamo o opasnostima na internetu	77	38%
2. Kontrolom računara	60	29%
3. Ograničavanjem korišćenja računara	41	20%
4. Pomoću nekih programa	6	3%
5. Verujem svom detetu, i ne treba da ga/je kontrolišem	20	10%



Analiza prikazanih rezultata:

Jedan od najinteresantnijih odgovora smo dobili na 13. pitanje, jer ispitanici, koji su na 12. pitanje odgovorili da prate aktivnosti svog deteta na internet, kod ove pitanje 10% ipak je odgovorio da veruju svom detetu, i ne treba da ga/je kontrolišu. Dok 38% kaže da pričaju o opasnostima na internet, 29% kontroliše računar, i samo 3% ispitanika koristi pomoć nekog programa.

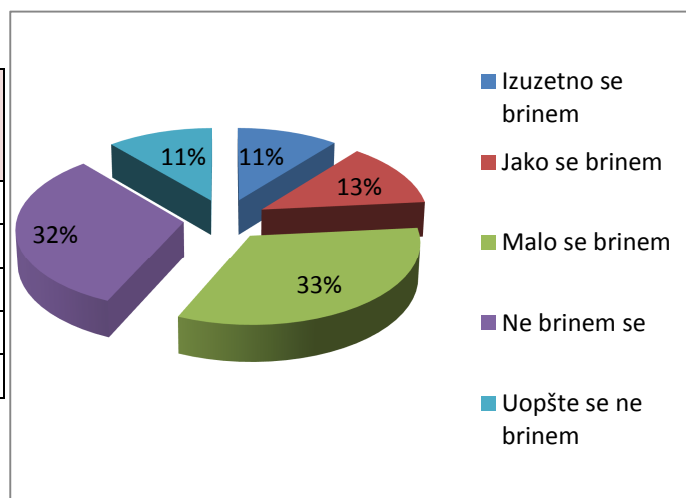
14. Da li ste Vi upoznati sa opasnostima interneta?	196	100%
1. Da	150	77%
2. Ne	46	23%



Analiza prikazanih rezultata:

Jedan od najvećih problema je da samo 36% od ukupno broja ispitanika zna da koristi računar na korisničkom nivou, a samo 4% na profesionalnom nivou, a 77% misli da su upoznati sa opasnostima na internetu.

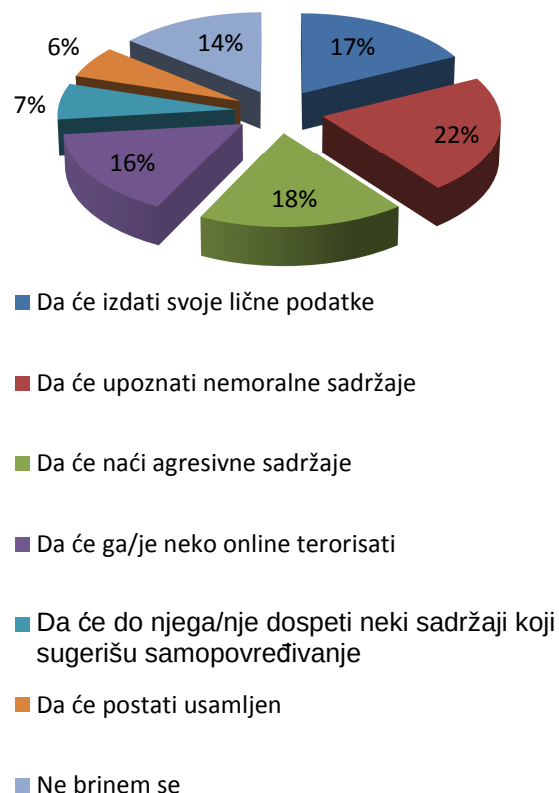
15. Koliko se brinete za bezbednost Vašeg deteta kada koristi internet?	196	100%
1. Izuzetno se brinem	21	11%
2. Jako se brinem	25	13%
3. Malo se brinem	65	33%
4. Ne brinem se	63	32%
5. Uopšte se ne brinem	22	11%



Analiza prikazanih rezultata:

Nema velika razlika (1%) između toga da se roditelji malo i da se ne brine o bezbednosti deteta na internetu, dok samo 11% se brine izuzetno za bezbednost njihovog deteta kada koriste internet.

