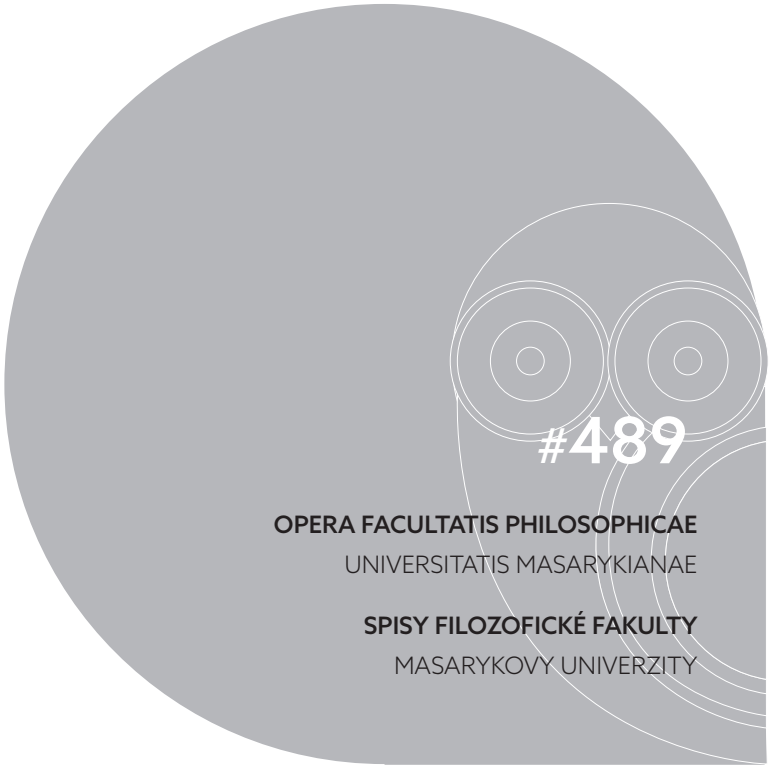
Kovářová, Pavla

Informační bezpečnost žáků základních škol : lekce v knihovnách

Informační bezpečnost žáků základních škol : lekce v knihovnách Vydání první
Brno: Filozofická fakulta, Masarykova univerzita, 2019

ISBN 978-80-210-9270-9; ISBN 978-80-210-9271-6 (online : pdf)
ISSN 1211-3034 (print); ISSN 2787-9291 (online)

Stable URL (DOI): https://doi.org/10.5817/CZ.MUNI.M210-9271-2019
Stable URL (handle): https://hdl.handle.net/11222.digilib/141112
Access Date: 27. 11. 2024
Version: 20220902



#489

OPERA FACULTATIS PHILOSOPHICAE
UNIVERSITATIS MASARYKIANAE

SPISY FILOZOFICKÉ FAKULTY
MASARYKOVY UNIVERZITY

MUNI
PRESS

Informační bezpečnost žáků základních škol

Lekce v knihovnách

Pavla Kovářová

FILOZOFICKÁ FAKULTA
MASARYKOVA UNIVERZITA

#489

BRNO 2019

KATALOGIZACE V KNIZE – NÁRODNÍ KNIHOVNA ČR

Kovářová, Pavla
Informační bezpečnost žáků základních škol : lekce v knihovnách / Pavla Kovářová. – Vydání první. – Brno : Filozofická fakulta, Masarykova univerzita, 2019. – 261 stran. – (Opera Facultatis philosophicae Universitatis Masarykianae = Spisy Filozofické fakulty Masarykovy univerzity, ISSN 1211-3034 ; 489)
Anglické resumé
ISBN 978-80-210-9270-9

004.056 * 37.03:[007+004] * 316.346.32-053.5 * 026/027 * 021.1/.4 * 303.442.2 * (437.3) * (048.8)
- informační bezpečnost – Česko
- informační výchova – Česko
- děti školního věku – Česko
- knihovny – Česko
- funkce knihoven – Česko
- akční výzkum – Česko
- monografie

37 - Výchova a vzdělávání [22]

Recenzovali: PhDr. Hana Landová, Ph.D. (Univerzita Karlova)
prof. PhDr. Helena Grecmanová, Ph.D. (Univerzita Palackého v Olomouci)
doc. Mgr. Jiří Zounek, Ph.D. (Masarykova univerzita)

ISBN 978-80-210-9270-9
ISBN 978-80-210-9271-6 (online : pdf)
ISSN 1211-3034
https://doi.org/10.5817/CZ.MUNI.M210-9271-2019

Obsah

PŘEDMLUVA

O současné společnosti se stále více hovoří jako o společnosti informační. Informace a informační technologie proměňují řadu dříve obvyklých a přijímaných přístupů a pravidel v oblasti formy a obsahu vzdělávání, ale také v zajištění informační bezpečnosti. Mění se také role knihoven, jejichž základním posláním je zpřístupňování informací uživatelům, kdy tyto informace jsou stále častěji zprostředkovány právě informačními technologiemi. Téma informační bezpečnosti se silně dotýká všech uživatelů internetu a informačních technologií, mezi nimi jsou však vyzdvihovány možné dopady a rizika pro děti. Ty prochází povinným vzděláváním, které je má připravit na profesní i soukromý život. Cílem této publikace je nabídnout daty podloženou analýzu a současně návrh pro vzdělávání žáků základních škol v informační bezpečnosti. Primárně monografie směřuje do knihoven, ale její výsledky lze jistě uplatnit i v dalších institucích, jak institucích neformálního vzdělávání, tak ve školách.

Pro dosažení tohoto cíle je monografie rozdělena do tří základních částí. První část přináší teoretické představení problematiky informační bezpečnosti. Zaměřuje se na rizika, hrozby a možná bezpečností opatření, která by měl lektor znát nejen pro realizaci dále řešených lekcí. První část tedy může být přínosná nejen pro lektory, ale i odbornou a širokou veřejnost pro získání přehledu o problematice informační bezpečnosti, bezpečnostních opatřeních, která by měl využívat běžný uživatel informačních technologií, i o důvodech jejich využití.

Druhá část publikace se již soustředí na samotnou koncepci vzdělávání žáků základních škol v informační bezpečnosti v knihovnách. Jsou představena východiska, která může knihovna využít pro argumentaci vůči zřizovateli a uživatelům ke zdůvodnění aplikace dané koncepce. Následně jsou popsány jednotlivé lekce do té míry podrobnosti, aby je knihovník mohl využít přímo, případně po přízpů-

sobení specifikům cílové skupiny. Akcentováno je proto nejen to, co bylo nastaveno, ale také proč a co je nutné zachovat pro dosažení stanovených cílů lekce. Tato část publikace je tedy již určena zejména lektorům v knihovnách, případně jiných vzdělávacích institucích, ale také managementu těchto organizací pro zdůvodnění realizace této služby (v anglickém prostředí označováno jako *information literacy advocacy*[1]).

Forma i důvody nastavení lekcí nevycházejí jen z odborné literatury, ale výrazně je ovlivnily také výsledky výzkumů, které byly využity jak pro orientaci v prostředí knihoven a jejich potenciálu lekce realizovat, tak pro ověření koncepce pomocí akčního výzkumu. Přestože v knihovnictví i dalších oblastech se diskutuje potřeba služeb založených na datech (*evidence-based librarianship*), knihovny poskytují své služby převážně na základě vlastního přesvědčení[2]. Tato část publikace tedy slouží jako empirický doklad reálnosti a efektivity navržené koncepce. Sekundárně může být využitelná pro knihovníky jako inspirace pro provádění vlastních výzkumů i jako ukázka jejich přínosu. V tomto ohledu jsou opět primární cílovou skupinou publikace lektoři informačního vzdělávání v knihovnách, ale sekundárně i ostatní zaměstnanci knihoven nebo lektoři neformálního vzdělávání.

Tato publikace navazuje na dizertační práci autorky[3]. S ohledem na výše představený cíl je ale větší část práce přepracována. Některé pasáže jsou rozpracovány podrobněji pro využitelnost v praxi, jiné jsou naopak zkráceny s ohledem na aktuálnost nebo volnější vztah k jádru knihy.

1 KATZ 2007.

2 KOVÁŘOVÁ 2016.

3 KOVÁŘOVÁ 2015.

ÚVOD

Téma informační bezpečnosti je diskutováno veřejností jako jeden ze základních problémů při využívání internetu[4]. Efektivní a bezpečná práce uživatelů s informacemi je řazena do kompetencí nezbytných pro digitální občanství[5]. Roste proto společenská poptávka po vzdělávání v této problematice. Oblast soukromí, která je silně propojena s digitálními stopami, byla zařazena do oblasti zájmu knihoven spolu s dalšími tématy informační bezpečnosti již v roce 2005, jak dokládá obsah dokumentu IFLA s titulem *Libraries, National Security, Freedom of Information News and Social Responsibilities*[6]. Problematika autorských práv a hodnocení informací představuje oblast, které se knihovny věnují dlouhodobě (např. již akvizicí jednotek do fondu). Knihovny tak právem patří mezi instituce, které naplňují předpoklady k zajištění vzdělávání uživatelů v informační bezpečnosti.

Problematika informační bezpečnosti je ve zde řešeném pojetí omezena na možnosti zvýšení bezpečnosti uživatelů, zejména dětských, pomocí vzdělávání v knihovnách. Téma je již nyní pokryté knihovnami v rámci informačního vzdělávání (viz kap. 2.1.4), které představuje tradiční službu knihoven. Informační vzdělávání je sice úzce spjato s didaktikou, ale nezabývá se jen formou vzdělávání, nýbrž i obsahem (práce uživatele s informacemi). Naopak aplikace výzkumu do informačního vzdělávání je významná pro hodnocení jeho efektivity[7], a to jak na úrovni jednotlivých aktivit, tak i v oblasti přístupů a řešených témat. Ta se

4 TAMBAUM 2010.

5 GALLAGHER 2011.

6 SEIDELIN a HAMILTON 2005.

7 Význam tohoto spojení ukazuje současný rozvoj tzv. „evidence-based teaching" (někdy také learning, education apod., terminologie zatím není ustálená). Přínosy přístupu pro jednotlivé vzdělávací aktivity prezentuje např. KOVÁŘOVÁ 2014.

v současné společnosti s informačními technologiemi rychle mění a je nutné se těmto změnám přizpůsobovat, aby informační vzdělávání bylo přínosné pro vzdělávané[8].

Aby koncepce vzdělávání odpovídala současným podmínkám a potřebám, bylo nutné zohlednit chování dětí, současnou podobu vzdělávání v knihovnách a vzdělávání v informační bezpečnosti. Průnik všech tří oblastí je v současnosti v odborné literatuře a výzkumech pokryt nedostatečně. Tato publikace usiluje o představení těchto témat a aplikovaného výzkumu pro posílení řešení informační bezpečnosti dětí v českém prostředí. Lekce jsou po úpravách využitelné i pro další cílové skupiny, informační bezpečnost není omezena jen na děti. To již ale není předmětem této publikace, byť může sloužit jako inspirace pro lektora v přípravě lekcí informační bezpečnosti i pro další uživatele.

Hlavním cílem publikace je představení daty podložené koncepce pro vzdělávání v informační bezpečnosti, která by byla uplatnitelná v současných podmínkách knihoven. Děti jsou kvůli svým omezeným životním zkušenostem, pozitivnímu vztahu k technologiím a dalším charakteristikám spojeným s vývojovou psychologií[9] náchylnější k zranitelnosti na internetu. Zahájení vzdělávání je vhodnější v době, kdy se lépe budují postoje v chování, následně získávané znalosti se ve spojení s nimi lépe rozšiřují. Knihovny v současnosti nabízejí své lekce do škol, čímž mají zajištěnu návštěvnost, školy zase vzdělávání v oblasti, která pokrývá mimo jiné i informační gramotnost[10]. Je tak umožněno plošné oslovení plošné oslovení a následně vzdělání velké části cílové skupiny – žáků základních škol, které je výrazně reálnější než oslovování osob v produktivním věku pro lekce, se kterými knihovny stále mají problém[11].

8 Změnám v informační gramotnosti vlivem IT se věnuje např. KOVÁŘOVÁ 2013.

9 Viz kap. 1.2.1, podrobněji viz KOVÁŘOVÁ 2011.

10 Vymezení pojmů informační gramotnost a vzdělávání a jejich vztahu se věnuje kap. 2.1.1.

11 ŠTEFEK 2012.

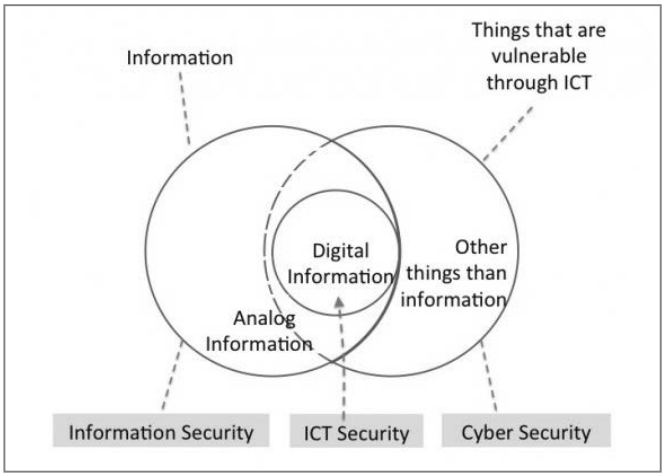
1 INFORMAČNÍ BEZPEČNOST A DIGITÁLNÍ STOPY

Označení *informační bezpečnost*, podobně jako digitální stopy (kap. 1.2), se objevuje v laickém vyjadřování spíše v intuitivním pojetí. I v odborných publikacích nepanuje shoda na obsahu termínu, k čemuž v českém prostředí přispívá jazykové omezení pro přenos ze zahraničních poznatků. Z historického pohledu se pojem vázal na technické zabezpečení informačních systémů, čímž problematika jednoznačně spadala do oblasti zájmů počítačové vědy (informatiky). Se zvyšujícím se počtem uživatelů v elektronickém prostředí, rozmachem internetu a následně Webu 2.0 se výrazně zvyšoval vliv člověka jako prvku informačního systém[12], a tak docházelo k postupnému vývoji od *information security* (ve smyslu technického zabezpečení) k *information safety* (bezpečí v informačním prostředí na úrovni sociální). Právě na druhou oblast je kladen důraz v této publikaci. Nicméně obě oblasti není možné zcela oddělovat, protože se úzce doplňují a prolínají. Kromě základního vymezení lze i v oblasti technického zabezpečení najít při konkrétnější terminologii doklad, že problematika informačního zabezpečení má jasnější vztah k informační než počítačové vědě, jelikož není omezena na spojení s IT, jak dokládá Obrázek 1 Informační bezpečnost ve vztahu k IT.

Informační bezpečnost je možné chápat jako ochranu před ohrožením způsobeným informacemi a s nimi spojenými technologiemi (pro účely publikace je pojem informační bezpečnost používán ve smyslu bezpečí s vědomím souvisejících prvků zabezpečení, obecně zahrnuje oba tyto významy). S rozvojem využití IT ve všech oblastech života se zvyšuje význam právě oblasti digitálních informací, a to od velmi malých dětí (Chang[13] uvádí vystavení dětí internetu od dvou let) po seniory.

12 POŽÁR 2005, s. 54–55.

13 CHANG 2010, s. 501.



Obrázek 1 Informační bezpečnost ve vztahu k IT[14]

Bezpečnostní problémy mohou vznikat v rámci různých fází práce s informacemi. V souladu se standardem mediální a informační gramotnosti[15] je možné klasifikovat tyto fáze jako získání, evaluace a tvorba. Již získávání informací je regulováno zákonnými a etickými pravidly, především v kontextu dodržování autorských práv, ale třeba i v rámci komunikace (např. využití manipulativních technik). Po získání informací by mělo následovat jejich posouzení, jehož výsledek je často klíčový pro odpovědné chování při práci s informacemi. Evaluace je proto významnou složkou jak práce se získanými informacemi, tak jejich tvorby. Ve chvíli, kdy jsou vytvořené informace zaznamenány, je lze označovat jako digitální stopy. Právě ty tvoří základ, příp. faktor zvyšující úspěšnost většiny informačních útoků, které jsou dnes diskutovány nejen ve směru k dětem na základních školách. Dítě by mělo vědět, jak se může bránit z pozice možné oběti, ale i jak se nestát útočníkem. S ohledem na standard mediální a informační gramotnosti a na analýzu RVP (viz kap. 2.1.2) byly proto pro koncepci definovány dva základní tematické ohruhy v rámci informační bezpečnosti: získávání a hodnocení informací a digitální stopy a bezpečná komunikace.

1.1 Získávání a hodnocení informací a jejich zdrojů

Pro tvorbu informací i představy o světě, učení, profesní i osobní život je vždy nutné vycházet z předchozích informací a v případě pocitu jejich nedostatku získat

14 IRGENS 2013.

15 Global Media and Information Literacy (...) 2013.

takové, které aktuální poznání vhodně obohatí. Pro získávání informací je možné využít různých typů informačních zdrojů, mezi kterými vzhledem k rychlosti, ceně, rozsahu a dalším výhodám dominuje internet. Získávání informací nejen z internetu je ale ovlivněno tím, že dostupný je i nelegální nebo pro děti nevhodný obsah. V případě, že dítě tento obsah získá a využije, porušuje etická a někdy i zákonná pravidla.

Aby rozšíření současných znalostí bylo efektivní, je nutné vycházet z vhodných informací, které nejsou zkreslené, ale důvěryhodné. Různé typy informačních zdrojů mají různý účel, kterým může být nejen zjednodušení faktů s ohledem na přiblížení určitého tématu širší veřejnosti, ale i cílená manipulace. Důležité je proto být si vědom kredibility získaných informací, ale i jejich zdrojů nebo poskytovatelů, a tomu přizpůsobit nakládání s nimi.

1.1.1 Získávání informací

Z hlediska informační gramotnosti a bezpečnosti by informace měly být získávány v souladu s pravidly etiky a zákona. V případě, že jsou tato pravidla porušena, jedná se o nevhodný nebo nelegální obsah, jehož získáním dítě může poškozovat někoho jiného (především ve vztahu k autorským právům), nebo samo může být negativně ovlivněno a za určitých okolností je narušen jeho psychický vývoj (např. pornografie, agresivní obsah, extremismus, sekty apod.). I když pro ochranu dětí je možné využít technické nástroje (různé typy filtrů obsahu, bezpečné vyhledávání na Google apod.), s ohledem na jejich limity (viz kap. 1.3.2) jejich bezpečnost ovlivňuje především chování. Pokud děti usilují o získání konkrétního obsahu, jsou vždy schopny najít způsob, jak toho dosáhnout (např. na počítači kamaráda).

Nelegální stahování cizích autorských děl je časté, podle finského výzkumu[16] 71 % dospívajících (15–16 let) ve vzorku během posledního roku nelegálně stáhlo soubor, přičemž 14 % dospívajících to dělá denně. Čím intenzivnější byla tato nelegální aktivita, tím silněji ji dospívající vnímali jako přijatelné chování. Celkově ale 60 % dospívajících vnímalo stahování hudby nebo filmů jako do určité míry nemorální. Dle staršího amerického výzkumu[17] 91 % dětí (8–18 let) si uvědomovalo autorská práva, ale přesto stahovaly soubory, více než polovina hudbu a třetina hry, o něco méně dětí pak komerční software a filmy. Nejčastěji uváděné důvody pro nelegální stahování softwaru byly ty, že nemají peníze na zaplacení (51 %), nepoužívaly by ho, kdyby za něj museli platit (35 %), a že to dělá hodně lidí (33 %). Oproti tomu třetina dětí si nebyla jistá, zda je v pořádku nahrát software na internet bez placení, a třetina si byla jistá, že je to v pořádku.

16 AALTONEN 2013.

17 Majority of Youth Understand (...) 2004.

Z hlediska autorského zákona je proto nutné věnovat se jak aspektu získávání, tak i dalšího sdílení, které (pokud se nejedná o dílo s to umožňující licencí nebo o vlastní autorské dílo) je nelegální (viz kap. 1.3.1). Při sdílení nestačí jen vymezit úpravu v autorském zákoně, ale především praktickou aplikaci např. pro uvědomění si, že i při stahování může uživatel současně ještě nestažený soubor sdílet (peer-to-peer sítě, včetně torrentů). Řada děl využívá technologickou ochranu autorských práv (především tvrdé nebo sociální DRM), která může bránit využití staženého souboru. K porušení autorského zákona pak může dojít i tím, že je tato ochrana odstraněna, např. pomocí speciálního softwaru pro kopírování nosičů, využitím nezakoupeného sériového čísla nebo smazáním jména legálního vlastníka e-knihy (sociální DRM). Woolley[18] doporučuje soustředit se na hlubší uvědomování si etického aspektu digitálního pirátství, protože děti sledují spíše osobní zisk, který z toho mají. Současně hrozba potrestání jim připadá vzdálená. V rámci osvěty je proto vhodné poukázat na případové studie, ideálně co nejbližší dětem (tj. situované do České republiky, s nezletilým pachatelem).

Zatímco v případě porušování autorských práv dochází jen k budování nevhodných návyků, v případě jiného typu závadného obsahu může dojít k problematičtějšímu ovlivnění psychického vývoje dítěte. Přesto, že tento obsah může mít negativní vliv na vývoj dítěte, samy děti o něj mají zájem. Vaníčková[19] například uvádí, že si pornografii opakovaně prohlíží 93 % patnáctiletých chlapců a přibližně 60 % dívek. Dle EU Kids online[20] 21 % dětí v posledních 12 měsících vidělo některý z potenciálně poškozujících obsahů (12 % nenávistné zprávy, 10 % omezování příjmu potravy, 7 % fyzické poškozování sebe sama, 7 % zkušenosti s drogami a 5 % spáchání sebevraždy), přičemž Česká republika byla na 1. místě mezi státy z hlediska počtu dětí, které některý ze sledovaných typů obsahu viděly. Pornografie, agresivní obsah, extremismus nebo třeba sekty mohou při dlouhodobém působení vést k tomu, že dítě začne dané jednání považovat za normální. To jej může dovést k nevhodnému chování v reálném prostředí (např. pornografie k prostituci). Dítě si ale také formuje obraz sebe sama, například dospívající může být ovlivněn modelem ideálního vzhledu (což opět může vést k problémům v tradičním prostředí, např. poruchám příjmu potravy).

Jedním z možných řešení je zákaz vyhledávání problematického obsahu dětmi. Toto řešení má ale řadu problémů (náhodný přístup, přístup u kamaráda, nemožnost řešit problém s rodičem kvůli porušení jeho zákazu apod.). Jak ukazuje kap. 1.3, děti by měly vědět, jak na nevhodný a nelegální obsah reagovat, pokud by se s ním setkaly, a aby věděly, že samy nemají zájem o přístup k němu. Základem je proto komunikace s dítětem. Důležité je přitom upozornit, že tento obsah může

18 WOOLLEY 2015.

19 VANÍČKOVÁ 2005, s. 28–29.

20 LIVINGSTONE 2011, s. 98–99.

nabývat různých forem, např. prezentace extremistických názorů může mít formát nejen webové stránky organizace, ale i hudební produkce nebo počítačových her, jejichž primárním cílem je právě přivést děti k přijetí těchto názorů ztotožněním se s daným obsahem.

1.1.2 Hodnocení informací

Při hodnocení informací je nutné přemýšlet nejen nad nimi samotnými, ale i nad jejich zdroji a nad subjekty, které vstupují do procesu distribuce od autora k příjemci. Pro hodnocení není podstatná jen kredibilita informací, ale především to, jak dané sdělení vnímá konkrétní člověk. Při tomto subjektivním hodnocení probíhá cyklus, který Harris[21] nazval zkratkou CAFE (Challenge, Adapt, File, Evaluate). Prvním krokem je výzva k autorovi informace (kdo to je, proč mu věřit apod.), následuje adaptace (skeptické přijetí s ohledem na předchozí znalosti), uložení (zapamatování si se zvažováním dále přijímaných informací) a vyhodnocení (zvážení přínosu informace pro vlastní osobu). V rámci všech kroků dochází ke komparaci poznatků z více zdrojů a zvážení, která informace bude akceptována v případě protichůdných zjištění. Pro vymezení jednotlivých kroků jsou popsány postupy hodnocení informací od těch nejobecněji využitelných až po subjektivní zhodnocení konkrétního argumentu.

Řada informačních zdrojů je spojena se zprostředkovatelem informací. Do této pozice se dostává například knihovna, která ovlivňuje to, jaké informace budou dostupné ve fondu. Při výběru (akvizice) může dojít k tomu, že část informací k tématu bude z různých důvodů chybět. Podobně je tomu například s redakční radou, příp. šéfredaktorem nebo vlastníkem u periodik, kdy opět může být ze zprostředkování odstraněna určitá informace. Důvody vyřazení informace mohou být různé – finanční, politické nebo osobní přesvědčení. Například zprostředkovatel se může obávat, že by zpráva vedla k růstu xenofobie, proto se rozhodne neinformovat o agresi člena minority. Z toho je patrné, že nejde jen o úmyslně manipulativní jednání, výběr informací může být ovlivněn i dobrou vůlí. Zprostředkovatelem může být také internetový vyhledávač, např. Google z finančních důvodů upřednostňoval některé výsledky vyhledávání[22]. Proto je vhodné při hodnocení informací přemýšlet nad tím, kdo je zprostředkovatelem informací a zda mohou existovat důvody ovlivňující způsob prezentace určité informace.

21 HARRIS 2015.

22 Antitrust: Commission probes allegations (...) 2010.

Dalším krokem je hodnocení informačního zdroje, např. článku, videa, ale třeba i diskuzního fóra. Metzger a Flanagin[23] řadí mezi nejčastěji využívané heuristiky:

- reputace (autorita autora, ale i informačního zdroje),
- potvrzení (doporučení známými nebo množstvím neznámých lidí),
- konzistence (potvrzení v jiných, nezávislých zdrojích),
- sebepotvrzení (soulad s předchozími informacemi),
- narušení očekávání (věrohodnost snižují jazykové, typografické a další chyby, pokud zdroj nepůsobí profesionálně, totéž ale platí i naopak – profesionální vzhled nekvalitního zdroje zvyšuje důvěru u příjemce informace),
- přesvědčivost úmyslu (negativní vliv má reklama, komerčnost zdroje apod., pokud tyto prvky nejsou zřejmé, příjemce má opět větší tendenci informaci věřit).

Jako pomůcka pro hodnocení informací bylo formulováno nesčetné množství různých klasifikací kritérií[24]. Mezi často zmiňované, které lze použít na libovolný informační zdroj, patří CRAP test[25] a CARS test[26], které si jsou obsahově podobné, jen dílčí hodnocené prvky jsou utříděné do jiných kategorií:

Currency	Datum publikování, aktualizace, zastarávání tématu	Credibility	Odbornost autora, kontrola kvality (např. recenzní řízení), formální kvalita, emocionální zkreslení
Reliability	Kompletnost a kvalita informací (obsahová i formální)	Accuracy	Aktuálnost, komplexnost, cílová skupina a účel, více úhlů pohledu
Authority	Identifikovatelnost autora, jeho odbornost, vydavatel, sponzor	Reasonableness	Férovost argumentace, konzistence, objektivita, přiměřenost fungování světa
Purpose	Důvod tvorby autorem, žánr (fakta, názor), stereotypy	Support	Dokumentace zdrojů, podepření dalšími zdroji, externí konzistence

Obecné testy je sice možné využít na libovolný zdroj (včetně komunikace, např. v diskuzních fórech[27]), neupozorňují ale na specifika důležitá pro hodnocení konkrétních typů zdrojů. V tom mohou pomoci specializované hodnotící testy, např. SMELL test pro masmédia (viz s. 266).

Po zhodnocení informačního zdroje následuje evaluace konkrétních informací, tedy posouzení argumentace a možné manipulace. Kvalitní argumentace je předpokladem pro přesvědčení příjemce informací o oprávněnosti sdělení. I bez

23 METZGER 2013.

24 CHOI 2015.

25 MCKENZIE 2013.

26 HARRIS 2015.

27 Viz SAVOLAINEN 2011.

ní může informaci přijmout, pokud odpovídá jeho smýšlení, navazuje na to, co již ví, nebo mu ji předkládá někdo, komu důvěřuje (viz heuristiky výše), může se ale jednat o zkreslené pojetí. Pro podložené obhájení věrohodnosti informací je správná argumentace klíčová.

Argumentaci je možné definovat jako „*verbální činnost, která se uskutečňuje prostřednictvím jazyka, a sociální aktivita, která je zpravidla zaměřená na ostatní lidi, a racionální činnost, která je obvykle založena na intelektuálních úvahách*."[28] Argumentace tedy vyjadřuje osobní stanovisko autora určené jiným lidem, proto by ho měl podložit důkazy. Typickým příkladem, kdy se objevují dvě protichůdné argumentace s cílem někoho přesvědčit, je soudní spor – obě strany předkládají podložená tvrzení ke stejné situaci. A rozhodnutí záleží na přesvědčivosti těchto tvrzení.

Pro hodnocení kvality argumentu je možné využít Toulminův model argumentace. Ten definuje několik prvků dobré argumentace[29]:

- Názor, tvrzení: vyjádření závěru, který následně budeme obhajovat;
- Data: fakta podporující tvrzení;
- Záruky: logické spojení mezi daty a tvrzením;
- Podklady: zdroje opravňující záruky;
- Kvalifikátory: určení síly tvrzení (pravděpodobně, téměř...);
- Vyvrácení: vyvrácené argumenty nebo výjimky.

Při hodnocení kvality argumentu tedy příjemce sleduje, jak se pracuje se zdroji dat k tvrzení, jestli z informací závěr logicky vyplývá a zda se správně pracuje s kvalifikátory (např. neoprávněné zevšeobecnění). Naopak varovnými signály by měly být tzv. argumentační fauly, mezi které patří důraz na rozum („každý rozumný člověk ví..."), na emoce, chybná práce s příčinou nebo důsledkem, obsahové chyby, útoky na osoby[30].

Setkat se lze ale i s vyloženě manipulativními přístupy. Ty jsou podobné argumentačním faulům, jde ale o cílené využití jejich podstaty. Může jít také o nesrozumitelnost (např. aby text působil odborně, byť je fakticky chybný), účelový výběr (informací, zdrojů..., včetně toho, že je např. uvedena informace s účelově vybraným původcem, ke kterému má příjemce informací negativní vztah), účelové řazení (např. zařazení nežádoucí zprávy mezi nezajímavé) nebo využití obrazové manipulace. Právě práce s obrazem může být přesvědčivá, zejména u fotografií a videozáznamů stále převažuje tendence důvěry (text je možné manipulovat snáz) a současně jsou lákavější než strohý text. Zkreslení obrazových informací nemusí být náročné, jak ukazuje např. manipulace s fotkou oslav 2. výročí komunistické revoluce, ze které byly postupně odstraňovány politicky nevhodné osoby, až v roce

28 EEMEREN 2004.

29 TOULMIN 2003.

30 Řadu příkladů argumentačních faulů je možné najít v infografice MCCANDLESS 2012.

1967 zůstal na fotce jen Lenin[31]. Ještě snazší je manipulace pomocí grafů, které jsou často přijímány podle prvního dojmu, i když to je zkreslující (např. nezobrazená celá osa, velikost neodpovídající měřítku, 3D zešikmení zvětšující bližší výseky)[32].

Kvalitní hodnocení informací zahrnuje zvážení všech výše uvedených kroků. Při výuce by praktické vyzkoušení mělo být spojeno s informacemi, jejich zdroji a zprostředkovateli, které daná cílová skupina využívá. Pro všechny věkové a profesní skupiny je vhodné upozornit na to, jak hodnotit informaci při vyhledávání na Google[33] nebo jak nakládat s mediálními zprávami, v případě vysokoškolských studentů má smysl věnovat se kritériím hodnocení v odborných databázích nebo hodnocení kvality vědeckých článků. Správná volba praktické situace je klíčová pro efektivitu vzdělávání (viz konstruktivistická výuka v kap. 3.1).

1.2 Digitální stopy jako riziková tvorba informací

Digitální stopy definoval Fish jako: „*záznam vašich interakcí s digitálním světem a jak data, která jsou zanechána za nimi, mohou být využita.*“[34] Tato definice akcentuje pozici člověka jako subjektu vytvářejícího aktivně digitální stopy s možností tuto aktivitu korigovat (byť jen do určité míry). Při zvážení definic z jiných oborů (kriminalistika, marketing, počítačová věda) lze konstatovat, že digitální stopy jsou informace v digitální podobě s vypovídací hodnotou o konkrétní osobě, primárně fyzické, ale i právnické a s reálným potenciálem využití třetí stranou a se zpětným vlivem na osobu, o které vypovídají. Vypovídací hodnota může být zprostředkována elektronickou reprezentací (např. nelze jej identifikovat ve smyslu osobních údajů) nebo spojením digitálních stop z více zdrojů. Reálný potenciál využití vylučuje údaje o uživateli, které jsou v současnosti využitelné jen hypoteticky nebo velmi omezeně. Využití je možné jen při zahrnutí všech tří činností spojených s digitálními stopami, tj. uložení, analýza a vytvoření hodnoty[35]. Zpětná vazba k dané osobě vylučuje anonymizované datové soubory (personifikace, ne personalizace), důraz je kladen na udržení spojení digitální stopy a konkrétní osoby, resp. persony (digitální reprezentace konkrétní osoby).

