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

Digitální bezpečnost ve školních vzdělávacích programech základních a středních škol

Vypracoval: David Kovář
Vedoucí práce: Mgr. Václav Šimandl

České Budějovice 2014

Pedagogická fakulta
Faculty of Education

Jihočeská univerzita v Českých Budějovicích
University of South Bohemia in České Budějovice

University of South Bohemia
Faculty of Education
Department of Informatics

Bachelor's thesis

Digital safety and security in the curriculum of primary and secondary schools

Author: David Kovář
Supervisor: Mgr. Václav Šimandl

Budweis 2014

JIHOČESKÁ UNIVERZITA V ČESKÝCH BUDĚJOVICÍCH
Fakulta pedagogická
Akademický rok: **2012/2013**

ZADÁNÍ BAKALÁŘSKÉ PRÁCE

(PROJEKTU, UMĚLECKÉHO DÍLA, UMĚLECKÉHO VÝKONU)

Jméno a příjmení:	**David KOVÁŘ**
Osobní číslo:	**P11049**
Studijní program:	**B7507 Specializace v pedagogice**
Studijní obor:	**Informační technologie a e-learning**
Název tématu:	**Digitální bezpečnost ve školních vzdělávacích programech základních a středních škol**
Zadávající katedra:	**Katedra informatiky**

Zásady pro vypracování:

Cílem práce je analýza školních vzdělávacích programů vybraných škol s důrazem na obsah a rozsah výuky problematiky digitální bezpečnosti.
Teoretická část bakalářské práce bude zaměřena na analýzu literárních zdrojů, především státních a dalších významných kurikulárních dokumentů a odborných e-bezpečnostních příruček. V praktické části bakalářské práce student provede rozbor školních vzdělávacích programů základních a středních škol, kdy se zaměří na zde popisovanou oblast výuky zálohování dat, používání softwarových bezpečnostních prvků, bezpečného chování na internetu včetně správy bezpečnostních hesel a problematiku autorského zákona. Praktická část práce bude dále zahrnovat vzájemné porovnání vybraných školních vzdělávacích programů, kdy důraz bude kladen na hledání signifikantních rozdílů v popisované digitálně-bezpečnostní problematice. Student dále ověří, zda a v jakém rozsahu jsou na vybraných školách ve výuce naplňovány vzdělávací požadavky, které jsou uvedeny v příslušných školních vzdělávacích programech a které se týkají digitální bezpečnosti. Toto ověření bude realizováno pomocí rozhovorů s žáky a učiteli daných škol.

Rozsah grafických prací:	**CD ROM**
Rozsah pracovní zprávy:	**40**
Forma zpracování bakalářské práce:	**tištěná**
Seznam odborné literatury:	**viz příloha**

Vedoucí bakalářské práce:	**Mgr. Václav Šimandl** Katedra informatiky
Datum zadání bakalářské práce:	**16. dubna 2013**
Termín odevzdání bakalářské práce:	**30. dubna 2014**

Mgr. Michal Vančura, Ph.D.
děkan

L.S.

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

V Českých Budějovicích dne 16. dubna 2013

Příloha zadání bakalářské práce

Seznam odborné literatury:

1. Buettner, Y., et. al. Information and Communication Technology in Education: A Curriculum for Schools and Programme of Teacher Development [online], 2002. UNESCO. Dostupné z: http://unesdoc.unesco.org/images/0012/001295/129538e.pdf

2. Eckertová, L., Dočekal, D., Bezpečnost dětí na Internetu. Computer Press, 2013. ISBN: 978-80-251-3804-5

3. Jeřábek, J., et al. Rámcový vzdělávací program pro základní vzdělávání. Praha: Výzkumný ústav pedagogický, 2007. Dostupné z: http://rvp.cz/informace/wp-content/uploads/2009/09/RVPZV_2007-07.pdf

4. Jeřábek, J., et al. Rámcový vzdělávací program pro gymnázia. Praha: Výzkumný ústav pedagogický, 2007. 102 s. Dostupný z : http://old.rvp.cz/soubor/RVP_G.pdf. ISBN 978-80-8700-11-3.

5. Katalog požadavků zkoušek společné části maturitní zkoušky: Informatika, základní úroveň obtížnosti [online]. Centrum pro zjišťování výsledků vzdělávání, 2010 Dostupné z: http://www.novamaturita.cz/index.php?id_document=1404034533&at=1

6. Katalog požadavků zkoušek společné části maturitní zkoušky: Informatika, vyšší úroveň obtížnosti [online]. Centrum pro zjišťování výsledků vzdělávání, 2010 Dostupné z: http://www.novamaturita.cz/index.php?id_document=1404034534&at=1

7. Kocman, R., Lohniský, J. Jak se bránit virům, spamu, dialerům a spyware. CP Books, 2005. ISBN: 80-251-0793-0.

8. Sechler, J. A Young Adult's Guide to Safety in the Digital Age. CreateSpace, 2010. ISBN: 978-1453618414.

Prohlášení

Prohlašuji, že jsem svoji bakalářskou práci 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 30.4.2014 David Kovář

Anotace

Obsah bakalářské práce se zabývá problematikou výuky digitální bezpečnosti s důrazem na obsah a rozsah. Samotná problematika digitální bezpečnosti je rozsáhlá a proto bylo toto spektrum informací vymezeno na vybrané oblasti výuky zálohování dat, používání softwarových bezpečnostních prvků, bezpečného chování na internetu včetně správy bezpečnostních hesel a problematiku autorského zákona. V teoretické části se bakalářská práce opírá o analýzu školních vzdělávacích programů vybraných škol. Dále práce zahrnuje analýzu českých kurikulárních dokumentů vzhledem k dané problematice a zpracovává potřebné spektrum informací a dat věnující se vybraným okruhům digitální bezpečnosti. Hlavním cílem bakalářské práce je porovnání vybraných školních vzdělávacích programů, u nichž bude kladen důraz na hledání signifikantních rozdílů v popisované digitálně-bezpečnostní problematice. Naplňování vzdělávacích požadavků na vybraných školách je ověřeno a realizováno pomocí rozhovorů s žáky a učiteli daných škol. Získaná data a informace od žáků a studentů spolu se školními a rámcovými vzdělávacími programy tvoří soubor informací reprezentující současný stav výuky digitální bezpečnosti a rozdíly mezi vybranými středními školami, gymnázii a základními školami.

Klíčová slova: Digitální bezpečnost, rámcový vzdělávací program, školní vzdělávací program, zálohování dat, bezpečnostní heslo, bezpečnost na internetu, softwarové bezpečnostní prvky, autorský zákon

Abstract

The bachelor thesis deals with teaching digital security issues with an emphasis on the content and range. The actual issue of digital security is extensive and therefore that range of information was defined on selected teaching areas of backup datas using software security features, safe behaviour on the internet including the management of passwords and security issues of copyright law. The theoretical part of Bachelor thesis is based on the analysis of educational programmes of selected schools. The Bachelor thesis also includes an analysis of curricular documents due to the issues and processes necessary range of information and data dedicated to selected area of digital security. The main aim of Bachelor thesis is the comparison of selected educational programmes where focus will be on finding significant differences in the described digital-security issues. Everything will be verified and implemented by interviews with students and teachers of the selected school. Acquired data and information from students along with school and framework educational programmes will generate set of information representing the current state of teaching digital security and the differences between high school, grammar school and elementary schools.

Key words: Digital safety, framework educational program, school educational program, data backup, password security, internet security, software security features, copyright

Poděkování

Rád bych poděkoval Mgr. Václavu Šimandlovi za cenné rady, věcné připomínky a vstřícnost při konzultacích a vypracování bakalářské práce. Mé poděkování patří též všem účastníkům rozhovorů za spolupráci při získávání údajů pro výzkumnou část práce.

Obsah

1 Úvod

Problematika digitální bezpečnosti je v současné době velice diskutované téma a z tohoto důvodu jsem si vybral bakalářskou práci zabývající se touto oblastí. V dnešní době, kdy dochází k rychlému rozvoji výpočetní techniky a téměř každý využívá informační technologie, patří práce s počítačem k základním dovednostem. V běžném životě můžeme narazit na různá rizika a hrozby. U výpočetní techniky a ve virtuálním světě platí to samé.

Digitální bezpečnost je rozsáhlá oblast, která zahrnuje různorodou řadu činností zabývající se ochranou informací před krádeží, neoprávněnou manipulací či ztrátou. Jak bezpečně informace uchovávat, bezpečně komunikovat apod. V rámci bakalářské práce byl obsah digitální bezpečnosti vymezen na oblasti zálohování dat, používání softwarových bezpečnostních prvků, bezpečného chování na internetu včetně správy bezpečnostních hesel a problematiku autorského zákona.

1.1 Cíl práce

Cílem práce je analýza vzdělávacích programů, kde jsem se věnoval popisované oblasti výuky digitální bezpečnosti. Dále jsem zjišťoval v jakém rozsahu jsou na vybraných školách naplňovány vzdělávací požadavky, které jsou uvedeny v příslušných školních vzdělávacích programech a týkají se oblasti digitální bezpečnosti. Cíle bakalářské práce jsou zaměřeny na hledání rozdílů v rozsahu a obsahu výuky digitální bezpečnosti. Výsledkem práce je deskriptivní obraz znázorňující současný stav výuky digitální bezpečnosti na vybraných středních a základních školách a rozdíly v rozsahu a obsahu výuky digitální bezpečnosti na vybraných školách.

1.2 Digitální bezpečnost ve vzdělávání

Nicméně bakalářská práce není založena pouze na digitální bezpečnosti, ale dále se zaměřuje i na vzdělávací instituce. Klíčovým bodem k zvládnutí současných a potenciálních rizik týkajících se právě digitálně-bezpečnostní problematiky se stává škola. Informační technologie si již našly místo v tomto prostředí a proto by měla škola být hlavním aktérem ve výchově a vzdělávání v oblasti digitální bezpečnosti.

Pro výzkumnou část je důležité zjistit jaké znalosti digitální bezpečnosti získali absolventi a v jakém rozsahu jsou tyto znalosti provázány se školními vzdělávacími programy vybraných škol. Vzhledem k tomu, že výuka digitální bezpečnosti probíhá v rámci edukačního procesu informačních technologií, je důležité zjistit, jaký pohled na tuto problematiku mají i jednotlivý pedagogové vybraných škol. Pro vytvoření uceleného obrazu o této problematice je důležité, aby součástí mého výzkumu bylo i studium kurikulárních dokumentů.

1.3 Kurikulární dokumenty

V rámcových vzdělávacích programech a vybraných školních vzdělávacích programech se zaměřuji na části, které se týkají digitálně-bezpečnostní problematiky. Dále dochází k ověření na základě získaných dat, zda a v jakém rozsahu jsou na vybraných školách ve výuce naplňovány vzdělávací požadavky, které jsou uvedeny v příslušných vzdělávacích programech. Výstupem bakalářské práce je deskriptivní popis znázorňující současný stav výuky digitální bezpečnosti a naplňování vzdělávacích požadavků, v závislosti na výše zmíněných cílech.

2 Digitální bezpečnost

V digitálním světě tvoří informační bezpečnost významné odvětví zahrnující celou řadu činností a operací od prevence podvodů, přes ochranu osobních údajů až po vyšetřování trestné činnosti. Informační bezpečnost lze chápat jako systém ochrany dat a informací před zneužitím během jejich vzniku, zpracování, ukládání, přenosů či likvidace. Toto odvětví se stává samostatným multidisciplinárním oborem vzhledem k faktu, že dochází k neustálému vývoji a rozšiřování informačních technologií. Nejde o fixní sféru informačních technologií, ale o proces trvalého budování a rozvoje (Požárek, 2007).

Hovoříme zde o poměrně mladém oboru, který obsahuje mnoho pojmů a definic determinující oblast bezpečnosti informačních a komunikačních technologií. Bezpečnost se nedá vymezit pouze na informační systémy nebo informační a komunikační technologie. S vybranou sférou informačních technologií souvisí aspekt, zahrnující, jak chování jednotlivců, tak jednání organizačních procedur. Osobní data či hospodářsky využitelné údaje jsou informace, které jsou nejčastěji v ohrožení (Požárek, 2007).

2.1 Hrozby a rizika

Ministr (2011) uvádí, že hrozbu v informační bezpečnosti můžeme vnímat jako nežádoucí incident, který může skončit škodou v informačním systému nebo organizaci, či poškozením dat, služeb nebo jiných aktiv. Hrozbou nazýváme jakoukoliv událost či okolnost, která zapříčiní škodu. Hrozby tak můžeme rozdělit na:

Objektivní

- Fyzické: poruchy, výpadky napětí či jiné fyzické poškození. Těmto hrozbám se předchází těžko, ale lze je minimalizovat.
- Technické či logické: softwarové poruchy, krádež, poškození paměťového média.

Subjektivní

- Neúmyslné: nešikovnost uživatele působící škody.
- Úmyslné: hrozby zapříčiněné lidským faktorem s úmyslným potenciálem (Ministr, 2011).

Příkladem charakteristických hrozeb v informačních technologiích jsou neautorizovaná modifikace a zpřístupnění informací různou formou odposlechů. Analýzou toků vyměňovaných zpráv a neoprávněné kopírování paměťových míst. K těmto vyjmenovaným neautorizovaným přístupům může útočník využít např. škodlivý software nebo elektromagnetické vyzařování. Dalšími hrozbami může být výčet informací z citlivých dílčích informací, dedukce ze znalosti existence informace či

odposlech prostřednictvím zařízení pro práci se zvukem ve výpočetním stroji. Dále neoprávněné používání zdrojů (krádeží) nebo neoprávněné používání jejich kopií (Požárek, 2007).

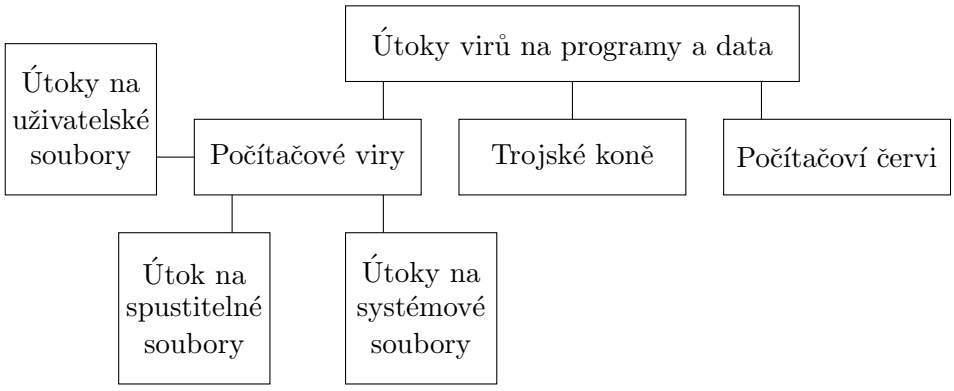
Neobezřetné chování vede k vážným následkům při napadení virem nebo spywarem. Od ztráty identity, podvodu, krádeži či ztráty dat až po uvedení počítače do nepoužitelného stavu. Způsobů jak virus nebo spyware může napadnout počítač je mnoho. Rizika lze eliminovat vyvarováním se následujícím aktivitám, jak uvádí na webovém portálu Get Safe Online (2012b):

- Otevření infikované emailové přílohy v podobě .exe souboru.
- Navštívení infikované webové stránky.
- Skrze USB zařízení nebo jiné paměťové zařízení (externí pevný disk, MP3 přehrávač, paměťové karty, CD/DVD).
- Pomocí MAKRA umístěného v aplikacích kancelářských balíků.

2.2 Počítačové viry a škodlivé kódy

První virus byl dokumentovaný v roce 1983, pouze několik let předtím vznikl první koncept osobního počítače. Počítačový virus je pro výpočetní stroj asi nejviditelnější hrozbou. Virus je program, který se snaží sám sebe šířit a to pokud možno nenápadným způsobem. V počítači se může projevovat a také nemusí. Když se v počítači naplno projeví, dojde v horším případě ke smazání dat a v lepším případě, bude uživatel překvapen. Nemusí to skončit u ztráty dat, ale virus může z počítače udělat stroj, ze kterého bude bez vašeho vědomí odesílat nevyžádanou poštu. Bude šířit dál viry do sítě nebo odesílat citlivé informace a přístupová hesla k uživatelským bankovním účtům (Kocman, Lohnický, 2005).

Doseděl (2014) podotýká, že oblast výpočetní techniky, která obsahuje tyto nežádoucí škodlivé kódy může pracovat proti uživatelskému pohodlí.



Obr. 1: Členění útoků počítačových virů (Požárek, 2007)

2.2.1 Základní rozdělení škodlivého kódu

Virus v informačním světe napadá informační stroje a jiná zařízení v podobě škodlivého počítačového kódu. Virus neboli škodlivý počítačový kód můžeme přirovnat k biologickému organizmu, který napadá nic netušícího hostitele a v případě počítačového viru se stává cílem počítač (Doseděl, 2004). K aktivaci viru dochází při spuštění infikovaného programu, kdy virus získává prostor k libovolnému šíření a narušení počítače, souborů a dat. Při ukončení infikovaného programu zůstává virus nadále v paměti počítače. Viry jsou komplikované kódy s různými variacemi, které lze rozčlenit podle způsobu šíření, aktivace, struktury a funkcionality (Požárek, 2007).

Doseděl (2004) charakterizuje trojské koně jako programy, tvářící se uživatelsky přínosně či zábavně. Kromě transparentní činnosti reprezentující uživateli, provádí na pozadí nežádoucí a v mnoha případech nekalé činnosti. V drtivé většině případů se zaměřuje na sběr uživatelských hesel zadávaných přes vstupní zařízení klávesnice. Mohou se vyskytovat i trojské koně, které se zajímají o vaše zájmy, což zahrnuje internetové stánky vámi navštívené a následně poskytují adekvátní reklamy. Z hlediska funkčnosti popisuje Požárek (2007) trojského koně, jako škodlivý kód, který je součástí jiného speciálního programu, který působí neškodně a mnohdy i prospěšně. Při dosažení cíle a místa určení, se tento program vygeneruje a začne se šířit do sítě. Následky přítomnosti trojského koně bývají ztráta dat, odeslání bezpečnostních hesel po síti či informační kriminalita v podobě ovládání administrativní sítě.

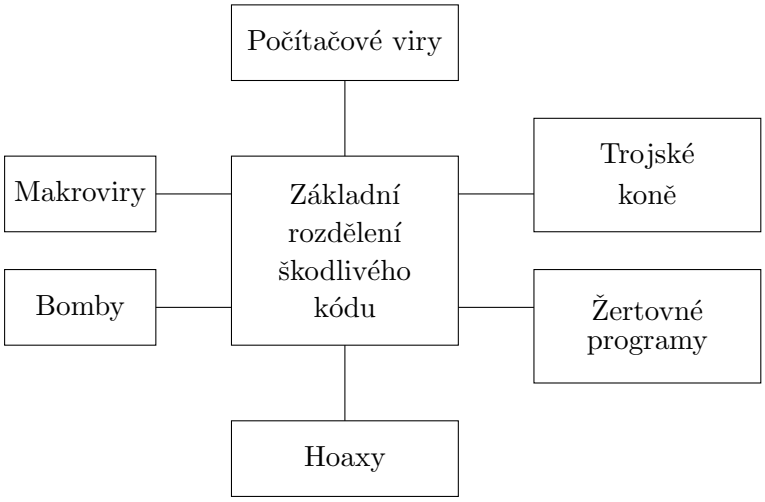
V předešlé kapitole bylo řečeno, že viry se mohou šířit pouze pomocí spustitelných souborů. Makroviry jsou ovšem výjimkou od doby, kdy byl implementován programovací jazyk do kancelářských balíků. Makroviry jsou psány v pokročilých makrojazycích současných moderních kancelářských balíků a umožňuje makrovirům šířit se v běžných kancelářských dokumentech. Bez vědomí uživatele a možnosti ovlivnit průběh, makrojazyky dokáží spustit libovolný program a převzít kontrolu na vybranými funkcemi (Doseděl, 2004).

Worm (červ) program infikuje počítač v drtivé většině pomocí elektronické pošty. Při otevření infikovaného souboru, u elektronické pošty máme na mysli jakoukoliv přílohu, dojde k aktivaci červa. Moderní červi nepotřebují k aktivaci otevření infikovaného souboru. Tento škodlivý kód se usadí v systému a ve vhodný se okamžik začne šířit do světa skrze přílohy e-mailu, které odesílá dalším osobám ve vašem adresáři kontaktů (Požárek, 2007).

Phishing je metoda spolupracující se spamem k získaní informace, jako jsou přihlašovací údaje, hesla, čísla platebních karet apod. Za využití sociálního inženýrství, kdy je uživatel vyzván k zadání důvěrných informací, třeba na fiktivní webové stránky vypadající jako stránky oficiální (Eckertová, Dočekal, 2013).

V překladu Hoax znamená falešný poplach, výmysl, žert, mystifikace nebo také podvod. V informačním světě je považován za poplašnou zprávu před neexistujícím nebezpečím. Hoaxy obsahují výzvu k přeposlání uživatelským kontaktům a tím se stává řetězovou zprávou. Dalo by se říct, že jsou hoaxy v podstatě neškodné, ale není tomu tak. Nepříjemným následkem je zaplněná emailová schránka těmito zprávami a to mnohdy

i ve větším počtu. Nabádá příjemce k činnostem, které můžou vést k poškození počítače nebo může mít poškozující dopad na uživatele. Tak jako zmiňované škodlivé kódy může hoax poškodit osobu, ale spíše instituci nepravdivou informací. Hoaxy využívají výborné znalosti jazyka a působí na příjemcovi city za pomocí logických argumentů založených na faktech (Kopecký, 2008).



Obr. 2: Členění počítačových virů podle Požárka (2007)

2.3 Softwarové bezpečnostní prvky

Způsobů, jak eliminovat hrozby v podobě škodlivých počítačových virů, lze za pomocí softwarových bezpečnostních prvků. Kocman, Lohnický (2005) tvrdí, že k softwarovým bezpečnostním prvkům nesmazatelně patří počítačový virus. Nebýt tohoto rafinovaného počítačového programu nebylo by pravděpodobně zapotřebí vyvíjet bezpečnostní prvky zvané antivirus.

2.3.1 Antivirová ochrana

Obranou proti škodlivému a nežádoucímu programu je antivirus. Tento bezpečnostní prvek by měl být nainstalován v každém počítači, který je připojen k internetu či lokální síti. Ale i počítače bez síťového připojení by měli být tímto způsobem chráněni, neboť počítačové viry se šíří i skrze přenosová média. Antivirový program dokáže úspěšně najít škodlivý program při kontrole počítače a následně jej smazat, bez poškození infikovaného souboru nebo v nejhorším případě napadený soubor smazat. Pokud dojde k nakažení virem, který je spuštěn již od startu počítače, antivirový program zvládne chránit počítač před útokem po celou dobu provozu (Kocman, Lohnický, 2005).