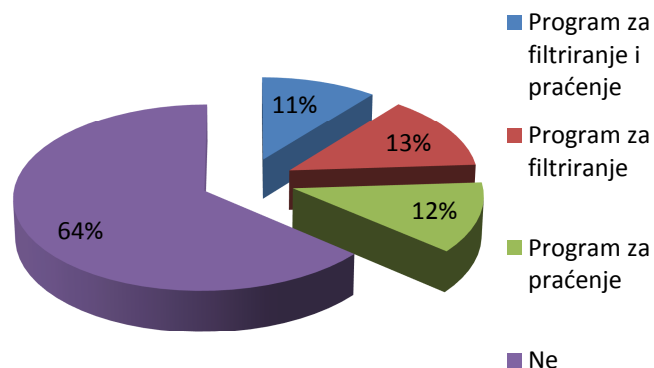
16. Zbog čega se najviše brinete?	283	100%
1. Da će izdati svoje lične podatke	50	18%
2. Da će upoznati nemoralne sadržaje	62	22%
3. Da će naći agresivne sadržaje	50	18%
4. Da će ga/je neko online terorisati	45	16%
5. Da će do njega/nje dospeti neki sadržaji koji sugerišu samopovređivanje	19	7%
6. Da će postati usamljen	17	6%
7. Ne brinem se	40	14%



Analiza prikazanih rezultata:

Roditelji procentualno isto toliko se boje (18%) da će dete izdati svoje lične podatke i da će naći agresivne sadržaje. Za 4% više se brine da će dete upoznati nemoralne sadržaje.

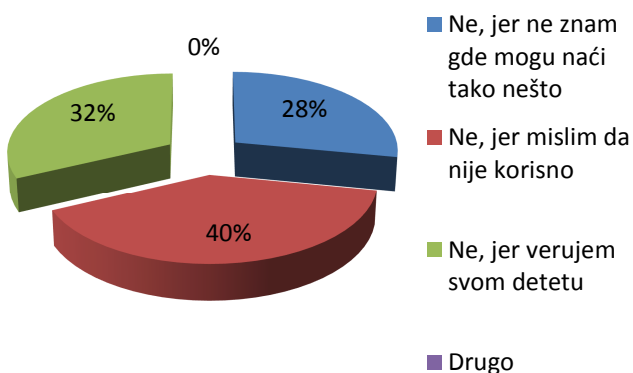
17. Koristite li program za praćenje ili program za filtriranje sadržaja?	196	100%
1. Program za filtriranje i praćenje	21	11%
2. Program za filtriranje	26	13%
3. Program za praćenje	24	12%
4. Ne	125	64%



Analiza prikazanih rezultata:

Ovaj podatak je očekivan da 64% od ukupni ispitanih roditelja ne koriste ni program za praćenje ni program za filtriranje sadržaja, je više od 60% roditelja do korisničkog nivo znaju da koriste računar.

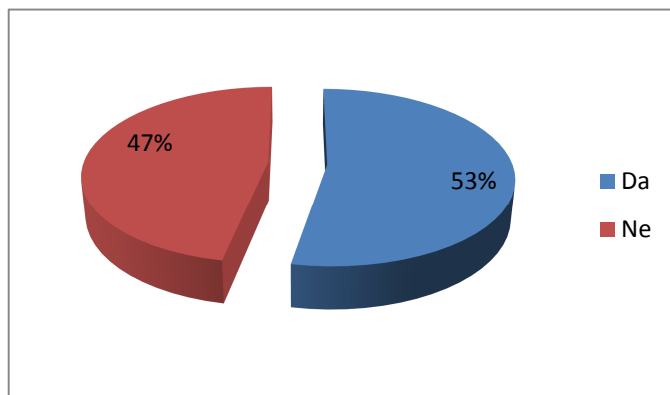
18. Ako je na 17. pitanje odgovor NE, zašto?	125	100%
1. Ne, jer ne znam gde mogu naći tako nešto	35	28%
2. Ne, jer mislim da nije korisno	50	40%
3. Ne, jer verujem svom detetu	40	32%
4. Drugo	0	0%



Analiza prikazanih rezultata:

Ono što je neočekivano da roditelji koji ne koriste program za praćenje ili program za filtriranje sadržaja, od njih 40% misle da ovi programi nisu korisni.

