

# mipro 2014



ISSN 1847-3938

organizer

**μpro**

37<sup>th</sup>

## international convention

May 26-30, 2014, Opatija – Adriatic Coast, Croatia

*Lampadem tradere*



mipro - path to knowledge and innovation

**mipro proceedings**



# **MIPRO 2014**

**37<sup>th</sup> International Convention**

**May 26 - 30, 2014  
Opatija, Croatia**

## **Proceedings**

Conferences:

**Microelectronics, Electronics and Electronic Technology /MEET**

**Distributed Computing, Visualization and Biomedical  
Engineering /DC VIS**

**Telecommunications & Information /CTI**

**Computers in Education /CE**

**Computers in Technical Systems /CTS**

**Intelligent Systems /CIS**

**Information Systems Security /ISS**

**Business Intelligence Systems /miproBIS**

**Digital Economy and Government, Local Government, Public  
Services / DE-GLGPS**

**MIPRO Junior - Student Papers /SP**

Edited by:  
**Petar Biljanović**

All papers are published in their original form

For Publisher:

**Petar Biljanović**

Publisher:

Croatian Society for Information and Communication Technology,  
Electronics and Microelectronics - **MIPRO**  
Office: Kružna 8/II, P. O. Box 303, HR-51001 Rijeka, Croatia  
Phone/Fax: (+385) 51 423 984

Printed by:

**GRAFIK, Rijeka**

**ISBN 978-953-233-078-6**

**Copyright © 2014 by MIPRO**

All rights reserved. No part of this book may be reproduced in any form, nor may be stored in a retrieval system or transmitted in any form, without written permission from the publisher.

<b>Visual Verification of the Properties of Pseudorandom Sequences .....</b>	<b>959</b>
S. Predanić, G. Vujisić, T. Horvat	
<b>Integration of Conceptual Data Modeling Methods: Higher Education Experiences... 963</b>	
Lj. Kazi, B. Radulovic, I. Berkovic, Z. Kazi	
<b>Technology Use in EFL Learning .....</b>	<b>969</b>
D. Pešut	
<b>Development of a Computer System to Support Knowledge Acquisition of Basic Logical Forms Using Fairy Tale “Alice in Wonderland” .....</b>	<b>974</b>
A. Mihaljević Španjić, A. Jakupović, M. Tomić	
<b>Designing the Programming Assignment for a University Compiler Design Course....</b>	<b>979</b>
I. Budiselić, D. Škvorc, S. Srbljić	
<b>Micro Assessment SaaS Cloud Solution.....</b>	<b>985</b>
A. Bundovski, M. Gusev, S. Ristov	
<b>The Role of IC Technology in Development and Application of Experimental Methods and Multivariate Analysis .....</b>	<b>991</b>
M. Orlić, M. Marinović	
<b>The Views of Students and Teachers on Implementation of E-learning in Educational Process .....</b>	<b>997</b>
D. Glušac, D. Radosav, D. Karuović, Ž. Juhas	
<b>The Model of Remote Video Surveillance in Hierarchical Autonomous E-testing <i>WbeTS</i> System for Knowledge Testing.....</b>	<b>1001</b>
D. Purković, E. Ban	
<b>Web Application Development with Component Frameworks .....</b>	<b>1007</b>
V. Okanović	
<b>Agile Management: A Teaching Model Based on SCRUM.....</b>	<b>1011</b>
Ž. Požgaj, N. Vlahović, V. Bosilj-Vukšić	
<b>Ethical Aspects and Capabilities of Social Networks – Students, Teachers, and Facebook in Elementary Schools .....</b>	<b>1017</b>
D. Vincek	
<b>Computer Classroom Operating System Security (Windows) .....</b>	<b>1023</b>
M. Zovkić, T. Vrbanec	
<b>Elementary School Students Using Facebook: A Case Study Of Croatian Elementary School ban Josip Jelačić.....</b>	<b>1029</b>
M. Draženović	
<b>Evaluation Study and Results of Intelligent Pedagogical Agent-led Learning Scenarios in a Virtual World .....</b>	<b>1032</b>
M. Soliman, C. Guetl	

<b>LeCTo: a Rich Lecture Capture Solution.....</b>	<b>1037</b>
P. Pale, J. Petrović, B. Jeren	
<b>Using Data Mining for Learning Path Recommendation and Visualization in an Intelligent Tutoring System.....</b>	<b>1042</b>
I. Jugo, B. Kovačić, V. Slavuj	
<b>Security Analysis of Wireless Network Access Following 802.11 Standard in Educational Institutions of the Republic of Croatia .....</b>	<b>1047</b>
A. Skendžić, B. Kovačić	
<b>Use of iPads in Foreign Language Classes .....</b>	<b>1055</b>
K. Starkl Crnković	
<b>Tablet PC &amp; Smartphone Uses in Education (TabletTours) .....</b>	<b>1058</b>
K. Bedi	
<b>Informatika kao izborni predmet ili izvannastavna aktivnost u razrednoj nastavi ....</b>	<b>1064</b>
J. Šurić, T. Pavičić, M. Dumančić	
<b>Primjer projekta u nastavi informatike – što je lijepo ljudskom oku.....</b>	<b>1070</b>
V. Skočir	
<b>Primjena interaktivnog videa u obrazovnim nastavnim sredstvima .....</b>	<b>1075</b>
D. Vrbanc	
<b>Primjena e-portfolija u nastavi.....</b>	<b>1080</b>
S. Šalković	
<b>Bonton digitalnog doba.....</b>	<b>1083</b>
M. Mirković	
<b>IKT, ljudski resursi te informacijska i računalna sigurnost u hrvatskom osnovnom školstvu.....</b>	<b>1088</b>
M. Zovkić, T. Vrbanec	
<b>Učinkovitost elektroničkog učenja u nastavi.....</b>	<b>1094</b>
M. Sertić	
<b>Analiza uspješnosti u usvajanju algoritamskog načina razmišljanja kod učenika u prvom razredu novog strukovnog kurikulumu za zanimanje Tehničar za računalstvo.....</b>	<b>1110</b>
K. Blažeka	
<b>iPad u nastavi matematike i fizike.....</b>	<b>1104</b>
M. Babić	
<b>#codeEU.....</b>	<b>1107</b>
I. Ružić	

