Pedagogická fakulta
Faculty of Education
Jihočeská univerzita v Českých Budějovicích
University of South Bohemia in České Budějovice

Jihočeská univerzita v Českých Budějovicích
Pedagogická fakulta
Katedra informatiky

Bakalářská práce

Výuka digitální bezpečnosti na ZŠ a SŠ

Teaching of digital safety at the secondary and high school

Jakub Zelenka

Vedoucí bakalářské práce:
Mgr. Václav Šimandl

České Budějovice 2013

JIHOČESKÁ UNIVERZITA V ČESKÝCH BUDĚJOVICÍCH
Fakulta pedagogická
Akademický rok: **2011/2012**

ZADÁNÍ BAKALÁŘSKÉ PRÁCE

(PROJEKTU, UMĚLECKÉHO DÍLA, UMĚLECKÉHO VÝKONU)

Jméno a příjmení:	**Jakub ZELENKA**
Osobní číslo:	**P10385**
Studijní program:	**B7507 Specializace v pedagogice**
Studijní obor:	**Informační technologie ve vzdělávání**
Název tématu:	**Výuka digitální bezpečnosti na ZŠ a SŠ**
Zadávající katedra:	**Katedra informatiky**

Zásady pro vypracování:

Cílem práce je analyzovat výuku digitální bezpečnosti na základních a středních školách. Student připraví dotazník, který se bude zabývat rozsahem, skladbou a kvalitou výuky digitální bezpečnosti. Dotazník bude pokrývat zejména problematiku používání SW bezpečnostních prvků (antivir, firewall), zálohování dat, obezřetného chování na internetu (včetně zveřejňování citlivých dat), výběru a správy bezpečnostních hesel a problematiku autorského zákona.

Na základě sestaveného dotazníku student zorganizuje dotazníkové šetření, jehož respondenty se stanou čerství absolventi dostatečného počtu základních a středních škol. Výsledky získané v dotazníkovém šetření budou statisticky zpracovány.

V teoretické části práci se student zaměří na vymezení jednotlivých oblastí problematiky digitální bezpečnosti. Student také analyzuje české státní dokumenty týkající se výuky ICT s důrazem na tuto problematiku.

V závěrečné části práce student porovná předpokládané a výzkumem zjištěné kompetence žáků obou stupňů škol.

Rozsah grafických prací: **CD ROM**

Rozsah pracovní zprávy: **40**

Forma zpracování bakalářské práce: **tištěná**

Seznam odborné literatury:

1. **Chráska, M. Metody pedagogického výzkumu. Praha: Grada, 2007. ISBN 80-247-1369-4.**
2. **i-SAFE. SAFE Internet Safety Activities: Reproducible Projects for Teachers and Parents. Jossey-Bass, 2010. ISBN 978-0470539507.**
3. **Jeřábek, J. a kol. Rámcový vzdělávací program pro gymnázia RVP G. Praha : Výzkumný ústav pedagogický, 2007. Dostupný z WWW: <old.rvp.cz/soubor/RVP_G.pdf>. ISBN 978-80-8700-11-3.**
4. **Kocman, R., Lohniský, J. Jak se bránit virům, spamu, dialerům a spyware. CP Books, 2005. ISBN: 80-251-0793-0.**
5. **Sechler, J. A Young Adult's Guide to Safety in the Digital Age. CreateSpace, 2010. ISBN 978-1453618414.**
6. **Vaníček, J. Informatika pro základní školy a víceletá gymnázia 2. CP Books, 2005. ISBN 80-251-0630-6.**
7. **Katalog požadavků zkoušek společné části maturitní zkoušky: Informatika, základní úroveň obtížnosti [online]. Centrum pro zjišťování výsledků vzdělávání, 2010 [cit. 2012-04-07]. Dostupné z WWW: <http://www.novamaturita.cz/index.php?id_document=1404034533&at=1>**

Vedoucí bakalářské práce: **Mgr. Václav Šimandl**
Katedra informatiky

Datum zadání bakalářské práce: **19. dubna 2012**

Termín odevzdání bakalářské práce: **26. dubna 2013**

Mgr. Michal Vančura, Ph.D.
děkan

L.S.

doc. PaedDr. Jiří Vaníček, Ph.D.
vedoucí katedry

V Českých Budějovicích dne 12. dubna 2012

Prohlášení

Prohlašuji, že bakalářskou práci jsem vypracoval samostatně pouze s použitím pramenů a literatury uvedených v seznamu citované literatury.

Prohlašuji, že v souladu s § 47b zákona č. 111/1998 Sb. v platném znění souhlasím se zveřejněním své bakalářské práce, a to v nezkrácené podobě elektronickou cestou ve veřejně přístupné části databáze STAG provozované Jihočeskou univerzitou v Českých Budějovicích na jejích internetových stránkách, a to se zachováním mého autorského práva k odevzdanému textu této kvalifikační práce. Souhlasím dále s tím, aby toutéž elektronickou cestou byly v souladu s uvedeným ustanovením zákona č. 111/1998 Sb. zveřejněny posudky školitele a oponentů práce i záznam o průběhu a výsledku obhajoby kvalifikační práce. Rovněž souhlasím s porovnáním textu mé kvalifikační práce s databází kvalifikačních prací Theses.cz provozovanou Národním registrem vysokoškolských kvalifikačních prací a systémem na odhalování plagiátů.

V Českých Budějovicích dne 24. dubna 2013 Jakub Zelenka

Anotace

Tato bakalářská práce se zabývá problematikou výuky digitální bezpečnosti na základních a středních školách. To znamená v první řadě zohledněním důležitých aspektů počítačové bezpečnosti, jako jsou ochrana svého zařízení před nebezpečnými viry a pirátskými útoky za pomoci bezpečnostního software, správná záloha a správa svých dat. Dále zaměření na rozvážné chování na internetu zahrnující opatrnost vůči emailovým hrozbám, podvodnému chování některých uživatelů a obezřetné používání sociálních sítí. Taktéž obsahuje bezpečnost hesel s důrazem na silné heslo a jeho správu a také problematiku autorského zákona.

V práci je zahrnuta obsahová analýza českých kurikulárních dokumentů vzhledem k dané problematice. Jsou zde uvedeny podobné výzkumy související s tématem, teorie výzkumu a hlavní výzkum této práce.

V tomto výzkumu je zahrnuto dotazníkové šetření zkoumající kompetence žáků výše uvedených škol při výuce počítačové bezpečnosti, jehož výsledky jsou vyhodnoceny a porovnány s poznatky ze státních dokumentů související s problematikou výuky ICT.

Klíčová slova

digitální bezpečnost, RVP, autorský zákon, antivir, firewall, záloha dat, bezpečnost hesel

Abstract

This thesis deals with the issue of digital security at primary and secondary schools. This means first of all taking into account important aspects of computer security, such as protection of your equipment from dangerous viruses and pirate attacks with security software, the correct backup and manage their data. Furthermore, the focus on prudent behavior on the Internet, including caution against email threats, fraudulent behavior of some users and prudent use of social networks. It also provides password security with an emphasis on strong password management and also the issue of copyright law.

The work included content analysis of Czech curricula given to the issue. They are listed here similar studies related to the topic of research theory and the main research of this thesis.

In this research included a survey investigating the competence of students of the above schools in teaching computer security, the results are evaluated and compared with the findings of state documents related to the issue of teaching ICT.

Keywords

digital safety, RVP, copyright, antivirus, firewall, backups, password security

Poděkování

Rád bych poděkoval vedoucímu své bakalářské práce Mgr. Václavu Šimandlovi za výborné vedení mé práce a poskytování cenných rad při její tvorbě.

Dále bych chtěl poděkovat všem, kteří mi pomohli realizovat výzkum, a také děkuji všem jeho respondentům.

Obsah

1 Úvod

Tématem této bakalářské práce je zejména výzkum v oblasti počítačové bezpečnosti vzhledem k výuce této problematiky na základních a středních školách. Částečně o tomto tématu existují různé studie, znalostní průzkumy a dále bakalářská práce J. Lhotáka (viz str. 33 a 34), ale žádný ze zdrojů není přímo zaměřen na kompetence žáků ZŠ a SŠ ve výuce informační bezpečnosti. Proto nám přišlo vhodné se touto problematikou zabývat.

1.1 Cíle práce

V teoretické části je potřeba se zaměřit zejména na úvod do digitální bezpečnosti, určit a charakterizovat její jednotlivá témata. Dále je nutné analyzovat vzdělávací programy České republiky z hlediska jejich obsahu týkajícího se informačních technologií a to především s ohledem na bezpečnost. V této části je dále nezbytné zmínit podobné výzkumy a také teorii výzkumu.

V praktické části je hlavním cílem zorganizování dotazníkového šetření, na jehož základě dojde ke zjištění a ověření hloubky znalostí žáků a studentů základních a středních škol v problematice digitální bezpečnosti. Poté dojde k vyhodnocení. Zjištěná data budou zpracována a následně porovnána s českými státními dokumenty zabývající se výukou ICT. Praktická část bude řádně vyhodnocena.

1.2 Metoda práce

Na počátku zpracování byla prostudována doporučená literatura, doplněna nalezením vlastních zajímavých zdrojů. Důležité bylo rozvrhnutí si celé práce a hlavně pochopení problematiky. Na základě získaných informací byl sestaven dotazník (viz str. 38), který byl následně aplikován (viz str. 39). Z šetření byly vyvozeny patřičné závěry, na základě kterých byla tato práce sepsána.

2 Problematika digitální bezpečnosti

2.1 Digitální bezpečnost

Počítačová bezpečnost je pojem, se kterým se v jednadvacátém století setkává stále větší procento uživatelů počítačových a komunikačních technologií. Dříve byla bezpečnost informačních technologií výsadou pouze několika skupin odborníků, v současné době této problematice musí věnovat pozornost i koncový uživatel [1].

S přibývajícím počtem poskytovaných online služeb, rostoucí dostupností a tím zvyšujícím se zastoupením uživatelů (viz *Obrázek 1*), kteří se na internetu objevují, přibývají také tací, kteří chtějí nad ostatními ukázat svoji pomyslnou převahu, ať už k tomu mají jakýkoliv důvod [2]. Proto nastává doba, kdy nám bohužel již nestačí spolehnout se na instalaci antiviru a neotvírat nevyžádanou poštu. Nejdůležitějším faktorem se stává uživatel, který se musí chopit zodpovědnosti, jež mu náleží a svým pečlivým a obezřetným chováním dbát nejenom na bezpečnost svých dat, ale také na svou bezpečnost [3]. Zvláštní pozornost by pak měli věnovat rodiče a učitelé dětem a dospívajícím, kteří tvoří v tomto ohledu nejzranitelnější skupinu.

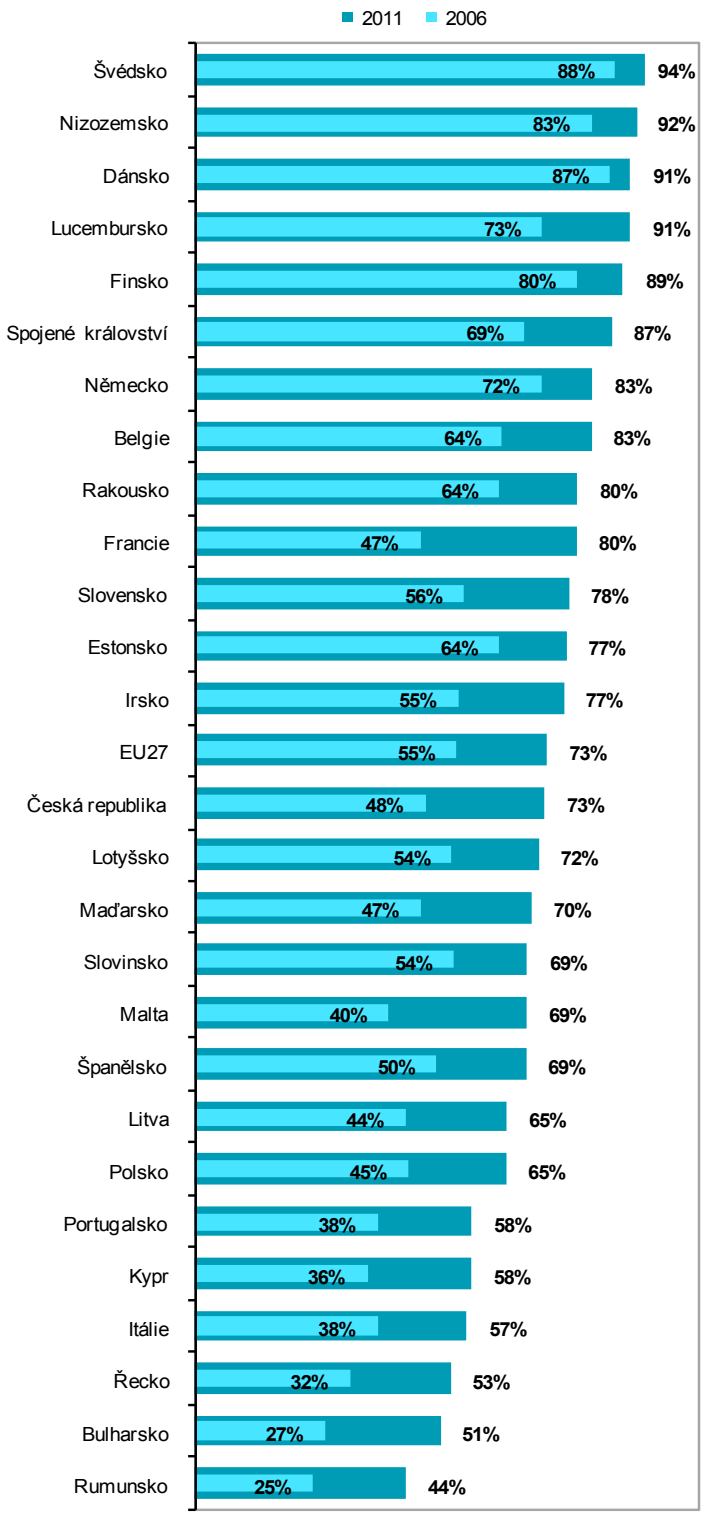
Základní formy nebezpečí, se kterým se můžeme setkat, se dají rozdělit do třech základních částí [4]:

- Osobní bezpečnost – do této části se zahrnuje vše, co se týká našeho fyzického, psychického zdraví a správného duševního rozvoje. Zde se můžeme setkat s nebezpečím kyberšikany a kybergroomingem, stalkingem, sms textingem a sextingem. Zahrnují se sem i internetové závislosti.

- Bezpečnost osobního vlastnictví - sem se zahrnují krádeže identity, jakékoliv online podvody, ať už se jedná o phishing či jiný podvod. Nesmí zde chybět také viry a spyware.
- Ostatní rizika – do těch řadíme online pověst každého uživatele. Dále problematiku autorského zákona a plagiátorství.

V této práci je vyčleněno jen několik základních pilířů, které však zahrnují většinu výše zmíněného. Těmito pilíři jsou:

- Software bezpečnostní prvky
- Záloha dat
- Obezřetné chování na Internetu
- Bezpečnost hesel
- Autorský zákon



Obrázek 1 - Zvyšující se počet uživatelů Internetu ve věku 16 - 74 let (Zdroj: Eurostat, 2012)

2.2 Softwarové bezpečnostní prvky

Jednou z nejzákladnějších metod ochrany našich dat je využití bezpečnostního softwaru. Pokud uživatel nevyužívá žádný bezpečnostní program na ochranu svých dat, vystavuje se vysokému riziku napadení svého počítače virem, popř. poskytne záchytný bod nějakému hackerovi, který snadno použije uživatelův PC a připojení k Internetu pro své další útoky. Udává se totiž, že nově připojený počítač k Internetu může být „vyhledán" a „vyzkoušen" do několika hodin [2].

Prvním způsobem, jak čelit nástrahám Internetu, je včas a pravidelně provádět aktualizace svého operačního systému. Jelikož operační systém je poměrně složitý programový balík s mnoha komponenty a spolupracuje s dalšími programy, mohou systém některé z nich zneužít či poškodit. Pokud se budeme bavit o Microsoft Windows, je důležité využívat takzvaný systém update, kdy Microsoft vydává bezpečnostní záplaty, které mají za úkol opravit bezpečnostní chyby a zamezit tak vstupu nepřátelského viru do systému [5]. Nejlepším řešením je proto nastavit si aktualizace, aby probíhaly automaticky vždy, když budou k dispozici.