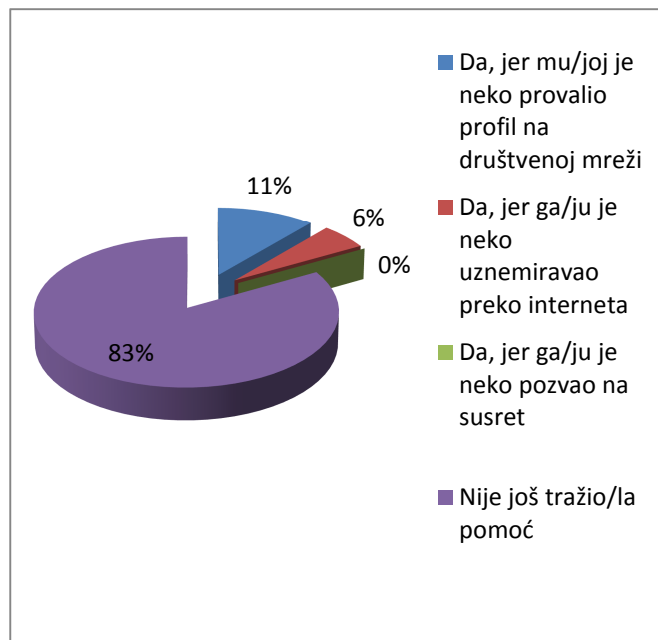
19. Zna li šta treba da radite u slučaju opasnosti?	196	100%
1. Da	104	53%
2. Ne	92	47%



Analiza prikazanih rezultata:

Još jedan neočekivani rezultat je da 47% od ukupno ispitanih ne zna šta da radi u slučaju opasnosti, ako je dete izdao svoje lične podatke, ako ga neko uznemirava, online teroriše dete, ili slično.

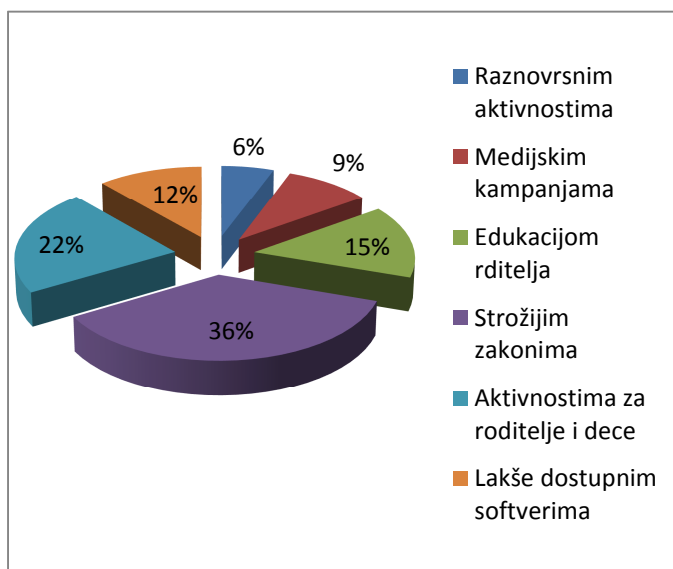
20. Da li je Vaše dete tražio/tražila pomoć?	196	100%
1. Da, jer mu/joj je neko provalio profil na društvenoj mreži	22	11%
2. Da, jer ga/ju je neko uznemiravao preko interneta	11	6%
3. Da, jer ga/ju je neko pozvao na susret	0	0%
4. Nije još tražio/la pomoć	163	83%



Analiza prikazanih rezultata:

Po drugim istraživanjima je ispitano da oko 70% maloletnih osoba je već preživeo neku online teror, neko ga uznemiravao ili pretio preko interneta. Iz našeg istraživanja možemo konsultovati da 83% od ispitanih ne zna šta se dešava sa svojom detetom.

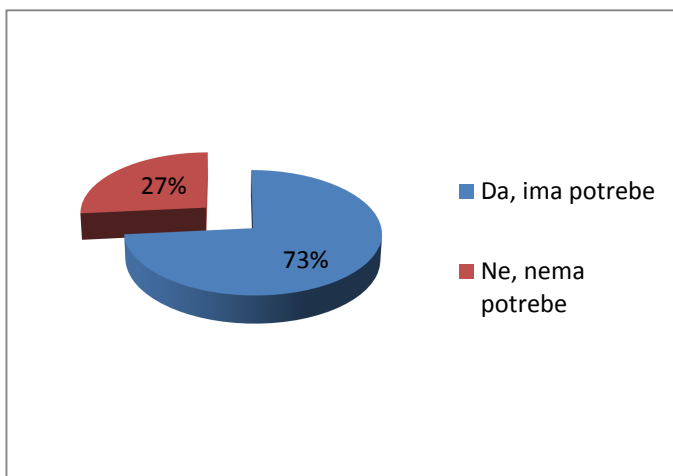
21. Po Vašem mišljenju kako bi roditelji mogli bolje da zaštite svoju decu?	245	100%
1. Raznovrsnim aktivnostima	14	6%
2. Medijskim kampanjama	23	9%
3. Edukacijom roditelja	37	15%
4. Strožijim zakonima	89	36%
5. Aktivnostima za roditelje i dece	54	22%
6. Lakše dostupnim softverima	28	11%



Analiza prikazanih rezultata:

Najveći procenat (36%) roditelja misle da sa strožijim zakonima roditelji bi mogli da bolje zaštite svoju decu u svetu interneta.

