



CHILD PROTECTION FROM UNWANTED INTERNET CONTENTS – CASE STUDY IN REPUBLIC OF SERBIA

Laslo Tot, Gojko Grubor

Singidunum University, Serbia

Abstract:

Cyber crime involving our children is obviously most dangerous and most serious for parents, schools and society, as well. Parents are not aware that they are making the greatest mistake in their life by physically separating their children and their computer in the separated room. Children are closed within their rooms and parents cannot control which web sites do they visit, how they behave on Internet and what are their activities? Children are convinced they know about computers a lot more than their parents, and there's no method by which someone would deceive them. Unfortunately, they behave uncontrollably and most usually improperly on Internet. As a consequence, there is rise of the children cyber abuse in the Republic of Serbia, too. As children's security and behavior on the Internet is not a regular school subject, many computer science teachers self initially inform children about this subject in their classes. In this paper authors made a survey among 196 parents of the children in Elementary school "Majšanski put" by questioners of the 22 questions put in Serbian and Hungarian, at the same time. The ten most usual tolls that are used to prevent children from unwanted Internet contents are researched and described, as well.

Key words:

Cyber abuse,
Children pornography,
Pedophilia,
Internet addiction,
Filtering & monitoring
software.

INTRODUCTION

What is Internet? Do parents know what are their children doing on Internet, which web sites do they visit? How can we protect them in the Internet world? Most often we alert our children not to talk to strangers, and to be careful when strangers approach them. But, how could we explain to our children that they have to behave in the same way, concerning the world of Internet. Internet is unregulated global media, and it is impossible to „censure“ it in any kind of traditional ways. Internet introduced unexpected changes in the education, giving children the opportunity to subject to their intellectual curiosity and to investigate their world. However, while it helps them to find out more about dinosaurs or about world history, it also can put them to an obscene (amoral), violent and improper Internet contents. So, the best way could be to integrate science into video games and educate children about threats from Internet [2]. Computer crime is rapidly rising, comparing to the crime of the all types. It is already 59% of the crime as a whole, with tendency to become predominant very soon [3, 26].

Today, about 15 percents of world population use Internet intentionally, while even 25 percent unintentionally use Internet by various devices, phones and television. Half of this population involves 5 years old children up to

adolescents. Children mostly use entertainment contents such as: pictures, movies, chat and other types of contents for 'games' or better to say *“for wasting their precious time“*. Usually family's attitude about that, with respect to exceptions, is such as: *„Let the children learn with computers, it will be useful or let them play. It is better to see them here than to roam the streets!“* [23].

Chat room is the most popular but at the same time most dangerous Internet area. This service provides children with possibility to “travel” at any part of the world, to talk and exchange messages with anyone without knowing them. However, the fact is that they could be complete strangers [8, 9].

RELATED WORKS

Despite increasing trend of child pornography on Internet, this subject is not comprehensively analyzed all around the world including Republic of Serbia, too. Internet child abuse is quite well analyzed both in our and in the foreign literature and many hardware and software tools for child protection from undesired Internet attacks are developed.

Many authors have described this phenomenon from different aspects, such as [2, 5, 12, 13, 14, and 42] for example. Some social organizations and NGO have organ-



ized scientific meetings on this issue with the aim to help kids and their parents to understand and prevent their own child from Internet abuse [3, 6, 7, 8, 9, 10, 24, 25, and 40]. Moreover, scholar computer science subjects have also dedicated more of their lectures which point out dangers and risks of uncontrolled Internet and computer use [11, 14, 26, and 27]. Digital forensic science has offered various tools for detecting and potentially preventing Internet pedophiles [26, 30, 31, 32, 33, and 34].

CHILD'S THREATS FROM INTERNET CONTENTS

Cyber abuse is most usual phenomena in Serbia in the past few years and it is done by children. Children and teachers are targeted, too. Most usually *Facebook* is used for creating groups of *haters* such as: „*Who hates that...*“ and by recording videos over phones in order to find and abuse other children intentionally, consciously and unfriendly, with the aim to harm an individual or group.