Antivirové programy jsou relativně finančně nenáročné. Na druhou stranu lze pořídit i freewarové verze u kterým se v některým případech platí pouze za aktualizaci virové

databáze. Dále vybrané antivirové programy je možno používat bezplatně po určitou dobu nebo pro domácí využití. Hlavní funkcí antivirového programu je prevence nákazy, kontrola spuštěných a příchozích souborů a v neposlední řadě eliminace nákazy. K dosažení těchto funkcí je požadována úplná a aktualizovaná virová databáze, dostupné prostředky pro hledání a odstranění virů a přístup k internetu pro aktualizace. Hackerské útoky jsou doprovázeny viry a za spolehlivou ochranu je považováno sloučení antivirového programu s bezpečnostním prvkem zvaným firewall (Kocman, Lohnický, 2005).

2.3.2 Záplaty a aktualizace

Žádný operační systém není dokonalý. Zaměříme-li se na operační systém Windows, dozvíme se, že jsou téměř neustále zveřejňovány chyby. Jedná se o menší chyby, ale čas od času se najde kritická chyba, která umožňuje útočníkovi zneužít počítač. Microsoft vydává pravidelné záplaty a aktualizace, kterými tyto chyby odstraňuje. Aplikace zvaná Windows Update tyto záplaty a aktualizace zveřejňuje a nabízí ke stáhnutí. Jedinou podmínkou je připojení k internetu, bez připojení je počítač teoreticky v bezpečí (Kocman, Lohnický, 2005).

Záplaty a aktualizace patří k jednomu ze způsobů jak udržet počítač v bezpečí před škodlivými kódy a jinými hrozbami. Doporučuje se instalovat aktualizace ihned po vybídnutí operačním systémem, pokud nejsou instalovány automaticky, jak tomu většinou bývá. Všechny aktualizace a záplaty se nemusí nezbytně opírat pouze o bezpečnost, ale starají se o funkcionalitu operačního systému a mohou také kontrolovat legalitu softwaru od vybrané společnosti poskytující operační systém (např. Windows a Microsoft Office). Na druhou stranu při zanedbání pravidelné aktualizace operačního systému, může dojít k vážným problémům zapříčiněným narušením bezpečnosti. Podstupujeme v tomto případě rizikům napadení viry a jinými škodlivými kódy, kriminálním útokům a zamrznutí počítače zapříčiněným sníženým výkonem (Get Safe Online, 2012d).

Preventivní opatření

- Nevyměňovat nebo nepoužívat nedůvěryhodná paměťová zařízení (CD, DVD a jiná přenosová média).
- Zálohování důležitých dat a nespouštět neznáme programy na počítači s citlivými daty.
- Pravidelná kontrola počítače antivirovým programem.
- Prevence kontaktu neoprávněných či cizích osob.
- Prověřovat vstupní zařízení (Požárek, 2007)

2.3.3 Firewall a jeho funkce

Pro kontrolu příchozích a odchozích dat slouží firewall, tento program působí mezi síťovým rozhraním a počítačem. Přes firewall projde každý paket putující jakýmkoliv

směrem. Firewall je nezbytnou součástí při připojení k internetu. Lze použít řadu freewarovým a sharewarových produktů. Firewall má podobu hardwarového zařízení, ale i softwarového zařízení, které se vyskytuje nejčastěji v domácích podmínkách (Kocman, Lohnický, 2005).

Jak už bylo řečeno, úkolem brány firewall je kontrola příchozí a odchozí dopravy mezi počítačem a sítí. Nicméně brána firewall, dále brání přístupu různým typům škodlivého kódu, jako jsou například červi a neustále chrání počítač před hackerským napadením a pokusu dostat se do počítače. Firewall se stává prvním obráncem vašeho počítače, ovšem na dosažení maximální bezpečnosti nestačí (Get Safe Online, 2012e).

Bezpečnostní prvek firewall dělíme na software a hardware firewall. Software firewall nebo také osobní firewall by měl být nainstalován na každém počítači, který je připojen k internetu. Osobní firewall bývá již součástí operačního systému a v podstatě funguje bez uživatelské konfigurace nebo jiného nastavení. Není třeba automaticky používat vestavěné firewally a spoléhat pouze na tento bezpečnostní prvek. Jsou i zdarma dostupné samostatné alternativy bezpečnostního prvku firewall, které mohou být bezpečnostně přínosnější, jak po stránce funkcionality, tak po stránce bezpečnosti. Hardware firewall se od software firewall nijak zvláště neliší. Hardware firewall funguje na vyhrazeném hardwaru, tím pádem se o hardware nedělí s ostatními aplikacemi a dosahuje většího zabezpečení (Get Safe Online, 2012e).

2.4 Ochrana dat

Data jsou mnohdy informace, které by neměli být přístupné všem lidem, přístupné proti modifikaci nebo proti ztrátě či zničení. Data jsou uchovávána v souborech na disku, uložena v tabulkách v databázích, přenášena elektronickou poštou a tak podobně. Nicméně, můžeme říct, že ke každým datům lze přistupoval individuálně. Snahou by mělo být zálohovat data co nejčastěji a samozřejmě pravidelně (Doseděl, 2004).

2.4.1 Rizika ztráty dat

Počítače obsahují data, která zahrnují dokumenty, fotografie, hudbu, videa, software atp. V dnešní době, kdy počítačové pevné disky dosahují velkých kapacit může být ztráta dat katastrofální a nepříjemná. Předejít ztrátě dat můžeme pravidelnou zálohou všech důležitých dat na bezpečném a dohledatelném místě. Rizika v pojetí ztráty dat zahrnují selhání hardwaru (pevného disku). Dále objektivní hrozby, jako požár a náhodné poškození, krádež, náhodné smazání, ať už vlastním zaviněním nebo působením škodlivého kódu (Get Safe Online, 2012c).

Tři skupiny dle určitého druhu nebezpečí

- Kompromitace: ochrana před prozrazením, ochrana důvěryhodnosti.
- Modifikace: ochrana před změnou (neoprávněnou).
- Zničení: ochrana před zničením úmyslným či neúmyslným (Doseděl, 2004).

2.4.2 Možnosti ochrany dat

Způsobů, jak udržet data v bezpečí je mnoho. Zálohování dat je jednoduchou metodou, jak ochránit citlivá a důležitá data. Vždy je třeba brát na vědomí, že data, například v notebooku jsou náchylná ke ztrátě ať cizím zapříčiněním nebo objektivní hrozbou (Get Safe Online, 2012c). Důležitá a nepostradatelná data by měly být umístěna alespoň na dvou na sobě nezávislých médiích (Čepička, 2008).

Možnou variantou pro uchování dat před ztrátou jsou zapisovatelné disky CD/DVD. Této metodě je lepší se vyhnout, neboť mají omezenou kapacitu a mnohdy pomalý přenos dat. Každopádně tato varianta se může zdát jako levná a pohodlná, ale stále je třeba myslet na riziko poškození, ke kterým jsou tyto zařízení náchylná (Get Safe Online, 2012c). Čepička (2008) uvádí, že CD/DVD jsou z dlouhodobého hlediska spolehlivější, ale v porovnání s externími pevnými disky, kde vzhledem k velké kapacitě a rychlému přenosu dat odpadne práce s organizací a snižuje riziko chyb, se stávají druhořadou možností.

V současné době se stává zálohování online rozsáhlým způsobem ochrany dat. Poskytovatelů online zálohování je mnoho. Příkladem může být ISPs, internetový bezpečnostní software a společnosti jako Apple nabízející iCloud službu. Uplatnění online zálohování je stále populárnější díky jednoduchosti a nízkým nákladům. Někteří poskytovatelé online zálohování nebo online úložným prostorů nabízí neomezený prostor zdarma, ovšem náklady vzrůstají s množstvím uloženým dat (Get Safe Online, 2012c).

2.5 Bezpečné chování na internetu

Sociální sítě jsou nástrojem pro kontakt s rodinou, přáteli a celkově s okolním světem. Sdílení zážitků, fotografií a vyměňování si osobního obsahu. Každopádně, tento způsob komunikace a sdílení života může být i zdrojem rizik a nebezpečí pro všechny uživatele a především pro mládež. I když všechny sociální sítě nastavují věkovou spodní hranici pro získání přístupu, není problém pro děti tuto překážku obejít (Get Safe Online, 2012f).

Zásady, které by měl uživatel dodržovat při pohybu na sociálních sítích podle Get Safe Online (2012g), jsou následující:

- Dávat si pozor na zveřejňování jakékoliv identifikačních údajů o vlastní osobě (na profilu nebo v příspěvcích).
- Volba uživatelské jméno, které neobsahuje žádné osobní informace.
- Nastavení samostatného e-mailového účtu, který bude přijímat poštu z webu.
- Používat silné heslo.
- Udržovat profil uzavřený a zobrazovat profil pouze vybraným uživatelům.

- Nepublikovat a nepsat nic, co by mohlo v budoucnu uškodit.
- Nepsat komentáře, které jsou urážlivé nebo mohou způsobit trestný čin.
- Naučit se, jak správně používat stránky. Pomocí funkce ochrany osobních údajů omezit přístup cizím lidem k profilu.
- Být na pozoru před phishingovými podvody, včetně falešných žádostí o přátelství nebo pozvání k navštívení cizích stránek.
- Uvědomovat si, že společnosti mohou prohlížet stránky sociálních sítí stávajících nebo budoucích zaměstnanců (Get Safe Online, 2012g).

2.5.1 Kyberstalking, kyberšikana a sexting

Na používání sociálních sítí se váží rizika, jako je kyberstalking, kyberšikana a možnost kontaktu s naprosto cizími osobami. Často diskutovaným tématem je ztráta identity, kdy dochází k odhalení soukromých informací ze soukromých profilů a sdílených příspěvků. V souvislosti s tímto rizikem, by se měl každý zamyslet nad množstvím sdílených osobních informací, jako je datum narození, adresa bydliště nebo datum odjezdu na dovolenou. Ztráta nebo zneužití těchto informací by mohlo uživateli uškodit a ublížit. Obezřetnost a důvěryhodnost osob je velmi důležitá. Mládež by mělo být vedena a učena k obezřetnému chování (Get Safe Online, 2012f).

Na rozdíl od setkání tváří v tvář, děti mnohdy nevědí s kým ve skutečnosti komunikují. Nicméně již zmíněným pojmem je kyberstalking, kdy nevědomost identity osoby, se kterou komunikujeme, může být nebezpečná jak pro děti, tak i pro dospělé (Get Safe Online, 2012i). Eckertová, Dočekal (2013) popisují kyberstalking jako dlouhodobé pronásledování, omezování a obtěžování. V první řadě se "stalker" snaží navázat kladný vztah. Po neúspěchu přechází k významnému narušování osobního života oběti za pomocí moderních informačních technologií, ale i osobně.

Kyberšikana má stejný význam jako šikana, akorát s tím rozdíl, že využívá elektronické prostředky. Nejobvyklejší projevy kyberšíkany představuje zasílání obtěžujících, urážejících či útočných mailů a SMS. V případě virtuálního světa a sociálních sítí mohou být lidé anonymní, mohou komunikovat, aniž by byli zatíženi společenskými rolemi, svými fyzickými nedostatky nebo psychickými bloky plynoucími z osobního kontaktu s lidmi (Get Safe Online, 2012h). Eckertová, Dočekal (2013) rozdělují kyberšikanu na úmyslnou a neúmyslnou. Úmyslnou kyberšikanu charakterizují jako opakované ohrožování, pronásledování a psychické týrání. Útočníkem může být jak jednotlivec, tak i skupina lidí. Na druhou stranu, neúmyslná kyberšikana ze strany útočníků může být chápaná jako vtip, který nemá oběti ublížit, ovšem může to mít jiný následek.

Vysokému riziku vydírání, zneužití a veřejného posměchu se vystavují uživatelé sociálních sítí, kteří zasílají nebo sdílejí materiály (fotografie, videa či texty) s erotickým nebo sexuálním podtextem. V souvislosti s moderními komunikačními technologiemi se tento jev nazývá sexting, který je kombinací slov sex a texting. Vybrané materiály se mohou stát v budoucnu vlastnictvím cizí osoby, mohou být zveřejněny na jiném zdroji a může být použit pro nim (Eckertová, Dočekal, 2013).

2.5.2 Facebook

Sociální síť se zdá být soukromým prostorem pro sdílení osobních informací pro určený okruh lidí, ale ať už jde o jakoukoliv internetovou službu stále se jedná o veřejný prostor, kde cokoliv sdílené může být veřejné pro kohokoliv (Eckertová, Dočekal, 2013). Jak uvádí Get Safe Online (2012f), tak se jedná o nejpopulárnější sociální síť, kde lze očekávat potenciální hrozby jako šikana, staling, scamming, krádeže identity a hacking.

Na co myslet při používaní sociální sítě

- Znáte své přátele?
- Kdo může vidět to, co jste sdíleli na Facebooku?
- Komu se bude zobrazovat váš profil a jak?
- Jak upravovat "timeline".
- Jak deaktivovat svůj profil (Get Safe Online, 2012f).

2.6 Správa bezpečnostního hesla

Nejpoužívanějším způsobem, jak prokázat totožnost je uživatelské heslo, které se používá při identifikaci na webové stránky, emailové účty a konec konců i na osobní účet na počítači. Užití silného hesla je proto nezbytné, nicméně veškeré výkonné bezpečnostní systémy jsou zbytečné, pokud dojde k napadení a pokusu o zlomení uživatelského hesla (Get Safe Online, 2012a).

Heslo je ve většině případech spojováno s uživatelským účtem. Dále se dá propojit s identifikací odděleného kódu PIN, ale i s takzvanou nezapomenutelnou informací (Get Safe Online, 2012a).

Rizika slabého hesla

- Dostupnost k vašemu bankovnímu účtu
- Nákup za vaše peníze.
- Vydávání se za vaši osobu na sociálních sítích.
- Odesílání emailů vaším jménem.
- Přístup k soukromým a jiným citlivým informacím (Get Safe Online, 2012a).

Předpoklady silného hesla

Pro vytvoření silného hesla je třeba myslet na následující pravidla, která zvyšují kvalitu vašeho hesla:

- Používat heslo
- Heslo by mělo být kombinací velkých a malých písmen, číslic a symbolů.
- Používat heslo o minimální délce osmi znaků.
- S rostoucí délkou hesla také roste doba na prolomení (Get Safe Online, 2012a).

Na druhou stanu vyhnout bychom se měli následujícím v podstatě neuvědomovaných prohřeškům, které mohou mít za následek ztrátu jedinečnosti hesla:

- Používat stejné heslo jako uživatelské jméno.
- Nepoužívat osobní údaje jako jména skutečného jména, rodinných příslušníku nebo domácích mazlíčku.
- Užívání hesla v podobě data narození.
- Používat všeobecně známa slova či jména.
- Používat číselné posloupnosti.
- Vyhnout se běžným slovům (Get Safe Online, 2012a).

2.6.1 Správa a údržba hesla

Bezpečnostní heslo je nedílnou součástí i ostatních oblastí digitální bezpečnosti, ve kterých se právě diskutuje jeho správa, tvorba a použití. Na portálu Get Safe Online (2012a) uvádí, že ochránit jedinečnost svého hesla bychom měli docílit pravidelnou změnou, nepoužívání hesla před zraky jiných osob a pokud možno nesdílením svého hesla s jinou osobou. K docílení nejvyšší ochrany je ideální vytvářet pro každý uživatelský účet odlišné heslo s co nejmenší podobností. Nikdy neposílejte bezpečnostní heslo přes email a jiné komunikační prostředky a vždy mějte na paměti, že vás žádný administrátor nepožádá o zaslání vašeho bezpečnostního hesla.

2.7 Autorský zákon

Na ochranu autorského díla se vztahuje autorské právo, které chrání dílo a nároky tvůrce po určitou dobu. Dle autorského práva má tvůrce nárok se rozhodnout jak s jeho dílem (filmy, písně, počítačové programy...) bude nakládáno. Dále autor nebo osoba svěřená rozhoduje o možnosti prodeje, pronájmu, sdílením na internetu, vystavováním. Bez oprávnění, souhlasu nositele autorských práv dochází k porušení autorského práva při nakládání s dílem a porušení vede k nepříznivým důsledkům (Filmynejsouzadarmo, 2014).

V §2, odst. 1, zákon č. 121/2000 Sb. v plném znění je uvedeno, že: „předmětem práva autorského je dílo literární a jiné dílo umělecké a dílo vědecké, které je jedinečným výsledkem tvůrčí činnosti autora a je vyjádřeno v jakékoliv objektivně vnímatelné podobně včetně podoby elektronické, trvale nebo dočasně, bez ohledu na jeho rozsah, účel nebo význam.“(Sbírka zákonů České republiky)

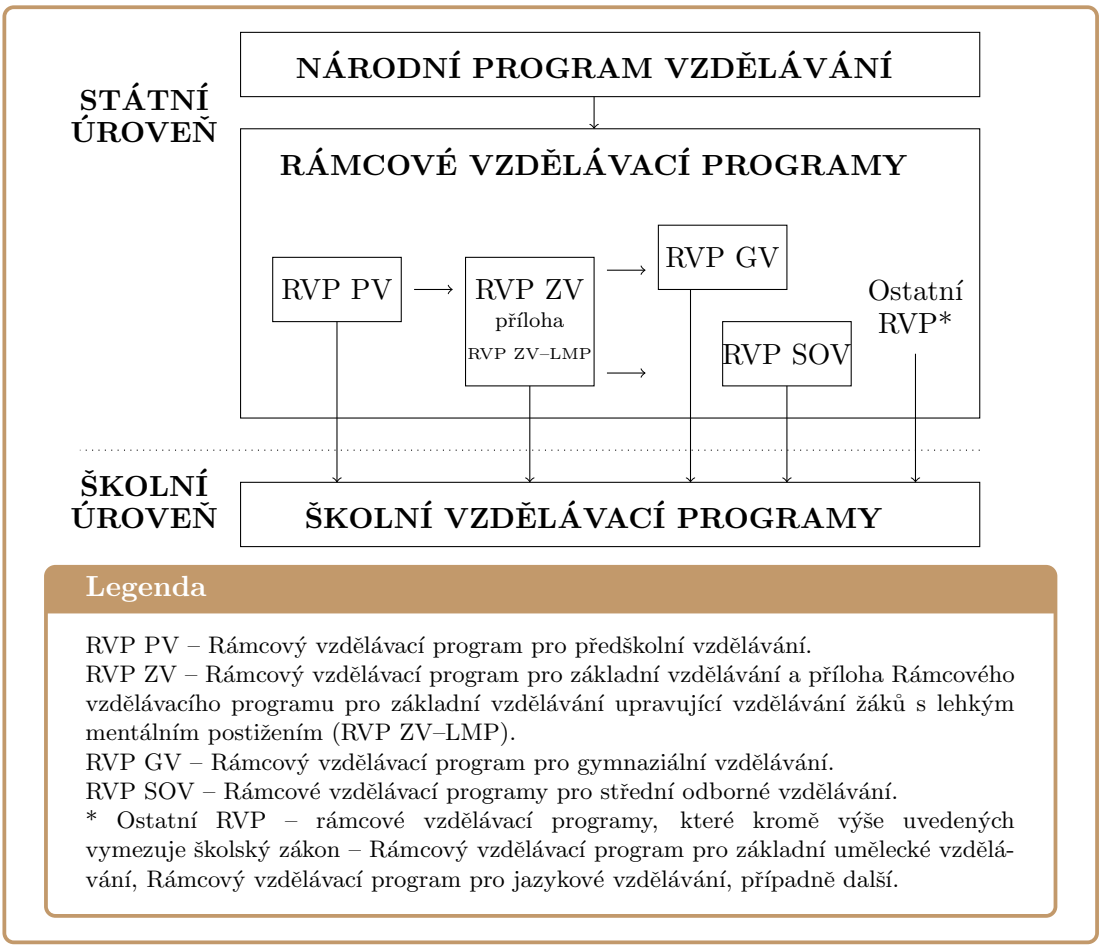
2.7.1 Software a licence

Základním typem dohody o autorských právech je tzv. licence, licenční smlouva. Pomocí licenční smlouvy autor poskytuje oprávnění k užití díla za určitých podmínek, podle kterých Štědroň (2010) rozděluje software do následujících základních kategorií:

- Shareware: zkušební verzi, jinak placený software. Omezené funkce a může být i funkčnost.
- Freeware: jde o programy, které jsou zdarma, ale ne vždy a úplně. Některé freeware se např. nemohou používat ke komerčním účelům.
- Trial: jedná se o časově omezenou licenci. Po uplynutí určité doby může přestat fungovat. Dál lze používat jen po zaplacení plné verze.
- Public domain: software, u kterého se jeho tvůrci dobrovolně vzdali autorských práv. Lze program jakkoliv upravovat i volně šířit.
- Demo: funkčně omezená verze programu, nejčastěji demoverze her.
- Opensource: tyto programy bývají většinou zdarma. Jedná se o upravitelný software s přístupným zdrojovým kódem.
- Plná verze zdarma: nevhodné platit tyto programy s freeware, tento software nelze volně šířit, jedná se o neomezené komerční programy.
- Adware: software poskytovaný zdarma, ale obsahují reklamu (Štědroň, 2010).

3 Digitální bezpečnost v kurikulárních dokumentech

Státní a školní úroveň je hlavní produkcí kurikulárních dokumentů (viz obr. 3), kde státní úroveň tvoří Národní program vzdělávání a Rámcové vzdělávací programy. Tímto způsobem vymezuje počáteční vzdělání žáků od 3 do 19 let jako celek a deklaruje hlavní vzdělávací rámce do jednotlivých etap předškolního, základního a středního vzdělání. Školní úroveň představuje školní vzdělávací programy, podle kterých se řídí individuální vzdělávání na jednotlivých školách. Všechny uvedené vzdělávací dokumenty je veřejně přístupné pro pedagogickou i nepedagogickou veřejnost (Jeřábek, 2007a).



Obr. 3: Systém kurikulárních dokumentů (Jeřábek, 2007a)

3.1 Rámcové vzdělávací programy

Ministerstvo školství mládeže a tělovýchovy České republiky (dále MŠMT ČR) na svém portále publikuje rámcové vzdělávací programy, které jsou zpracovány konkrétně pro

jednotlivé obory vzdělání. V nich jsou konkrétně uvedeny jak cíle vzdělání, kompetence a obsah včetně očekávaných výsledků. V podstatě tím MŠMT ČR stanovuje pravidla a rámce pro tvorbu vlastních školních vzdělávacích programů i učebních plánů. Školní vzdělávací programy základních škol, středních škol a gymnázií vychází z rámcových vzdělávacích programů a pravidel v nich uvedených (Národní ústav pro vzdělávání, 2013).