22. Prema Vašem mišljenju, ima li potrebe za firmom ili civilnom organizacijom koja bi instalirala monitoring softvere i davala pomoć roditeljima?	196	100%
1. Da, ima potrebe	144	73%
2. Ne, nema potrebe	52	27%



Analiza prikazanih rezultata:

Za pohvalu je taj podatak da 73% od roditelja misle da ima potreba za firmu ili civilnu organizaciju koja bii davala pomoć roditeljima u okviru ove problematike.

7. VREDNOVANJE REZULTATA

7.1. Zaključak

Izučavanje ove problematike je poseban izazov teorijsko-empirijskih istraživanja naučnika iz različitih nauka i naučnih disciplina. Međutim, pregled rezultata dosadašnjih istraživanja upućuju nas na potrebu daljeg razvijanja prikladnih naučnih istraživanja i pristupa u vezi sa problemskim područjem: Zaštita dece od neželjenih internet sadržaja.

Proučavanje ovog problema u osnovnoškolskom uzrastu se pokazalo kao izrazito značajan društveni problem u čijem rešavanju treba da učestvuje škola, izrazito nastavnici informatike, roditelji a i uža i šira društvena zajednica. Nedostatak sličnih istraživanja, uslovio je pomanjkanje naučne osnove za prethodno bliže raščlanjivanje i utvrđivanje veza između istraživačkih faktora, kao i za pouzdanost izvedenih zaključaka.

U teorijskom delu rada nastojali smo da ukažemo na teorijska polazišta, koja smo smatrali posebno značajnim za naše istraživanje. Zaštita dece od neželjenih internet sadržaja kao društvena pojava posmatra se iz različitog ugla gledišta, zbog toga su i tumačenja fenomena različita ali se u jednom slažu da ovoj problematici treba više pažnje posvetiti pošto se internet tehnologija ogromnom brzinom razvija i iz tog razloga mnogi zaostaju i stvara se sve veći jaz između roditelja i dece. Tu ima najveću i najznačajniju ulogu škola a posebno nastavnici informatike da ovu veliku razdaljinu između roditelja i učenika približe.

U poslednje vreme pitanje koje se najčešće postavlja jeste da li roditelji znaju šta im deca rade na internetu, s kim se dopisuju i koje veb-stranice posećuju? Decu najčešće upozoravamo da nikada ne razgovaraju sa strancima i da budu oprezna kada im prilaze nepoznate osobe. Ali, kako im objasniti da isto tako moraju da se ponašaju i u svetu interneta. Od trenutka kada je dete zakoračilo u virtuelni svet, moramo znati kako ga možemo zaštititi, jer uz brojne prednosti, globalna mreža krije i pregršt opasnosti za najmlađe.

Decu i maloletnike treba zaštititi od nasilnih i pornografskih sadržaja, neprimerenih poruka, od osoba koje mogu zloupotребiti dečje poverenje, pokušaju da ih nagovore da odaju privatne podatke, razmenjuju slike, čak i da sami, bez pratnje roditelja ili nastavnika, dođu i upoznaju onlajn „prijatelja“. Treba ih naučiti kako da sigurno i primereno koriste internet.

Ovaj istraživački rad pokazuje da u poslednje vreme sve više dece koristi internet, a da njihovi roditelji o tome nemaju pojma ili misle da su njihova deca bezbedna i dovoljno „zrela“ za korišćenje interneta. Ali je ipak osnovno pravilo - ne ostavljajte decu, pogotovo onu mlađu, samu za računarom. Ako koriste kompjuter u svojoj sobi, bez nadzora, i pri tom im je još omogućeno da to traje satima, decu će surfovanje pre ili kasnije odvesti do nekog neprimerenog sadržaja ili će dobiti uznemirujuću poruku koja će poremetiti zdrav psihofizički razvoj deteta.

Detetu svakako treba objasniti da su osobe s kojima se dopisuje možda lažno predstavile, i da obavezno prijavi svaki neprimereni način komunikacije ili poruku zbog koje se oseća nelagodno. Istraživački rad je, takođe, ukazalo da za decu koja

intenzivnije koriste internet, i čije su aktivnosti više istraživački usmerene, postoji veći rizik za izlaganje nepoželjnom sadržaju.

