Programski odbor simpozija / Programme Committee

Mario Dumančić
Vatroslav Zovko
Predrag Oreški
Jože Rugelj

ISBN: 978-953-7210-83-0

CIP zapis je dostupan u računalnome katalogu Nacionalne i sveučilišne knjižnice u Zagrebu pod brojem 000903536.

Autori snose svu odgovornost za sadržaj i jezičnu kvalitetu radova. Nadalje, izjave i stavovi izraženi u radovima isključivo su stavovi autora i ne moraju nužno predstavljati mišljenja i stavove Uredništva i izdavača.

The authors are solely responsible for the content and the language of the contributions. Furthermore, statements and views expressed in the contributions are those of the authors and do not necessarily represent those of the Editorial Board and the publisher.
# Contents / Sadržaj

Jozef Bushati, Shkelqim Kuka, Kozeta Sevrani and Ardiana Sula  
*Original research paper / Izvorni znanstveni rad*  
Integration of the GIS/GPS technologies in the pre-university education  
O uvrštavanju koncepta GIS/GPS tehnologije u predsveučilišnom obrazovanju  

Krešo Tomljenović and Vatroslav Zovko  
*Izvorni znanstveni rad / Original research paper*  
Primjena informacijsko komunikacijske tehnologije u nastavi matematike – komparativna analiza uspjeha učenika 7. razreda osnovne škole  
The use of ICT in teaching mathematics - comparative analysis of the success of 7th grade primary school students  

Vatroslav Zovko, Ana Didović and Maja Matijaš  
*Original research paper / Izvorni znanstveni rad*  
ICT enabled education – need for paradigm shift  
Nužnost promjene paradigme obrazovanja podržanog informacijsko komunikacijskim tehnologijama  

Ivana Jurakić i Renata Marinković Kravica  
*Prethodno priopćenje / Preliminary communication*  
Informacijsko-komunikacijske tehnologije kao čimbenik odgojno-obrazovnog rada u suvremenim vrtićima  
IT and communications technologies as a factor in education and upbringing in contemporary kindergartens  

Suzana Tomaš i Snježana Dobrota  
*Prethodno priopćenje / Preliminary communication*  
Oblikovanje glazbene priče Peća i Vuk u sustavu e-učenja Moodle  
Instructional design of the music story Peter and the Wolf in the Moodle e-learning system  

Florenc Vavla, Lynn Zimmerman and Vilma Tafani  
*Preliminary communication / Prethodno priopćenje*  
Mind the gap: Technology and teacher training issues  
Pazi razmak: Pitanja tehnologije i obrazovanja nastavnika
<table>
<thead>
<tr>
<th>Author(s)</th>
<th>Title</th>
<th>Type</th>
<th>Pages</th>
</tr>
</thead>
<tbody>
<tr>
<td>Elona Hasmujaj</td>
<td>Online games addiction: the psychological consequences at the teenagers</td>
<td>Review paper / Pregledni rad</td>
<td>62</td>
</tr>
<tr>
<td>Željko Knok, Ana Didović i Nenad Breslauer</td>
<td>Intelligent systems in education</td>
<td>Pregledni rad / Review paper</td>
<td>69</td>
</tr>
<tr>
<td>Kristina Kopričanec</td>
<td>Homo, but not Sapiens - A new kind of kids</td>
<td>Pregledni rad / Review paper</td>
<td>77</td>
</tr>
<tr>
<td>Sonja Petrovska, Despina Sivevska, Biljana Popeska and Jadranka Runceva</td>
<td>Application of ICT in teaching in secondary schools in the Republic of Macedonia</td>
<td>Review paper / Pregledni rad</td>
<td>87</td>
</tr>
<tr>
<td>Tedo Vrbaneč</td>
<td>The Discrepancy Between the Need and the Inclusion of Education on Information Security in Croatian Elementary Education System</td>
<td>Review paper / Pregledni rad</td>
<td>97</td>
</tr>
<tr>
<td>Marija Ajša Peuc</td>
<td>ICT capabilities in the classroom</td>
<td>Stručni rad / Professional paper</td>
<td>114</td>
</tr>
<tr>
<td>Tomislav Težak</td>
<td>Tablet as a form of e-notebook in primary education teaching</td>
<td>Stručni rad / Professional paper</td>
<td>124</td>
</tr>
<tr>
<td>Bujane Topalli</td>
<td>Teen’s social networking and ethic education</td>
<td>Professional paper / Stručni rad</td>
<td>139</td>
</tr>
</tbody>
</table>
The Discrepancy Between the Need and the Inclusion of Education on Information Security in Croatian Elementary Education System
Tedo Vrbanec
Department of information sciences, The Faculty of Teacher Education University of Zagreb

Abstract
A multitude of laws, regulations, ordinances and decisions (directly or indirectly) determine or prescribe the elementary school curriculum in Croatia. The paper summarizes, aggregates and presents them in the most possible understandable and meaningful way, which is not easy due to their complex, interwoven character. It also determines how the prescribed IT curriculum, the educational goals and objectives include the domain of information security. The author analyses the content of the prescribed IT literature and its compliance with the prescribed IT curriculum, discusses the findings - identifies problems, proposes solutions and raises some new questions. The author argues that the topics of information and communication security, methods, procedures and measures for the protection of users, protection of user data, computers and computer networks, are both de facto and de jure ignored by formal primary education in Croatia.