V §3, odst. 2, zákon č. 561/2004 Sb. v plném znění je uvedeno, že: „pro každý obor vzdělání v základním a středním vzdělávání a pro předškolní, základní umělecké a jazykové vzdělávání se vydávají rámcové vzdělávací programy. Rámcové vzdělávací programy vymezují povinný obsah, rozsah a podmínky vzdělávání; jsou závazné pro tvorbu školních vzdělávacích programů.“(Sbírka zákonů České republiky)

Rámcové vzdělávací programy základního vzdělání vedou žáky k dosáhnutí základní úrovni informační gramotnosti. Žák by měl získat elementární dovednosti v ovládání výpočetní techniky a moderních informačních systémech. Dále by si měl osvojit praktické znalosti výpočetní techniky, zahrnující orientaci v informačním světě, pracovat s informacemi a vědět, jak je využít v dalším vzdělávání i praktickém životě. V dnešní době, kdy dochází k rychlému rozvoji a rozšiřování výpočetní techniky je tato vzdělávací oblast zařazena jako povinná součást základního vzdělání prvního a druhého stupně základní školy a je nezbytným předpokladem pro budoucí využití výpočetní techniky. Rámcové vzdělávací programy základního vzdělání po obsahové stránce bezpečnosti zahrnují tyto digitálně-bezpečnostní prvky: respektování práv k duševnímu vlastnictví, ochrana data před poškozením, ztrátou a zneužitím (Jeřábek, 2007a).

Na informační gramotnost dosaženou na základní škole dále navazuje výuka informačních a komunikačních technologií na gymnáziích a středních školách, kde rámcové vzdělávací programy prohlubují žákovi znalosti výpočetní techniky. Rámcové vzdělávací programy gymnázií dále vedou žáka k pokročilejšímu využití výpočetní techniky v oblasti aplikování pokročilejších funkcí, zpracování informací a seznámí se s informatikou jako vědním oborem, který zkoumá informační technologie z hlediska používaného hardwaru i softwaru. Rámcové vzdělávací programy gymnázií po obsahové stránce bezpečnosti navazují na již získané znalosti na základní škole a dále se věnují ochraně dat před zneužitím a poškozením, antivirové ochraně, bezpečnostním prvkům, zálohování dat, ochraně osobních údajů a autorskému právu (Jeřábek, 2007b).

Rámcové vzdělávací programy středních škol nejsou jednotné pro všechny střední školy, ale dělí se do kategorií dle oborového zaměření. Hloubka a rozsah výuky informačních technologií se v tomto případě liší u středních škol se zaměřením na výpočetní techniku a u středních škol bez zaměření na výpočetní techniku. Od toho se dále odvíjí vzdělávací obsah a očekávané výstupy (Národní ústav pro vzdělávání, 2013).

3.2 Školní vzdělávací programy

Školní vzdělávací program jakožto kurikulární dokument umožňuje formulovat představy k docílení nejvhodnějšího a jedinečného způsobu vzdělávání na dané škole.

Tvorba vlastního školního vzdělávacího programu je příležitost pro jednotlivé učitelé vyjádřit vlastní úsilí a zkušenosti, které vedou k vytvoření představy o realizaci požadavků uvedených v rámcových vzdělávacích programech, vymezení vzdělávacího obsahu, očekávaných výstupů atp. Základní školy při tvorbě vlastního školního vzdělávacího programu vychází ze struktury školního vzdělávacího programu uvedeného v rámcovém vzdělávacím programu základního vzdělání (Jeřábek, 2005c).

Při tvorbě školních vzdělávacích programů střední škol je nutné provést analýzu podmínek školy, při které se stanový hlavní záměry a vzdělávací činnosti dané školy. Pro každý obor vzdělání, ke každému rámcovému programu se zpracuje samostatný školní vzdělávací program. Na základě rámcového vzdělávacího programu je stanoveno potřebné učivo a jeho obsah a rozsah se nedá redukovat. Koncepce jednotlivých předmětů dané školy je založena na prioritách a celkovém pojetí vzdělávací strategie, která se odráží v daném oboru (Kašparová, 2012).

3.3 Digitální bezpečnost u maturitní zkoušky

Od žáka střední školy či gymnázia se u maturitní zkoušky z informatiky očekává, že bude prakticky a teoreticky ovládat vybrané digitálně-bezpečnostní okruhy. Žák s porozuměním používá antivirový program, firewall a ostatní bezpečnostní nástroje. Dokáže vysvětlit problematiku šíření počítačových virů a jiného škodlivého softwaru. Zná metody jak se bránit útokům přes webové stránky a elektronickou poštu. Dokáže aplikovat zásady tvoření bezpečného hesla a dovede chránit svá data před ztrátou, odcizením a zneužitím. Je si vědom podstaty autorského zákona, práva autorském ve vztahu k softwaru a charakterizovat různé druhy licencí softwaru. Katalog požadavků obsahově zahrnuje široké spektrum témat. Nicméně zmíněné digitálně-bezpečnostní okruhy obsahující obecné bezpečnostní zásady, etické zásady a právní normy související s informatikou a všeobecné zabezpečení počítače jsou očekávanými požadavky vymezenými v katalogu požadavků zkoušek společné části maturitní zkoušky z informatiky vyšší a základní úrovně obtížnosti (Ministerstvo školství, mládeže a tělovýchovy, 2010).

4 Související výzkumy

Eckerová, Dočekal (2013) uvádí, že za uplynulá léta se změnil vztah mezi rodiči a dětmi. Nachází se zde generační propast, což v tomto případě znamená, že rodiče nejsou vybaveni znalostmi potřebnými k pomoci dětem v oblasti výpočetní techniky. Děti předběhly své rodiče ve znalosti digitálních technologií a proto rodiče nemohou dostatečně vychovávat své potomky k bezpečnosti v digitálním světě. Děti jsou v tomto směru na vyšší úrovni, učí své rodiče jak se v tomto světě pohybovat a jak používat výpočetní techniku. Děti už téměř nerozlišují virtuální svět od světa reálného a je tedy nesporné, že v používání informačních technologií můžeme očekávat nebezpečí, jak je tomu i ve světě reálném.

Jak uvádí Haddon (2012), každý den je 75 % českých dětí online a zbylých 22 % českých dětí je online jednou až dvakrát týdně. Z domova je připojeno k internetu 99 % dětí

z toho 63 % dětí je připojeno z vlastního pokoje. Dále 27 % českých dětí se stalo obětmi šikany a z toho 7 % šikany kybernetické. Dalším zarážejícím faktem je, že 44 % českých dětí bylo v online kontaktu s lidmi, které vůbec neznaly. České děti patří v Evropském měřítku k nadprůměru v používání internetu a s poměrně vysokým výskytem online rizik oproti jiným Evropským zemím. Představuje to výzvu jak pro školy, tak rodiče a jiné odpovědné osoby v zajištění bezpečného prostředí pro děti a pomoc dětem vypořádat se s těmito riziky. Děti by měly být vzděláváni v tomto směru více ve škole, neboť na rodičovské rady mnohdy není brán zřetel (Haddon, 2012).

Byron (2008) uvádí, že klíčovým bodem k zvládnutí současných a potenciálních rizik týkajících se právě digitálně-bezpečnostní problematiky se stává škola. Informační technologie si již našly místo v tomto prostředí a proto by měla škola být hlavním aktérem ve výchově a vzdělávání v oblasti digitální bezpečnosti.

5 Vlastní výzkum

5.1 Metoda práce

Vzhledem k faktu, že byla zvolena kvalitativní forma výzkumu, tak byla využita metoda dotazování a to za pomocí techniky polostrukturovaných rozhovorů.

5.2 Charakteristika výzkumného souboru

Znázornění vybraných respondentů pro výzkum

Vybraná základní škola, střední škola nebo gymnázium	Počet absolventů zařazených do výzkumu. (IT/bez IT)	Počet učitelů zařazených do výzkumu
Vyšší odborná škola, Střední škola, Centrum odborné přípravy, Sezimovo Ústí	2/2	2
Střední odborná škola veterinární, mechanizační a zahradnická a Jazyková škola s právem státní jazykové zkoušky	2/2	1
Střední škola spojů a informatiky	2/2	2
Střední průmyslová škola strojní a elektrotechnická	2/2	1
Obchodní akademie, Husova 1	3/0	1
Základní škola Kubatova	3/0	1
Základní škola Dukelská	3/0	1
Základní škola Rudolfov	3/0	1
Základní škola, Matice školské 3	3/0	1
Základní škola Lišov	3/0	1
Gymnázium Jírovcova	3/0	1
Gymnázia J. V. Jirsíka	3/0	1
Gymnázium Česká a Olympijských nadějí	3/0	1

Obr. 4: Znázornění vybraných respondentů pro výzkum

U každé mnou zvolené základní školy byly uskutečněny tři rozhovory s absolventy a jeden rozhovor s faktickým vyučujícím vybraných absolventů. U každé střední školy byli dotazováni dva absolventi oboru zaměřeného na informační technologie a dva absolventi bez zaměření na informační technologie. Zároveň byl uskutečněn vždy alespoň jeden rozhovor s vyučujícím vybraných absolventů. Tři absolventi a jeden vyučující byli dotazování v rámci vybraných gymnázií (viz obr. 4).

Hlavním kritériem výběru bylo absolvování vybrané základní školy, střední školy nebo gymnázia v Jihočeském kraji. Jednalo se o současné studenty prvního ročníku středních škol nebo studenty prvního ročníku vysokých škol. Absolventi vybraných škol byli vybíráni náhodně, jedinou podmínkou byla ochota uskutečnit rozhovor.

Pro naplnění komplexního pohledu na danou problematiku byl vybrán cílený doplňkový soubor učitelů vybraných základních škol, středních škol a gymnázií, kteří vyučují informační technologie a digitální bezpečnost. Učitelé, kteří byli vybráni museli splňovat kritérium faktické výuky respondentů.

5.3 Výběr škol

Výběr všech typů základních škol, středních škol a gymnázií v Jihočeském kraji byl náhodný. Střední školy byly vybírány dle zaměření, tak aby cílový vzorek respondentů obsahoval absolventy středních škol se zaměřením na výpočetní techniku a středních škol bez zaměření na výpočetní techniku. Poměr typů škol byl zachován dle poměru, který je v rámci Jihočeského kraje, kde rámcově na dvě střední odborné školy připadá jedno gymnázium. Typ gymnázia (čtyřleté, víceleté) nebyl pro výběr relevantním kritériem, vzhledem k faktu, že zkoumáni jsou absolventi, jejichž znalosti by měli být shodné.

5.4 Metody výzkumu

Pro získání aktuálního obrazu znázorňujícího stav výuky digitální bezpečnosti na vybraných základních a středních školách byla analýza výsledků provedena pomocí deskriptivního popisu.

Jednalo se o srovnání požadavků uvedených ve školních vzdělávacích programech, znalostí žáků a způsobu výuky digitální bezpečnosti, kde byly hledány rozdíly a odchylky mezi školními vzdělávacími programy a znalostmi digitální bezpečnosti u absolventů vybraných základních škol, středních škol a gymnázií. Pro můj výzkum bylo důležité zjistit s čím se absolventi ve výuce informatiky setkali a v jakém rozsahu.

Na základě rozhovorů s učiteli vybraných základních a středních škol byly hledány rozdíly mezi výpověďmi učitele, školními vzdělávacími programy a samotnými respondenty. Pro můj výzkum bylo důležité zjistit do jaké hloubky a v jakém rozsahu učitelé učí digitální bezpečnost na vybraných středních a základních školách. Digitální bezpečnost je vymezena na oblast výuky zálohování dat, používání softwarových bezpečnostních prvků, bezpečného chování na internetu včetně správy bezpečnostních hesel a problematiku autorského zákona.

V průběhu analýzy dat mohlo dojít k neshodě mezi výpověďmi respondentů vybrané školy a to v rozsahu a hloubce získaných znalostí z výuky. V tomto případě bylo přihlédnuto k výpovědi vyučujícího vybrané školy.

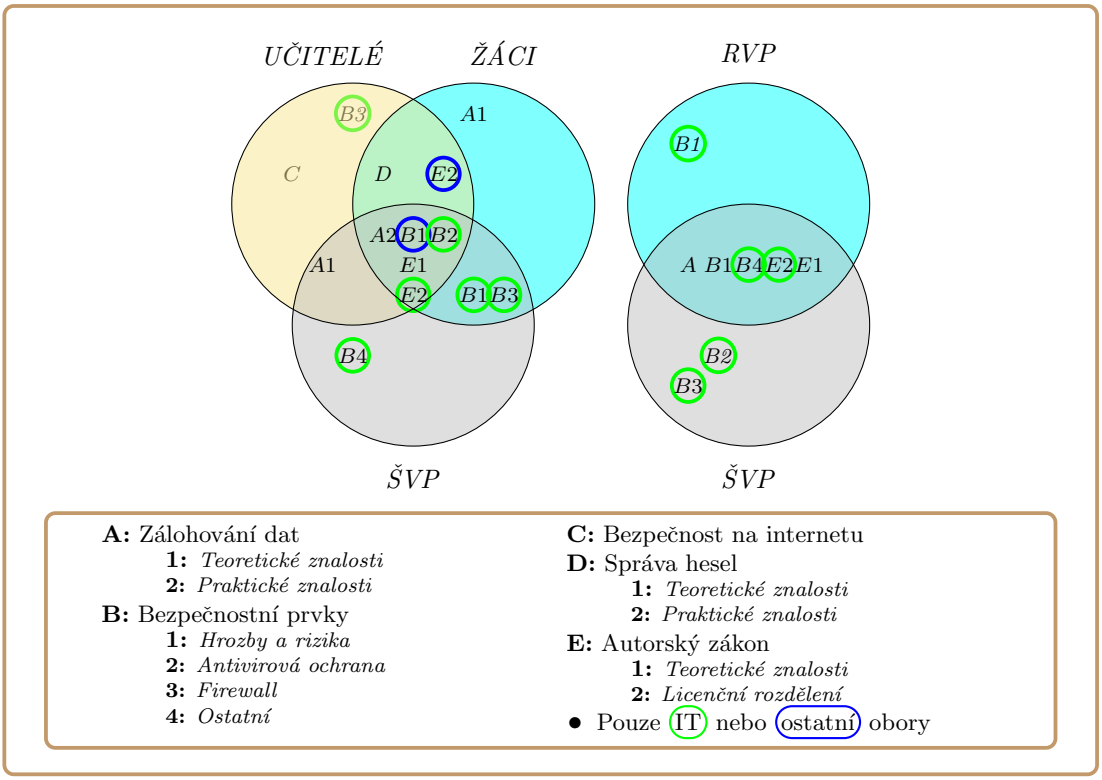
5.4.1 Výzkumné otázky

Výzkumné otázky byly stanoveny a zaměřují se na vybranou problematiku:

- Výzkumná otázka 1
  - Liší se výpovědi respondentů (absolventů) vybrané školy ohledně digitální bezpečnosti?
  - Jak a v čem se liší výpovědi učitelů výpočetní techniky a jejich žáků ohledně digitální bezpečnosti?
- Výzkumná otázka 2
  - Kooperují výpovědi žáků s obsahem, který je uveden ve školních vzdělávacích programech?
  - Odpovídají výpovědi učitelů obsahu, který je uveden ve školních vzdělávacích programech?

5.5 Výsledky analýzy vybraných středních škol

Střední škola, Centrum odborné přípravy Sezimovo Ústí



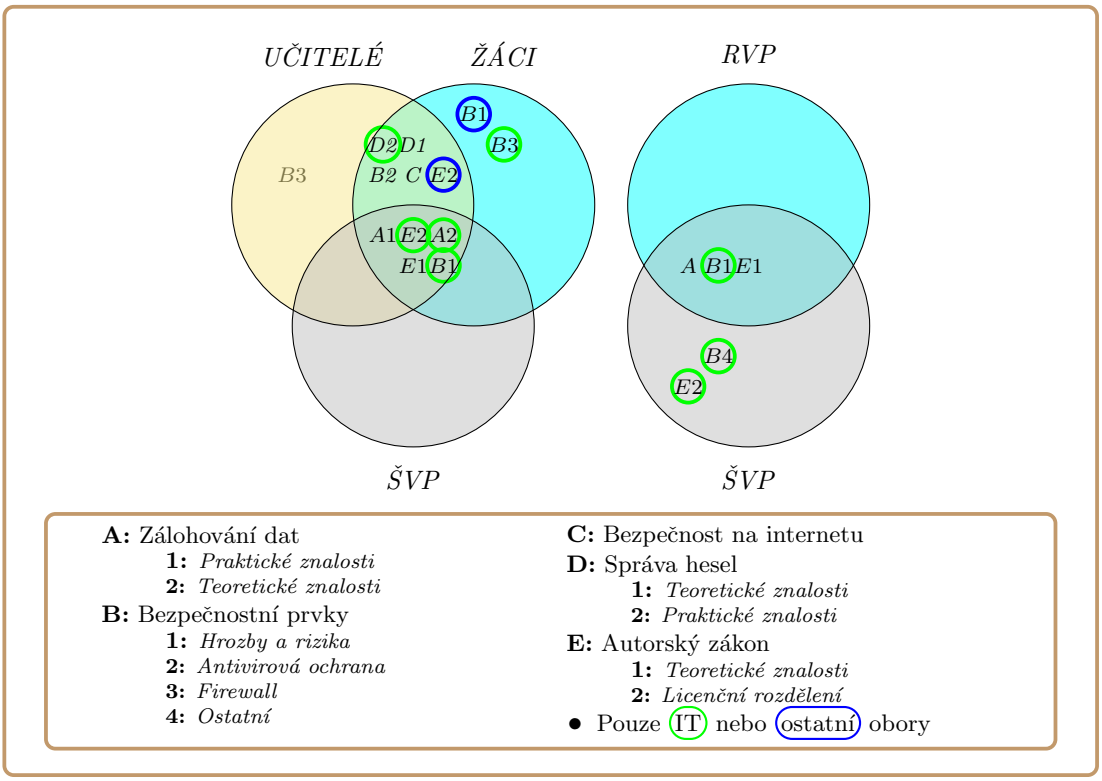
Obr. 5: Výsledky analýzy: Střední škola, Centrum odborné přípravy Sezimovo Ústí

Diagram tří množin znázorňuje výpovědi vyučujícího, výpovědi absolventů a vymezené oblasti digitální bezpečnosti ve školních vzdělávacích programech. V průniku množiny učitelů a respondentů lze poznat, že oblast výuky správy bezpečnostního hesla a licenční rozdělení u oborů bez IT zaměření se shodují v získaných znalostech absolventů a výpovědi vyučujícího. Z množiny vyučujících, která reprezentuje soubor pedagogů, kteří na škole učí, poznáme, že vyučující tvrdí, že se věnuje výuce firewall a bezpečného chování na internetu. Nicméně se neshoduje s výpovědí vyučujícího a školními vzdělávacími programy. Z množiny žáků poznáme, že absolventi byli učeni teorii zálohování dat, u které vyučující neuvedl, že se vybrané oblasti věnuje. Dále žáci IT oborů získali ve výuce znalosti v oblasti rizik a hrozeb, kterým lze čelit na internetu a firewall, u kterého se liší v rozsahu. V průniku množin učitele a ŠVP je shoda ve výuce teorie zálohování dat, ovšem neshoduje se v hloubce a rozsahu s žáky. Středový průnik vyjadřuje shodu u všech tří množin u oblasti praktických znalostí zálohování dat a autorského zákona. Dále jsou zde shody v oblasti antivirové ochrany a licenčního rozdělení softwaru u IT oborů a teorie zálohování dat u oborů bez zaměření na IT.

Diagram dvou množin vyjadřuje výskyty a shody digitální bezpečnosti mezi rámcovými a školními vzdělávacími programy. Průnik těchto dvou množin vyjadřuje

shodu mezi školními vzdělávacími programy a rámcovými vzdělávacími programy v oblastech zálohování dat, hrozeb a rizik, kterým lze čelit na internetu a autorského zákona. Dále je zde shoda u licenčního rozdělení softwaru a nutnosti aktualizace operačního systému. Oblasti digitální bezpečnosti mimo průnik znázorňují výskyt, ale neshodují se navzájem. Konkrétnější zpracování naleznete v tabulce viz příloha 1.

Střední odborná škola veterinární, mechanizační a zahradnická a Jazyková škola s právem státní jazykové zkoušky



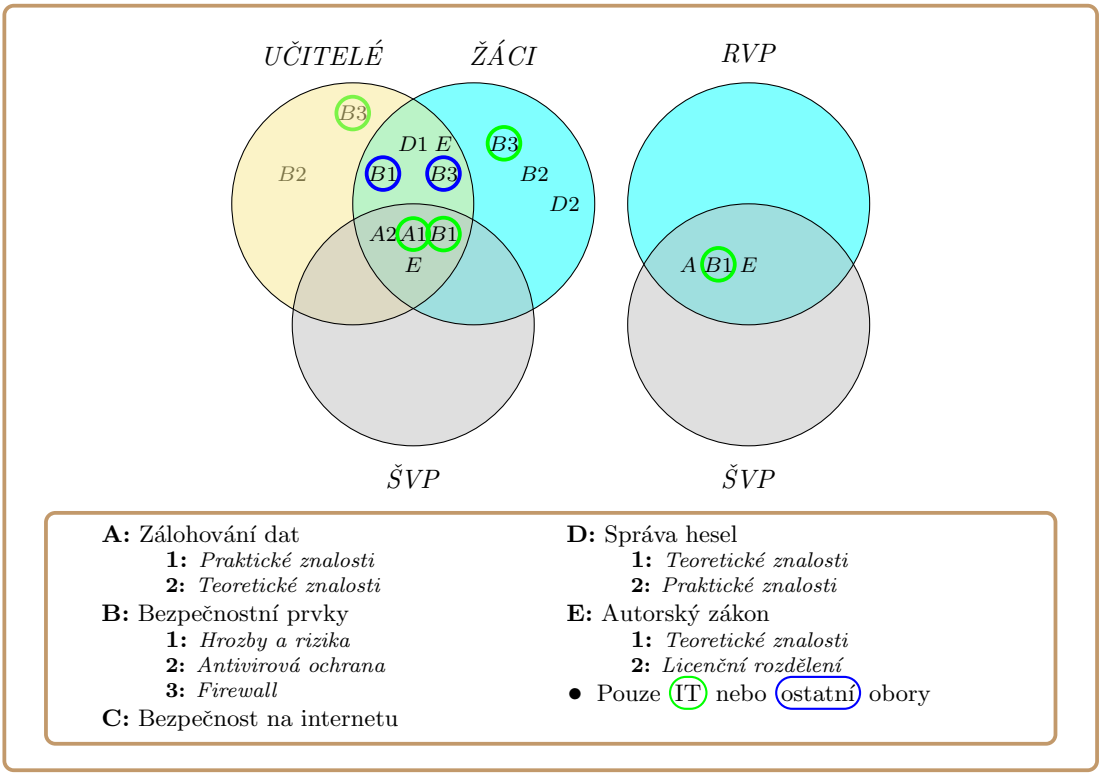
Obr. 6: Výsledky analýzy: Střední odborná škola veterinární, mechanizační a zahradnická a Jazyková škola s právem státní jazykové zkoušky

Diagram tří množin znázorňuje výpovědi vyučujícího, výpovědi absolventů a vymezené oblasti digitální bezpečnosti ve školních vzdělávacích programech. V průniku množiny učitelů a žáků lze poznat, že oblast výuky bezpečného chování na internetu, antivirové ochrany, teorie správy bezpečnostního hesla je naplňována. U IT oborů dochází ke shodě u praktických dovedností správy bezpečnostního hesla, oproti oborům bez zaměření, kde se vyskytuje shoda u licenčního rozdělení softwaru. Množina žáků dále reprezentuje získané znalosti z výuky v oblasti hrozeb a rizik, kterým lze čelit na internetu u oborů bez IT zaměření a získané znalosti v oblasti firewall u IT oborů, o které se vyučující nezmiňuje. Množina vyučujícího zobrazuje přítomnost výuky firewall, ovšem neshoduje se získanými znalostmi žáků. Středový průnik vyjadřuje shodu u všech tří množin u oblasti praktických znalostí zálohování dat a autorského zákona. Dále je zde shoda

u oborů zaměřených na IT v oblastech licenčního rozdělení softwaru, hrozeb a rizik, kterým zle čelit na internetu a teorie zálohování dat.