# IKT, ljudski resursi te informacijska i računalna sigurnost u hrvatskom osnovnom školstvu

Mario Zovkić\*, Tedo Vrbanec\*\*

\*Osnovna škola Barilović, Barilović & Osnovna škola "Katarine Zrinski" Krnjak, Krnjak, Hrvatska

\*\*Učiteljski fakultet, Sveučilište u Zagrebu, Zagreb, Hrvatska

\*mario.zovkic1@skole.hr, \*\*tedo.vrbanec@gmail.com

**Abstract** - Nastavnici informatike u hrvatskim osnovnim školama često su "volonteri" u ulozi sistemskih administratora. Ta je uloga tehnički i tehnološki zahtjevna, a vremenski izuzetno zahtjevna. U školama se takav angažman uglavnom ne primjećuje. Sistemsku administraciju dodatno otežavaju sljedeće činjenice: (a) računala su često različitih hardverskih konfiguracija što onemogućava neke metode održavanja, (b) računala su u prosjeku stara osam godina pa imaju slabije hardverske mogućnosti (slabiji procesor te nedovoljna/minimalna količina radne memorije), zbog čega su spora. Računalne učionice u prosjeku sadrže 19 računala, što predstavlja problem ako su razredna odjeljenja većeg broja učenika, a razredna odjeljenja nije moguće dijeliti na manje grupe. U manjim školama nastavnici informatike često su pored računalne učionice zaduženi za održavanje i svih drugih računala u školi. Učenici se uobičajeno prijavljuju na računala u svojstvu administratora, sve se više raznih uređaja poput pametnih telefona, tableta i fableta spaja na školsku mrežu, a informatičari i ostali nastavnici zbog kroničnog nedostatka novaca za stručno usavršavanje nisu dovoljno educirani s novim prijetnjama i metodama zaštite u pogledu računalne i informacijske sigurnosti. Stoga edukacija o IKT sigurnosti ovisi o dobroj volji, slobodnom vremenu i entuzijazmu pojedinog nastavnika (informatike). Rad predstavlja pregled sigurnosti internet komunikacija te fizičke sigurnosti IKT u školskim računalnim učionicama.

**Ključne riječi:** e-sigurnost, IKT, računalna učionica.

## I. UVOD

Računala u hrvatskim osnovnim školama krajem svake školske godine najčešće su puna virusa, pomiješanih/izbrisanih prečaca, promijenjenih ikona, izbrisanih programa ili programa koji javljaju čudne greške i/ili se jako dugo pokreću, nakrcana su raznim nepotrebnim programima (engl. bloatware), zbog svega toga su usporena i općenito se nalaze u jednom konfuznom stanju – reklo bi se da su "zrela za reinstalaciju" OS-a i svih potrebnih programa. Ukoliko se o sigurnosti ne vodi računa te ukoliko se u nj ne uloži potrebno vrijeme i trud, za godinu dana simptomi su isti.

Nastavnici informatike u hrvatskim osnovnim školama najčešće su i administratori školskih IT resursa. Prema CARNetu, [1] administrator je "u ime članice odgovoran za ispravnost i stabilnost funkcioniranja resursa koje je CARNet stavio na raspolaganje članici, kao i za opće tehničko i sigurnosno stanje računalno-komunikacijskog sustava članice spojene u CARNet mrežu." Realnost je da se s vremena na vrijeme, unatoč svim poduzetim mjerama zaštite, poneka računala zaraze malicioznim kodom koji

se potom počne širiti - lokalnom mrežom, prijenosnim medijima (tipično USB memorijama) ili elektroničkom poštom. Bez obzira no to ima li škola pristup Internetu putem CARNeta ili putem nekog drugog ISP-a, isti može zbog pritužbi Abuse službi, biti prisiljen ukinuti pristup Internetu cijeloj ustanovi dok se problem ne riješi. Tko za taj propust i kome odgovara? Trenutno odgovara nastavnik informatike i to najprije ravnatelju, a onda potencijalno i CARNetu<sup>1</sup> koji može [2] "privremeno ili trajno uskratiti pravo korištenja mreže i njezinih servisa", odnosno "u slučaju težih prekršaja, povrede zakona, CARNet će prekršitelja prijaviti nadležnim organima".

U svakodnevnom radu, nastavnicima informatike se (prirodno) nameće zahtjev da njihova sredstva rada pomoću kojih održavaju nastavu i ona kojima se učenici služe tijekom nastave, budu upotrebljiva, funkcionalna, bez malicioznog koda i grešaka u radu. Kad god postoji problem s računalima u informatičkoj učionici, nepisano je pravilo da ga nastavnik informatike sam riješi. U protivnom je ostao bez dijela sredstava za rad (računala) zbog čega trpi nastava. To je to više izraženo što je veća disproporcija broja učenika i računala. Ne riješi li nastavnik informatike problem, (zbog nedostatka vremena, neznanja, dobre volje ili jednostavno zato jer to nije ni dužan raditi), mora čekati dozvolu ravnatelja odnosno raspoloživost financijskih sredstava škole kako bi se računalo poslalo u servis, te čekati na (uvijek skuplji negoli je potrebno) popravak. Što je škola po broju učenika manja, to je problem veći, jer u Republici Hrvatskoj škole primaju financijska sredstva za materijalne troškove prema broju učenika [3]. Nadalje, kolektiv očekuje, a ponekad čak i zahtijeva od nastavnika informatike, da rješava računalne probleme cijele ustanove. Ponekad ravnatelj takvo zaduženje i formalno dodijeli nastavniku informatike. Naizgled je logično da nastavnik informatike održava računala u školi, ali u suštini je nepravedno ukoliko ga se proporcionalno ne rastereti nastave. Ilustrirajmo to primjerom: želi li nastavnik informatike naučiti ili usavršiti strani jezik, po istoj bi ga logici tome trebao besplatno naučiti nastavnik stranog jezika; a za usavršavanje matematike, besplatno bi ga trebao podučiti nastavnik matematike, itd. Dakle, da li bi računalo drugih nastavnika trebao besplatno servisirati nastavnik informatike? Svi ti popravci i održavanje računala (uključujući i instalaciju sigurnosnih zakrpi, ažuriranja programa i slično), rade se izvan nastave, a svi ostali poslovi koje nastavnik ima u zaduženju odgađaju se za kasnije. Ipak, u praksi nastavnici informatike obično