Microsoft vydává bezpečnostní záplaty a opravné balíčky ve dvou druzích oprav [5]:

- Hotfix – jednorázové záplaty pro opravu jediné chyby
- Service Pack – bezpečnostní balíček, který obsahuje všechny opravy za určité období

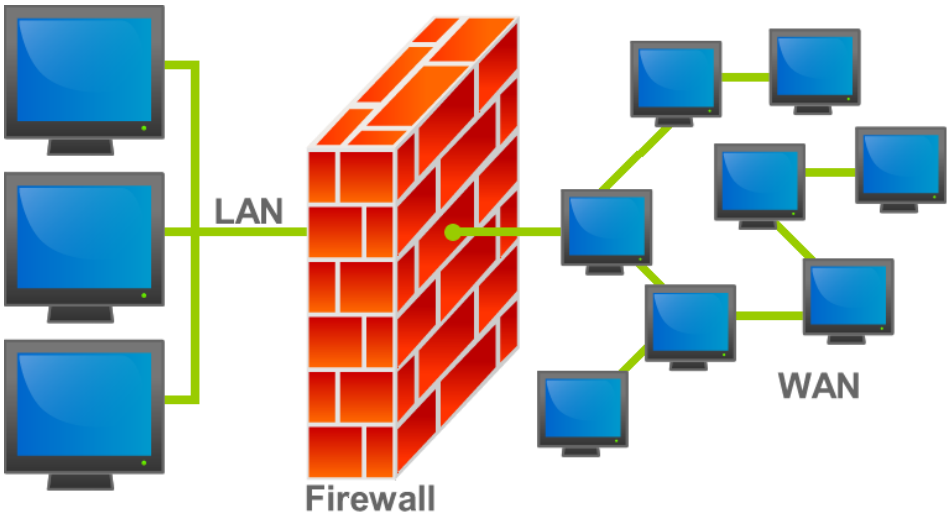
2.2.1 Antivir

Je jeden ze softwarových nástrojů určený k ochraně uživatelských dat. Antiviry slouží k vyhledávání škodlivého softwaru, který by jinak mohl mezi daty napáchat škody. Antiviry většinou pracují dvěma způsoby. U prvního

způsobu porovnávají při procházení disku počítače nalezené soubory s částí těl virů, jejich názvy a kroky k jejich odstranění, které mají ve své databázi. Toto tedy probíhá na základně signatury, proto jsou tyto antiviry nazývány signaturové. Dalším způsobem je heuristický způsob, kdy antivir spouští testované soubory v tzv. testovacím prostředí a zkoumá jejich neobvyklé chování. Tento proces je oproti signaturové metodě pomalejší, ale dokáže odhalit i novější viry, které ještě nemusí být ve virové databázi daného antiviru. Právě kvůli databázi virů a dalších škodlivých souborů je nutné antivir pravidelně aktualizovat, to se však u většiny antivirů dá automatizovat, tudíž při správném nastavení není potřeba pravidelného zásahu uživatele [6].

2.2.2 Firewall

Tento termín nám označuje počítač, neboli spíše software na něm pracující, který slouží k ochraně lokální sítě před přístupem z Internetu [5]. Jak již napovídá název, jedná se o imaginární zeď, která nám odděluje lokální síť od Internetu. Tato „zeď“ nám kontroluje všechny pakety, které putují mezi Internetem a místní sítí. Pokud je firewall správně nastaven pro kontrolu protokolů, které chce administrátor propouštět, pak nabízí tu možná nejlepší ochranu před útokem „zvenčí“ [7]. Firewall je též zpravidla součástí operačního systému, pokud tedy zůstaneme u Microsoft Windows, neměl by mít uživatel větší problém s jeho správným nastavením.



Obrázek 2 - Zjednodušené schéma fungování firewallu (zdroj: Wikipedia.org, autor Bruno Pedrozo)

2.3 Záloha dat

Velice často podceňovaný proces, který není nikterak složitý. Při zálohování dat jde o vytvoření kopie, která je poté dále umístěna na médium odlišné od originálu. Díky tomu můžeme při poškození, krádeži, ztrátě či smazaní originálu nebo kopie data obnovit z kopie nebo popř. vytvořit další kopii z originálu. Tímto způsobem můžeme zamezit tomu, abychom o data přišli trvale.

S nově se rozvíjejícími technologiemi a neúprosně se zvyšující kapacitou disků, ať už jde o pevné či přenosné, je bohužel tato velmi důležitá činnost často podceňována celou řadou jednotlivců, kteří si myslí, že zrovna jejich disk je spolehlivý a pravou cenu svých dat si uvědomí až po jejich nenávratné ztrátě [8]. Proto není dobré situaci podcenit a nejjednodušším řešením je svá data zálohovat, protože při tomto procesu ztratíme maximálně jen data vytvořená od poslední zálohy. v současné době má vytváření kopií našich důležitých i méně důležitých souborů jedno velké pozitivum, a to je rozšiřující se kapacita a dostupnost přenosných médií jako jsou externí disky a různé flash disky,

které obstarávají slušnou kapacitu a jejich skladování není poněkud tak složité jako uchování několika desítek CD nebo DVD, nemluvě o vyhledávání a manipulaci s nimi. Zálohu nemusíme také vůbec řešit ukládáním na přenosná média, ale již můžeme pro naše potřeby využít dostupných online služeb [6] a [8].

2.4 Obezřetné chování na internetu

Kromě aktualizace antiviru, správně nastaveného firewallu, používání silných hesel a zálohy dat je také potřeba vědět, jak se chovat v rámci Internetu, aby jeho využívání pro nás bylo maximálně bezpečné. Proto je důležité vědět, jak se správně chovat a jak se vyvarovat všem současným nástrahám nejrozšířenější světové sítě. K tomu by nám mělo pomoci naše prozíravé a obezřetné chování, kdy je potřeba se pořádně zamyslet a neuvěřit každé zprávě či podvodnému emailu, se kterými se na Internetu setkáme v hojném počtu.

2.4.1 Internet

V první řadě je potřeba vyvrátit mýtus o tom, že Internet je zcela anonymní. V dnešní době lze spoustu věcí dohledat, jelikož většina provozovatelů ukládá logy (záznamy o návštěvě) uživatelských účtů, které mohou být později zpřístupněny policii [9]. Dále musíme zmínit to, že všechny informace uvedené na Internetu nemusí být pravdivé. Protože ne každý uživatel používá světovou síť s dobrými úmysly, musíme být velmi obezřetní, abychom někomu „nenaletěli“ nebo dokonce nebyli někým ohroženi. Při procházení webů si musíme také dávat pozor na falešné webové stránky, na první pohled vypadající stejně jako pravé stránky, ale jedná se o podvod často související s phishingem [9]. Tyto stránky lze rozeznat v adresovém řádku, kdy přesná adresa neodpovídá originální stránce, rozeznat rozdíl na první pohled však může být obtížné. Bezpečný web poznáme tak, že počátek adresy webu začíná https, písmenko „s“ značí anglický název secure, což znamená

v překladu zabezpečit. Jedná se tedy web s vyšším zabezpečením, často se s ním můžeme setkat u webových stránek bankovních domů, kde je vyšší zabezpečení nezbytné [12].

2.4.2 Sociální sítě

Dle zdrojů [4] a [9].

Hlavními riziky sociálních sítí jsou ta, že nikdy nevíme, komu se informace námi sdílené na těchto sítích dostanou do rukou a dále podobně jako u chatu si nikdy nemůžeme být jisti, s kým doopravdy komunikujeme. v tomto ohledu mohou být sociální sítě ještě nebezpečnější, protože nejenže můžeme komunikovat s osobou, co s námi nemá dobré úmysly, ale dokonce si tato osoba může přímo na sociální síti zjistit leckteré informace, které může snadno použít v náš neprospěch.

Proto je nutné vzít tato rizika na vědomí. Čím méně věcí o sobě budeme zveřejňovat, tím samozřejmě lépe. Zásadně se nedoporučuje uveřejňovat přesnou adresu, telefonní číslo popř. jiný kontakt. Dále je dobré nezveřejňovat ani nikomu neposílat své intimní fotografie, hrozí zde riziko pozdějšího zneužití. Dbejme, abychom si do přátel či okruhu svých „blízkých“ nepřidali někoho neznámého, často se může jednat o někoho, kdo nás později může ohrozit. K tomu se váže pravidlo, abychom se rozhodně s nikým, koho neznáme osobně, nescházeli.

2.4.3 Email

Zásadním pravidlem pro bezpečné používání je neotvírat přílohy nevyžádané pošty. Je zde vysoká pravděpodobnost, že obsahují nějaký škodlivý software. Stejné pravidlo platí i pro odkazy uvedené v nežádoucí poště. Další důležitou součástí v rámci bezpečné komunikace je nerozšiřování poplašných zpráv, tzv. Hoax. Dbát zvýšené pozornosti u dalších podvodných praktik jako je phishing, který nás vyzývá k vyplnění osobních nebo platebních

údajů a přitom se vydává za námi známou banku či jinou službu. Z toho plyne, že nejlepší ochranou pro uživatele a jeho data je zacházení pouze s takovou poštou, u které si je zcela jist jejím původem nebo účelem, za kterým byla zaslána. Pro všechny ostatní případy je v emailovém klientu k dispozici koš.[9]

2.5 Bezpečnost hesel

Heslo je v první řadě bezpečnostních prvků, měla by to být nejsilnější stránka ochrany našeho soukromí a našich dat, ale často se může stát nejslabším článkem zabezpečení. K odhalení hesel útočníci používají software, který dokáže vyzkoušet během několika málo minut i stovky tisíc hesel, z toho vyplývá, že prolomit se dá každé heslo, pokud na to bude mít hacker dostatek času. [3], [5]

2.5.1 Silné heslo

Abychom své uživatelské účty nejlépe ochránili, je potřeba používat dostatečně silná hesla. Silným heslem se rozumí takové heslo, které co nejvíce útočníkovi znesnadní jeho dešifrování. Proto by mělo být dostatečně dlouhé a obsahovat různé druhy znaků. [5], [9]

- Bezpečné heslo musí obsahovat dostatečný počet znaků. Doporučuje se 7 až 14.
- Mělo by obsahovat co největší spektrum znaků. To znamená využití písmen, číslic, ale i ostatních alfanumerických znaků. v některých případech se dá počítat i s psaním mezery.
- Heslo je potřeba měnit v časových intervalech a nové heslo by se mělo od starého lišit zásadním způsobem. Nemělo by být jakkoliv podobné.
- Jakékoliv slovo nebo slovo ze slovníku není bezpečné heslo. Útočníci většinou zkouší obyčejná slova či používají seznamy

nejčastěji používaných hesel, proto je potřeba se tomuto vyvarovat.

2.5.2 Ochrana hesla

Vytvořením silného hesla však naše starost o bezpečnost našich účtů nekončí. Pokud s ním nebudeme bezpečně zacházet, je jedno, jak silné bude [3], [5], [9].

- Heslo není vhodné kamkoliv zapisovat v jeho textové podobě.
- Je naprosto vylučitelné sdělovat ho jiným osobám včetně rodinných příslušníků, kamarádů a svých partnerů.
- Nepoužívat stejné heslo na více místech.
- V případech, kdy používáme veřejně dostupné počítače, není vhodné se přihlašovat ke svým účtům. Nikdo nám nemůže zaručit, že zde není nainstalovaný škodlivý software, přes který může naše údaje někdo získat.
- Pokud nastane situace, kdy máme podezření, že by naše heslo mohlo být prolomeno, je nezbytně nutné ho ihned změnit.

2.6 Autorský zákon

Autorský zákon je takový zákon, který přiznává autorovi všechna práva k dílu, které vytvořil v souladu se zákony České republiky. Předmětem práva autorského je dílo (dle zákona č.121/2000 §2), které je výsledkem tvůrčích dovedností autora a je vnímatelné v jakékoliv podobě [10]. *„Autorská práva se dělí na osobnostní a majetková. Osobnostní zahrnují především právo osobovat si autorství, rozhodnout o zveřejnění díla, právo na nedotknutelnost díla, zejména právo udělit souhlas ke změně nebo jinému zásahu do díla. Majetková práva zahrnují hlavně právo dílo užít a udělit souhlas k užití.“* [9]

Porušování autorského zákona se nás netýká pouze v jediném případě. Ze zákona je dáno, že si každý může z díla udělat kopii pouze však pro vlastní potřebu, pokud ovšem není dílo chráněno proti kopírování. Avšak tuto kopii může uživatel používat pouze v souladu se zákonem. To znamená, že nesmí dělat další kopie, šířit dílo dále, půjčovat, prodávat, hromadně promítat ani sdílet na Internetu či někomu darovat. Bohužel toto pravidlo neplatí na všechna díla, např. počítačové hry a software, na které si klade autor svá práva, se nesmí kopírovat ani pro své vlastní účely. [10], [11]

Z výše uvedeného tedy plyne, že v určitých případech si můžeme vytvořit z díla kopii, ovšem nesmíme ji dál šířit, a to žádným způsobem. v tomto ohledu jsou nebezpečné peer to peer sítě, kdy sice stahujeme data, ale zároveň je poskytujeme pro ostatní a tím se dostáváme do rozporu s autorským zákonem, pokud tedy mluvíme o datech, na něž se zákon vztahuje.

3 Digitální bezpečnost v českých kurikulárních dokumentech

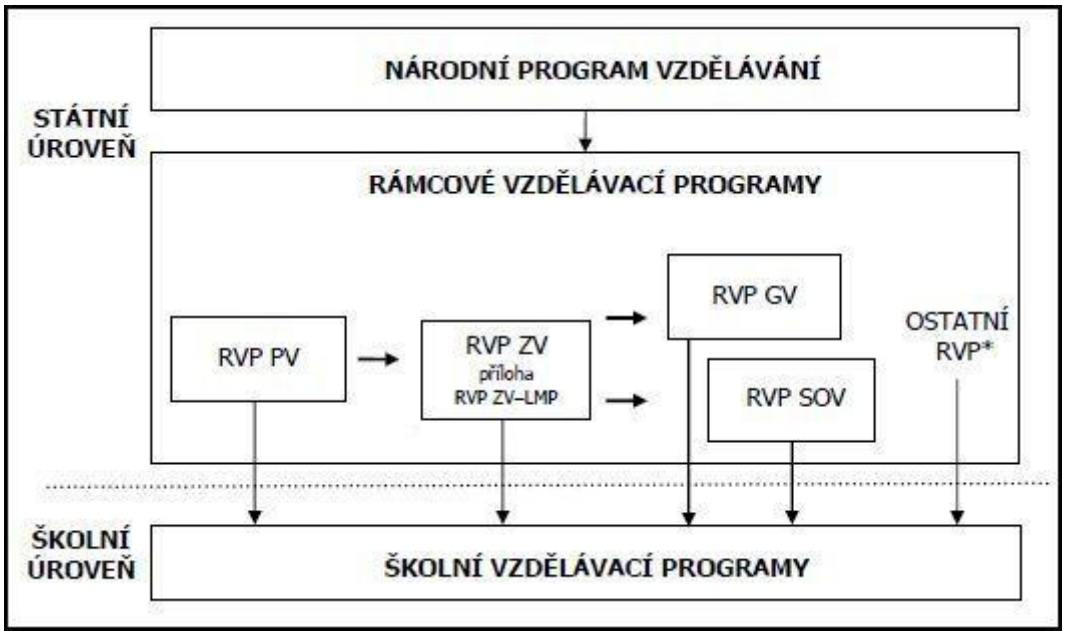
3.1 Systém vzdělávání v ČR

V České republice v současné době vzdělání dětí a mládeže od 3 do 19 let podléhá státní kurikulární politice, která v souladu s tzv. Bílou knihou[1] a zákonem č. 561/2004 Sb., o předškolním, základním, středním, vyšším odborném a jiném vzdělávání (školský zákon) rozděluje principy a postupy vzdělávání do dvou sfér viz obrázek [14].

Do první sféry neboli státní úrovně řadíme Národní program vzdělávání, který zahrnuje vzdělávání jako celek a je dále rozdělován na tzv. Rámcové vzdělávací programy (RVP), které se rozdělují podle etap vzdělávání na předškolní, základní a střední vzdělání [14]. Tyto programy určují na úrovni státu požadovanou úroveň kompetencí, všeobecný základ vzdělání a obecně odborný základ vzdělání v odborném vzdělávání. Tím pádem jsou jasně dána pravidla a obsahový rámec k tvorbě školních vzdělávacích programů, čímž se zajišťuje srovnatelnost získávaného vzdělání [20].