Diagram dvou množin vyjadřuje výskyty a shody digitální bezpečnosti mezi rámcovými a školními vzdělávacími programy. Průnik těchto dvou množin vyjadřuje shodu mezi školními vzdělávacími programy a rámcovými vzdělávacími programy v oblastech zálohován dat, autorského zákona a hrozeb a rizik, kterým lze čelit na internetu. Oblasti digitální bezpečnosti mimo průnik znázorňují výskyt, ale neshodují se navzájem. Konkrétnější zpracování naleznete v tabulce viz příloha 2.

Střední škola spojů a informatiky

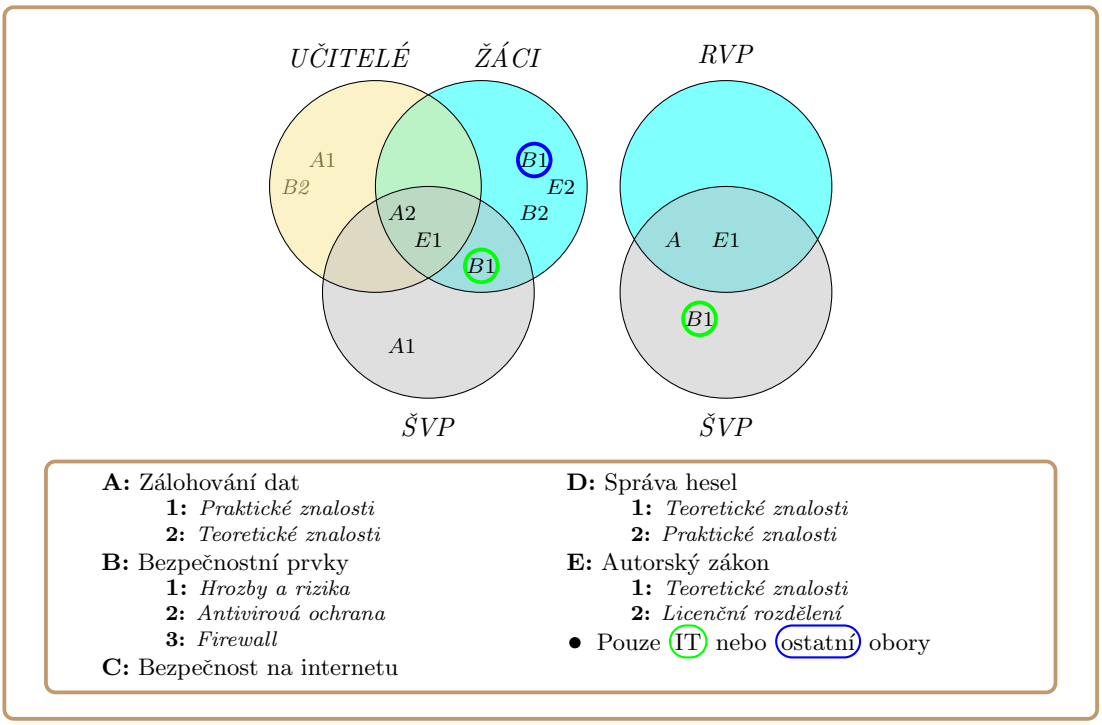


Obr. 7: Výsledky analýzy: Střední škola spojů a informatiky

Diagram tří množin znázorňuje výpovědi vyučujícího, výpovědi absolventů a vymezené oblasti digitální bezpečnosti ve školních vzdělávacích programech. V průniku množin vyučujícího a žáků lze poznat, že oblast výuky teorie správy bezpečnostních hesel a autorského zákona je naplňována. Dále u oborů bez zaměření na IT u oblastí firewall a hrozeb a rizik, kterým lze čelit na internetu. Množina žáků dále reprezentuje získané znalosti z výuky v oblasti antivirové ochrany a praktických znalostech správy bezpečnostního hesla. V množině žáků se dále nachází oblast výuky bezpečnostního prvku firewall u IT oborů, nicméně se neshoduje v rozsahu s výpovědí vyučujícího. Středový průnik vyjadřuje shodu u všech tří množin u oblasti autorského zákona, teorie zálohování dat a u IT oborů také praktické znalosti zálohování dat a hrozby a rizika.

Diagram dvou množin vyjadřuje výskyty a shody digitální bezpečnosti mezi rámcovými a školními vzdělávacími programy. Průnik těchto dvou množin vyjadřuje shodu mezi školními vzdělávacími programy a rámcovými vzdělávacími programy v oblastech zálohování dat a autorského zákona. Dále v oblasti hrozeb a rizik u IT oborů. Konkrétnější zpracování naleznete v tabulce viz příloha 3.

Střední průmyslová škola strojní a elektrotechnická



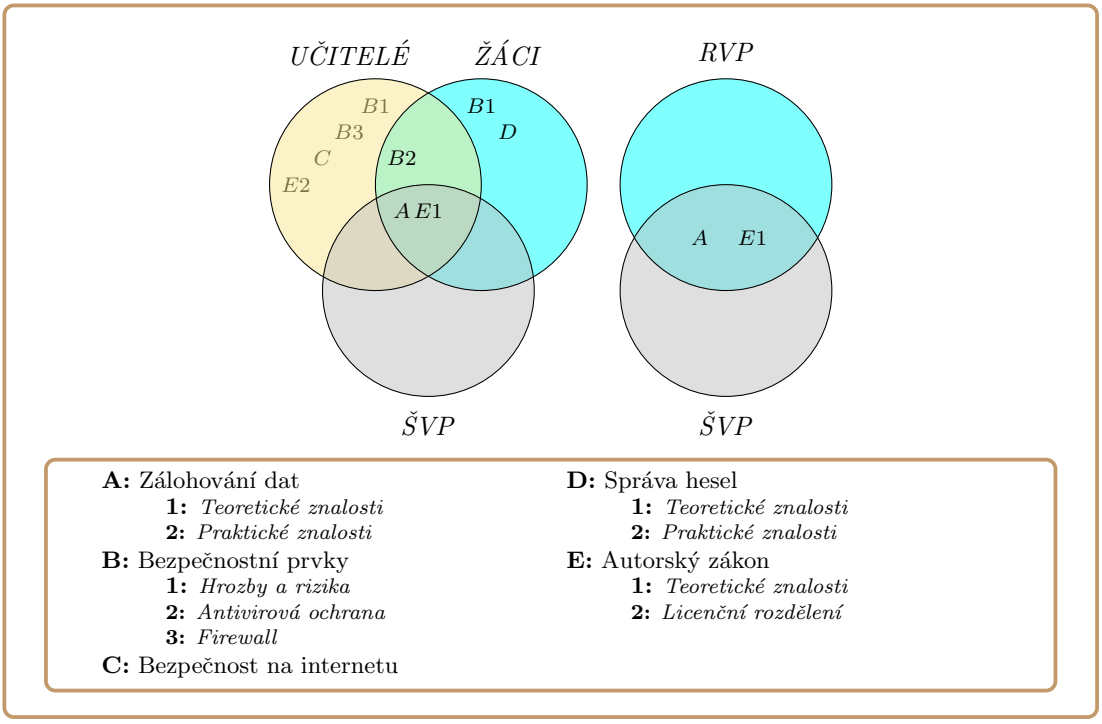
Obr. 8: Výsledky analýzy: Střední průmyslová škola strojní a elektrotechnická

Diagram tří množin znázorňuje výpovědi vyučujícího, výpovědi absolventů a vymezené oblasti digitální bezpečnosti ve školních vzdělávacích programech. V množině žáků můžeme pozorovat, že se absolventi ve výuce setkali s oblastí antivirové ochrany a licenčního rozdělení softwaru. Dále v oblasti hrozeb a rizik, kterým lze čelit na internetových stránkách u oborů bez zaměření na IT. Množina učitelů vyjadřuje oblasti, kterým se ve výuce vyučující věnuje a jsou to oblasti praktického zálohování dat a antivirové ochrany, ovšem neshodují s výpověďmi žáků. Středový průnik vyjadřuje shodu u všech tří množin u oblasti teorie zálohování dat a autorského zákona. V množině školních vzdělávacích programů se nachází oblast praktického zálohování dat, která není naplňována a žáci tvrdí, že se s vybranou oblastí ve výuce nesetkali. U průniku žáků a školních vzdělávacích programů je zřejmé, že praktické znalosti zálohování dat u IT oborů jsou naplňovány v porovnání se školními vzdělávacími programy.

Diagram dvou množin vyjadřuje výskyty a shody digitální bezpečnosti mezi rámcovými a školními vzdělávacími programy. Průnik těchto dvou množin vyjadřuje shodu mezi školními vzdělávacími programy a rámcovými vzdělávacími programy

v oblastech zálohování dat a teorie zálohování dat. Konkrétnější zpracování naleznete v tabulce viz příloha 4.

Obchodní akademie, Husova 1



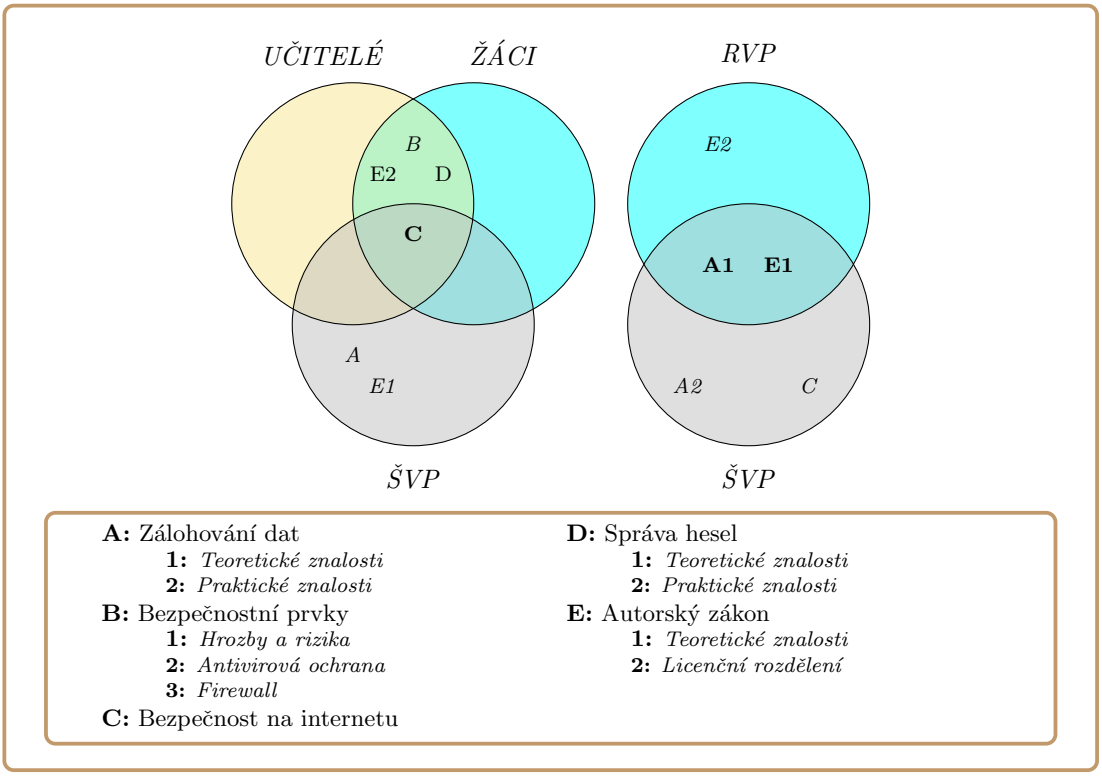
Obr. 9: Výsledky analýzy: Obchodní akademie, Husova 1

Diagram tří množin znázorňuje výpovědi vyučujícího, výpovědi absolventů a vymezené oblasti digitální bezpečnosti ve školních vzdělávacích programech. V průniku množin vyučujícího a respondentů lze poznat, že v oblasti výuky antivirové ochrany se shodují. Množina vyučujícího znázorňuje oblasti, u kterých vyučující uvádí, že se věnuje. Jsou to oblasti bezpečné chování na internetu, hrozby a rizika, kterým lze čelit na internetu, bezpečnostní prvek firewall a licenční rozdělení software, ale neshodují s výpověďmi žáků. Z množiny žáků lze vyčíst, že byli učeni správě bezpečnostního hesla a hrozby a rizika, kterým lze čelit na internet, ovšem neshodují s tvrzením vyučujícího a školními vzdělávacími programy. Středový průnik vyjadřuje shodu u všech tří množin u oblasti zálohování dat a teorie autorského zákona.

Diagram dvou množin vyjadřuje výskyty a shody digitální bezpečnosti mezi rámcovými a školními vzdělávacími programy. Průnik těchto dvou množin vyjadřuje shodu mezi školními vzdělávacími programy a rámcovými vzdělávacími programy v oblastech zálohování dat a teorie autorského zákona. Konkrétnější zpracování naleznete v tabulce viz příloha 5.

5.6 Výsledky analýzy vybraných základních škol

Základní škola Kubatova

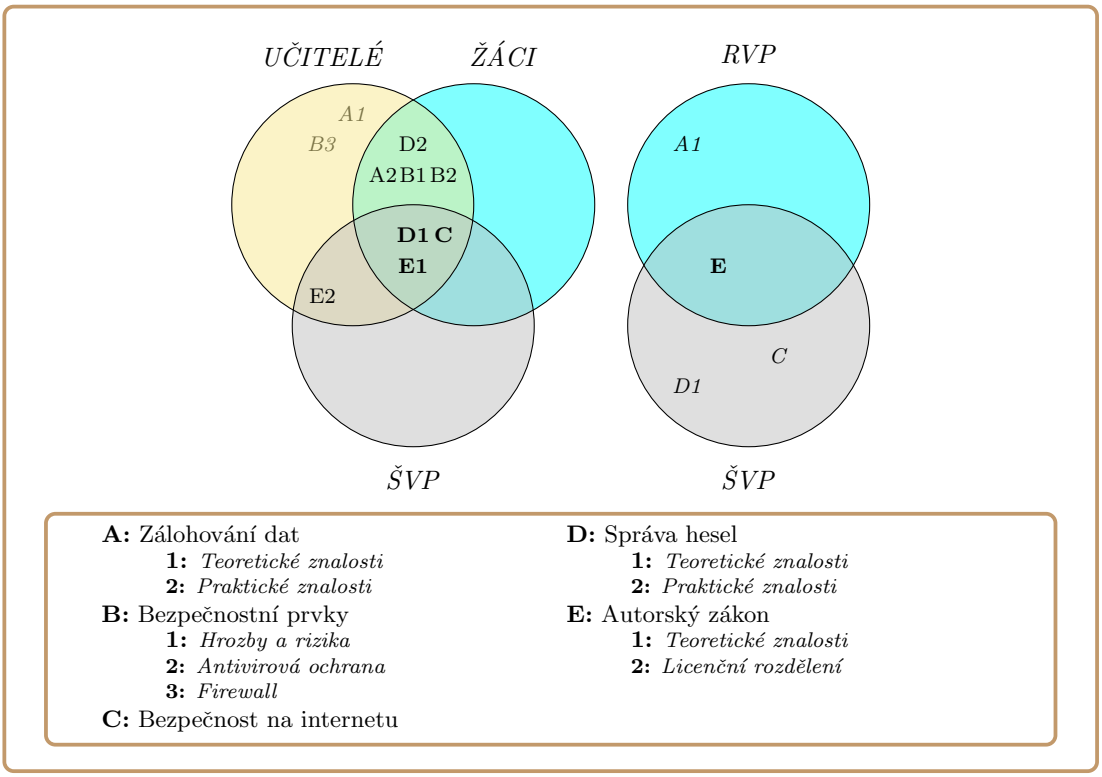


Obr. 10: Výsledky analýzy: Základní škola Kubatova

Diagram tří množin znázorňuje výpovědi vyučujícího, výpovědi absolventů a vymezené oblasti bezpečnosti ve školních vzdělávacích programech. Z průniku množin vyučujícího a žáků lze poznat, že oblast výuky softwarových bezpečnostních prvků, správy bezpečnostních hesel a licenčního rozdělení se shoduje v rozsahu získaných znalostí žáků a výpovědí učitele. Středový průnik vyjadřuje shodu všech tří množin u oblasti bezpečného chování na internetu. V množině školních vzdělávacích programů je obsaženo zálohování dat a teoretické znalosti autorského zákona. Ze strany učitele nebyla potvrzena výuka této oblasti a žáci uvádí, že se nesetkali s vybranou problematikou.

Diagram dvou množin vyjadřuje výskyty a shody digitální bezpečnosti mezi rámcovými a školními vzdělávacími programy. Průnik těchto dvou množin vyjadřuje shodu mezi školními vzdělávacími programy a rámcovými vzdělávacími programy v oblastech praktických znalostech zálohování dat a autorského zákona. Oblasti digitální bezpečnosti mimo průnik znázorňují výskyt, ale neshodují se navzájem. Konkrétnější zpracování naleznete v tabulce viz příloha 6.

Základní škola Dukelská

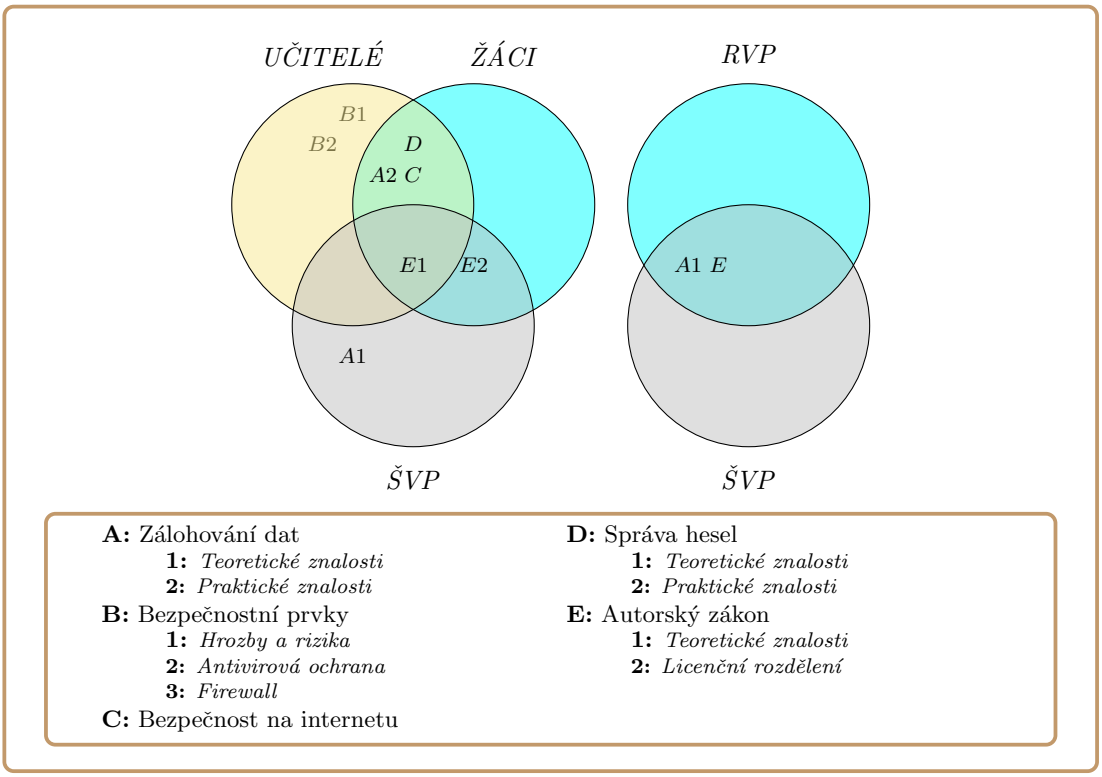


Obr. 11: Výsledky analýzy: Základní škola Dukelská

Diagram tří množin znázorňuje výpovědi vyučujícího, výpovědi absolventů a vymezené oblasti bezpečnosti ve školních vzdělávacích programech. Z průniku množin vyučujícího a žáků lze poznat, že oblast praktického zálohování dat, znalost hrozeb a rizik, praktických znalostí tvorby hesel se shodují ve výuce a získaných znalostech žáků. Z množiny vyučujících poznáme, že vyučující se věnuje výuce praktických postupů zálohování dat a výuce bezpečnostního prvku firewall, nicméně se neshoduje s žáky a školními vzdělávacími programy. Středový průnik vyjadřuje shodu u všech tří množin u oblastí bezpečného chování na internetu, teoretických znalostí bezpečnostního hesla a autorského zákona. Licenční rozdělení softwaru je vyučováno a shoduje se s školními vzdělávacími programy, ale žáci uvádí, že se s problematikou nesetkali.

Diagram dvou množin vyjadřuje výskyty a shody digitální bezpečnosti mezi rámcovými a školními vzdělávacími programy. Průnik těchto dvou množin vyjadřuje shodu mezi školními vzdělávacími programy a rámcovými vzdělávacími programy v oblasti bezpečného chování na internetu. Oblasti digitální bezpečnosti mimo průnik znázorňují výskyt, ale neshodují se navzájem. Konkrétnější zpracování naleznete v tabulce viz příloha 7.