<sup>1</sup> Gotovo sve škole u Hrvatskoj imaju besplatan pristup internetu preko CARNeta, a troškove pokriva MZOS.

rado educiraju svoje kolege, pomažu im savjetima i rješavaju njihove IT probleme, ali to je stvar prijateljstva ili kolegijalnosti te bi trebalo biti dobrovoljno.

U sklopu obrazovnog sustava, malo se toga može postići. Nastavnik informatike je u prošlosti dobivao uz satnicu i funkciju "voditelj informatičke učionice", pod uvjetom da je ravnatelj osnovne škole to zatražio od MZOS-a te dobio dozvolu. Time mu se oslobodilo dva do četiri sata nastave na ime održavanja računala. Posljednjim važećim kolektivnim ugovorom za zaposlenike u osnovnoškolskim ustanovama (koji je 27. prosinca 2013. odlukom Vlade Republike Hrvatske otkazan, a trenutno teče otkazni rok od tri mjeseca [4]) naziv "voditelj informatičke učionice" je izbačen. Škola koja do sada nije imala voditelja informatičke učionice teško da će je dobiti jer je funkcija vezana za određenu školu koja je tu dozvolu po starom kolektivnom ugovoru ishodila. Male škole (prema osobnom iskustvu autora) u pravilu ne dobiju odobrenje da se nastavniku informatike do popunjenja satnice odobri nekoliko sati tjedno za održavanje računala. U srednjim školama RH zakonski je uređeno zapošljavanje osoba kojima je jedini zadatak brinuti o ispravnosti, ažurnosti i sigurnosti računala i računalnih mreža [5]. U susjednoj Sloveniji "Pravilnikom o normativih in standardih za izvajanje programa osnovne šole" uvedeno je 2007. godine radno mjesto [6] "računalnikar - organizator informacijskih dejavnosti" kojem se priznaje određen dio sati u redovnu satnicu s obzirom na broj odjeljenja u školi, pa ako primjerice škola ima do 8 razrednih odjeljenja onda računalnikar dobije 0,20 udjela radnog mjesta, a ako škola ima 46 odjeljenja onda je udio radnog mjesta 1, odnosno puno radno vrijeme prema članku 11 [6].

U Njemačkoj se u srednjim gimnazijskim školama (5-9 razred) predaje informatika, a za održavanje se zapošljava druga osoba ili se informatičaru to ubraja u satnicu. U SAD-u, obrazovne institucije u cijeloj obrazovnoj vertikali (osnovne škole, srednje, fakulteti) zapošljavaju tzv. "Computer Technician" koji su zapravo dio radnog mjesta pod imenom "Chief Operating Officer"<sup>2</sup>. Svaki okrug (district) samostalno plaća osobu, a institucija samostalno određuje da li je ta pozicija striktno vezana za IT ili npr. mrežu koja ne uključuje posao poučavanja. "Building technicians" kako ih zovu u SAD-u prosječno provedu oko 1.5 dana svaki tjedan u manjim školama, dok u većim školama svaki tjedan provedu oko 4-5 dana. [7]

Primjeri na koje bi se u Hrvatskoj mogli ugledati jesu Makedonija i Indonezija (Sumatra) gdje postoje tzv. "Student Support Technician Clubs" (SSTCs) u kojima se učenici/studenti organiziraju u grupu/sekciju koja je zadužena za održavanje računala. [8] Skupine se sastoje od najuspješnijih učenika/studenata koji i poučavaju mlađe generacije o brizi za računalima.

U nastavku donosimo pregled osnovnih tema računalne sigurnosti u informatičkoj učionici: fizičke sigurnosti i sigurnosti komunikacije uz koje ćemo predložiti neka poželjna pravila korištenja računala.

<sup>2</sup> Drugi nazivi koji se još susreću su: School Technology Integration Coordinator, Technology Coordinator, Director of Educational Technology.

## II. INSTITUCIONALNI OKVIR ZA JAČANJE E-SIGURNOSTI U RH

U Hrvatskoj se pitanjima informacijske, komunikacijske, računalne, podatkovne i ostalih oblika sigurnosti te privatnošću i povjerljivošću uvelike bavi CARNet, posebno sa svojim projektom "Informacijsko-komunikacijska tehnologija u obrazovanju – ICT Edu" koji se provodi kroz 3 modula, po jedan za svaku školsku godinu. On ima za cilj [9] "upoznati sve učitelje, nastavnike, stručne suradnike i ravnatelje osnovnih i srednjih škola u Republici Hrvatskoj s brojnim sadržajima i uslugama koje im pruža MZOS i CARNet, te ih o nekim sadržajima detaljnije educirati". Sa stajališta ICT sigurnosti, projekt sadrži teme iz "Sigurnosti na internetu" gdje su dani savjeti za roditelje i učenike o štetnim programima te problemima komunikacije na Internetu.