Druhou úrovní vzdělávání jsou školní vzdělávací programy (ŠVP). Školní vzdělávací program si na rozdíl od rámcových vzdělávacích programů vytváří každá škola sama [14]. Tím jsou školám dány povinnosti takový program vytvořit, a to dle rámcově vzdělávacího programu příslušnému etapě vzdělání, v níž se daná škola nachází. Zde je projevena jistá volnost, kde lze využít znalostí a zkušeností učitelů při tvorbě tohoto dokumentu a přitom je vše v souladu s platnou legislativou. Za správnost tohoto dokumentu a jeho využití zodpovídá vždy ředitel školy [19].

[1] Bílá kniha – Národní program rozvoje a vzdělávání v ČR [20].



Obrázek 3 - Systém kurikulárních dokumentů [14]

Legenda: RVP PV – Rámcový vzdělávací program pro předškolní vzdělávání; RVP ZV – Rámcový vzdělávací program pro základní vzdělávání a příloha Rámcového vzdělávacího programu pro základní vzdělávání upravující vzdělávání žáků s lehkým mentálním postižením (RVP ZV–LMP); RVP GV – Rámcový vzdělávací program pro gymnaziální vzdělávání; RVP SOV – Rámcové vzdělávací programy pro střední odborné vzdělávání [14].

* Ostatní RVP – rámcové vzdělávací programy, které kromě výše uvedených vymezuje školský zákon – Rámcový vzdělávací program pro základní umělecké vzdělávání, Rámcový vzdělávací program pro jazykové vzdělávání, případně další [14].

3.2 Výuka digitální bezpečnosti na ZŠ

Jak je uvedeno výše, v dnešní době jsou žáci a studenti vzděláváni dle školních vzdělávacích programů, které vychází z pro ně příslušných RVP. v dokumentu RVP pro základní vzdělávání jsou informační technologie uvedeny jako jedna z devíti hlavních vzdělávacích oblastí pod názvem: „Informační a komunikační technologie“ a jsou zároveň i vzdělávacím oborem. Z hlediska toho, že jsou ICT vyčleněny jako samostatná oblast, což je podle nás jenom dobře, je zajímavé, že vyučovacímu předmětu, který má tento obor reprezentovat, je vyčleněna mimořádně malá minimální týdenní hodinová dotace [14]. Pro splnění této dotace stačí škole vyučovat předmět zaměřený na ICT jen jednu hodinu týdně, a to pouze v jednom ze čtyř ročníků druhého

stupně. To ovšem neznamená, že tuto „jednohodinovku“ bezmezně všechny školy dodržují. Z praxe víme, že si některé základní školy jsou vědomy důležitosti vzdělávání v oblasti informačních technologií, a tak v rámci ŠVP přidávají více hodin [18], [21]. Mnohdy se však nejedná o rozšíření na základě kvality, ale často jsou do informačních předmětů zahrnuty i části jiných předmětů, popř. začleněno některé z průřezových témat[2]. Vše záleží na tom, jak si RVP vyloží daná základní škola, popř. víceleté gymnázium. S rozdílnými hodinovými dotacemi mohou ale bohužel vzniknout rozdíly ve vědomostech žáků.

Pokud se zaměříme na RVP z pohledu digitální bezpečnosti a její výuky v základním vzdělávání, dozvíme se pouze následující:

Cíle zaměření vzdělávací oblasti [14]:

Vzdělávání v dané oblasti směřuje k utváření a rozvíjení klíčových znalostí tím, že žáka vede k:

- *porozumění toku informací, počínaje jejich vznikem, uložením na médium, přenosem, zpracováním, vyhledáváním a praktickým využitím*
- *respektování práv k duševnímu vlastnictví při využívání SW*
- *zaujetí odpovědného, etického přístupu k nevhodným obsahům vyskytujících se na internetu či jiných médiích*

Dále do zahrnutého učiva pro druhý stupeň patří učivo o ochraně práv k duševnímu vlastnictví, copyright, informační etice.

[2] Průřezová témata - reprezentují v RVP ZV okruhy aktuálních problémů současného světa a stávají se významnou a nedílnou součástí základního vzdělávání [14].

Ačkoliv bychom čekali oproti strohému výkladu RVP v problematice bezpečnosti podrobnější výklad u ŠVP, setkáváme se pouze s několika nastíněnými poznámkami, jako jsou [21]:

Student ovládá a je schopen vysvětlit:

- *bezpečnost práce na internetu*
- *bezpečností práce v sítí (hesla)*
- *antivirové programy*
- *informační etika a autorský zákon*
- *student chápe, co může způsobit počítačový vir a zná prostředky prevence a ochrany proti němu* [18]
- *při použití vhodného softwaru dodržuje vymezená pravidla pro jeho používání (softwarové právo)* [18]

Z tohoto plyne, že při výuce digitální bezpečnosti v základním vzdělávání má vysoký a konečný podíl kompetence a ochota pedagoga vzdělávat žáky v oblasti bezpečného používání služeb, které ICT nabízejí.

3.3 Výuka digitální bezpečnosti na SŠ

Pro střední vzdělávání platí stejná pravidla jako pro vzdělávání základní. Stěžejním dokumentem v této etapě vzdělávání zůstává rámcový vzdělávací program, ze kterého vychází školní vzdělávací programy. Jediný rozdíl spočívá v tom, že ve středním vzdělávání máme několik typů RVP pro různé typy středních škol, rozlišujeme například RVP pro gymnaziální vzdělávání od RVP pro střední odborné vzdělávání a dále i popř. další RVP pro umělecké či jazykové školy atd.

V této bakalářské práci se zaměříme na RVP pro gymnázia, protože gymnázium nabízí zejména všeobecné vzdělávání na rozdíl od odborných škol, které mají za úkol z jedince vyprofilovat odborníka ve směru jejich zaměření. Proto pokud by byla zaměřena škola na ICT, je vcelku jasné, že bude mít daný žák naprosto jiné znalosti ve spektru informační bezpečnosti.

Pokud nahlédneme do RVP pro gymnázia, ihned najdeme markantní rozdíl mezi základním a středním vzděláváním a tím je hodinová dotace pro obor Informační a komunikační technologie. Oproti zmiňované jedné hodině je pro gymnázia stanovena minimálně jedna hodina týdně, a to v každém ze čtyř ročníků gymnázia, samozřejmě s prostorem pro úpravy ve ŠVP. Bohužel volnost daná školním vzdělávacím programům a nápověda v podobě manuálu [22] pro tvorbu ŠVP, v tomto případě nemusí být nutně vhodná, jak ukazuje [24], kdy čtyřleté gymnázium v Olomouci vyučuje z možných 4 hodin pouze 2 a zbylé 2 hodiny integrovalo do předmětů Matematika, Fyzika a Zeměpis. Samozřejmě se informační technologie často prolínají s ostatními předměty, ale nastává otázka, zda nebudou žáci ochuzeni o podstatné znalosti v oboru ICT, které se mohou dotknout i znalostí z pohledu bezpečnosti těchto technologií. Oproti tomuto dle [25] naopak gymnázium v Písku ke čtyřem hodinám přidalo pátou hodinu informatiky ze svých disponibilních hodin. Vyučuje tedy po dvou hodinách v prvním a druhém ročníku a jednu hodinu v ročníku třetím. V jiné časové dotaci předmětu mohou žáci získávat znovu naprosto jinou kvalitu a kvantitu vědomostí z tohoto oboru. Samozřejmě zde nebereme v potaz možnosti volitelných hodin, které školy mohou v rámci výuky nabídnout.

Cíle zaměření vzdělávací oblasti z ohledu na bezpečnost ICT dle RVP pro gymnázia [13]:

Vzdělávání v dané oblasti směřuje k utváření a rozvíjení klíčových znalostí tím, že žáka vede k:

- *„uvědomění si, respektování a zmírnění negativních vlivů moderních informačních a komunikačních technologií na společnost a na zdraví člověka, ke znalosti způsobů prevence a ochrany před zneužitím a omezováním osobní svobody člověka*“ [13]

- *„poznání základních právních aspektů a etických zásad týkajících se práce s informacemi a výpočetní technikou, k respektování duševního vlastnictví, copyrightu, osobních dat a zásad správného citování autorských děl“* [13]

Do učiva ICT nám zmiňovaný RVP GV v části Digitální technologie v učivu pro tuto část s názvem Údržba a ochrana dat, která zahrnuje kromě správy souborů a složek mimo jiné i antivirovou ochranu, firewall a zálohování dat. v další části Zdroje a vyhledávání informací je v učivu uvedeno Informační etika a legislativa, která by se měla zaměřit na ochranu autorských práv a osobních údajů [13]. Tímto tvůrci tohoto vzdělávacího programu vyhradili alespoň nějaký prostor pro vzdělávání v oblasti bezpečnosti informačních technologií. Vybrané gymnaziální ŠVP [23], [24], [25] pouze potvrzují znění RVP a soustředí se zejména na vybraná odvětví, jako jsou vir a antivirová ochrana, firewall, práce s daty a jejich záloha, etika a legislativa, ochrana autorských práv a osobních údajů a možná nebezpečí internetu.

3.4 Digitální bezpečnost k maturitě

Vzhledem k tomu, že jsou informační technologie součástí vzdělávacího procesu v České republice a vzdělávací obory související s IT jsou vůči ostatním oborům taktéž plnohodnotné, má každý žák právo vybrat si tento obor jako svůj maturitní. Proto byly stanoveny požadavky, které musí žák splnit, pokud chce maturitní zkoušku absolvovat úspěšně. K těmto požadavkům by mělo směřovat jeho středoškolské vzdělávání, aby byl žák k maturitě dostatečně připraven. Jelikož závěrečná středoškolská zkouška z informatiky se

skládá z celého spektra informací a znalostí z ICT oboru, je zde i prostor pro digitální bezpečnost.

3.4.1 Základní úroveň

Základní úroveň neboli nižší stupeň maturitní zkoušky z Informatiky zahrnuje devět tematických celků. Z nichž nejvíce nás zajímá celek s názvem Člověk, společnost a počítačové technologie, do kterého jsou zařazeny následující kapitoly [15]:

Bezpečný počítač

Žák ovládá:

- *vysvětlení potřeby aktualizací operačního systému a aplikačních programů, provedení aktualizace a nastavení způsobu jejího provádění;*
- *používání antivirového programu, firewallu a další bezpečnostních nástrojů a jejich porozumění;*
- *vysvětlení problematiky a způsobu šíření počítačových virů a červů, malware a spyware;*
- *popsaní nejčastějších metod útoků přes webové stránky a elektronickou poštu a bránění se proti nim;*
- *vysvětlení problematiky spamu a používání obrany proti němu, rozpoznaní hoax;*
- *rozlišení nebezpečí podvodů (tzv. technik sociálního inženýrství), rozpoznání základních rysů takového podvodu;*
- *zdůvodnění důležitosti komplexního přístupu k bezpečnosti IT.*

Obecné bezpečnostní zásady a ochrana dat

Žák ovládá:

- *aplikování zásad vytvoření bezpečného hesla pro identifikaci přístupu do systému;*
- *popsaní způsobů zabezpečení dat před jejich zneužitím;*
- *chránění svých dat před ztrátou, zálohování svých dat.*

Etické zásady a právní normy související s informatikou

Žák ovládá:

- *respektování etických zásad při práci s informacemi;*
- *charakterizovaní principů stanovených v zákonech o svobodném přístupu k informacím a o ochraně osobních údajů;*
- *vysvětlení podstaty ochrany autorských práv a základního ustanovení zákona o právu autorském ve vztahu k software a k šíření digitálních dat;*
- *aplikovaní norem pro citování z knih a z on-line zdrojů;*
- *vysvětlení pojmu licence k užití programu a charakterizování jednotlivých nejčastěji používaných druhů licencí;*
- *objasnění principů obsažených v licencích GNU/GPL a Creative Commons;*
- *uvedení příkladů běžných proprietárních programů a Open Source programů;*
- *mít přehled o způsobech ochrany software proti nelegálnímu šíření, uvědomovaní si protiprávnosti prolomení těchto ochran a rozpoznání souvisejících rizik.*

Využívání služeb Internetu

Žák ovládá:

- *popsaní způsobů sdružování lidí v sociálních sítích, zhodnocení přínosů a rizik těchto sítí;*
- *rozpoznaní zabezpečeného připojení a vysvětlení pojmu digitální certifikát serveru.*

3.4.2 Vyšší úroveň

Stejně jako v základní úrovni maturitní zkoušky je zde totožných devět tematických celků s tím rozdílem, že kapitoly v nich obsažené jsou zaměřeny do větších detailů dané problematiky. Tím pádem je kladen větší důraz na znalosti a vědomosti žáka. Informační bezpečnosti se týká stále stejná kapitola, která je ovšem rozšířena o: [16]

Obecné bezpečnostní zásady a ochrana dat

Žák ovládá:

- *vysvětlení pojmů jako jsou: integrita dat, hash, autenticita, šifrovací algoritmus a klíč;*
- *popsaní principů šifrování pomocí symetrické kryptografie a oblasti jejího nasazení v praxi;*
- *popsaní principů šifrování pomocí asymetrické kryptografie a oblasti jejího nasazení, pojmy privátní a veřejný klíč a princip elektronického podpisu;*
- *praktické provádění šifrování souborů.*

3.4.3 Shrnutí

Znalostní požadavky k maturitě z předmětu Informatika shledáváme jako dobré jak pro základní, tak i vyšší úroveň maturity, alespoň pokud se jedná o informační bezpečnost. Jednoznačně obsahují důležité pojmy jako antivirové programy, firewall, zálohování dat, autorský zákon atd. Bohužel z pohledu této problematiky je poněkud nedostačující, že se stejné nebo alespoň podobné okruhy neobjevují již v RVP nebo poté v ŠVP. Takto se celá situace jeví tak, že žák, který nematuruje z Informatiky, je ochuzen o podstatné informace z hlediska bezpečnosti ICT.

4 Výzkumy související s problematikou

4.1 Jaké počítačové dovednosti mají české děti?

Dle zdrojů [26], [27].

Ve dnech 1. 3. – 30. 4. 2012 probíhal v České republice test IT dovedností IT Fitness, který nabízel zdarma všem zájemcům Dům zahraničních služeb v rámci kampaně Evropský týden počítačových dovedností 2012 – „European e-Skills Week 2012“. Hlavní cílovou skupinou byly základní a střední školy, ale i zájemci z řad široké veřejnosti. Test byl složený z 24 otázek zaměřen převážně na teoretické znalosti, praktické schopnosti a efektivitu vyhledání informací na internetu. Do kampaně se zapojilo celkem 841 základních a středních škol. Průměrná úspěšnost se pohybovala kolem 49,7%.

„Test ukázal, že čeští žáci a studenti se dobře orientují v otázkách bezpečnosti a etiky internetu (nejúspěšnější byla otázka týkající se pravidel zveřejňování informací na internetu) a jsou si vědomi nástrah virtuálního světa. Dobře dopadli i v oblasti teoretických znalostí, například v oblasti složení počítače, nebo jednotlivých programů a jejich funkcí (např.které zařízení je výstupní nebo k čemu slouží komprimační program). Největším problémem pro české žáky a studenty byly prakticky zaměřené úkoly, ve kterých museli pracovat např. s textovými editory, nebo ve kterých museli vyhledávat konkrétní informace na internetu, jako je vlakové spojení či autor obrázku“, říká k výsledkům testu Barbora Grečnerová z Domu zahraničních služeb.

Z pohledu informační bezpečnosti test obsahoval otázky z okruhu zveřejňování informací na internetu, převážně pak problematiku phishingu, hoax, pharmingu a dále také problematiky copyrightu.