Základní škola Rudolfov

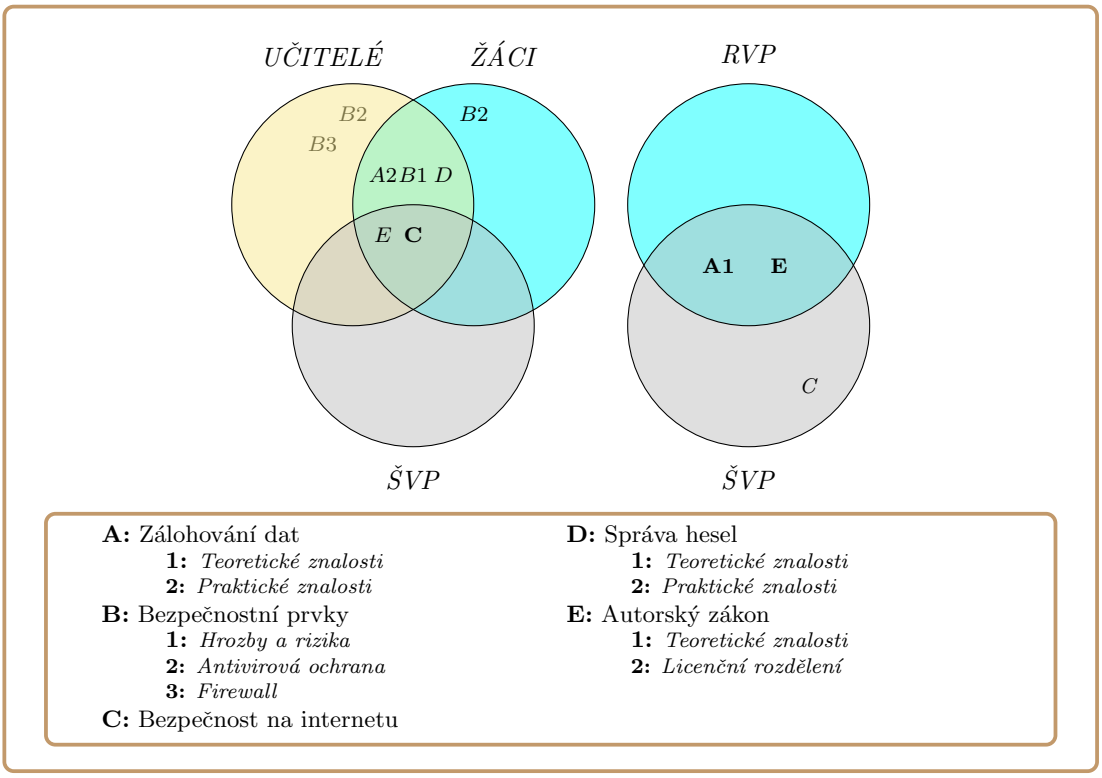


Obr. 12: Výsledky analýzy: Základní škola Rudolfov

Diagram tří množin znázorňuje výpovědi vyučujícího, výpovědi absolventů a vymezené oblasti bezpečnosti ve školních vzdělávacích programech. Z průniku množin vyučujícího a žáků lze poznat, že oblast teorie zálohování dat, bezpečného chování na internetu a správy bezpečnostního hesla se shodují ve výuce a získaných znalostech žáků. Z množiny vyučujících poznáme, že vyučující se věnuje výuce antivirových programů a možným nástrahám a hrozbám, nicméně se neshoduje s tvrzením žáků a školními vzdělávacími programy. Středový průnik vyjadřuje shodu u všech tří množin u oblasti teorie autorského zákona. Paradoxním jevem je shoda výpovědí žáků se školními vzdělávacími programy v oblasti licenčního rozdělení softwaru, navzdory faktu, že vyučující neuvedl výuku vybraného okruhu. Množina školních vzdělávacích programů zahrnuje praktické znalosti zálohování dat, nicméně se neshoduje se s ostatními množinami.

Diagram dvou množin vyjadřuje výskyty a shody digitální bezpečnosti mezi rámcovými a školními vzdělávacími programy. Průnik těchto dvou množin vyjadřuje shodu mezi školními vzdělávacími programy a rámcovými vzdělávacími programy v oblasti praktických znalostí zálohování dat a autorského zákona. Oblasti digitální bezpečnosti mimo průnik znázorňují výskyt, ale neshodují se navzájem. Konkrétnější zpracování naleznete v tabulce viz příloha 8.

Základní škola, Matice školské

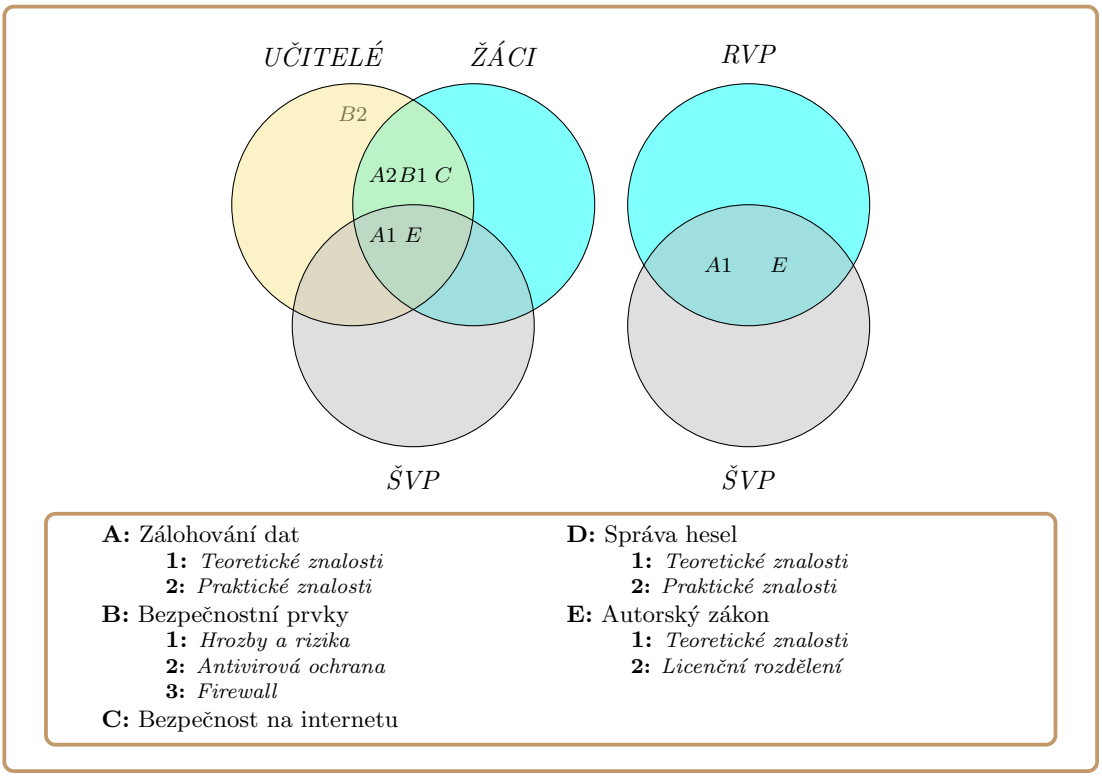


Obr. 13: Výsledky analýzy: Základní škola, Matice školské

Diagram tří množin znázorňuje výpovědi vyučujícího, výpovědi absolventů a vymezené oblasti bezpečnosti ve školních vzdělávacích programech. Z průniku množiny vyučujícího a žáků lze poznat, že oblast hrozby a rizika, teorie zálohování dat a správy bezpečnostního hesla se shodují ve výuce a získaných znalostech respondentů. Z množiny vyučujících poznáme, že vyučující uvádí výuku antivirové ochrany, bezpečnostnímu prvku firewall, nicméně se neshoduje s žáky a školními vzdělávacími programy. Množina žáků dále reprezentuje získané znalosti v oblasti antivirové ochrany, ovšem neshodují se s výpovědí učitele a školními vzdělávacími programy. Středový průnik vyjadřuje shodu u všech tří množin u oblasti bezpečného chování na internetu a autorského zákona.

Diagram dvou množin vyjadřuje výskyty a shody digitální bezpečnosti mezi rámcovými a školními vzdělávacími programy. Průnik těchto dvou množin vyjadřuje shodu mezi školními vzdělávacími programy a rámcovými vzdělávacími programy v oblasti teorie zálohování dat autorského zákona. Oblasti digitální bezpečnosti mimo průnik znázorňují výskyt, ale neshodují se navzájem. Konkrétnější zpracování naleznete v tabulce viz příloha 9.

Základní škola Lišov



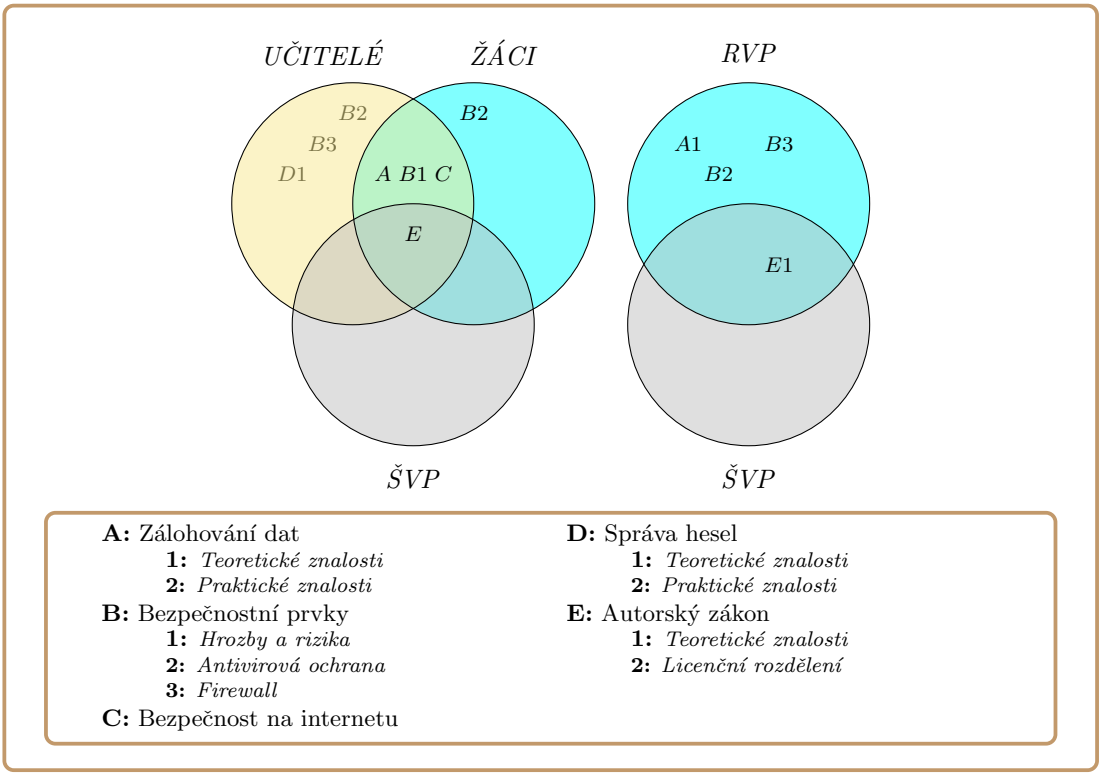
Obr. 14: Výsledky analýzy: Základní škola Lišov

Diagram tří množin znázorňuje výpovědi vyučujícího, výpovědi absolventů a vymezené oblasti bezpečnosti ve školních vzdělávacích programech. Z průniku množiny vyučujícího a respondentů lze poznat, že oblasti praktického zálohování, hrozeb a rizik a bezpečného chování na internetu se shodují ve výuce a získaných znalostech žáků. Z množiny vyučujících poznáme, že vyučující se věnuje výuce antivirové ochrany, nicméně se neshoduje s výpovědí žáků a školními vzdělávacími programy. Středový průnik vyjadřuje shodu u všech tří množin u oblastí autorského zákona a teorie zálohování dat.

Diagram dvou množin vyjadřuje výskyty a shody digitální bezpečnosti mezi rámcovými a školními vzdělávacími programy. Průnik těchto dvou množin vyjadřuje shodu mezi školními vzdělávacími programy a rámcovými vzdělávacími programy v oblasti teorie zálohování dat a autorského zákona. Oblasti digitální bezpečnosti mimo průnik znázorňují výskyt, ale neshodují se navzájem. Konkrétnější zpracování naleznete v tabulce viz příloha 10.

5.7 Výsledky analýzy vybraných gymnázií

Gymnázium Jírovcova

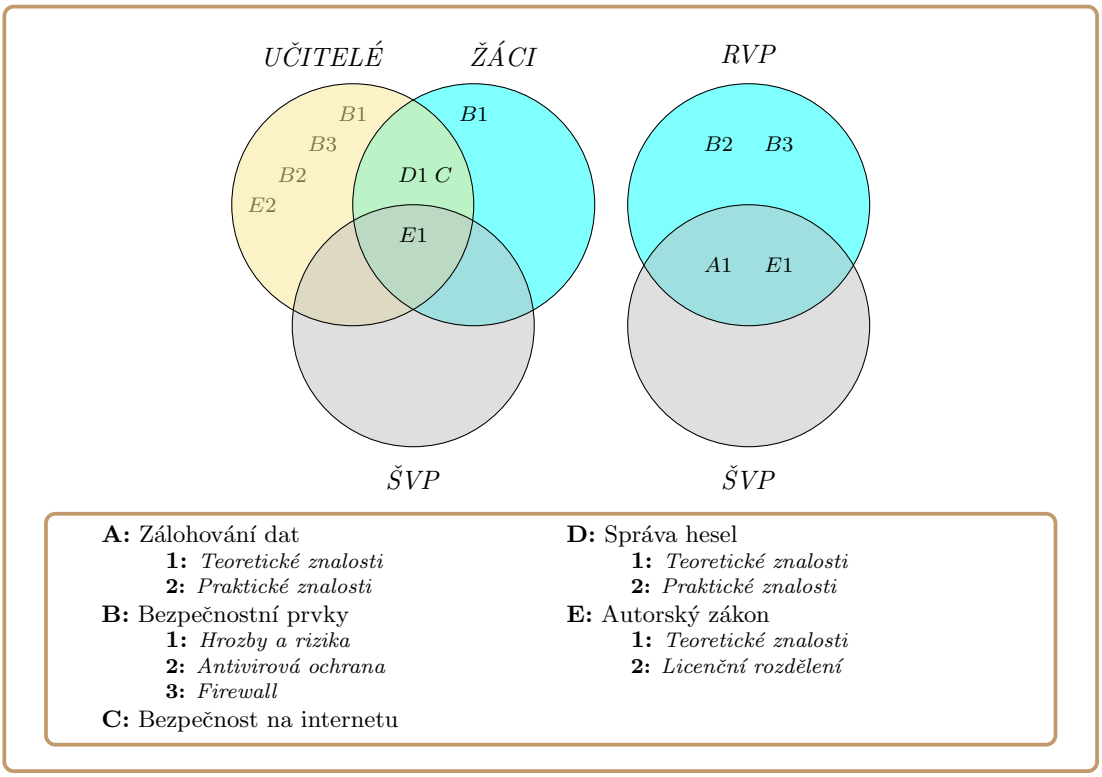


Obr. 15: Výsledky analýzy: Gymnázium Jírovcova

Diagram tří množin znázorňuje výpovědi vyučujícího, výpovědi absolventů a vymezené oblasti bezpečnosti ve školních vzdělávacích programech. Z průniku množiny vyučujícího a žáků lze poznat, že oblasti zálohování dat, hrozby a rizika a bezpečné chování na internetu se shodují ve výuce a získaných znalostech žáků. Z množiny vyučujícího poznáme, že vyučující uvádí výuku antivirové ochrany, bezpečnostního prvku firewall a teorii správy bezpečnostního hesla, nicméně se neshoduje s výpověďmi žáků a školními vzdělávacími programy. Středový průnik vyjadřuje shodu u všech tří množin u oblasti autorského zákona. Množina žáků dále prezentuje získané znalosti v oblasti antivirové ochrany, ovšem neshodují se s výpovědí vyučujícího a školními vzdělávacími programy.

Diagram dvou množin vyjadřuje výskyty a shody digitální bezpečnosti mezi rámcovými a školními vzdělávacími programy. Průnik těchto dvou množin vyjadřuje shodu mezi školními vzdělávacími programy a rámcovými vzdělávacími programy v oblasti teorie autorského zákona. Oblasti digitální bezpečnosti mimo průnik znázorňují výskyt, ale neshodují se navzájem. Konkrétnější zpracování naleznete v tabulce viz příloha 11.

Gymnázia J. V. Jirsíka

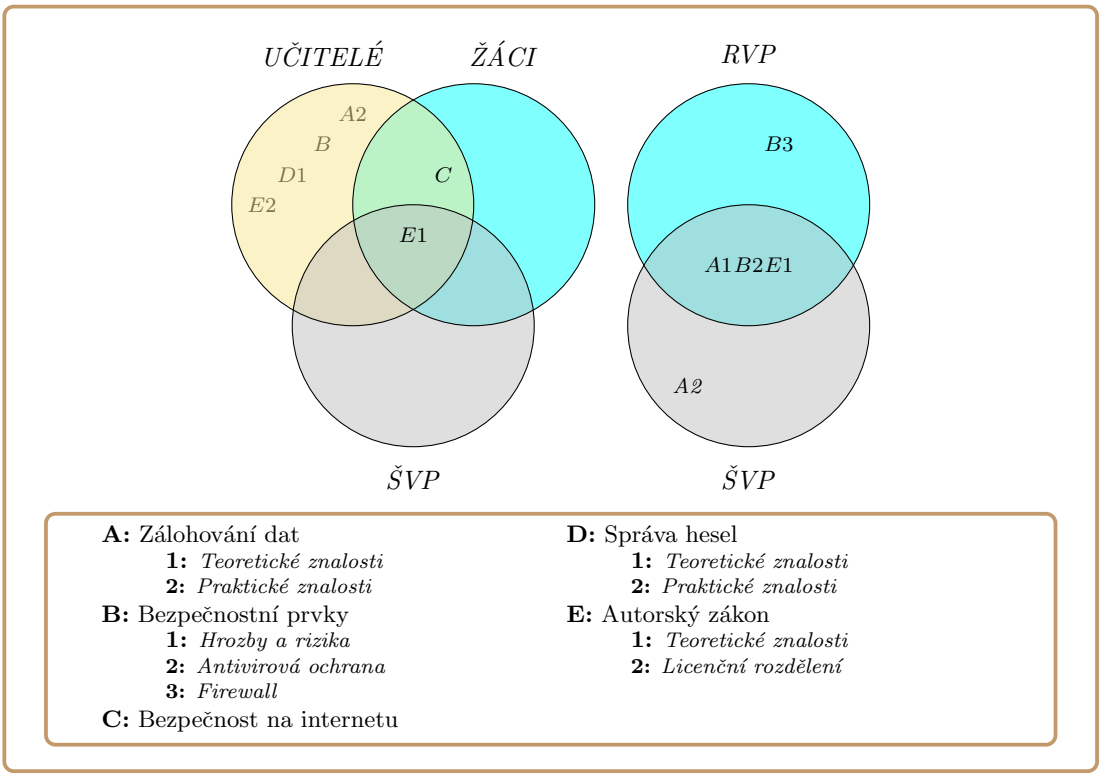


Obr. 16: Výsledky analýzy: Gymnázia J. V. Jirsíka

Diagram tří množin znázorňuje výpovědi vyučujícího, výpovědi absolventů a vymezené oblasti bezpečnosti ve školních vzdělávacích programech. Z průniku množiny vyučujícího a žáků lze poznat, že oblasti teorie správy bezpečnostního hesla a bezpečného chování na internetu se shodují. Z množiny vyučujícího poznáme, že učitel uvádí výuku bezpečnostních prvků a licenčního rozdělení softwaru, nicméně se neshoduje s výpověďmi žáků a školními vzdělávacími programy. Množina žáků dále reprezentuje získané znalosti v oblasti teorie zálohování dat, ovšem neshodují se s vyučujícím a školními vzdělávacími programy. Středový průnik vyjadřuje shodu u všech tří množin u oblasti teorie autorského zákona.

Diagram dvou množin vyjadřuje výskyty a shody digitální bezpečnosti mezi rámcovými a školními vzdělávacími programy. Průnik těchto dvou množin vyjadřuje shodu mezi školními vzdělávacími programy a rámcovými vzdělávacími programy v oblasti teorie zálohování dat a autorského zákona. Oblasti digitální bezpečnosti mimo průnik znázorňují výskyt, ale neshodují se navzájem. Konkrétnější zpracování naleznete v tabulce viz příloha 12.

Gymnázium Česká a Olympijských nadějí



Obr. 17: Výsledky analýzy: Gymnázium Česká a Olympijských nadějí

Diagram tří množin znázorňuje výpovědi vyučujícího, výpovědi absolventů a vymezené oblasti bezpečnosti ve školních vzdělávacích programech. Z průniku množin vyučujícího a respondentů lze poznat, že oblasti bezpečného chování na internetu. Z množiny vyučujících poznáme, že vyučující se věnuje výuce bezpečnostních prvků, praktickému zálohování dat, teorie správy bezpečnostního hesla a autorskému zákonu. Středový průnik všech tří množin vyjadřuje shodu u oblasti teorie autorského zákona.

Diagram dvou množin vyjadřuje výskyty a shody digitální bezpečnosti mezi rámcovými a školními vzdělávacími programy. Průnik těchto dvou množin vyjadřuje shodu mezi školními vzdělávacími programy a rámcovými vzdělávacími programy v oblasti teorie zálohování dat, antivirové ochrany a teorie autorského zákona. Oblasti digitální bezpečnosti mimo průnik znázorňují výskyt, ale neshodují se navzájem. Konkrétnější zpracování naleznete v tabulce viz příloha 13.

6 Diskuze

V rámci empirické části bakalářské práce jsem se rozhodl provést rozbor rámcových a vybraných školních vzdělávacích programů, kde jsem zjišťoval jaké prvky digitální bezpečnosti obsahují a v jaké hloubce. Dále jsem provedl vlastní šetření, kdy jsem ověřoval v jakém rozsahu a s jakými rozdíly jsou naplňovány vzdělávací požadavky na vybraných školách. Z toho důvodu jsem se rozhodl věnovat u diskuzi vybraným typům škol odděleně, k dosáhnutí co nejpodrobnějšímu popisu aktuálního stavu výuky digitální bezpečnosti.

6.1 Diskuze k základním školám

První částí výzkumné části bylo zjistit, jaké prvky digitální bezpečnosti jsou obsaženy ve školních vzdělávacích programech vybraných základních škol. Školní vzdělávací programy vycházejí z rámcových vzdělávacích programů základních škol, která doporučují výuku digitální bezpečnosti v rozsahu zálohování dat a autorského zákona. Výsledky mého výzkumu prokazují shodu rámcových a školních vzdělávacích programů. Další část mého výzkumu prokázala že tato shoda nemusí být zcela relevantní pro vlastní výuku digitální bezpečnosti. Z mého pohledu se nejedná o důležitý faktor, protože výuka digitální bezpečnosti je na základních školách na rozdílné úrovni. Nedochází k výrazným neshodám a na druhou stranu se mnohdy školní vzdělávací programy stávají přínosnějšími, než rámcové vzdělávací programy.