Key words: compsec; education privacy; infosec; data protection

Introduction
In order to avoid possible different interpretations, we will adopt common definitions of several concepts. “Computer security is a combination of confidentiality, integrity and availability of computer systems and data storage” (Glavor, 2009a, p. 3). Communication security “refers to the security of any information that is transmitted, transferred or communicated” (Janssen, 2014). It includes integrity and confidentiality of data during transmission through communication channel and ensuring secure communications. Data protection, sometimes also called file security, indicates that the user data are an important object of protection and prevention of unauthorized (accidental or intentional) modification, loss, accidental damage or unauthorized access and disclosure of data. User’s privacy indicates that the user can knowingly and independently decide whether they will entrust personal, possibly sensitive data, to whom, why and under what conditions. User’s privacy implies that the user may at any time withdraw some rights.

The author considers that the topics of information and communication security, methods, procedures and measures for user’s protection, protection of user data, computers and computer networks, are both de facto and de jure ignored by formal primary education in Croatia. Although this hypothesis could be extended to all levels of education, this review is limited to the domain of primary education. The reasons for this limitation are logical and semantic:

- Working habits, models of thinking and human responsibility are creating and developing from the earliest age.
- At the higher level of education, students should be educated further into information security (infosec) and their knowledge about security topics should be updated due to fast emergence of new security issues and threats.

The school subject named Informatics (in Croatia), which covers a wide range of topics from Computer Science (in the USA) seems to be a natural place to educate students about infosec. From Grade One to Grade Four, Informatics in Croatia is only an extracurricular school activity, with a time schedule of one hour a week. From Grade Five to Grade Eight, (Croatian primary schools lasts eight years), Informatics is an optional school subject with a two hours week schedule. So, in Croatian primary education, Informatics is still not an obligatory subject.
and therefore has an awkward position: its status depends (a) on the school capabilities in the form of equipment and personnel and (b) students (whether they want to choose it). Consequently, students can finish their primary education without any formal computer training, including about information security.

Given optional nature of Informatics, it is questionable whether that school subject can seriously be considered as a channel and mediator of infosec training: if IT teachers want to fulfill their lecture norms and keep their current job, they cannot be as demanding to students as they are supposed to be. In practice, IT teachers are not able to implement the existing curriculum, because it has been made in expectation that Informatics will become a mandatory school subject.

In Croatian primary school most teachers are in charge of one class of students (usually 15-25). They are called main class teachers. They spend one school hour with them discussing current problems or dealing with general education topics, e.g. civic education and health education. IT security education could be done during these classes, as it has recently been realized with health education. But then a new problem emerges – the competence and willingness of educators – main class teachers. They are class teachers in Grades One to Four, teaching all the core subjects or subject teachers in Grades Five to Eight teaching only one or two subjects they are qualified for. In the absence of qualified IT teachers they should carry education about infosec. But (Bakić-Tomić & Dumančić, 2009, p. 5) “being an expert in one area means knowing all the mistakes and weaknesses of the area. Experience brings wisdom and if teachers and professors today want to use new technology to transfer knowledge to their students then they must become familiar with these technologies.” In addition to the lack of knowledge about infosec by the teachers themselves, it is questionable whether there is any time left in that one hour per week.

**Global experiences**

In the USA there are three government organizations who are the main stake-holders in the effort to improve the level of training students in information security. These are National Initiative for Cybersecurity Education (NICE), National Cyber Security Alliance (NCSA) and Multi-State Information Sharing and Analysis Center (MS-ISAC). NICE specifically aims to help users stay safe while they are online. The initiative puts the emphasis of its work on education so that (McDuffie, 2012) the general population can be prepared in the sense that it can identify and avoid risks in cyberspace. MS-ISAC is an organization whose mission is to improve the state of cyber security of the American states, territories, district, and local governments. NCSA is an organization whose mission is to nurture a digital society by educating people for the safe Internet usage at work, at home and at school. Teaching materials are fully available online in pdf format and include Plans, Programmes and an e-picture book.