Celý test je dostupný zde:
http://www.itfitness.cz/files/IT_Fitness_otazky_spravne_odpovedi_0.pdf

4.2 Jak škola chrání před počítačovým pirátstvím

Podobným výzkumem, jako je v této bakalářské práci, se zabývá Jan Lhoták taktéž ve své bakalářské práci z roku 2010 s názvem „Jak škola chrání před počítačovým pirátstvím.“[34]. V této práci se zabývá zejména problematikou autorských práv, softwarového pirátství, ochrany dat apod. Ve výzkumné části se zaměřuje na vědomosti a postoje žáků základních škol k této problematice, rozsah a kvalitu výuky informatiky a vliv bydliště a pohlaví na znalosti žáků. Získané informace porovnává a vyhodnocuje. Dále také analyzuje a hodnotí vybrané učebnice informatiky pro základní školy.

5 Teorie výzkumu

5.1 Metoda výzkumu

Pro potřeby této bakalářské práce z hlediska časového horizontu, jejího zpracovávání a typu sbíraných dat k realizaci výzkumu vzhledem k tématu a zaměření se jeví jako nejlepší možnost využít kvantitativní výzkum. Při kvantitativním výzkumu jsou sbírána pouze ta data, která výzkumník potřebuje, tzn. data související pouze s danou problematikou. Jednou z několika kvantitativních technik sběru dat je dotazníkové šetření.

Výhody kvantitativního výzkumu [28]:

- vyhnutí se rušivým proměnným, které by mohly výzkum ovlivnit
- relativně rychlý sběr dat
- efektivní a rychlé zpracování dat, které se dají zpracovat statisticky
- dosáhnutí celkem nezávislých výsledků vzhledem k autorovi výzkumu

5.2 Dotazník

Dotazníkové šetření je jeden z nástrojů kvantitativního výzkumu. Dotazník jako takový je nejběžnější možností při sběru dat při různých výzkumech. Jedná se vlastně o způsob psaného řízeného rozhovoru, kde tazatel vede rozhovor za pomocí série napsaných otázek, za jejichž pomoci získává fakta a názory respondentů. Avšak oproti rozhovorům osobním a jiným metodám, je dotazník o mnoho méně časově náročnější, lze ho totiž nechat vyplnit od více respondentů najednou. Realizace tohoto šetření není finančně nákladná a výsledky jsou snáze zpracovatelné. [29], [30]

Zásady při sestavování dotazníku [30], [31].

- určení hlavních cílů
- výběr skupin/y respondentů
- vytvoření logické vazby a návaznosti otázek
- vybrání správných typů otázek
- určení počtu otázek
- vyzkoušení dotazníku na malé skupině
- ponechaní dotazníku anonymním

5.3 Otázky v dotazníku

Dle zdroje [30].

5.3.1 Otevřené

Otázky otevřené dávají možnost otevřené odpovědi, kdy poskytnou odpovídajícímu větší prostor pro jeho vyjádření k otázce. Tudíž se z nich dá zjistit více informací a mohou poukázat na důležité vztahy a souvislosti. Tyto otázky mají možnost prohloubení do tématu. Mohou objasnit určité okolnosti, podnítit spolupráci tázaných a dosáhnout nečekaných odpovědí. Někdy může dojít k odpovědím, které dávají nový rozměr zkoumané oblasti a může tak dojít k novým mnohdy nečekaným poznatkům.

5.3.2 Uzavřené

Otázky uzavřené dávají jasné možnosti odpovědí, a to zejména mezi dvěma odpověďmi, např. ano – ne. v některých případech se dají využít i pro výběr více odpovědí, např. ano – nevím – ne. Uzavřené otázky jsou používány v případech, kdy nám stačí jednoznačné odpovědi. Tím se dosahuje větší jednotnosti a snadnějšího statistického zpracování. Tyto otázky mají však i své zápory, pro jejich povrchnost se nemohou dostat pod povrch odpovědi. Někdy

se stane, že tázaný neshledává žádnou odpověď jako vhodnou nebo zvolí alternativu, která se přesně neshoduje s jeho přesvědčením a názory. Tázaný také může zvolit odpověď pro zakrytí své nevědomosti.

5.3.3 Škálové

Otázky vynucující si škálové odpovědi jsou typické pro posuzování určité škály možností. Posuzovací škála neboli hodnotící stupnice se dá vyjádřit jako souhrn odpovědí, které mají za úkol popsat, posoudit, zhodnotit nebo jinak určit posuzovaný předmět či vlastnost. Tázaný vybere jednu z nabízených možností nejbližší jeho posudku. Nejčastěji se setkáme s hodnotící škálou např. „Líbil se Vám tento film?“ ano velmi – ano – nevím – ne – vůbec se mi nelíbil. Existují však i další možnosti většinou podobné známkování ve škole, kdy ohodnocujeme známkami 1-5, kde jednička zastupuje nejlepší a pětka nejhorší variantu. Škálové otázky mají pevně stanovené možné odpovědi, ze kterých si musí tázaný jednoznačně zvolit některý bod škály.

6 Výzkum výuky digitální bezpečnosti

6.1 Tvorba dotazníku

Dotazníkové šetření bylo vytvořeno na základě zadání práce. Po prostudování a pochopení dané problematiky počítačové bezpečnosti a kurikulárních dokumentů s důrazem na tuto problematiku ve výuce na základních a středních školách byl vytvořen dotazník, jehož hlavním obsahem jsou otázky z této problematiky. V tomto dotazníku jsou zahrnuta témata antivirové ochrany a firewallu, správné zálohy dat, obezřetného chování na Internetu, bezpečnosti hesel a autorského zákona.

Dotazník obsahuje celkem 20 otázek, které jsou tvořeny tzv. škálové otázkami, kde respondent vybírá svoji odpověď z hodnotící škály 1-5 od kladné přes neutrální až k záporné odpovědi a vyjádří tak nejblíže svůj postoj k otázce. Tyto otázky jsou doplněny otázkami tzv. výběrovými, kde student vybírá odpověď z nabízených možností. U těchto otázek jsou na výběr dvě až čtyři možnosti. U několika odpovědí na výběrové otázky je po studentovi vyžadováno upřesnění odpovědi pomocí místa pro poznámku, což kombinuje výběrovou otázku a otázku s krátkou odpovědí. Toto poskytuje daleko více prostoru pro sběr informací.

V prvních dvou otázkách se jedná o rozřazení studentů dle stupně vzdělání na základní a střední školy a také zjištění studovaného zaměření. Ve druhé části otázky 3-6 je dotazník zaměřen na otázky získávající informace o ochraně před viry, antiviry a firewallu. Další část, což jsou otázky 7-10, je věnována oblasti zálohování dat. Pod ní je uvedená část s otázkami 11-14, kde jsou otázky vztahující se k tématu bezpečnosti sociálních sítí a Internetu. Dále pak otázky 15-17 zohledňují bezpečnost hesel. Na závěr celého dotazníku je vyčleněn sektor pro otázky 18-20, které se týkají informací o autorském zákoně.

Celý dotazník je uveden v příloze této bakalářské práce.

6.2 Cíle

Hlavními cíli dotazníkového šetření jsou zjištění a ověření hloubky znalostí žáků a studentů zmiňovaných škol v dané problematice ICT. Dále schopnost využití znalostí v praxi, přístup a zájem studentů ke vzdělávání v oblasti počítačové bezpečnosti, uvědomování si rizik s tímto oborem spojených a vytvoření představy o vlivu výuky na znalosti žáků a studentů v těchto ohledech.

6.3 Cílová skupina

Na základě sestaveného dotazníku bylo zorganizováno dotazníkové šetření, jehož respondenty se stali čerství absolventi základních a středních škol. To znamená, že cílová skupina musela být rozdělena do dvou podskupin, kde první podskupinu tvoří absolventi základních škol, to pro šetření znamenalo oslovení studentů prvních ročníků středních škol. Druhá podskupina je tvořena z absolventů středních škol, tudíž bylo potřeba získat mezi respondenty studenty prvních ročníků vysokých škol.

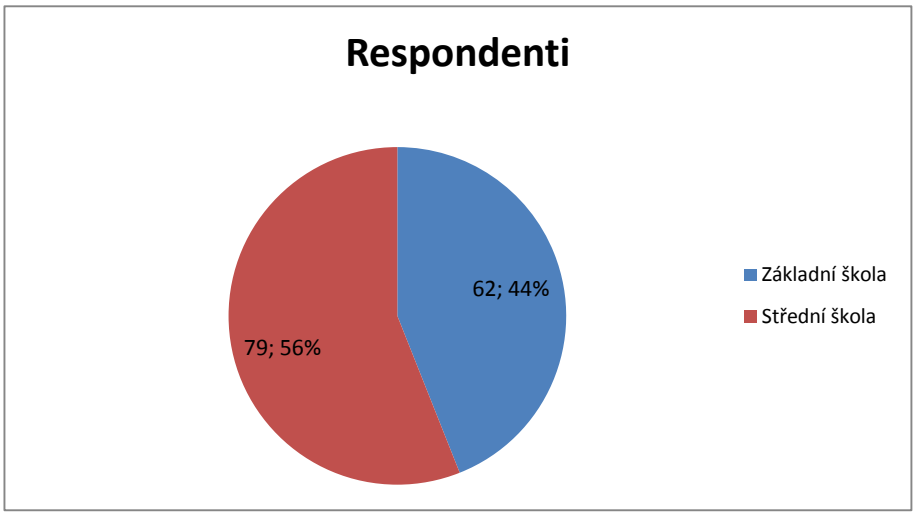
6.4 Metodika výzkumu

Sběr dat byl realizován během předchozího zimního semestru, tj. na podzim roku 2012. Respondenti byli osloveni za pomocí výše zmíněného dotazníku. Dotazník byl rozdán na několika místních středních a vysokých školách, jeho dotazovaní byli studenti prvních ročníků těchto škol. V šetření byla zachována naprostá anonymita všech respondentů a všem bylo sděleno, za jakým účelem dotazník vyplňují. Vyplněné dotazníky bylo potřeba roztřídit na dvě skupiny dle stupně ukončeného vzdělání dotazovaných.

6.5 Vyhodnocení výzkumu

6.5.1 Respondenti

Dotazníkového šetření se celkem zúčastnilo 141 respondentů. Z toho 62 respondentů byli čerství absolventi základních škol a zbylých 79 studentů byli absolventi škol středních.



Graf 1 - Počet respondentů

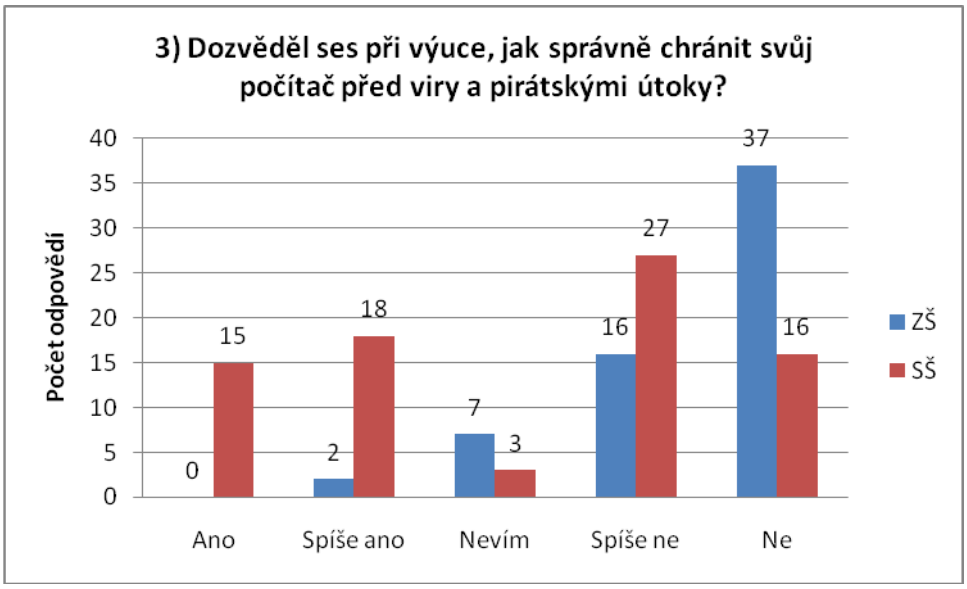
6.5.2 Zaměření školy

V následující tabulce jsou uvedeny informace o spektru zaměření respondenty studovaných škol. Dotazovaní žáci základních škol ve všech případech absolvovali výuku na klasických základních školách, tudíž se jim dostávalo všeobecně zaměřeného vzdělání. U žáků středních škol je obsaženo široké spektrum zaměření. Největší zastoupení mají studenti, kteří přišli na vysokou školu z obchodních akademií v počtu 20 následováni 14cti gymnazisty. Dále pak 9 studentů ze středních škol zaměřených na informační technologie a 8 se zaměřením elektrotechnickým. Dohromady tedy dobré procento studentů, kteří dle zaměření a typů škol, by měli mít dobré znalosti z oblasti ICT.

Škola	Zaměření	Počet	Procenta
Základní	Všeobecné	62	100 %
Střední	Obchodní akademie	20	25,32 %
	Gymnázium	14	17,72 %
	Informační technologie	9	11,39 %
	Elektrotechnické	8	10,13 %
	Stavební	7	8,86 %
	Podnikání	5	6,33 %
	Počítačové systémy	2	2,53 %
	Umělecké	2	2,53 %
	Cestovní ruch	2	2,53 %
	Automobilní	1	1,27 %
	Gastronomie	1	1,27 %
	Hotelnictví a turismus	1	1,27 %
	Mechanik a elektronik	1	1,27 %
	Oděvnictví	1	1,27 %
	Přírodovědné lyceum	1	1,27 %
	Slaboproud	1	1,27 %
	Dřevařství a nábytek	1	1,27 %
	Spoje a informatika	1	1,27 %
	Strojírenství	1	1,27 %

Tabulka 1 - Zaměření škol

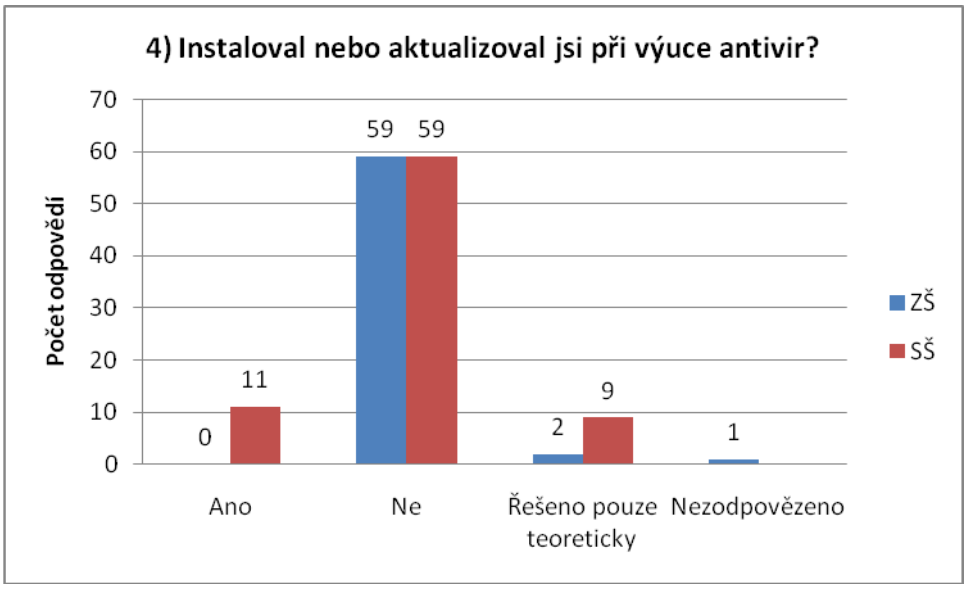
6.5.3 Ochrana počítače ve výuce



Graf 2 - Ochrana počítače ve výuce

Více jak polovina žáků základních škol uvedla, že se při výuce nedozvěděla, jak správně ochránit svůj počítač. Naopak nikdo nevybral možnost vyjadřující opak. Pouze 3 % žáků se přiklání k tomu, že se to spíše dozvěděli a zbytek žáků neví nebo se přiklání k záporné odpovědi. Co se týká studentů středních škol, zde jsou počty odlišné. 19 % žáků, což je zhruba necelá čtvrtina dotázaných, odpovědělo, že se ve výuce dozvědělo, jak svůj počítač chránit, naopak 20 % žáků si to nemyslí a dalších 34 % se k nim přiklání.