Dete se može zaštititi od najrazličitijih oblika onlajn zlostavljanja i korišćenjem odgovarajućih, specijalizovanih programa koji blokiraju pristup neželjenim stranicama. Na taj način roditelji sprečavaju odlazak na web-stranice u vreme kad ne može da nadgleda detetove aktivnosti na internetu, a ipak se možete pouzdati da za računarom nije izloženo uznemirujućim sadržajima i porukama. Programi za zaštitu najčešće nisu besplatni. Osnovna namena im je da filtriraju web-stranice, a pojedini softveri omogućavaju i da se vremenski ograniči pristup internetu. Takođe, postoji mogućnost da se ograniči i vrsta datoteka i igrice koje dete sme da koristi.

Roditelji, nastavnici, institucije, stručnjaci, moraju da preduzmu preventivne mere zaštite dece od nasilja i zlostavljanja putem interneta. Istraživački rad je pokazalo da 64% roditelja uopšte ne koristi program za praćenje ili program za filtriranje sadržaja. Ovaj podatak nas dodatno potvrđuje da se ovom problemu moramo hitno, bez odlaganja da se posvetimo i da preduzmemo hitne korake u edukaciji kompletne populacije za bezbedno korišćenje interneta.

Detetu treba objasniti da su osobe s kojima se dopisuje možda lažno predstavile, i da obavezno prijavi svaki neprimeren način komunikacije, poruku zbog koje se oseća nelagodno.

Po drugim istraživanjima je dokazano da oko 70% maloletnih osoba je već preživeo neku vrstu online terora, neko ga je uznemiravao ili pretio preko interneta. Iz našeg istraživačkog rada možemo konstatovati da 83% ispitanika ne zna šta se dešava sa njihovim detetom odnosno dete još nije zatražio pomoć roditelja. Ovaj podatak je isto alarmantan i upućuje nas na to da uz edukaciju roditelja moramo hitno da se osvrćemo i deci jer iz nekog razloga (može da bude tema jednog drugog istraživanja) deca ne traže pomoć odraslih. A još jedan neočekivani rezultat ankete je da 47% od ukupno ispitanih ne zna šta da radi u slučaju opasnosti, ako je dete izdao svoje lične podatke, ako ga neko uznemirava, online terorise, ili slično.

Osnovno pravilo - ne ostavljajte decu, pogotovo onu mlađu, samu za računarom.

Ovaj istraživački rad nije obuhvatilo učenike i nastavnike samo roditelje. Anketiranjem učenika i nastavnika bi smo dobili kompletnu sliku stanja u osnovnim školama Srbije ali to iziskuje mnogo veći uloženi trud i veća materijalna ulaganja što bi mogao da bude tema jednog velikog studioznog istraživanja.

Posledice nasilja preko interneta katkad mogu biti i ozbiljnije od posledica nasilja u stvarnim situacijama. Nasilje preko interneta često je mnogo šira od one na školskom igralištu, u razredu, ispred zgrade i dostupnija mnogo većoj publici. Uz to, kod nasilja na internetu postoji snaga pisane reči, jer žrtva može svaki put ponovno da pročita šta je nasilnik o njoj napisao, a u verbalnom obliku uvrede se lako mogu zaboraviti. Pisana reč deluje konkretnije i realnije od izgovorene. Veliki broj korisnika kompjutera i interneta upravo su deca, a samim tim i moguća grupa koja će se suočiti s ovim problemom je osnovnoškolskog uzrasta.

Potreba za izradom ovog projekta nastala je kao rezultat želje za mojim samostalnim napretkom i ličnom usavršavanju iz ove oblasti kao i potrebe roditelja i učenika mlađeg školskog uzrasta za edukacijom iz oblasti bezbednog korišćenja interneta i internet sadržaja. Izrada projekta je trajala tri meseca i tokom ovog vremena se stekao uvid u neke osnovne i napredne web tehnologije, kao i u upotrebu alata za tu namenu. Stekla su se mnoga dragocena saznanja koja će se iskoristiti u budućem radu i radu sa roditeljima i učenicima. Projektni zadatak nas je podstakao da tražimo uvek nove i nove mogućnosti rešavanja problema, a najvrednija koju smo

stekli tokom izrade ovog rada je iskustvo. Održano je više edukativnih predavanja gde je glavni cilj bio edukacija roditelja i nastavnika o opasnostima koje prete deci sa interneta.