Oproti školním vzdělávacím programům dochází k deficitu znalostí a výuky u oblasti zálohování dat, u které nejsou naplňovány vzdělávací požadavky a žáci se s vybranou problematikou nesetkávají nebo jsou znalosti minimální. V rozhovorů s vyučujícími jsem dospěl k závěru, že oblast zálohování dat se dostává do útlumu a vyučující upřednostní výuku bezpečného chování na internetu, která se stává opravdu dominantní a vyučující jí přikládají velký význam. Za další pozitivní aspekt výuky digitální bezpečnosti na vybraných základních školách je teoretická výuka správy bezpečnostního hesla a praktická výuka autorského zákona.

Haddon (2012) tvrdí, že každý den je 75 % českých dětí online a zbylých 22 % českých dětí je online jednou až dvakrát týdně. Dalším zarážejícím faktem je, že 44 % českých dětí bylo v online kontaktu s lidmi, které vůbec neznaly. České děti patří v Evropském měřítku k nadprůměru v používání internetu a s poměrně vysokým výskytem online rizik oproti jiným Evropským zemím. Na základě výsledků mé práce a faktům uvedeným výše se domnívám a troufám si tvrdit, že žáci vybraných škol získávají dostatečné znalosti v oblasti digitální bezpečnosti, neboť výuka bezpečného chování na internetu je velice důležitá oproti ostatním okruhům výuky digitální bezpečnosti na vybraných základních školách.

6.2 Diskuze k středním školám

Druhou částí výzkumné části bakalářské práce bylo zjistit jaké prvky digitální bezpečnosti jsou obsaženy ve školních vzdělávacích programech vybraných středních

školách, kde jsem kladl důraz na rozlišení IT oborů a oborů bez zaměření na IT. Navzdory faktu, že rámcové vzdělávací programy středních škol jsou odlišné, tak všechny vybrané rámcové vzdělávací programy deklarují výuku oblasti zálohování dat a autorský zákon. Další oblasti digitální bezpečnosti už jsou závislé na konkrétním rámcovým vzdělávacím programu. Školní vzdělávací programy pokrývají oblasti digitální bezpečnosti uvedené v rámcových vzdělávacích programech, každopádně z rozboru vzdělávacích programů jsem dospěl k závěru, kdy pouze jedna škola z pěti zkoumaných škol měla své školní vzdělávací programy u IT oborů bohaté ohledně digitální bezpečnosti a plně pokrývala navíc oblast bezpečnostních prvků.

Z porovnání dílčích analýz středních škol jsem zjistil, že dochází k navazování a k doplnění chybějících znalostí ze základních škol. Výsledky mého výzkumu prokazují, že znalosti zálohování dat na středních školách jsou optimální, a dále také i softwarové bezpečnostní prvky. U rozhovorů s učiteli jsem narazil na fakt, že znalosti bezpečného chování na internetu by si měli žáci odnášet ze základní školy a proto se věnují problematice pouze okrajově, nicméně v dostatečném rozsahu. Mimo jiné vyučující vyučují oblasti správy bezpečnostního hesla, který není obsažen v rámcových vzdělávacích programech a rámcově ani ve školních vzdělávacích programech. U oblasti autorského zákona se na středních školách rozšiřuji toto téma o licenční rozdělení softwaru, které u základních škol chybělo.

Z porovnání výpovědí žáků IT oborů a žáků bez zaměření na IT vyplývá shoda v rozsahu a hloubce získaných digitálně-bezpečnostních znalostí. Shodu můžeme vnímat pozitivně, ale i negativně. Pokud bychom se zaměřili na žáky bez zaměření na IT, získané znalosti odpovídají získaným znalostem IT oborů, navzdory faktu, že školní vzdělávací programy oborů bez zaměření na IT neobsahují vybrané okruhy. Ovšem na druhou stranu, IT obory v tomto případě strádají. Získané znalosti neodpovídají v rozsahu a hloubce školních vzdělávacích programům vybraných IT oborů nebo výpovědi vyučujícího ohledně vyučované hloubky a rozsahu.

6.3 Diskuze k gymnáziím

Poslední částí mé výzkumné části bakalářské práce byl rozbor rámcových a školních vzdělávacích programů u vybraných gymnázií. Z rozboru vzdělávacích programů jsem dospěl k závěru, který není optimální. Rámcové vzdělávací programy jsou přínosnější ve srovnání s rámcovými vzdělávacími programy některých středních škol. Obsahují oblasti praktického zálohování dat a teorii autorského zákona, dále zahrnuje i softwarové bezpečnostní prvky. U školních vzdělávacích programů vybraných škol se shodují pouze částečně. Z výzkumu vyplývá, že získané znalosti žáků jsou minimální a nelze s jistotou tvrdit jaké oblasti digitální bezpečnosti jsou dominantní nebo v útlumu. Dochází k teoretickému předání znalosti, ale faktická znalost této problematiky se nepodařila prokázat.

Vzhledem k faktu, že na gymnáziích se vyučuje vše obecně a musí pokrýt široké spektrum učiva, tak to platí i u výuky digitální bezpečnosti. Vyučující tvrdí, že není dostatek času pro výuku této oblasti, ale i přesto se snaží pokrýt co nejširší spektrum. Výsledky mého výzkumu prokazují jediné a to je dostatečná znalost bezpečného

chování na internetu. U ostatních oblastí nelze s určitostí tvrdit, zda jsou naplňovány vzdělávací požadavky, neboť výpovědi vyučujících a žáků jsou velice rozdílné a dosahují minimální shody.

7 Závěr

Kvalitativní formou výzkumu bylo zjištěno v jakém rozsahu je na vybraných školách vyučována digitální bezpečnost a jak rozsáhlé znalosti získali žáci na vybraných školách. Dále bylo provedeno porovnání dílčích výsledků vybraných škol se školními vzdělávacími programy, díky kterému bylo možno dospět k závěru, zda jsou naplňovány vzdělávací požadavky uvedené v rámcových a školních vzdělávacích programech.

Po vyhodnocení získaných dat a rozboru školních vzdělávacích programů u základních škol se přikláním k závěru, že na mnou vybraných základních školách získané znalosti žáků odpovídají rozsahu učiva vyučovaného ve výuce informatiky. Nebyl jsem schopen prokázat plnou shodu se školními vzdělávací programy. Nicméně, vzdělávací požadavky, které nejsou naplňovány, jsou nahrazeny jinými oblastmi digitální bezpečnosti, které upřednostňují vyučující. K tomuto rozdílu dochází na základě možnosti úpravy školních vzdělávacích programů, ke které mají učitelé pravomoc v případě, že se domnívají, že by se vybrané problematice měli věnovat. U středních škol jsou naplňovány školní vzdělávací požadavky v plném rozsahu, ale rozsah a hloubka se liší u jednotlivých škol, neboť každá škola si vymezuje výuku digitální bezpečnosti dle svého uvážení. Pozitivním výsledkem můžu být zjištění, že základní znalosti vymezené ve školních vzdělávacích programech jsou naplňovány. Problematika výuky digitální bezpečnosti na mnou zvolených gymnáziích se v mém výzkumu jeví jako nejkomplikovanější. Můj výzkum na mnou zkoumaných gymnáziích neprokázal naplňování vzdělávacích požadavků stanovených ve školních vzdělávacích programech.

V této práci jsem se snažil popsat současný stav výuky digitální bezpečnosti na vybraných základních školách, středních školách a gymnáziích. Vzhledem k faktu, že šlo o kvalitativní sondu zaměřenou na na vybrané školy, bylo by zajímavé navázat na moji bakalářskou práci výzkumnou prací, která pomocí standardního statistického nástroje ověří závěry mého výzkumu ve větším rozsahu a dále ověří vybrané znalosti digitální bezpečnosti na základních a středních školách v praxi.

Literatura

[1] BYRON, Tanya. *Safer Children in a Digital World*. 2008. Department for Children, Schools and Families, and the Department for Culture, Media and Sport. Dostupné z: <http://goo.gl/GBmHcM>

[2] ČESKÁ REPUBLIKA. Zákon č. 561 ze dne 24. září 2004 o předškolním, základním, středním, vyšším odborném a jiném vzdělání. In: *Sbírka zákonů České republiky*. 2004. částka 190, s. 10262-10348. Dostupný z: <http://aplikace.mvcr.cz /sbirka-zakonu/ViewFile.aspx?type=c&id=4494>

[3] ČESKÁ REPUBLIKA. Zákon č. 121 ze dne 12. května 2000 o právu autorském, o právech souvisejících s právem autorským a o změně některých zákonů. In: *Sbírka zákonů České republiky*. 2000. částka 36, s. 1658. Dostupný z: <http://aplikace.mvcr.cz /sbirka-zakonu/ViewFile.aspx?type=c&id=3424>

[4] DOSEDĚL, T. *Počítačová bezpečnost a ochrana dat*. 2004. Computer Press. ISBN: 80-251-0106-1

[5] ECKERTOVÁ, L., DOČEKAL, D. *Bezpečnost dětí na Internetu*. 2013. Computer Press. ISBN: 978-80-251-3804-5

[6] FILMY NEJSOU ZADARMO. *Co je autorské právo?*. 2014. [online][cit. 2014-18-03]. Dostupné z: <http://www.filmynejsouzadarmo.cz /cs/co-je-autorske-pravo/>

[7] Get Safe Online. *Backups*. 2012c. [online][cit. 2014-02-23]. Dostupné z: <https://www.getsafeonline.org/protecting-yourself/passwords/#.UwjL CIXapRw>

[8] Get Safe Online. *Cyberbullying*. 2012h. [online][cit. 2014-02-23]. Dostupné z: <https://www.getsafeonline.org/safeguarding-children/cyber bullying/>

[9] Get Safe Online. *Cyberstalking*. 2012i. [online][cit. 2014-02-23]. Dostupné z: <https://www.getsafeonline.org/protecting-yourself/cyber stalking/>

[10] Get Safe Online. *Firewalls*. 2012e. [online][cit. 2014-02-23]. Dostupné z: <https://www.getsafeonline.org/protecting-your-computer/windows-up dates1/#.UxTaNIXapRw>

[11] Get Safe Online. *Passwords*. 2012a. [online][cit. 2014-02-23]. Dostupné z: <https:// www.getsafeonline.org/protecting-yourself/passwords/#.UwjL CIXapRw>

[12] Get Safe Online. *Social Networking Sites*. 2012g. [online][cit. 2014-02-23]. Dostupné z: <https://www.getsafeonline.org/social-networking/social -networking-sites/>

[13] Get Safe Online. *Viruses And Spyware*. 2012b. [online][cit. 2014-02-23]. Dostupné z: <https://www.getsafeonline.org/protecting-yourself/viruses-and-spyware/#.UwlDvoXapRw>

[14] Get Safe Online. *Windows Updates*. 2012d. [online][cit. 2014-02-23]. Dostupné z: <https://www.getsafeonline.org/protecting-your-computer/windows-updates1/#.UxTaNIXapRw>

[15] Get Safe Online. *Your Child and Social Networking*. 2012f. [online] [cit. 2014-02-23]. Dostupné z: <https://www.getsafeonline.org/safeguarding-children/your-child-and-social-networking/>

[16] HADDON, Leslie, LIVINGSTONE, Sonia and at al. *EU Kids Online: National perspectives*. 2012. Policy Press. Dostupné z: <http://goo.gl/0RAv9l>

[17] JEŘÁBEK, J., et al. *Manuál pro tvorbu školních vzdělávacích programů v základním vzdělávání*. 2005c. Praha: Výzkumný ústav pedagogický. Dostupné z: <http://www.nuv.cz/file/188_1_1/>. ISBN 80-87000-03-X

[18] JEŘÁBEK, J., et al. *Rámcový vzdělávací program pro gymnázia*. 2007b. Praha: Výzkumný ústav pedagogický. Dostupné z: <http://old.rvp.cz/soubor/RVP_G.pdf>. ISBN: 978-80-8700-11-3.

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

[20] KAŠPAROVÁ, J., et al. *Metodika tvorby školních vzdělávacích programů SOŠ a SOU*. 2012. Praha. Národní ústav pro vzdělávání, školské poradenské zařízení a zařízení pro další vzdělávání pedagogických pracovníků. Dostupné z: <http://www.nuv.cz/file/320_1_1/>. ISBN: 978-80-87652-05-3

[21] KOCMAN, L., LOHNISKÝ, J. *Jak se bránit virům, spamu, dialerům a spyware*. 2005. CP Books. ISBN: 80-251-0793-0.

[22] KOPECKÝ, K. *Co je hoax*. 2008. [online][cit. 2014-18-03]. Dostupné z: <http://www.e-bezpeci.cz/index.php/temata/hoax-spam/91-25>

[23] MINISTERSTVO ŠKOLSTVÍ, MLÁDEŽE A TĚLOVÝCHOVY. *Katalog požadavků zkoušek společné části maturitní zkoušky: Informatika, vyšší úroveň obtížnosti*. 2010. [online]. Centrum pro zjišťování výsledků vzdělávání. Dostupné z: <http://www.novamaturita.cz/index.php?id_document=1404034534&at=1>

[24] MINISTERSTVO ŠKOLSTVÍ, MLÁDEŽE A TĚLOVÝCHOVY. *Katalog požadavků zkoušek společné části maturitní zkoušky: Informatika, základní úroveň obtížnosti*. 2010. [online]. Centrum pro zjišťování výsledků vzdělávání. Dostupné z: <http://www.novamaturita.cz/index.php?id_document=1404034533&at=1>

[25] MINISTR, J. *INFORMATIKA - informační bezpečnost*. 2011, Karviná. Dostupné z: <http://www.ivsosoom.cz/_doc_download.php?idd=15>

[26] NÁRODNÍ ÚSTAV PRO VZDĚLÁVÁNÍ. *Rámcové vzdělávací programy*. 2013. [online][cit. 2013-26-12]. Dostupné z: <http://www.nuv.cz/ramcove-vzdelavaci-programy>

[27] POŽÁREK, J. a kol. *Základy teorie informační bezpečnosti*. 2007. PA ČR v Praze. ISBN: 987-80-7251-250-8

[28] ŠTĚDROŇ, B. *Ochrana a licencování počítačového programu*. 2010. [online]. Praha: Wolters Kluwer Česká republika. ISBN: 9788073575557

Seznam obrázků

Seznam příloh

Výsledky deskriptivní analýzy středních škol

- Příloha 1: Střední škola, Centrum odborné přípravy Sezimovo Ústí
- Příloha 2: Střední odborná škola veterinární, mechanizační a zahradnická a Jazyková škola s právem státní jazykové zkoušky
- Příloha 3: Střední škola spojů a informatiky
- Příloha 4: Střední průmyslová škola strojní a elektrotechnická
- Příloha 5: Obchodní akademie

Výsledky deskriptivní analýzy základních škol

- Příloha 6: Základní škola Dukelská
- Příloha 7: Základní škola Kubatova
- Příloha 8: Základní škola Rudolfov
- Příloha 9: Základní škola, Matice školské
- Příloha 10: Základní škola Lišov

Výsledky deskriptivní analýzy gymnázií

- Příloha 11: Gymnázium Jírovcova
- Příloha 12: Gymnázia J. V. Jirsíka
- Příloha 13: Gymnázium Česká a Olympijských nadějí

Ostatní

- Příloha 14: Dotazník pro absolventa
- Příloha 15: Dotazník pro učitele

Příloha 1

Střední odborná škola veterinární, mechanizační a zahradnická a Jazyková škola s právem státní jazykové zkoušky

IT obory / Ostatní obory	Vymezená oblast výuky	Rámcový vzdělávací program	Školní vzdělávací program	Hodnocení ŠVP s ohledem na RVP	Respondenti	Vyučující	Hodnocení znalostí respondenta s ohledem
Zálohování dat	Praktické dovednosti	Zná a aplikuje prostředky na zabezpečení dat před zničením a zneužitím.	Umí aplikovat prostředky pro zabezpečení dat před zneužitím a zničením. Návrh zabezpečení dat.	RVP a ŠVP se shodují.	Vytvoření bodu obnovy, paměťová média.	Možnosti zálohování.	Znalosti respondentů jsou odpovídající a shodují se s výpovědí vyučujícího.
	Teoretické znalosti	Je si vědom výhod a rizik spojených s prostředky ICT (zabezpečení dat před zneužitím a zničením).	Je si vědom výhod a rizik spojených s prostředky ICT (zabezpečení dat před zneužitím a zničením).	RVP a ŠVP se shodují.	Znají bod obnovy a vytvoření zálohy PC.	Důležitost zálohování. Diskuze na dotazy - Cloud.	Znalosti respondentů odpovídají až na okrajové téma (Cloud).
Softwarové bezpečnostní prvky	Hrozby a rizika		Chápe problematiku virové infekce.	ŠVP vybrané školy obsahují toto učivo, které není v RVP.	Viry, spam. Phishing, hacking.	Viry, hoax, škodlivé kódy. V rámci (WWW, PHP, email).	Znalosti respondentů nedosahují takové hloubky a rozsahu jak tvrdí vyučující u nonIT oborů.
	Antivirové programy			V této oblasti není učivo zadané jak v RVP, tak v ŠVP vybrané školy.	Instalace antiv. programu.	Instalace antivirového programu. DOS útok na server.	Znalosti respondentů jsou odpovídající a shodují se s výpovědí vyučujícího.
	Firewall			V této oblasti neni učivo zadané jak v RVP, tak v ŠVP vybrané školy.	V krajních případech teoreticky.	Firewall, nastavení výjimek, filtrování IP adres.	Respondenti se nesetkali s touto problematikou, ovšem vyučující se tématu věnuje.
	Ostatní		Znalost nutnosti aktualizace OS.	ŠVP vybrané školy obsahují toto učivo, které není obsaženo v RVP.			Respondenti nebyli seznámeni a vyučující se nevěnuje problematice.
Bezpečnost na internetu	Praktické dovednosti			V této oblasti není učivo zadané jak v RVP, tak v ŠVP vybrané školy.	Sdílené informace. Ochrana osobních údajů. Neznámé nekontaktovat.	Sociálních sítí. Anonymita. Vše je dohledatelné. Komunikace.	Znalosti respondentů se shodují s výpovědí vyučujícího.
Správa hesel	Teoretické dovednosti			V této oblasti není učivo zadané jak v RVP, tak v ŠVP vybrané školy.	Znají pravidla a další náležitosti pro tvorbu bezpečného hesla .	Základní pravidla tvorby bezpečného hesla.	Znalosti respondentů se shodují s výpovědí vyučujícího.
	Praktické znalosti			V této oblasti není učivo zadané jak v RVP, tak v ŠVP vybrané školy.	Dokáží vytvořit dostatečně bezpečné heslo.	Vytvoření si vlastního hesla kontrolované servrem.	Znalosti respondentů se shodují s výpovědí vyučujícího.
Autorský zákon	Teoretické znalosti	Ochrana autorského zákona.	Zná právní normy, autorský zákon, ochrana vlastnictví informací.	ŠVP obsahují další témata tohoto učiva.	Znají duševní vlastnictví, porušení autorského zákona.	V rámci autorského zákona. Legalita a rozdíly v zahraničí.	Znalosti respondentů se shodují s výpovědí vyučujícího.
	Licenční rozdělení software		Uvědomuje si výhody, nevýhody a rizika při práce se software.	ŠVP vybrané školy obsahují toto učivo, které není obsaženo v RVP.	Mají znalosti různých typů software dle licence.	Teoreticky. Komerční-freeware. Možnosti softwaru.	Znalosti respondentů se shodují s výpovědí vyučujícího.

Příloha 2

Střední škola spojů a informatiky							
IT obory / Ostatní obory	Vymezená oblast výuky	Rámcový vzdělávací program	Školní vzdělávací program	Hodnocení ŠVP s ohledem na RVP	Respondenti	Vyučující	Hodnocení znalostí respondenta s ohledem
Zálohování dat	Praktické dovednosti	Zná a aplikuje prostředky na zabezpečení dat před zničením a zneužitím. Zálohuje OS a data.	Umí aplikovat prostředky pro zabezpečení dat před zneužitím a zničením. Návrh zabezpečení dat.	ŠVP vybrané školy neobsahují učivo, které je obsaženo v RVP.	Záloha systému. Záloha serverů.	Možnosti zálohování. Pravidelnost a automatizace. Záloha serverů.	Znalosti respondentů jsou v tomto případě poloviční a nedosahují odpovídající hloubky.
	Teoretické znalosti	Je si vědom výhod a rizik spojených s prostředky ICT (zabezpečení dat před zneužitím a zničením).	Je si vědom výhod a rizik spojených s prostředky ICT (zabezpečení dat před zneužitím a zničením).	ŠVP vybrané školy neobsahují učivo, které je obsaženo v RVP.	Možnosti zálohování (média).	Důležitost a způsoby zálohování.	Znalosti respondentů jsou odpovídající a shodují se s výpovědí vyučujícího.
Softwarové bezpečnostní prvky	Hrozby a rizika	Viry, spyware.	Zabezpečení proti virům a jiným škodlivým kódům.	RVP a ŠVP se shodují u IT oboru.	Viry, spam, phishing, zneužití os. údajů	Viry, červy, malware, adware, hacking, DOS útoky.	Znalosti respondentů jsou odpovídající až na DOS útok.
	Antivirové programy			V této oblasti není učivo zadané jak v RVP, tak v ŠVP vybrané školy.	Aktualizace a instalace anti. programu. Diskuze jaký a proč.	Prakticky ne, pouze zabezpečení serveru.	Znalosti respondentů jsou v tomto případě poloviční a nedosahují odpovídající hloubky.
	Firewall			V této oblasti není učivo zadané jak v RVP, tak v ŠVP vybrané školy.	Funkce firewall, kontrola dat. IT obor, nastavení portů.	Zabezpečení portů. Tvorba vlastní IP tabulky. Nastavení časový, lokální.	Znalosti respondentů se shodují minimálně a to v rozsahu základní znalosti.
	Ostatní			V této oblasti není učivo zadané jak v RVP, tak v ŠVP vybrané školy.			Respondenti nebyli seznámeni a vyučující se nevěnuje problematice.
Bezpečnost na internetu	Praktické dovednosti			V této oblasti není učivo zadané jak v RVP, tak v ŠVP vybrané školy.	Identita/anonymita. Množství sdílených dat. Obtěžování. Diskuze na Cloud.	Diskuze. Ochrana dat, sdílení os. údajů. Diskuze na Cloud, bezpečnost.	Znalosti respondentů jsou odpovídající a shodují se s výpovědí vyučujícího.
Správa hesel	Teoretické dovednosti			V této oblasti není učivo zadané jak v RVP, tak v ŠVP vybrané školy.	Základní pravidla pro tvorbu bez. hesla.	Základní pravidla. Jakým způsobem řešit tuto problematiku.	Znalosti respondentů jsou odpovídající a shodují se s výpovědí vyučujícího.
	Praktické znalosti			V této oblasti není učivo zadané jak v RVP, tak v ŠVP vybrané školy.	Dovedou vytvořit dostatečně silné heslo.		Respondent svede vytvořit bez. heslo, i když vyučující se prak. postupům nevěnuje.
Autorský zákon	Teoretické znalosti	Ochrana autorského zákona.	Ochrana autorského zákona.	ŠVP vybrané školy neobsahují učivo, které je obsaženo v RVP.	Duševní vlastnictví, postihy za porušení. Stahování.	Ochrana autora. Stahování a kopírování, postihy u nás a svět.	Znalosti respondentů jsou odpovídající a shodují se s výpovědí vyučujícího.
	Licenční rozdělení software	Licence, druhy SW, shareware, freeware. Autorská práva.	Základní a aplikační programové vybavení.	ŠVP vybrané školy neobsahují učivo, které je obsaženo v RVP.	Freeware, shareware, trial, demo, komerční.	Základní rozdělení, možnosti jak přistupovat k SW.	Znalosti respondentů jsou odpovídající a shodují se s výpovědí vyučujícího.