Pew Research Center[36] dělí digitální stopy na aktivní („*Osobní informace zpřístupněné online záměrným odesláním nebo sdílením informace uživatelem.*“[37]) a pasivní

31 MACDONALD 2007, s. 17.

32 Příklady chyb v grafech, které mohou být využity i jako manipulace viz MAREK 2015.

33 TAYLOR 2014.

34 FISH, Tony. Definition of a digital footprint (again). In: EKE 2012.

35 FISH 2009, s. 21.

36 MADDEN 2007.

37 MADDEN 2007, s. 4.

(„*Osobní informace zpřístupněné online bez jakékoli záměrné intervence od jedince.*“[38]). Aktivní stopy mohou mít různou podobu. Na jedné straně se jedná o informace, které o sobě člověk sám uvádí, např. blogy, informace v registračním formuláři, fotografie, e-maily apod. Proti tomu pasivní vytváří technická zařízení při jejich používání, např. soubory Cookies, záznamy IP adres a činností na navštívených webových serverech, souřadnice GPS (např. pro sledování pomocí mobilního zařízení s GPS přijímačem), videozáznamy z kamer atd. Z hlediska definice je možné mezi pasivní digitální stopy zařadit také informace, které o člověku zpřístupnil online někdo jiný, typově jde ale spíše o údaje blízké aktivním digitálním stopám. Vzhledem k této nejasnosti publikace nebude s pojmy aktivní a pasivní digitální stopa příliš operovat. Toto dělení ale pomáhá vymezit zaměření publikace, která se soustředí na aktivní digitální stopy, jenž ovlivňuje především sám uživatel, příp. digitální stopy, které o uživateli vytvořil někdo jiný.

Jiné dělení, podstatné pro tuto práci, je podle zneužitelnosti informací obsažených v digitálních stopách. Jedno z nich uvádí Král:

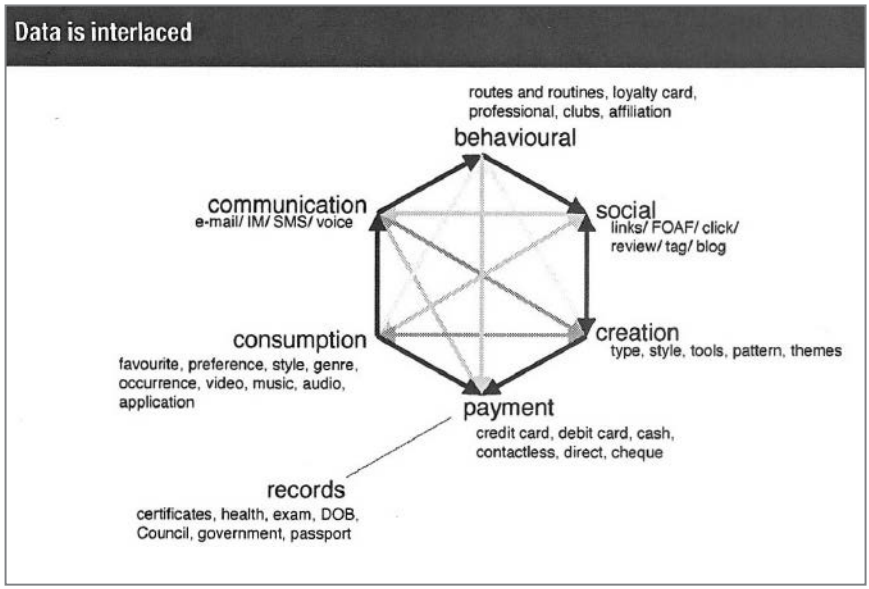
> *„Červená – rodné číslo, číslo pojištění, identifikační čísla (PIN) účtů, rodné jméno matky, informace o zdravotním stavu, trestní rejstřík, podrobné informace o financích, cestovní plány, seznam předchozích zaměstnání, informace o rodině a přátelích vč. jejich telefonních čísel, e-mailových i skutečných adres, atp.*
> *Oranžová (žlutá) – telefonní číslo, adresa, datum narození, stav, zaměstnavatel, vzdělání, e-mailová adresa, oblíbené nákupy, číslo kreditní karty, zájmy a koníčky, spolky a sdružení, navštívené WWW stránky, apod.*
> *Zelená – směrovací číslo, věk, přibližná výše platu, povolání, průzkumy veřejného mínění, atd., pokud tyto informace nejsou ve spojení s jinými, choulostivějšími údaji z předchozích skupin.*“[39]

Problémem tohoto členění je silné zaměření na fyzickou osobu, přestože informace stejného typu a stejných možností využití mohou být spojeny s personou (např. heslo k elektronické službě). Na příkladu e-mailové adresy, která se nachází v prvních dvou kategoriích, je zřejmé, že informace může být zneužitelná na různých úrovních v závislosti na okolnostech. Spojování nevýznamných a významnějších informací vede k vyšší míře užití digitální stopy (viz Obrázek 2). Toto spojení digitálních stop může vést k identifikaci jedince i po anonymizaci datových souborů (odstranění tradičních identifikátorů jako jméno, datum narození apod.)[40].

38 MADDEN 2007, s. 3.

39 KRÁL 2006, s. 100.

40 OHM 2009.



Obrázek 2 Typologie digitálních stop se zdůrazněním spojení[41]

Uvedená kategorizace slouží spíše jako vodítko, vždy záleží na uvážení hodnoty pro konkrétní osobu a situaci, např. při žádosti o zaměstnání je nutné uvažovat jinak než při zakládání profilu v online hře. Především pro děti by měly být za problematické považovány informace o denní rutině a rozvrhu[42]. Podstatné je neopomenout, že se může jednat i o metadata (např. místo pořízení fotky) nebo odvozenou hodnotu (např. lokalizace počítače pomocí IP adresy).

Přestože digitální stopy mohou mít jak jak korektní využití (např. nabídka reklamy odpovídající zájmům), tak i takové, které je pro uživatele nepříjmené, pro tuto práci je podstatnější právě druhá uvedená možnost. Lze konstatovat, že se jedná o zásah do soukromí, jelikož hodnotou informace je její spojení s konkrétní osobou. Pojem soukromí je možné vymezit jako nárok jednotlivců, skupin či institucí sám určit, kdy, jak a v jakém rozsahu jsou informace o nich šířeny dál[43]. Problémem ovšem zůstává, jak dopředu posoudit, zda bude zásah nežádoucí. V uvedené definici by i žádoucí zásah byl narušením soukromí, ale nebyl by pravděpodobně vnímán jako bezpečnostní incident. Dále v publikaci narušení soukromí označuje nežádoucí užití digitálních stop bez ohledu na právní dopad.

41 FISH 2009, s. 79.

42 GRAYSON 2011, s. 24.

43 Volně dle WESTIN 1967.

1.2.1 Vznik a získání digitální stopy

Vznik aktivních digitálních stop závisí většinou na vlastním rozhodnutí člověka, proto by si měl být vědom důsledků, ke kterým jejich zpřístupnění může vést. Digitální stopy člověk zpřístupňuje dvěma základními způsoby:

a) Zveřejněním je informace uložena tak, že je dostupná každému, kdo má odpovídající autorizaci (v případě veřejné informace není nutná) a je možné ji vyhledat a získat. Tyto postupy jsou často legální, pokud nedojde k narušení informačního systému, např. prolomením hesla (viz kap. 1.3.2).
b) V přímé komunikaci může být zpřístupněná informace obsažena v obsahu sdělení (např. text e-mailu) nebo v metadatech[44] (např. kontaktní údaje dalších adresátů v hlavičce odeslaného e-mailu).

S rozvojem Webu 2.0 se výrazně zvýšila možnost uživatele publikovat libovolné informace. Může se jednat o komentáře v diskuzních fórech, fotoalba, vlastní videonahrávky, deníčky (blogy) a další digitální stopy. Tyto informace je pak možné vyhledat, pokud je ponechána často přednastavená možnost veřejného přístupu nebo nedůsledně hlídána autorizace (např. povolení přístupu mobilní aplikace k facebookovému profilu uživatele). Význam autorizace a autentizace si lidé často neuvědomují. Podle Technet.cz[45] přijalo 60 % českých dospívajících mužů a 42 % žen (15–20 let) na sociální síti žádost o přátelství od neznámého člověka druhého pohlaví. Americký průzkum[46] ukázal, že za poukaz na kávu za tři dolary sdělilo své heslo 66 % dotázaných a dalších 19 % jeho formát. V kap. 1.2.3 jsou rozvedeny podrobnosti ke zveřejňování osobních a citlivých informací dětmi, včetně např. fotografie se sexuálním podtextem (pro získání pozitivního ohlasu na vzhled či vyjádření zájmu o vztah, který je pro dospívajícího podstatný pro budování statusu ve vrstevnické komunitě a sebevědomí[47]).

Sociální sítě mohou být snadným zdrojem informací pro internetový útok, protože umožňují získat mnoho údajů na jednom místě. Jedná se také o častý způsob komunikace dítěte (viz Tabulka 1), přes který je snadno dosažitelné a který je pro něj důležitý, je proto problém se v případě útoku (např. kyberšikany) od něj odpoutat. Přitom mnoho profilů obsahuje identifikující informace, 20 % dotazovaných z České republiky má jako součást profilu adresu nebo telefonní číslo a v průměru 2,7 ze šesti sledovaných typů informací[48]. Podle jiného výzkumu[49] byli

44 Přestože tyto typy údajů jsou jen omezeně chráněny zákonem (viz kap. 1.3.1), jejich hodnota může být vysoká, jak zdůrazňuje FISH 2009, s. 19, 44, 177.

45 KASÍK 2009.

46 LEYDEN 2005.

47 Tyto a související psychologické charakteristiky dospívání vedoucí k zveřejňování problematických informací podrobněji popisuje např. ŠIMÍČKOVÁ – ČÍŽKOVÁ 2003.

48 LIVINGSTONE 2011.

49 WALRAVE 2012.

dospívající (10–19 let) ochotni zveřejnit 13 z 18 sledovaných osobních informací a ve srovnání s dospělými statisticky méně často využívali nastavení soukromí. Oolo a Siibak[50] se zaměřili na děti ve věku 14–16 let, které již více využívají postupy pro ochranu soukromí, k čemuž aplikují různorodé strategie od omezování uváděných informací po jejich skrývání mezi jinými informacemi (tzv. sociální steganografie). Zmínit lze také například to, že třetina dospívajících sdílí své internetové heslo s přáteli a čtvrtina neví, že obsah nahraný na internet nemůže být permanentně smazán[51]. Téměř čtvrtina studentů si není vědoma toho, jak snadno může neznámý dospělý získat na sociálních sítích přístup k jejich osobním informacím nebo s nimi zahájit chat[52].

Tabulka 1 Profil dětí na sociálních sítích dle EU Kids Online[53]

	9–10 let	11–12 let
Profil na sociální síti	26 %	46 %
Zcela veřejný profil	28 %	26 %
Částečně veřejný profil	19 %	24 %
Neví o vlastním nastavení profilu	9 %	4 %

Při zohledňování výsledků mezinárodních výzkumů je nutné postupovat uvážlivě, protože byly prokázány rozdíly mezi státy. Pro tuto publikaci jsou podstatné výsledky z ČR[54], která patří ke státům, kde má nejvíce dětí zkušenost s jedním nebo více rizikovými faktory. Na druhou stranu je u nich zjištěn jeden z nejvyšších průměrů v množství online dovedností.

Podle výzkumu Kopeckého[55] sdílí nebo na žádost internetového známého zašle významné množství českých dětí (8–17 let) své osobní informace (v Grafu 1 jsou uvedeny jen informace s výskytem větším než 5 %). Vzhledem k tomu, že tento výzkum je opakován každoročně od roku 2010, po mírném snižování sdílených a zasílaných osobních informací je možné od roku 2013 sledovat zvýšení tohoto rizikového jednání.

50 OOLO 2013.

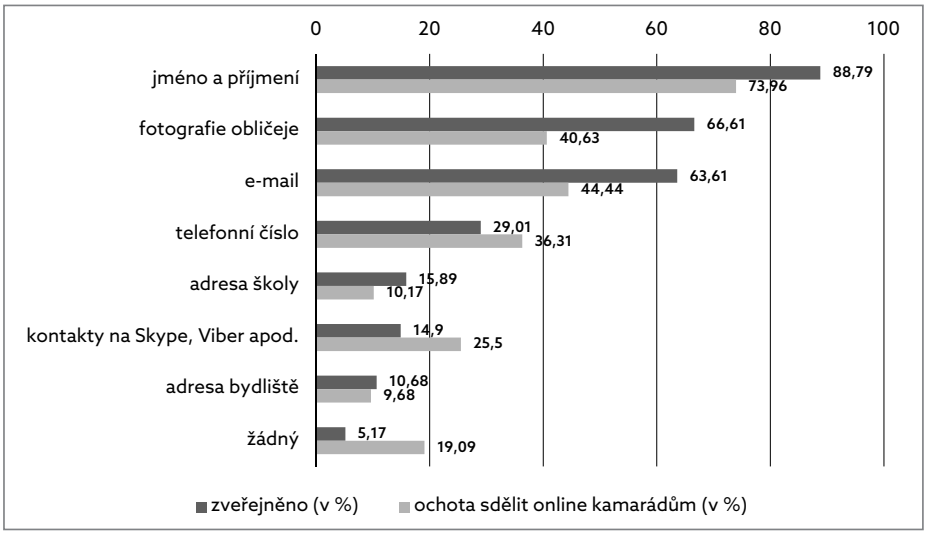
51 JOINER 2005.

52 WEEDEN 2013.

53 LIVINGSTONE 2011; Sběr dat pro tento klíčový výzkum probíhal v letech 2009–2011. Navazující výzkum (LIVINGSTONE 2012) se sběrem dat z roku 2014 byl realizován jen v sedmi státech, kdy nebyla pokryta Česká republika. Vzhledem k dříve zjištěným rozdílům mezi státy a nastavení koncepce vzdělávání na východiska v ČR jsou relevantní spíše starší výsledky, které ČR pokrývají.

54 LIVINGSTONE 2011.

55 KOPECKÝ 2017.



Graf 1 Zpřístupňování osobních informací na internetu dětmi[56]

Hledání zveřejněných digitálních stop je totožné jako u jiných informací. Mnoho lze získat přímo při hledání v nejčastěji využívaných službách, jako je Facebook, příp. přes vyhledávače, které indexují i veřejné informace na sociálních sítích. Problém se může objevit při velkém množství výsledků, ze kterých je těžké získat žádoucí informace, příp. v určení, zda patří ke sledované osobě a ne např. jmenovci. Pro toto ověření se využívá shody informací v různých zdrojích, vzhledu (fotografie apod.), přezdívky, e-mailové adresy a dalších kontaktních údajů. Možnost pro získání smazaných informací, tj. i digitálních stop, představují webové archivy, např. WayBackMachine. Při vyhledání je možné použít různých nástrojů, které mají primárně sloužit jako bezpečnostní opatřední (viz egosurfing v kap. 1.3.3). Pro tento účel lze využít i speciální vyhledávače, tzv. People search engines[57], které se uplatňují především v USA, v českém prostředí nelze využít všech funkcí (např. hledání v databázi kriminálních činů v People Finders). Jejich výhodou je zaměření na digitální stopy fyzických osob, proto jsou výsledky spíše faktografické nejen seznam zdrojů.

Jak bylo popsáno při vymezení digitálních stop (kap. 1.2), může být zjišťována jakákoli informace. Rozdíl je ale ve snadnosti jejich zneužití, ke kterému někdy může dojít až při spojení s dalšími zjištěnými údaji. Proto vznikají cykly zjišťování informací, kdy dříve zjištěné digitální stopy jsou uplatněny pro zvýšení úspěchu dalšího kroku. Důležité je, že citlivější informace takto mohou být získány složitějšími postupy, kdy každý cyklus představuje možnost odhalení útoku na informace.

56 KOPECKÝ 2017, s. 21.

57 Např. Pipl, Spock nebo Spokeo.

Tyto cykly, obvykle začínající u rešerše volně dostupných informací, jsou typické také pro sociální inženýrství. To představuje „*využití podvodu, přesvědčování, vydávání se za jinou osobu, emocionální manipulaci a zneužití důvěry pro získání informace nebo přístupu k počítačovému systému přes člověka.*“[58] Jeho úspěch stojí na přesvědčivých, ale falešných žádostech. Jedná se tedy spíše o psychologický útok, kdy informační technologie jsou jen možným prostředkem. Thomson[59] uvádí, že právě knihovny mohou být jednoduchým zdrojem informací o třetích stranách při sociálním inženýrství. Náchylné jsou především na situace, kdy se jedná o vděk (sociotechnik potřebuje pomoc, protože něco zapomněl a měl by problém), protože základní funkcí knihovny je uspokojování informačních potřeb. K úspěchu také přispívá vydávání se za jinou osobu (např. pracovníka IT oddělení ve velké knihovně), kdy k důvěryhodnosti využívá znalost jazyka, zavedených postupů a osobních informací.

Sociální inženýrství obecně vychází z toho, že prostředkem k získání informace je člověk, jehož slabiny se projevují především vlivem emocí. Aby sociotechnik působil důvěryhodně, musí vystupovat sebevědomě a způsobem, jaký je očekáván, kdyby se nejednalo o falešnou situaci (vč. grafické šablony, která je obvykle využívána osobou, za kterou se sociotechnik vydává). Při samotné interakci usiluje o vyvolání emočního nátlaku, který může být pozitivní (zájem o lákavou nabídku, zvědavost, empatie apod.) nebo negativní (strach z finančního či jiného postihu, krátký časový limit, nebezpečí)[60]. Sociální inženýrství je využíváno, aby byla sdělena informace (např. phishing), ale také aby byl vykonán nějaký čin (např. otevřena příloha e-mailu pro infikování malwarem). Vzhledem ke své efektivitě je podstatou nebo alespoň zvýšením úspěšnosti mnoha internetových útoků.

Protože děti a dospívající mají omezené životní zkušenosti, mohou být více ovlivněny sociálním inženýrstvím, zejména pokud je využito psychických charakteristik typických pro tato vývojová období. Děti, především citově deprivované, mohou být ovlivnitelné z důvodu usilování o uznání a náklonost, roli může hrát také výchova dětí k respektu k autoritám, kdy dítě může podlehnout osobě, která se za autoritu (např. učitele) vydává. V případě dospívajícího roste význam společenských kontaktů a budování vlastního společenského postavení, kdy může podlehnout nabídce, která jej podle jeho názoru přiblíží žádoucímu statusu. Nutné je ovšem připomenou, že navzdory charakteristikám vývojových období je každý jedinec odlišný působením biologických, sociálních a psychologických faktorů. Pro omezení vlivu sociálního inženýrství je zásadní dodržování pravidel bezpečného chování (viz kap. 1.3.3).

Přestože pasivní digitální stopy nejsou pro obsah této publikace tak významné, s aktivními digitálními stopami se ovlivňují a při útoku mohou být využity oba

58 THOMPSON 2013, s. 222.

59 THOMPSON 2013, s. 223–224.

60 MITNICK 2003.

typy. Základní, ale tím také nejvyužitelnější informace nabízí internetový prohlížeč. Další informace poskytují zařízení podle toho, jaké senzory obsahují (např. mobilní telefon může informovat o aktuální pozici, různé softwary a online nástroje mohou zasílat autorovi informace, např. pro zkvalitňování produktu, řešení problémů apod.). Tyto postupy a informace by měly být popsány v licenčních podmínkách daného produktu, které ale většina uživatelů nečte[61]. To je problém především samotného uživatele, ale do určité míry i autora produktu, protože tak lze pochybovat, že byl opravdu udělen informovaný souhlas se zpracováním těchto informací[62]. Svou roli hraje i dynamika dokumentů, opakovaně vznikají nové verze. Opustit zavedenou službu ale nemusí být snadné, i když uživateli přestanou vyhovovat nově nastavené podmínky v oblasti soukromí, jak ukázal pokus Facebooku se službou Beacon[63]. Přitom součástí podmínek nemusí být jen využití digitálních stop provozovatelem produktu, ale také třetí stranou. Podle Bechmann je rozhodnutí o přijetí podmínek využití digitálních stop především u sociálních médií (vč. social-pluginů, např. *Like* nebo *Tweet* na stránkách třetích stran) podmíněno ne jejich obsahem, ale předchozím přijetím přáteli, kterým člověk důvěřuje[64].

1.2.2 Legální narušení informačního soukromí

Narušení informačního soukromí mohou představovat informační incidenty (viz kap. 1.2.3), ale také legální, v některých případech i zákonem dané postupy, např. vyšetřování internetového trestného činu s využitím digitálních stop. K pochopení důvodů proč věnovat pozornost informační bezpečnosti přispívá znalost možných důsledků obou forem využití[65].

Legálně dostupné digitální stopy, především zveřejněné či poskytnuté se souhlasem člověka, kterého se týkají (subjekt údajů), mohou mít vysokou hodnotu pro jejich zpracovatele, ale subjekt údajů může považovat jejich (byť legální) využití za narušení svého soukromí. V marketingu se dlouhodobě prosazuje využití podobných postupů, které jsou popsány u sociálního inženýrství v kap. 1.2.1[66]. Cílený marketing je přizpůsoben zájmům člověka. To je pozitivní jak pro subjekt údajů i pro prodejce, protože se omezí množství reklamy, které je člověk vystaven

61 BECHMANN 2014, s. 22.

62 Toto je nutný předpoklad pro legální zpracování osobních údajů podle práva Evropské unie dle Směrnice Evropského parlamentu a Rady 95/46/ES.

63 FISH 2009, s. 109.

64 BECHMANN 2014, s. 35.

65 CHANG 2010, s. 526.

66 MCLUHAN 2008, s. 20.

a kterou prodejce platí, na tu s větší pravděpodobností úspěchu[67]. To odpovídá přímému prodeji, kdy dobrý prodavač odhaduje na základě pozorování a zkušenosti charakteristiky možného kupujícího[68]. Intenzivnější formu představuje behaviorální marketing[69], který je založený na analýze chování pro jeho predikci. Pokročilá predikce staví na psychografických charakteristikách (nejčastěji dle marketingové segmentace PRIZM do 66 typů) a aktuálně vykonávaných činnostech (od vyhledávacích dotazů, přes geografickou polohu po fyzickou aktivitu, např. zatloukání hřebíků)[70].

Cílený marketing k dětem je často diskutován kvůli etice. Děti mohou být předmětem analýz stejně jako jiní lidé, ale někdy jsou úmyslně využívána prostředí a zájmy spojené primárně s dětmi, např. internetové hry se sociálními prvky pro virální šíření. Informace z profilu dítěte slouží jako zdroj pro cílenou reklamu. Ve hře může být zobrazena reklama formou tzv. product placement, dětem jsou nabízeny produkty s nízkou finanční hodnotou (např. poukaz na hamburger) za informace nebo šíření reklamy. Sofistikované spojení těchto metod bývá označeno jako *game-vertising*[71]. Jinou variantou ceny za produkt je stažení žádaného softwaru[72].

Jako zdroj informací pro marketing i další využití jsou nejvíce využívány vyhledávače (záznamy vyhledávacích dotazů, např. pro včasné detekování počátku chřipkové epidemie[73]) a sociální sítě (např. pro predikci vývoje společenské situace v politicky nestabilních oblastech[74] nebo nezaměstnanosti[75]). Jedná se v zásadě o monitoring společnosti pro předvídání nežádoucích jevů a možnost včasného zásahu. Pro tento účel slouží monitoring digitálních stop i na úrovni jednotlivců. Například senioři jsou monitorováni především pro kontrolu zdravotního stavu (tzv. telemonitoring)[76], v případě dětí se spíše jedná o monitoring místa pohybu, ale také různých činností online (viz mediační strategie v kap. 1.3). Často je využíváno mobilní zařízení, které v současnosti obvykle obsahuje všechny potřebné senzory. Při tomto opatření se někdy děti úmyslně rozhodnou *zapomínat* mobilní telefon doma, aby si uchránily své soukromí před rodiči[77] (viz kap. 1.3.2). Podobně je tomu u monitoringu zaměstnanců, který ale slouží spíše pro ochranu zaměstna-

67 WEAVER 2007, s. 326.

68 MÜLLER 2011, s. 83–85.

69 Part IV: Marketing & Promotion 2006; SULLIVAN, 2011.

70 MÜLLER 2011, s. 87–90.

71 CHESTER 2008.

72 CHESTER 2008.

73 GINSBERG 2008.

74 SUJA 2011.

75 NIKOS 2009.

76 VÁLEK 2009.

77 FISH 2009, s. 64.

vatele. Sledována je pracovní činnost na služebních zařízeních. Mezi eticky i právně problematické postupy patří např. čtení e-mailů[78] v pracovní schránce, ale také v osobní poště otevřené v pracovní době na pracovním počítači, bezproblémové není ani využití kamerových systémů. Podobné prostředky využívají školy pro monitoring chování svých žáků, zejména na sociálních sítích[79].

Ve vztahu zaměstnavatel – zaměstnanec není monitoring jediným využitím digitálních stop. Dle výzkumů jsou často využity digitální stopy při rozhodování o přijetí zaměstnance, s čímž operuje také vzdělávání k digitálnímu občanství[80] (viz kap. 2.3). Vlivem impulzivnosti a experimentování dospívajících[81] a omezené možnosti odstranit vzniklou digitální stopu, může dospívajícím neuvážeností vzniknout problém, který si uvědomí až po letech právě při hledání zaměstnání. Mezi typické nežádoucí záznamy lze zařadit[82] informace o depresích, myšlenkách na sebevraždu, uvěznění, potratu, těhotenství nebo závislosti, ale i fotografie užívání alkoholu či drog a jiného nevhodného chování, nevhodné komentáře, špatné vyjadřování o předchozím zaměstnavateli, nekvalitní sebeprezentace (i jazyková), příp. nepravdivé údaje o kvalifikaci. Na druhou stranu je nutné upozornit, že digitální stopy mohou mít i pozitivní vliv ve vztahu k potenciálnímu zaměstnavateli, když prezentují schopnosti daného člověka. Rozšířenost užití digitálních stop pro tento účel lze doložit výzkumy:

- 59 %[83] – 75 % potenciálních zaměstnavatelů dělá rešerši žadatelů o zaměstnání na sociálních sítích[84];
- totéž dělá 91 % personalistů, využívají především Facebook (76 %), Twitter (53 %) a až následně specializovanou profesní sociální síť LinkedIn (48 %), 69 % dotázaných někdy odmítlo žadatele kvůli jeho digitální stopě[85];
- 26 % manažerů si ověřovalo digitální stopy žadatelů o zaměstnání a 63 % z nich se kvůli výsledku rozhodlo někoho nepřijmout; podobně 26 % administrativních pracovníků vysokých škol hledalo digitální stopy žadatelů o studium.[86]

Monitoring v řízení lidských zdrojů, ať žadatelů o zaměstnání nebo zaměstnanců, slouží jako prevence problému. Když už k němu dojde, přichází ke slovu jiné

78 POŽÁR 2005, s. 282.

79 WEAVER 2010, s. 26.

80 GRAYSON 2011, s. 9–10.

81 VÁGNEROVÁ 2000, s. 210.

82 MOORE 2012, s. 86; SWALLOW 2011.

83 Careerbright. You have been searched – What did we find about you? In: EKE 2012.

84 GRAY, Deborah M. A Linda CHRISTIANSEN. A call to action: The privacy dangers adolescents face through use of Facebook.com. In: MOORE 2012, s. 86.

85 SWALLOW 2011.

86 GRAYSON 2011, s. 9.

uplatnění digitálních stop, a to vyhledávání, analyzování a vyhodnocení v rámci forenzního, příp. kriminálního vyšetřování. Mohou prokázat jak alibi, tak i spáchání nežádoucího jednání. V evropském i českém prostředí bylo diskutováno tzv. data retention, tj. poskytování provozních a lokalizačních údajů od poskytovatelů připojení k internetu a mobilních operátorů pro účely vyšetřování dle zákona č. 127/20058 Sb., o elektronických komunikacích, který byl po zásahu Ústavního soudu[87] právě v této oblasti upraven pro větší ochranu soukromí. Mobilní zařízení lze při vyšetřování využít i jako mikrofony, a to i při vypnutí po vzdálené aktivaci[88]. Na straně pachatelů i vyšetřovatelů jsou používány sofistikované metody práce s digitálními stopami[89]. Rak a Porada[90] uvádějí, že digitální stopy při šetření neslouží jen pro doložení klíčových činností, ale i pro budování profilů zájmových osob, např. pomocí záznamů e-komerce.

Kriminalistika spadá pod výkon veřejné správy. V ní digitální stopy slouží pro ochranu zájmů státu nebo jiných lidí než subjektu údajů (např. ve veřejných informačních systémech typu katastr nemovitostí si může kupující ověřit majitele a případná břemena na nemovitosti). Podle zákona o informačních systémech veřejné správy musí být všechny veřejné rejstříky a systémy dostupné i přes internet. Stát ale i pro své potřeby vytváří nebo požaduje po uživateli vytvoření digitálních stop, které sám využívá[91]. Jedná se například o různé elektronické identifikační karty nebo EET (elektronická evidence tržeb). Stát se tak stává správcem rozsáhlé databáze digitálních stop o každém občanovi, které mohou být zneužity, např. nesprávným chováním úředníka[92].

1.2.3 Informační útoky se zaměřením na dětské oběti

Přestože jedinec může pociťovat narušení soukromí, řada institucí využívá jeho digitální stopy legálně. Způsoby užití digitálních stop uvedené v předchozí kapitole jsou korektní při splnění zákonem daných podmínek (např. omezení cílové skupiny při obsahově nevhodné reklamě, informovaný souhlas při zpracování osobních údajů atp.). Určité typy digitálních stop vznikají i proti vůli člověka, kterého se týkají, většinu ale může ovlivnit. V případě internetových útoků hraje klíčovou roli uvážlivé jednání člověka. Digitální stopy jsou často zneužívány při internetových

87 Nález Ústavního soudu ze dne 22. 3. 2011, spis. zn. Pl.ÚS 24/10.

88 GRAYSON 2011, s. 11-12.

89 Formou kazuistik prezentuje LATTA 2011.

90 PORADA 2006, s. 14.

91 Výhody i nevýhody v oblasti omezení soukromí podrobně popisuje LYON 1994.

92 V roce 2007 společnost HM Revenue and Customs (britská organizace pro oblast daní) ztratila dvě CD s osobními a bankovními informacemi o 25 milionech žadatelů o příspěvek na dítě. Viz NIXON 2010, s. 177.

útocích z jejich podstaty nebo pro podpoření efektivity, roli při tom hraje zkvalitňování technického zabezpečení[93] a omezená informační gramotnost uživatelů. Stále silněji se projevuje, že nejslabším článkem zabezpečení je člověk[94].

Sama ztráta či získání informace je *„významným motivačním faktorem pro páchání trestné činnosti“*[95]. Cílem může být získání dalších, citlivějších informací (viz kap. 1.2.1) nebo poškození uživatele či jeho zařízení (především dat). Obecně mohou být internetové útoky cílené nebo necílené (plošné, např. hoax). Často se ale jedná o stav mezi těmito extrémy, protože určitá cílenost může být dána již jazykovou mutací. Čím méně je útok cílený, tím je méně efektivní, proto oslovuje více potenciálních obětí. Proti tomu cílené útoky jsou sice náročnější, ale o to úspěšnější. Dále jsou popsány vybrané typy informačních útoků, se kterými se mohou běžně setkat děti a dospívající.

Běžný útok pro získání informací nebo jiné formy poškození uživatele představuje využití malwaru (škodlivého kódu). Různé typy malwaru se mohou objevit i na nedostatečně zabezpečeném veřejném počítači, např. v knihovně, kde používání stejného počítače mnoha uživateli znamená přínos pro útočníka. K nákaze může dojít různými způsoby, aktuálně je běžné infikování přes USB disk považovaný za ztracený (např. knihovník jeho užitím chce zjistit, komu disk vrátit), přes software stažený ze služby pro sdílení souborů, přílohu v e-mailu, neošetřenou zranitelnost v prohlížeči, přehrávači videí, klienta pro zprávy atd.[96]

Jak je uvedeno v kap. 1.2.1, mezi útoky pro získání citlivějších informací je možné zařadit phishing a pharming, které jsou založeny na kontaktování uživatele a jeho přesvědčení pomocí sociálního inženýrství o nutnosti zadat autentizační a případně i další údaje do připraveného (podvrženého) formuláře. Získané autentizační údaje jsou obvykle využity ke krádeži identity (viz níže). Často, i když ne nezbytně[97], jsou tyto útoky ve spojení s finančními institucemi. Phishing využívá pro sběr dat podvrženou webovou stránku, proto je možné ho odhalit díky nesprávné URL adrese. Proti tomu pharming využívá tzv. *DNS cache poisoning*, kdy dojde ke změně záznamů DNS pro převod jmenných adres na IP adresy[98], a to buď uložených v počítači uživatele, nebo přímo v DNS serveru. Při pharmingu je pak po zadání správné URL adresy zobrazena podvržená stránka, odhalení je tím náročnější. K získání autentizačních údajů může dojít i uhodnutím či zjištěním specializovaným softwarem. O tento útok se často pokouší i děti, které se tak

93 Institute of Management & Administration. Six Security Threats That Will Make Headlines in ’05. In: THOMPSON 2013, s. 222 .

94 MITNICK 2003.

95 POŽÁR 2005, s. 53.

96 KIM 2011, s. 684.

97 KIM 2011, s. 677.

98 KRÁL 2006, s. 230.

stávají útočníky. Podle výzkumu[99] ve Velké Británii 25 % dospívajících někdy zkusilo prolomit přístup do facebookového účtu jejich kamaráda, přestože si byli vědomi toho, že to není správné. Jak by mělo vypadat silné heslo, aby se omezilo, až znemožnilo prolomení, popisuje kap. 1.3.2.