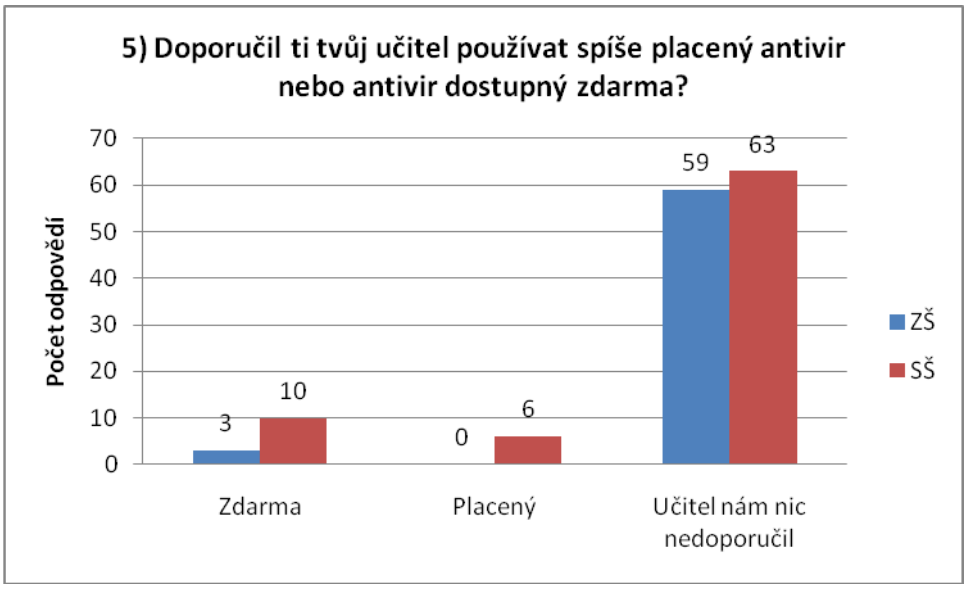
6.5.4 Instalace antiviru



Graf 3 - Instalace antiviru

Naprostá většina žáků a studentů ZŠ i SŠ odpověděla záporně. Pouze 14 % ze SŠ instalovalo nebo aktualizovalo antivirový program ve výuce. Dalších 11 % studentů střední školy a 3 % ze základní školy, uvedlo, že toto alespoň řešilo teoreticky. 1 žák otázku nezodpověděl.

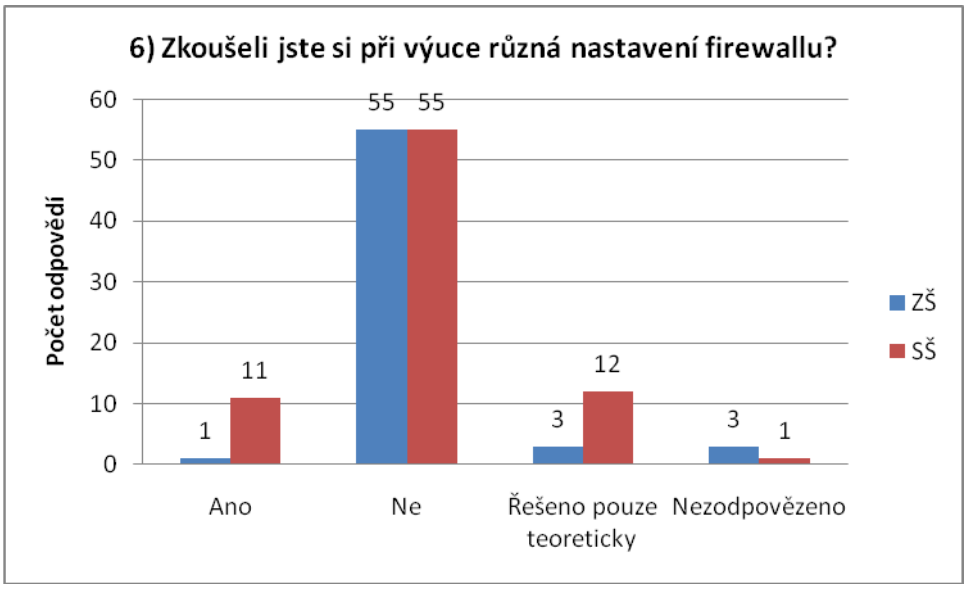
6.5.5 Doporučený antivirový program



Graf 4 - Doporučený antivirový program

U této otázky se většina žáků shodla na tom, že jim při výuce učitel nedoporučoval placený antivir, ale ani antivir dostupný zdarma. Pouze 5 % žáků základní školy a 13 % studentů školy střední uvádí, že jim vyučující doporučil antivir dostupný zdarma. Jen 8 % absolventů střední školy uvádí, že jim byl doporučen placený antivirový program.

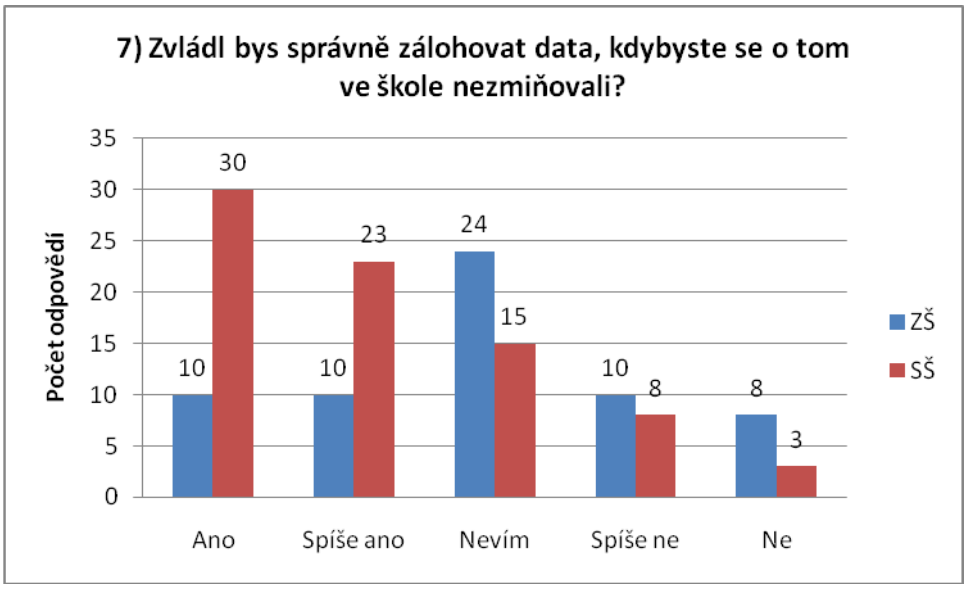
6.5.6 Nastavení firewallu



Graf 5 - Nastavení firewallu

88 % žáků ze ZŠ a 70 % studentů SŠ odpovědělo, že si ve výuce nezkoušeli různá nastavení firewallu. Jen 2 % žáků ZŠ a 14 % studentů SŠ uvedlo, že toto zkoušeli a další 5 % žáků a 15 % studentů řešilo firewall a jeho nastavení pouze teoreticky. 4 respondenti nezodpověděli otázku.

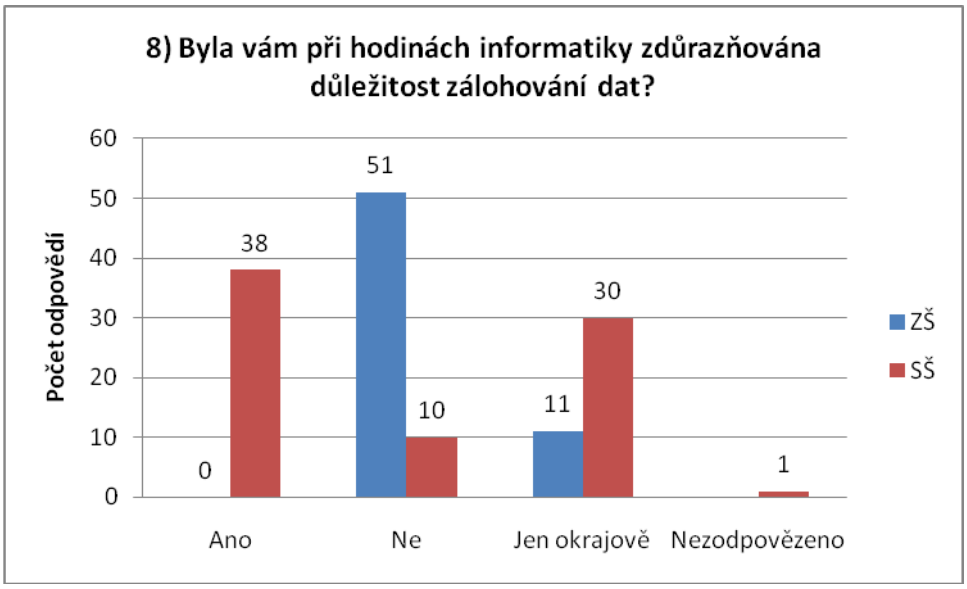
6.5.7 Zvládnutí zálohy dat



Graf 6 - Zvládnutí zálohy dat

Pokud mluvíme o záloze dat, 32 % žáků základní školy se přiklání k možnosti zvládnutí správné zálohy dat i bez zmiňování při výuce. Stejný názor má 67 % studentů škol středních. Zbytek respondentů neví či si nejsou úplně jisti. Minimální počet by zálohu bez školy nezvládl.

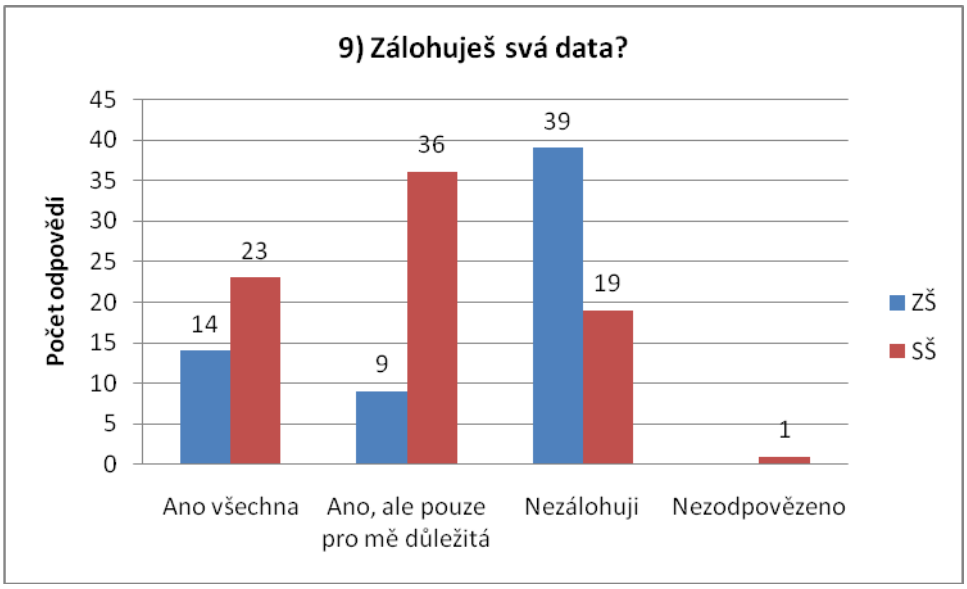
6.5.8 Důležitost zálohy dat



Graf 7 - Důležitost zálohy dat

Ze žáků základních škol ani jediný nepotvrdil, že mu byla ve škole zdůrazňována důležitost zálohování dat. Pouze 18 % žáků odpovědělo, že se o této problematice v hodinách učitelé částečně zmiňovali. Ostatní, tedy 82 % respondentů ze ZŠ, si při výuce důležitost zálohování nezdůrazňovali. U studentů ze středních škol je tomu jinak, naprostá většina se této problematice věnovala minimálně alespoň okrajově.

6.5.9 Záloha dat



Graf 8 - Záloha dat

Pouze přibližně jedna třetina žáků základních škol zálohuje svá data, ať už se jedná o důležitá nebo všechna data. Necelé dvě třetiny vůbec data nezálohují. Oproti tomu středoškoláci si svých dat váží o poznání více. Celkem 75 % studentů si svá data zálohuje. Zbytek studentů data nezálohuje a jeden respondent otázku nezodpověděl.

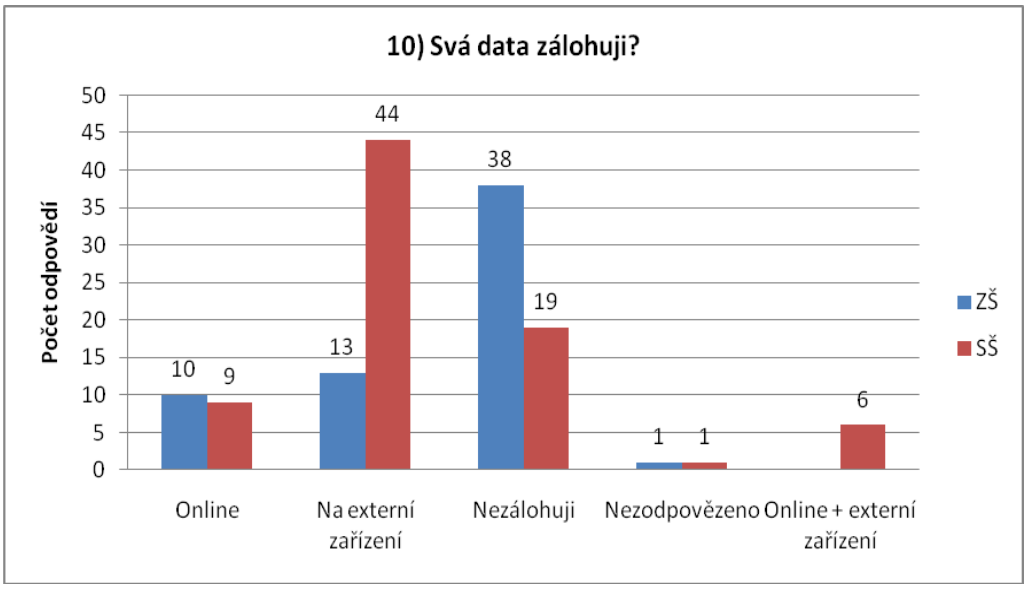
	ZŠ	SŠ
Školní dokumenty	1×	19×
Dokumenty mimo školu	-	10×
Fotografie	3×	12×
Pracovní záležitosti	-	3×
Videa, filmy, seriály	-	4×

Tabulka 2 - Předměty zálohy

V této otázce při odpovědi, kde žák uvádí, že zálohuje data jen pro něj důležitá, byla možnost zodpovězení, jaká data jsou pro žáky důležitá.

Z předchozí tabulky je jasné, že nejvíce si respondenti zálohují dokumenty související se školou, dále si nejvíce cení svých fotografií a ostatních dokumentů.

6.5.10 Typ zálohy dat



Graf 9 - Typ zálohy dat

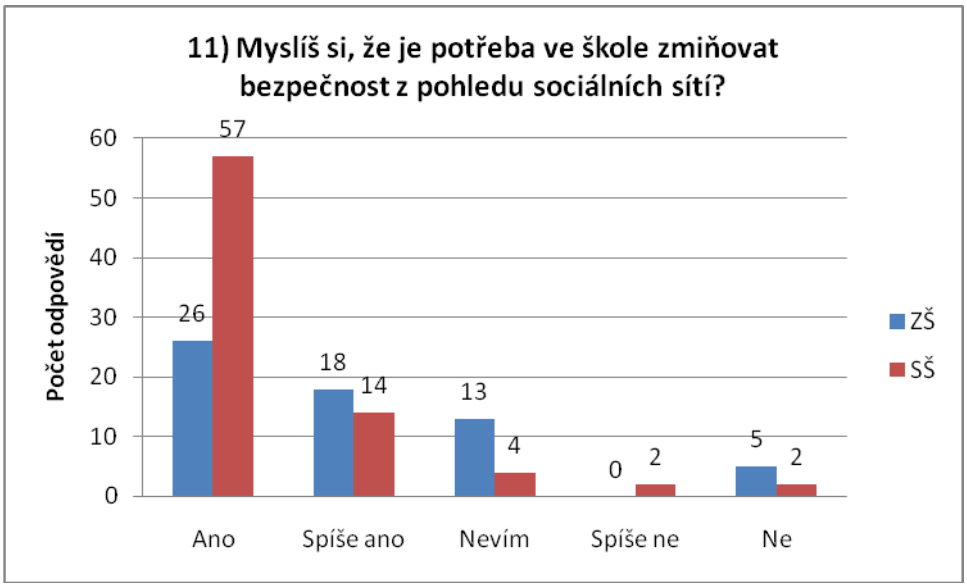
Nadpoloviční většina přesněji 61 % žáků základních škol svá data nezálohuje, což vyplývá i z otázky číslo 9. Online zálohuje 16 % žáků a 21 % používá pro zálohu externí zařízení. Ze studentů středních škol nezálohuje 24 % respondentů, 56 % zálohuje na externí zařízení, 11 % online a 8 % zálohuje online i na externí zařízení.