Some other types of groups are opened where students hate their teachers and professors: „*Who hates biology teacher (name and last name) from MS...* ” On the *Facebook*, at the time of this group creation, were 1.400 groups that contained words: *everyone who hates*

“*Internet addictions* considered if someone use computer more than six hours without taking a break. It is the limit after which somebody could be qualified as an „addict “or sent to treatment [20, 29]. Specialized centers for Internet addiction treatments spread all over the world. Simply, addiction is – bad habit, behavior we cannot get rid of even though it has negative effects in our lives and endanger our daily activities. In average, it is the fact that we spent our time online increasingly. Research done in Stanford at 2005 shown that average American spent about 3.5 hours online. This number is enormously increasing from 2005 onward. There is no absolutely safe Internet child protection, but there is software (most of them are free and could be found by Google search) which can monitor child activity and prevent access to unacceptable web content [4, 28, and 29].

CHILD PROTECTIONS FROM INTERNET THREATS

Content control software

Content –control software, also known as *sensor warrior* web filtering software, is software term designed and optimized for content control that is allowed to a reader, especially when used to limit given material over the web [22]. Software for content – control chooses which content is available on the specific computer or network; reason for this is preventing persons to see content which computer owners or some other authorities may consider as unacceptable; when a user does not authorize it, content - control could be censor shipped[10]. Regular cases used in these programs involve parents who want to limit web pages that their children visit from their home

computers, and schools that do the same with computers within their schools, and also, school stuff, limiting them to specific contents they could see while they are at their work [17, 18, 40, 41, and 6].

Internet Filters Review

As our families are using it ever more, the active role to protect our closest relatives from improper Internet contents is increasing. Even though nothing could replace well informed parents involved in active segments of their children's life, Internet filter software adds up a strong, additional defense layer – by giving to parents additional control measure and inner peace. Internet software filtering gives liability to control displayed content, block web pages and to create passwords. Powerful services such as e-mail filtering and pop up blocking and monitoring chat rooms are only few tools available with modern Internet software filters designed to prevent and protect users from aggressive online companies' tactics offering improper contents [15].

Most important characteristics of that software are as follows [33, 34 and 19]:

- ◆ *Ease of use*
- ◆ *Effective filtering*
- ◆ *Filtering algorithm*
- ◆ *Activity reporting*
- ◆ *Client – server based*
- ◆ *Foreign language filtering*
- ◆ *Port filtering and blocking*

Results of testing different programs for filtering and monitoring Internet contents

Using monitoring system and software for filtering Internet contents, parents could protect their children from online unacceptable contents [6, 7, 12, 13, and 36]. In this paper ten software tools and their feature set and filtering effectiveness were tested and the total grades from 1 to 5 we reassessed, as shown in Table I [23]:

TABLE I: DIFFERENT PROGRAMS FOR FILTERING AND MONITORING TESTED CHARACTERISTICS

Tested characteristics	Operational functions
<i>Feature set</i>	Remote control and reporting; Alarm; Blocking; Adding exceptions; HD scanning on unwanted content; E-mail filtering; Spam filtering; Web site profile and key words; Reporting Internet activities; Family profiling; Setting time feature; Log in for any user; Logging accessed web pages; Receiving alarms via e-mail or textual message or phone call; Selections of categories to be blocked; Making monitor display image to see blocked web sites



Tested characteristics	Operational functions
<i>Filtering effectiveness</i>	<i>Relocking</i> (web site that should not be blocked); <i>Under blocking</i> (web sites that should be blocked but they didn't); Discovering unwanted contents on web sites written in foreign languages; Key words from black listed web sites recognition[4]; Giving alarms and turning off program; Filtering based on key words, not on contents; After clicking OK blocked web site allows entry at that page; Allow entry to many blocked web sites written in foreign languages

In evaluation process of the filtering and monitoring programs the following grade scale were used: **Excellent – 5; Very good – 4; Good – 3; Satisfactory – 2; and Failed – 1.** The test results of filtering and monitoring software are shown in Table II.

TABLE II: RESULTS OF TESTING FILTERING AND MONITORING SOFTWARE

Internet filter	Feature set (1 to 5)	Filtering Effectiveness (1 to 5)
<i>Net nanny</i>	3	3
<i>CYBER sitter</i>	4	3
<i>Cyber Patrol</i>	2	3
<i>Max Protect</i>	4	3
<i>Filter Pak</i>	1	3
<i>Netmop</i>	2.5	2
<i>Safe Eyes</i>	3	2.5
<i>WiseChoice.net</i>	2.5	2
<i>Cyber Sentinel</i>	2	2
<i>McAfee Parents Controls</i>	3	3

However, some other security mechanisms and techniques could help to protect underage from unwanted threats and contents from Internet and from security breaches and misuses of home computer. Some of security mechanisms and techniques are briefly introduced in Table 3. [1, 23, 31, 32, and].