MUP, Ministarstvo uprave, Hrvatska akademska i istraživačka mreža - CARNet, Tehničko veleučilište u Zagrebu, Udruga „Suradnici u učenju“, Poliklinika za zaštitu djece Grada Zagreba, Agencija za zaštitu osobnih podataka i drugi pridružujući partneri Ministarstva znanosti, obrazovanja i športa, Ministarstvo socijalne politike i mladih, Agencija za odgoj i obrazovanje, Učenički dom Hrvatskoga Radiše i Hrvatska agencija za poštu i elektroničke komunikacije su 05. lipnja 2012. godine potpisali Sporazum o strateškom partnerstvu na uspostavi Centra za sigurniji Internet [10] kojem je cilj zajedničko promicanje računalne i informacijske sigurnosti u RH, te se "zalagati za institucionalizirano uvođenje računalne i informacijske sigurnosti u obrazovni sustav, npr. kao dio nastavnog programa informatike za osnovne i srednje škole." Taj centar omogućava prijave eventualnih povreda on-line sigurnosti djece (svih nezakonitih, štetnih i opasnih sadržaja počinjenih na štetu djece i mladih) te je predstavljen 28. rujna 2013. u Zagrebu. Nastao je kao dio IPA twinning projekta pod punim nazivom „Jačanje kapaciteta u području suzbijanja seksualnog iskorištavanja i seksualnog zlostavljanja djece te pružanje pomoći policije ranjivim žrtvama kriminaliteta.“ Takvi centri za sigurniji Internet (engl. Safer Internet Center) su trenutno smješteni u svih 28 zemalja EU te u Islandu, Norveškoj i Rusiji [11] te su dio Insafe-INHOPE joint mreže.

U RH je CARNet 19. srpnja 1996. osnovao CCERT (CARNet Computer Emergency Response Team) - nacionalno središte za sigurnost računalnih mreža. Dobivanjem suglasnosti Ureda vijeća za nacionalnu sigurnost, u CARNetu je 13. svibnja 2009. počeo s radom Odjel za Nacionalni CERT osnovan u skladu sa Zakonom o informacijskoj sigurnosti RH i prema tom zakonu jedna od njegovih zadaća je [12] "obrada incidenata na Internetu, tj. očuvanje informacijske sigurnosti u RH", a misija "prevencija i zaštita od računalnih ugroza sigurnosti javnih informacijskih sustava u Republici Hrvatskoj." Nacionalni CERT preuzeo je ulogu i nasljednik je CARNet CERT-a.

Europska mreža centara za sigurniji Internet - Insafe i Međunarodna zajednica online linija za pomoć – INHOPE, obilježavaju Safer Internet Day - SID. SID [11]

organizira "Insafe" u veljači svake godine s ciljem promicanja sigurnije i odgovornije uporabe online tehnologije i mobilnih telefona, posebice među djecom i mladima diljem svijeta. Inicijativa je pokrenuta u okviru Programa za sigurniji Internet Europske komisije, a jednom godišnje poziva na uključivanje u aktivnosti za stvaranje sigurnijeg i boljeg Interneta za djecu i mlade. SID je prvi puta u svijetu obilježen 2004. g., u RH 2009-te, a svake godine se provode razne aktivnosti na određenu temu.

Najnoviji projekt pod nazivom "Sigurnost djece na Internetu" ima za cilj ući u Hrvatski kvalifikacijski okvir, tj. pokušaj je da se MZOS-u dokaže da teme e-sigurnosti uđu u kurikulum predmeta (koje će ministarstvo tek izraditi za svaki pojedini predmet). Nositelj gore navedenog projekta je OŠ Veliki Bukovec, a partneri osnovne škole: OŠ Popovača, OŠ Mato Lovrak iz Nove Gradiške, OŠ Gripe iz Splita i OŠ Mladost iz Osijeka. Projekt će trajati od 19. kolovoza 2013. do 19. prosinca 2014. uz sudjelovanje učenika, učitelja, roditelja te lokalne i šire zajednice. [13]. U sklopu tog projekta učitelji iz nabrojanih pet osnovnih škola iz Hrvatske izradit će i zatim primijeniti školski kurikulum o sigurnosti djece na internetu u sklopu Hrvatskog kvalifikacijskog okvira kojim će direktno biti uključeno 200 učitelja, 220 učenika te 220 roditelja. Bit će izrađeni i priručnici, radni materijali, multimedijalni sadržaji i interaktivne igre za pomoć u edukaciji djece, roditelja i učitelja te prevenciji elektroničkog nasilja. Školski kurikulum bit će pripremljen za sve razrede osnovne škole, odnosno organiziran u četiri grupe prema uzrastu učenika. Svi pripremljeni sadržaji bit će besplatni i dostupni za korištenje svim školama u Hrvatskoj. Projekt financira IPA program Europske unije s 2,5 milijuna kuna. [13]

### III. FIZIČKA SIGURNOST ICT-A U ŠKOLI

"Osnova fizičke sigurnosti je zaštita fizičkog dijela informatičke infrastrukture, zgrade u kojoj je ona smještena, kao i medija za pohranu podataka te komunikacijske opreme. Mjere fizičke sigurnosti obuhvaćaju sve obrambene mjere poduzete u svrhu zaštite računalne infrastrukture od prirodnih nepogoda, problema u okolini, nezgoda i namjernih oštećenja". [14] "Značaj fizičke zaštite sustava je distribucijom opreme i podataka te uključivanjem u Internet postao još važnijom, ali i znatno složenijom." [15]

Nastavnik informatike mora utvrditi tko ima izravan fizički pristup računalima, da li je to neophodno te kako zaštititi računala od oštećenja ili krađe. Oprema poput monitora ili kućišta može se pričvrstiti na radni stol s raznim kablovima ukoliko postoje utori na samom sklopovlju, običnim i jeftinim jednokratnim plastičnim vezicama (engl. "tie straps") ili se pričvršćuju vijcima za radni stol (LCD i LED monitori). Manje je predmete, poput miša i tipkovnice, teže osigurati od krađe, no u tom slučaju poželjno je na takve stvari staviti inventarni broj ili neko drugo obilježje (npr. logo/natpis ustanove). Na taj se način obeshrabruju lopovi, a ujedno je situacija uvijek spremna za popis inventure.