V této otázce u odpovědi „zálohuji na externí zařízení“, měli žáci a studenti možnost také odpovědět, na jaké zařízení zálohují. V největším počtu případů zálohují na jiné disky, z nichž naprostá většina zálohuje na disky externí. Dále jsou k zálohování oblíbené flash disky, zejména mezi žáky základních škol.

	ZŠ	SŠ
HDD	2×	31×
Flash disk	6×	13×
DVD	2×	5×
CD	1×	4×

Tabulka 3 - Uložiště pro zálohu dat

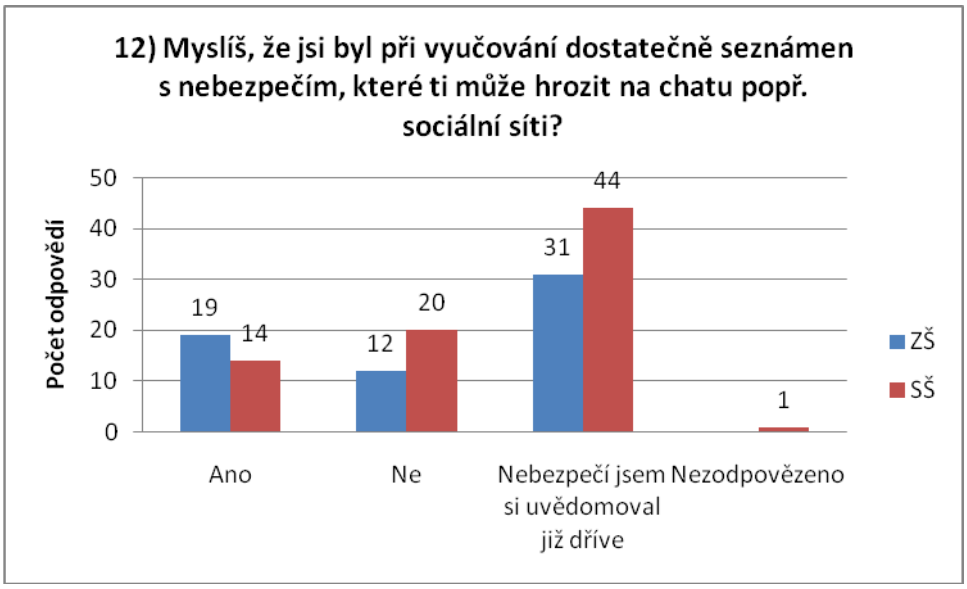
6.5.11 Bezpečnost sociálních sítí



Graf 10 - Bezpečnost sociálních sítí

Celkem 42 % žáků ZŠ si myslí a dalších 29 % se k tomu spíše přiklání, že je potřeba zmiňovat při výuce bezpečnost sociálních sítí. Dalších 21 % neví a 8 % žáků je proti. Podobného názoru jsou studenti středních škol, z nichž dokonce 72 % odpovědělo, že je zapotřebí zmiňovat bezpečnost z pohledu sociálních sítí a pouze 3 % byli přímo proti.

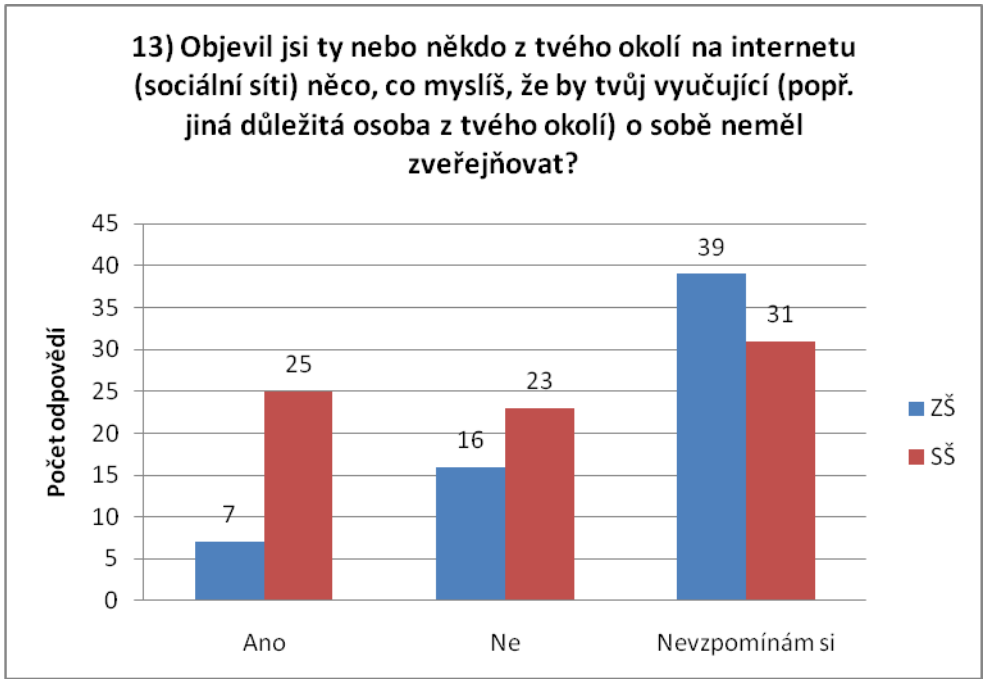
6.5.12 Nebezpečí sociálních sítí



Graf 11 - Nebezpečí sociálních sítí

Z 62 žáků základních škol, kteří vyplnili dotazník, si přesně celých 50 % z nich myslí, že si nebezpečí spojené se sociálními sítěmi uvědomovali již předtím, než se o tom zmiňovali ve škole, pokud se ovšem těmto žákům seznámení s touto problematikou dostalo. Podobný názor mají i studenti středních škol, kterých shodně odpovědělo 56 %. Naopak 31 % žáků ZŠ a 18 % studentů SŠ si myslí, že byli v tomto ohledu dostatečně poučeni. Zbytek žáků si myslí opak.

6.5.13 Údaje důležitých osob



Graf 12 - Údaje důležitých osob

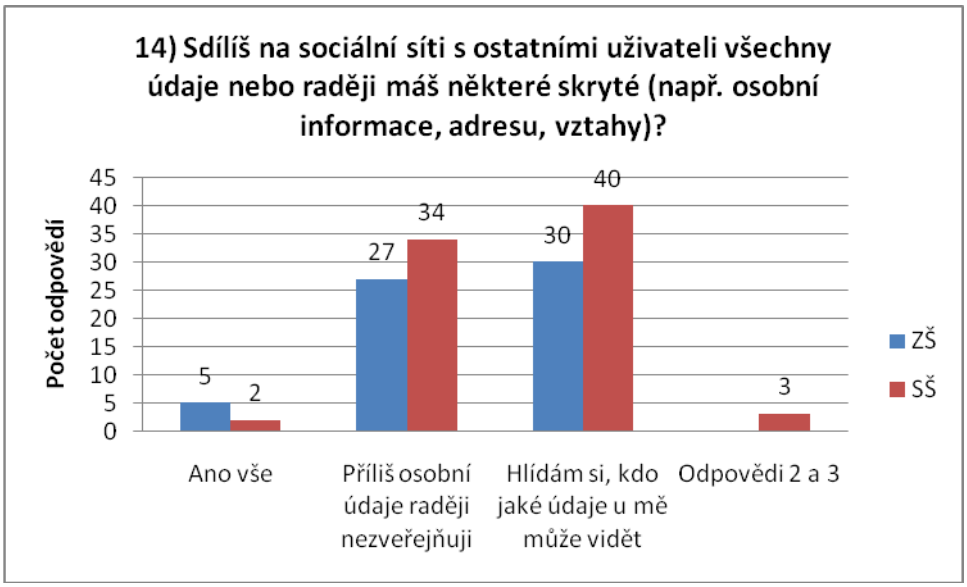
U této otázky velké množství z obou dotazovaných skupin zvolilo třetí možnost odpovědi, a to, že si nevzpomínají, zda objevili na nějakou důležitou osobu něco nevhodného. V ostatních dvou případech odpovědí jsou jejich počty vcelku vyrovnané. Jen u žáků základních škol převládá odpověď, že na nikoho důležitého nic nevhodného na Internetu neobjevili.

Respondenti, kteří si vzpomněli na nějakou věc a odpověděli na otázku kladně, měli možnost připsat, o co se přesně jednalo. Bohužel této možnosti nevyužili všichni. Nejčastěji nacházeli adresu, osobní údaje, telefonní kontakt, fotografie, a to dokonce i intimní. Výjimkou však nejsou ani bankovní údaje nebo přesný údaj o nepřítomnosti v bydlišti.

	ZŠ	SŠ
Adresa	3×	3×
Osobní údaje	1×	4×
Osobní tel. kontakt	1×	3×
Fotografie	-	2×
Bankovní údaje	-	2×
Údaje o nepřítomnosti v bydlišti	-	2×
Údaje, kde se právě nachází	-	1×
Informace o vztazích	-	1×
Velmi osobní statusy	-	1×

Tabulka 4 - Nejčastější údaje

6.5.14 Sdílení informací

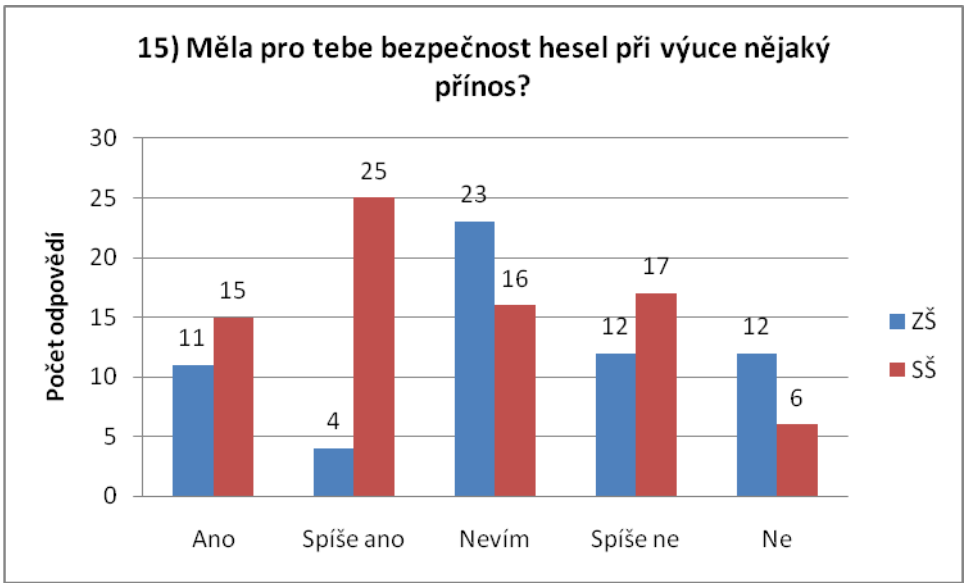


Graf 13 - Sdílení informací

Jen několik jedinců v této otázce zodpovědělo, že sdílí všechny své údaje s ostatními uživateli. Převážná většina tedy příliš osobní informace raději

nezveřejňuje, a pokud ano, tak si dávají pozor, kdo by se k těmto informacím mohl dostat. 4 % dotázaných středoškoláků dokonce uvedlo obě možnosti naráz.

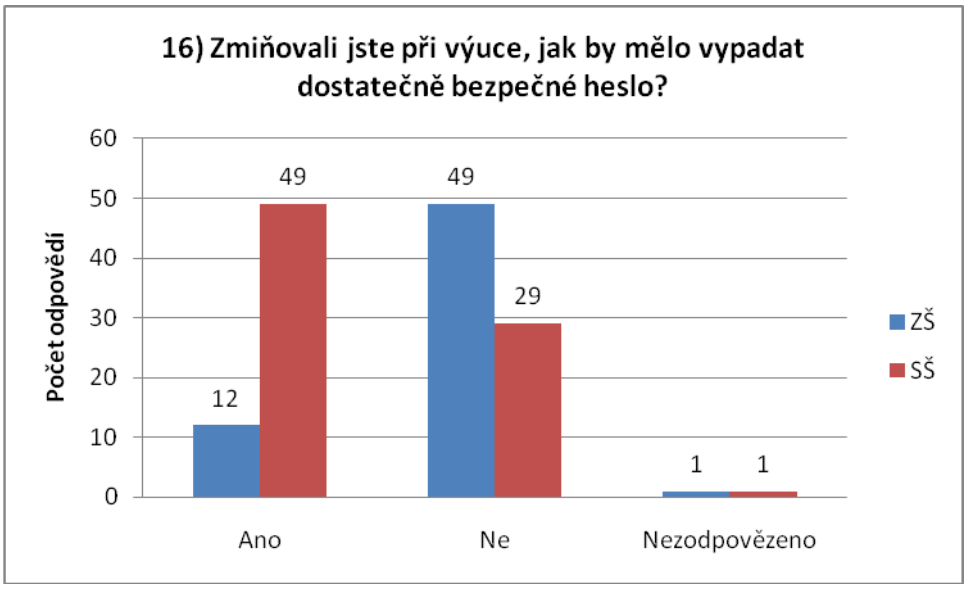
6.5.15 Bezpečnost hesel při výuce



Graf 14 - Bezpečnost hesel při výuce

V širokém spektru odpovědí v této otázce převládá u žáků základních škol odpověď „nevím“, kterou uvedlo 37 % jedinců. Další žáci se mírně přiklánějí k tomu, že bezpečnost hesel ve výuce pro ně neměla přínos. Naopak pro 51 % respondentů ze střední školy mělo toto téma přínos, 20 % neví a 29 % zodpovědělo, že problematika bezpečnosti hesel ve výuce pro ně přínos neměla.

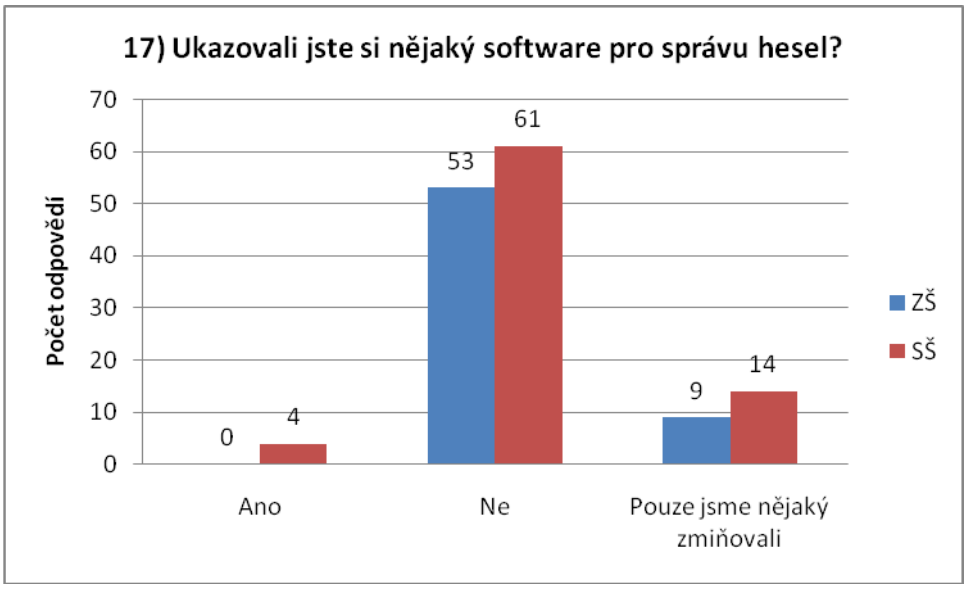
6.5.16 Bezpečné heslo



Graf 15 - Bezpečné heslo

Jak by mělo vypadat dostatečně silné heslo, se na základní škole nedozvědělo 80 % žáků. Oproti tomu na střední škole je vidět značný rozdíl, kde se naopak celých 62 % studentů o tom, jak by mělo vypadat správné a silné heslo, dozvědělo.