The Australian Government has established the Australian National Educational Program About Cybersafety and Cybersecurity Called Cybersmart (Cybersmart.gov.au, 2012), managed by the Australian Communications and Media Authority (ACMA), with the aim of improving the state of cyber security. Cybersmart aims to inform children, youth, parents, teachers and library staff on issues of cyber security, educate the public through information, resources and practical advice and to enable children and young people to be safe on the Internet.

In 2004 the European Union launched a complex programme “Safer Internet” (European Commission, 2004), which is comparable to those in Australia and the USA and is indeed much richer, but the EU has not done much in terms of introducing education about information security in education programmes. The European documents, one of the key competences for lifelong learning (European Parliament, 2007), and the other on key competences in European education (European Commission, EACEA, & Eurydice, 2012), does not include topics of information security. Members of the EU Parliament (MEP) vote periodically on resolutions related to information security (European Parliament, 2012a, 2012b; European Parliament - The Committee on Culture and Education, 2012; HRT, 2012), such as seeking better protection for children online. The Parliament supports the adoption of technologies such as tools for parental control and age
verification system designed to prevent child access to content unsuitable for their age. Thus, fighting against security threats, the EU is moving in the direction of repression and technological solutions for the protection and containment. At the same time, at the supranational level, the EU has no mandatory educational programs that include topics of information security. At the EU level there is no systematic approach to the inclusion of information security topics in the formal education system. European Commission survey (European Schoolnet & University of Liege, 2013) that does not examine the issue of information security. This indicates that the EU is not sufficiently aware of information security issues. On the other hand, the EU has an agency established in 2004 (European Network and Information Security Agency - ENISA), whose main task is (Helmbrecht, 2015) “cyber security issues of the European Union”. In its report (Marinos & Psarras, 2011, p. 8), ENISA provides summaries of problems in the domain of network information security in order to “provide concise information from ENISA work that can be easily integrated into existing educational material”. In addition to ENISA, the EU has a number of other projects, papers, reports and discussions which are raising awareness on the topic of information security, especially among young people, and targeting mostly school children, their parents and the education system, like (European Commission, 2011; ITU - International Telecommunication Union, 2011; Livingstone, Haddon, Görzig, & Ölafrsson, 2012; The Economist, 2011).

In EU, Czech Republic is an example of the implementation of information security education. University teachers have lectures in the domain of information security to teachers in primary and secondary schools (who pass on that knowledge to their students), in the form of supplementary education (Beranek, 2009). Upon completion of this training, teachers evaluate education in which they have participated and provide feedback to their university teachers who can modify future lectures if necessary. The lectures are organized in the form of modules:

- General questions about information security.
- Principles of computer security.
- Security projects.
- Trust on the Internet.
- Information security policies.

Education on Information Security in China is not done in an organized manner, it is not supported by the programmes and plans, but rather depends on the level of education and awareness of the teachers (AiJun & Yu, 2012; Lindsay, 2012). Situation is very similar in India, Africa (Dlamini, Taute, & Radebe, 2011) and most other countries of the world. Everywhere exists a certain level of awareness of the need for the inclusion of infosec in the educational system, but rarely anything beyond this.

South Korea is a shining example of the state in which the information security has become part of the formal primary education system (Abele-Wigert, 2006) included in the education of computer literacy.

**Related works**

The author thinks that it is a high time for the questions and issues of ICT security to be moved from media and professional debates into the educational programmes. There are two groups of opinions. The first group are those who advocate the urgency of educating adults already involved in the life of society. The second group prefers the education of children and young people, as they are already part of the educational process and because they can easier and faster acquire new knowledge and skills.

In his article (Fraser, 2012), J. Fraser argues that the security issues should be moved from the academic and technological circles into the civil society, i.e. he advocates the need of the attention to be finally paid to information security so that it should be properly treated and acted upon.

K. Townsend believes that the user is the weakest link (Townsend, 2011) in human-technology-communication system and that all attacks depend entirely on human involvement. The
article includes the most common mistakes that users make and which threaten safety and security of the organization to which they belong to.

B. Radic stresses the need for education and prevention (Radić, 2012). The work presents the sources of computer threats, ways of the arrival of malignant code to computers and forms of fraud.

Study written by R. Anderson et al (Anderson et al., 2012, p. 1) which claim to be “the first systematic study of the costs of computer crime”, was made at the request of the UK Government, but it also presents the global data. The study concludes that the overall damage done by cybercriminals is far greater than the sum of all their personal benefits. For example, the 2010 botnet that was responsible for a third of spam earned their owners $2.7 million, while the costs of activities to prevent spam were estimated to have been one billion dollars. Furthermore, the direct and indirect costs in the world are measured in billions of dollars, and the total costs of protection are several orders of magnitude greater than the costs of damage.