Cilj ovog istraživačkog rada je da roditelji dobro zaštite svoj računar, kako bi njihova deca kao i razne informacije na računaru bile dovoljno zaštićene od zloupotrebe.

Osnovna hipoteza ovog pristupnog rada, je da roditelji ne štite svoj računar i raznovrsne privatne inoformacije na adekvatan način od zloupotrebe. Kako bi sa tim istovremeno zaštitili svoju decu od štetnih virtuelnih sadržaja. Kod pitanja o tome da kakvu zaštitu imaju na računaru ispitanici su mogli da zaokruže više odgovora, od ukupnog broja ispitanika samo 67% se izjasnio da ima najosnovniju zaštitu računara a to je Anitivirus, a samo 19% ima Firewall zaštitu, koji je znatno ispod očekivanog broja. Na osnovu ovakvog rezultata možemo zaključiti da je postavljena hipoteza osnovana.

Podhipoteza je dokaz za osnovnu hipotezu, da roditelji nisu ni računarski dovoljno obučeni da bih znali zaštititi svoju maloletnu decu, a najveći problem je da nisu ni svesni kojim opasnostima su izložena današnja deca. Dokaz za ovu tvrdnju je pitanje o tome da kakvu zaštitu ima koriste na računaru, gde smo dobili odgovor da 64% anketiranih roditelja ne koristi ni program za praćenje ni program za filtriranje sadržaja, iz tog razloga što više od 60% roditelja koristi računar samo na korisničkom nivou. Međutim neočekivani podatak je da roditelji koji ne koriste program za praćenje ili program za filtriranje sadržaja 40% misli da ovi programi nisu ni korisni. Ovaj rezultat je zastrašujući i treba da skrene pažnju stručnjaka na alarmantnu situaciju u kojoj se trenutno nalazimo. Veoma brzo treba da reaguju svi relevantni faktori na to da se dodatno edukuju i roditelji iz ove oblasti da bi bili upoznati sa opasnostima koje prete njihovoj deci na internetu.

Roditeljska kontrola je jedina potpuno sigurana metoda, nijedan od dostupnih alata za automatsku zaštitu nije 100 odsto pouzdan. Svaki od alata na neki način blokira pristup, ali sigurnosne prepreke mogu da se zaobiđu i alati za zaštitu često propuštaju i štetan sadržaj.

Iz tog razloga slobodno se može reći da najveću i najefikasniju ulogu ima preventivna aktivnost.

Zadatak je svakoga a naročito profesora informatike u školama da pomaže roditeljima, učenicima i ostalim zaposlenima u školi kako da izbegnu kritične situacije a ako se problem eventualno pojavi kako da reše nastalu situaciju. Samim tim smo sastavili savete svim važnim činiocima sa namerom da za zajedničkim delovanjem zaštitimo maloletnu decu od neželjenih internet sadržaja.

Saveti za zaposlene:

- Nađite mirno mesto za razgovor i pažljivo saslušajte dete. Dajte detetu do znanja da je učinilo dobru stvar jer je nekome reklo o svom iskustvu;
- Informišite roditelje i dajte im uputstva u skladu sa preporukama za roditelje
- Informišite policiju ako se radi o ozbiljnim oblicima nasilja, pretećim porukama ili mogućem krivičnom delu;
- Savetujte detetu da ne odgovara na provokativne, uvredljive poruke i sve ostale poruke zbog kojih se oseća loše. Važno je podsticati osećaj sigurnosti kod deteta i ublažiti uznemiravajuće emocionalne reakcije.

- Predložite neke od načina koji bi mogli sprečiti ponavljanje nasilja: promena broja mobilnog, e-mail adrese, napuštanje internet strana (foruma, chat-a, vebloga...) na kojima se nasilje događa ili promena nadimka kojim se dete koristi;
- Upoznajte dete i roditelje da unutar komunikacijskih programa postoji mogućnost blokiranja i filtriranja neželjenih poruka, putem opcija „ignore” ili „block”, kao i sprečavanje pristupa određenim pošiljaocima e-mail ili detetov blog.
- Pomozite učeniku da sačuva sve informacije važne za istragu
Rad sa onima koji čine elektronsko nasilje i posledice nasilnog ponašanja:
Čim se otkrije osoba koja čini nasilje, potrebno je preduzeti korake kako bi se promenio njen stav i ponašanje. Ako se radi o odrasloj osobi, slučaj treba prijaviti policiji. Ako se radi o učeniku, treba mu, osim posledica predviđenih za nasilje u školi, pružiti podršku i pomoć u promeni ponašanja.