Příloha 3

Střední průmyslová škola strojní a elektrotechnická							
IT obory / Vymezená oblast výuky	Ostatní obory	Rámcový vzdělávací program	Školní vzdělávací program	Hodnocení ŠVP s ohledem na RVP	Respondenti	Vyučující	Hodnocení znalostí respondenta s ohledem
Zálohování dat	Praktické dovednosti	Zná a aplikuje prostředky na zabezpečení dat před zničením a zneužitím.	Umí aplikovat prostředky pro zabezpečení dat před zneužitím a zničením. Návrh zabezpečení dat.	RVP a ŠVP se shodují.		Způsoby ukládání dat a zálohování. Raid, mirroring.	Respondenti nezískali vybrané znalosti i když vyučující se okruhu věnuje.
	Teoretické znalosti	Je si vědom výhod a rizik spojených s prostředky ICT (zabezpečení dat před zneužitím a zničením).	Je si vědom výhod a rizik spojených s prostředky ICT (zabezpečení dat před zneužitím a zničením).	RVP a ŠVP se shodují.	Možnosti zálohy, cloud.	Možnosti zálohování a pravidelnost.	Znalosti respondentů jsou odpovídající a shodují se s výpovědí vyučujícího.
Softwarové bezpečnostní prvky	Hrozby a rizika		Chápe problematiku virové infekce.	V této oblasti není učivo zadané jak v RVP, tak v ŠVP vybrané školy.	Viry, spam, validita stránek.		Respondenti získali vybrané znaslosti i když vyučující se okruhu nevěnuje.
	Antivirové programy			V této oblasti není učivo zadané jak v RVP, tak v ŠVP vybrané školy.	Slabé znalosti, pouze teoretické (nusnost antiviru).	Instalace antivirového programu. Principy (vir. databáze, scann, rozdělení).	Znalosti respondentů nedosahují takové hloubky a rozsahu jak tvrdí vyučující.
	Firewall			V této oblasti není učivo zadané jak v RVP, tak v ŠVP vybrané školy.			Respondenti nezískali vybrané znalosti a vyučující se nevěnuje problematice.
	Ostatní			V této oblasti není učivo zadané jak v RVP, tak v ŠVP vybrané školy.			Respondenti nezískali vybrané znalosti a vyučující se nevěnuje problematice.
Bezpečnost na internetu	Praktické dovednosti			V této oblasti není učivo zadané jak v RVP, tak v ŠVP vybrané školy.		Očekává se znalost ze ZŠ. Okrajově (identita, anonymita, sdílená data).	Respondenti nezískali vybrané znalosti i když vyučující se okruhu věnuje.
Správa hesel	Teoretické dovednosti			V této oblasti není učivo zadané jak v RVP, tak v ŠVP vybrané školy.			Respondenti nezískali vybrané znalosti a vyučující se nevěnuje problematice.
	Praktické znalosti			V této oblasti není učivo zadané jak v RVP, tak v ŠVP vybrané školy.			Respondenti nezískali vybrané znalosti a vyučující se nevěnuje problematice.
Autorský zákon	Teoretické znalosti	Ochrana autorského práva.	Zná právní normy, autorský zákon, ochrana vlastnictví informací.	RVP a ŠVP se shodují.	Duševní vlastnictví, legalita a postihy.	V rámci práce s internetem. Duševní vlastnictví, stahování, kopírování textů.	Znalosti respondentů jsou odpovídající a shodují se s výpovědí vyučujícího.
	Licenční rozdělení software			V této oblasti není učivo zadané jak v RVP, tak v ŠVP vybrané školy.	Freeware, shareware, demo, komerční. Podmínky použití.		Respondenti získali vybrané znalosti i když vyučující se okruhu nevěnuje.

Příloha 4

Střední škola, Centrum odborné přípravy Sezimovo Ústí							
IT obory / Vymezená oblast výuky	Ostatní obory	Rámcový vzdělávací program	Školní vzdělávací program	Hodnocení ŠVP s ohledem na RVP	Respondenti	Vyučující	Hodnocení znalostí respondenta s ohledem
Zálohování dat	Praktické dovednosti	Zná a aplikuje prostředky na zabezpečení dat před zničením a zneužitím.	Umí aplikovat prostředky pro zabezpečení dat před zneužitím a zničením. Zálohuje OS.	RVP a ŠVP se shodují.	Zálohování Cloud a paměťová média.	Principy zálohování. Windows záloha.	Znalosti respondentů nedosahují takové hloubky a rozsahu jak tvrdí vyučující.
	Teoretické znalosti	Je si vědom výhod a rizik spojených s prostředky ICT (zabezpečení dat před zneužitím a zničením).	Je si vědom výhod a rizik spojených s prostředky ICT (zabezpečení dat před zneužitím a zničením).	RVP a ŠVP se shodují.	Možnosti zálohování. Důležitost a pravidelnost.	Možnosti zálohování. Produkty třetí strany.	Znalosti respondentů jsou odpovídající a shodují se s výpovědí vyučujícího.
Softwarové bezpečnostní prvky	Hrozby a rizika	Viry, spyware. Zná způsoby napadení sítí.	Viry, hacking.	RVP a ŠVP se shodují. RVP nonIT oboru neobsahují dané téma.	Viry, spam, hacking, červy	Viry, virové politiky, mail security (spam). IT zabezpečení sítě.	Znalosti IT respondentů nedosahují takové hloubky a rozsahu jak tvrdí vyučující.
	Antivirové programy		Používat vhodné antivirové a spamové programy.	ŠVP vybrané školy obsahují toto učivo, které není obsaženo v RVP.	Praktické znalosti instalace a možností ativ. programu.	Virové programy, co nabízí, jak a jaké využít.	Znalosti respondentů jsou odpovídající a shodují se s výpovědí vyučujícího.
	Firewall		Naučí se nastavit firewall.	ŠVP vybrané školy obsahují toto učivo, které není obsaženo v RVP.	Existence firewall, základní princip a nastavení.	Základní znalosti. Hardware, software. Firewall prakticky + router firewall.	Znalosti respondentů nedosahují takové hloubky a rozsahu jak tvrdí vyučující.
	Ostatní	Aktualizace OS	Aktualizace OS	RVP a ŠVP se shodují.			Respondenti nebyli seznámeni a vyučující se nevěnuje problematice.
Bezpečnost na internetu	Praktické dovednosti			V této oblasti není učivo zadané jak v RVP, tak v ŠVP vybrané školy.		Formou diskuze, jaké očekávat hrozby, množství sdílených dat.	Znalosti se neshodují s výpovědí vyučujícího.
Správa hesel	Teoretické dovednosti			V této oblasti není učivo zadané jak v RVP, tak v ŠVP vybrané školy.	Pravidla a náležitosti bezpečného hesla.	Politika vytváření hesel. Základní pravidla.	Znalosti respondentů jsou odpovídající a shodují se s výpovědí vyučujícího.
	Praktické znalosti			V této oblasti není učivo zadané jak v RVP, tak v ŠVP vybrané školy.	Dostatečné k vytvoření bezpečného hesla.	Každý student vytváří svoje heslo.	Znalosti respondentů jsou odpovídající a shodují se s výpovědí vyučujícího.
Autorský zákon	Teoretické znalosti	Ochrana autorského zákona.	Ochrana autorského zákona.	RVP a ŠVP se shodují.	Duševní vlastnictví, autorské práva, plagiátorství.	Na co si dávat pozor, následky. Copyright.	Znalosti respondentů jsou odpovídající a shodují se s výpovědí vyučujícího.
	Licenční rozdělení software	Druhy SW, shareware, freeware. Licence.	Základní a aplikační programové vybavení.	RVP a ŠVP se shodují.	Rozdělení SW, freeware, shareware, trial, demo.	Jedná se o základní znalosti. Pouze okrajově základní rozdělení.	Znalosti respondentů jsou odpovídající a shodují se s výpovědí vyučujícího.

Příloha 5

Obchodní akademie, Husova 1							
Vymezená oblast výuky		Rámcový vzdělávací program	Školní vzdělávací program	Hodnocení ŠVP s ohledem na RVP	Respondenti	Vyučující	Hodnocení znalostí respondenta s ohledem na vyučujícího
Zálohování dat	Praktické dovednosti	Zná a aplikuje prostředky na zabezpečení dat před zničením a zneužitím.	Zná a aplikuje prostředky na zabezpečení dat před zničením a zneužitím.	RVP a ŠVP se shodují.	Internetová úložiště, Flash.	Možnosti zálohování.	Znalosti respondentů jsou odpovídající a shodují se s výpovědí vyučujícího.
	Teoretické znalosti	Je si vědom výhod a rizik spojených s prostředky ICT (zabezpečení dat před zneužitím a zničením).	Je si vědom výhod a rizik spojených s prostředky ICT (zabezpečení dat před zneužitím a zničením).	RVP a ŠVP se shodují.	Pravidelnost zálohování a důležitost.	Důležitost zálohování. Jakým způsobem a jak často.	Znalosti respondentů jsou odpovídající a shodují se s výpovědí vyučujícího.
Softwarové bezpečnostní prvky	Hrozby a rizika			V této oblasti není učivo zadané jak v RVP, tak v ŠVP vybrané školy.	Viry.	Kde lze přijít k viry. Čemu se vyvarovat.	Znalosti se neshodují s výpovědí vyučujícího.
	Antivirové programy			V této oblasti není učivo zadané jak v RVP, tak v ŠVP vybrané školy.	Proč mít antivirus.	Důležitost antivirového programu.	Znalosti respondentů jsou odpovídající a shodují se s výpovědí vyučujícího.
	Firewall			V této oblasti není učivo zadané jak v RVP, tak v ŠVP vybrané školy.		Existence Windows firewall	Respondenti nezískali vybrané znalosti i když vyučující se okruhu věnuje.
	Ostatní			V této oblasti není učivo zadané jak v RVP, tak v ŠVP vybrané školy.			
Bezpečnost na internetu	Praktické dovednosti			V této oblasti není učivo zadané jak v RVP, tak v ŠVP vybrané školy.		Proč by měl být každý ostražitý. Jak je to se soukromím.	Respondenti nezískali vybrané znalosti i když vyučující se okruhu věnuje.
Správa hesel	Teoretické dovednosti			V této oblasti není učivo zadané jak v RVP, tak v ŠVP vybrané školy.	Znají pravidla a další náležitosti pro tvorbu bezpečného hesla .		Respondenti získali vybrané znalosti i když vyučující se okruhu nevěnuje.
	Praktické znalosti			V této oblasti není učivo zadané jak v RVP, tak v ŠVP vybrané školy.	Dokáží vytvořit dostatečně bezpečné heslo.		Respondenti získali vybrané znalosti i když vyučující se okruhu nevěnuje.
Autorský zákon	Teoretické znalosti	Ochrana autorského práva.	Ochrana autorského práva.	RVP a ŠVP se shodují.	Duševní vlastnictví. Porušení autorského zákona.	Jaké jsou postihy při porušení. Nepřivlastňovat si cizí díla.	Znalosti respondentů jsou odpovídající a shodují se s výpovědí vyučujícího.
	Licenční rozdělení software			V této oblasti není učivo zadané jak v RVP, tak v ŠVP vybrané školy.		Základní rozdělení. Freeware, shareware...	Respondenti nezískali vybrané znalosti i když vyučující se okruhu věnuje.

Příloha 6

Základní škola Dukelská							
Vymezená oblast výuky		Rámcový vzdělávací program	Školní vzdělávací program	Hodnocení ŠVP s ohledem na RVP	Respondenti	Vyučující	Hodnocení znalostí respondenta s ohledem na vyučujícího
Zálohování dat	Praktické dovednosti	Chrání data před poškozením, ztrátou a zneužitím.		ŠVP vybrané školy neobsahují učivo, které je obsaženo v RVP.		Jak lze chránit dat, minimalizovat ztrátu. Základní způsoby zálohy.	Respondenti nezískali vybrané znaslosti i když vyučující se okruhu věnuje.
	Teoretické znalosti			V této oblasti není učivo zadané jak v RVP, tak v ŠVP vybrané školy.	Možnosti zálohování. Co, kam a jak.	Kompilace dat. Možnosti zálohy.	Znalosti respondentů jsou odpovídající a shodují se s výpovědí vyučujícího.
Softwarové bezpečnostní prvky	Hrozby a rizika			V této oblasti není učivo zadané jak v RVP, tak v ŠVP vybrané školy.	1/2 nezná. Zbytek ví o červech, virech.	Seznámení se základními pojmy. U vyšších ročníků.	Znalosti respondentů jsou odpovídající a shodují se s výpovědí vyučujícího.
	Antivirové programy			V této oblasti není učivo zadané jak v RVP, tak v ŠVP vybrané školy.	Znalost existence antivirového programu bez praktické znalosti.	Kontrola email přílohy. Nenavštěvovat pochybné stránky. Antivir.	Znalosti respondentů jsou odpovídající a shodují se s výpovědí vyučujícího.
	Firewall			V této oblasti není učivo zadané jak v RVP, tak v ŠVP vybrané školy.		Seznámení se základním vybením počítače. Firewall a jeho funkce.	Respondenti nezískali vybrané znaslosti i když vyučující se okruhu věnuje.
	Ostatní			V této oblasti není učivo zadané jak v RVP, tak v ŠVP vybrané školy.			Respondenti nebyli seznámeni a vyučující se nevěnuje problematice.
Bezpečnost na internetu	Praktické dovednosti		Bezpečnost na internetu. Uvědomuje si nebezpečí spojená s internetem.	ŠVP vybrané školy obsahují toto učivo, které není obsaženo v RVP.	1/2 si je vědoma o nástrahách a čemu se vyvarovat.	Né přímo. Seznam se bezpečně od seznamu.	Znalosti respondentů jsou odpovídající a shodují se s výpovědí vyučujícího.
Správa hesel	Teoretické dovednosti		Bezpečné heslo.	ŠVP vybrané školy obsahují toto učivo, které není obsaženo v RVP.	Znalost základním pravidel pro tvorbu bez. hesla.	Základní principy a pravidla pro vytvoření bez. hesla.	Znalosti respondentů jsou odpovídající a shodují se s výpovědí vyučujícího.
	Praktické znalosti			V této oblasti není učivo zadané jak v RVP, tak v ŠVP vybrané školy.	Dovedou vytvořit bez. heslo.	Prakticky náročné.	Znalosti respondentů jsou odpovídající a shodují se s výpovědí vyučujícího.
Autorský zákon	Teoretické znalosti	Ochrana práv k duševnímu vlastnictví, copyright, informační etika.	Práce s informacemi v souladu se zákonem o duševním vlastnictví.	RVP a ŠVP se shodují.	Ve spojitosti s citováním a duševním vlastnictvím při práci s obrázky a textem.	V souvislosti s prací v textem. Citace a uvádění autora přebraného textu.	Znalosti respondentů jsou odpovídající a shodují se s výpovědí vyučujícího.
	Licenční rozdělení software	Respektování práv k duševnímu vlastnictví při využívání SW.	Druhy programů z hlediska licencí.	RVP a ŠVP se shodují.		Povědomě, freeware, shareware, komerční. Co očekávat.	Respondenti nezískali vybrané znaslosti i když vyučující se okruhu věnuje.

Příloha 7

Základní škola Kubatova							
Vymezená oblast výuky		Rámcový vzdělávací program	Školní vzdělávací program	Hodnocení ŠVP s ohledem na RVP	Respondenti	Vyučující	Hodnocení znalostí respondenta s ohledem na vyučujícího
Zálohování dat	Praktické dovednosti	Chrání data před poškozením, ztrátou a zneužitím.	Bezpečně ukládá a šíří.	RVP a ŠVP se shodují.			Respondenti nezískali vybrané znaslosti a vyučující se okruhu nevěnuje.
	Teoretické znalosti		Teorie ochrany dat.	ŠVP vybrané školy obsahují toto učivo, které není obsaženo v RVP.			Respondenti nezískali vybrané znaslosti a vyučující se okruhu nevěnuje.
Softwarové bezpečnostní prvky	Hrozby a rizika			V této oblasti není učivo zadané jak v RVP, tak v ŠVP vybrané školy.	Viry, spam, nebezpečné stránky.	Vir, spam, hrozby na internetových stránkách (čemu se vyhnout).	Znalosti respondentů jsou odpovídající a shodují se s výpovědí vyučujícího.
	Antivirové programy			V této oblasti není učivo zadané jak v RVP, tak v ŠVP vybrané školy.	1/2 nezná a prakticky nemá žádné znalosti.	Praktická ukázka, reinstal antiv. programu. Účel antiviru.	Znalosti respondentů jsou odpovídající a shodují se s výpovědí vyučujícího.
	Firewall			V této oblasti není učivo zadané jak v RVP, tak v ŠVP vybrané školy.	1/2 se setkala s firewallem a zná význam tohoto prvku.	Existence firewallu. Názorná ukázka.	Znalosti respondentů jsou odpovídající a shodují se s výpovědí vyučujícího.
	Ostatní			V této oblasti není učivo zadané jak v RVP, tak v ŠVP vybrané školy.			
Bezpečnost na internetu	Praktické dovednosti		Rizika komunikace na internetu a problematika bezpečnosti. Kriminalita na internetu.	ŠVP vybrané školy obsahují toto učivo, které není obsaženo v RVP.	Bohaté znalosti ochrany identity. Bezpečnosti, možností ochrany.	Chování na sociálních sítích. Možnosti nastavení. Dostupnost informací. Zneužití.	Znalosti respondentů jsou odpovídající a shodují se s výpovědí vyučujícího.
Správa hesel	Teoretické dovednosti			V této oblasti není učivo zadané jak v RVP, tak v ŠVP vybrané školy.	Základní pravidla pro tvorbu bez. hesla.	Jak se ukládají hesla, jak je smazat.	Znalosti respondentů jsou odpovídající a shodují se s výpovědí vyučujícího.
	Praktické znalosti			V této oblasti není učivo zadané jak v RVP, tak v ŠVP vybrané školy.	Dokáže vytvořit bezpečnostní heslo.	Kombinační možnosti hesla. Pravidla pro tvorbu bez. hesla.	Znalosti respondentů jsou odpovídající a shodují se s výpovědí vyučujícího.
Autorský zákon	Teoretické znalosti	Ochrana práv k duševnímu vlastnictví, copyright, informační etika.	Pojmy a pravidly obsažený v zákonech o duševním vlastnictví. Vlastnická práva.	RVP a ŠVP se shodují.			Respondenti nezískali vybrané znaslosti a vyučující se okruhu nevěnuje.
	Licenční rozdělení software	Respektování práv k duševnímu vlastnictví při využívání SW.		ŠVP vybrané školy neobsahují učivo, které je obsaženo v RVP.	Základní znalosti rozdělení, freeware, shareware...	Základní rozdělení. Freeware, shareware, komerční.	Znalosti respondentů jsou odpovídající a shodují se s výpovědí vyučujícího.

Příloha 8

Základní škola Rudolfov							
Vymezená oblast výuky		Rámcový vzdělávací program	Školní vzdělávací program	Hodnocení ŠVP s ohledem na RVP	Respondenti	Vyučující	Hodnocení znalostí respondenta s ohledem na vyučujícího
Zálohování dat	Praktické dovednosti	Chrání data před poškozením, ztrátou a zneužitím.	Chrání data před poškozením, ztrátou a zneužitím.	RVP a ŠVP se shodují.			Respondenti nezískali vybrané znalosti a vyučující se okruhu nevěnuje.
	Teoretické znalosti			V této oblasti není učivo zadané jak v RVP, tak v ŠVP vybrané školy.	Zálohování na přenosná média, alespoň dvakrát důležitá data.	Co zálohovat a jakým způsobem.	Znalosti respondentů jsou odpovídající a shodují se s výpovědí vyučujícího.
Softwarové bezpečnostní prvky	Hrozby a rizika			V této oblasti není učivo zadané jak v RVP, tak v ŠVP vybrané školy.		Pouze věnování pozornosti přílohám u mailu.	Respondenti nezískali vybrané znaslosti a vyučující se okruhu věnuje.
	Antivirové programy			V této oblasti není učivo zadané jak v RVP, tak v ŠVP vybrané školy.		Jaké jsou freeware programy na internetu.	Respondenti nezískali vybrané znalosti a vyučující se okruhu věnuje.
	Firewall			V této oblasti není učivo zadané jak v RVP, tak v ŠVP vybrané školy.			Respondenti nezískali vybrané znalosti a vyučující se okruhu nevěnuje.
	Ostatní			V této oblasti není učivo zadané jak v RVP, tak v ŠVP vybrané školy.			Respondenti nezískali vybrané znaslosti a vyučující se okruhu nevěnuje.
Bezpečnost na internetu	Praktické dovednosti			V této oblasti není učivo zadané jak v RVP, tak v ŠVP vybrané školy.	Nesdílet osobní inromace. Anonymita. Komunikace. Možnosti profilu a rizika.	Kyberšikana, profily, sdílení osobních informací. Soukromí, fotky. Anonymita	Znalosti respondentů jsou odpovídající a shodují se s výpovědí vyučujícího.
Správa hesel	Teoretické dovednosti			V této oblasti není učivo zadané jak v RVP, tak v ŠVP vybrané školy.	Náležitosti silného hesla.	Základní pravidla a náležitosti bez. hesla.	Znalosti respondentů jsou odpovídající a shodují se s výpovědí vyučujícího.
	Praktické znalosti			V této oblasti není učivo zadané jak v RVP, tak v ŠVP vybrané školy.	Dokáže vytvořit dostatečně bezpečné heslo.	V rámci výuky, vlastní heslo na přístup k školnímu serveru.	Znalosti respondentů jsou odpovídající a shodují se s výpovědí vyučujícího.
Autorský zákon	Teoretické znalosti	Ochrana práv k duševnímu vlastnictví, copyright, informační etika.	Pojmy a pravidly obsažený v zákonech o duševním vlastnictví. Vlastnická práva.	RVP a ŠVP se shodují.	Odkazy na autora textu nebo obrázku.	V rámci práci s textem a obrázky, odkaz na autora. Duševní vlastnictví.	Znalosti respondentů jsou odpovídající a shodují se s výpovědí vyučujícího.
	Licenční rozdělení software	Respektování práv k duševnímu vlastnictví při využívání SW.	Respektuje práva k duševnímu vlastnictví při využívání software.	RVP a ŠVP se shodují.	Freeware, shareware, placené programy. Jak je možno je používat.		Respondenti znají vybranou oblast i když se jí vyučující nevěnoje.