Za neophodnu razinu fizičke sigurnosti, preporučljivo je zaključati komunikacijske ormariće i prostorije u kojima se nalazi mrežna oprema i poslužitelji. Ukoliko u informatičkoj učionici nema video nadzora, kada se ona koristi uvijek bi trebao biti nazočan netko od zaposlenika škole, a kada se računala ne koriste prostoriju bi trebalo zaključavati.

#### A. Videonadzor

Video nadzor učionice, uz jasne obavijesti o njegovu postojanju, vrlo je poželjna zaštitna mjera koja obeshrabruje potencijalne lopove i vandale. Računalo skromnih performansi i web kamera [16] dovoljni su za izradu jednostavnog video nadzora "iako je uporaba video-nadzora u Republici Hrvatskoj u samom začetku i nedovoljno normativno uređena" obzirom [17] "na ograničenu uporabu tehničkih snimki kao dokaza u postupcima (kazneni i prekršajni)". Zakonom o kaznenom postupku [18] donesenim 2008. godine započela je primjena načela pretežitog interesa kod kojeg postoji mogućnost korištenja tehničkih snimki te drugih dokaza pribavljenih na nezakoniti način ako interes pravde i pravičnosti preteže nad interesom zaštite dobara. "Što se tiče valjanosti tehničkih snimki u prekršajnom postupku, Prekršajni zakon propisuje da su bilješke i tehničke snimke i formalno dokazi u prekršajnom postupku ukoliko ih je ovlaštena službena osoba tijela državne uprave sačinila u okvirima svojih nadležnosti za provođenje nadzora provedenog neposrednim opažanjem. U tim situacijama takve snimke mogu poslužiti kao dokaz u prekršajnom postupku, ali i tada sud može provjeravati njihovu vjerodostojnost te slobodno ocjenjivati njihovu dokaznu vrijednost." [19]

Što se tiče videonadzora u školama, postavljanje videokamera predstavlja važnu odluku za položaj radnika, jer se radi o mjeri u svezi sa sigurnošću na radu, o kojoj se poslodavac mora savjetovati s radničkim vijećem što je propisano [20] u odredbi čl. 149. st. 1. Zakona o radu. Prema Agenciji za zaštitu osobnih podataka, po pitanju videonadzora u školama [21], a na temelju odredbi Zakona o zaštiti osobnih podataka [22] članka 2. stavak 1. točka 1. razvidno je da video snimka dobivena video nadzornom kamerom predstavlja osobni podatak fizičke osobe – ispitanika. Člankom 9. [22] propisana je obveza informiranja ispitanika prije prikupljanja bilo kojih osobnih podataka. Dakle škole bi trebale "adekvatnim internim aktom regulirati uporabu istog (svrha, opseg tj. zahvat podataka koji se prikupljaju, način i vrijeme čuvanja te uporaba snimljenih podataka kao i zaštita prava ispitanika) a s činjenicom kojeg postavljanja bi na odgovarajući način pravovremeno trebalo upoznati učenike (roditelje) i zaposlenike." [21] Nadalje, "potrebno je ukazati da predmetni video nadzor (postavljen u svrhu sigurnosti) treba pokrivati samo zajedničke prostore škole (hodnike, ulazni prostor i sl.) kao i moguće dvorište škole (bez zahvaćanja u okolni javni prostor), dok nije prihvatljivo da video nadzorom budu pokrivena učionice, svlačionice i toaletni prostori. Također, kod uvođenja (postavljanja) video nadzora potrebno je uočljivo i nedvosmisleno označiti (slikom i tekstom) da je odnosni prostor pod video nadzorom, koja informacija mora biti pružena svim trećim osobama koje dolaze u školu, za



ostvarivanje spoznaje da ih se snima i na taj način prikupljaju njihovi osobni podaci." [22]

Škola može angažirati pravnu i fizičku osobu registriranu za obavljanje poslova tehničke zaštite, na način i pod uvjetima utvrđenim [23] Zakonom o privatnoj zaštiti koja će izraditi projektnu dokumentaciju prema Pravilniku o uvjetima i načinu provedbe tehničke zaštite [24] koji određuje tko ga smije postaviti i određuje uvjete, poput elaborata, održavanja. Na ovaj zadnji način je snimanje legalno.

#### B. Sigurnosne mjere za korisnike

Prema M. Baći [14] "najveća ranjivost svakog računalnog sustava i najveća prijetnja računalnom sustavu su ljudi koji s njim imaju vezu, kroz svakodnevni rad i kroz povremeno održavanje." Prema K. Rhodesu [25] zaposlenici u organizaciji imaju ključnu ulogu u prevenciji i detektiranju sigurnosnih incidenta. Dok su sistem administratori odgovorni za sigurnu konfiguraciju vatrozida i poslužitelja, korisnici su odgovorni za vježbanje sigurnosnih protumjera poput odabira i zaštite odgovarajućih lozinki. Stoga, za efektivnu sigurnost, korisnici moraju napraviti svjesne odluke da bi se pridržavali organizacijske sigurnosne politike i da bi prihvatili računalno sigurnosno ponašanje.

Nastavnik informatike često puta je jedina osoba koja u školi ima (dostatno?) znanje o računalima i računalnoj sigurnosti. Učitelji uglavnom koriste USB memorijske štapiće često zaražene virusima koji se šire na računalo u zbornici ili preko mreže, često jedni drugima "posuđuju" osobna korisnička imena i lozinke za prijavu na službene servise (npr. E-matica, CMS školskog web sjedišta), koje koriste na javnom računalu za koje se ne može uvijek pretpostaviti da je čisto od virusa i drugih malicioznih programa.