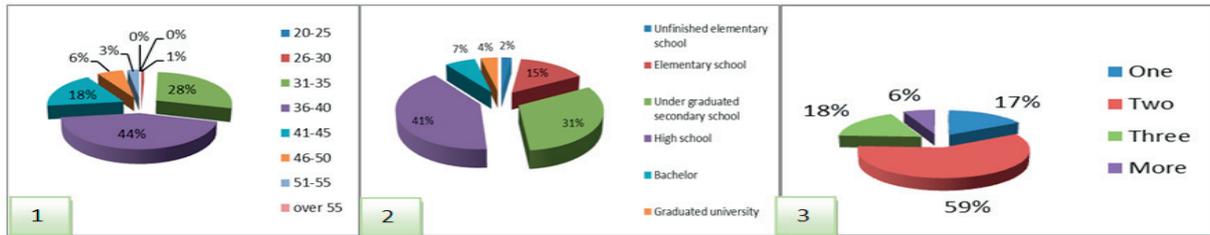
TABLE III: MOST USED SECURITY MECHANISMS AND TECHNIQUES FOR COMPUTER PROTECTION [21, 11]

Security mechanism	Advantage	Disadvantage
<i>Access Control List (ACL)</i>	Determines access control for individuals and authorizes them what to do in own computer system	It is not applicable for access control to the web site with unwanted contents

Security mechanism	Advantage	Disadvantage
<i>Proxy Server</i>	Computer or application software that accepts and passes client's request to another server	Could be misused and could give false security protection
<i>Caching Proxy server</i>	Proxy server that caches content from lased requirement	Could be misused and could give falls security protection
<i>Web proxy</i>	Mostly used as cashed proxy for blocking access to black listed web sites	Could be misused and could give false security protection
<i>Content Filtering Web Proxy[37]</i>	Mostly used in school for filtering unwanted contents from Internet	Could be misused and could give false security protection
<i>Anonymizing Proxy Server[27]</i>	Anonymizing Internet surfing	Web site administrators easy could overtake it
<i>Hostile Proxy Server</i>	Requires often changes of password for webmail and e-banking	Intercepts data flow between client and network
<i>Intercepting Proxy Server</i>	Link between proxy server and gateway without need for configuration	Possible to discover it by IP addresses comparison
<i>Transparent and non-transparent proxy server</i>	Choking identifications, but do not changes client's request	Could be easily deceived
<i>Forced proxy</i>	Filters all traffic on a gateway and Internet	Every time user has to configures proxy for access to Internet
<i>Open proxy server</i>	It tests client for opened proxy servers	Could be illegal and no ethical
<i>Reverse proxy server</i>	It is installed next to net server	There is several reason to use it
<i>Circumventor[14]</i>	Most of them are proxy servers	Allow access to blocked web sites
<i>Proxy +</i>	Run on Windows platforms as firewalls, proxy and mail server	Requires antivirus program installation
<i>Proxy software</i>	Many of them are available	Could be misused and could give false security protection

RESEARCH RESULTS ANALYSIS

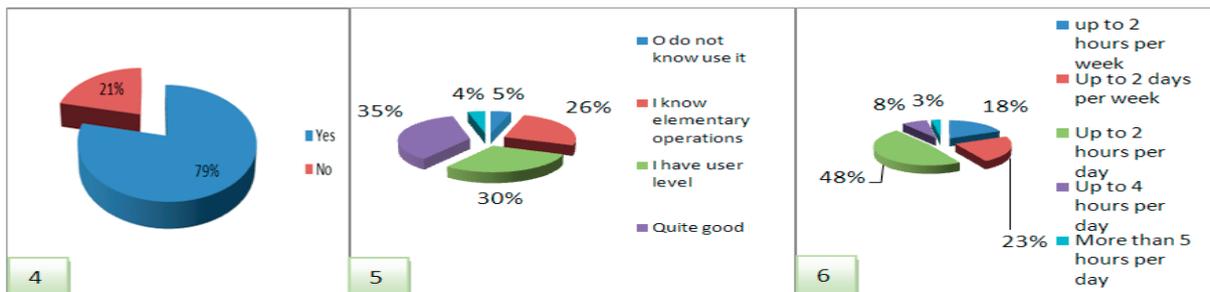
This research is conducted at Elementary school "Majšanski put" by questioners given to the 196 parents in 2012 [35]. The questioner included 22 questions put in Serbian and Hungarian, at the same time. Results of the survey and analysis are given as follows:



1. Analysis of the results: Highest parents age average is between 36 and 40 years or 44%, followed by 31 and 35 years or 28%.

2. Analysis of the results: Highest parents average education level is middle school or 41%, followed by undergraduate school - 31%, and elementary school - 15% and only 4% - finished university.

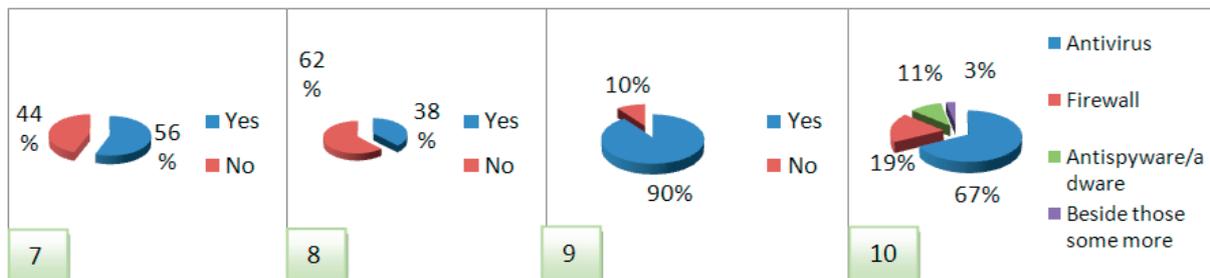
3. Analysis of the results: 59% of parents have two children, 18% - three children, and 17% of them have only one child.



4. Analysis of the results: 79% of parents are computer owners, what is good percentage in spite of level of education

5. Analysis of the results: Only 35% of parents know to use computer quit well, but only 4%of them are professionals. The others do not know to use it or they know only at user's level.

6. Analysis of the results: Only 3% of children use computer more than 5 hours per day and 48% up to 2 hours per day.

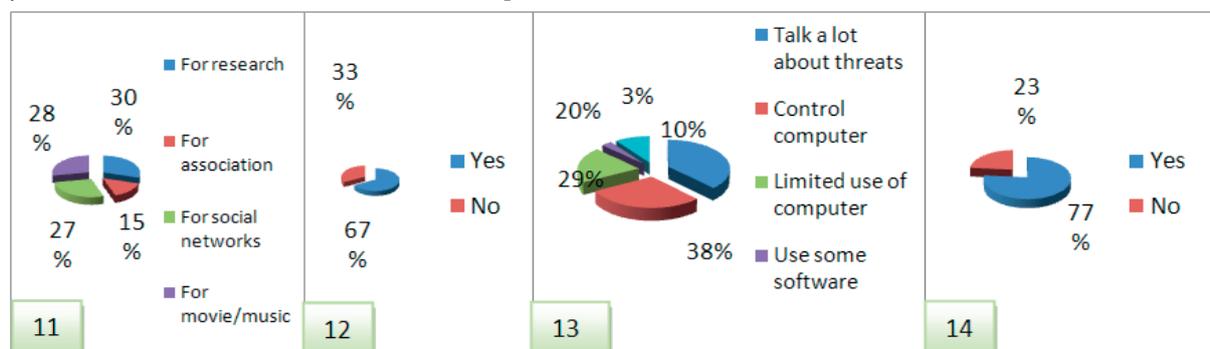


7. Analysis of the results: 56% of children have their own computers and 44% of them use parents' computers.

8. Analysis of the results: Only 38% of children have smart phone that is less than expected.

9. Analysis of the results: 90% of parents have Internet access, that is much higher than expected, and only 10% do not have Internet access at all.

10. Analysis of the results: As for this question parents could give more than one answer, only 67% of them have basic antivirus, and only 19% of them have firewalls, what is bellow expected number.