According to Croatian CERT (Načionalni CERT, 2009, p. 18) “the human factor is the cause of many incidents, but our ability to learn and change their behavior represents the area with the greatest potential for development and progress of the global computer security.” In another document (CARNET CERT & LS&S, 2005a, p. 4) CERT states that “it is a widely known fact” that “the organization’s human resources are one of the biggest threats to information security”, and it confirms it with the data that “nearly 75% of security incidents come from the internal users”.

N. Ruzic argues (Ružić, 2011, p. 1) that the Internet is technically impossible to control. Therefore, the “Internet requires strict restrictions”. Furthermore, Ruzic believes that it is particularly important to protect children, because “no one on the Internet is protected from cyber-theft, cyber-violence and cyber-porn. And while adults are responsible for their own recklessness, the effects on children can be catastrophic because only a small number of children use the Internet for the education. Therefore, it is necessary to protect the youngest population through legislation, but parents must supervise their children’s usage of the Internet”.

Zhang and Wang (Aijun & Yu, 2012) advocate that the education on ICT security issues must be included into existing training programs of education in information literacy for students. The article presents the results of the research done in China with 1200 participants, where over 91% of the students thought the use of ICT in teaching to be very positive. The paper presents many interesting statistics from China and the world that support the view that the situation in terms of information security is very bad and getting worse. The authors advocates that it is really essential that students are educated to be aware of the network and security problems and they regret that there is no organized training on infosec in China.

Based on the results of his own research in the Middle East (UAE, Bahrain, Qatar) (Aloul, 2010), F. A. Aloul also concludes that it is necessary to introduce training programs in information security for all age groups and to raise the level of awareness of governments and private organizations.

Dlamini, Taute and Radebe (Dlamini et al., 2011) deal with the condition of information security on the African continent, especially its south. There is no organized security policy of countries, groups of countries or of the entire continent. The authors propose Conceptual Framework for African Cyber Security Policy and call for the introduction of education about cyber security from the first grade of formal education.

**Domains, objectives and methodology**

We shall take a brief look at the Croatian education system. According to the MSES (MZOS, 2012b) the education system consists of pre-school education, primary education, secondary education, higher education and lifelong learning or adult education, which MSES schematically showed in Fig. 1.
Infosec topics are important and are becoming even more important every year. Therefore, it is necessary that education system acts preventively - to educate children as early as possible. Preschool education is beyond the scope of this paper, and the trivial reason is that children are barely using ICT at that age, and if they do, it should be under the supervision and instruction of adults.

Primary education is just the right time for the required educational activities, because at this age children begin to use ICT through all types of devices, such as desktops, laptops, tablets, phablets, smartphones, media centers, iPods, smart TVs, etc. Simultaneously, children begin to explore the Internet and to use Internet services. Their full supervision is impossible due to the high availability of ICT devices and the Internet. Furthermore, at this age children become more and more independent. It is quite possible that they might enter various dangerous situations, relationships and communication, out of ignorance and naivety. It is questionable whether parents are aware and educated enough to take on self the task of educating their children in security and safety issues associated with the usage of ICT.

As it has already been indicated, the focus of this paper are themes, programs, activities, literature and regulations associated with all security related issues of using ICT at the primary level of education in the Republic of Croatia. In this context, the aims of this review are the following:

1. To identify and collect all documents and regulations which define and have influence on school subjects in elementary education and associated curriculum in general and for them to set aside all those which have any impact on the teaching of the school subject Informatics and to determine their interconnection and interdependence.
2. To identify and physically collect all IT literature required in primary education e.g. to determine which official lists of textbooks and additional teaching resources are currently valid and relevant and to collect that IT literature for further processing.
3. To determine the extent to which the curriculum of computer, communications and data security are already present in the existing IT curriculum and prescribed primary education literature.
4. To examine the compliance of prescribed IT literature and curriculum.
To achieve these goals, the following methodological steps were performed:

1. Given that required documents and regulations are publicly available, web mining has been used to find all documents that formally affect curriculum and those that have been implemented in the elementary school.

2. These documents, as well as objects and events that are defined and regulated through them, were analysed both causally and structurally. Synthesis, with the help of mind mapping tools, was used to cover their role in the overall primary educational system. Documents that deal exclusively with organizational issues of primary education system, were rejected as irrelevant (in order not to lose focus of research).

3. Content analysis was used reading the entire set of documents twice (the first time for selection and familiarization with the content, and the second time the relevant documents were studied in detail). Links and conditioning between documents have been identified and shown graphically by Fig. 2. It was indispensable for comprehension of the entire system and its complexity.