U novije vrijeme su učestali slučajevi da neki učenici pomoću aplikacije za udaljeni pristup računalu (npr. TeamViewer), u odsutnosti učitelja instaliraju aplikaciju, a kasnije se pomoću pametnog telefona spajaju na računalo te ga kontroliraju. Takva je nepodopština kažnjiva prema člancima 226. i 227. Kaznenog zakona [26] na što je 4.10.2013. reagiralo i ravnateljstvo policije RH poslavši dopis MZOS-u, a potonji prosljedio dopis svim osnovnim i srednjim školama te učeničkim domovima [27].

CARNet je temeljem dokumenta CDA0035 [2] točke 1. stavka 1. propisao: "Obveza je svake ustanove članice propisati sigurnosnu politiku na svojoj ustanovi...". Ustanova članica CARNeta ima obavezu izraditi sigurnosnu politiku te s njome upoznati svoje djelatnike i korisnike o dužnosti poznavanja i primjenjivanja iste. Do danas tek je nekolicina osnovnih škola izradila sigurnosnu politiku iako je trebala biti donesena još u rujnu 2006-te, odnosno šest mjeseci od dana spajanja u CARNet mrežu [2]. Provedba sigurnosnih mjera među korisnicima koji teško prihvaćaju promjene i ne shvaćaju opasnosti korištenja ICT-a teško je izvediva, no ovdje je riječ o visoko obrazovanim korisnicima i možemo reći da je žalosno što je tako.

#### IV. SIGURNOST INTERNET KOMUNIKACIJA U ŠKOLI

Internet je medij putem kojega korisnici žele komunicirati s osobama kojima vjeruju kao i onima kojima ne vjeruju, a isto vrijedi i za uređaje posredstvom kojih bi se ta komunikacija trebala odvijati. Na žalost ne postoji pouzdani način razlučivanja jednih od drugih. Kriptografija u koju se polagalo puno nade, nije uspjela iznaći pouzdane metode zaštite računala i korisnika od mreže u kojoj je četvrtina računala pod utjecajem bot mreža, a polovina e-maila neželjena pošta [28].

U školama uobičajen problem predstavlja nedozvoljeno posjećivanje društvenih mreža, stranica sumnjivog (ilegalnog) sadržaja, pa čak i stranica za odrasle. Doduše ako su računala spojena na Internet putem CARNetove mreže, ona imaju djelomičnu "zaštitu" od neželjenih i neprimjerenih sadržaja - "content filtering" baziran na CA eTrust Secure Content Manager content filter sustavu. O učinkovitosti ovog filtera bi se dalo raspravljati, jer ponekad blokira i sasvim legalne stranice i poveznice za preuzimanje legalnih programa, no zaštita se neprestano razvija i poboljšava. Još jedno rješenje za osnovno filtriranje sadržaja na internetu je projekt OpenDNS koji blokira sadržaje na DNS razini, a po potrebi se razina filtriranja može detaljnije konfigurirati. Konfiguriranje se vrši unutar postavki korisničkog računa, a osim već unaprijed definiranih kategorija po kojima se vrši filtriranje, moguće je dodavati svoje unose u listu dozvoljenih i zabranjenih domena.

Unutar škole bi bilo poželjno imati dvije (pod)mreže: jednu za učenike, a drugu za djelatnike. Na taj način rasterećujemo mrežni promet, a ako dođe do nekog sigurnosnog incidenta ili malicioznog programa koji se počne širiti jednom mrežom, druga će podmreža ostati netaknuta ukoliko mreže međusobno štitimo i filtriramo promet između njih. S 2011/2012. nastavnom godinom CARNet je krenuo u praktičnu realizaciju projekta e-dnevnik te preporuča prilikom planiranja bežičnih mreža dati učenicima mogućnost spajanja na nju. Projekt e-dnevnik je web aplikacija za vođenje razredne knjige u elektroničkom obliku, koji je iste godine uveden kao pilot projekt u tri srednje škole: XV. Gimnaziji u Zagrebu, Gimnaziji Požega i u Medicinskoj školi Ante Kuzmanića u Zadru. Dakle službena evidencija se vodi u aplikaciji, a nastavnici u razrede ulaze s tablet računalima putem kojih pristupaju aplikaciji. "E-dnevnik je izradio CARNet te ona ima sve funkcionalnosti postojeće razredne knjige, uz dodatne funkcionalnosti koje omogućava uporaba informacijsko-komunikacijskih tehnologija (ICT)." [29] Od školske godine 2013./2014. se za njegovo korištenje prijavilo preko 250 škola uključujući područne škole.

U Europskoj uniji se nastoji izglasati novi zakon pod imenom "Pravo na zaborav informacija". [30] Ukoliko to osoba zatraži, neugodni, netočni ili jednostavno osobni podaci morati će biti izbrisani s Interneta ili bilo kakvih baza podataka kompanija. Europska Komisija smatra da se pojedincu mora omogućiti da zatraži brisanje podataka o njoj/njemu, ukoliko ne postoje pravne prepreke za to. Također, pojedinac ima pravo da se njegovi podaci ne skladište u podatkovnim centrima te ne koriste za obradu, ukoliko to ne želi [30]. Nedavno je i bivši izvršni direktor Googlea Eric Schmidt izjavio: "Ovaj manjak gumba za brisanje na Internetu je u biti važno pitanje." [31] "Pravo

na zaborav" još nije doneseno kao dio EU prava niti je prošlo ili stavljeno u praksu. Ovaj zakon (ako bude donesen) će u praksi biti teško provesti. "Jednom kad se osobna informacija objavi, nemoguće ju je tehničkim mjerama spriječiti, ili čak promatrati/slijediti, stvaranje neautoriziranih kopija te informacije. U otvorenom sistemu kao što je Internet, pravo na zaborav se ne može ojačati samo tehničkim mjerama. Ojačanje mora polaziti na kombinaciji tehničkim i međunarodnih pravnih osiguranja." [32]