Při zjištění dostatku informací o oběti se za ni může začít útočník vydávat (krádež identity). Podle toho, jaké údaje zjistil, a kde se jimi může dostatečně prokázat, může vykonávat různé škodlivé činnosti. Pokud byly zjištěny autentizační údaje k elektronickému bankovnictví, může z účtu oběti posílat peníze, žádat o půjčku apod. V případě, že získal přístup do profilu oběti na sociální síti, nabízí se mnoho možností pro kyberšikanu. Pro krádež identity ale nejsou nutné jen autentizační údaje, může se jednat např. o osobní informace, se kterými je vytvořen falešný účet na jméno oběti. Náprava důsledků krádeže identity je velmi složitá, Identity Theft Resource Center odhaduje její časovou náročnost v průměru na 330 hodin[100].

Krádež nebo vytvoření falešné identity může útočník využít i při sexuálně orientovaných útocích často spojovaných s dětmi, což je především grooming a sexting. Je běžné, že útočník mění své jméno, věk i pohlaví[101]. Problém je v tom, že děti se často mylně domnívají, že by v komunikaci dospělého poznaly[102], čímž se zvyšuje rizikové chování. K tomu je vhodné uvést, že 33,2 % dětí na internetu říká vždy pravdu a naopak 2,49 % respondentů absolutně věří tomu, co jim o sobě někdo na internetu říká[103].

Grooming představuje získávání digitálních stop, často z přímé komunikace mezi obětí a útočníkem, kdy cílem je sexuální zneužití dítěte. To nemusí probíhat jen pohlavním aktem ve fyzickém prostředí, může mít i nekontaktní formu, jako svlékání dítěte před webkamerou (sexting, viz další odstavec) nebo vystavení dítěte obscénní komunikaci[104]. Kybergrooming není jen záležitost preferenčních pedofilů[105], pro snadnost úspěchu jej využívají i osoby neschopné navázat partnerství s dospělou osobou, morálně narušení či sexuálně nevyzrálí jedinci experimentující s dětmi a osoby trpící duševní poruchou.

Pokud má dojít ke kontaktnímu zneužití, bývá dlouhodobě budována důvěra dítěte, aby souhlasilo se schůzkou. Při budování vztahu mezi útočníkem a dítětem má opět silný vliv sociální inženýrství, uplatňuje se především při tzv. zrcadlení (útočník se snaží přesvědčit oběť, že má stejné zájmy i problémy, takže si dokonale rozumí). K dospívání totiž patří zájem o hledání (určitou dobu platonického)

99 WEAVER 2010, s. 27.

100 KIM 2011, s. 678.

101 Využití internetu dětmi ve věku od 12 do 17 let 2006.

102 Safer Internet for Children 2007.

103 SZOTKOWSKI 2013.

104 VANÍČKOVÁ 1997, s. 12.

105 VANÍČKOVÁ 1999, s. 33.

partnera[106]. Komunikaci s neznámými uživateli internetu přiznalo 48,59 % dětí, přičemž podle 22,92 % jejich internetový známý žádal, aby jejich komunikace byla udržena v tajnosti. Dalším krokem ke kybergroomingu je osobní schůzka, kterou by odmítlo 50,3 % dětí (17,78 % by ji akceptovalo, 31,02 % nedokáže posoudit, jak by se rozhodlo)[107]. Schůzka je možná i v případě, že útočník o oběti zjistí, kde se nachází, což může být snadné díky již zmíněné oblibě sociálních sítí a zveřejňování místa bydliště, školy a kroužků. Na druhou stranu i děti někdy podléhají kybergroomingu s jasným vědomím situace, např. s vidinou odměny ve formě financí, dárků, nebo jen zájmu, u dospívajících může být pohlavní styk dobrovolný z přesvědčení, že se jedná o lásku[108].

S groomingem souvisí sexting, tj. zasílání sexuálně explicitního obsahu spojeného s obětí[109], který může být následně zveřejněn. Problém se obvykle vyskytuje u dospívajících (méně často dospělých, častěji žen), kteří si tyto záznamy posílají v partnerském vztahu. Po jeho ukončení ale může s cílem pomsty dojít ke zpřístupnění materiálu dalším lidem. Toto byl případ Jessicy Logan a Hope Witsell, které v důsledku sextingu spáchaly sebevraždu[110]. Sexting je problémem i u českých dětí. Podle výzkumu Kopeckého 12,14 % dotazovaných dětí poslalo a 7,41 % zveřejnilo fotografii nebo video, na kterém byly zobrazeny částečně či zcela nahé[111]. I v tomto směru výzkum prokázal výraznou růstovou tendenci v posledních letech. V roce 2012 odeslalo sexuálně laděné materiály 8,99 % dětí, v roce 2014 to bylo 12,14 % a v roce 2017 již 15,47 % dětí[112]. Mezi nejčastější důvody sextingu v ČR patří dárek pro přítele/přítelkyni (38,53 %), flirt (35,47 %) a odpověď na zaslanou „sexy" fotografii, video a podobně (33,73 %). Podle National Center for Missing & Exploited Children 51 % dívek, které takové materiály poslaly, k tomu byly tlačeny chlapcem[113]. Vzhledem k obsahu materiálů u dospívajících při sextingu v podstatě dochází k šíření dětské pornografie, což je trestné.

Zneužití sexuálního zobrazení dítěte zase naplňuje podstatu kyberšikany, která spočívá v poškození s využitím informačních technologií[114], ať už má formu ponižování, pomluvy, pronásledování, sexuálního harašení, záznamu násilí nebo jinou. Kyberšikana proti tradiční šikaně má specifika, která zesilují důsledky pro oběť, jež jsou vázány především na neustálou dostupnost komukoli. Ke kyberšikaně se tak

106 ŘÍČAN 1990, s. 197.

107 SZOTKOWSKI 2013.

108 LEANDER 2008, s. 1261.

109 DÖRING 2014.

110 DÖRING 2014.

111 KOPECKÝ 2015.

112 KOPECKÝ 2017.

113 GRAYSON 2011, s. 30.

114 LIVINGSTONE 2011, s. 61.

mohou přidat nejen děti z okolí, ale miliony lidí na internetu, únik je v podstatě nemožný. Protože při kyberšikaně vznikají digitální stopy jednání způsobujícího oběti újmu, problémem je dlouhodobější působení na oběť a pravděpodobnost, že se poškozující obsah může objevit kdykoli znovu. I v tomto případě již mezi důsledky kromě psychických obtíží patří i sebevraždy dětí, např. Megan Meier[115]. Původci kyberšikany si často nejsou vědomi toho, že jinému ubližují, považují své jednání za nevinnou hru[116]. S kyberšikanou úzce souvisí stalking, nebezpečné pronásledování, které oběť také poškozuje, protože stalker chce, aby o jeho činnosti věděla. Podle Moore[117] zatím stalkeři neobjevili plně sílu IT a stále se silně váží na tradiční metody, proto je pravděpodobné, že se rozšířenost tohoto typu útoků bude zvyšovat. Stalking je v České republice trestný čin, ale až po překročení stanovené úrovně (dlouhodobé, min. 4–6 týdnů, opakované, min. 10 pokusů, obtěžování přítomností útočníka s důvodnou obavou o život či zdraví oběti či jejích blízkých)[118].

Mezi další internetové útoky, se kterými se děti běžně setkávají, by bylo možné zařadit různé typy nevyžádaných zpráv. Ty se šíří přeposíláním, kdy přeposílající neopodstatněně důvěřuje uvedeným informacím (např. řetězové zprávy nebo hoax). Druhou variantou je zneužití kontaktních údajů, které jsou často shromážděny automaticky pomocí robotů (např. rozpoznání typického tvaru e-mailové adresy při procházení webu) nebo jsou prodávány jejich databáze. Rozpoznání těchto zpráv je založeno na identifikaci manipulativních technik (viz kap. 1.2.1), základním bezpečnostním opatřením je tedy hodnocení informací a jejich zdrojů.

1.3 Bezpečnostní opatření

Digitální stopy mohou být využity i zneužity. Bez ohledu na jejich obsah lze najít způsob, jak hodnotu vytěžit. Zanechání pozitivní digitální stopy je žádoucí, ale i ta je výsledkem odpovědného chování při produkci digitálních stop. Je proto vhodné znát a aplikovat bezpečnostní opatření, která omezí možnosti nežádoucího užití digitálních stop.

Jak je uvedeno v kap. 1.2, některé digitální stopy vznikají bez ohledu na přání člověka, kterého se týkají. I když nebude sám využívat žádné elektronické zařízení, s největší pravděpodobností o něm budou existovat stopy, které vytvořil někdo jiný, např. stát. Podstatné tedy není to, jestli digitální stopa člověka existuje, ale jak vypadá na úrovni kvantitativní i kvalitativní. Z hlediska kvalitativního lze rozlišovat, jak snadno informace umožňují identifikaci nebo využití třetí stranou.

115 KIM 2011, s. 679.

116 Safer Internet for Children 2007.

117 MOORE 2012, s. 90.

118 ŠÁMAL 2010, s. 3006–3008.

Kvantitativní rozměr je podstatný proto, že čím více informací o subjektu údajů je dostupných, tím snazší je jejich využití[119].

Pro podporu informační bezpečnosti lze využít různé typy opatření. Chování člověka při práci s IT by nemělo být paranoidní, ale uvážlivé. Pro podporu bezpečnosti lze využít i různých softwarů a online nástrojů, které mohou přispět v různých, ale spíše dílčích směrech. Jako prevence, ale také pro řešení dopadů informačního útoku, mohou pomoci právní předpisy. Všechny tři směry mohou nabývat různé úrovně sofistikovanosti a specifická opatření jsou závislá i na prostředí, do kterého jsou začleněna (např. v zaměstnání). S ohledem na zaměření této publikace budou tři jmenované směry popsány na úrovni, kterou by měly znát děti a dospívající pro omezení nejčastějších typů hrozeb (viz kap. 1.2.3). Současně se jedná o opatření, která jsou určitým způsobem ukotvena v navržených lekcích (kap. 3.2).

Děti, stejně jako rodiče, učitelé nebo knihovníci, mají možnost využít různých opatření pro zvýšení informační bezpečnosti dětí. Bezpečnostní opatření ale mohou snižovat komfort (např. požadavek opakované autentizace) nebo i možnost svobodného přístupu k informacím (např. filtry obsahu), což je zásadní hodnota demokratické společnosti, a také hodnota reprezentující knihovnu. Je proto klíčové zvážit, která opatření aplikovat, aby bylo dosaženo co největší rovnováhy mezi přístupem k informacím a bezpečností. Opatření, která lze aplikovat, jsou předmětem následujících podkapitol.

Není možné definovat jednotnou šablonu vhodných opatření, vždy záleží na individuálním posouzení, např. na základě dřívějšího chování dětí, jejich věku nebo psychických dispozicích. Lidé, kteří pracují s dětmi (zde především učitelé a knihovníci) by také měli zvážit, do jaké míry akcentují právo dítěte na soukromí a nakolik je toto právo omezeno tím, že na informace o dítěti má nárok i jeho rodič[120]. Poskytnutí informací by mohlo poznamenat důvěru dítěte v knihovnu nebo školu.

Mediační strategie knihoven v oblasti práce na internetu jsou popsány jen omezeně[121]. Více pozornosti je věnováno školám[122], primárně se ale odborné publikace zaměřují na rodiče[123], jako klíčové subjekty při řízení přístupu dětí k internetu. Při stanovování možností mediací knihovnou se proto lze inspirovat právě strategiemi odlišných subjektů. Pro přiblížení typů mediačních strategií pro informační bezpečnost je využito klasifikace z výzkumu EU Kids Online[124]:

– Aktivní mediace používání internetu (bez omezení na informační bezpečnost): rozmluva o činnostech dítěte na internetu, přítomnost (rodiče) při

119 ANGWIN 2010.

120 WOLD 2010, s. 72.

121 WOLD 2010.

122 LIVINGSTONE 2011, s. 121-127.

123 LIVINGSTONE 2011, s. 103.

124 LIVINGSTONE 2011, s. 103–130.

používání internetu dítětem, podpora samostatného objevování a učení o internetu, sezení vedle dítěte při používání internetu, společné sdílení aktivit na internetu;
- Aktivní mediace dětské internetové bezpečnosti: vysvětlení, proč jsou některé stránky dobré nebo špatné, pomoc při obtížích udělat nebo najít něco na internetu, navrhování způsobů bezpečného používání internetu, doporučení způsobů chování k jiným lidem online, mluvení o reakcích na pocit poškození něčím na internetu, pomoc s něčím, co dítě v minulosti na internetu poškodilo;
- Restriktivní mediace: stanovení pravidel pro uvedené činnosti, zejména zpřístupňování osobních informací, sdílení fotek, videí nebo hudby, stahování hudby nebo filmů přes internet, vlastní profil na sociální síti, sledování videoklipů na internetu, používání komunikačních služeb;
- Monitoring: kontrola navštívených webových stránek, profilu dítěte na sociální síti nebo v online komunitě, přátel nebo kontaktů přidávaných k profilu na sociální síti, zpráv v komunikačních službách využívaných dítětem;
- Technická mediace: software pro prevenci proti malwaru a nevyžádaným zprávám, filtr obsahu (zejména webu), prostředek sledování navštívených webových stránek, prostředek omezení doby strávené na internetu.

Při volbě mediační strategie by knihovna, stejně jako rodiče, měli zvážit možnosti různých přístupů, jejich výhod i nevýhod a možností kombinací. Vliv může mít prostředí, tedy co je pro danou komunitu obvyklé a akceptované. Podle EU Kids Online[125] patří Česká republika ke státům, kde je nejvíce zastoupena aktivní mediace internetové bezpečnosti (94 % rodičů), naopak restriktivní strategie patří mezi nejméně využívané (78 % rodičů). V oblasti monitoringu a technické mediace Česká republika vykazuje srovnatelné zastoupení s jinými státy. Využití všech mediačních strategií s rostoucím věkem dětí ubývají, především mezi 14. a 15. rokem života[126]. Při hodnocení dle socio-ekonomického statusu nejsou rozdíly kromě aktivní mediace, která se při vyšším statusu také objevuje častěji. To naznačuje skupiny dětí, na které by bylo vhodné zaměřit aktivní mediaci zajištěnou jiným subjektem než rodiči. Přístupy rodičů se liší také podle jejich věku, vzdělání, místa bydliště a dalších faktorů (např. charakteristik, které se u dítěte časem mění, jako délka času strávená na internetu nebo ročník ve škole), které se promítají do úrovně digitální propasti (viz kap. 2.1). Proto je vhodné zvážit i tyto faktory při nastavování mediační strategie knihovny[127].

Dle 72 % dětí by se neměly měnit rodičovské mediace, snížení nebo zvýšení zájmu rodiče o dítě na internetu se objevují ve srovnatelném množství ve zbývají-

125 LIVINGSTONE 2011.

126 LIVINGSTONE 2011.

127 ÁLVAREZ 2013.

cích odpovědích[128]. V ČR přitom zájem o zvýšení zájmu patří mezi nejméně projevované (7 % dětí), naopak ve srovnání s jinými státy české děti pociťují výraznější omezení rodičovskými mediacemi (48 % dětí) a nejčastěji ze všech států ignorují, co jim rodiče o chování na internetu říkají (54 % dětí). To opět podporuje význam aktivní mediace zajištěné vedle rodičů i dalšími subjekty, mezi které patří knihovny. Výhodou škol, kterou uznávají i knihovníci, je jejich možnost zasáhnout všechny děti[129]. Poměrně výrazný, především v České republice[130], je vliv vrstevníků i v mediaci používání internetu, což přispívá k vhodnosti kooperativního učení, které je aplikováno v navržených lekcích (viz kap. 3.2). Subjektem pro poradenství o internetové bezpečnosti mohou být i knihovny, protože již v současnosti je děti uvádějí mezi zdroji pro tyto rady[131], byť ne ve výrazné míře.

Pokud tedy knihovny budou reflektovat přesvědčení rodičů o vhodných přístupech, měly by se zaměřit na aktivní a méně restriktivní mediaci. To umožňuje také nižší omezení přístupu dětí k informacím, spíše na ně bude přeneseno rozhodnutí o způsobu nakládání s informacemi s tím, že si budou uvědomovat jeho důsledky. Toto řešení odpovídá také výzkumu Wolda[132] mezi učiteli a knihovníky v Norsku. Aktivní mediace používání internetu současně vede k snížení poškození dětí na internetu, naopak technická nemá na riziková jednání vliv[133]. Aktivní mediace internetové bezpečnosti a monitoring vedou ke zvýšení rizikového jednání, nicméně se může jednat o strategii učení pro vyrovnávání se s riziky[134]. Proti tomu podle jiného výzkumu[135] vede diskuze dětí s rodiči o problémech zpřístupňování osobních informací na internetu k redukci tohoto jednání dětí.

Wold[136] vidí možnosti knihoven ve srovnání se školami i rodiči jako jedinečné, které by měly být reálně nabízené a podpořené, protože staví na vyšší volnosti přístupu k informacím a také nabídce důvěryhodného místa, na kterém je možné žádat poradenství v tématech, která jsou ve formálnějších prostředích, jako je škola, nepředstavitelné. Podle jeho výzkumu sami knihovníci vidí internetové služby v knihovně jako pokračování jejich tradiční role zpřístupňování informací[137]. Tyto služby zahrnují (především u dospívajících) komunikaci přes internet,

128 LIVINGSTONE 2011.

129 WOLD 2010, s. 71.

130 LIVINGSTONE 2011, s. 124.

131 LIVINGSTONE 2011, s. 127.

132 WOLD 2010.

133 DUERAGER 2012.

134 DUERAGER 2012.

135 ÁLVAREZ 2013.

136 WOLD 2010.

137 WOLD 2010, s. 67.

a nejen vyhledávání informací, podpora těchto činností zlepšuje i vztah dospívajících ke knihovně[138].

Pro zjednodušení s lepší možností prezentace vazeb jednotlivých opatření jsou dále popsány možnosti knihoven v mediaci pro zvýšení bezpečnosti digitálních stop rozdělené do tří kategorií: právní možnosti, technické možnosti a možnosti chování uživatele internetu. Vzdělání, které je klíčovou složkou aktivní mediační strategie, podporuje efektivitu všech jmenovaných oblastí a současně představuje jádro této práce. Při zavedení libovolných opatření nikdy není možné garantovat stoprocentní jistotu bezpečí, protože vždy se může najít cesta kolem opatření. Každé ale staví bariéru, která může být pro konkrétní útok nepřekonatelná nebo odrazující, protože cíl není tak zajímavý, aby útočník vynaložil potřebnou energii.

1.3.1 Právní předpisy

Již stát nastavuje první, minimální úroveň informační bezpečnosti pomocí právních aktů. Zákon musí dodržovat každý, v opačném případě může být potrestán stanovenou sankcí. V případě informační bezpečnosti lze využít jako prevenci nebo řešení dopadu útoku řadu různých předpisů. Vždy záleží na kontextu, nebude zde proto uveden vyčerpávající seznam všech předpisů, které by mohly být aplikovány. Jmenovány budou pouze ty, které jsou nejčastěji využitelné v souvislosti s útoky popsanými v kap. 1.2.3. Všechny dále uvedené předpisy jsou využity ve znění platném ke dni 1. 2. 2018.

V první řadě s ohledem na právní sílu je nutné uvést Listinu základních práv a svobod. Pro oblast informační bezpečnosti se jedná především o čl. 10, kde je zaručena ochrana osobnosti člověka na úrovni pověsti, důstojnosti, jména a cti, ochrana před neoprávněným zásahem do soukromí a „*před neoprávněným shromažďováním, zveřejňováním nebo jiným zneužíváním údajů o své osobě*“[139]. Listina akcentuje údaje o osobě, což je výrazně širší definice než osobní údaj dle zákona č. 101/2000 Sb., o ochraně osobních údajů. Garantována je také ochrana tajemství listovního a jiných písemností a záznamů uchovávaných v soukromí nebo zasílaných poštou, podávaných telefonem, telegrafem a podobným zařízením, tedy i internetem. V těchto směrech jsou sankce stanoveny zákonem č. 40/2009 Sb., trestní zákoník (§ 182 a § 183), kdy tajemství představuje obsah komunikace a dokumentů, ale ne metadatové údaje, přestože i ony mohou prozradit podstatné informace. Bouřlivé reakce nedávno vyvolalo například zveřejnění lokalizačních

138 WOLD 2010, s. 68.

139 Usnesení č. 2/1993 Sb.

anonymizovaných údajů firmou Strava[140]. Naopak čl. 17, odst. 4 Listiny dává právo svobodně vyhledávat a šířit informace, což ale lze omezit zákonem pro ochranu druhých.

Trestní zákoník zahrnuje v současnosti 421 paragrafů, z nichž mnoho může být využito při specifických formách zneužití digitálních stop. Jako příklady lze uvést: § 228 Poškození cizí věci (byl použit při prolomení přístupu k uživatelskému účtu v počítačové hře a jeho zneužití[141]) nebo § 354 Nebezpečné pronásledování (viz kap. 1.2.3). Trestní zákoník upravuje také činy proti majetku při zneužití počítačového systému (§§ 230–232). Trestný je neoprávněný přístup k datům, přihlašovací údaje jsou samy o sobě chráněny jak na úrovni získání, tak i přechovávání, pokud je prokázán úmysl je využít. Poslední jmenovaný paragraf se zaměřuje na poškození dat nebo zásah do vybavení počítače, které je trestné i z nedbalosti, pokud k němu dojde při výkonu funkce, povolání, postavení apod. Zásah i z nedbalosti v zastávané pozici je také v případě neoprávněného nakládání s osobními údaji (§ 180).

Zákon č. 101/2000 Sb. stanovuje ochranu při jakémkoli nakládání s osobními údaji mimo vymezené výjimky, např. zpracování pro osobní potřebu fyzické osoby. Základní charakteristikou osobních údajů je dle § 4, písm. a) jejich schopnost identifikace konkrétní fyzické osoby (jednou informací nebo jejich souborem). Osobním údajem tedy může být i fotografie nebo video, kde je rozeznatelný konkrétní člověk. Citlivé údaje jsou zvláštní typ osobních údajů kvůli vyšší možnosti zneužití, jedná se o informace s potenciálem diskriminace (např. národnost nebo odsouzení za trestný čin) a biometrické údaje, které umožňují přímou identifikaci jedinečnou charakteristikou (např. otisk prstu). Pokud chce kdokoli shromažďovat nebo zpracovávat osobní údaje, musí k tomu mít zákonný důvod nebo poučený souhlas subjektu údajů (zákon definuje, o čem je nutné ho poučit) a zajistit technická a organizační bezpečnostní opatření. Ochrana osobních údajů v nejbližších měsících zaznamená výrazné změny s ohledem na nařízení Evropského parlamentu a Rady (EU) 2016/679 ze dne 27. dubna 2016 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů a o zrušení směrnice 95/46/ES, známého též pod zkratkou GDPR. To mimo jiné posiluje ochranu osobních údajů dětí a také ochranu osobních údajů v digitálním prostředí. Pro knihovny byla vytvořena příručka pro snazší přechod na novou úpravu[142].

Zákon č. 480/2004 Sb., o některých službách informační společnosti zahrnuje odpovědnost za obsah služeb informační společnosti, které jsou poskytovány

140 Viz např. MINELLE, Bethany. US military to review security amid Strava fitness app fears. *SkyNews* [online]. 29 January 2018 [cit. 2018-02-07]. Dostupné z: https://news.sky.com/story/us-military-to-review-security-amid-strava-fitness-app-fears-11228045.

141 LochyProduction 2013.

142 DANIELISOVÁ 2018.

na žádost, přičemž žádost i služba sama jsou řešeny elektronicky a slouží zejména pro vyhledávání a zpřístupňování informací. Poskytovatel je odpovědný za obsah, pokud se dozvěděl o jeho protiprávnosti. Tento zákon tedy například umožňuje, aby člověk vyžadoval od provozovatele služby smazání informací, které jsou pomluvou (protizákonné dle § 184 trestního zákoníku), kterou o něm někdo jiný napsal na veřejně dostupnou webovou stránku.

Z hlediska protiprávního obsahu je pro koncepci klíčový zákon č. 121/2000 Sb., autorský zákon (a návazně § 270 trestního zákoníku, který ale přináší blanketní úpravu vázanou na autorský zákon) a jeho porušování především při nelegálním stahování a sdílení autorských děl a obcházení technologických ochran. Autorský zákon vymezuje autorské dílo jako *„dílo literární a jiné dílo umělecké a dílo vědecké, které je jedinečným výsledkem tvůrčí činnosti autora a je vyjádřeno v jakékoli objektivně vnímatelné podobě včetně podoby elektronické, trvale nebo dočasně, bez ohledu na jeho rozsah, účel nebo význam*“[143], autorským dílem není myšlenka, například parafráze tedy není zákonem upravena, ale mělo by se s ní nakládat podle etických pravidel. Autorský zákon specifikuje omezení autorských práv, především v rámci zákonných licencí (citace, užití pro osobní potřebu atd.). Pro řešenou problematiku je ale stěžejní uvědomění si naopak jednání, které je možné autorským zákonem sankcionovat.

Nakládání s elektronickými autorskými díly je ovlivněno určitou nezávislostí na nosiči, kdy jsou umožněny jiné způsoby užití díla spojeného s nosičem (např. možnost půjčování) a bez něj (pro nehmotná díla je jediným možným užitím sdělování veřejnosti). Tento rozdíl například vede k tomu, že není možné půjčování e-knihy bez zaplacení odměny vlastníkovi majetkových autorských práv (pokud e-kniha nebyla zakoupena jako součást čtečky e-knih). Pro všechna elektronická díla je proto nutné důkladné seznámení se s licenčními podmínkami, které specifikují, jaké nakládání s dílem je možné.

Specifická úprava je v autorském zákoně pro počítačové programy (§ 65 a § 66). Většina omezení práv autora v § 66 pokrývá nakládání se softwarem způsoby, které jsou nutné pro jejich korektní využití, ale nebyly by v souladu s jinými částmi zákona (např. vytvoření rozmnoženiny v paměti počítače, tj. instalace). Pro software není možné využít užití pro osobní potřebu, stejně jako další bezúplatné zákonné licence (hlava I, díl 4). Různé typy elektronických děl mohou být spojeny s technickými prostředky ochrany práv, které je zakázáno obcházet (§ 43), stejně jako je zakázáno odstraňovat či měnit elektronickou informaci o správě práv k dílu či podporovat šíření takto upraveného díla (§ 44).

Vedle autorských práv upravuje autorský zákon i práva související, což jsou především práva výkonných umělců. Z tohoto důvodu je proto často porušením

143 Zákon č. 121/2000 Sb., § 2.

zákona, pokud například je bez souhlasu umělce vytvořena nahrávka koncertu a následně je umístěna na internet, a to přesto, že to udělá autor této nahrávky.

Bylo by možné pokračovat jmenováním dalších zákonů, které jsou využitelné při konkrétních internetových útocích, to ale není předmětem této práce. Důležité je uvědomit si, že i když zákonná úprava existuje, její role je na jednu stranu preventivní a na druhou stranu represivní. Jako prevence slouží tak, že lidé, kteří vědí, že by jednali protiprávně, si často čin rozmyslí, protože výsledek je pro ně méně zajímavý než obava z možné sankce. To ale předpokládá, že o dané právní úpravě ví, tato prevence tedy nefunguje bez osvěty. Není nutná znalost konkrétní právní úpravy, je ale potřebné povědomí o možnosti zákonného postihu. Současně ne pro každého je obava z postihu dostatečná, aby jej odradila.

Pokud prevence nebyla účinná, lze předpisy využít při represi. I zde se objevují významné problémy. Prvním je působnost práva, která je ohraničena státními hranicemi a občanstvím (teritorialita[144]). Tu je na internetu snadné obejít, např. využitím elektronických služeb, jejichž poskytovatelé nemají pobočku v ČR, příp. skrytím datových přenosů přes různé státy, kdy není výjimečný problém při předávání informací. V mezinárodním prostředí sice existují snahy o harmonizaci práva, především v rámci Evropské unie, problémy se ale objevují při jednání o dotčení suverenity států. Zásadní vliv má také složitost vzniku právních aktů, které mohou být problémem z hlediska rychlosti vývoje informačních technologií. Problém může nastat také v případě, že poškozený potřebuje podporu, ale neví, na koho se obrátit, příp. mu daná instituce nemůže pomoci kvůli omezeným pravomocím (Policie ČR[145], Úřad pro ochranu osobních údajů[146] atd.). Poškozený také nemusí vědět, že existuje možnost právní obrany, nebo se může obávat vložení velkého úsilí a finančních prostředků do soudního řešení bez jistoty, že výsledek bude v jeho zájmu. Posledním, ale významným nedostatkem je aplikace až po útoku, jelikož některé mohou způsobit nevratné následky, např. znásilnění nebo sebevraždu (viz kap. 1.2.3).

Vzhledem k jmenovaným výhodám i nevýhodám předpisů pro řešení internetových útoků je patrné, že usilovat o vhodně nastavené právní akty má smysl, ale současně by měla být jejich omezení zohledněna zavedením dalších typů bezpečnostních opatření.

144 Podrobněji např. NOVOTNÝ 1997; SMEJKAL 2001; MATĚJKA 2002.

145 Působnost dle zákona č. 273/2008 Sb.

146 Působnost dle zákona č. 101/2000 Sb.

1.3.2 Technické zabezpečení

Technické zabezpečení je v kontextu této publikace zaměřeno na koncové stanice[147]. Právě na technickou stránku se dříve informační bezpečnost omezovala[148], s rozšiřováním sociálních hrozeb (např. kyberšikana) jsou technická řešení vnímána jen jako část bezpečnostních opatření. Jejich výhodou je často automatizovaná prevence či řešení útoků, které pro běžného uživatele mohou být transparentní. Technická bezpečnostní opatření je možné rozdělit do čtyř základních kategorií: specializované bezpečnostní aplikace, operační systém, internetový prohlížeč a ostatní aplikace.

U operačního systému záleží na jeho charakteristikách, vývoji a bezpečnostní politice. V tradičním prostředí (stolní počítače a notebooky) silně převažují systémy Windows, nejčastěji ve verzi 7 (postupně nahrazována verzí 10)[149], v mobilním prostředí Android (68,63 %) a iOS (29,52 %)[150]. Tato tři prostředí se liší již svojí podstatou a vyžadují odlišná řešení. Přesto je možné vymezit alespoň základní bezpečnostní pravidla, která jsou společná.

V první řadě je nezbytností pro každý software od operačního systému po bezpečnostní aplikaci pravidelná, ideálně automatická aktualizace co nejdříve po jejím vydání. Tímto postupem jsou ošetřeny zjištěné slabiny v informačních systémech. Aktualizace brání zneužití přes známou a popsanou zranitelnost, na kterou existuje řešení.

Dalším krokem je vhodné využití autorizace (stanovení oprávnění). V prostředí Windows se jedná především o uživatelské účty. Jeden účet by měl odpovídat jednomu uživateli s tím, že nastavená oprávnění by měla reflektovat jeho znalosti a potřeby (sdílení přístupových údajů je bezpečnostním rizikem a omezuje řešení při bezpečnostním incidentu). Uživatelské účty jsou použitelné i v prostředí Android od verze 4.2 Jelly Bean[151]. Na jiné úrovni autorizace odpovídá udělení oprávnění aplikaci. Ta jsou přidělována při instalaci v OS Android, v iOS si o ně může aplikace požádat, když je aktuálně potřebuje k výkonu požadované činnosti, např. polohové služby pro zjištění místa na mapě. Autorizace je základním opatřením při ochraně digitálních stop, pokud chce uživatel využívat ukládání dat, a to nejen na úrovni operačního systému, ale i v mnoha dalších softwarech a službách, např. pro nastavení soukromí.

S autorizací úzce souvisí autentizace (prokázání identity), která je podstatná nejen u operačních systémů. Varianty autentizace lze kategorizovat podle toho, čím

147 Využíváno v širším slova smyslu, tj. stolní, přenosný (vč. tabletů) i kapesní (hl. smartphony).

148 Viz např. POTÁČEK 2003–.

149 Operating System Share by Version 2018.

150 Operating System Market Share 2018.

151 Jelly Bean 4.2 [2012].

je totožnost prokazována:[152] znalostí (hesla), vlastnictvím (např. mobilní telefon u SMS s autentizačním kódem) a bytím (tj. biometrické ověření, např. otisk prstu při odemykání telefonu). V případě operačního systému je autentizace využívána pro umožnění práce s počítačem po zapnutí nebo obnovení z režimu spánku, hibernace apod. S ohledem na možnost fyzických útoků je vhodné při každém opuštění počítače vyžadovat heslo a také mít nastavený optimální co nejkratší interval přechodu do režimu spánku při zapomenutí manuálního nastavení.

Autentizace se nejčastěji provádí pomocí hesla. Pro silná textová (tradiční) hesla jsou poměrně známá pravidla, doporučená je kombinace různých typů použitých znaků, dostatečná délka (8–12 znaků) i práce s ním, např. pravidelná změna po určitém období[153]. Mnohá pravidla jsou ale přenositelná i na jiné typy hesel. Především v mobilním prostředí se prosazují grafická hesla, která spočívají v zapamatování si vedení čáry do obrazce, výběru obrázků apod. I při jejich použití by si měl uživatel dát pozor především na tzv. piggybacking[154], tedy jejich neoprávněné zjištění pozorováním při zadávání. Základem funkčnosti autentizace je důsledné odhlašování od všech služeb. Hesla jsou ale využívána i na jiných úrovních, například v bezdrátových sítích je zásadní udržení bezpečnosti hesel, protože cizí připojený počítač v síti může mít přístup k přenášeným datům[155].