4. All prescribed IT literature (28 pairs of textbooks and workbooks) were read carefully, searching for topics in information security. There are three sets (textbook + workbook) for lower grades (1-4) and four sets for upper grades (5-8). The same analysis was performed with the curriculum documents.

The authors believe that this article has laid the necessary foundation for research on the state of computing, communications and data security for primary school children in Croatia.

Results

The results have been obtained by the research of official documents, prescribed literature and other sources, so they will be considered in the following subchapters.

Official documents

Official documents in the primary education system that influence the content of the curriculum are:

- Law on Education in Primary and Secondary Schools (NN 87/08, 86/09, 92/10, 105/10, 90/11, 5/12, 16/12) (Zakon.hr, 2012),
- Law on Elementary and Secondary School Textbooks (NN 27/10, 55/11) (Zakon.hr, 2010),
- Curriculum (so called HNOS) (MZOS, 2006i),
- Textbook Standards (MZOS, 2006j),
- Regulations on Mandatory Textbooks and Related Supplementary Teaching Materials (MZOS, 2010c),
- Rules of Procedure For the Approval and Use of Additional Teaching Resources For Teaching Subjects in Primary Schools, Secondary Schools and General Education Courses (AOO, 2010),
- List of Textbooks and Related Supplementary Teaching Materials (MZOS, 2010b),
- Catalogue of Compulsory Textbooks and Related Supplementary Teaching Materials (MZOS, 2012a),
- The Final List of Selected Textbooks and Related Supplementary Teaching Materials (MZOS, 2010a),
- List of Approved Additional Teaching Resources (AOO, 2011),
- State Educational Standard for Elementary Education (Hrvatski sabor, 2008),
- Annual school plans and programmes,
- Informatics curricula,
- School curriculum,
- School statutes.
The existence of documents and the connections between them is shown in Fig. 2 - diagram of entities (documents) and relations between them.

Central place in the system belongs to The Law on Education in Primary and Secondary Schools, which is highlighted in Fig. 2. Connections are defined by three parameters: direction, orientation, and a brief description of the influence. What has been indicated by the previous list of documents, now can be easily seen from the analysis presented in Fig. 2 - it illustrates and proves that the Croatian elementary education system seem to be extremely complex.

It is obvious that there is space for simplification and optimization. Such a complex system needs to be carefully disassembled and reestablished, as all large systems tend to be sluggish and inert, and it is common that any change causes resistance that is proportional to the system size and intensity of changes.

Figure 2. Diagram of Interwoven Character and Interdependence of Official Documents

Officially prescribed literature
This section provides an overview of information security topics in the current literature prescribed in Croatian primary education as well as in documents that form the HNOS.

Information technology as a subject in Croatian primary education system exists as an extracurricular activity in Grades One to Four and as an optional subject in Grades Five to Eight. As for all other school subjects, the Ministry prescribes a range of literature that can be used, and can legally transfer that part of the authority to the Agency for Education and the Agency for Vocational Education. The current literature at the primary level of education is prescribed by three documents - two passed by MSES and one by the Agency for Education:

- List of Approved Additional Teaching Resources issued by the Agency for Education. The list for school year 2011/2012 (AOO, 2011) does not include literature for the subject Informatics, except the collection of test questions from Grade Five to Eight. New list for 2013/2014 does contain it.
• List of Textbooks and Related Supplementary Teaching Resources for Primary School 2013-2014 (MZOS, 2014) contains a number of competing titles of Informatics unlike the year before, when there was no officially prescribed literature. However, teachers were still working as they used to work years before, that is, they have their own copies of textbooks and curricula on which the “lost” textbooks are based (MZOS, 2010b). This paper in its analysis uses the outdated list as a reference for the first four grades of elementary school, because a new one is not yet available.

According to the list of titles of the two still official documents (the third contains no literature in computer science), the author of this paper has managed to extract topics about information, computer, communications and data security therein. A comparison was made with the curriculum for each grade as a separate HNOS document (MZOS, 2006a, 2006b, 2006c, 2006d, 2006e, 2006f, 2006g, 2006h) and the NOK (MZOS, 2011). Several other documents are consulted (Budin, 2006a, 2006b, 2006c, 2006d, 2006e; Kniewald, 2006; Stankov, 2006), which together make up HNOS: “Education in the Field of ICT in Primary School” (Budin, 2006a), “Appendix A: Methodological Notes for Program Units Making Presentations and Troubleshooting Programming” (Kniewald, 2006), “Appendix B: Background for Detailed Methodical Elaboration of Some Topics” (Budin, 2006d), and “Foundations for the Development of Standards” (Budin, 2006b). These annexes do not address security issues.

The results of the content analysis are summarized in Table 1 and Fig. 3.