Faktori o kojima treba voditi računa prilikom određivanja adekvatnih posledica na ponašanje:

- stepen povređenosti;
- da li se vinovnik skrivao?;
- na koliko je adresa poruka poslata ili kolikoje uznemiravajući materijal (tekst, fotografija, snimak...) uzburkao javnost;
- motivacija osobe i razlozi za nasilje;
- postoji li sukob i u stvarnom životu između te dve osobe ili se radi o zlostavljanju;
- jeli nasilje bilo nenamerno ili namerno.

Saveti i pravila za decu:

- Nikad nemojte davati podatke ni fotografije osebi, svojoj porodici i prijateljima, jer se mogu zloupotrebiti.
- Imajte na umu mogućnost lažnog predstavljanja.
- Nemojte pisati ništa čega biste se stideli ako to pročitaju vaši prijatelji u školi ili u komšiliku,
- Ne šaljite fotografije koje ne biste želeli pokazati drugima.
- Niste vi krivi zbog toga što vam prete i vređaju vas.
- Zatražite pomoć od starijih čak i kad mislite da ste učinili nešto nedopušteno.
- Nemojte izbrisati podatke i fotografije koje vam je neko poslao jer će pomoću njih policija lakše pronaći osobu koja vam preti.
- Nikad nemojte ići sami na sastanak s osobom koju ste upoznali na chat-u ili putem bloga.

Saveti roditeljima:

Vaša deca mogu znati više od vas o tehnologiji, ali Vi znate više o životu, i u ovoj oblasti oni treba od Vas da nauče sigurno da „hodaju” svetom. Ako saznate da je Vaše dete bilo izloženo nasilju putem interneta, morate preduzeti ove korake:

- naučite dete da ne odgovara na nasilne, preteće ili ikakve sumnjive poruke ili pozive;

- ne brišite poruke ili slike jer mogu poslužiti kao dokaz;
- kontaktirajte provajdera internet usluga i prijavite primanje poruke;
- kontaktirajte školu i obavestite ih o neprihvatljivom ponašanju/zlostavljanju ili eventualnim promenama raspoloženja i ponašanja kod deteta;
- kontaktirajte policiju ako poruke sadrže pretnje nasiljem, uhođenje, napastvovanje, dečju pornografiju i sl., ili kada prethodni koraci nisu dali rezultate;
- ako Vam je poznat identitet vinovnika, obavestite o tome školu, policiju, provajdere internet usluga

Ne može se tvditi da sa ovim savetima možemo iskoreniti elektronsko nasilje ali ako će se svi pridržavati ovih saveta onda će biti puno manje onih koji će eventualno steći loše iskustvo ili stradati zbog neznanja ili nedovoljne upućenosti. Veoma je važno da se svi udružimo i na taj način zaštitimo našu decu od neželjenih ili štetnih internet sadržaja.

8. LITERATURA

- [1] Zaštita dece na internetu, izvor: zena.hr
<http://www.poslovnazena.biz/porodica/zastita-dece-na-internetu-27-2785>
- [2] Džordž Orvel, Filtriranje internet sadržaja -
<http://www.sk.rs/2009/02/sktr08.html>
- [3] Access Control List - <http://c2.com/cgi/wiki?AccessControlList>
- [4] Proxy Server - <http://www.publicproxyservers.com>
- [5] Proxy Plus - <http://www.proxyplus.net>
- [6] Webalizer - <http://www.snapfiles.com/get/webalizerwin32.html>
- [7] Blacklist - <http://www.sharewareconnection.com/602lan-suite-content-filter.htm>
- [8] Squid - <http://www.squid-cache.org>
- [9] SquidGuard – <http://www.squidguard.org/>
- [10] Network Guardian 2008 -
<http://www.smoothwall.net/products/networkguardian2008/>
- [11] Branislav Bubanja, Patental Lock Guard, Sveobuhvatna zaštita računara
(<http://www.sk.rs/2004/07/skpd01.html>)
- [12] Milan Milosavljević, Gojko Grubor - Istraga Kompjuterskog Kriminala
(Beograd, 2009)
- [13] Milan Milosavljević, Gojko Grubor – Digitalna Forenzika Računarskog
Sistema (Beograd, 2009)
- [14] Gojko Grubor, Milan Milosavljević – Osnove Zaštite informacija
Metodološko – tehnološke osnove (Beograd, 2010)
- [15] Mladen Veinović, Aleksandar Jevremović – Računarske Mreže (Beograd,
2011)
- [16] Infomreža, Zaštita dece na internetu
(<http://www.infomreza.com/tehnologija/zastita-dece-na-internetu/>)
- [17] Content Control - <http://legal-dictionary.thefreedictionary.com/Content-control>
- [18] Internet Filters - <http://internet-filter-review.toptenreviews.com>
- [19] Crawler Parental Controll - <http://www.crawlerparental.com/>
- [20] Cyber Angels- <http://www.cyberangels.org>
- [21] CyberPatrol <http://www.cyberpatrol.com>
- [22] Zaštitimo decu na internetu - <http://www.kliknibezbedno.rs/>
- [23] Damjan Pelemiš, Odgovorna kriptografija -
<http://www.sk.rs/2003/04/skin01.html>
- [24] Zaštita dece na internetu, priredio: Redakcija -
<http://www.personalmag.rs/it/e-uprava/zastita-dece-na-internetu/>
- [25] Microsoft – Računar u nastavi za decu sa posebnim potrebama (drugo izdanje,
2007.)
- [26] Krstarica Pomoć, Zaštitite svoju decu na Internetu -
http://pomoc.krstarica.com/index.php?action=article&cat_id=002007&id=97