Dalším klíčovým softwarem je internetový prohlížeč. Z hlediska bezpečnosti běžného uživatele je vhodné opět zvážit vhodnou kombinaci nastavení pro konkrétního uživatele. V prohlížeči je možné nastavit blokování vyskakovacích oken, blokování instalace doplňků, blokování nebezpečného, klamavého nebo nevhodného obsahu (např. zobrazujícího násilí), pamatování přihlašovacích údajů nebo ochranu soukromí. Možné je smazání různých digitálních stop, např. historie prohlížení, uložená uživatelská jména a hesla apod. Další nabídka záleží na konkrétním produktu.

Jedna z obvyklých možností je nastavení Cookies. Ty primárně ukládají informace o relaci, pokud v ní ale byly zadány osobní informace, mohou se i tyto v Cookies uložit a být přes ni dostupné[156]. Jejich zakázání v podstatě znemožňuje práci s internetovými službami (mnoho jich funguje na personalizované úrovni, která při zákazu Cookies není realizovatelná). V minulosti vznikaly různé iniciativy, především v angloamerickém prostředí (USA, konkrétně Federal Trade Commision[157], a Velká Británie), jejichž cílem bylo zlepšit vztah se zákazníky tím, že

152 NIXON 2010, s. 154.

153 Podrobné vymezení pravidel pro silná hesla a jejich užívání, vč. tipů pro praktické vyvážení použitelnosti a bezpečnosti uvádí BOTT 2004, s. 111-123.

154 POŽÁR 2005, s. 119.

155 SALTZMAN 2008, s. E.14.

156 BOTT 2004, s. 42.

157 Federal Trade Commission Decision and Order 2011.

mu umožnily oznámit, že nechce být sledován. Respektování tohoto přání se ale v praxi příliš nepodařilo prosadit.[158] Opačný princip preferuje Evropská unie, kdy naopak uživatel musí vyjádřit souhlas (ne nesouhlas) s uložením Cookies[159], která ale navzdory stanoveným lhůtám ještě nebyla přenesena plnohodnotně do českého prostředí.

V případě využití cizího počítače (např. počítač v knihovně), je možné využít anonymní mód prohlížeče, jehož výhodou je, že po ukončení relace nejsou uloženy v prohlížeči žádné informace o předchozí aktivitě uživatele. To je ale omezeno jen na prohlížeč, např. stažené soubory v počítači zůstávají. Současně se jedná o opatření jen na straně používaného zařízení, při použití anonymního módu nedojde k omezení informací, které o uživateli prohlížeč posílá do prostředí internetu (např. zobrazovaným webovým stránkám). Pokud by uživatel chtěl omezit i tyto informace, musel by použít specializované nástroje, jako jsou anonymizéry, proxy servery nebo služby využívající Onion Routing[160], které jsou ale již nad rámec zaměření této publikace. Všechny výše jmenované nástroje se zaměřují jen na pasivní digitální stopy, je nutné doplnit je vhodným nakládáním s informacemi, které uživatel na internetu vědomě zveřejňuje.

Existují také specializované bezpečnostní aplikace využitelné běžnými uživateli, především různé typy antimalware (antivir, antispyware, antirootkit), firewall, antispam, filtr obsahu, antiphishingový nástroj nebo anonymizér. Antiviry by měly být schopny detekovat a odstranit různé typy škodlivého softwaru. Firewall oddělující chráněnou a nechráněnou část sítě může pomoci při zjištění odesílaných informací, nebo naopak při jejich přijímání, pokud jsou vyhodnoceny jako nevhodné. Pomáhá také zjištění skenování portů a řešení otevřenosti nevhodných. Antispam slouží k automatickému vyhodnocování přijímaných e-mailů jako nežádoucích (dle nastavených pravidel), podobně jako filtry internetového obsahu. Poměrně málo rozšířené jsou antiphishingové nástroje, jejichž cílem je varovat před podvrženou webovou stránkou. Lze se s nimi setkat např. při vyhledávání na Google, kdy vyhledávač varuje při pokusu otevřít webovou stránku, která je dle něj podvodná.

Podobně jako je apelováno na bezpečnou skartaci dokumentů[161], je nutné uvažovat i nad elektronickým košem. Umístění souborů do něj totiž neznamená smazání, což nemusí být méně počítačově gramotnému uživateli zřejmé. I po příkazu *odstranit z* koše je možné za určitých okolností obnovit data pomocí specializovaného softwaru[162], v případě klíčových informací je proto vhodné (i několikanásobné)

158 Overview [b.r.].

159 Směrnice Evropského parlamentu a Rady 2009/136/ES.

160 HUSSAIN 2012.

161 MITNICK 2003, s. 164–166.

162 Např. File Scavenger, Disk Checker, Recuva, GetDataBack, Pandora Recovery a mnohé další.

přepsání[163] nebo zformátování nosiče, na kterém byly uloženy, např. flash disku nebo harddisku prodávaného počítače.

Při správě počítače je možné využít nástroje, které usnadní odstranění digitálních stop bez jednotlivých manuálních příkazů. Obvykle se jedná o odstranění dočasných souborů, historie prohlížení a stahování, vyplněných formulářů, hesel a Cookies. K tomu lze využít produkty jako Ccleaner, Advanced Cleaner, Eusing Cleaner nebo BleachBit. Vzhledem k tomu, kolik problematických digitálních stop vzniká na sociálních sítích[164], je přínosný nástroj specializovaný právě na jejich odstranění. Příkladem je Web 2.0 Suicidal Machine, který ale tuto funkci plní jen pro Facebook, MySpace, Twitter a LinkedIn[165]. Pro splnění své funkce nezbytně vyžaduje zadání přístupových údajů do služeb pro úpravu v nich uložených digitálních stop, proto je vhodné před využitím ověřit, že heslo nebude diskreditováno s ohledem na využití v jiných prostředích.

Jak bylo řečeno, jmenované technické možnosti obvykle neřeší nevhodné chování uživatele a aktivní tvorbu digitálních stop. Přesto je možné využít několik technických pomůcek pro jejich nalezení a odstranění. Pokud digitální stopa vznikne, pro automatizaci a zjednodušení základního vyhledávání informací o vlastní osobě (viz kap. 1.3.3) lze použít tzv. alertů, které v pravidelných intervalech zadávají dotaz a nové výsledky zpřístupní uživateli, např. automaticky zasílaným e-mailem. Takto lze využít Me on the web, který je součástí Google Dashboard, nebo alternativy pro Yahoo! a Bing. Tyto nástroje lze samozřejmě zneužít při získávání digitálních stop jinou osobou, podobně je pro egosurfing možné využít postupy popsané u získávání digitálních stop (viz subkapitoly 1.2). Jinou kategorii zjištění existující digitální stopy zastupuje možnost stažení přehledu zpracovávaných dat z Facebooku (od roku 2010). Zásluhu o vznik této možnosti má iniciativa Europe vs. Facebook, jejíž zakladatel s využitím Směrnice Evropského parlamentu a Rady 95/46/ES prosadil, že mu navzdory neochotě byl Facebook nucen sdělit, jaké informace o něm shromažďuje[166]. Přesto existují dohady, že rozsáhlý seznam informací[167] neobsahuje všechny, které Facebook zpracovává[168].

Tento přehled různých směrů, ve kterých je možné aplikovat technická řešení pro zvýšení bezpečnosti uživatele, ukazuje, že možností je mnoho. Problémem u všech zůstává, že je možné je obejít, a pokud ne v daném okamžiku, tak při zvýšení výkonu počítače (např. problém délky hesla) nebo zjištění nečekaného

163 Např. pomocí softwarů FileShredder, Secure Eraser, Active@ KillDisk, FCleaner, O&O SafeErase a další.

164 MOORE 2012.

165 Web 2.0 suicide machine [b.r.].

166 SOLON 2012.

167 Viz Přístup k osobním údajům na Facebooku c2014.

168 Get your Data! [b.r.].

problému (např. tzv. *Zero day attack*). Obejít je se ale může pokusit také uživatel, kterého mají chránit, např. dostupné jsou návody na překonání blokování Facebooku ve škole[169]. I technická prevence, podobně jako právní, je tedy nutně spojena s osvětou, aby mohla být efektivní. Podle Herrington[170] je také osvěta přínosnější než přísná restrikce pomocí bezpečnostních nástrojů, které omezují svobodný přístup k informacím, včetně těch hodnotných.

1.3.3 Prevence chováním

Předchozí dvě kapitoly ukazují, že oba popsané typy bezpečnostních opatření mohou přinést výraznou pomoc v oblasti digitálních stop, ale současně mají svá omezení. Vzhledem k trendům vývoje internetu význam chování uživatele roste. Ukázkou je např. princip Webu 2.0, který staví na příspěvcích běžných uživatelů, tj. vytváření aktivních digitálních stop. Jiným souvisejícím trendem je rozšiřování personalizace služeb (viz kap. 1.2.2). Proto je vhodné uvažovat nad bezpečností na úrovni uživatele.

Odpovědné chování je klíčovým aspektem informační bezpečnosti, zejména při zaměření na informační soukromí a digitální stopy. Pokud si uživatel chce ponechat právo rozhodovat o svém informačním soukromí, měl by tomu přizpůsobit své chování při práci s IT. V případě zaměření na bezpečné informační chování jsou opatření méně závislá na konkrétním zařízení (např. využití počítače u kamaráda nebo v knihovně). Bezpečnost závisí především na znalostech, dovednostech, postojích a zkušenostech konkrétního uživatele. Technická řešení často slouží jako bariéra, kterou musí uživatel potvrdit svým jednáním, např. webový prohlížeč může zobrazit varování pro uživatele, že SSL/TLS certifikát je nedůvěryhodný, je ale na rozhodnutí uživatele, jak na toto varování bude reagovat. To vše podporuje význam bezpečného chování v elektronickém prostředí.

Základním krokem při odpovědném chování při práci s informacemi je důsledné zvažování důvěryhodnosti. To by mělo probíhat na úrovni zprostředkovatelů informací, jejich zdrojů i informací samotných. Jednotlivé postupy popsané v kap. 1.1.2 lze uplatnit pro hodnocení různých forem informací (text, video apod.). Například při hodnocení komunikace na sociální síti, která je zprostředkovatelem informací, lze zvažovat, jaké umožňuje nastavení soukromí a zabezpečení (např. jaké zabezpečení služba využívá pro ochranu proti narušení informačního systému). Uživatel služby, se kterým komunikujeme, je informační zdroj, u kterého zvažujeme, nakolik je známý a důvěryhodný. Následně je zhodnocena samotná

169 XNOTION 2010.

170 HERRINGTON 2010, s. 10.

informace, kterou sdílí. Při tom je možné využít podobné postupy, jako při hodnocení kvality argumentů.

Vzhledem k náročnosti postupu je evidentní, že mnohem více subjektů dokáže využít informaci o člověku zveřejněnou na sociální síti než například verzi jeho webového prohlížeče (viz kap. 1.2.3). Právě úroveň využití, resp. zneužití, by měla odpovídat tomu, jak je uživatel opatrný při sdílení konkrétní informace v elektronickém prostředí (nejen zveřejněním). Obecně lze konstatovat, že bezpečné chování stojí na zvažování možných pozitivních a negativních důsledků chování s tím, že výsledné jednání odpovídá převažující hodnotě. Pokud by totiž vytvoření stejné digitální stopy mělo mít za následek jen nevýznamný přínos pro uživatele, měl by od něj upustit. Naopak pokud je pro něj klíčový, měl by vědomě rozhodnout, že je ochotný přistoupit na riziko pro něj nepříjemného využití digitální stopy. Toto rozhodování staví na podobných principech jako risk management[171]. Často se uplatňují podobná bezpečnostní doporučení jako ve fyzickém prostředí, např. děti by se neměly bavit s cizími lidmi nebo si od nich brát sladkosti (lákavé výhody, např. ve stahovaném souboru nebo službě po registraci či jiném úkonu), protože v tom může být skrytý negativní zájem útočníka.

Pro konkrétnější vymezení vhodného chování je nutné uvažovat jak úroveň prevence vzniku digitální stopy, tak nakládání s již existující. První ze jmenovaných přístupů je podstatný proto, že již digitální stopa se může dostat mimo řízení uživatelem, o kterém vypovídá, například může být uložena na různých místech, o kterých neví[172]. Může se také objevovat opakovaně i po dlouhé době. I firmy specializované na odstranění digitálních stop garantují jen omezené vyřešení (např. firma ReputationDefender stanovuje tuto hodnotu na 80–90 %[173]). Na druhou stranu i při nejlepším chování může nastat problém tím, že informaci o subjektu údajů vytvoří někdo jiný. Je ale možné omezit potenciál využití digitální stopy tím, že je řešena alespoň ta, která je dobře dostupná a subjekt údajů o ní ví.

Prvním krokem by mělo být omezování sdělování kontaktních údajů. Ty patří mezi nejsnáze využitelné informace, mohou sloužit také pro propojování informací z různých zdrojů (viz kap. 1.2), protože bývají jedinečné. Takovou informací je např. e-mailová adresa, ale i fyzická adresa, nejen bydliště, ale také školy či zaměstnání. Vzhledem k rozšíření sociálních sítí, kdy pro identifikaci stačí jméno, příp. přezdívka, je i tento údaj samotný možné považovat za kontaktní. Přezdívka je také problematickou informací, protože si ji často člověk přenáší do různých služeb, proto opět dobře slouží k propojování různých informačních zdrojů. Vzhledem k možnosti kompromitace služby (nejen nechtěné využití po oprávněném

171 POŽÁR 2005, s. 42–43.

172 GRAYSON 2011, s. 8.

173 MARTÍNEZ-CABRERA 2010.

přístupu) je vhodné sdělovat co nejméně osobních informací, a to i v registračních formulářích.

Zvažovány by měly být samotné informace, ale také důvěryhodnost prostředí či subjektu, kterému jsou zpřístupňovány. Zejména v oblasti e-komerce je zásadní hodnocení důvěryhodnosti obchodního partnera, který může být podvržený, kdy usiluje o získání financí nebo informací od oběti. Nedůvěryhodný obchodní partner může poskytnout osobní informace třetí straně či s nimi sám nezachází eticky. Na úrovni e-shopů lze pro hodnocení důvěryhodnosti využít různých typů certifikátů, v českém prostředí především APEK[174]. V případě obchodní transakce typu Consumer-to-Consumer, např. v elektronické aukci, lze využít nastavených reputačních mechanismů prodejců a nakupujících[175].

Dalším typem bezpečného chování je budování pozitivní digitální stopy[176]. Není reálné nemít digitální stopu, spíše je otázkou, co vypovídá o člověku. Proto je dobré přemýšlet nad obsahem informace, než se z ní stane digitální stopa, ale také nad možným vlivem na člověka při jejím využití různými subjekty. Např. fotografie z oslavy může mít vliv ze strany přátel (pozitivní ukázka společenského charakteru a zábavy), tak i ze strany zaměstnavatele (pokud úroveň zábavy převyšuje úroveň, kterou považuje za vhodnou) nebo útočníka (možnost vydírání obsahem fotky nebo při fotomontáži).

Pro ochranu proti útokům, které začleňují sociální inženýrství (viz kap. 1.2.1), je vhodné ověřování oprávněnosti jakéhokoli požadavku na poskytnutí informace nebo vykonání činnosti (např. instalace softwaru), nejlépe ne elektronicky, aby nedošlo k využití podvrženého informačního zdroje. S tím také souvisí to, že by neměly být využívány odkazy ve zprávách, ale ověření přes oficiální kanály. Dále je vhodné navrhovat alternativní řešení, všímat si podrobností a usilovat o vedení rozhovoru tak, aby mohly být identifikovány nepřesnosti při komunikaci v oblasti, na kterou se sociotechnik nemohl dopředu připravit[177]. Protože sociální inženýrství často využívá nátlak přes emoce, je vhodné si toto uvědomovat a zpozornět v situacích, kdy by právě emoce mohly vést k rizikovému jednání.

Chování je vázáno také na vhodnou práci s bezpečnostními technickými opatřeními. Jejich funkce je informační, varovná, může se ale stát, že se jedná o falešně pozitivní oznámení, proto je rozhodnutí ponecháno uživateli. Navzdory nepohodlnosti je pro zvýšení bezpečnosti vhodné číst certifikáty, licenční podmínky, varování, potvrzení apod. Nicméně především licenční podmínky vzhledem k jejich délce slouží spíše pro právní ochranu poskytovatele služby než pro ochranu uživatele.

174 Certifikáty a ocenění e-shopů c2014.

175 Např. Aukro nápověda [b.r.].

176 GRAYSON 2011.

177 MITNICK 2003.

Je nutné poznamenat, že chování při nastavení softwaru a internetových služeb závisí i na úrovni porozumění, což je podle O'Neilla[178] důvod problému, že třetina uživatelů sociálních sítí neví, jak zde změnit nastavení soukromí. Na úrovni dospělých uživatelů se ukazuje, že od roku 2009 se zvyšuje aktivní úprava dostupnosti sledovaných digitálních stop (nejméně omezený přístup je u osob ve věku 18–29 let a nad 65 let, současně ale polovina z nich měla problémy při řízení nastavení soukromí)[179]. Po nastavení soukromí je nutné věnovat se udělování autorizace, typicky přidávání kontaktů (např. přátel na sociální síti Facebook).

Pro řešení rizikové situace v podobě nežádoucí digitální stopy je nutné nejdříve se o ní dozvědět, protože, jak již bylo opakovaně uvedeno, ne všechny digitální stopy o sobě člověk vytváří sám. Při zjišťování existence digitálních stop je nejsnazším postupem jejich vyhledání. Tento postup je označován jako egosurfing[180] a především v USA se jedná o často zmiňované bezpečnostní opatření[181]. Egosurfing by měl být prováděn pravidelně, a to ve vyhledávačích i v sociálních médiích. V případě zde existující nežádoucí stopy vytvořené někým jiným je na sociální síti jednodušší řešení, protože je možné požádat známého o odstranění daných informací. Pokud digitální stopu vytvořila třetí strana, ke které subjekt údajů nemá užší vztah, např. organizátor soutěže, které se zúčastnil, nebo firma, od které si něco koupil, je možné i ji požádat o smazání. Pokud není možné kontaktovat přímo osobu zodpovědnou za zveřejnění, např. v příspěvku v diskuzním fóru, lze využít oprávnění správce služby odstranit tuto informaci. V obou případech by mělo být požadavku vyhověno podle evropské a české legislativy (viz kap. 1.3.1). Z rozsudku Soudního dvora (velkého senátu) Evropské unie[182], vyplývá, že o smazání je možné požádat také internetový vyhledávač, který dané informace neobsahuje přímo, ale zobrazuje ve vyhledávání a umožňuje k nim přístup. Pak ale není smazána samotná digitální stopa, ale jen její záznam ve vyhledávači – stránka tedy není tímto nástrojem vyhledaná, ale informace je dál na této stránce dostupná. V případě, že digitální stopa vznikla působením subjektu, který má tuto činnost danou ze zákona, je nutné se s digitální stopou smířit a být si nadále vědom, že daná informace je veřejně dostupná (např. nevyužívat ji jako heslo).

Informační bezpečnost je vhodné podpořit všemi možnostmi, které se nabízejí. Měla by být propojena technická a právní opatření s vhodným informačním chováním. Každé bezpečnostní opatření je možné překonat, ale čím více bude bariér

178 O'NEILL 2012.

179 MADDEN 2012.

180 Egosurf © 2014.

181 Egosurfing někdy využito 47 % dospělých Američanů, z nich 25 % opakovaně. Viz MADDEN 2007, s. 7.

182 Rozsudek Soudního dvora (velkého senátu) ze 13. května 2014, spis. zn. C-131/12.

při útoku, tím je vyšší je pravděpodobnost, že některá útok zastaví nebo alespoň omezí.

Zásadním prvkem spojeným s každým z těchto přístupů k zvýšení bezpečnosti je vzdělání. Osvěta v informační bezpečnosti by měla zahrnovat nejen možná bezpečnostní opatření, ale i důvody jejich využití. Vedle řízeného vzdělávání by uživatelé měli znát kontaktní místa, která jim mohou pomoci s řešením konkrétních problémů. Jedním z těchto míst může být knihovna, jak ukazuje následující kapitola. Knihovník ale nemusí být nutně ten, kdo zná všechny odpovědi. Stačí, když bude důvěryhodným subjektem, který je schopný dohledat potřebné informace k tématu, příp. kontaktovat instituci, která se na dané téma specializuje. Vždy je nezbytné, aby knihovník byl pozorný posluchač a umožnil sdělení všech aspektů útoku, které mohou hrát roli při pochopení i řešení situace. Pokud je událost nepříjemná, není vhodné podporovat pocit sekundární viktimizace[183] projevy negativních emocí (např. *To je strašné!*), ale spíše usilovat o přesvědčení, že problém je řešitelný a měl by se řešit, ne přetrpět. K tomu jsou nutné důkazy a jednání s oprávněnými osobami, což jsou v případě dětí vždy rodiče. To může být pro dítě náročné, častá je obava ze zákazu dalšího použití internetu[184]. V případě překročení zákona při útoku může pomoci Policie. Pro podporu z psychologického hlediska i hledání řešení, ať už pro dítě nebo knihovníka či rodiče, mohou pomoci horké linky, kde působí pracovníci školení pro tyto případy.

183 Druhotné poškození řešením incidentu – VÁGNEROVÁ 1999, s. 393.

184 JUVONEN 2008.

2 KNIHOVNY JAKO SOUČÁST VZDĚLÁVACÍHO SYSTÉMU ČR

Právo na vzdělání je v ČR zaručeno ústavním pořádkem, konkrétně Listinou základních práv a svobod[185]. V souladu s Evropskou unií[186] je zajišťováno nejen formálním vzděláváním, ale i neformálním a informálním[187], protože jejich spojení usnadňuje zavádění celoživotního učení, které se v současné společnosti stává nezbytností.

Základem systému vzdělávání je školství, které představuje formální vzdělávání a spadá pod Ministerstvo školství, mládeže a tělovýchovy. Podporuje rozvoj na všech úrovních, kterými jsou: úroveň preprimární, primární a nižší sekundární, vyšší sekundární, postsekundární neterciární, terciární a další vzdělávání a odborná příprava[188]. Primární stupeň je povinný pro každé dítě ve stanoveném věku a seznamuje žáky s povinným minimálním standardem kompetencí. Od 1. 1. 2005[189] je obsahová náplň vymezena tzv. Rámcovým vzdělávacím programem[190], který definuje tematické okruhy a cílové znalosti, dovednosti a postoje (podrobněji k RVP v zaměření této publikace viz kap. 2.1.2). Stanovený rámec si každá škola specifikuje ve vlastním Školním vzdělávacím programu a dále jsou témata přizpůsobitelná každým učitelem s dodržením nadřazených dokumentů. Žáci tak mohou být seznámeni do určité míry s různým obsahem vzdělání.

185 Usnesení č. 2/1993 Sb., čl. 33.

186 Communication from the Commission of the European communities 2001.

187 Formy vzdělávání, jejich vztah a specifika jsou předmětem kap. 3.1.

188 Struktury systémů vzdělávání a odborné přípravy v Evropě 2009/10.

189 Dáno účinností zákona č. 561/2004 Sb.

190 Ty existují pro různé úrovně školství: RVP Předškolní vzdělávání, RVP Základní vzdělávání, RVP Základní vzdělávání – LMP, RVP Základní škola speciální, RVP Gymnázia, RVP Gymnázia se sportovní přípravou, RVP Odborné vzdělávání.

Před vstupem na pracovní trh připravuje na profesi počáteční vzdělávání. Mimo něj lze využít tří forem vzdělávání dospělých: všeobecného pro přípravu na studium na střední nebo vysoké škole, dalšího odborného vzdělávání a přípravy (doplnění kvalifikace, vč. v některých profesích požadované pravidelné aktualizace vědomostí) a *„občanského/zájmového vzdělávání (v naší zemi tradičního), které má obecně kultivační charakter a uspokojuje zájmy občanů"*[191]. Další vzdělávání mohou zajišťovat školy, orgány veřejné správy nebo vzdělávací instituce, nestátní neziskové i komerční organizace. Přestože knihovny spadají pod Ministerstvo kultury, jsou uznány jako instituce zajišťující významnou část zájmového vzdělávání s jasnou tradicí v tomto směru.[192] Vzhledem k tomu, že vzdělávání dospělých není předmětem této publikace, nebude mu dále věnována pozornost. Právě uvedené informace jsou ale klíčovým východiskem pro potenciál knihoven jako institucí vzdělávajících v informační bezpečnosti (viz kap. 2.3).

Krajské knihovny, příp. jimi pověřené knihovny, vykonávají pro základní knihovny v kraji tzv. regionální funkce, mezi které patří poradenství, vzdělávání a koordinace další činnosti pro rozvoj knihoven a jejich služeb. V metodickém pokynu Ministerstva kultury k zajištění výkonu regionálních funkcí knihoven a jejich koordinaci na území České republiky[193] jsou tyto činnosti dále rozvedeny. Přitom se předpokládají znalosti knihovníka mj. v oblasti výpočetní techniky a využívání informačních technologií, a to na úrovni ECDL. Mezi jeho základní moduly patří i bezpečné používání informačních technologií[194]. Bez ohledu na úroveň vzdělávání neškolské instituce zajišťují vzdělávání nejčastěji v oblasti výuky cizích jazyků, využívání počítačů, managementu a účetnictví[195]. Vzdělávání v knihovnách v informační bezpečnosti tedy může navázat na to, jak je distribuováno zaměření částí systému vzdělávání v České republice. Z hlediska formy vzdělávání mimo školské instituce je zdůrazňováno využití škály metod, *„[n]a významu nabývají interaktivní metody výuky: hraní rolí, simulace, případové studie, často z vlastní praxe frekventantů."*[196] Interakce je základem aktivního učení, které staví na konstruktivistických přístupech ve výuce, a je aplikována také jako výchozí přístup k navrženým lekcím v kap. 3.2.

Knihovní zákon nevymezuje předmět nebo formu vzdělávání v knihovnách, jen odůvodňuje jeho realizaci. Je ale logické, že knihovny vzdělávají v oblastech, kde mohou zajistit kvalitu, tedy primárně v práci s informacemi. Vedoucí knihovních a informačních služeb na All Hallows' School, Brisbane, dokonce vyjádřila přesvědčení, že *„dnes knihovny patří do oboru informací a, pokud chtějí přežít, komunika-*

191 Struktury systémů vzdělávání a odborné přípravy v Evropě 2009/10, s. 48.

192 Struktury systémů vzdělávání a odborné přípravy v Evropě 2009/10, s. 50.

193 Metodický pokyn Ministerstva kultury (...) 2011.

194 Sylaby a moduly [2014].

195 Struktury systémů vzdělávání a odborné přípravy v Evropě 2009/10, s. 53.

196 Struktury systémů vzdělávání a odborné přípravy v Evropě 2009/10, s. 54.

ce.“[197] To vychází z potřeb pro digitální občanství, v rámci kterého hraje informační bezpečnost zásadní roli, jak je patrné na jeho devíti složkách[198]. Které oblasti by knihovny měly rozvíjet, jsou proto předmětem strategických dokumentů na různých úrovních, které knihovnám ukazují preferované příležitosti vlastního rozvoje. V případě jejich využití si budují vlastní postavení[199] a oprávněnost existence, protože odpovídají na společenskou poptávku[200].

2.1 Vzdělávací politika a knihovny

Ze strategických dokumentů v oblasti vzdělávání, které vytvářejí státy i mezinárodní organizace, je patrný důraz na celoživotní vzdělávání formálně, neformálně a informálně ve spojení, a to už více než 15 let. Knihovny jako vzdělávací instituce obvykle nabízejí vzdělávací akce všem zájemcům na dobrovolné úrovni a uživatele vzdělávají bez udělení certifikátu, jako odpověď na jeho zájmy či potřeby v osobním rozvoji. Tato forma odpovídá typu vzdělávání označovanému jako neformální. S tím jsou sice spojeny limity využitelnosti, na druhou stranu může být efektivnější, protože reflektuje oblast, ve které je vzdělávaný motivovaný se rozvíjet[201]. Neformální učení lze definovat jako „*nezávislý učební proces, ke kterému dochází v rozdílných prostředích, ale je charakterizováno plánovanou povahou, má své vlastní cíle a je limitováno časem*“[202]. Oproti formálnímu typicky nevede k certifikaci. Za klíčové při prosazování neformálního vzdělávání lze považovat především snahy UNESCO[203] a Evropské komise[204]. Informální vzdělávání je také nezávislé a v různých prostředích, ale není organizované. Z toho důvodu mu dále není věnována pozornost, protože se objevuje neřízeně.

Propojení různých forem vzdělávání má přinést spojení jejich výhod s omezením limitů. To je ale možné jen v případě, že si jednotlivé strany budou důvěřovat a vzájemně se podporovat[205]. Toho lze dosáhnout kvalitou vzdělávání a komunikací klíčových osob, jejichž vzdělávací snahy se budou propojovat, budou respektovat práci ostatních, ne ji degradovat na nižší. Protože se jedná o systém založený na důvěře, spolupráce přestává být funkční, pokud se důvěra ukáže jako nepodlo-

197 WEAVER 2010, s. 24.

198 RIBBLE, M. Nine themes of digital citizenship. In: EKE 2012.

199 LEEDER 2014.

200 PINTO 2013.

201 STASIUNAITIENE 2009.

202 STASIUNAITIENE 2009.

203 DELORS 1996.

204 Communication from the Commission of the European communities 2001.

205 HARRIS 2012.

žená (např. kvůli nekvalitní výuce), pak je náročné získat ji zpět. Není možné, aby se spolupráce omezovala na tolerování se, je nutné najít vazby mezi formálním a neformálním vzděláváním, na což upozorňuje i Asociace evropských univerzit[206].

Přestože role neformálního vzdělávání je uznávána již dlouho, v praxi není dostatečně rozvíjeno. Stává se ale stále populárnějším vzhledem k rostoucí kritice současného formálního vzdělávání[207]. Právě neformálnost totiž umožňuje snazší reflektování proměn ve společnosti, a to jak na úrovni formy vzdělávání, tak i obsahu. Neformální vzdělávání je významné pro profesní rozvoj, ale často více pro rozvoj osobní a občanský. Dává prostor vzdělávat se v oblastech, které aktuálně člověk pociťuje jako potřebné. Neformální vzdělávání přitom dává jedinci větší prostor vytvořit si vlastní cestu k učení, která odpovídá právě jeho osobním potřebám[208]. Tento rozvoj se pak často neodráží v profesním uplatnění, jako spíše v sebevědomí jedince a spokojenosti se schopností udržet si svou roli ve společnosti[209].

Význam knihoven v neformálním vzdělávání je dán jeho vymezením odpovídajícím aktuálním činnostem a roli knihoven. Nedeklarují to jen samy instituce. Při výzkumu vzdělávaných, jaké preferují místo pro učení (bez ohledu na to, zda formální či neformální), se knihovny objevily na 5. místě, jako preferované je označilo 6,9 % respondentů[210]. Podpora vzdělávání v knihovnách pro potřeby informační společnosti má základ ve Státní informační politice[211] z roku 1999. Vzdělávání bylo prezentováno jako cesta ke konkurenceschopnosti Evropské unie, proto je na něj kladen důraz opakovaně až do současnosti, někdy s výslovným uvedením knihoven. Role knihoven pro omezení digitální propasti je spatřována jak na úrovni primární (dle knihovního zákona musí bezplatně umožnit přístup k počítači a internetu), tak sekundární (lekce a poradenství). V rámci spolupráce se školami se objevují knihovny i v aktuálních strategiích jako jeden z aktérů vzdělávání[212]. Informační bezpečnost se v koncepcích také objevuje od roku 1999[213] do současnosti[214], protože důvěryhodnost je chápána jako nezbytný předpoklad pro použití veškerých elektronických služeb od e-komerce po e-Government.

Samotné knihovny a organizace, které je sdružují, také vytvářejí strategické dokumenty zahrnující jak vzdělávání, tak i téma informační bezpečnosti. Zásadní postavení zde zaujímají koncepce rozvoje knihoven, vzhledem k jejich přípravě

206 BJØRNÅVOLD 2008.

207 TERESEVIČIENĖ 2008.

208 JANSSEN 2011.

209 TERESEVIČIENĖ 2008.

210 TUOMAITE 2008.

211 Státní informační politika 1999.

212 Dlouhodobý záměr vzdělávání a rozvoje vzdělávací soustavy ČR (2011-2015) 2011.

213 Státní informační politika 1999.

214 Strategie digitální gramotnosti ČR na období 2015 až 2020 2015.

knihovnami a následné podpoře státu schválením Vládou ČR. Již od roku 2004 se v koncepci[215] objevuje požadavek na vzdělávání uživatelů knihoven vzdělanými knihovníky, kdy mezi podpořená témata patří počítačová a informační gramotnost občanů a zmíněna je i podpora spolupráce knihoven a škol v oblasti informační gramotnosti. Následující koncepce pro období 2011–2015[216] pokračuje v podpoře jmenovaných témat a současně upozorňuje, že na vzdělávací akce navazuje činnost knihovny jako kontaktního a poradenského bodu pro uživatele při používání internetu. Vzdělávání a spolupráce se školami především na čtenářské a digitální gramotnosti jsou přeneseny i do aktuální koncepce[217].