<table>
<thead>
<tr>
<th>Source</th>
<th>1</th>
<th>2</th>
<th>3</th>
<th>4</th>
<th>5</th>
<th>6</th>
<th>7</th>
<th>8</th>
</tr>
</thead>
<tbody>
<tr>
<td>Textbook</td>
<td>2</td>
<td>0</td>
<td>3</td>
<td>15</td>
<td>29</td>
<td>49</td>
<td>5</td>
<td>15</td>
</tr>
<tr>
<td>Workbook</td>
<td>0</td>
<td>0</td>
<td>1</td>
<td>7</td>
<td>1</td>
<td>5</td>
<td>0</td>
<td>6</td>
</tr>
<tr>
<td>HNOS Curriculum</td>
<td>0</td>
<td>0</td>
<td>1</td>
<td>2</td>
<td>0</td>
<td>1</td>
<td>0</td>
<td>0</td>
</tr>
</tbody>
</table>

Table 1

<table>
<thead>
<tr>
<th>Grade</th>
<th>Number of Info-Security Topics</th>
</tr>
</thead>
<tbody>
<tr>
<td>One</td>
<td>2 0 0 0 3 1 1 15</td>
</tr>
<tr>
<td>Two</td>
<td>6 0 0 0 7 2 20</td>
</tr>
<tr>
<td>Three</td>
<td>5 1 0 1 5 5 1 49</td>
</tr>
<tr>
<td>Four</td>
<td>3 1 0 0 1 0 1 15</td>
</tr>
</tbody>
</table>

Figure 3. Involvement of Info-Security Topics in Curriculum and in Prescribed Literature

Data from Table 1 and the corresponding graph in Figure 3, offers two conclusions.

1. Topics relating to computer, data and communications security are ignored by the HNOS. That is explicitly evident in the number of topics that curriculum includes.
2. A substantial number of topics in the textbooks and workbooks leads to the conclusion that the authors are aware of the need for teaching students about infosec. However,
there is a large disparity between the number of topics per grade (and individual books / authors for the same grade), and between the distribution of the number of these topics from textbooks and workbooks.

It was shown that the existing HNOS curriculum and NOK has insufficient contents and topics related to ICT security. The existing curriculum does not have the required minimum coverage of information security. The subject matter present in the existing literature has a minimum of the required security features. However, their uneven distribution between school years (grades) and within them, has a negative influence on the final acquisition of knowledge. Given the dynamics of changes in ICT, the current textbooks and workbooks are increasingly outdated.

Supplementary literature and resources

In addition to the prescribed, there is supplementary literature, which includes resources that have some significance and impact on the quality of teaching. That significance is reflected in the correct methodological background that is necessary for teachers. Teachers must properly implement education (methodical approach and other tutorials can help them in this task). Teachers of informatics must continually improve their IT competence, including the competence related to infosec.

Methodological manuals for teachers

Methodical and other manuals are part of the optional literature and are intended solely for teachers. It is logical to assume that the teacher (of Informatics) reads a few methodical manuals before entering the classroom. Therefore, teacher manuals deserve our attention. Unlike the prescribed literature in which there are multiple titles for each class, the teacher’s manual has a much smaller number. There are two manuals for Grade One (Silvano, Sanja, & Neven, 2003; Žezlić & Šrdić, 2000) (which does not include topics from the safety of the use of ICT) and methodical manuals for Grades Five to Eight by a group of authors (V. Galešev, Glavan, Kniewald, & Sokol, 2004; Vinkoslav Galešev, Kniewald, Kralj, & Sokol, 2004; Vinkoslav Galešev, Kralj, Kniewald, & Sokol, 2005; Kralj, Kniewald, Sokol, Galešev, & Glavan, 2005) The beginning of each manual for each year covers the theme “protection from viruses and spam”, which provides 14 tips to teachers regarding protection against malicious software.

Literature for students

A small group of titles is intended for future primary and secondary school teachers of Informatics (Computer Science). Here are two prominent titles. The first is a course-book published by The Faculty of Teacher Education (University of Zagreb) (Bakić-Tomić & Dumančić, 2009) targeting university students - future teachers, to assist them in overcoming the methodological issues of using computers in the education of children and the education and self-education of teachers. The course-book successfully examines many aspects of the use of ICT in the field of education, especially in the context of teacher education, which is the first official contact of children with the education system. Completeness and comprehensiveness of its information security contents is neither its purpose nor need. Yet, despite this, the course-book has a lot of content covering that subject material.

The second title is a book (Bača, 2004) that is “made for the course dealing with the study of computer security” at the Faculty of Organization and Informatics (University of Zagreb). Therefore it covers a very broad topic of computer security and crime related to computer security.