- [27] Donna Rice Hughes, Protecting children in cyberspace - <http://www.protectkids.com/>
- [28] Microsoft, Age-based guidelines for kids' Internet use - <http://www.microsoft.com/security/family-safety/childsafety-age.aspx>
- [29] Zaštita dece na internetu, izvor: zena.hr
(<http://www.poslovnazena.biz/porodica/zastita-dece-na-internetu-27-2785>)
(posećeno:02.01.2011)
- [30] Aleksandar Arsenin, Sprečavanje zloupotrebe u Srbiji, referenca:
www.netcentar.org
(<http://www.internetservis.co.rs/zloupotreba/3.php?idtxt=134>)
(posećeno:06.02.2011)
- [31] Kako zaštititi decu na internetu, izvor: BETA
(<http://www.b92.net/info/vesti/index.php?yyyy=2009&mm=02&dd=10&navid=344237>) (posećeno:16.01.2011)
- [32] Prof. Dr Srbobran Branković - Uvod u metodologiju kvalitativni metodi istraživanja društvenih pojava (Beograd, mart 2007.)
(<http://www.scribd.com/doc/23863224/Metodologija-naucnog-istrazivanja>)
(posećeno:04.03.2012)
- [33] Milan Milosavljević, Gojko Grubor - Istraga Kompjuterskog Kriminala (Beograd, 2009)
- [34] Bezbednost i zaštita dece na internetu – I deo: Sajber zlostavljanje (Cyber bullying, Virtuelno zlostavljanje)
(<http://blog.positive.rs/2010/06/09/bezbednost-i-zastita-dece-na-internetu>)
(posećeno:06.02.2011)
- [35] Dečja pornografija (http://sr.wikipedia.org/sr-el/Дечја_порнографија)
(posećeno: 04.05.2012)
- [36] Wikipedia-Pedofilija(<http://bs.wikipedia.org/wiki/Pedofilija>) (posećeno: 04.05.2012)
- [37] Nova bolest - internet zavisnost
(<http://www.rts.rs/page/stories/sr/story/14/Nauka/106481/Nova+bolest+-+internet+zavisnost.html>) (posećeno:12.04.2011)
- [38] Internet zavisnost – deo drugi (<http://www.nikolinal.com/2010/04/internet-zavisnost-deo-drugi/>) (posećeno:12.04.2012)
- [39] Wikipedija- Operacija Plava Orhideja (http://sr.wikipedia.org/sr-el/Операција_Плава_Орхидеја) (posećeno: 04.05.2012)
- [40] Wikipedija-Operacija Delego (http://sr.wikipedia.org/sr-el/Операција_Делеро) (posećeno: 04.05.2012)
- [41] Bezbednost prilikom upotrebe računara i interneta, autor: HERMES
(<http://serbianforum.org/obrazovanje/18037-bezbednost-prilikom-upotrebe-racunara-i-interneta.html>) (posećeno:08.05.2012)

- [42] Verat.net, Zaštita i edukacija dece na internetu(<http://www.verat.net/sr/novosti/2010-08-02/zastita-i-edukacija-dece-na-internetu/>) (posećeno:18.04.2011)
- [43] Infomreža, Zaštita dece na internetu (<http://www.infomreza.com/tehnologija/zastita-dece-na-internetu/>) (posećeno:18.04.2011)
- [44] <http://www.rts.rs/page/stories/sr/story/125/Dru%C5%A1tvo/38276/Pravilnik+o+kontroli+interneta+stupio+na+snagu.html> (posećeno:18.04.2012)