České strategie reflektují místní specifika, ale navazují i na mezinárodní dokumenty knihovnických organizací, především IFLA, která vzdělávání věnuje výraznou pozornost již řadu let[218]. V dokumentech IFLA mají knihovny v oblasti informačních technologií pro společnost zásadní roli zajištěním infrastruktury, vzdělávání a poradenství (tedy zmírňování primární i sekundární digitální propasti). Podporují vzdělávání knihovníků i uživatelů knihovny, a to v informační i počítačové gramotnosti, včetně spolupráce se školami. Podle IFLA Trend Report[219] bude informační prostředí v nejbližších letech nejvíce ovlivněno pěti trendy, které jsou silně propojeny s důsledky využívání informačních technologií, přičemž první tři z nich úzce souvisí se vzděláváním v knihovnách v informační bezpečnosti:

- rozšiřování digitální propasti vlivem nových technologií,
- růst významu celoživotního učení, především pomocí neformálního a informálního vzdělávání,
- přehodnocení hranic soukromí, kdy lze očekávat vážné důsledky v oblasti důvěry především vlivem sofistikovaných metod práce s digitálními stopami uživatelů.

Jmenované oblasti nepodporuje jen IFLA, objevují se i v dalších knihovnických strategiích, např. The Public Library in the Electronic Word[220]. Vzdělávání o informační bezpečnosti tedy odpovídá doporučením pro vývoj knihoven v nezávislých strategických dokumentech.

Specifika neformálního vzdělávání a aktivního učení by měly knihovny využívat pro zvýšení efektivity svých lekcí i odlišení se od institucí neformálního vzdělávání, které nemusí každému vyhovovat. Knihovny mohou pro vzdělávání v relevantních tématech být alternativou, kde tradiční postupy nefungují. Knihovny by si měly být

215 Koncepce rozvoje knihoven v České republice na léta 2004–2010 2004.

216 Koncepce rozvoje knihoven ČR na léta 2011-2015 včetně internetizace knihoven 2012.

217 Implementace Koncepce rozvoje knihoven v ČR na léta 2017–2020 2016.

218 Např. IFLA/UNESCO Public Library Manifesto 1994; Manifest IFLA o přístupu k internetu 2002; The Role of Libraries in Lifelong Learning 2003; Manifest IFLA pro digitální knihovny 2010.

219 Riding the Waves or Caught in the Tide? 2013.

220 *PORS* [2002].

svého postavení ve vzdělávacím systému vědomy, protože jen tak budou plnit roli, která je jim stanovena, a nebudou jen omezenými možnostmi opakovat činnosti, které již zastává škola.

2.1.1 Informační gramotnost a bezpečnost

V rámci vzdělávání v českých knihovnách se lze setkat s pojmem informační vzdělávání, jeho výskyt v zahraničních odborných zdrojích je ale omezený. Ty operují spíše s pojmem informační gramotnost, kdy informační vzdělávání (v angličtině *information literacy education*) označuje organizovaný proces vzdělávání s cílem přiblížit se cílovému stavu, kterým je právě informační gramotnost. Tento pojem pak označuje komplexní schopnost efektivní práce s informacemi a technologiemi s nimi spojenými[221]. Toto široké vymezení bylo zvoleno vzhledem k tomu, že předmět informační gramotnosti se stále vyvíjí.

Extrémní názory řadí počátky vzdělávání k informační gramotnosti do poloviny 19. století[222], poprvé ale definoval informačně gramotné jedince až v roce 1974 Paul G. Zurkowski jako *„lidi vyškolené v používání informačních zdrojů pro svou práci“*[223]. Zvýšená dostupnost informací vedla k potřebě rozšířit tuto definici a v roce 1989 ALA představila vymezení, které je nejčastěji akceptované do současnosti: *„Aby byl informačně gramotný, člověk musí být schopný uvědomit si, kdy je informace potřebná, a mít schopnost najít, zhodnotit a použít efektivně potřebnou informaci.“*[224] Následovně je přitom uvedena potřeba začlenit takto pojímané gramotnosti do vzdělávacích programů ve školách. Vzhledem k tomu, že informační prostředí se rychle mění, ale definice je již téměř 20 let stará, objevují se její kritiky[225]. Pro jasnější vyjádření vztahu k informační bezpečnosti je nutné využít standardy informační gramotnosti. Následně budou popsány vybrané standardy splňující kritérium odlišnosti.

K primární cílové skupině této práce má nejblíže model Big6™[226], protože se zaměřuje na informační gramotnost od tzv. K12 po dospělé. Tento model je tradiční a odpovídá definici ALA, nezdůrazňuje proto specifická témata jako informační bezpečnost. Právě to bylo kritizováno a byl kladen důraz na to, aby nebyla opomíjena bezpečnost v kyberprostoru, v níž byla jmenována i ochrana soukromí a dat v elektronickém prostředí[227].

221 Toto široké pojetí pokrývá různé definice, několik tomu odpovídajících uvádí např. LLOYD 2010, s. 42.

222 COX 2008, s. 14.

223 ZURKOWSKI 1974, s. 6.

224 Presidential Committee on Information Literacy 1989.

225 Např. KOVÁŘOVÁ 2013.

226 Big6 Skills Overview c2013.

227 LI 2009, s. 573–574.

Standard Information Literacy Standards for Student Learning[228], který je také zaměřený na K12 a podpořila jej i ALA, se dělí se tři části, z čehož první tvoří jádro informační gramotnosti a další dvě (nezávislé učení a sociální odpovědnost) *„jsou zakotveny v informační gramotnosti, ale popisují obecnější aspekty učení studentů, ke kterému školní knihovní mediální programy také významně přispívají.*“[229] K informační bezpečnosti se vztahuje standard 2 (hodnocení informací kriticky a kompetentně), kde všechny jmenované indikátory odpovídají bezpečnému chování. Protože standard je již z roku 1998, neakcentuje příliš produkci informací, nicméně odpovědné vytváření informací lze zařadit do užití informací (standard 3), především indikátoru produkce a komunikování informací a myšlenek ve vhodných formátech. V rámci širších oblastí se nabízí sociální odpovědnost. Především standard 8, indikátor 3 odkazuje na odpovědné použití informačních technologií.

Jmenovaný model Big6™ i další se odkazují na standard ACRL, který je ale primárně určen pro vysokoškolské prostředí, jak jasně ukazuje jeho plný název Information Literacy Competency Standards for Higher Education[230]. Ten je členěn na pět standardů a dvacet dva indikátorů. Podobně jako u předchozího pojetí i zde je vztah k bezpečnosti zahrnut do kritického hodnocení zdrojů a informací (standard 3, konkrétně indikátory 2 a 5). Zásadnější je ale standard 5 (porozumění etickým, právním a sociálním otázkám použití informací a přístup a použití informací eticky a legálně) a všechny tři jeho indikátory, kde se objevují témata jako netiketa, soukromí, zabezpečení dat, bezpečná autentizace apod. Tento model byl ale již v roce 2015 nahrazen novějším (ale s předchozím kompatibilním) vymezením informační gramotnosti popsaném v dokumentu Framework for Information Literacy for Higher Education[231], kde vztah k informační bezpečnosti je možné najít ve všech šesti složkách.

V českém prostředí se prostřednictvím podpory komise IVIG projevuje vliv standardu CILIP[232]. Ten opět uvádí hodnocení důvěryhodnosti nalezených informací, etiku a odpovědnost při použití informací, komunikaci a sdílení nalezených informací, vč. porozumění výhodám a nevýhodám různých komunikačních kanálů. Na závěr standard uvádí i management nalezených informací, kdy mezi příklady je uvedeno také jejich zabezpečení.

Vlivem nových informačních technologií a zejména rozvojem Webu 2.0 se objevují otázky, zda i nově potřebné oblasti je možné pod definici začlenit. Nejedná se jen o oblast získávání, ale i evaluace a tvorby informací. Všechny tyto tři oblasti

228 Information literacy standards for student learning 1998.

229 Information literacy standards for student learning 1998, s. 1.

230 Information Literacy Competency Standards for Higher Education 2000.

231 Framework for Information Literacy (...) 2015.

232 Information literacy skills 2012.

považuje za rovnocenné aktuální pojetí mediální a informační gramotnosti[233], které podporuje také UNESCO a které je výchozí i pro tuto publikaci (viz kap. 1). Výhodou tohoto standardu je, že se neomezuje na konkrétní cílovou skupinu, ale akcentuje celoživotní učení. Kompetence, které vymezuje, by měly pomoci člověku v rámci jeho učení, profesního uplatnění i v osobních a občanských potřebách. V rámci všech dvanácti kompetencí můžeme najít určitý vztah k informační bezpečnosti, nejužší je ale spojení s následujícími[234]:

1. Získávání: (3) přístup k potřebnému mediálnímu obsahu účinně, efektivně a eticky, stejně jako k médiím a poskytovatelům informací.
2. Hodnocení: (6) vyhodnocení, analýza, srovnání, formulování a aplikace vstupních kritérií pro hodnocení získané informace a jejích zdrojů, stejně jako pro evaluaci médií a poskytovatelů informací ve společnosti; (7) evaluace a ověření shromážděných informací a mediálního obsahu a jejich zdrojů a médií a poskytovatelů informací ve společnosti.
3. Tvorba: (9) tvorba a produkce nové informace, mediálního obsahu nebo znalosti pro určitý účel inovativním, etickým a kreativním způsobem; (10) sdělování informací, mediálního obsahu a znalostí etickým, legálním a efektivním způsobem s použitím vhodných forem a nástrojů; (11) interakce s médii a poskytovateli informací pro sebevyjádření, mezikulturní dialog a demokratickou účast prostřednictvím různých prostředků etickým, efektivním a účinným způsobem.

Z tohoto přehledu přístupů, které jsou využity pro vymezení vzdělávání v informační gramotnosti v českých knihovnách, je patrné, že informační bezpečnost má místo v každém z nich. Zejména se jedná o úzce související kritické myšlení a evaluaci informací a zdrojů a právní a etické užití informací a zdrojů, včetně odpovědnosti za vlastní jednání v informačním prostředí. Těsnost spojení informační gramotnosti a informačních technologií je evidentní, nicméně otázkou zůstává, nakolik se překrývají. Někdy je počítačová a tím i internetová gramotnost vnímána jako složka informační gramotnosti[235], při tom ještě význam informační bezpečnosti vzrůstá. Pro tuto práci je podstatný především ISTE standard pro studenty[236], kde se v rámci digitálního občanství objevuje požadavek na praktikování bezpečného, legálního a odpovědného použití informací a technologií a na osobní zodpovědnost za celoživotní učení. Informační bezpečnost je také často zmiňována ve standardu FIT (Fluency with Information Technology)[237], na jehož vzniku

233 Global Media and Information Literacy (...) 2013.

234 Global Media and Information Literacy (...) 2013, s. 59.

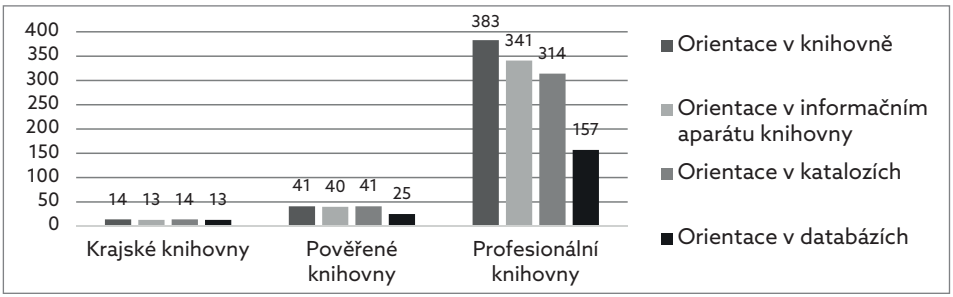
235 DOMBROVSKÁ 2004.

236 ISTE Standards c2007.

237 SNYDER c2011.

se podíleli experti na různé oblasti práce s informacemi a informačními technologiemi, včetně knihovníků.

I když teoreticky informační bezpečnost má své místo v informační gramotnosti, v rámci praxe v českých knihovnách téma příliš rozšířené není, jak ukazují výzkumy organizací, které se specializují na informační vzdělávání – IVU SDRUK (základní a krajské knihovny) a komise IVIG (vysokoškolské knihovny). Tato situace se ale rychle mění. Ve vysokoškolském prostředí[238] více než polovina respondentů (53,3 %) vykazuje existenci koordinátora informačního vzdělávání, čímž knihovny dávají najevo své přesvědčení o významu této služby. Podobná pozice ve veřejných knihovnách byla v rozhovorech deklarována jako nedostatečně uznaná a zavedená (viz kap. 3.3.4.2), což nepřímo vyplývá také z výzkumu IVU[239]. Dle výzkumu IVIG[240] je jasné zaměření lekcí v akademických knihovnách na tradiční služby knihovny a práci s informacemi (např. získávání informací a práce s literaturou), která není významněji ovlivněna aktuálním vývojem IT, včetně informační bezpečnosti. Obsahová náplň lekcí zjišťovaná IVU SDRUK není tak jasná, přesto i zde je možné spatřit vazbu na tradiční témata, jak ukazuje Graf 2. Základní a krajské knihovny se také musí vyrovnávat s tím, že knihovníci nemají povědomí o tom, co má být obsahem vzdělávání jednotlivých věkových skupin a jakými metodami má být výuka realizována[241]. Na druhou stranu je pozitivní, že si knihovníci tento stav uvědomují, stejně jako častou zastaralost výukových materiálů, díky čemuž také vykazují zájem o metodické materiály, které by jim pomohly tento nedostatek redukovat.



Graf 2 Obsah informačního vzdělávání v knihovnách[242]

238 LANDOVÁ 2010.

239 NEJEZCHLEBOVÁ, Jana. Veřejné knihovny 21. století a informační vzdělávání. In: KOVÁŘOVÁ 2012a, s. 42.

240 LANDOVÁ 2010.

241 NEJEZCHLEBOVÁ, Jana. Veřejné knihovny 21. století a informační vzdělávání. In: KOVÁŘOVÁ 2012a, s. 43.

242 NEJEZCHLEBOVÁ, Jana. Veřejné knihovny 21. století a informační vzdělávání. In: KOVÁŘOVÁ 2012a, s. 45.

Pro zlepšování informační gramotnosti je nutné *„zabývat se všemi třemi složkami této problematiky: tedy samotným definováním toho (nebo shody o tom), co je informační gramotnost, dále pak vytvořením standardů informační gramotnosti (na různých úrovních) a nakonec problematikou informačního vzdělávání samotného, tedy onoho 'jak učit' informační gramotnost, nebo přesněji přispívat k jejímu rozvoji.*"[243] Jelikož první dvě složky je možné navázat na již existující odborné zdroje, je cílem této publikace poslední uvedený krok, tedy koncepce stanovující jak učit v knihovnách o informační bezpečnosti se zaměřením na děti na základních školách.

2.1.2 Standardizace českého vzdělávání na ZŠ a informační bezpečnost

Základním dokumentem, který standardizuje obsah i způsob vzdělávání na základních školách, je Rámcový vzdělávací program pro základní vzdělávání[244] (dále jen RVP ZV). Vzhledem k cíli této publikace je možné v RVP ZV identifikovat řadu témat, která jsou spojená s informační bezpečností a která jsou také pokryta v navrhované koncepci (viz kap. 3.2). Tato vazba nabízí argument pro knihovny, proč by lekce mohly být využity jako alternativní forma vzdělávání v tématech, které je škola povinna žáky učit, tedy oprávněně věnovat učební čas návštěvě lekce. Vzhledem k tomu, že RVP ZV definuje témata poměrně široce a ukotvuje je časově na první nebo druhý stupeň vzdělávání, je při argumentaci pro konkrétní instituce nutné reflektovat zařazení a pojetí témat v konkrétní škole, která upřesňuje RVP ZV ve svém Školním vzdělávacím programu (ŠVP). Při specifikaci témat je možné vyjít také z vymezení klíčových gramotností dle doporučení Evropského parlamentu a Rady o klíčových schopnostech pro celoživotní vzdělávání, které specifikují metodiky NIQUES (viz níže).

Vzhledem k tomu, že témata z různých částí RVP ZV je možné integrovat, a to i v základních vzdělávacích oblastech, častěji pokud se jedná o průřezová témata, není využito obsahové klasifikace RVP ZV, ale spíše tematických okruhů, které byly vymezeny v souladu se standardem mediální a informační gramotnosti. Byly identifikovány dva základní tematické okruhy, kdy první se zaměřuje na získávání a hodnocení informací, především s ohledem na autorství (první dvě komponenty standardu mediální a informační gramotnosti, z hlediska bezpečnosti viz kap. 1.1), druhý cílí na bezpečnost digitálních stop se zaměřením na odpovědnou komunikaci na internetu (třetí komponenta standardu mediální a informační gramotnosti, viz kap. 3.3.4.2). V navržené koncepci se oba okruhy střídají pro průběžný rozvoj ve všech definovaných tématech. V rámci každého okruhu jsou specifikovány dotčené části RVP ZV i NIQUES (spojení s oběma standardy jsou dále upřesněna u jednotlivých lekcí v kap. 3.2).

243 DOMBROVSKÁ 2004.

244 Příloha č. 1 (...) 2015.

1. Bezpečnost při získávání a hodnocení informací

Problémy při získávání informací spočívají zejména v nedodržování autorských práv a etiky, k čemuž patří i využívání manipulativních technik. Neetická komunikace, byť pro získání informací, je v podstatě rizikovou komunikací, proto je zařazena do druhého tematického okruhu. Hodnocení informací je klíčové pro jejich správné pochopení a také využití, což se objevuje v metodikách NIQUES pro hodnocení informační[245] a také čtenářské gramotnosti[246]. Konkrétní části RVP ZV a medotik NIQUES na řešenou problematiku v tomto i následujícím tematickém okruhu specifikuje příloha 3.1.

2. Digitální stopy a riziková komunikace

Další tematický okruh lekcí se zaměřuje na rizikovou komunikaci a hrozby, které na ni mohou navazovat. Toto téma je podstatou nejvíce diskutovaných oblastí informační bezpečnosti se zaměřením na děti, navazuje ale na předchozí okruh (útoky často zneužívají nesprávného hodnocení informací a jejich zdrojů). Jeho podstatou není tolik technický pohled na IT, jako spíše způsoby jejich využívání s ohledem na bezpečnost.

V rámci témat informační gramotnosti metodika NIQUES[247] upozorňuje, že RVP ZV je nutné revidovat, protože v současnosti vzdělávací systém nepokrývá problematiku vhodně, což je patrné také z rozdílů v tématech, které oba materiály uvádějí. Rozdíly lze najít také v tom, na výstupy kterých stupňů jsou některá témata zařazena (např. hodnocení informací je v RVP až na 2. stupni, zatímco NIQUES tuto činnost řadí jako vhodný výstup již na 1. stupeň). Problém je také s nedostatečným vzděláváním učitelů pro výuku těchto témat, která by měla být provázána se všemi vzdělávacími oblastmi. Nedostatky na straně učitelů by měly být podpořeny rozsáhlejší nabídkou metodické podpory v informační gramotnosti. Tyto nedostatky podporují vznik a využití předkládané koncepce.

Celou navrženou koncepcí prostupují dva aspekty, které navazují na cíle a způsoby základního vzdělávání a ukotvení témat do prostředí internetu s tím, že, kde je to možné, je poukázáno na srovnání s tradičními informacemi a jejich zdroji. Specifika práce s elektronickými informacemi a informačními technologiemi tvoří rámec, který je v RVP ZV akcentovaný, ale z pohledu informační gramotnosti spíše podřadný. Elektronické informace mají svá specifika, pro děti a dospívající představují častější prostředí práce s informacemi než tradiční zdroje, ale současná vymezení informační gramotnosti je neoddělují, spíše je srovnávají. V pojetí této publikace jsou zahrnuty činnosti spočívající ve znalostech a dovednostech práce s hardwarem a softwarem, které prostupují všemi navrženými lekcemi. Toto

245 Metodika pro hodnocení rozvoje informační gramotnosti 2015.

246 Metodika pro hodnocení rozvoje čtenářské gramotnosti 2015.

247 Metodika pro hodnocení rozvoje informační gramotnosti 2015, s. 5.

pojetí IT jako předpokladu řešení informační gramotnosti odpovídá i metodice NIQUES[248].

RVP ZV akcentuje mimo jiné klíčové kompetence, v rámci metodiky NIQUES se jedná především o sociální gramotnost[249]. Tyto kompetence, především kvůli zaměření na postojovou rovinu, jsou rozvíjeny tak, že lekce staví na kooperativním (rozvíjejícím spolupráci, komunikaci a prezentaci) a aktivním učení (rozvíjejícím kritické myšlení, spojení s reálným životem a kreativní činnost všech jedinců ve třídě)[250], které tvoří druhou průřezovou charakteristiku navržených lekcí. V rámci spojení s RVP ZV pokrývají tuto charakteristiku především klíčové kompetence (komunikativní, sociální a personální a občanské) a v návaznosti na ně některé výstupy vzdělávacích oblastí a průřezových témat:

- Jazyk a jazyková komunikace – Komunikační a slohová výchova: ČJL-3-1-07 a 11 (1. období 1. stupeň), ČJL-5-1-04 a 10 (2. období 1. stupeň), ČJL-9-1-07 a 08 (2. stupeň),
- Člověk a jeho svět – Lidé kolem nás: ČJS-5-2-01 až 04 (2. období 1. stupeň),
- Člověk a společnost – Výchova k občanství: VO-9-1-08 (2. stupeň),
- Osobnostní a sociální výchova – sebepoznání a sebepojetí, seberegulace a sebeorganizace, kreativita, poznávání lidí, mezilidské vztahy, komunikace, kooperace a kompetice, řešení problémů a rozhodovací dovednosti a hodnoty, postoje, praktická etika,
- Multikulturní výchova – lidské vztahy.

2.1.3 Zprostředkovatelé poznatků o informační bezpečnosti pro děti

Děti se setkávají s problémy často důsledkem vlastního rizikového chování (viz kap. 1.2.3). S ohledem na omezenou možnost použití a snadnost obcházení bezpečnostních opatření proti internetovým útokům v podobě legislativy a technických řešení se jako stěžejní ukazuje osvěta pro zvýšení internetové bezpečnosti[251]. Zejména sociálním problémům, např. kyberšikaně, lze předcházet především bezpečným chováním. Předpokladem je znalost vhodných modelů chování, jejichž využití je podmíněno uvědoměním si možných důsledků. Podstatná je tedy znalost internetových hrozeb i možných protiopatření.

Mezi státy jsou silné rozdíly ve vzdělávání o internetové bezpečnosti[252]. Jedná se o poměrně nové téma a státy teprve hledají způsob jeho zařazení do vzdělávání.

248 Metodika pro hodnocení rozvoje informační gramotnosti 2015.

249 Metodika pro hodnocení rozvoje sociální gramotnosti 2015.

250 Aktivní učení je doporučeno také metodikou NIQUES zaměřenou na informační gramotnost, viz Příloha č. 5 Soubor indikátorů dosažné úrovně informační gramotnosti 2015.

251 RANGUELOV 2010; LIVINGSTONE 2009; MARTIN 2012; KOPECKÝ 2012.

252 RANGUELOV 2010.

Ze šesti nejčastěji řešených témat je pět rizikovou komunikací či jejím důsledkem (od nejčastějšího: bezpečné chování online, otázky soukromí, kontakt s cizími lidmi, kyberšikana, bezpečné použití mobilních telefonů). Každý stát má odlišný přístup ke stanovování způsobu a povinností pokrytí tématu ve vzdělávání. V České republice je formální školství postaveno na RVP, které dávají velkou volnost v pojetí internetové bezpečnosti. Toto nedostatečné ukotvení akcentuje i Kopecký a kol.[253], východisko vidí v kombinaci přímé edukace, mediálních kampaní a pozitivních vzorců chování rodičů, učitelů a vrstevníků. Ranguelov[254] upozorňuje, že celou výuku třídy na 1. stupni zajišťuje jeden učitel, je tedy pravděpodobné, že se nejedná o odborníka na IT (to se potvrdilo na škole v případové studii, viz kap. 3.3.4.3). Na vyšších stupních je již IT specialista obvyklý, je ale stále otázkou jeho erudovanost v internetové bezpečnosti. Vedle toho existují nabídky neformálního vzdělávání, a to ve spolupráci se školami či zcela mimo ně. Je tedy pravděpodobné, že různé lokality v ČR se budou v tomto směru lišit, neexistuje ale výzkum, který by rozdíly zmapoval.

Výzkumy vzdělávání o bezpečnosti na internetu se často zaměřují na formální vzdělávání, i v nich se ale objevují instituce neformálního vzdělávání včetně knihoven[255]. Hlubší pozornost jim však není věnována. Problém zkoumání jejich postavení ve vzdělávání o internetové bezpečnosti je spojen s omezeními kvantitativních výzkumů, pokud totiž jejich činnost není součástí zkoumaných variant, jejich aktivita se do výsledků nemůže dostat. To je možná důvodem, proč lekce internetové bezpečnosti v českých knihovnách nezmiňuje Ranguelov[256], přestože se v době sběru dat pro jeho šetření (2008/2009) realizovaly. Mimo dílčí lekce byly knihovny zapojeny do mezinárodního Dne bezpečnějšího internetu (viz kap. 2.1.4). Tuto akci Ranguelov[257] zdůrazňuje jako možnost spolupráce institucí na osvětě v internetové bezpečnosti. Neodmítá ani knihovny, jak je patrné na jeho popisu situace v Řecku.

Knihovny díky spolupráci s více školami v okolí mohou pokrýt poměrně rozsáhlou skupinu dětí. Právě šířku pokrytí osvěty zdůrazňují Moreno a kol.[258], měla by ale být spojena se zkušenostmi ve výuce o internetu a příbuzných tématech. Přestože knihovníci nemají akreditované pedagogické vzdělání, toto téma se v ČR dostává do jejich odborné přípravy (vyučuje se např. od jara 2014 na Kabinetu informačních studií a knihovnictví Masarykovy univerzity), jsou nabízeny kurzy dalšího vzdělávání pro knihovníky a zkušenosti získávají často z praxe.

253 KOPECKÝ 2012.

254 RANGUELOV 2010.

255 RANGUELOV 2010; MARTIN 2012.

256 RANGUELOV 2010.

257 RANGUELOV 2010.

258 MORENO 2013.

Martin a Rice[259] knihovny zahrnují jako jednu ze vzdělávacích institucí spolupracujících se školou, příp. jako její součást u školních knihoven (ty mají v ČR jiné postavení než v angloamerickém prostředí, kde vykonávají některé činnosti jako veřejné knihovny v ČR). V tomto pojetí je celá skupina pracovníků ve vzdělávání (ředitelé, učitelé, knihovníci) považována za klíčovou pro zvýšení internetové bezpečnosti dětí. Podle 47 % respondentů musí spolupracovat s rodiči pro zajištění adekvátní bezpečnosti dětí.

Výzkumy se shodují na zásadním postavení rodičů, ať už se zaměřují na názory rodičů, dětí či učitelů. Podle Moreno a kol.[260], zkoumající všechny tyto tři skupiny a klinické lékaře, 40,3 % respondentů uvádí, že o internetové bezpečnosti by měli pravidelně své děti učit rodiče, ti jsou za to primárně zodpovědní, jen podle 20,8 % by to měli dělat učitelé. I zde je z demografických dat patrné, že mezi učitele jsou řazeni také knihovníci. Na druhou stranu při dotazování dospívajících, od koho se dozvídali o problematice, jsou na prvním místě učitelé (87,5 %), následovaní rodiči (75 %). Fungování rodičů jako zdrojů osvěty je tedy v praxi méně časté, což je podle Moreno a kol.[261] ovlivněno nedostatečnými zkušenostmi rodičů v této oblasti, především ve srovnání s *digital natives*[262]. Rodiče by ale většina učitelů a klinických lékařů chtěla doplňovat a také by podle Moreno a kol.[263] měla, a to kooperativním způsobem.

Kromě omezení rodičů v jejich zkušenostech s internetovou bezpečností je limitem při vzdělávání přesvědčení, že se problém jejich dětí netýká. Liší se ale názory rodičů a dětské zkušenosti s problémem (vidění či přijmutí obrázků se sexuálním obsahem, přijímání sprostých či zraňujících zpráv přes internet a setkání off-line s člověkem známým jen z internetu)[264]. Přesto se podle stejného šetření většina rodičů snaží aplikovat různé mediační strategie[265] pro zvýšení bezpečnosti dětí na internetu. Přístup rodičů ale nestačí pro řešení bezpečnosti dětí, protože 37 % dětí rodiče ignoruje (málo nebo hodně), ČR je v tomto s 54 % dětí na prvním místě[266]. Postavení rodičů jako zdrojů osvěty oslabuje také to, že 50 % z nich nesleduje u dětí dodržování pravidel pro ochranu soukromí na sociálních sítích[267]. To formuje nezanedbatelnou skupinu, pro kterou je nutné hledat jiné formy osvě-

259 MARTIN 2012.

260 MORENO 2013.

261 MORENO 2013.

262 Lidé narození do prostředí, kde již byly informační technologie běžnou součástí života, aktuálně od malých dětí po vysokoškolské studenty – viz PRENSKY 2001.

263 MORENO 2013.

264 LIVINGSTONE 2011.

265 Podrobněji viz kap. 1.3.

266 LIVINGSTONE 2011.

267 Polovina dětí reaguje na internetu (...) 2010.

ty. Současně nejde jen o to, aby byly děti a dospívající vzděláváni o internetové bezpečnosti, klíčové je zahrnout zásadní subtémata, včetně budování digitální stopy, důsledků zveřejňování konkrétních informací a řízení soukromí (*privacy management*)[268]. Toto potvrdili i Weeden a kol.[269]

Mezi informačními zdroji o online bezpečnosti pro děti Livingstone a kol.[270] identifikovali vedle rodičů (63 %), učitelů (58 %) a vrstevníků (44 %) další, mezi nimiž je na pátém místě knihovna. Význam roste s ochotou těchto institucí zapojovat se do celoživotního vzdělávání. Zájem vzdělávat místní komunitu o internetové bezpečnosti se neřeší jen v České republice, podobné iniciativy je možné sledovat i v řadě dalších států, nejvíce zřejmě v USA[271]. Zájem je naopak problematický, když je role v celoživotním vzdělávání přisuzována českým školám, jak zjistily Rabušicová a kol.[272]

Přestože existují výzkumy názorů, kdo by měl vzdělávat děti o internetové bezpečnosti, i nabídky, „*několik organizací, včetně AAP [American Academy of Pediatrics], nabízelo odborné poradenství týkající se bezpečnosti na internetu, ale přístup založený na důkazech vzdělávat mládež o nebezpečí bytí online, v současné době neexistuje.*“[273] V České republice lze zmínit edukaci programem e-Bezpečí, který pro osvětu využívá rozbory kazuistik z ČR i zahraničí[274].

2.1.4 Inspirace pro lekce informační bezpečnosti v knihovnách

Reálnost řešení tématu podporují existující snahy zahraničních i českých knihovníků zavést jej do svých vzdělávacích akcí. V českém prostředí je obvykle řešena obecně informační bezpečnost, někdy ještě jako dílčí téma práce s internetem nebo počítačem. V anglicky mluvících oblastech existuje výrazně více lekcí zaměřených na informační bezpečnost jako součást digitálního občanství.

Iniciativa Common Sense Media[275] nabízí mnoho lekcí k informační bezpečnosti, a to od stupně K2 (přibližně 6–7 let dítěte) po K12 (17–18 let), včetně lekcí pro knihovny. Na ni se s pozitivními zkušenostmi odkazují mnohé knihovny, např.

268 WALRAVE 2012.

269 WEEDEN 2013.

270 LIVINGSTONE 2011, s. 127.

271 MARCOUX 2010.

272 RABUŠICOVÁ 2004.

273 MORENO 2013.

274 KOPECKÝ 2012.

275 Scope & Sequence 2012.

na blozích pro sdílení zkušeností[276], umírněnější, ale jasné ukázky využití těchto lekcí ukazují i webové stránky škol a školních knihoven[277]. Nejedná se ale o jediný vyskytující se přístup, knihovnice na Hong Kong International School uvádí pozitivní zkušenost[278] s lekcí založenou na aktivním učení, kdy studenti vyhledávají na internetu dostupné informace o třech zadaných osobách a následně diskutují o nalezených informacích z hlediska bezpečnosti digitálních stop[279]. Z přehledu je také patrné, že se jedná především o oblast USA, lekce lze ale najít třeba i v Austrálii[280].

V případě koncepčního pojetí (opět především USA)[281] je odkazováno i na mnohé další zdroje lekcí, které jsou volně dostupné a týkají se informační bezpečnosti. Koncepční pojetí odpovídá doporučenému přístupu pro školní knihovny, podle kterého by měl každý ročník (K1 až K12) zvyšovat znalosti v oblasti odpovědnosti a bezpečnosti v digitálním prostředí, kdy digitální stopy představují jedno ze tří vyzdvižených témat[282]. Lekce o bezpečnosti digitálních stop se objevují také v Evropě ve vysokoškolském prostředí. Obojí reprezentuje lekce *Who am I? My digital footprint*, která vznikla v Birkbeck Library v programu Informační a digitální gramotnosti[283].

Jak bylo popsáno v kap. 2.1.1, informační bezpečnost je úzce spojena s řadou kompetencí zařazených do standardu mediální a informační gramotnosti. Vzhledem k tomu, že se jedná o poměrně nový standard, ale se silnou podporou, pro plánování lekcí je možné využít volně dostupnou knihu *Media and information literacy curriculum for teachers*[284], která vedle představení kurikulárního rámce a významu lekcí mediální a informační gramotnosti přináší i bohatou nabídku výukových aktivit. Ty jsou uspořádány do jádrových a doplňkových témat, v rámci obou jsou pak definovány tematické okruhy, v nich klíčová témata, výukové cíle, stručné vymezení řešené problematiky, tipy na aktivity, doporučení pro hodnocení a další témata ke zvážení. Výukové aktivity sice nejsou popsány podrobně (např. včetně pracovních listů, konkrétních textů apod.), jsou ale dostatečně přesné, aby sloužily jako opora pro tvorbu lekcí.