Příloha 9

Základní škola, Matice školské 3							
Vymezená oblast výuky		Rámcový vzdělávací program	Školní vzdělávací program	Hodnocení ŠVP s ohledem na RVP	Respondenti	Vyučující	Hodnocení znalostí respondenta s ohledem na vyučujícího
Zálohování dat	Praktické dovednosti	Chrání data před poškozením, ztrátou a zneužitím.	Bezpečně ukládá a šíří.	RVP a ŠVP se shodují.			Respondenti nezískali vybrané znalosti a vyučující se okruhu nevěnuje.
	Teoretické znalosti			ŠVP vybrané školy obsahují toto učivo, které není obsaženo v RVP.	Možnosti zálohování. Co, kam a jak.	Možnosti zálohy. Jak zálohovat a proč.	Znalosti respondentů jsou odpovídající a shodují se s výpovědí vyučujícího.
Softwarové bezpečnostní prvky	Hrozby a rizika			V této oblasti není učivo zadané jak v RVP, tak v ŠVP vybrané školy.	Viry, spam, hoax.	Kde mohou narazit na viry, jak se vyvarovat spamu. A ostatní rizika.	Znalosti respondentů jsou odpovídající a shodují se s výpovědí vyučujícího.
	Antivirové programy			V této oblasti není učivo zadané jak v RVP, tak v ŠVP vybrané školy.	Znalost existence antivirového programu bez praktické znalosti.	Důležitost antivirového programu. Význam a možnosti.	Znalosti respondentů jsou odpovídající. Nicméně se neshodují v rozsahu.
	Firewall			V této oblasti není učivo zadané jak v RVP, tak v ŠVP vybrané školy.		Jako okrajové téma. Existuje Windows firewall.	Respondenti nezískali vybrané znalosti, i když vyučující se okruhu věnuje.
	Ostatní			V této oblasti není učivo zadané jak v RVP, tak v ŠVP vybrané školy.			Respondenti nezískali vybrané znalosti a vyučující se okruhu nevěnuje.
Bezpečnost na internetu	Praktické dovednosti		Bezpečnost na internetu.	ŠVP vybrané školy obsahují toto učivo, které není obsaženo v RVP.	Anonymita. Množství sdílených dat. Soukromí, kyberšikana.	Hlavně sociální sítě. Na co si dávat pozor a jak spravovat svůj profil.	Znalosti respondentů jsou odpovídající a shodují se s výpovědí vyučujícího.
Správa hesel	Teoretické dovednosti			V této oblasti není učivo zadané jak v RVP, tak v ŠVP vybrané školy.	Základní pravidla pro tvorbu bez. hesla.	Jako okrajové téma. Délka hesla, různorodost znaků.	Znalosti respondentů jsou odpovídající a shodují se s výpovědí vyučujícího.
	Praktické znalosti			V této oblasti není učivo zadané jak v RVP, tak v ŠVP vybrané školy.	Dokáží vytvořit dostatečně bezpečné heslo.		Znalosti respondentů jsou odpovídající a shodují se s výpovědí vyučujícího.
Autorský zákon	Teoretické znalosti	Ochrana práv k duševnímu vlastnictví, copyright, informační etika.	Práce s informacemi v souladu se zákonem o duševním vlastnictví.	RVP a ŠVP se shodují.	V rámci práce s textem a obrázky. Citace. Duševní vlastnictví.	Prakticky při výuce kancelářského balíčku (word, excel). Citace obrázků a textů.	Znalosti respondentů jsou odpovídající a shodují se s výpovědí vyučujícího.
	Licenční rozdělení software	Respektování práv k duševnímu vlastnictví při využívání SW.	Druhy programů z hlediska licencí.	RVP a ŠVP se shodují.	Jaké jsou programy z hlediska licence v rozmezí - freeware, shareware, placené.	Základní rozdělení. Co očekávat od software. Délka použití a za jakých podmínek.	Znalosti respondentů jsou odpovídající a shodují se s výpovědí vyučujícího.

Příloha 10

Základní škola Lišov							
Vymezená oblast výuky		Rámcový vzdělávací program	Školní vzdělávací program	Hodnocení ŠVP s ohledem na RVP	Respondenti	Vyučující	Hodnocení znalostí respondenta s ohledem na vyučujícího
Zálohování dat	Praktické dovednosti	Chrání data před poškozením, ztrátou a zneužitím.	Chrání data před poškozením, ztrátou a zneužitím.	RVP a ŠVP se shodují.	Práce s přenosnými médii.	U vyšších ročníků. Pracujeme ve výuce s Flash disky atd.	Znalosti respondentů jsou odpovídající a shodují se s výpovědí vyučujícího.
	Teoretické znalosti			V této oblasti není učivo zadané jak v RVP, tak v ŠVP vybrané školy.	Důležitost zálohování. Pravidelnost a možnosti zálohování dat.	Uvědomění si důležitost zálohování dat, co zálohovat a kam.	Znalosti respondentů jsou odpovídající a shodují se s výpovědí vyučujícího.
Softwarové bezpečnostní prvky	Hrozby a rizika			V této oblasti není učivo zadané jak v RVP, tak v ŠVP vybrané školy.	Viry, spam.	Jaké webové stránky nenavštěvovat. Spam a email.	Znalosti respondentů jsou odpovídající a shodují se s výpovědí vyučujícího.
	Antivirové programy			V této oblasti není učivo zadané jak v RVP, tak v ŠVP vybrané školy.		Pouze ukázka virového programu na školním počítači.	Respondenti nezískali vybrané znalosti i když vyučující se okruhu věnuje.
	Firewall			V této oblasti není učivo zadané jak v RVP, tak v ŠVP vybrané školy.			Respondenti nezískali vybrané znalosti a vyučující se okruhu nevěnuje.
	Ostatní			V této oblasti není učivo zadané jak v RVP, tak v ŠVP vybrané školy.			Respondenti nezískali vybrané znaslosti a vyučující se okruhu nevěnuje.
Bezpečnost na internetu	Praktické dovednosti			V této oblasti není učivo zadané jak v RVP, tak v ŠVP vybrané školy.	Bohaté znalosti ochrany identity. Bezpečnosti, možností ochrany.	Vše je veřejné a dohledatelné. Profily, rizika spojená s užitím soc. sítí.	Znalosti respondentů jsou odpovídající a shodují se s výpovědí vyučujícího.
Správa hesel	Teoretické dovednosti			V této oblasti není učivo zadané jak v RVP, tak v ŠVP vybrané školy.			Respondenti nezískali vybrané znalosti a vyučující se okruhu nevěnuje.
	Praktické znalosti			V této oblasti není učivo zadané jak v RVP, tak v ŠVP vybrané školy.			Respondenti nezískali vybrané znalosti a vyučující se okruhu nevěnuje.
Autorský zákon	Teoretické znalosti	Ochrana práv k duševnímu vlastnictví, copyright, informační etika.	Duševním vlastnictví. Vlastnická práva.	RVP a ŠVP se shodují.	Duševní vlastnictví.	Duševní vlastnictví. Následky za porušení	Znalosti respondentů jsou odpovídající a shodují se s výpovědí vyučujícího.
	Licenční rozdělení software	Respektování práv k duševnímu vlastnictví při využívání SW.	Respektuje práva k duševnímu vlastnictví při využívání software.	RVP a ŠVP se shodují.	Základní znalosti rozdělení, freeware, shareware, placené.	Základní rozdělení. Freeware, shareware, komerční.	Znalosti respondentů jsou odpovídající a shodují se s výpovědí vyučujícího.

Příloha 11

Gymnázium Jírovcova							
Vymezená oblast výuky		Rámcový vzdělávací program	Školní vzdělávací program	Hodnocení ŠVP s ohledem na RVP	Respondenti	Vyučující	Hodnocení znalostí respondenta s ohledem na vyučujícího
Zálohování dat	Praktické dovednosti	Organizuje účelně data a chrání je proti poškození či zneužití.		ŠVP vybrané školy neobsahují učivo, které je obsaženo v RVP.	Vytvoření bodu obnovy, paměťová média.	Možnosti zálohování.	Znalosti respondentů se shodují s výpovědí vyučujícího.
	Teoretické znalosti			V této oblasti není učivo zadané jak v RVP, tak v ŠVP vybrané školy.	Jak a proč zálohovat. Jak často.	Důležitost zálohování. Jaké jsou možnosti na ochranu dat před ztrátou.	Znalosti respondentů se shodují s výpovědí vyučujícího.
Softwarové bezpečnostní prvky	Hrozby a rizika			V této oblasti není učivo zadané jak v RVP, tak v ŠVP vybrané školy.	Spam - emaily. Viry, škodlivé kódy, kde na ně lze narazit.	Viry, hoax, škodlivé kódy, spam.	Znalosti respondentů se shodují s výpovědí vyučujícího.
	Antivirové programy	Antivirová ochrana		ŠVP vybrané školy neobsahují učivo, které je obsaženo v RVP.	Aktualizace antivirového programu.	Instalace antivirového programu. Diskuze na toto téma. Jaký a proč.	Znalosti respondentů nedosahují takové hloubky a rozsahu jak tvrdí vyučující.
	Firewall	Firewall		ŠVP vybrané školy neobsahují učivo, které je obsaženo v RVP.		Windows firewall - účel. Další možnosti firewall.	Respondenti nezískali vybrané znalosti i když vyučující se okruhu věnuje.
	Ostatní			V této oblasti není učivo zadané jak v RVP, tak v ŠVP vybrané školy.			Respondenti nezískali vybrané znalosti a vyučující se nevěnuje problematice.
Bezpečnost na internetu	Praktické dovednosti	Ochrana osobních údajů.		ŠVP vybrané školy neobsahují učivo, které je obsaženo v RVP.	Míra sdílených informací. Ochrana osobních údajů.	Diskuze na téma sociálních sítí. Upozornění na anonymitu.	Znalosti respondentů se shodují s výpovědí vyučujícího.
Správa hesel	Teoretické dovednosti			V této oblasti není učivo zadané jak v RVP, tak v ŠVP vybrané školy.		Základní pravidla tvorby bezpečného hesla.	Respondenti nezískali vybrané znalosti i když vyučující se okruhu věnuje.
	Praktické znalosti			V této oblasti není učivo zadané jak v RVP, tak v ŠVP vybrané školy.			Respondenti nezískali vybrané znalosti a vyučující se nevěnuje problematice.
Autorský zákon	Teoretické znalosti	Ochrana autorských práv.	Autorské práva a zákony, upozorňuje na problémy spojené s jejich porušením.	RVP a ŠVP se shodují.	Postihy za porušení. Znají duševní vlastnictví.	V rámci autorského zákona. Legalita a následky za porušení.	Znalosti respondentů se shodují s výpovědí vyučujícího.
	Licenční rozdělení software		Rozlišuje pojmy shareware, freeware, trial, copyright, multilicence, public domain.	ŠVP vybrané školy obsahují toto učivo, které není obsaženo v RVP.	Freeware, shareware, komerční SW.	Teoreticky formou výkladu. Od komerčních po freeware.	Znalosti respondentů se shodují s výpovědí vyučujícího.

Příloha 12

Gymnázia J. V. Jirsíka							
Vymezená oblast výuky		Rámcový vzdělávací program	Školní vzdělávací program	Hodnocení ŠVP s ohledem na RVP	Respondenti	Vyučující	Hodnocení znalostí respondenta s ohledem na vyučujícího
Zálohování dat	Praktické dovednosti	Organizuje účelně data a chrání je proti poškození či zneužití.	Organizuje účelně data a chrání je proti poškození či zneužití.	RVP a ŠVP se shodují.			Respondenti nezískali vybrané znalosti a vyučující se nevěnuje problematice.
	Teoretické znalosti			ŠVP vybrané školy neobsahují učivo, které je obsaženo v RVP.			Respondenti nezískali vybrané znalosti a vyučující se nevěnuje problematice.
Softwarové bezpečnostní prvky	Hrozby a rizika			ŠVP vybrané školy neobsahují učivo, které je obsaženo v RVP.	Pouze viry a jak ohrožují počítač.	Možné hrozby na internetu. Viry, spam, pochybné webové stránky.	Znalosti respondentů nedosahují takové hloubky a rozsahu jak tvrdí vyučující.
	Antivirové programy	Antivirová ochrana		ŠVP vybrané školy neobsahují učivo, které je obsaženo v RVP.		Důležitost antivirového programu. Kde ho vzít.	Znalosti respondentů nedosahují takové hloubky a rozsahu jak tvrdí vyučující.
	Firewall	Firewall		ŠVP vybrané školy neobsahují učivo, které je obsaženo v RVP.		Existence firewall. Co vlastně dělá.	Respondenti nezískali vybrané znaslosti i když vyučující se okruhu věnuje.
	Ostatní			V této oblasti není učivo zadané jak v RVP, tak v ŠVP vybrané školy.			Respondenti nezískali vybrané znalosti a vyučující se nevěnuje problematice.
Bezpečnost na internetu	Praktické dovednosti	Ochrana osobních údajů.		ŠVP vybrané školy neobsahují učivo, které je obsaženo v RVP.	Množství sdílených údajů. Možné následky.	Anonymita. Sdílené údaje. Čemu se vyvarovat u komunikace.	Znalosti respondentů se shodují s výpovědí vyučujícího.
Správa hesel	Teoretické dovednosti			V této oblasti není učivo zadané jak v RVP, tak v ŠVP vybrané školy.	Základní pravidla tvorby bezpečného hesla.	Základní pravidla tvorby bezpečného hesla.	Znalosti respondentů se shodují s výpovědí vyučujícího.
	Praktické znalosti			V této oblasti není učivo zadané jak v RVP, tak v ŠVP vybrané školy.			Respondenti nezískali vybrané znalosti a vyučující se nevěnuje problematice.
Autorský zákon	Teoretické znalosti	Ochrana autorských práv.	Respektování právních zásad při používání prostředků ICT.	RVP a ŠVP se shodují.	Duševní vlastnictví. Co mohu a nemohu kopírovat.	Duševní vlastnictví. Jak pracovat s převzatým materiálem.	Znalosti respondentů se shodují s výpovědí vyučujícího.
	Licenční rozdělení software			ŠVP vybrané školy neobsahují učivo, které je obsaženo v RVP.		Základní rozdělení. Freeware, shareware, trial. Jaké jsou podmínky použití.	Respondenti nezískali vybrané znalosti i když vyučující se okruhu věnuje.

Příloha 13

Gymnázium Česká a Olympijských nadějí							
Vymezená oblast výuky		Rámcový vzdělávací program	Školní vzdělávací program	Hodnocení ŠVP s ohledem na RVP	Respondenti	Vyučující	Hodnocení znalostí respondenta s ohledem na vyučujícího
Zálohování dat	Praktické dovednosti	Organizuje účelně data a chrání je proti poškození či zneužití.	Organizuje účelně data a chrání je proti poškození či zneužití.	RVP a ŠVP se shodují.			Respondenti nezískali vybrané znalosti a vyučující se nevěnuje problematice.
	Teoretické znalosti	Zálohování dat.		ŠVP vybrané školy neobsahují učivo, které je obsaženo v RVP.		Možnosti zálohování. Cloud	Respondenti nezískali vybrané znalosti i když vyučující se okruhu věnuje.
Softwarové bezpečnostní prvky	Hrozby a rizika			V této oblasti není učivo zadané jak v RVP, tak v ŠVP vybrané školy.		Nestahovat všechny přílohy. Viry, spam, hoax.	Respondenti nezískali vybrané znalosti i když vyučující se okruhu věnuje.
	Antivirové programy	Antivirová ochrana.	Používá vhodné antivirové programy.	RVP a ŠVP se shodují.		Teoreticky. K čemu slouží. A jaký zvolit a proč.	Respondenti nezískali vybrané znalosti i když vyučující se okruhu věnuje.
	Firewall	Firewall.		ŠVP vybrané školy neobsahují učivo, které je obsaženo v RVP.		Existence firewall.	Respondenti nezískali vybrané znaslosti i když vyučující se okruhu věnuje.
	Ostatní			V této oblasti není učivo zadané jak v RVP, tak v ŠVP vybrané školy.			Respondenti nezískali vybrané znalosti a vyučující se nevěnuje problematice.
Bezpečnost na internetu	Praktické dovednosti	Ochrana osobních údajů.		ŠVP vybrané školy neobsahují učivo, které je obsaženo v RVP.	Množství sdílených dat. Profily. Proč nastavovat soukromí.	Seznam se bezpečně. Rizika soukromích/veřejných profilů. Následky.	Znalosti respondentů se shodují s výpovědí vyučujícího.
Správa hesel	Teoretické dovednosti			V této oblasti není učivo zadané jak v RVP, tak v ŠVP vybrané školy.		Základní pravidla. Náležitosti silného hesla.	Respondenti nezískali vybrané znalosti i když vyučující se okruhu věnuje.
	Praktické znalosti			V této oblasti není učivo zadané jak v RVP, tak v ŠVP vybrané školy.			Respondenti nezískali vybrané znalosti a vyučující se nevěnuje problematice.
Autorský zákon	Teoretické znalosti	Respektování duševního vlastnictví, copyright, správné citování.	Ochrana autorského zákona.	RVP a ŠVP se shodují.	Co můžeme kopírovat/stahovat. Duševní vlastnictví.	Duševní vlastnictví. Copyright. Citování. Stahování.	Znalosti respondentů se shodují s výpovědí vyučujícího.
	Licenční rozdělení software			V této oblasti není učivo zadané jak v RVP, tak v ŠVP vybrané školy.		Základní dělení SW.	Respondenti nezískali vybrané znalosti i když vyučující se okruhu věnuje.

Příloha 14

1) *Přišli jste ve výuce Informatiky do styku s pojmem "bezpečnost"?*

- ☐ Ano
- ☐ Ne

2) *Znáte z výuky Informatiky hrozby, kterým lze čelit na interntových stránkách? (jak správně chránit svůj počítač)*

- ☐ Znám

  Jaké: .....

  .....

- ☐ Neznám

a. *Znáte z výuky Informatiky nějaké antivirové programy? Zkoušeli jste instalovat nebo alespoň provést aktualizaci antivirového programu? Doporučil vám vyučující nějaký antivirový program ?*

- ☐ Znám, zkoušel jsem instalovat i aktualizovat
- ☐ Znám, ale pouze teoreticky
- ☐ Neznám

  Antivirový program: .....

a. *Byl jste při výuce Informatiky seznámen s bezpečnostním prvkem zvaným firewall? Zkoušeli jste nějaká nastavení?*

- ☐ Ano, znám
- ☐ Ano, pouze teoreticky

  Co to je a jaké nastavení jste zkoušeli: .....

  .....

  .....

- ☐ Neznám

3) *Říkali jste si ve výuce Informatiky o nástrahách, které vyplývají z virtuálního společenství? (diskuzní fóra, soukromé profily, sociální sítě a počítačové hry)*

- ☐ Znám

  Jaké: .....

  .....

- ☐ Neznám

4) *Probírali jste ve výuce Informatiky zálohování dat ? Zálohujete data ?Jakým způsobem?*

☐ Znám a zálohuji

☐ Znám, ale pouze teoreticky

Jak: .....

.....

☐ Neznám

5) *Máte představu o pojmu copyright – autorské právo? Probírali jste ve výuce Informatiky?*

.....

.....

☐ Neznám

6) *Jaké znáte z výuky Informatiky rozdělení software? Vysvětlete.*

☐ Znám

Jaké: .....

.....

☐ Neznám

7) *Jaké znáte z výuky Informatiky pravidla vytváření a používání bezpečných hesel (tj. pravidelná změna hesla, odpovídající délka hesla a používání směsice znaků a čísel).*

☐ Ano, znám

Pravidla: .....

.....

Silné heslo: .....

.....

Proč: .....

.....

☐ Neznám

8) *Učili jste se ve výuce Informatiky něco více v oblati bezpečnosti, než o čem jsme se momentálně bavili ?*

.....

.....

☐ Ne

Příloha 15

1) *Vyučujete Digitální bezpečnost ve výuce Informatiky?*

☐ Ano

Do jaké hloubky: .....

.....

☐ Ne

2) *Seznamujete studenty s hrozbami, kterým lze čelit na interntových stránkách ve výuce Informatiky?*

☐ Vyučuji.

Jak: .....

.....

☐ Nevyučuji.

a. *Vyučujete ve výuce Informatiky praktické postupy jak se chránit hrozbám přicházejcím z Internetu. Jakým způsobem ?*

☐ Vyučuji.

Jak: .....

.....

☐ Nevyučuji.

b. *S jakými bezpečnostními prvky studenty seznamujete ?*

☐ Ano, vyučuji.

☐ Ano, pouze teoreticky.

Jaké a jak: .....

.....

.....

☐ Nevyučuji.

3) *Upozorňujete studenty na rizika vyplývající z virtuálního společenství (diskuzní fóra, soukromé profily a optimální množství zveřejněných informací).*

☐ Upozorňuji.

Jakým způsobem: .....

.....

☐ Nevyučuji.

4) *Jaké oblasti zálohování dat (archivace kopií) se studenty řešíte a do jaké hloubky?*

☐ Vyučuji.

☐ Vyučuji, ale pouze teoreticky.

Jak a jakým způsobem: .....

.....

☐ Nevyučuji.

5) *Do jaké hloubky vyučujete problematiku autorského práva?*

.....

.....

.....

6) *V jakém rozsahu vyučujete studenty určité rozdíly mezi software licencí?*

☐ Vyučuji

Jak: .....

.....

☐ Nevyučuji.

7) *Učíte studenty vytvořit bezpečné heslo?*

☐ Ano, vyučuji.

☐ Ano, vyučuji pouze teoreticky.

Jak: .....

.....

☐ Nevyučuji.

8) *Myslíte, že hodinová dotace Informatiky je dostatečná? Kolik myslíte, že by byl ideální prostor pro digitální bezpečnost ve výuce Informatiky?*

☐ Ano

☐ Ne

Proč: .....

.....

9) *Učíte ve výuce Informatiky něco víc v oblasti bezpečnosti, než o čem jsme se momentálně bavili ?*

.....