Although small in number, there are other titles, for instance (Klasić, 2002), however, further expanding literature would not bring new subjects important for the education of children, their current and future teachers, i.e. the elements of the two titles represent the minimal set of titles that would include all the topics that would be included even by a potentially larger set of titles.
Brochures and manuals

Almost all schools in Croatia are members of the Croatian Academic and Research Network (CARNet). In 1996 CARNet center for computer security has been established, called a CARNet CERT, with the aim of (CARNet, 2011), “the collection of data on computer security incidents and their solving cooperating with relevant institutions in the Republic of Croatia, and raising awareness of the importance of computer security in general.” CARNet declares that the school is responsible for its safety and that it is also responsible for the safety of CARNet that it is connected to, because by using “computers in the network it is possible to commit a crime, cause considerable financial damage and endanger other users” (Glavor, 2009a, f. 3). Decisions about the appropriate use of CARNet from 2006 (CARNet, 2006, p. 1) declare: “In the case of a computer security incident, it is necessary to be able to identify the perpetrators.” Unfortunately, the same document does not define who is responsible for training and teaching users what is considered to be allowed and acceptable behavior on the Internet. CARNet requires that each member institution is responsible for defining its own security policy. To facilitate the procedure, CARNet offers its members template to create security policies (CARNet & Dimitrovic, 2003).

For the context of this work a particularly important position is that of CARNet CERT (Glavor, 2009b), which argues that it is necessary to find a systematic way of introducing computer security in formal education as well as to educate the teachers themselves (not necessarily only those who teach Informatics).

Besides CARNet CERT, in Croatia exists the National CERT. However, in early 2013, the National CERT took over the duties of CARNet CERT (Nacionalni CERT, 2013). It can be said that these two CERTs have at least functionally merged. In 2010 the two CERTs published a brochure (Štifić & Čamagajevac, 2010) “Safer Internet” which tends to disseminate knowledge required for the safe use of new technologies.

In 2012 CARNet and National CERT issued a brochure (Nacionalni CERT, 2012, p. 1) about privacy on Facebook, in order to inform students “about the dangers caused when posting personal data and content on the most popular social network and how to set a profile on Facebook so as to keep one’s privacy”. The brochure, speaking of risks, states that (Nacionalni CERT, 2012, p. 4) “a piece of information that users put on their profiles on Facebook, malicious persons or criminal groups can misuse”, and lists possible misuse. The brochure explains how to set privacy settings in order to minimize the risks.

CARNet and CERT brochures are popular among students and are regularly distributed in schools. They represent an extremely important means of education in the area of the current security issues which were not represented in the regular classroom.

“Child Safety on the Internet” is a manual that was published (Net Akademija, 2009) under the auspices of the former Ministry of Family, Veterans and Intergenerational Solidarity, on the occasion of the International Day of Families on May 15th, 2009. The handbook is a valuable overview of the dangers and threats for children, primarily intended for parents, i.e. to educate parents and their children. It provides ten tips about children and the Internet, eleven rules for parents and ten rules for children.

In 2012 the National CERT and CARNet released another excellent brochure entitled “Safer Business on the Internet” (Štifić & Čamagajevac, 2012). Due to its high quality (intelligibility and completeness) this brochure can be self-supporting literature for parents and teachers, and a motivation for teachers of Informatics to update their curriculum.

Finally we shall look at a document with the title “Raising Awareness of Information Security” (CARNet CERT & LS&S, 2005b) which was jointly produced by CARNet CERT and LS & S - Laboratory for Systems and Signals at the Department of Electronic Systems and Information Processing, Faculty of Electrical Engineering and Computer Science (University of Zagreb). It is an official document intended for people in senior management positions and is a strategic reflection on structured programmes and training to raise awareness of information security. Although the document was released in 2005, it is not yet obsolete due to the strategic level that it was made for.
Discussion
Effective education systems stand out through clear and ambitious standards (OECD, 2010). In Effective education systems everyone knows what needs to be done in order to reach certain qualifications, both in terms of content and in terms of the knowledge and abilities of its application. If the primary education system still does not contain a mandatory subject of ICT education, as it is in most countries including Croatia, one cannot be satisfied. Speaking from the author’s personal experience, it could be said that even that small amount of content that is part of the obligatory curriculum is not dealt with in accordance with the prescribed curriculum. At the time of the creation of the curriculum, all the stakeholders expected that the subject of Informatics would soon become mandatory, but it has not happened until today. Primary school teachers should have a prescribed number of teaching hours so as to be full-time employed. Otherwise they can lose their jobs. In order to prevent this from happening, they avoid conflicts with their students, parents and principals. The result of this is that primary school teachers often stick to minimalistic version of the curriculum (more games, less work). The consequences are the following: majority of the students come to secondary school incompetent and semi-literate in IT usage and IT related knowledge including infosec. The problem is even worse in those Croatian schools where, due to the lack of space, tuition is one week in the morning and the other in the afternoon (a considerable percentage of schools belong to this group). In those schools, Informatics classes are always held in the “shift” opposite from all other subjects.