Situace v ČR je odlišná. Knihovny téma neignorují, často jej ale řeší spíše informativně, tedy v podobě tipů pro bezpečné používání internetu, které jsou do-

276 HEMBREE 2013 (zde problematika prezentována jako součást standardu ISTE – viz kap. 2.1.1); In the fishbowl 2013; MORRIS 2013; SWETNAM 2013; LIBRARIANTIFF 2014.

277 Digital Footprint 2014; Davis Elementary Internet Safety Month Lesson Plans © 2002–2014.

278 What is a digital footprint? c2010.

279 FISHER 2010.

280 STOWER 2013; REID 2014.

281 SULLIVAN 2011; Library lessons calendar c2002–2014.

282 Citizenship in the Digital Age 2012, s. 2.

283 ZAZANI 2013.

284 WILSON 2011.

stupné na webu v různých sekcích, např. počítačové učebny Městské knihovny Litvínov[285] nebo dětského oddělení Městské knihovny Pelhřimov[286]. Knihovny se také zapojují do širších organizovaných snah upozornit na problematiku bezpečného internetu především v rámci Dne bezpečnějšího internetu (roce 2017 patřily knihovny mezi nejčastější zapojené organizace[287]). Knihovny se do této akce zapojují již několik let, lze najít doklady propagace tématu bezpečnosti dětí na internetu už z prvního ročníku tohoto projektu[288].

Osvětu knihovny ne vždy řeší vlastními silami, někdy jen nabízí prostředí pro realizaci vzdělávací akce, často přednášky, příp. besedy vedené zástupci policie[289]. Externistou vedené přednášky si často zajišťují školy samy[290]. Obě tato zastoupení mají své limity (viz kap. 2.3).

Je ale nutné podotknout, že existují školy, kde téma zajišťuje pracovník školní knihovny, resp. informačního centra[291]. Jindy je možné setkat se s názorem vedení školy, že téma informační bezpečnosti patří knihovně a škola s ní má na tomto zájem spolupracovat[292]. Nicméně názor knihoven je odlišný: „*To téma je pro nás zajímavé a má velkou důležitost, ale myslím, že školám se dostává takovýchto přednášek hodně právě od specializovaných institucí a neziskovek, které se rizikovými tématy zabývají prioritně.*“[293]

Problematika je již zahrnována do vzdělávací nabídky knihoven, především lekcí nabízených školám. Jen minimálně jsou zastoupeny přednášky, např. v již uvedené Městské knihovně ve Svitavách, nebo lekce pro dospělé, např. jako dílčí téma kurzu Základy ovládání PC v Městské knihovně Přerov, který probíhal šest týdnů od poloviny února do konce března 2014[294]. Na jiné úrovni jsou pak vzdělávací akce ve vysokoškolském prostředí, kdy lze najít zcela ojediněle zaměření i na digitální stopy[295].

V oblasti spolupráce se školami převažují lekce zaměřené na problematiku kyberšikany a kybergroomingu, takové vzdělávací akce již nabízely především

285 PC učebna 2013.

286 Dětské oddělení [b.r.].

287 Zapojené organizace 2017.

288 Březen měsíc Internetu 2008 2008.

289 Např. CHRÁSTKOVÁ KNÍŘOVÁ 2013; BAUEROVÁ 2014.

290 Např. Plán ZŠ Aloisina výšina na měsíc říjen 2012 2012 (přestože tato škola uskutečňuje jiné vzdělávací akce i v knihovně); Akce – kyberšikana 2014; Preventivní programy c2014 (škola si pozvala lektora z občanského sdružení z téměř 30 km vzdálených Letovic).

291 Např. RÁBLOVÁ 2014.

292 Vedle totožného názoru v kap. 3.2.9 byl vyjádřen také na semináři IVU 2014 – viz ZAŤKO 2014.

293 E-mailová komunikace s Marikou Zadembskou (Městská knihovna Třinec) ze dne 16. 7. 2014.

294 Městská knihovna Přerov – březen 2014 2014.

295 Přednáškový blok 2014.

městské knihovny[296]. Někdy se lze setkat i s širším pojetím[297]. Často se nejedná o lekce využívající možností neformálního vzdělávání (viz kap. 2.1), ale spíše jen besedy. Oproti zahraničnímu pojetí informační bezpečnost nepředstavuje téma, které by bylo řešeno jako podstatné. Podle názoru Aleny Srovnalové z Městské knihovny Rožnov pod Radhoštěm se i toto bude měnit[298].

2.2 Vzdělávání v knihovnách v informační bezpečnosti

Kvantitativní mapování činnosti knihoven je realizováno pomocí každoročních statistických výkazů, které knihovny odevzdávají Ministerstvu kultury[299]. Následně jsou data zpracována Národním informačním a poradenským střediskem pro kulturu (NIPOS). Hustota knihovní sítě je v České republice nesrovnatelně vyšší, než představuje evropský průměr – v roce 2011 na 10 000 obyvatel připadalo v ČR 5,1 knihoven, zatímco v EU 1,3[300]. Široká síť knihoven je tvořena především těmi neprofesionálními, jejichž vybavení a služby jsou výrazně horší než u těch profesionálních[301]. Velikost instituce je nepřímo úměrná jejich počtu, ale přímo úměrná množství vybavení a služeb, včetně vzdělávacích (viz Tabulka 2).

Tabulka 2 Vybavení a služby podle typu knihovny v roce 2016 [302]
(průměry na knihovnu za rok)

	NK	MZK	Krajské	Základní s reg. funkcí	Další zákl. profes.	Další zákl. neprofes.
Počet knihoven	1	1	13	85	700	4 552
PC pro uživatele s internetem	29	91	730 (⌀ 56)	1 639 (⌀ 19)	2 736 (⌀ 4)	5 227 (⌀ 1)
Návštěvníci na internetu	260 480	214 499	377 666 (⌀ 29 051)	577 470 (⌀ 6 794)	656 334 (⌀ 938)	145 203 (⌀ 32)
Lekce pro veřejnost	78	27	5 815 (⌀ 447)	18 261 (⌀ 215)	15 518 (⌀ 22)	2 457 (⌀ 0,5)
Návštěvníci vzdělávání	11 692	753	147 082 (⌀ 11 314)	352 898 (⌀ 4 152)	337 984 (⌀ 483)	45 513 (⌀ 10)

296 Např.: Nabídka knihovnických lekcí a besed na školní rok 2012–2013 2012; Na internetu bezpečně 2014; Nástrahy v online světě 2014; PINTÉR 2014.

297 Např. ZVONKOVÁ 2009; OGROCKÁ 2013; Barevný svět poznání 2014; Nabídka pro školy [2014]; Nabídka tematických besed pro školy (...) c2009 – 2014; Nabídka vzdělávání pro střední školy a gymnázia [2014]; Školy [2014]; ZADEMBSKÁ 2014.

298 E-mailová komunikace s Alenou Srovnalovou ze dne 18. 6. 2014.

299 Statistika kultury c2007.

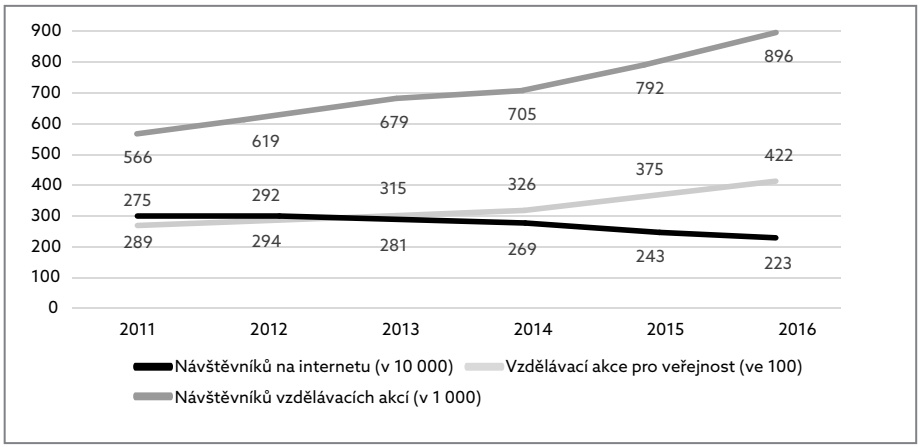
300 QUICK 2013, s. 8.

301 NIPOS za neprofesionální označuje ty, kde knihovníci vykonávají svou činnost jako dobrovolníci.

302 Dle Základní statistické údaje o kultuře (...) 2017.

Knihovny poskytují nezanedbatelnému množství lidí přístup k internetu. Proti evropskému prostředí, kde uživatele motivuje k využití služby její bezplatnost a absence jiných možností, v ČR jsou jako důvod uváděny spíše poradenství zaměstnanců a pomoc od jiných uživatelů[303]. Vzhledem k tomu, že uživatelé v tomto případě neřeší technické zabezpečení (to je záležitostí knihovny), jsou problémy spojeny právě s jejich chováním na internetu. Z těch, kdo využili internet v knihovně, to 35 % udělalo pro aktivity spojené se zaměstnáním a 23 % ke komunikaci s veřejnou správou (17 % získání informací z internetových stránek, 9 % stahování úředních formulářů a 9 % množství odeslání vyplněných formulářů)[304]. Vzhledem k významu těchto činností je nezbytné, aby byla zajištěna jejich bezpečnost.

Motivace uživatelů internetu odpovídá i vývoji dle NIPOS, podle kterého roste nabídka vzdělávání v knihovnách i zájem o ni, naopak ubývá využívanosti internetu (viz Graf 3 Vývoj využití internetu a vzdělávacích akcí v knihovnách). ČR s 34 % uživatelů knihoven, kteří se zúčastnili vzdělávací akce v knihovně, převyšuje evropský průměr (25 % uživatelů)[305]. Tyto výsledky je vhodné reflektovat nejen navýšením akcí stejného typu, ale je zde prostor i pro nová témata odpovídající současným potřebám uživatelů. Lze tedy konstatovat, že existují podmínky pro zavedení či rozšíření lekcí informační bezpečnosti.



Graf 3 Vývoj využití internetu a vzdělávacích akcí v knihovnách[306]

Aby mohla být navržená koncepce efektivní, je nutné ji přizpůsobit aktuálním aktivitám knihoven a kompetencím knihovníků v informační bezpečnosti. Empi-

303 QUICK 2013, s. 12–14.

304 QUICK 2013, s. 23–24.

305 QUICK 2013, s. 19.

306 Dle Základní statistické údaje o kultuře (...) 2017.

rická data o tématech lekcí v českých knihovnách jsou ale omezená a rozšířenost informační bezpečnosti samotné nebyla zjišťována. Proto byla uskutečněna vlastní dotazníková šetření a pedagogické testování zjišťující rozšířenost lekcí informační bezpečnosti pro uživatele, znalosti knihovníků a jejich postoje k vzdělávání uživatelů v tomto tématu. Podrobné zpracování těchto šetření je popsáno v dizertační práci[307], na kterou tato publikace navazuje, zde jsou uvedeny jen hlavní zjištění ve vztahu k navrhované metodice.

2.2.1 Současné vzdělávací akce v knihovnách a informační bezpečnost

Základním východiskem pro navrženou koncepci je otázka, jaké postavení má informační bezpečnost ve vzdělávacích aktivitách knihoven, tedy na co je možné navazovat. Protože koncepce směřuje k vzdělávání dětí na základních školách, byla zvláštní pozornost věnována lekcím pro děti. V době, kdy se o tématu informační bezpečnosti v českých knihovnách v podstatě nemluvilo, a proto nebylo jasné, do jaké míry se objevuje v jejich vzdělávacích aktivitách, bylo nezbytné zmapovat situaci, do které by měla navržená koncepce vstoupit. Situace se v posledních letech jistě změnila, základní poznatky ale navzdory době svého vzniku mají stále význam.

2.2.1.1 Metodologie úvodního šetření

K mapování vzdělávacích aktivit byl použit anonymní elektronický dotazník v aplikaci Survs (viz příloha 1.1). Cílem bylo zjištění, kolik knihoven se věnuje nabídnutým tématům. Pro lepší pochopení, proč je nebo není téma pokryto, byli dále knihovníci dotazováni na názor, zda by se knihovny měly věnovat vzdělávání uživatelů v informační bezpečnosti a odkud o ní sami knihovníci berou odborné poznatky.

Sběr dat probíhal 8. – 19. 8. 2011, v této době nebyly známé žádné informace o tom, které knihovny se problematice vzdělávání v informační bezpečnosti věnují. Proto byly populací výzkumu všechny knihovny aktivní ve vzdělávání uživatelů. Protože neexistuje jejich seznam, byly o distribuci požádány vedoucí organizací specializovaných na vzdělávání uživatelů knihoven, Hana Landová za IVIG a Veronika Peslerová, následně kvůli její nepřítomnosti Jana Nejezchlebová za IVU SDRUK. Vzhledem k nízké návratnosti byly jako další komunikační kanál vybrány e-mailové knihovnické konference (konkrétně Andersen, AKM, Drtina, Knihovna, členů ČIS, SKIP, Výchova). Výzkum se uskutečnil v roce 2011, kdy bylo evidováno celkem 5408 knihoven, z toho 791 profesionálních[308]. Pro další zpracování bylo

307 KOVÁŘOVÁ 2015.

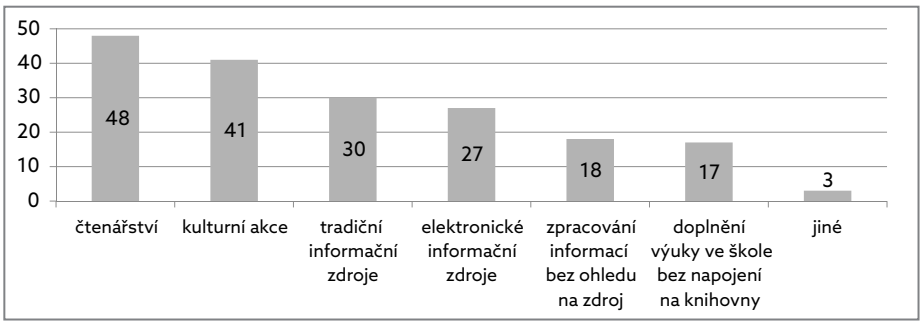
308 Základní statistické údaje o kultuře (...) 2013.

získáno 210 odpovědí z knihoven, z toho 94 z veřejných nespecializovaných (dle knihovního zákona). Dále jsou uvedeny jen výsledky této skupiny s ohledem na navrženou koncepci. Protože většina knihoven s neprofesionálními knihovníky se nezapojuje do elektronických konferencí, je pokrytí výzkumu zajímavější, i když je možné, že více odpovědí pochází ze stejné knihovny.

Pro upřesnění zjištění byl po několika měsících zpracován další elektronický dotazník (otevřený od 2. 1. 2012 do 30. 1. 2012 v nástroji SurveyGizmo) v rámci studentského projektu iNeBe pod vedením Pavly Kovářové. Tento dotazník se již zaměřoval s ohledem na počet vzdělávacích akcí a jejich návštěvnost pouze na knihovny plnící regionální funkce. Po malé návratnosti při přímém oslovování e-mailem byly opět pro distribuci využity e-mailové konference a o podporu byli požádáni regionální metodici v knihovnách. Zpracováváno bylo 121 odpovědí z jedinečně zastoupených krajských a městských knihoven, což představuje 18,1 % populace[309]. Výsledky celého výzkumu jsou publikovány v časopise ProInflow[310].

2.2.1.2 Výsledky dotazníků

Z 94 respondentů úvodního dotazníku 84 uvedlo, že jejich knihovna nabízí vzdělávací akce pro veřejnost, a 50 respondentů, že pro tyto akce jsou jednou z primárních cílových skupin děti (nabízí jim min. 6 vzdělávacích akcí za rok). Informační bezpečnost spadá do práce s informacemi v elektronickém prostředí. Pokud tedy knihovna zatím informační bezpečnost neřeší, ale již pokrývá elektronické informace, je možné obohacení lekcí o toto téma. Základní členění vzdělávacích aktivit pro děti v knihovnách podle prostředí pro práci s informacemi ilustruje Graf 4. Ten ukazuje, že knihovny se stále silně zaměřovaly na čtenářství a tradiční informační zdroje.



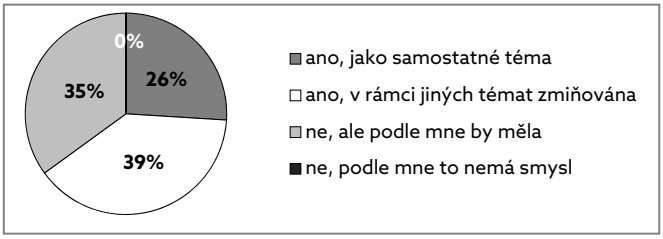
Graf 4 Základní kategorie obsahu vzdělávání dětí v knihovnách

309 Zastoupení je spočítáno na základě součtu knihoven krajských, základních pověřených regionální funkcí a základních s profesionálními knihovníky po odečtení počtu specializovaných knihoven z roku 2012 podle statistiky NIPOS – Základní statistické údaje o kultuře (...) 2013.

310 KOVÁŘOVÁ 2012b.

Necelá třetina respondentů se ale elektronickému prostředí již v roce 2011 věnovala, bylo tedy možné při zavádění informační bezpečnosti navazovat na stávající aktivity. Graf 5 ukazuje, že knihovníci jsou lekcím informační bezpečnosti velmi nakloněni. Dokonce již v roce 2011 je více než polovina respondentů pokrývala. Vzhledem k limitům dotazníku nelze konkretizovat podobu lekcí, převažující zahrnutí v souvisejícím tématu může mít formu zmínky i rozsáhlého rozboru. Pokud výsledek konfrontujeme s výše uvedeným zastoupením témat, ukazuje se, že je elektronické prostředí méně akcentováno, přitom je ale častěji zapojena informační bezpečnost. Lze předpokládat, že s přizpůsobováním knihoven stále silněji komputerizované společnosti bude prostředí ještě více podporovat řešení informační bezpečnosti, což naznačoval i růst zájmu knihovníků o vyžádané semináře na toto téma, např. v rámci Podzimního setkání Klubka SKIP 10 (15. 10. 2013) nebo na Poradě vedoucích pracovníků pověřených knihoven Jihomoravského kraje 25. 9. 2012.

Navazující dotazník se již nezaměřoval na děti, věnoval se informační bezpečnosti bez ohledu na cílovou skupinu vzdělávání. Vzdělávací aktivity podle něj nabízí 75,2 % dotázaných institucí, zahrnutí informační bezpečnosti do nich deklarovalo 44,4 % knihovníků. Jak ukazuje Tabulka 3, pokud knihovna lekce cílené na počítač či internet nenabízí, obvykle se nevěnuje ani informační bezpečnosti. To naznačuje vztah mezi oběma tématy, kdy informační bezpečnost není řešena v širším pojetí (manipulace s informacemi, hodnocení informací v tradičním zpravodajství apod.). Vztah těchto proměnných je statisticky významný (na hladině 1 % Personův Chí-Kvadrát s hodnotou 8,225).



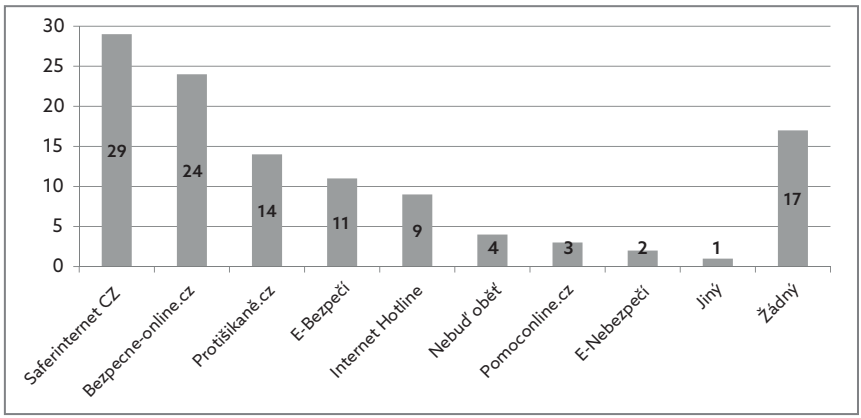
Graf 5 Zařazení bezpečnosti na internetu do lekcí pro děti

Tabulka 3 Srovnání zaměření lekcí

		Vzdělávací aktivita na počítačovou gramotnost nebo práci s počítačem či internetem		
		Ano	Ne	Celkem
Informační bezpečnost v některé vzdělávací aktivitě	Ano	33	6	40
	Ne	25	20	45
	Celkem	62	27	90

V tom, že informační bezpečnost je již v lekcích zahrnuta, lze spatřovat i zájem knihovníků o téma a jeho předání uživatelům knihovny. Pokud jsou lekce realizovány, v knihovně se musí nacházet osoba, která v tom vidí smysl a téma prosadila. V případě, že knihovna téma neřeší, se může jednat o nezájem, ale i o obavu z realizace, která vychází z nedostatečných znalostí, strachu z konfrontace znalostí knihovníka a uživatelů (zejména dětí), nedostatek času či pochopení ze strany vedení knihovny či uživatelů a podobně[311]. Pozitivní postoj knihovníků k informační bezpečnosti ukazuje jejich zájem o osobní vzdělávání v této problematice (83,6 % respondentů) a také o metodické materiály pro realizaci lekcí (76,3 % respondentů). Vzhledem k tomu, že mezi negativními ohlasy mohou být projevy knihovníků, kteří si chtějí lekce stavět sami, je výsledek až překvapivě pozitivní.

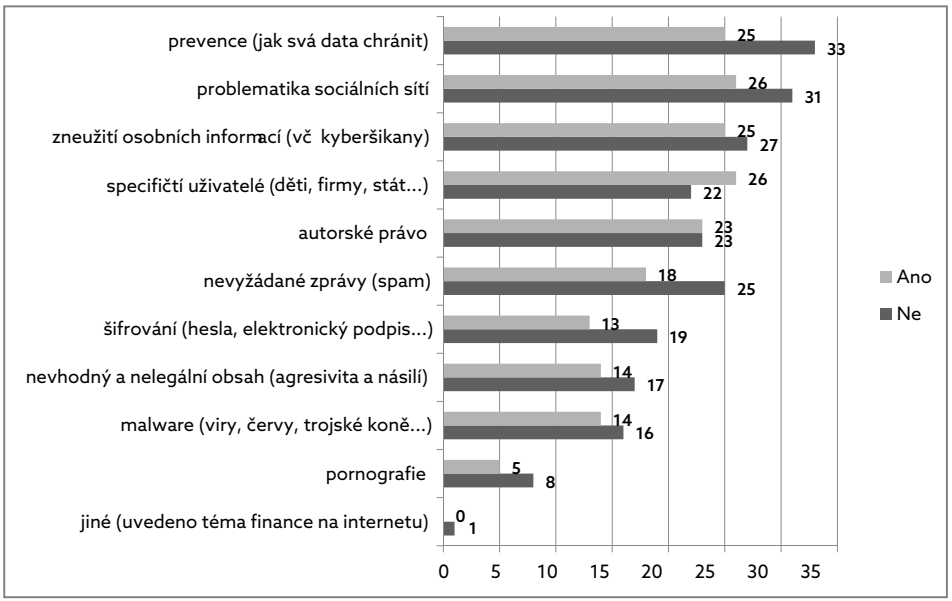
Známé internetové zdroje k informační bezpečnosti (Graf 6) byly zjišťovány proto, že na nich je možné najít materiály pro výuku o této problematice a také je možné na ně odkazovat zájemce o další informace. Řádově méně zastoupené proti projektům Saferinternet CZ byly iniciativy Centra PRVoK, přestože právě ty by knihovníkům mohly při lekcích výrazně pomoci.



Graf 6 Projekty označené za známé

Pro zjištění postoje knihovníků k subtématům informační bezpečnosti bylo využito nepřímého dotazování, kdy respondenti měli v rámci polouzavřené otázky zvolit témata, která by je zajímala z hlediska osobního rozvoje (viz Graf 7). Z výsledků je patrné, že informační bezpečnost v knihovnách je úzce svázána s oběma kategoriemi definovanými v kap. 2.1.2, zájem se příliš neliší podle toho, zda již lekce informační bezpečnosti knihovníci realizují.

311 Tento nekompletní výčet obsahuje příklady důvodů pro ilustraci, všechny byly jmenovány knihovníky z praxe při různých příležitostech, kdy se vyjadřovali k zavedení tématu do jejich vzdělávacích aktivit.



Graf 7 Zájem o téma dle zkušenosti s lekcí o informační bezpečnosti

2.2.1.3 Závěry výchozího stavu v knihovnách

Již v roce 2011 bylo zjištěno široké pokrytí práce s informacemi v elektronickém prostředí, i když pro dětské uživatele byla upřednostňována tradičnější témata, což odpovídá výzkumu IVU SDRUK[312]. Knihovny ale již poměrně často v lekcích pokrývaly i informační bezpečnost, i když různými formami. Důsledkem proto může být, že děti prezentují knihovny jako zdroj rad o online bezpečnosti[313]. Je samozřejmé, že se to netýká všech knihoven, protože pokrývají různá témata a někdy se vůbec do vzdělávacích aktivit nepouštějí. I v případě, že se informační bezpečnosti nevěnují, převažuje názor, že by se toto mělo změnit. Tématu jsou veřejné nespecializované knihovny příznivě nakloněny. Z preference subtémat v rámci informační bezpečnosti vyplývá zájem o problematiku digitálních stop, což odpovídá doporučením zahraničních výzkumů[314].

Příklady dobré praxe a další podpora (např. usnadnění získání znalostí v této problematice) by dále mohly zvýšit zájem knihovníků i množství lekcí. Knihovníci projevili zájem o metodické materiály, což podporuje návrh koncepce v kap. 3.2.

312 NEJEZCHLEBOVÁ, Jana. Veřejné knihovny 21. století a informační vzdělávání. In: KOVÁŘOVÁ 2012a, s. 45–47.

313 LIVINGSTONE 2011, s. 127.

314 WALRAVE 2012; WEEDEN 2013.

Řešení problematiky vyžaduje dostatečnou úroveň znalostí knihovníků s ohledem na zjištěné nízké povědomí o osvětových projektech v informační bezpečnosti. Výsledky této otázky nebyly zcela pozitivní, pro přesnější zjištění ale bylo nezbytné návazně realizovat didaktické testování.

2.2.2 Znalosti knihovníků v informační bezpečnosti

Protože předávat znalosti může jen ten, kdo je sám má, důležité východisko pro navrženou koncepci představují výsledky pedagogického testování knihovníků v oblasti informační bezpečnosti. Vzhledem k tomu, že problematika autorského práva a hodnocení informací je knihovníkům bližší, bylo testování zaměřeno především na téma digitálních stop, v rámci kterého je ale možné některé výsledky spojit s oběma tematickými okruhy v navrhované koncepci. Stejně jako u předchozích šetření jsou i zde popsány jen vybrané výsledky, podrobnější vyhodnocení testování lze najít v dizertační práci autorky. Znění testu se správnými odpověďmi je uvedeno v příloze 1.3.

2.2.2.1 Metodologie testování

Populaci tvořili na jedné straně učící knihovníci v praxi, na druhé straně studenti oboru informační studia a knihovnictví (Univerzita Karlova v Praze, Masarykova univerzita v Brně a Slezská univerzita v Opavě), kteří jsou připravováni v aktuálních tématech na uplatnění v knihovnách. Vzhledem k tomu, že koncepce by měla rozvíjet již existující aktivity knihoven, snahou bylo zahrnout aktivní knihovníky, proto k jejich oslovení bylo stejně jako v případě dotazníků (viz kap. 2.2.1.1) využito elektronických knihovnických konferencí. Pro oslovení studentů byli využiti zprostředkovatelé z řad vyučujících. Test (viz Příloha 1.3) byl dostupný v online aplikaci Survio v období 21. 6. – 15. 9. 2013, kdy bylo získáno 213 kompletních odpovědí.

S ohledem na cíle výzkumu bylo využito pedagogické testování pro měření kognitivní úrovně znalostí[315]. Test byl časově neomezen a sledoval především relativní výkon jednotlivců ve sledované skupině a srovnání skupin dle absolvovaného vzdělání. Zajímavé je i srovnání výsledků s požadovanou úrovní znalostí. Jsou proto zařazeny otázky základní, jejichž správné řešení je nezbytné pro prokázání zvládnutí problematiky, ale také otázky rozšiřující, které ukazují hloubku znalostí nad rámec nezbytné úrovně. Otázky byly pokládány ze šesti provázaných oblastí (vymezení pokrytí digitálních stop, aktivní a pasivní digitální stopy a problémy s nimi spojené, řešení problémů chováním uživatele, technickými a zákonnými možnostmi).

315 BYČKOVSKÝ 1982.

Validita vycházela z obsahové náplně předmětů spojených s informační bezpečností vyučovaných na zahrnutých vysokoškolských oborech a známé náplně seminářů o informační bezpečnosti pro knihovníky v praxi. Posouzení stupně validity bylo svěřeno také pěti vyučujícím z oboru informační studia a knihovnictví, dle jejichž zpětné vazby došlo k přeformulování některých vyjádření. Reliabilita byla nižší než je vhodné pro didaktický test (Cronbachovo Alfa 0,508 a po seřazení otázek od nejjednodušších[316] Guttmanův koeficient pro metodu půlení o hodnotě 0,535). Při odstranění otázek s nevyhovujícími charakteristikami (viz s. 84) se reliabilita výrazně přiblížila požadované hodnotě. Vzhledem k polytematickému zaměření bylo množství otázek drženo na středním doporučeném počtu[317], časová náročnost byla zvýšena jejich typem. Otázky testovaly nejen pamětní osvojení učiva, ale také ostatní úrovně v Niemierkově taxonomii výukových cílů[318] (viz Tabulka 4).

Tabulka 4 Specifikační tabulka pro test k tématu digitální stopy (dále jen DS)

Tematická oblast	Č. otázky	**Téma otázky**	Úroveň dle Niemierkovy taxonomie
Vymezení DS	1	Formy DS	Porozumění poznatkům
	2	Užití DS	Použití v typových situacích
Aktivní DS	3	Úroveň zneužití DS	Použití v typových situacích
	4	Deaktivace Facebooku	Použití v typových situacích
Pasivní DS	5	Zdroje pasivních DS	Zapamatování poznatků
	6	Zneužití DS	Použití v typových situacích
Řešení chováním	7	Signály manipulace	Zapamatování poznatků
	8	Formy prevence chováním	Použití v typových situacích
Technická řešení	9	Anonymní prohlížení	Zapamatování poznatků
	10	Proxy server	Zapamatování poznatků
	11	Onion Routing	Zapamatování poznatků
	12	Blokování Cookies	Použití v typových situacích
	13	Specializované nástroje	Použití v typových situacích
Legislativní možnosti	14	Vymezení osobních údajů	Zapamatování poznatků
	15	Digitální stopy při opravě	Použití v problémových situacích

Při vyhodnocování bylo využito jednoduchého skórování. V případě více správných odpovědí byl počet bodů stanoven poměrově dle počtu zvolených a nezvolených správných odpovědí. Při analýze byla pozornost věnována i nenormovaným odpovědím pro zvážení, zda by téma nemělo být hlouběji řešeno při dalších vzdělávacích aktivitách pro knihovníky. Dvě otázky byly sebehodnotící s doplněním informace o chování pro orientační zjištění rozdílu mezi znalostmi a praktickým jednáním.

316 CHRÁSKA 2007, s. 200–202.

317 CHRÁSKA 1999, s. 22.

318 CHRÁSKA 1999, s. 21.

2.2.2.2 Popis výsledků

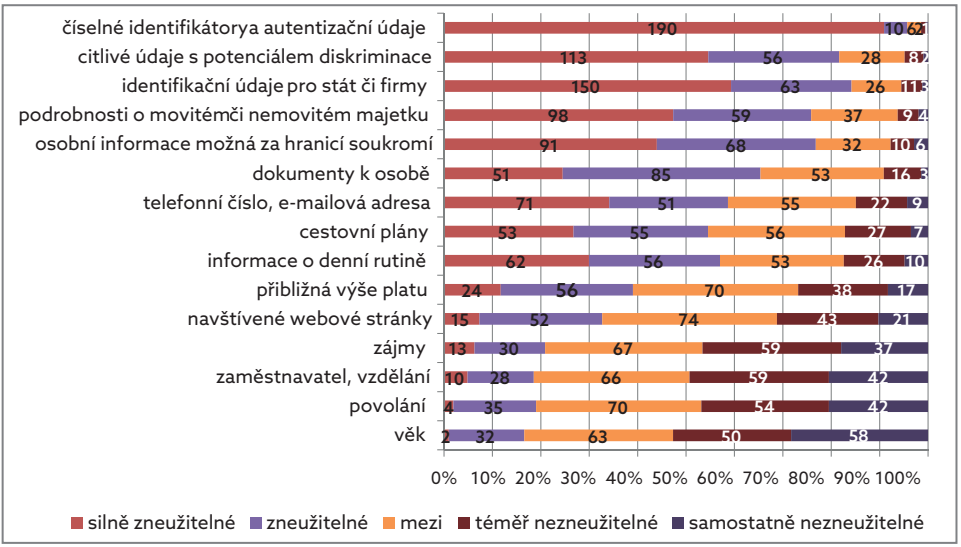
První otázka byla zaměřena na vymezení pojmu digitální stopy. Přestože byla v zadání uvedena možnost volby více odpovědí a všechny nabídnuté byly správné, ve výsledcích převažuje jediná. 93,4 % respondentů označilo jako správnou odpověď „*Soubor informací, které za sebou uživatel zanechává (ať již vědomě, či nevědomě) během využití informačních technologií*". Je pozitivní, že respondenti si uvědomují šíři problematiky, na druhou stranu pod širokým obecným vymezením mají již omezenou představu konkrétních typů informací, které patří mezi digitální stopy (ostatní varianty zvolené 18,3–46,5 % respondenty).