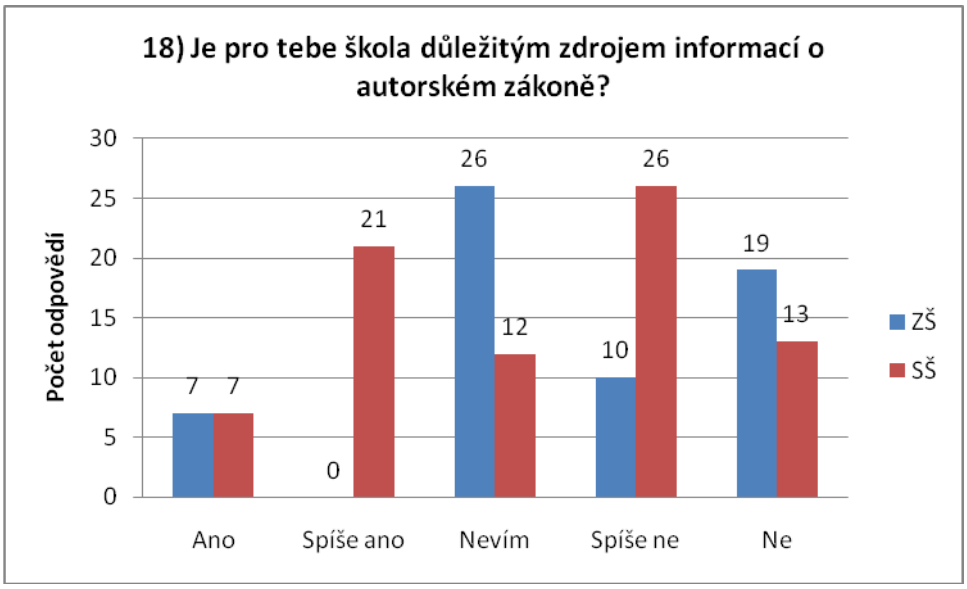
6.5.17 Software pro správu hesel



Graf 16 - Software pro správu hesel

Jednoznačná většina ze všech dotazovaných zodpověděla, že si při výuce neukazovali žádný software pro správu hesel. Pouze 5 % studentů střední školy odpovědělo, že si software ukazovali a zbytek žáků a studentů uvádí, že se alespoň o nějakém softwaru pro správu bezpečnostních hesel při výuce zmiňovali, a to v 15 % případů na ZŠ a v 18 % na SŠ.

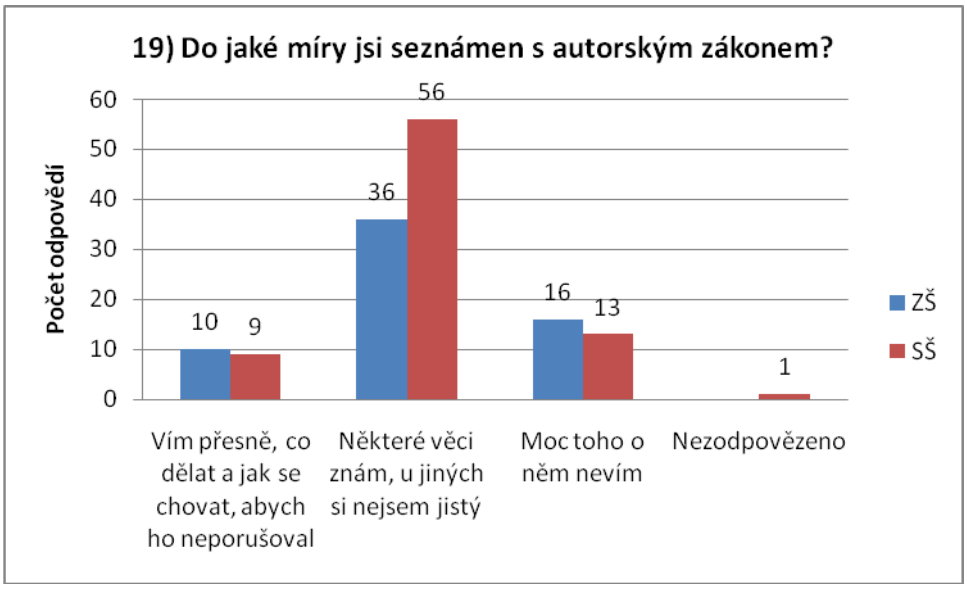
6.5.18 Zdroj informací o autorském zákoně



Graf 17 - Zdroj informací o autorském zákoně

V celkovém hodnocení této otázky si pouze 11 % žáků ze základních škol myslí, že pro ně byla škola důležitým zdrojem informací o autorském zákoně, 42 % žáků neví a zbylých 47 % se přiklání k tomu, že spíše nebyla nebo vůbec nebyla škola přínosným zdrojem informací v tomto ohledu. Podobně na tom jsou i studenti středních škol pouze s výjimkou toho, že místo odpovědi „nevím“ se přikláněli k tomu, že škola spíše byla zdrojem informací o autorském zákoně.

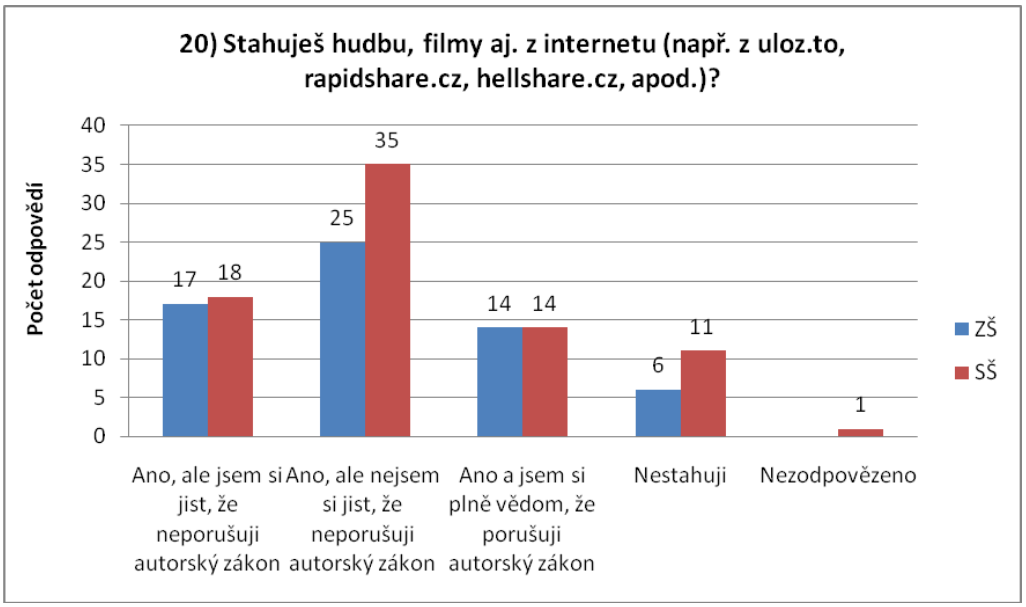
6.5.19 Seznámení s autorským zákonem



Graf 18 - Seznámení s autorským zákonem

16 % žáků ze základních škol a 11 % ze škol středních si je naprosto jistých, že ví, jak se chovat, aby tento zákon neporušovali. Dále 58 % žáků a 71% studentů přiznává, že něco znají, ale u všeho si nejsou moc jistí. Naopak 26 % a 17 % jedinců říká, že toho o autorském zákoně moc neví. Jeden člověk otázku nezodpověděl.

6.5.20 Stahování



Graf 19 - Stahování

Tato poslední otázka dokazuje, že většina respondentů stahuje své oblíbené skladby a filmy z Internetu. 27 % žáků a 23 % studentů si je jistých, že stahováním z uvedených a podobných serverů neporušuje autorský zákon. 40 % žáků se základním a 44 % se středním vzděláním si nejsou zcela jisti, zda zákon neporušují. Dále 23 % žáků a 18 % studentů stahují i přes vědomí, že porušují autorský zákon. 10 % žáků ZŠ a 14 % ze SŠ odpovědělo, že nestahují.

6.6 Vyhodnocení výzkumu

6.6.1 Ochrana počítače, antivirové programy a firewall

Pokud se zaměříme na základní školy, tak přímo v rámcově vzdělávacím programu není tato problematika zakotvená. Ovšem v některých školních vzdělávacích programech dle [18] a [21] jsou antivirové programy a hrozba počítačového viru zmíněny. Budeme-li vycházet z výše uvedeného šetření, tak situace není nikterak dobrá. Naprostá většina dotázaných se při výuce spíše nedozvěděla nebo vůbec nedozvěděla, jak správně chránit svůj počítač. Dále ve

škole všichni žáci kromě třech nezkoušeli ve výuce instalovat nebo aktualizovat antivirový program a stejnému počtu se nedostalo doporučení, zda je lepší používat placený software na ochranu dat nebo software dostupný zdarma. Podobný počet, tedy bez několika všichni žáci, se nesetkal s možnostmi firewallu.

U středních škol podobně jako u škol základních se v RVP nevyskytují potřebné informace k tomuto tématu. Zlepšovat to mohou ŠVP, ve kterých se pojmy viru, antivirové ochrany a firewallu objevují například v [23], [24] a [25]. O mnoho lépe je tato problematika uvedena v požadavcích k maturitám, kde student musí tyto pojmy s porozuměním používat a dokázat se orientovat v této problematice. Tyto skutečnosti nic nemění na výsledcích šetření, které nám říkají, že oproti základním školám dosahují středoškoláci pouze mírného zlepšení. Necelá polovina respondentů se ve škole dozvěděla, jak chránit svůj počítač před viry a pirátskými útoky. Jen zhruba jedna čtvrtina studentů ve vyučování instalovala nebo aktualizovala antivirový software a pracovala s firewallem, stejnému počtu byl doporučován tento software, ať šlo o ten zdarma či placený.

Tyto nedobré výsledky v obou případech lze částečně přisuzovat právě opomíjení počítačové bezpečnosti v RVP, jejímu neúplnému či špatnému zakotvení ve ŠVP. Dále slabým hodinovým dotacím v případě základních škol a také neadekvátnímu přístupu škol k této problematice a špatným přístupům vyučujících.

6.6.2 Zálohování dat

Toto téma je v RVP i ve výše uvedených ŠVP pro základní vzdělávání zcela opomenuto. Bohužel tomu odpovídají i výsledky šetření. Dozvěděli jsme se, že třetina odpovídajících žáků by zvládla správně zálohovat svoje data i bez přičinění školy. Dále ale z výzkumu vyplývá, že přibližně 4 z 5 žáků nebyla důležitost zálohování při vyučování vůbec zmiňována a zbylým žákům pouze

částečně. Z toho může plynout zjištěný údaj, kdy svá data zálohuje pouze něco málo přes třetinu respondentů. Pokud již data zálohují, tak fotografie a zálohují je převážně na usb flash disky.

O poznání lépe jsou na tom studenti ze středních škol, kdy sice v RVP záloha dat není uvedena, ale v ŠVP a v požadavcích k maturitě se ochrana a záloha dat objevuje. Což by mohlo do jisté míry ovlivnit výzkum, ve kterém zhruba 7 z 10 studentů uvedlo, že by dokázalo správně zálohovat data i přes zdůrazňování důležitosti zálohy při vyučování. Toto téma bylo při výuce zdůrazňováno alespoň okrajově v 8 z 10 případů, z čehož se poučili přibližně 3 ze 4 studentů, kteří uvedli, že svá data zálohují. Nejvíce se obávají o ztrátu dokumentů spojených se školní výukou, dále pak o fotografie a jiné dokumenty. Zřejmě z důvodu větších objemů svých dat používají nejčastěji pro zálohu pevné disky, a to zejména ty externí.

6.6.3 Bezpečnost Internetu a sociálních sítí

Bezpečnost internetu zejména pak sociálních sítí se snadno může stát podceňovanou sférou výuky počítačové bezpečnosti. Ve vzdělávacích programech pro ZŠ se toto téma zdá být uvedeno pod pojmy „bezpečnost práce na internetu“ či „zaujetí zodpovědného přístupu k nevhodným obsahům se zde vyskytujících“, u středního vzdělávání pod pojmem „možná nebezpečí Internetu“. Nedá se však posoudit, zda se dá toto téma pod tyto pojmy zcela jistě zařadit. Proto je těžké posoudit, zda jsou žáci a studenti v tomto ohledu dostatečně vzděláváni nebo jejich znalosti ovlivňují do jisté míry i různé informačně-vzdělávací projekty jako např. bezpecnyinternet.cz [9] nebo další podobné projekty. Každopádně dvě třetiny žáků základních škol a bezmála všichni dotázaní studenti škol středních si myslí, že je potřeba ve výuce zmiňovat bezpečnost sociálních sítí. To by mohla být skutečnost, že si děti a dospívající lidé uvědomují rizika s tímto tématem spojené. Polovina žáků ZŠ

odpovědělo, že si tento druh nebezpečí uvědomovala již dříve bez ohledu na výuku. U studentů SŠ se jednalo o několik lidí nad polovinu.

Zajímavé je, že 1 z 10 žáků a 3 z 10 studentů objevili na Internetu či sociální síti nějaký nevhodný materiál týkající se učitele popř. jiné důležité osoby. Zejména se jednalo o přesnou adresu, osobní telefonní kontakt a nevhodné fotografie. Z toho plyne, že pokud děti vyhledávají nějaké informace o někom jiném, mohly by si uvědomit, že to, co samy zveřejňují, může být také nevhodné nebo nebezpečné. Dále je to poučení pro učitele a další dospělé osoby, že se jejich osobní informace mohou snadno dostat mezi žáky a studenty, což může mít neblahý dopad nejen pro jejich reputaci a autoritu.

U sdílení osobních informací na sociálních sítích byli všichni dotázaní velice opatrní a v naprosté většině případů odpovídali, že příliš osobní údaje raději nezveřejňují nebo si hlídají, kdo by jaké údaje mohl zjistit. Lepší variantou je raději údaje nezveřejňovat, jelikož nikdy si nemůžeme být jisti, kdo se k nim doopravdy dostane. Tu však zvolilo o několik žáků méně. Povzbudivé je, že žáci alespoň o tomto přemýšlejí a uvědomují si, že není dobré své osobní informace zpřístupnit komukoliv.

6.6.4 Bezpečnost hesel

Pro základní vzdělávání je bezpečnost hesel uváděna ve zmiňovaných školních vzdělávacích programech. Ale jen jeden z pěti žáků se při výuce dozvěděl, jak by mělo vypadat dostatečné silné heslo a necelých 15 % si zmiňovalo software pro správu hesel. Pouhá polovina z těchto nízkých počtů pak dále shledává bezpečnost hesel ve výuce jako přínosnou. Vzniká zde tedy zvláštní situace, kdy někteří zbylí žáci uvádějí toto téma ve výuce jako přínosné, ale dále odpovídají, že již nezmiňovali, jak má vypadat správné a silné heslo. Jedná se o několik jedinců, může to být tedy způsobeno špatným přístupem ve výuce, kdy mohl vyučující vysvětlit, že jsou hesla důležitá, ale

opomněl uvedení příkladu některých hesel nebo způsobu, jak takové heslo vytvořit. Může se jednat ale i o nepochopení otázky či zapomenutí žáků, co vlastně doopravdy ve škole o tomto tématu probírali.

Ve středoškolském vzdělávání se ve vzdělávacích programech problematika hesel přímo neobjevuje, ale v požadavcích k maturitě už ano. Šetření ukázalo, že o bezpečném hesle se dozvěděly ve škole přibližně dvě třetiny respondentů, ale pouze jednomu z pěti byly zmiňovány některé softwarové nástroje pro správu těchto hesel. Dále plyne, že pokud si studenti ve škole říkali, jak vypadá silné heslo, ukazovali si nebo zmiňovali nějaký software pro jeho správu, zároveň ve většině případů hodnotili bezpečnost hesel při výuce jako spíše přínosnou nebo zcela přínosnou. To poukazuje na skutečnost, že pokud se studenti nedozvěděli, jak vypadá správné a silné heslo, hodnotili bezpečnost hesel ve škole jako nepřínosnou. To znamená, že ti respondenti, pro které toto téma nemělo přínos, v něm nemuseli být řádně vzděláváni a nedozvěděli se základní informace. Tento problém může částečně již kořenit v nezačlenění tohoto tématu v RVP či ŠVP. Ale také zřejmě většina škol a vyučujících může toto téma brát jako zcela nedůležité pro výuku. Poté ale mohou vznikat ty situace, kdy nejběžnějším heslem je „heslo“ nebo nějaká číselná kombinace např. „1,2,3,4,5“ či jiná snadno odhalitelná hesla [33].