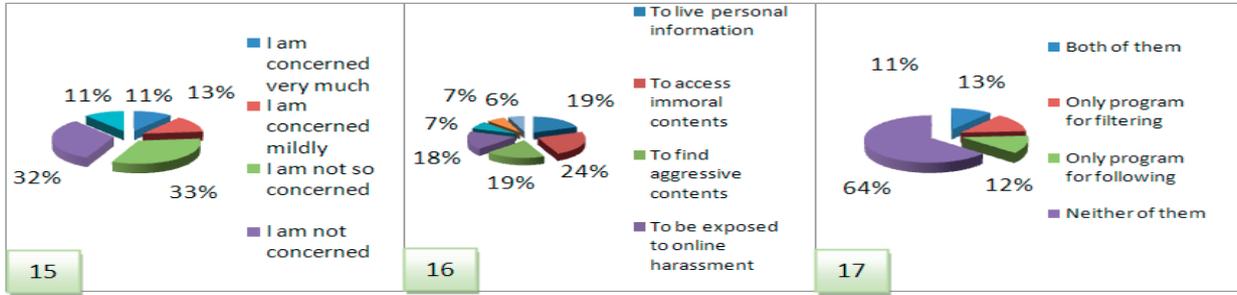


11. Analysis of the results: As for this question parents could give more than one answer, 30% of children use computer for research, 28% - for move/music and 27% - for social networks. Obviously the children use computer evenly for offered options.

12. Analysis of the results: Only 67% parents follow child activities on Internet, what is much less than expected number and show that parents are not aware of threats from the Internet.

13. Analysis of the results: 10% of parents believe their children, 38% - talk about threats on Internet, 29% - control computer and only 3% use some software

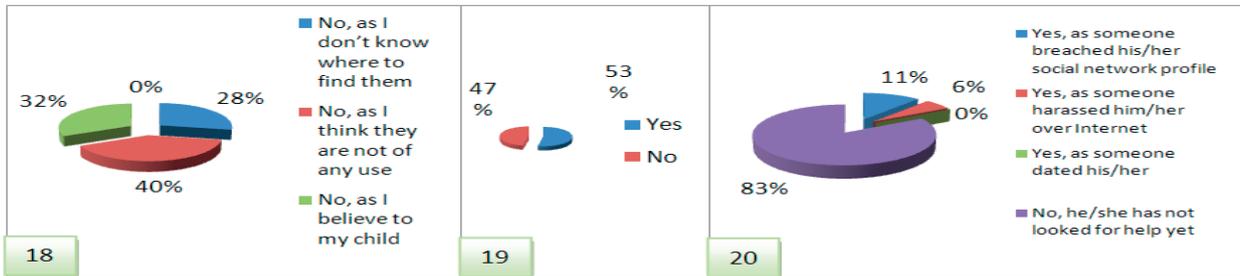
14. Analysis of the results: One of the main problems is that 35% of parents know computer on user's level and only 4% are professional users, but 77% of them believe to know threats from the Internet.



15. Analysis of the results: 11% of parents are concerned very much and the same number is not concerned at all.

16. Analysis of the results: 19% of parents are afraid of living personal information and finding aggressive contents. But 24% of them are concerned that their children could access immoral contents.

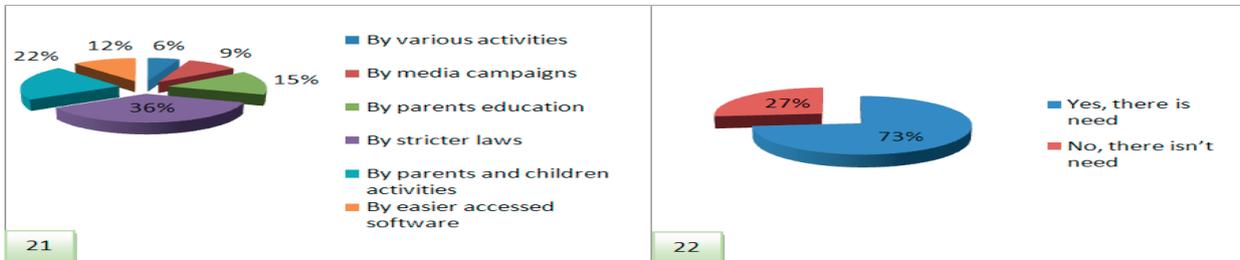
17. Analysis of the results: 64% of parents do not use any program, what is expected as more than 60% of them use computer at user's level only.