Z hlediska nakládání s digitálními stopami většina respondentů uváděla, že různé subjekty je mohou využít nebo zneužít. Výrazná převaha buď zneužití, nebo využití se objevila jen u hackingu a kriminalistiky (v obou případech správně). V případě správců informačních systémů a sítí a státní správy si ale více než 10 % respondentů myslí, že s digitálními stopami nenakládají, stejné položky zaznamenaly výrazné množství odpovědí „*nevím*"[319]. Přitom právě v jejich případě bývá zpracováván poměrně široký soubor digitálních stop, jehož omezení subjektem je často problematické až nemožné. O to více by respondenti měli mít povědomí, o jaké informace se jedná, jakým způsobem jsou shromažďovány a zpracovávány.

Základem bezpečnosti je uvědomovat si potenciál zneužitelnosti konkrétních informací a podle jeho úrovně dbát na to, komu a zda je vůbec poskytnout. Respondenti vyjádřili své přesvědčení o zneužitelnosti konkrétních typů informací pomocí Lickertovy škály (Graf 8). Odpovědi odpovídají deklarované úrovni zneužitelnosti[320] závislé na kontextu a spojení s dalšími údaji. Protože lze jen přibližně, ne přesně určit, která z pěti úrovní je správná, za správné byly tedy považovány i sousední hodnoty vedle správné v příloze 1.3. Výjimku představují podrobnosti o majetku. Zatímco ostatní informace lze snadno zneužít mnoha způsoby a osobami, majetkové poměry jsou zneužitelné omezeněji (fyzické krádeže, omezeně pro prodej). Ještě více omezené využití má přibližná výše platu, která bývá označována za slabě zneužitelnou (oproti přesné hodnotě), proto patří mezi běžné otázky v průzkumech veřejného mínění apod. Respondenti tedy vnímají za více zneužitelné to, co má přímou vazbu na finance, a opačně hodnotí pouhé informace, přestože v důsledku mohou způsobit horší poškození.

319 CHRÁSKA 1999, 54–55.

320 Např. KRÁL 2006.



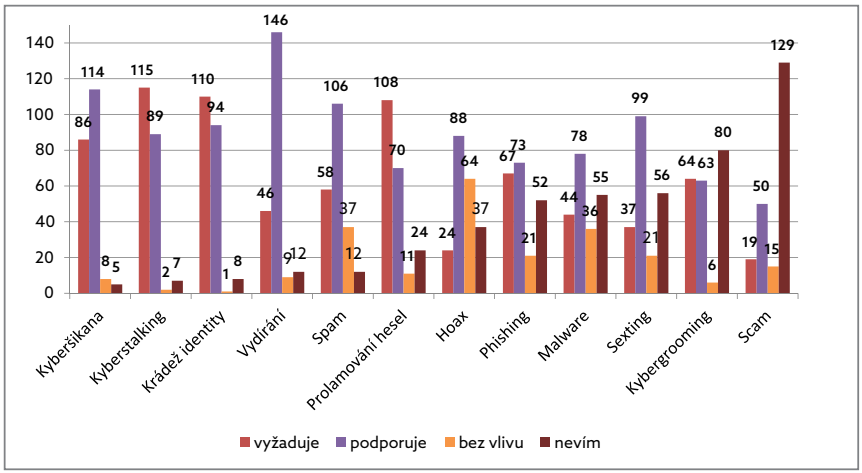
Graf 8 Síla zneužitelnosti informací z digitálních stop[321]

S ohledem na využitelnost sociálních sítí v kontextu digitálních stop bylo zjišťováno, nakolik si respondenti uvědomují možnosti omezení přístupu k nim. 61,5 % dotázaných za tuto otázku získalo plné bodové ohodnocení, knihovníci si uvědomují trvalost digitálních stop i při snaze o jejich smazání. Správa pasivních digitálních stop vyžaduje jak znalost pojmů, tak i uvědomění si možností jejich ukládání různými softwary a internetovými nástroji. Až po uvědomění si tohoto ukládání může uživatel zvažovat jejich správu. Více než polovina respondentů správně označila Cookies (82,16 %), historii v prohlížeči (73,71 %) a sociální síť (60,09 %). Velmi malého počtu volby dosáhl webbug (6,57 %), pozitivní ale není také méně než poloviční hodnota uvedená u vyhledavačů (45,07 %) a pluginů v prohlížeči (28,17 %), proto by těmto oblastem mělo být v dalším vzdělávání věnováno výrazně více pozornosti.

Problémy, které mohou vycházet ze zneužití digitálních stop, sledovala šestá otázka. Volby odpovědí byly velmi různorodé, jak je patrné z grafu 9. Nejvýraznější výsledek získala varianta *podporuje* v případě vydírání, přestože to v prostředí internetu musí být spojeno se znalostí informace, která je předmětem tohoto útoku. Spam a hoax z podstaty nejsou zacílené, z digitálních stop jsou při nich využity jen e-mailové adresy, na které jsou zasílány. Jednoznačně špatné jsou silně převažující varianty u sextingu a prolamování hesel. Základní charakteristikou sextingu je šíření digitálních stop zobrazujících subjekt se sexuálním podtextem, správně odpovědělo jen 17,37 % respondentů. Naopak digitální stopy jen podporují prolamování hesel, i bez jejich použití je možný útok hrubou silou, proto 50,70 % respondentů

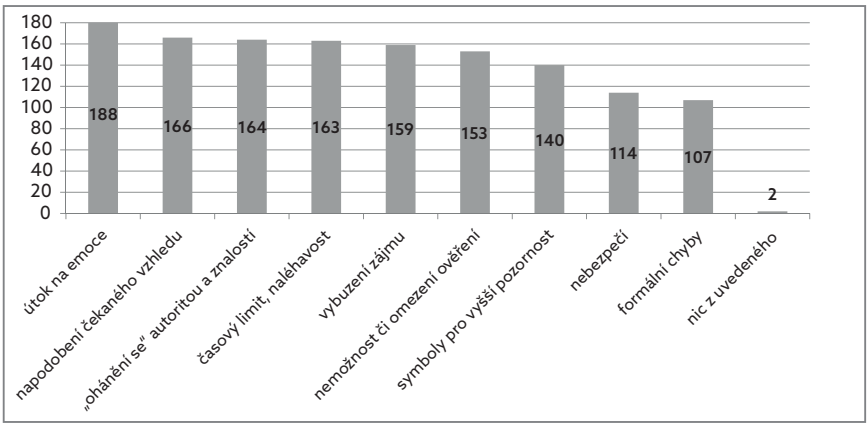
321 Řazeno dle průměrné zneužitelnosti, škála je zleva doprava od nejvíce po nejméně zneužitelné informace, středová hodnota je označena zelenou barvou.

volbou *vyžaduje* označilo chybnou odpověď. Sexting, malware a phishing překvapivě velké množství respondentů nedokázalo posoudit, přestože jsou poměrně často řešeny i v médiích. Ještě méně rozšířená znalost byla zjištěna u kybergroomingu (37,56 %) a scamů (60,26 %). Navzdory předpokladu rozšířeného povědomí o těchto problémech a s ohledem na důsledky daných hrozeb je proto vhodné výše jmenovaným tématům věnovat pozornost při dalším vzdělávání knihovníků.



Graf 9 Upotřebení digitálních stop v hrozbách

Jak bylo popsáno v teoretické části, se zlepšujícími se technickými možnostmi, ale stabilním lidským chováním je stále častěji využíváno prvků sociálního inženýrství. Každá varianta byla zvolena více než 50 % respondentů, nejčastější odpověď útok na emoce (88,26 %) do určité míry svou obecností pokrývá i další nabídnuté postupy.



Graf 10 Varovné signály manipulace

Respondenti deklarují u většiny bezpečnostních opatření, že je nejen znají, ale i používají. Jedná se o postupy chování (např. uvážlivé publikování fotografií), odpovědné reakce při znalosti problémů (např. silná hesla) a použití bezpečnostních nástrojů (např. prověřování aplikacemi typu antivir všeho staženého z internetu). Výrazně nižšího počtu deklarovaného použití dosáhlo sledování aktuálních problémů a bezpečnostních řešení a šifrování či elektronický podpis, které kladou na subjekt vyšší nároky. Kromě těchto dvou možností ještě v případě čtení upozornění více respondentů zvolilo, že možnost znají, ale nepoužívají. I ta je náročnější, ale ne tolik na kompetence subjektu, jako spíše na čas.

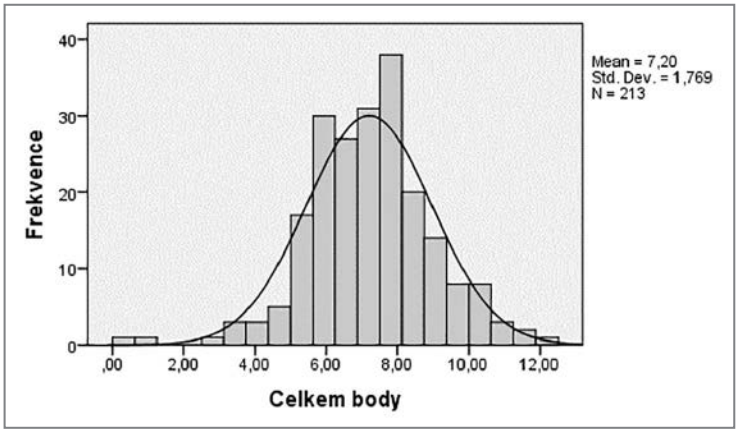
Další série otázek se zaměřila na znalost technických možností ochrany soukromí (anonymní mód v prohlížeči, proxy server a onion routing). Všechny měly více než 70 % špatných odpovědí, většina nulových ohodnocení byla udělena vlivem označení odpovědi *nevím*. Limity blokování Cookies si uvědomuje většina respondentů. I zde mnoho z nich (20 %) zvolilo odpověď *nevím*.

Technické nástroje mají omezené možnosti, ale při vhodném nastavení mohou dlouhodobě snižovat množství útoků a tvoří klíčový doplněk chování pro zajištění bezpečnosti. Jednoznačně mezi nimi převazuje použití antivirů a firewallů, otázkou zůstává, zda jsou si respondenti vědomi toho, proti čemu je chrání. Aplikace typu antispam a antispyware ještě vykazují užití poměrně velkým množstvím respondentů, zejména u antispywaru je ale není možné označit za dostatečné. Přitom právě tento je silně spojen s ochranou digitálních stop. U filtrů obsahu nejvíce respondentů uvedlo, že sice možnost znají, ale nepoužívají. Ostatní tři typy nástrojů (anonymizér, antirootkit a antiphishing) zná již méně než polovina respondentů, většina z nich je pak nepoužívá. Při analýze nenormovaných odpovědí 20% hranici překročily všechny typy nástrojů kromě antiviru, firewallu a antispamu. To ukazuje silnou nedostatečnost znalostí, kterou je nezbytné reflektovat při dalším vzdělávání.

Závěrečná část otázek pokrývala právní opatření pro ochranu digitálních stop. První směřovala k definování klíčového pojmu osobní údaj. 59,2 % respondentů zvolilo správnou variantu, 25 % mezi osobní údaje nesprávně zařadilo i identifikátory v elektronickém prostředí a 5 % identifikátory právnických osob. Otázka na aplikaci zákona do praxe již získala nižší množství správných odpovědí (32,9 %) a 28 % odpovědí *nevím*.

2.2.2.3 Bodové hodnocení a vlastnosti testových úloh

V celkovém hodnocení se ukázalo menší množství velmi slabých výsledků. Naopak výrazný počet respondentů se pohybuje okolo průměrného bodového hodnocení, které je slabě nad polovinou maxima bodů (Graf 11 Body za Q1-Q15 (celkové hodnocení)). Rozložení splňuje kritéria normality (Kolmogorov-Smirnovův test s významností 0,200 a Shapiro-Wilkův test s hodnotou 0,002).



Graf 11 Body za Q1-Q15 (celkové hodnocení)

Vzhledem k tomu, že test proběhl jednorázově, nebylo možné provést optimalizaci. Je ale vhodné pro interpretaci výsledků a další testy zohlednit vlastnosti jednotlivých úloh. Proto byly analyzovány obtížnost a citlivost testových úloh (viz Tabulka 5) a nenormované odpovědi, které byly popsány výše při deskripci odpovědí na jednotlivé otázky. Součástí tabulky je také průměrné bodové hodnocení u otázek.

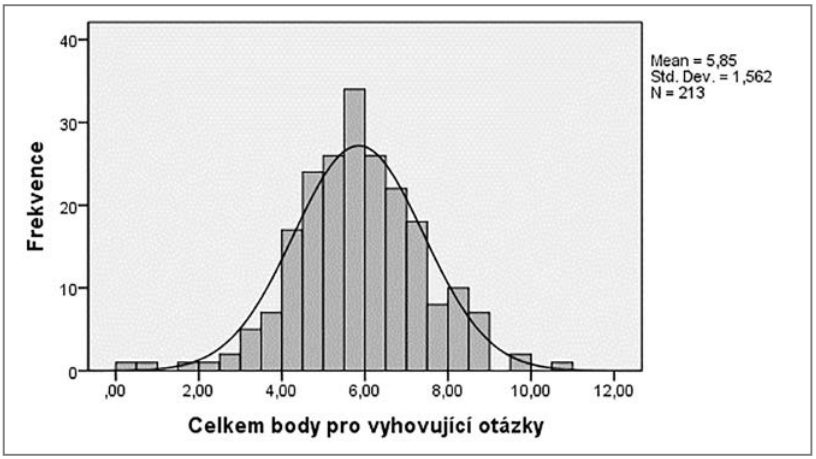
Tabulka 5 Obtížnost a citlivost testových úloh

Otázka č.	Bodový průměr	Q1	Q	ULI	r_{tet}	$_{b}r_{bis}$
1	,42	5,16*	61,03	,330	-,4737*	,3943
2	,62	1,41*	18,31**	,226	-,7375*	,4577
3*	,71	1,88*	6,10*	,085*	-,2768*	,4008
4	,62	38,50	38,50	,264	-,4175*	,3467
5	,49	4,69*	35,68	,377	-,5923*	,4674
6	,34	2,35*	77,93	,198	,8291	,3202
7	,71	,94*	20,66	,585	-,4866*	,4032
8	,62	,47*	,94*	,981	1,0000	,3576
9	,3	70,42	70,42	,330	-,9948*	,3912
10	,11	89,20*	89,20*	,142**	-,9862*	,3398
11*	,05	94,84*	94,84*	,085*	-,5818*	,2821
12	,37	62,91	62,91	,340	,9724	,3968
13	,64	,47*	22,07	,274	-,2714*	,4922
14*	,59	40,85	40,85	,123*	-,9987*	,2135
15	,33	67,14	67,14	,151**	,6912	,2434

(* označuje nevyhovující koeficienty, ** značí hodnoty blížící se kritické hodnotě koeficientu)

Vzhledem k tomu, že v testu byly otázky často složeny z dílčích složek a s možností více odpovědí, nebyly body hodnoceny postupem *všechno a nic*, ale hodnota obtížnosti byla stanovena na základě počtu odpovědí, kde respondenti dosáhli minimálně 0,5 bodu (viz hodnota Q v Tabulka 5 Obtížnost a citlivost testových úloh). Tím se snížil počet nevyhovujících otázek (Q1) kvůli nízké hodnotě obtížnosti[322] z osmi na tři, z nichž jedna se blíží ke stanovené hodnotě. Dvě otázky byly naopak velmi obtížné, jedná se o technické možnosti anonymního prohlížení internetu. Hodnoty obtížnosti mimo doporučenou úroveň nejsou překážkou pro zařazení otázek do testu, pokud jich není mnoho, jednoduché otázky totiž odbourávají obavy dotazovaných, obtížné naopak ukazují, kde je přibližně hranice znalostí respondentů a že celý test není příliš povrchní.

Chráska[323] pro hodnocení citlivosti, tj. schopnosti rozlišit dotazovaného s vyššími a nižšími znalostmi, doporučuje tři typy koeficientů: koeficient ULI, tetrachorický koeficient (r_{tet}) a bodově biseriální koeficient ($_{b}r_{bis}$). Zatímco bodově biseriální koeficient citlivosti vyšel u všech úloh jako vyhovující, naopak tetrachorický koeficient nabýval u 11 z 15 otázek nevyhovujících hodnot. Proto bylo pro rozlišení úloh o nevyhovující citlivosti využito zbývajícího koeficientu ULI a za nevyhovující byly hodnoceny otázky 3 (škálování informací podle zneužitelnosti), 11 (Onion Routing) a 14 (definice osobního údaje). Otázky 10 a 15 sice také nevyhovují kritériím, jejich hodnoty jsou ale blízké hraničním, proto byly ponechány pro další testování. Změnu ve výsledném bodovém hodnocení prezentuje Graf 12 Výsledné bodové hodnocení vyhovujících otázek. Odpovídá normálnímu rozložení dle Kolmogorov-Smirnova testu a pro další testování lze použít i parametrické testy.



Graf 12 Výsledné bodové hodnocení vyhovujících otázek

322 Otázky příliš snadné mají hodnotu Q > 20, velmi obtížné Q < 80 (CHRÁSKA 1999, s. 47).

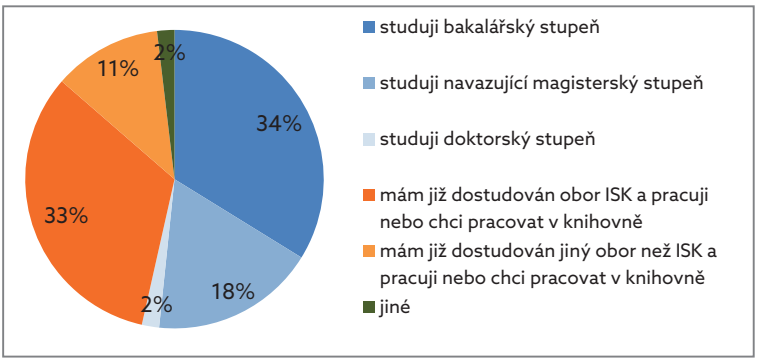
323 CHRÁSKA 1999, s. 49–51.

V rámci interkorelace znalostních otázek bylo zjištěno, že se vyskytují jen v několika málo případech, a to vždy jen na úrovni nízkého stupně korelační závislosti. Mezi kategoriemi se neobjevují vyšší závislosti. To ukazuje na problémy ve stanovení testových otázek, které během přípravy nebylo možné odhalit, znemožňují však test posunout ke standardizaci. Pozitivním zjištěním je, že negativní korelační hodnoty nikdy nepřekročily hodnotu, aby bylo možné pozorovat opačnou závislost, tedy kdyby byly otázky nastaveny zcela špatně.

2.2.2.4 Vliv pohlaví, vzdělání a přesvědčení knihovníků

Zbývající otázky nebyly určeny ke zjišťování znalostí, ale charakteristik respondentů, vzdělání a názorů na vzdělávání o digitálních stopách. Výsledný poměr 172 žen ku 41 mužům ukazuje nevyváženost zastoupení ve vzorku, výsledek je ale ovlivněn tím, že v obou skupinách v populaci je zastoupeno více žen než mužů. Při srovnání bodového hodnocení dle pohlaví jsou patrné lepší výsledky mužů než žen, u ochranných možností mají muži výrazně lepší výsledky (r = 0,5) proti ženám (r = 0,3125), bez překrytí 95 % intervalu spolehlivosti.

Ve vzorku bylo zastoupeno podobné množství studentů a knihovníků z praxe (viz Graf 13). Rozdíl v bodovém hodnocení byl statisticky prokázán pomocí Kruskal-Wallisova testu pouze v některých dílčích otázkách (otázky č. 6, 12 a 13 na hladině významnosti 5 %). Vzhledem k velikosti skupin má smysl věnovat se bodovým hodnocením všech skupin mimo doktorandy a nevalidní hodnotu jiné (tyto dvě skupiny nejsou dále zahrnuty do statistického testování).



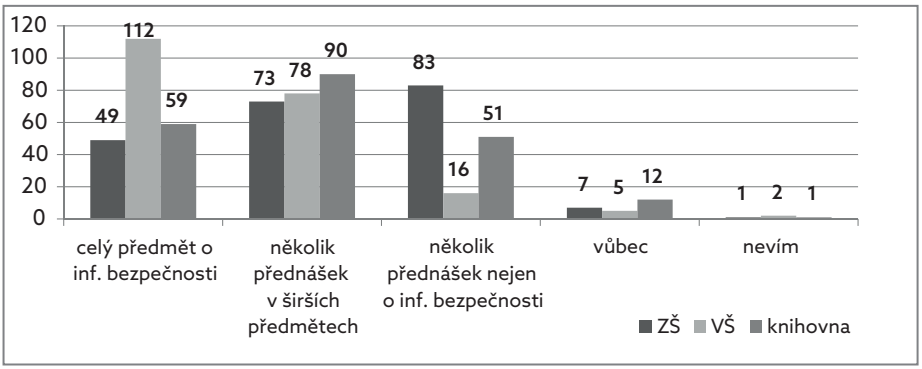
Graf 13 Pozice respondentů v systému školství a knihovnictví

V rámci absolvovaného vzdělávání o tématu digitálních stop otázka zjišťovala jeho rozsah i instituci, která ho organizovala. V případě nejvyššího rozsahu vzdělávání o digitálních stopách je modus i medián varianta 1–3 přednášky (42,7 % respondentů). Samostatný kurz uvedlo 20,7 % dotázaných, naopak žádné vzdělá-

vání 26,3 %. Vzdělávání v tématu se nejčastěji uskutečnilo na vysoké škole (63,4 % respondentů) nebo po ní (19,1 %), vždy v rámci ISK, ostatní varianty byly zastoupeny přibližně u 10 % respondentů.

Podle předpokladu bylo podstatnou proměnnou, jaký zájem pociťuje respondent o řešenou problematiku. Jasně převažoval zájem z pozice běžného uživatele (71,8 %). 15 % respondentů by ale znalosti tohoto tématu chtělo prohlubovat u sebe či ostatních, což je základní předpoklad pro rozvoj problematiky v praxi i pro smysluplnost navržené koncepce. Vliv na bodové hodnocení vzhledem k výrazně převažující jedné variantě není vypovídající, respondenti, podle kterých nemá smysl tématu věnovat čas, ale získali výrazně méně bodů.

Graf 14 Názory na vzdělávání o DS na různých úrovních podobně jako dotazníky (kap. 2.2.1) ukazuje přesvědčení respondentů o smyslu vzdělávání v informační bezpečnosti ve všech třech sledovaných typech insitucí. V případě výuky pro základní školy převažují varianty několika přednášek, proti tomu v případě vysokých škol je patrná tendence k celému předmětu o informační bezpečnosti. Knihovny by mohly využívat oba přístupy (roli může hrát jejich zaměření na děti i dospělé). V bodovém hodnocení podle přesvědčení o úrovni vzdělávání nejsou významné rozdíly.



Graf 14 Názory na vzdělávání o DS na různých úrovních

Pomocí ANOVA testu celkového hodnocení s faktory danými charakteristikami respondentů (viz Tabulka 6) byly statisticky průkazné rozdíly zjištěny jen u pohlaví a osobního zájmu o problematiku digitálních stop. Z hlediska názoru na vzdělávání o digitálních stopách je statisticky rozdílný rozptyl při hodnocení prostředí základních škol, pro vysoké školy a knihovny rozdíl průkazný není. Test vzhledem k malému zastoupení většiny kategorií pokrývajících vzdělávání není vypovídající.

Tabulka 6 ANOVA test pro celkové bodové hodnocení

			Sum of Squares	df	Mean Square	F	Sig.
Pohlaví		Mezi sk.	53,922	1	53,922	24,539	,000*
		Uvnitř skupin	463,655	211	2,197		
		Celkem	517,577	212			
Pozice v systému vzdělávání		Mezi sk.	8,107	6	1,351	,546	,772
		Uvnitř skupin	509,470	206	2,473		
		Celkem	517,577	212			
Osobní zájem o digitální stopy		Mezi sk.	94,359	3	31,453	15,533	,000*
		Uvnitř skupin	423,218	209	2,025		
		Celkem	517,577	212			
Názor na vzdělávání o digitálních stopách	na ZŠ	Mezi sk.	36,009	4	9,002	3,888	,005*
		Uvnitř skupin	481,568	208	2,315		
		Celkem	517,577	212			
	na VŠ	Mezi sk.	10,242	4	2,560	1,050	,383
		Uvnitř skupin	507,335	208	2,439		
		Celkem	517,577	212			
	v knihovnách	Mezi sk.	10,178	4	2,545	1,043	,386
		Uvnitř skupin	507,399	208	2,439		
		Celkem	517,577	212			

Protože celkové bodové hodnocení může být ovlivněno nerovnoměrnými znalostmi v dílčích tématech, byly sledovány výsledky ve dvou různých kategorizacích. V případě dělení na otázky zaměřené na technickou stránku (č. 4, 5, 9, 10, 12, 13) a chování (č. 1, 2, 6, 7, 8, 15) byl zjištěn Pearsonův korelační koeficient 0,295, který je statisticky významný na hladině 1 % při jednostranném testu. Protože technické otázky měly nižší průměr bodového zisku v otázkách (r = 0,4204) proti otázkám směřujícím k chování (r = 0,5547) a nedošlo k překrytí intervalů spolehlivosti, lze prohlásit, že respondenti vykázali vyšší znalosti právě v oblasti chování.

Druhé dělení odpovídá složení testu, kategorie jsou různě rozsáhlé dle významnosti (vymezení tématu zahrnuje jen dvě otázky, zbývající kategorie vždy pět). I zde byly zjištěny statistické závislosti mezi proměnnými (r = 0,169 mezi vymezením tématu a ochranou, r = 0,268 mezi vymezením a užitím digitálních stop a r = 0,273 mezi užitím a ochranou; všechny statisticky významné na hladině 1 % při jednostranném testu). Stejně jako v předchozím případě byly srovnány kategorie pomocí t-testu, který prokázal rozdíly mezi proměnnými bez překrytí intervalů spolehlivosti. Vymezení problematiky vykazovalo v průměrném bodovém zisku otázky r = 0,5165 bodu, užití digitálních stop r = 0,6149 a ochrana r = 0,3486. Nejslabší znalosti tedy byly zjištěny u ochrany digitálních stop, přestože právě ta je důvodem, proč by měly být známy i předchozí dvě řešené oblasti.

Pro kategorizaci respondentů vzhledem k znalostem problematiky bylo využito logistické regrese. Identifikovala charakteristiky nejvíce přispívající pravděpodobnosti, že respondent bude mít dostatečnou úroveň znalostí digitálních stop. Aby bylo možné logistickou regresi realizovat, bylo nutné stanovit požadovanou úroveň. Bodové hodnocení uvedené výše nereflektuje, že některé otázky představují nezbytný základ znalostí a další již zjišťují hloubku znalostí nad nutný základ. Těmto dvěma kategoriím byly přiřazeny otázky:

- Nezbytný základ: 1, 5, 8, 9
- Prohlubující otázky: 2, 4, 6, 7, 10, 12, 13, 15
- Z důvodu nízké citlivosti vyřazeny: 3, 11, 14

Výsledné hodnoty testu zobrazuje tabulka 7, kdy pro úspěšnost v testu bylo nutné správně odpovědět na všechny základní otázky a min. polovinu prohlubujících.

Tabulka 7 Logická regrese charakteristik pro úspěšnost v testu

	Sig.	**Exp(B)**	**95% C.I.for EXP(B)**	
			Lower	**Upper**
Bi_pohlaví	,007	2,589	1,294	5,182
Bi_praxe	,289	1,332	,784	2,262
Bi_zajem	,011	2,935	1,282	6,723
Bi_před	,234	1,659	,720	3,819
Bi_nic	,838	1,221	,180	8,268
Bi_málo	,474	1,214	,714	2,064
Bi_víc	,339	1,446	,679	3,080
Bi_celý	,030	2,068	1,072	3,988
Bi_zš	,309	2,126	,498	9,089
Bi_vš	,819	1,222	,220	6,792
Bi_knihovna	,718	1,231	,398	3,800

Z hodnoty Odds Ratio vyplývá, že k úspěšnosti přispívá postupně od nejsilnějšího vlivu: osobní zájem, pohlaví, názor na vzdělávání o digitálních stopách na základní škole, absolvování celého semináře k problematice, vzdělání o digitálních stopách před vysokou školou, více než tři přednášky k tématu a zda je respondent student či člověk již pracující nebo zajímající se o práci v knihovně. I ostatní čtyři proměnné přispívají k výsledku, hodnoty se ale již blíží k hraničnímu vlivu. Interval spolehlivosti se celý pohybuje nad hraniční hodnotou jen u zájmu respondenta, jeho pohlaví a absolvovaného celého semináře, proto u těchto tří proměnných je vliv nezpochybnitelný. Naopak u názoru na vzdělávání o digitálních stopách na základní a vysoké škole a u neabsolvovaného vzdělání k této problematice jsou intervaly spolehlivosti velmi široké, vliv tedy statisticky existuje, ale u poměrně velké části vzorku se neprojevuje.

2.2.2.5 Závěry z testování znalostí

Cílem testování bylo zmapovat znalosti digitálních stop u lidí pohybujících se v oblasti knihovnictví, a to jak na úrovni praxe, tak i studia. Tyto znalosti jsou nezbytným předpokladem, aby mohli pomáhat uživatelům knihovny či jiné instituce ve zvýšení bezpečnosti digitálních stop. Test pomohl identifikovat témata, na která je vhodné se při vzdělávání knihovníků více soustředit.

Z šetření vyplynulo, že respondenti mají poměrně nízké znalosti o problematice, jen několik jednotlivců prokázalo velmi dobrou orientaci v tématu. Slabá místa jsou především ve znalostech technických nástrojů pro správu digitálních stop, naopak v chování uživatelů jsou silnější. To ukazuje zájem knihovníků právě o chování pro zvýšení informační bezpečnosti.

To odpovídá evaluačnímu dotazníku semináře v Městské knihovně v Praze[324], kdy knihovníci reflektovali svůj postoj k užitečnosti lekce zaměřené na sociální aspekty informační bezpečnosti pozitivně v 77 %, při negativním hodnocení byly jako důvody uvedeny, buď že se knihovník již problematikou zabývá nebo ji ve své práci nevyužije. Z otevřených otázek byly získány informace potvrzující smysluplnost lekce i zájem a překvapení ze škály problémů na internetu i omezených možností knihoven jim předcházet a klíčových prvků pro ochranu knihovny proti zákonným postihům jednáním knihovníků i uživatelů na internetu (viz kap. 1). Pro podporu znalostí knihovníků se snahou omezit bariéry časové, geografické a odborné byl v rámci projektu VISK2 vytvořen e-learningový kurz o informační bezpečnosti dostupný přes portál kurzy.knihovna.cz.

Základním předpokladem rozvoje znalostí je vnitřní motivace, tento vliv se projevoval ze sledovaných charakteristik nejsilněji. I další sledované faktory posilují zlepšování znalostí, jejich vliv je ale méně průkazný. Nicméně potřebné je zajištění podpory vedení, jak dokládá e-mailová komunikace s knihovnicí z městské knihovny ze dne 18. 7. 2013, která projevila zájem o téma i vzhledem k nedostatečné připravenosti z formálního vzdělávání, nicméně spíše na rovině osobní než pracovní, kde by vzhledem k omezeným časovým a finančním možnostem volila vzdělávání spíše v práci s dětmi nebo o přehledu současné literatury. Tato knihovnice také dodává, že didaktický test nedokončila z důvodu přílišné odbornosti otázek s komentářem, že seminář o informační bezpečnosti, který absolvovala v rekvalifikačním kurzu, byl zaměřen „*spíše [na] praktické věci, se kterými se i „běžný smrtelník" může setkat*". To ukazuje nedostatečnou představu o reálnosti zde řešených rizik internetu.

324 Využití výsledků evaluace semináře z roku 2012 odsouhlasil Ondřej Hartman z MKP v e-mailové komunikaci z 8. července 2013.

2.2.3 Zhodnocení současného stavu

Prvním krokem pro zlepšování zjištěného stavu je dostatečné vysvětlení knihovníkům, proč by se právě oni měli v informační bezpečnosti vzdělávat. Obecně již problematiku není nutné obhajovat, protože pouze výjimečně respondenti neviděli smysl vzdělávání v ní. Z dotazníků v kap. 2.2.1 vyplynula potřeba podpořit knihovníky v zahrnutí vzdělávání v informační bezpečnosti do současných aktivit. Přitom se nejedná o zcela novou oblast, ale spíše rozšíření zjištěné nabídky. Vzdělávání uživatelů je již v knihovnách poměrně zavedenou aktivitou, přičemž především u dospělých uživatelů je často pozornost věnována i práci s informačními technologiemi, v případě dětí je stále převažující zaměření na čtenářství. Knihovníci deklarují, že do svých vzdělávacích aktivit problematiku informační bezpečnosti zahrnují, ale hlubší pozornost v samostatných lekcích není častá. Důvodem omezené implementace informační bezpečnosti není nezájem o problematiku nebo její odmítání v prostředí knihoven. Naopak téma je podle respondentů důležité, ale sami často mají problém se v tomto směru rozvíjet, příp. vytvářet lekce, proto by uvítali poskytnuté metodické materiály.