## V. ZAKLJUČAK

Nastavnici informatike u RH su de facto "sistem administratori u malom" koji svoj posao rade uglavnom volonterski, ali ponegdje/ponekad i prisilno (poštivanjem odluka ravnatelja), snose pravnu i moralnu odgovornost kako za ispravnost mreže tako i za računala. Njihova motivacija je u njihovom pozivu i osobnoj satisfakciji u onome što rade. Gotovo uvijek sami rješavaju različite probleme vezane za informatiku iz učionice ili zbornice. Educiraju svoje učenike i kolege i ukupno gledajući su u neravnopravnom položaju u odnosu na svoje kolege iz drugih predmeta. Na žalost tako će i ostati neko vrijeme u RH barem što se tiče situacije u osnovnoj školi. Jedan od mogućih smjerova u budućnosti (pod pretpostavkom još većih problema s financiranjem škola/opreme) jest da se problem održavanja prebaci na učenike, tako da učenici donose sami svoja prijenosna računala, tablete, fablete i pametne telefone pa ih i održavaju. (U Americi škole su već počele primjenjivati takav način rada poznat pod skraćenicom (BYOD - bring your own device) gdje učenici donose sami svoje uređaje no kako ne bi bilo još više problema (npr. zaražena računala) trebalo bi prije toga svakako educirati i učenike o sigurnosti računala. Jedan od preduvjeta takvom načinu rada jest pokrivenost Internetom u cijeloj školi, pa posebnu pažnju treba posvetiti konfiguraciji mreže. Slijedeće rješenje koje autori predlažu jest da se na razini općina ili županija odaberu (kvalifikacijskim ispitom ili formalnom potvrdom kvalificiranosti) osobe koje bi bile svojevrсни helpdesk za računala u školama. Nastavnici bi mogli preko on line obrazaca ispuniti kratki opis problema, a helpdesk bi uz pomoć telefona i/ili videokonferencije i spajanja na nastavnikovo računalo rješavao problem (ako kvar nije fizičke prirode ili ne zahtijeva intervenciju "in vivo"). Takvih osoba vjerojatno ne bi ni trebalo biti puno. U budućnosti bi se mogla provesti reorganizacija posla da osobama kojima nedostaju nastavni sati u školama dobiju dopunu do pune satnice na način da satnicu dopune radom u helpdesku. Moguća druga rješenja su zaključavanje postavki računala, virtualizacija ili brisanje promjena na računalu (npr. VHD ili sandbox tehnologijom).

## REFERENCES

- [1] Carnet, "Administratori škola," 02-Jan-2013. [Online]. Available: [http://www.carnet.hr/ustanove\\_clanice/administratori\\_skola](http://www.carnet.hr/ustanove_clanice/administratori_skola). [Accessed: 03-Dec-2012].
- [2] CARNet, "Odluka o prihvataljivom korištenju CARNet mreže," 15-Jun-2012. [Online]. Available: <ftp://ftp.carnet.hr/CARNet/docs/rules/CDA0035.pdf>. [Accessed: 14-Mar-2013].
- [3] Narodne novine, "Odluka o kriterijima i mjerilima za utvrđivanje bilančnih prava za financiranje minimalnog financijskog standarda