Primary school teachers who are not ICT related specialists, have a very low level of ICT practical knowledge and as such they are no exception from the rest of the Croatian society. Their level of knowledge and their habits regarding information security (data, computing, communications and network security) are even worse. The author does not have enough objective data to support this but most of Croatian teachers who teach ICT related subjects at all educational levels would agree with this view.

Under such conditions, is it possible to make a move in the direction of introducing infosec themes and contents? It is clear that there should be a reduction of theoretical and factual content. It is also clear that students should be taught to find relevant pieces of information quickly and efficiently and to search for them in the relevant sources and to question their authenticity. The precondition for any qualitative change regarding the infosec education is that Informatics should become an obligatory school subject (at least starting from Grade Five).

Conclusion
This review laid the necessary groundwork for further field research of computer, communication, data and information security among elementary school children. Educational programmes that are implemented in Croatian elementary school seem to be defined by only two documents: Croatian National Educational Standard (which itself is a set of documents) and the National Curriculum Framework. In reality, there is a delicate interwoven character of a complex regulatory structure whose final result represents three documents that outline prescribing curriculum and supporting textbooks. This article has found and described all the relevant laws, rules, regulations, directives and decisions and has illustrated their structure in the form of lists, descriptions, explanations and diagrams. It can be concluded that the elementary education system is overregulated. Such a complex and regulated system is too slow, inert and loaded with numerous restrictions.

Within the Croatian primary education system, school subject about ICT called Informatics is optional for students. This status is extremely harmful to the quality of teaching and dissemination of ICT knowledge and skills. Important topics about infosec should be incorporated in it.

At the time when more and more personal and secret pieces of information become perversely public because of ignorance, at a time when corporations and governments want to know everything about their citizens and have access to everything they do/think/talk/write, it is really high time for all the stakeholders to act and so to start educating children about the infosec.
Children are vulnerable mainly out of ignorance and because sophisticated ICT technology is used to trick them. Therefore we cannot be satisfied. In contrast to the great need, the Croatian curriculum of primary education does not include almost any information security content. However, thanks to the knowledge of some authors, there are quite a few of such contents in textbooks and workbooks, but they are unsystematically distributed, concentrated in a few sections through the eight years of education. On the other hand, according to the HNOS Curriculum, students in primary schools who choose Informatics learn the material in programme modules: basics of information and communication technology, hardware and software, multimedia, word processing, spreadsheets, databases, presentations, web design, problem solving and programming, and the Internet. We must ask ourselves whether this should be appropriate for all students or not?

Not knowing legislation does not exempt anyone from not acting in accordance with them. There are numerous problems related to ICT security, and students should be learning about them. In the of ICT security and privacy domain, ignorance is very dangerous, and the potential damage is very large, both in measurable and in immeasurable dimensions. Education at an early age is the best assumption for later info-security awareness. The ultimate goal is increasing the level of information safety for children, so
1. they are not become an object of an attack and
2. that their actions (out of ignorance and lack of awareness) do not become a source of threats to the systems they use.

References


Tedo Vrbanc
Department of Information Sciences, The Faculty of Teacher Education, University of Zagreb, Savska cesta 77, 10000 Zagreb, Croatia
tedo.vrbanc@gmail.com
Raskorak između potrebe i stvarne uključenosti obrazovanja o informacijskoj sigurnosti u hrvatskom osnovnom školstvu
Tedo Vrbanec
Katedra za informacijske znanosti, Učiteljski fakultet Sveučilišta u Zagrebu, Hrvatska

Sažetak
U Hrvatskoj je na snazi znatan broj zakona, propisa, pravilnika, uredbi i odluka koji neposredno ili posredno propisuju osnovnoškolske nastavne sadržaje. U ovom ih se radu agregira i izlaže na što je (autoru) moguće razumljiviji i smisljeniji način. U radu se nadalje utvrđuje u kojoj se mjeri u propisanim nastavnim programima te u obrazovnim ciljevima i postignućima predmeta informatike nalaze oni koji su sigurnosne prirode. Prikazana je analiza sadržaja cjelokupne propisane informatičke osnovnoškolske literature te njezina usklađenost s propisanim nastavnim programima informatike. Završno, u radu se raspravlja o nalazima i uočenim problemima, predlažu rješenja te postavljaju neka nova pitanja.

Ključne riječi: komunikacijska sigurnost; obrazovanje; privatnost; računalna sigurnost; zaštita podataka