18. Analysis of the results: It is unexpected as 40% of parents, which do not use any program, think that those programs are not useful.

19. Analysis of the results: Another unexpected result, as 47% of parents don't know what to do in emergency state.

20. Analysis of the results: According to someone else's researches around 70% of underage have went through some type of online harassment/violence.



21. Analysis of the results: The most number of parents (36%) considered that stricter laws could help them to protect their children.

22. Analysis of the results: It is very good that 73% of parents considered there is need for a company or a NGO which could help them regarding this subject.

CONCLUSION AND FUTURE WORK

Research of this issue about elementary school children behavior on Internet in the case study in The Republic of Serbia proved to be strikingly important social issue that must be solved together, not only with schools authorities, computer science teachers and parents but also with closer and wider social community. Deficiency of a similar researches caused lack of scientific element for previously set apart and established relations between research factors as well as for reliability of deducted conclusions. Children and minors should be protected from

violent and pornographic contents, incorrect messages from people that could take advantage of their trust, trying to persuade them to give away their personal data, exchange photos, even to meet with their online 'friends' without being accompanied by their parents or teachers. We should educate them how to use Internet safely and correctly.

Any child can be protected from most various types of online assaults by using proper programs that block access to unwonted web sites. This method enables parents to keep their children away from web sites at the time they cannot monitor their Internet activities and, after all, to



be certain that their children are not exposed to disturbing contents and messages. Security programs are mostly not free of charge. Their basic function is to filter web pages and some of these programs even let users to set time limits for Internet access. Moreover, there is option to also set limit for games and file types which child may use. Therefore, much more researches in this field must be done in future, particularly in area of more sophisticated and automated hardware and software tools.