6.6.5 Autorský zákon

Z výše vybraných bezpečnostních hledisek je zřejmě autorský zákon jediný, který je ať už nepřímo nebo přímo zakotven ve všech zde uvedených vzdělávacích programech a u požadavků k oběma stupňům maturit. Proto by měla být škola hlavním zdrojem informací o tomto zákoně pro žáky a studenty. Jak ale dokazuje výzkum, není to tak úplně pravda. Pro zhruba polovinu žáků základních škol není škola důležitým zdrojem znalostí o autorském zákoně a necelá druhá polovina neví, zda se přiklonit k těmto žákům nebo k žákům, pro které škola důležitým zdrojem je. Ale dále více než dvě třetiny žáků

potvrzují, že minimálně některé znalosti mají a nejsou si však ve všem úplně jistí. Různou úroveň znalostí autorského zákona potvrdilo i šetření poslední znalostní otázkou, kde se ukázalo, že necelá třetina disponuje alespoň základními znalostmi. U zbytku žáků není možné jednoznačně určit rozsah znalostí v tomto ohledu, jelikož si ve svých odpovědích nejsou jistí nebo odpovídají špatně.

V případě škol středních dosahovali studenti podobných výsledků jako žáci škol základních, rozdílné snad jen bylo, že více žáků zvolilo místo odpovědi „nevím“, odpověď, ze které je zřejmé, že je pro ně spíše škola důležitým zdrojem informací o autorském zákoně. A část počtu, o který převyšují respondenti ze středních škol ty ze škol základních, se spíše přiklonila k neutrálním odpovědím, ze kterých plyne, že něco znají, ale nejsou si zcela jisti, což zase potvrzuje poslední otázka průzkumu. U této části výzkumu mohlo dojít k částečnému zkreslení výstupních dat, jelikož žáci a studenti mohli okrajově svou nevědomost zakrývat odpovědí typu: „vím, ale u některých věcí si nejsem jist“.

7 Závěr

Hlavní cíle této bakalářské práce byly splněny. Práce obsahuje úvod do problematiky digitální bezpečnosti s charakteristikou jednotlivých oblastí. Dále je zde zohledněn obsah vzdělávacích programů České republiky z pohledu dané problematiky.

Za pomocí dotazníkové šetření byly zjištěny a vyhodnoceny znalosti žáků a studentů základních a středních škol. Zejména pak schopnost využití znalostí v praxi, přístup a zájem žáků ke vzdělávání v oblasti počítačové bezpečnosti a uvědomování si rizik spojených s tímto oborem. Vše bylo porovnáno se vzdělávacími dokumenty a patřičně zhodnoceno.

Vybrané poznatky z této práce byly prezentovány v rámci 19. ročníku konference s mezinárodní účastí o vyučování informatiky DidInfo 2013 v Banské Bystrici.

Další oblastí v návaznosti na tuto práci, na které je možné se v jiném rozsáhlejším výzkumu zaměřit, je například rozsáhlá analýza školních vzdělávacích programů z hlediska problematiky výuky digitální bezpečnosti. Popřípadě průzkum klíčových kompetencí učitelů informačních technologií vzhledem k této problematice.

Literatura

[1] RYCHNOVSKÝ L. Počítačová bezpečnost. Zpravodaj ÚVT MU. ISSN 1212-0901, 2005, roč. XVI, č. 1, s. 13-16.

[2] MATYSKA L. Bezpečnost na Internetu. Zpravodaj ÚVT MU. ISSN 1212-0901, 2002, roč. XII, č. 4, s. 1-5.

[3] KROPÁČOVÁ. Uživatel a počítačová bezpečnost. Zpravodaj ÚVT MU. ISSN 1212-0901, 2006, roč. XVI, č. 3, s. 16-20.

[4] SECHLER, J. A Young Adult's Guide to Safety in the Digital Age. CreateSpace, 2010. ISBN 978-1453618414.

[5] HORÁK, Jaroslav. Bezpečnost malých počítačových sítí (praktické rady a návody). 1. vyd. Praha: Grada, 2003, s. 64-69. ISBN 80-247-0663-6.

[6] DOSEDĚL, Tomáš. Počítačová bezpečnost a ochrana dat. Vyd. 1. Brno: Computer Press, 2004, s. 61-62. ISBN 80-251-0106-1.

[7] STREBE, Matthew a Charles PERKINS. Firewally a proxy-servery. Vyd. 1. Brno: Computer Press, 2003. ISBN 80-7226-983-6.

[8] SALVET Z., MATYSKA L. Zálohování dat v METACentru. Zpravodaj ÚVT MU. ISSN 1212-0901, 2000, roč. X, č. 5, s. 1-3.

[9] BEZPEČNÝ INTERNET. Bezpečný internet: Rady pro vaši bezpečnost na internetu [online]. 5.2.2012 [cit. 2013-03-14]. Dostupné z: <http://www.bezpecnyinternet.cz/>.

[10] Zákon č. 121/2000 Sb., o právu autorském, o právech souvisejících s právem autorským. In: Sbírka zákonů č. 398/2006. 2006, 126. Dostupné z: <http://www.mkcr.cz/assets/autorske-pravo/01-3982006.pdf>.

[11] Filmy nejsou zadarmo [online]. 2006 [cit. 2013-03-14]. Co je autorské právo. Dostupné z WWW:< http://www.filmynejsouzadarmo.cz/cs/co-je-autorske-pravo/>.

[12] LUKEŠ, Dan. HTTPS - bezpečnost jen pro vyvolené?. In: *Lupa.cz* [online]. 2001 [cit. 2013-04-20]. Dostupné z: <http://www.lupa.cz/clanky/https-bezpecnost-jen-pro-vyvolene/>.

[13] JEŘÁBEK, J. a kol. Rámcový vzdělávací program pro gymnázia RVP G. Praha: Výzkumný ústav pedagogický, 2007. Dostupný z WWW: <old.rvp.cz/soubor/RVP_G.pdf>. ISBN 978-80-8700-11-3.

[14] JEŘÁBEK, J. a kol. Rámcový vzdělávací program pro základní vzdělávání. Praha: Výzkumný ústav pedagogický, 2007. Dostupný z WWW:< http://rvp.cz/informace/wp-content/uploads/2009/09/RVPZV_2007-07.pdf >.

[15] Katalog požadavků zkoušek společné části maturitní zkoušky: Informatika, základní úroveň obtížnosti [online]. Centrum pro zjišťování výsledků vzdělávání, 2010 [cit. 2012-04-07]. Dostupné z WWW: <http://www.novamaturita.cz/index.php?id_document=1404034533&at=1>.

[16] Katalog požadavků zkoušek společné části maturitní zkoušky: Informatika, vyšší úroveň obtížnosti [online]. Centrum pro zjišťování výsledků vzdělávání, 2010 [cit. 2012-04-07]. Dostupné z WWW: <http://www.novamaturita.cz/index.php?id_document=1404034534&at=1>

[17] MANĚNOVÁ, Martina. *ICT a učitel 1. stupně základní školy*. 1. vyd. Česko: Martina Maněnová, 2009, 112 s. ISBN 978-80-254-7531-7.

[18] ZÁKLADNÍ ŠKOLA LIPENEC, okres Louny. *Školní vzdělávací program pro základní vzdělávání*. Lipenec, 2007. Dostupné z: <http://www.zs-lipenec.eu/dokumenty/SVP 2010_11.doc> .

[19] JEŘÁBEK, J. a kol. Manuál pro tvorbu školních vzdělávacích programů v základním vzdělávání. Praha: Výzkumný ústav pedagogický, 2005. Dostupný z WWW: <http://clanky.rvp.cz/wpcontent/upload/prilohy/6631/1_manual_pro_tvorbu_skolnich_vzdelavacich_programu_v_zakladnim_vzdelavani.pdf>.

[20] *Národní program rozvoje vzdělávání v České republice: Bílá kniha*. 1. vyd. Praha: Ústav pro informace ve vzdělávání, 2001, 98 s. ISBN 80-211-0372-8.

[21] GYMNÁZIUM ČESKÁ A OLYMPIJSKÝCH NADĚJÍ. *Školní vzdělávací program pro základní vzdělávání*. České Budějovice, 2012. Dostupné z: <http://www.gymceon.cz/docs/documents/12-SVP-RVP-ZV-2012-2013-zari.pdf>.

[22] DOLEŽALOVÁ, Olga. *Manuál pro tvorbu školních vzdělávacích programů na gymnáziích*. Praha: Výzkumný ústav pedagogický v Praze, c2007, 140 s. ISBN 978-808-7000-137. Dostupný z WWW: <http://clanky.rvp.cz/wp-content/upload/prilohy/9643/manual.pdf>.

[23] GYMNÁZIUM ČESKÁ A OLYMPIJSKÝCH NADĚJÍ. *Školní vzdělávací program pro gymnázia*. České Budějovice, 2012. Dostupné z: <http://www.gymceon.cz/docs/documents/vzdelavaci_program_gym.pdf>.

[24] GYMNÁZIUM OLOMOUC – HEJČÍN. *Školní vzdělávací program pro gymnaziální vzdělávání*. Olomouc – Hejčín. 2009. Dostupný z WWW: <http://www.gytool.cz/soubory/skolni-vzdelavaci-program.pdf>.

[25] GYMNÁZIUM PÍSEK. *Školní vzdělávací program pro čtyřleté gymnázium a vyšší stupeň osmiletého gymnázia*. Písek, 2009. Dostupný z WWW: <http://www.gymna-pi.cz/files/VP%20%C4%8Dty%C5%99let%C3%A9%20a%20vy%C5%A1%C5%A1%C3%AD%20osmilet%C3%A9.pdf>.

[26] JIŘIČKA, Jan. Nástrahy webu čeští žáci znají, najít informace jim však dělá problém. In: HUDÁK, Luděk. *Digitální žurnalistika na příkladu iDnes* [online]. Brno: [s.n.], 2001 [cit. 2013-04-20]. Dostupné z: <http://zpravy.idnes.cz/cesti-zaci-maji-problem-s-hledanim-informaci-na-internetu-pza-/domaci.aspx?c=A120208_134158_domaci_jj>.

[27] Čeští žáci mají dobré teoretické znalosti práce s počítači, ale pokulhávají v praxi. *IT Fitness* [online]. Praha, 2012 [cit. 2013-04-20]. Dostupné z: http://www.itfitness.cz/node/105451

[28] HENDL, Jan. *Kvalitativní výzkum: základní metody a aplikace*. Vyd. 1. Praha: Portál, 2005. 407 s. ISBN 8073670402.

[29] *Dotazník - online: ...jak na dotazník* [online]. 2007 [cit. 2012-02-10]. Dostupné z WWW: <http://www.dotaznik-online.cz/>.

[30] Prof. PhDr. Rudolf Kohoutek, CSc. *Dotazník jako průzkumná metoda* [online]. 2010, 10. února 2010 [cit. 2013-04-03]. Dostupné z: <http://rudolfkohoutek.blog.cz/1002/dotaznik-jako-pruzkumna-metoda>.

[31] DEMČÁK, Marek. Jak správně vytvořit dotazník. *Vyplňto.cz - řešení pro Váš internetový průzkum* [online]. 2008 - 2013 [cit. 2013-04-20]. Dostupné z: <http://www.vyplnto.cz/tipy/jak-spravne-sestavit-dotaznik/>.

[32] CHRÁSKA, M. Metody pedagogického výzkumu. Grada, 2007. ISBN 80-247-1369-4.

[33] KASÍK, Pavel. Najdete v této tabulce své heslo? Tak se chyťte za hlavu a změňte ho. In: HUDÁK, Luděk. *Digitální žurnalistika na příkladu iDnes* [online]. Brno: [s.n.], 2001 [cit. 2013-04-20]. Dostupné z: <http://technet.idnes.cz/najdete-v-teto-tabulce-sve-heslo-tak-se-chytte-za-hlavu-a-zmente-ho-p9n-/sw_internet.aspx?c=A111129_185621_sw_internet_pka>.

[34] LHOTÁK, Jan. Jak škola chrání před počítačovým pirátstvím. České Budějovice, 2010. Bakalářská práce. Jihočeská univerzita v Českých Budějovicích.

Seznam obrázků, tabulek a grafů

Příloha

Výuka digitální bezpečnosti na základních a středních školách

Dotazník je určen čerstvým absolventům základní a středních škol tj. studentům prvních ročníků navazujícího studia. Dotazník je anonymní, prosím o vyplnění pouze pravdivých údajů.

1) Absolvent:
   a) Základní školy b) Střední školy
2) Zaměření (základní, resp. střední školy):
   ……..
3) Dozvěděl ses při výuce, jak správně chránit svůj počítač před viry a pirátskými útoky?
   a) Ano b) Spíše ano c) Nevím d) Spíše ne e) Ne
4) Instaloval nebo aktualizoval jsi při výuce antivir?
   a) Ano b) Ne c) Řešeno pouze teoreticky
5) Doporučil ti tvůj učitel používat spíše placený antivir nebo antivir dostupný zdarma?
   a) Zdarma b) Placený c) Učitel nám nic nedoporučil
6) Zkoušeli jste si při výuce různá nastavení firewallu?
   a) Ano b) Ne c) Řešeno pouze teoreticky

7) Zvládl bys správně zálohovat data, kdybyste se o tom ve škole nezmiňovali?
   a) Ano b) Spíše ano c) Nevím d) Spíše ne e) Ne
8) Byla vám při hodinách informatiky zdůrazňována důležitost zálohování dat?
   a) Ano b) Ne c) Jen okrajově
9) Zálohuješ svá data?
   a) Ano všechna
   b) Ano, ale pouze pro mě důležitá (napiš jaká)……
   c) Nezálohuji
10) Svá data zálohuji?
   a) Online
   b) Na externí zařízení (napiš na jaké)……..
   c) Nezálohuji

11) Myslíš si, že je potřeba ve škole zmiňovat bezpečnost z pohledu sociálních sítí?
    a) Ano b) Spíše ano c) Nevím d) Spíše ne e) Ne
12) Myslíš, že jsi byl při vyučování dostatečně seznámen s nebezpečím, které ti může hrozit na chatu popř. sociální síti?
    a) Ano b) Ne c) Nebezpečí jsem si uvědomoval již dříve
13) Objevil jsi ty nebo někdo z tvého okolí na internetu (sociální síti) něco, co myslíš, že by tvůj vyučující (popř. jiná důležitá osoba z tvého okolí) o sobě neměl zveřejňovat?(Pokud odpovíš ano, napiš, o co šlo konkrétně – nepovinné)
    a) Ano …….
    b) Ne
    c) Nevzpomínám si
14) Sdílíš na sociální síti s ostatními uživateli všechny údaje nebo raději máš některé skryté (např. osobní informace, adresu, vztahy)?
    a) Ano vše
    b) Příliš osobní údaje raději nezveřejňuji
    c) Hlídám si, kdo jaké údaje u mě může vidět

15) Měla pro tebe bezpečnost hesel při výuce nějaký přínos?
    a) Ano b) Spíše ano c) Nevím d) Spíše ne e) Ne
16) Zmiňovali jste při výuce, jak by mělo vypadat dostatečně bezpečné heslo?
    a) Ano b) Ne
17) Ukazovali jste si nějaký software pro správu hesel?
    a) Ano b) Ne c) Pouze jsme nějaký zmiňovali

18) Je pro tebe škola důležitým zdrojem informací o autorském zákoně?
    a) Ano b) Spíše ano c) Nevím d) Spíše ne e) Ne
19) Do jaké míry jsi seznámen s autorským zákonem?
    a) Vím přesně, co dělat a jak se chovat, abych ho neporušoval
    b) Některé věci znám, u jiných si nejsem jistý
    c) Moc toho o něm nevím
20) Stahuješ hudbu, filmy aj. z internetu (např. z uloz.to, rapidshare.cz, hellshare.cz, apod.)?
    a) Ano, ale jsem si jist, že neporušuji autorský zákon
    b) Ano, ale nejsem si zcela jist, zda neporušuji autorský zákon
    c) Ano a jsem si plně vědom, že porušuji autorský zákon
    d) Nestahuji