- javnih potreba osnovnog školstva u 2012. godini," NN 52/12. [Online]. Available: [http://narodne-novine.nn.hr/clanci/sluzbeni/2012\\_05\\_52\\_1276.html](http://narodne-novine.nn.hr/clanci/sluzbeni/2012_05_52_1276.html). [Accessed: 23-Dec-2013].
- [4] Vlada RH, "Odluka o otkazivanju Kolektivnog ugovora za zaposlenike u osnovnoškolskim ustanovama." [Online]. Available: <https://www.vlada.hr/hr/content/download/282525/4165491/file/134.%20-%202012.c.pdf>. [Accessed: 30-Dec-2013].
- [5] Narodne novine, "Pravilnik o stručnoj spremi i pedagoško-psihološkom obrazovanju nastavnika u srednjem školstvu," 1996. [Online]. Available: <http://narodne-novine.nn.hr/clanci/sluzbeni/263720.html>. [Accessed: 23-Oct-2013].
- [6] Ministarstvo za školstvo in šport, "Pravilnik o normativih in standardih za izvajanje programa osnovne šole," 09-Jan-2007. [Online]. Available: [http://www.mizks.gov.si/fileadmin/mizks.gov.si/pageuploads/zakonodaja/pdf/OS/Pravilnik\\_normativi\\_OS\\_7\\_5\\_07.pdf](http://www.mizks.gov.si/fileadmin/mizks.gov.si/pageuploads/zakonodaja/pdf/OS/Pravilnik_normativi_OS_7_5_07.pdf). [Accessed: 20-Mar-2013].
- [7] Doug Johnson (Director of Libraries and Technology for the Mankato (MN) Public Schools), "School administrators", poruka elektroničke pošte, 18-Sep-2013.
- [8] Eric Rusten, Josh Woodard, "Enabling, Accelerating & Sustaining Quality Education," 2011. [Online]. Available: [http://siteresources.worldbank.org/EDUCATION/Resources/278200-1099079877269/547664-1099079956815/547670-1128086743752/BBL\\_4\\_4\\_2011\\_AED.pdf](http://siteresources.worldbank.org/EDUCATION/Resources/278200-1099079877269/547664-1099079956815/547670-1128086743752/BBL_4_4_2011_AED.pdf). [Accessed: 12-Mar-2013].
- [9] CARNet, "Ict edu," 20-May-2013. [Online]. Available: [http://www.carnet.hr/ictedu/o\\_projektu](http://www.carnet.hr/ictedu/o_projektu). [Accessed: 28-Mar-2013].
- [10] "Centar za sigurniji Internet," 2013. [Online]. Available: <http://www.sigurnijiinternet.hr/>. [Accessed: 28-Jun-2013].
- [11] Insafe, "Safer Internet Day," 22-Oct-2013. [Online]. Available: <http://www.saferinternet.org/safer-internet-day>. [Accessed: 30-Jun-2013].
- [12] "CERT," 2013. [Online]. Available: <http://www.cert.hr/>. [Accessed: 28-Jun-2013].
- [13] Darko Rakić, "Projekt 'Sigurnost djece na internetu' za edukaciju i prevenciju elektroničkog nasilja," Sigurnih pet za sigurniji net, 25-Oct-2013. [Online]. Available: <http://www.petzanet.hr/Blog/ArticleID/7>. [Accessed: 12-Jan-2014].
- [14] Miroslav Bača, Uvod u računalnu sigurnost. Narodne novine, 2004.
- [15] Ksenija Klasić, "Zaštita informacijskih sustava u poslovnoj praksi," Sigurnost, vol. 49., no. 1, 2007.
- [16] Neil Mohr, "How to set up a webcam security system," PC Plus, 17-Nov-2012. [Online]. Available: <http://www.techradar.com/news/computing/how-to-set-up-a-webcam-security-system-1112863>. [Accessed: 10-Mar-2013].
- [17] Franjo Podhraški, Stjepan Tršinski, Krešo Kancir, "Prijedlog unapređenja rada policije uvođenjem videonadzora javnih prostora," Policija i sigurnost, vol. 17., no. 3-4., 2009.
- [18] Narodne novine, "Zakon o kaznenom postupku," 01-Jan-2013. [Online]. Available: <http://www.zakon.hr/z/174/Zakon-o-kaznenom-postupku>. [Accessed: 28-Jun-2013].
- [19] Vlada RH, "Prijedlog zakona o prekršajima protiv javnog reda i mira," listopad-2012. [Online]. Available: [www.sabor.hr/fgs.axd?id=21935](http://www.sabor.hr/fgs.axd?id=21935). [Accessed: 21-May-2013].
- [20] Narodne novine, "Zakon o radu," 2013. [Online]. Available: <http://www.zakon.hr/z/307/>. [Accessed: 21-May-2013].
- [21] Agencija za zaštitu osobnih podataka, "Videonadzor u školi," 2013. [Online]. Available: <http://www.azop.hr/news.aspx?newsID=229&pageID=25>. [Accessed: 21-May-2013].
- [22] Narodne novine, "Zakon o zaštiti osobnih podataka," NN, 2012. [Online]. Available: <http://www.zakon.hr/z/220/Zakon-o-za%C5%A1titi-osobnih-podataka>.
- [23] Narodne novine, "Zakon o privatnoj zaštiti," 2010. [Online]. Available: <http://www.zakon.hr/z/291/Zakon-o-privatnoj-za%C5%A1titi>. [Accessed: 28-Jun-2013].

- [24] Ministarstvo unutarnjih poslova (MUP), "Pravilnik o uvjetima i načinu provedbe tehničke zaštite," 05-Sep-2013. [Online]. Available: [http://www.mup.hr/UserDocsImages/SAVJETOVANJE/2013/zozni/PRAVILNIK\\_O\\_TEH\\_ZASTITI\\_.pdf](http://www.mup.hr/UserDocsImages/SAVJETOVANJE/2013/zozni/PRAVILNIK_O_TEH_ZASTITI_.pdf). [Accessed: 30-Dec-2013].
- [25] K. Rhodes, "Operations security awareness: the mind has no firewall," *Computer Security Journal* 18 (3), 2001.
- [26] Narodne novine, "Kazneni zakon," 01-Jan-2013. [Online]. Available: <http://www.zakon.hr/z/98/>. [Accessed: 09-Oct-2013].
- [27] Ravnateljstvo policije, "Neovlašteni pristup računalnim sustavima," 30-Sep-2013. [Online]. Available: [http://os-barilovic.skole.hr/upload/os-barilovic/newsattach/793/neovlasteni\\_pristup\\_racunanim\\_sustavima.pdf](http://os-barilovic.skole.hr/upload/os-barilovic/newsattach/793/neovlasteni_pristup_racunanim_sustavima.pdf). [Accessed: 14-Dec-2013].
- [28] Diffie W., "Information security: 50 years behind 50 years ahead," *Communications of the ACM*, vol. 51, no. 1, pp. 55–57, 2008.
- [29] CARNet, "E-dnevnik," 19-Mar-2013. [Online]. Available: <http://www.carnet.hr/e-dnevnik>. [Accessed: 30-Jun-2013].
- [30] Viviane Reding, Vice President of the European Commission, "The EU Data Protection Reform 2012: Making Europe the Standard Setter for Modern Data Protection Rules in the Digital Age 5," 22-Jan-2012. [Online]. Available: <http://europa.eu/rapid/pressReleasesAction.do?reference=SPEECH/12/26&format=PDF>. [Accessed: 28-Mar-2013].
- [31] Leonard N. Stern School of Business, "Eric Schmidt intervju," 2013. [Online]. Available: <http://www.stern.nyu.edu/experience-stern/news-events/google-schmidt-cohen>. [Accessed: 28-Jun-2013].
- [32] Druschel P., Backes M., Tirtza R., "The right to be forgotten-between expectations and practice," European Network and Information Security Agency (ENISA), 18-Oct-2011. [Online]. Available: [http://www.enisa.europa.eu/activities/identity-and-trust/library/deliverables/the-right-to-be-forgotten/at\\_download/fullReport](http://www.enisa.europa.eu/activities/identity-and-trust/library/deliverables/the-right-to-be-forgotten/at_download/fullReport). [Accessed: 12-Sep-2013].