REFERENCES

- [1] *Access Control List*, <http://c2.com/cgi/wiki?AccessControlList>, (accessed in May 2012).
- [2] Aleksandar Arsenin, *Prevention of misuse in Serbia*, (www.netcentar.org).<http://www.internetservis.co.rs/zloupotreba/3.php?idtxt=134>, (accessed 06.02.2012).
- [3] BETA, *How to protect children on Internet*, http://www.b92.net/info/vesti/index.php?yyyy=2009&mm=02&dd=10&nav_id=344237, (accessed:16.01.2011)
- [4] *Blacklist*, <http://www.sharewareconnection.com/602lan-suite-content-filter.htm>, (accessed in May 2012).
- [5] Branislav Bubanja, *Parental Lock Guard, Comprehensive Computer Protection*, <http://www.sk.rs/2004/07/skpd01.html>, (accessed in May 2012).
- [6] *Content Control*,<http://legal-dictionary.thefreedictionary.com/Content-control>, (accessed at 21 of February, 2013).
- [7] *Crawler Parental Control*, <http://www.crawlerparental.com/>, (accessed at 21 of February, 2013).
- [8] *Cyber Angels*, <http://www.cyberangels.org>, (accessed at 21 of February, 2013).
- [9] *Cyber bullying, Virtual violence*, <http://blog.positive.rs/2010/06/09/bezbednost-i-zastita-dece-na-internetu>, (accessed: 06.02.2011)
- [10] *Cyber Patrol*, <http://www.cyberpatrol.com>, accessed at 21 of February, 2013.
- [11] Damjan Pelemiš, *Responsible cryptography*, <http://www.sk.rs/2009/02/sktr08.html>, (accessed at 21 of February, 2013).
- [12] Donna Rice Hughes, *Protecting children in cyberspace*, <http://www.protectkids.com/>, (accessed at 21 of February, 2013).
- [13] Gorge Orwell, *Filtrating Internet Content*, <http://www.sk.rs/2009/02/sktr08.html>, (accessed in May 2012).
- [14] Gojko Grubor, Milan Milosavljević, *Information Security Basic*, Singidunum University, Belgrade, 2010.
- [15] HERMES, *Security of computer use on Internet*,(<http://serbianforum.org/obrazovanje/18037-bezbednost-prilikom-upotrebe-racunara-i-interneta.html>) (accessed:08.05.2012)
- [16] <http://www.rts.rs/page/stories/sr/story/125/Dru%C5%A1tvo/38276/Pravilnik+o+kontrolni+interneta+stupio+na+snagu.html> (accessed:18.04.2012)
- [17] Infomreža, *Children protection on Internet*, <http://www.infomreza.com/tehnologija/zastita-dece-na-internetu/>, accessed at 21 of February, 2013.
- [18] Infomreža, *Children protection on Internet*,<http://www.infomreza.com/tehnologija/zastita-dece-na-internetu/>) (accessed:18.04.2011)
- [19] *Internet Filters*, <http://internet-filter-review.toptenreviews.com>, accessed at 21 of February, 2013.
- [20] *Internet addiction– 2. part*,<http://www.nikolinal.com/2010/04/internet-zavisnost-deo-drugi/>, (accessed:12.04.2012).
- [21] Károly Hercegfı, *Heart Rate Variability Monitoring during Human-Computer Interaction*, Department of Ergonomics and Psychology, Budapest University of Technology and Economics, Hungary, Acta Polytechnica Hungarica Vol. 8, No. 5, 2011.
- [22] Krstarica Pomoć, *Protect Your Children on Internet*, <http://pomoc.krstarica.com/index.php?action=article&catid=002007&id=97>(accessed at 21 of February, 2013).
- [23] Laslo Tot, *Children protection from unwanted Internet contents*, master theses, Singidunum University, Belgrade, 2013.
- [24] Microsoft, *Computers in educational system for disabled children*, 2007.
- [25] Microsoft, *Age-based guidelines for kids' Internet use*,<http://www.microsoft.com/security/family-safety/childsafety-age.aspx>, 2011.
- [26] Milan Milosavljević, Gojko Grubor, *Computer Crime Investigation- Methodology & Technology Basic*, Singidunum University, Belgrade, 2009.
- [27] Mladen Veinović, Aleksandar Jevremović, *Computer Network*, Singidunum University, Belgrade, 2011.
- [28] *Network Guardian*, <http://www.smoothwall.net/products/networkguardian2008/>, 2008
- [29] *New disease - Internet addiction*, (<http://www.rts.rs/page/stories/sr/story/14/Nauka/106481/Nova+bolest+-+internet+zavisnost.html>) (accessed:12.04.2011)
- [30] Péter Tóth, *Learning Strategies and Styles in Vocational Education*, Trefort Ágoston Centre for Engineering Education, Óbuda University, Budapest, Hungary, Acta Polytechnica Hungarica Vol. 9, No. 3, 2012.
- [31] *Proxy Plus*, <http://www.proxyplus.net>, accessed in May 2012.
- [32] *Proxy Server*, <http://www.publicproxyservers.com>, accessed in May 2012.
- [33] *Squid*, <http://www.squid-cache.org>, accessed in May 2012.
- [34] *Squid Guard*, <http://www.squidguard.org/>, accessed in May 2012.
- [35] Srbobran Branković, *Uvod u metodologiju: kvalitativni metodi istraživanja društvenih pojava*, Beograd, mart 2007. <http://www.scribd.com/doc/23863224/Metodologija-naucnog-istrazivanja>, (accessed: 04.03.2012)
- [36] Verat.net, *Children protection and education on Internet*, <http://www.verat.net/sr/novosti/2010-08-02/zastita-i-educacija-dece-na-internetu/>, (accessed:18.04.2011)
- [37] *Webalizer*, <http://www.snapfiles.com/get/webalizerwin32.html>, (accessed in May 2012).
- [38] Wikipedia, *Child pornography*, http://sr.wikipedia.org/sr-el/dečija_pornografija (accessed: 04.05.2012)
- [39] Wikipedia, *Pedophilia*, <http://bs.wikipedia.org/wiki/pedofilija> (accessed: 04.05.2012)
- [40] *Children protection on Internet*, <http://www.personalmag.rs/it/e-uprava/zastita-dece-na-internetu/>, (accessed at 21 of February, 2013).
- [41] *Children protection on Internet*, <http://www.kliknibezbedno.rs/>, (accessed at 21 of February, 2013).
- [42] Zona Kostić, *Child pornography digital forensic investigation*, Scientific Conference "Sinergija", Bijeljina, BiH, 2009.