Žádaná podpora na úrovni metodických materiálů je dále reflektována koncepcí v kap. 3. Zjištěné znalosti sice nedosahují ideální úrovně, měly by ale být dostatečné pro realizaci lekcí v kap. 3.2. Nedostatečné znalosti mohou být pro knihovníky bariérou pro to, aby vzdělávali v tomto směru především děti, které bývají někdy označovány jako digitální domorodci[325]. Knihovníci proto potřebují získat dostatečnou jistotu ve znalostech, aby se problematikou zabývali. V dalším vzdělávání knihovníků by se lektoři proto měli soustředit zejména na nedostatečně známá témata, která identifikovalo testování v kap. 2.2.2. Tato témata jsou také předmětem kap. 1. Znalosti knihovníků ale nemusí přesahovat ve všech směrech znalosti dětí, protože *„děti jsou často dobře obeznámeny s počítačem a internetem jako zdrojem zábavy, ale nejsou zvyklé je používat jako nástroje.“*[326] Proto je vhodné soustředit se v lekcích především na rozvoj kritického přístupu k tomu, co internet nabízí, a uvědomění si možných negativních, nejen zábavných důsledků využívání internetu.

2.3 Potenciál knihoven pro vzdělávání v informační bezpečnosti

Informační bezpečnost by měly odrážet všechny služby knihoven, především vzdělávací. Pokud knihovny zahrnou problematiku do svých vzdělávacích aktivit, nebude se jednat o zcela novou oblast, ale spíše rozšíření subtémat informační gramot-

325 PRENSKY 2001.

326 WOLD 2010, s. 77; CHANG 2010, s. 526.

nosti, která je s knihovnami úzce propojená. Vzdělávání navíc zvyšuje efektivitu všech typů bezpečnostních opatření, jak bylo prezentováno v kap. 1.3. S ohledem na růst významu informační bezpečnosti mohou knihovny nabídkou lekcí v této oblasti dávat odpověď na společenskou poptávku, řešit problém spojený nejen se současnou, ale jistě i budoucí společností, což není pravidlem pro všechny služby knihovny.

I když knihovny nejsou jedinou institucí, která by mohla a také měla realizovat lekce informační bezpečnosti, jejich aktivity v tomto směru je možné podložit řadou argumentů, které představují základní souhrn toho, co podrobněji popisovaly předchozí kapitoly, a současně vymezují jejich výhody proti jiným institucím.

1. Lokální vyústění sítě knihoven

Vzdělávání patří dle knihovního zákona mezi služby základních knihoven, které nejsou povinné (podobně jako třeba reprografické služby), ale žádoucí, proto na ně lze žádat účelové veřejné dotace. Díky hustotě sítě knihoven, především základních (viz kap. 2.2), která je v České republice nesrovnatelně hustší než v jiných státech[327], je možné téma dostat do mnoha lokalit. Geografická blízkost je důležitá, protože i přes rozvoj e-learningu stále dominuje prezenční, příp. kombinované vzdělávání. Díky zákonem danému systému spolupracujících knihoven[328] se nabízí široký dosah aktivit, např. pro přenos osvědčené koncepce vzdělávání v informační bezpečnosti. Spolupráce v neformálním vzdělávání veřejnosti se odráží ve fungování různých organizací, především IVU SDRUK a IVIG AKVŠ.

2. Přístup veřejnosti k internetu

Podle knihovního zákona patří mezi základní služby knihovny umožnění přístupu veřejnosti k volně dostupným informacím na internetu, knihovny proto mají povinnost internet svým uživatelům zprostředkovat, a to zdarma a v případě zájmu s pomocí (viz kap. 2.1.1). Že k této pomoci i k zajištění přístupu k internetu patří také informační bezpečnost, dokládá Manifest IFLA o přístupu k Internetu: „*Uživatelům by měla být poskytnuta pomoc v oblasti nezbytných dovedností a vhodné prostředí, v němž by mohli poskytnutých informací svobodně a bezpečně využívat.*“[329] Knihovna by měla tyto uživatele podpořit, aby její služby používali tak, aby se sami neohrozili[330].

3. Důvěryhodnost knihoven jako institucí zprostředkujících informace

Knihovna jako informační instituce se musí zaměřovat na informace, nejen na jejich nosiče. Tím se stává druhořadou otázka, zda je informace digitální nebo ana-

327 GÉBLOVÁ 2013.

328 Zákon č. 257/2001 Sb., § 3.

329 Manifest IFLA o přístupu k internetu 2002.

330 WEAVER 2010, s. 30.

logová, obě by měla řešit stejným dílem. A pokud má být knihovna vnímána jako důvěryhodný zprostředkovatel digitálních informací, je nutné, aby při správném využití jejích služeb nedošlo k ohrožení uživatele. Jen tak si může knihovna udržet reputaci důvěryhodné instituce, přestože veřejné počítače jsou obecně považovány za informační hrozbu.

4. Důvěra místní komunity založená na dlouhodobém vztahu
Důvěru je nutné budovat dlouhodobě na pozitivní zkušenosti. Dlouhodobý vztah se svými uživateli knihovny mají, až na výjimky se jedná o instituce fungující desítky let. Důvěra uživatelů je závislá na jednání knihovny, vzhledem k neustálému nátlaku pro udržení finančních prostředků od poskytovatele je ale pravděpodobné, že v případě ztráty důvěry uživatelů ke knihovně by došlo k omezení využívání jejích služeb, což by mohlo vést k omezení až likvidaci knihovny. Statistiky využívání služeb knihoven (viz kap. 2.2) ale ukazují stálý zájem o služby relevantní k tématu této práce. K budování důvěry je využíváno spolupráce s dalšími subjekty, např. jinými příspěvkovými organizacemi v obci nebo i dobrovolnickými jako např. ekocentry[331], které mohou zprostředkovat navázání vztahu s novými uživateli. Díky dlouhodobému působení si proto různí lidé mohou kdykoli vytvořit ke knihovně vztah a při kvalitních a vždy dostupných službách si k ní vybudovat důvěru.

5. Specializace vzdělávací instituce na práci s informacemi
Knihovny přispívají do systému zajištěním neformálního vzdělávání, příp. spolupracují se školami jako externí subjekt formálního vzdělávání. Knihovny si nemohou nárokovat místo ve vzdělávací činnosti školy, mohou jen vyjádřit zájem a případně přesvědčit o přínosech, ale rozhodnutí je jen na škole, jaké zapojení knihovně umožní. Přesto spolupráce škol a knihoven probíhá[332] a je hodnocena jako pozitivní (po zkušenosti se od ní neustupuje). Mimo vysoké školy[333] jsou státní školy zřizovány obcí či krajem, stejně jako knihovny. Společný zřizovatel usnadňuje spolupráci, která je v jeho prospěch – instituce si mohou vypomoci svou odborností v rámci běžné pracovní činnosti bez dalších nákladů, které jdou z rozpočtu zřizovatele. Odborností knihoven je práce s informacemi, což vede k jejich specializaci na informační vzdělávání (viz kap. 2.1.1).

6. Možnost přizpůsobení potřebám známých cílových skupin
Dlouhodobé působení v místní komunitě vede k tomu, že knihovny znají její charakteristiky a potřeby. Tomu pak mohou přizpůsobit lekce o informační bezpeč-

331 Viz např. Ekopolička v blanenské knihovně iniciovaná centrem Ulita v roce 1999.

332 NEJEZCHLEBOVÁ, Jana. Veřejné knihovny 21. století a informační vzdělávání. In: KOVÁŘOVÁ 2012a.

333 Ty jsou dle zákona č. 561/2004 Sb. samosprávné.

nosti. To je rozdíl oproti celostátním organizacím specializovaným na toto téma, jako Národní centrum bezpečnějšího internetu (NCBI) nebo Centrum PRVoK, které jsou centralizované, a tedy vázané na jedno místo, ze kterého dodávají své aktivity nárazově do místa poptávky. Proto tyto organizace mají omezené možnosti reagovat na potřeby místní komunity, protože ji, na rozdíl od knihovny, neznají. Nárazové aktivity také mohou být spojené jen s omezenou úrovní důvěry při řešení citlivého tématu, jakým je informační bezpečnost, protože staví jen na deklarované odbornosti.

7. Neustálá dostupnost pro řešení problémů

Důvěra je vázaná také na to, že knihovna je neustále dostupná pro řešení problému, je kdykoli k dispozici, právě když to její uživatel potřebuje, omezená je jen otevírací dobou. Pokud by vzdělávání v knihovnách o informační bezpečnosti bylo dostatečné na úrovni jednorázové přednášky, stačila by její nahrávka online, v případě fyzického kontaktu pak nárazové zajištění specializovanou organizací. Cílem této práce je ale návrh komplexního řešení, kdy jsou nutné opakované lekce pro různé cílové skupiny (např. pro všechny třídy ve všech ročnících škol a další skupiny uživatelů v lokalitě) a také poradenství v případě problému. To musí zajistit důvěryhodná lokální organizace s kapacitou a schopností koncepčního vzdělávání o informační bezpečnosti.

8. Dostupnost jen v případě zájmu

Knihovna sice je k dispozici uživateli, kdykoli o to projeví zájem, pokud ho ale neprojeví, nemusí být v kontaktu. Citlivá problematika informační bezpečnosti by měla být řešena v prostředí, které není formální, ale je důvěryhodné, takže člověk nemá obavu svěřit se s problémem[334]. Po řešení informačních incidentů může být nekomfortní se setkávat s člověkem, který o nepříjemném zážitku ví. To může být problematické při řešení s učitelem, především v menších městech, protože s ním se dítě musí potkávat každý den. V případě knihovníka může po dobu, dokud mu je to nepříjemné, návštěvy knihovny omezit.

9. Neomezená cílová skupina vzdělávání

Jiným důvodem podporujícím dostupnost v případě zájmu mohou být situace, kdy knihovna slouží jako alternativa nefungujícího či neexistujícího kanálu pro osvětu či řešení problému. Ne každý člověk má v informační bezpečnosti oporu a podporu v rodině. Dosah škol je mnohdy širší než jen na aktuální žáky, ale ne neomezený. Jedná se například o lekce pro děti v oblastech, které jsou spojené s aktuálními zájmy a potřebami školy, např. při řešení výchovných problémů, zavádění nových technologií pro kontakt mezi rodiči a školou apod. To představuje

334 WOLD 2010.

bariéru v celoživotním a zájmovém učení, kterou ale knihovny nemají. Samozřejmě i knihovny, stejně jako školy, snáze informují o svých aktivitách ty, s kterými mají aktuálně navázaný vztah, ale neomezují své služby na ně. Knihovna svým zaměřením na práci s informacemi, vzdělávání a služby pro veřejnost může být ideálním místem, kde hledat podporu v informační bezpečnosti v rámci celoživotního učení.

10. Oslovení mnoha lidí přes spolupracující organizace
Knihovna může dosáhnout kontaktu s mnoha lidmi tím, že využije nastavené spolupráce s různými organizacemi, nejčastěji se společným zřizovatelem. To je často případ škol, se kterými knihovny v současnosti již poměrně silně spolupracují i v lekcích informační bezpečnosti. Vzhledem k omezení témat knihovny a spolupráci s mnoha institucemi, např. školami, může jedna knihovna lekcemi zasáhnout výrazně více lidí. Stejně tak to může být i jiná instituce, která se této role ujme, z hlediska dalších výhod uvedených výše i specializace na práci s informacemi je ale logické, pokud se rozhodne tuto roli vykonávat knihovna.

Vzdělávací akce iniciované knihovnou nebo jinou institucí jsou vhodným prostředkem pro rozšíření povědomí o řešené problematice. V oblasti informační bezpečnosti je ale nutný i druhý směr, tj. kontaktní bod pro případ, že člověk aktuálně řeší informační problém, se kterým potřebuje pomoci. Knihovny v rámci svých služeb nabízejí podporu uživatele poradenstvím v práci s elektronickými informačními zdroji a službami, je proto vhodné zařadit sem i podtéma informační bezpečnosti. Právě tento kontaktní bod má svůj význam na lokální úrovni, je jen těžce zastupitelný outsourcingem experta. Jsou sice k dispozici kontakty typu Linka bezpečí, ale v citlivých oblastech informační bezpečnosti může být těžké svěřit se cizímu člověku, výrazně lehčí to může být v místě, kde je jasné, že se téma řeší a že s problémem je osloven ten, koho člověk zná a má k němu důvěru.

V rozhodování knihovny, zda se této role ujme, může být relevantní také fakt, že společnost se mění, a to zejména vlivem informací, které tvoří podstatu knihoven. Je proto nutné, aby se změnily i knihovny, otázkou je jak. Je pravděpodobné, že knihovny v příštích letech budou muset upravit nabídku svých služeb, aby odpovídala potřebám společnosti, pro kterou fungují a kterou jsou financovány. Bylo by proto logické, aby knihovny využily právě představený potenciál v oblasti vzdělávání v informační bezpečnosti a odpovědí na tento problém společnosti si upevnily své místo v ní. Neodchýlí se tím od svého tradičního poslání, jen podpoří své postavení důvěryhodných zprostředkovatelů informací, ale novými způsoby, které odpovídají novým potřebám společnosti[335].

335 HERRINGTON 2010.

3 KONCEPCE VZDĚLÁVÁNÍ V INFORMAČNÍ BEZPEČNOSTI PRO ŽÁKY ZÁKLADNÍCH ŠKOL

Informační technologie jsou nástroj jako každý jiný, proto mohou být využity i zneužity. Knihovny by neměly omezovat vzdělávací nabídku na poměrně rozšířené výhody, které informační technologie nabízejí, ale měly by se zaměřit i na problémy, které je mohou doprovázet. Nemá smysl duplikovat činnost škol, ale působení by mělo být dlouhodobé. Především v případě dětí (které se, stejně jako jejich používání internetu, vyvíjejí) by měly být reflektovány aktuálně využívané služby a způsob práce na internetu. Je proto vhodné nastavit celou koncepci, která by postupně rozvíjela znalosti a dovednosti žáků dle jejich aktuální úrovně poznání[336] a současně by budovala postavení knihovny jako instituce, která zprostředkovává přístup k informacím i s využitím internetu, a to způsobem, který je komplexní a bezpečný. Dostatečně vzdělaný knihovník přitom dokáže poradit i nabídnout možnosti dalšího rozvoje. Knihovny by přitom měly využít možností, které se váží na neformální vzdělávání, a tím zaujmout svou pozici v systému, kde budou doplňovat instituce formálního vzdělávání.

Dále jsou představena teoretická východiska neformálního vzdělávání a aktivního učení, které knihovny mohou zavést a které odpovídají konstruktivistickým výukovým principům. Jsou aplikovány do návrhu ucelené koncepce vzdělávání o informační bezpečnosti pro žáky na základní škole. Knihovny jejím využitím získávají ověřený nástroj (viz kap. 3.3), který mohou použít pro zvýšení informační bezpečnosti dětských uživatelů a sekundárně pro zlepšení své role v komunitě tím, že budou přispívat k řešení stále silněji pociťovaného společenského problému, který je v současnosti, především mimo velká města, řešen spíše nahodile nebo vůbec.

336 ANDERSON 2010.

3.1 Edukační východiska

Podobně jako v jiných vědách i v pedagogice se můžeme setkat s různými paradigmaty, která ovlivňují to, co je považováno za vhodný obsah i formu výuky (tedy aktivity pedagoga) a učení (aktivity žáka). Přestože je v současnosti preferován humanisticko-kreativní model výuky rozvíjející nejen znalosti a dovednosti, ale i emotivní svět žáka a jeho tvořivé potence, především ve formálním vzdělávání se lze stále setkat s udržováním zažitých tradic a přístupů, které jsou spojeny s preferencí modelu direktivně řízeného učení, tradičních výukových metod a zaměření na znalosti[337]. Nové paradigma výuky proti tomu usiluje o intenzivnější interakci mezi různými subjekty výuky, o rozvoj celé osobnosti, samostatnosti a odpovědnosti žáka za vlastní učení a využití všech zdrojů učení, včetně těch mimo učebny a učebnice. V souladu s tímto přístupem se nabízí využití také neformálního vzdělávání v knihovnách s aplikací moderních výukových metod.

Aktuální proud teorií v pedagogických vědách, který zdůrazňuje výše uvedené principy a současně patří mezi dominantní pedagogická paradigmata současnosti, je konstruktivismus. Ten zdůrazňuje *„jak aktivní úlohu subjektu a význam jeho vnitřních předpokladů v pedagogických a psychologických procesech, tak důležitost jeho interakce s prostředím a společností.* (...) *[P]rosazuje ve výuce řešení problémů ze života, tvořivé myšlení, práci dětí ve skupinách a méně teorie a drilu*“[338]. Vztah k existujícím vnitřním předpokladům vyžaduje, aby se každý účastník vzdělávání učil sám v autentických situacích, i když za intenzivní interakce s učitelem a ostatními učícími se[339].

3.1.1 Aktivní a kooperativní učení

Konstruktivismus, jako moderní přístup k výuce, může ovlivnit podobu tradiční výuky, radikálněji se ale projevuje při využití aktivizačních výukových metod v rámci tzv. aktivního učení[340]. *„Aktivizující výukové metody jsou takové postupy, které vedou výuku tak, aby se výchovně-vzdělávacích cílů dosahovalo hlavně na základě vlastní učební práce žáků, přičemž důraz se klade na myšlení a řešení problémů.*“[341] Aby to bylo možné, staví na reálných situacích, které vzdělávaní znají nebo si je snadno dokáží představit. Jako aktivní učení nelze označovat jakoukoli výukovou aktivitu, je nutné splnit podmínku, že studenti *„musí číst, psát, diskutovat nebo být zapojeni do řešení*

337 MAŇÁK 2003.

338 PRŮCHA 2003, s. 105–106.

339 SMEJKALOVÁ 2014, s. 3.

340 SMART 2012.

341 JANKOVCOVÁ 1989, s. 84.

problémů. Zejména, aby se aktivně zapojili, studenti musí využít myšlení vyššího řádu, jako je analýza, syntéza a evaluace.“[342]

Aktivní učení je založeno na zapojení vzdělávaných do výuky pomocí různých aktivit, přičemž probíhá interakce mezi vzdělávanými i směrem k vzdělávajícímu, častá je proto skupinová práce a diskuze v různých formách. Tím, že je výuka založena na aktivitách pro jednotlivce a malé skupiny, je kladen důraz na to, že vzdělávaný si učení přizpůsobuje svým potřebám a aktuální situaci, vč. předchozích znalostí a zkušeností (viz výše principy konstruktivismu a humanisticko-kreativního modelu výuky). Při aktivním učení není kladen důraz jen na znalosti, ale také na vytváření dovedností a postojů[343], což odpovídá současným snahám na mezinárodním poli vzdělávání i v českých koncepcích, např. formalizovaných do Rámcových vzdělávacích programů různých úrovní[344].

Zapojení vzdělávaných vede ke zvýšení motivace k učení a také ke zvýšení retence získaných znalostí[345], současně se skrz ně učitel stává facilitátorem znalostí a vzdělávaní získávají pozici, kdy kvalita výuky je dána jejich vlastní činností, což vede k větší zodpovědnosti za výuku i její výsledky, ale také vzdělávané více baví. „*Přednostmi tohoto učení jsou silné podněty, rychlé vnímání plné zájmu, spontánní aha-efekty a prožitky úspěchu a rovněž snadno vybavitelné uložení v paměti.*“[346] Mezi další přínosy aktivního učení patří: rozvoj osobnosti žáka na myšlenkové i charakterové úrovni (samostatnost, odpovědnost, tvořivost, spolupráce), přenos nejen odborných informací, ale i zájmu, respektování kognitivního rozvoje jednotlivce a částečné ovlivnění výuky žáky, využití individualizované a kooperativní výuky, vytváření příznivého školního klimatu a seberealizace žáků s větším propojením školy s reálným životem[347]. To vše reflektuje charakteristiky připisované především mladším generacím (od Generace Y)[348]. Odpovědnost a nadšení vzdělávaného také zvyšuje pravděpodobnost přenesení získaných znalostí po lekci do jeho širšího okolí[349], což by v případě informační bezpečnosti bylo pozitivní vzhledem k stále nevyřešenému způsobu zaujetí dospělých v produktivním věku pro tuto problematiku.

Omezená rozšířenost aktivního učení je ovlivněna jeho limity. Aktivní učení se silně odvíjí podle aktivit a prekonceptů vzdělávaných, je tedy výrazně náročnější pro vzdělávajícího. Ten sice musí mít nastavený plán lekce, vždy by ale měl reflektovat aktuální průběh a potřeby třídy i žáků a svůj plán pružně přizpůsobovat.

342 BONWELL 1991.

343 HANSEN ČECHOVÁ 2006, s. 10.

344 Rámcové vzdělávací programy © 2013–2014, podrobněji viz kap. 2.1.2.

345 POLING 2009.

346 BELZ 2001, s. 65.

347 MAŇÁK 2003, s. 106.

348 HARRIS 2010.

349 PETRESS 2008.

Lektor musí být dobře připraven jak znalostmi, tak na změnu formy vzdělávání, pokud se některá z plánovaných aktivit ukáže jako nevhodná pro danou skupinu nebo se vyvíjí odlišně, než bylo plánováno (např. její provedení trvá déle, takže bude nutné zkrátit jinou aktivitu). Další výraznou změnou oproti tradiční výuce je silný nárůst hlučnosti vzdělávaných a vyšší nároky na obnovu pozornosti směrem k vyučujícímu, což je logický důsledek toho, že interakce mezi vzdělávanými a zaujetí pro aktivitu jsou základem aktivního učení. Protože vzdělávaní ovlivňují směr výuky, je zásadní, aby byli na začátku lekce dobře seznámeni s výukovými cíli a byli také schopni zhodnotit jejich dosažení[350]. Musí mít také dostatek času na promyšlení postupu. Při aktivním učení je možné probrání jen menšího množství učiva ve srovnání s tradičním přístupem, což je cenou za hlubší pochopení tématu. Ve srovnání s tím je efektivnější frontální výuka, kterou je vhodné použít v případě potřeby časově úsporného přímého výkladu nových poznatků všem studentům současně[351]. Při diskuzi časové náročnosti je nutné připomenout, že i úspěšní učitelé věnují jen 50 % času interaktivním činnostem, zbytek je nutné využít pro řízení výuky a organizační záležitosti[352]. I po obsahové stránce ale má aktivní učení limity, a to horší úroveň dosažení vzdělávacích výsledků, ale na druhé straně i lepší rozvoj kreativity, nezávislosti, zvídavosti a pozitivních postojů k učení oproti tradiční výuce, jak dokládá řada výzkumů[353].

Interakci s prostředím zdůrazňuje sociální konstruktivismus, který je nejvíce rozvíjen v rámci tzv. kooperativního učení, které je založeno na spolupráci při dosahování cílů. Tento přístup vychází ze způsobu řešení neznalosti v běžném životě zeptáním se na odpověď, proto jsou v něm preferovány zejména úkoly problémové povahy, které motivují žáky hledat společně správné řešení a diskutovat o postupech a možných variantách řešení[354]. Ne vždy odpověď poskytne expert, někdy je přínosnější zeptat se známé osoby, které člověk důvěřuje a která sdělí potřebné způsobem, který je pro příjemce sdělení přijatelný, byť z odborného hlediska ne zcela přesný. Pozitiva vzdělávání dětí touto formou uvádí Kasíková: „*U dětí se projeví v úrovni začlenění do procesů učení, v kvalitě myšlenkových operací, v rozsahu a úrovni řeči, v kvalitě dokončené práce, vyšší míře samostatnosti a nezávislosti na vzorech, vyšším sebevědomí a sebedůvěře.*“[355] Tak je rozvíjena znalost tématu, ale i tzv. klíčové kompetence (také kompetence pro 21. století apod.), které zvyšují uplatnitelnost člověka v kolektivu a vedou také k návykům pro celoživotní učení[356]. Vedle pozitiv

350 PIHT 2012.

351 VALIŠOVÁ 2007, s. 179.

352 JONES 1990 in MAŇÁK 2003, s. 106.

353 MAŇÁK 2003, s. 106.

354 VALIŠOVÁ 2007, s. 180.

355 KASÍKOVÁ 1997, s. 8.

356 BELZ 2001.

k vlastní osobě Kasíková[357] upozorňuje i na změny vůči okolí: učení se postojům, hodnotám, dovednostem a znalostem od vrstevníků nápodobou těch, kteří vlastní uznanou kvalitu, učení se pomoci a sdílení, budování schopnosti pohlížet na problém nejen z vlastního úhlu pohledu, budování autonomie osobnosti, přijetí odlišnosti vlastní i ostatních, zvýšení výkonu motivací, když je spatřována práce ostatních ve skupině a současně je odbourána obava z chyby. Skupinové vyučování je vhodné, pokud nejde o prosté učení faktů, ale o řešení komplexních úloh[358], vhodné jsou menší skupiny (3–5 žáků[359]) a hlavním úkolem pedagoga je zajistit, že ve skupině pracují všichni členové a dosáhnou potřebné úrovně znalostí[360]. Obava z chyby je odbourávána první kontrolou ve skupině před prezentací ostatním, ale i při jejím výskytu je nutné k ní přistupovat odlišně než v tradiční výuce, měla by představovat stimul pro další učení. Přes výhody kooperativní výuky je vhodné zvážit i výhody jiných organizačních forem, mezi které patří frontální výuka nebo samostatná práce žáků. Různorodost forem umožní rozvoj odlišných kompetencí, není vhodné se tedy omezit pouze na jednu z nich.

Tradiční škola je pro realizaci aktivního učení často omezena nutností změnit zavedený systém výuky, ale často i prostorové a časové dispozice, pomůcky a pomocníky výuky[361], nárůstem časové náročnosti přípravy na výuku a nedostupností potřebného materiálu, vybavení a zdrojů[362], nezbytností probrat všechnu látku vymezenou v ŠVP, nastaveným klimatem třídy pro dlouhodobou práci (např. pravidla komunikace mezi žáky a s učitelem) během výuky atd. Samozřejmě tato omezení jsou různě silná ve školách či ve třídách, ale mnoho z nich je nezbytných pro každodenní efektivní formální vzdělávání v tradičních základních školách, naopak aktivizační metody jsou spojeny s alternativními školami, které ale v současnosti nejsou příliš rozšířeny[363]. Jedna z výhod neformálního vzdělávání je možnost většího prostoru pro aktivní učení, protože se často jedná o doplňkovou výuku, kterou může využít i tradičně nastavená škola pro čerpání výhod aktivního učení při zachování přístupu k vyučování udržovaného v dané škole[364]. Alternativní školy pak mohou aktivní učení v knihovně využít jako další zdroj, jehož pojetí odpovídá přístupu, který škola preferuje. Pozitivní přijetí lekcí v tradičních i alternativních školách bylo prokázáno i v rámci výzkumu popsaného v této publikaci (viz kap. 3.3).

357 KASÍKOVÁ 1997, s. 35–37.

358 SKALKOVÁ 2007, s. 225.

359 SKALKOVÁ 2007, s. 224.

360 PASH 2005, s. 255–256.

361 MAŇÁK 2003, s. 51.

362 BONWELL 1991.

363 MAŇÁK 2003.

364 GRECMANOVÁ 2000.

Výběr výukové aktivity vychází ze zvolené výukové metody, ale také z organizační formy, která může mít podobu výuky v knihovně (příp. muzeu apod.)[365]. Spojení aktivního učení a informační gramotnosti, která je doménou především knihoven, jak popisuje kap. 2, vidí Grecmanová tak silné, že by mělo být začleněno jako přístup k celému učebnímu obsahu[366]. Aktivní učení se již v knihovnách osvědčilo, dokonce i v akademických, např. knihovna Pennsylvania State University ho využila formou hry při rozvoji informační gramotnosti studentů, jiná hra pro stejný účel vznikla na University of North Carolina[367]. V ČR je využíváno spíše v základních knihovnách.

3.1.2 Proces výuky

Aktivní učení, jak bylo řečeno, vychází z konstruktivismu, ovšem může mít různé výukové rámce. V návaznosti na Piagetovu teorii patří mezi nejčastěji užívané v rámci aktivního učení rozdělení do tří fází: evokace, uvědomění a reflexe[368]. Každá fáze má svou roli a vychází z někdy intuitivně používaných postupů ve vzdělávání. V základní charakteristice odpovídá tradičním fázím výuky – motivace (evokace), expozice (uvědomění) a fixace (reflexe)[369]. Fáze diagnózy, která je čtvrtou etapou v tradiční výuce, se zaměřuje na prověřování, hodnocení a známkování žáků[370]. Známkování není součástí neformálního vzdělávání, na základní úrovni je prověřování součástí všech aktivit v navržené koncepci, protože pomocí interakce s žáky lektor ověřuje pochopení látky. Jedná se o jednu z metod opakování a procvičování, které uvádí Skalková[371] a která je také z nabízených metod spolu s neformálními pretesty a posttesty v knihovnách využitelná. Oba postupy byly také uplatněny v rámci navržené koncepce. Jiný přístup k diagnóze v rámci zvoleného přístupu je ten, že diagnóza má podobu sebehodnocení žáky. Správné řešení je sdíleno, žáci si tak mohou ověřit správnost svého výsledku, i když jej přímo nesdílí s lektorem. Tento odlišný přístup k hodnocení může být vhodný, právě pokud se zaměřujeme na rozvoj tvořivosti v moderním přístupu k výuce[372]. Poslední fáze tradiční výuky – aplikace je cílem všech lekcí, ale v rámci neformálního vzdělávání, kdy se lektor k tématu setkává se žáky obvykle jen jednou za rok, je omezená

365 MAŇÁK 2003, s. 46–47.

366 GRECMANOVÁ 2000, s. 9.

367 HARRIS 2010.

368 PIHT 2012.

369 NOVOTNÝ 2002.

370 MAŇÁK 1999, s. 30–31.

371 SKALKOVÁ 2007, s. 203–205.

372 MAŇÁK 1999, s. 91-92; podrobněji k autoregulaci žáků viz MAŇÁK 2003, s. 18–19.

možnost jejího ověření, protože spočívá v přenosu poznání do praxe. Částečně je tento nedostatek řešitelný rozhovory s učitelem žáků, případně s jejich rodiči. Z hlediska organizace lekcí v knihovnách ale opět není tato fáze snadno realizovatelná. Z těchto důvodů je možné považovat třífázový model učení pro navrženou koncepci za dostatečný a vhodný. Současně by ale učící knihovník měl podpořit učitele v možné návaznosti na lekci tím, že další dvě fáze výuky, které nepokrývá sám, může zajistit právě učitel. V rámci koncepce popsané v následující kapitole jsou k tomuto cíli určeny materiály, které si žáci z lekce odnáší, včetně návrhů na diskuzní otázky s dospělými.

Struktura E-U-R představuje základní výukový rámec, který je preferován projektem Reading and Writing for Critical Thinking (čtením a psaním ke kritickému myšlení). Jedná se o celosvětově velmi rozšířenou iniciativu, která akcentuje kritické myšlení, přebírání zodpovědnosti za vlastní učení, vytváření si nezávislých názorů a schopnost si je obhájit a současně brát ohled na názory druhých[373]. Kritické myšlení definuje Grecmanová jako *„schopnost posoudit nové informace a pozorně a kriticky je zkoumat z více perspektiv, tvořit si úsudky o jejich věrohodnosti a hodnotě, posoudit význam nových myšlenek a informací pro své vlastní potřeby*.“[374] Kritické myšlení je rozvíjeno pomocí aktivního učení a s důrazem na spojení s každodenním životem vzdělávaných, vzájemného učení mezi žáky a, jak název programu napovídá, pomocí práce s textem, čtení a psaní, ale i grafických znázornění (viz např. metody I.N.S.E.R.T. nebo t-graf). *„Program RWCT klade důraz na využití metod, které umožňují proces učení „prožít“, které rozvíjejí samostatné a kritické myšlení žáků, vedou je k tomu, aby nespoléhali na učitele jako jedinou autoritu, ale snažili se především diskutovat mezi sebou navzájem a odhalovat další zdroje informací. Žáci se dobírají poznání, že na řadu otázek neexistuje jediná správná odpověď a lze tolerovat více řešení. Převládají metody problémového charakteru, vedoucí žáky k aktivitě a účinné kooperaci, kompetice zůstává v pozadí*.“[375] Cílem projektu tedy není jen učení, ale i metakognitivní učení, tedy snaha naučit se učit se a cítit odpovědnost za vlastní učení – i k tomu vede čitelnost rámce E-U-R, který je známý žákům[376].

Kritické myšlení je jednou z komplexních metod v klasifikaci dle Maňáka[377]. Vedle tříúrovňového modelu učení Maňák zdůrazňuje specifické poslání rozhovoru mezi učitelem a žáky, kdy je vhodné využít víceúrovňového systému kladení otázek (od jednoduchých, vyžadujících doslovnou odpověď, po otázky evaluační, hodnotící). Význam otázek a formy vhodné pro podporu myšlení vyššího řádu

373 VALIŠOVÁ 2007, s. 102.

374 GRECMANOVÁ 2000, s. 7.

375 VALIŠOVÁ 2007, s. 102.

376 GRECMANOVÁ 2000, s. 22–23.

377 MAŇÁK 2003, s. 159–163.

zdůrazňuje také Grecmanová[378]. Těsné spojení kritického myšlení se čtením a psaním, od získání, přes hodnocení a tvorbu informací váže tuto výukovou metodu k informační gramotnosti a činnosti knihoven. Proto se ukazuje jako vhodná právě pro aplikaci v rámci navržené koncepce. Přesto, že se jedná o převažující princip, ve výukovém rámci nacházejí uplatnění další komplexní a aktivizující metody (např. diskuze, výuka dramatem, didaktické hry, simulace a další)[379]. Různé metody lze také použít v různých fázích výuky popsaných níže, ale s odlišným záměrem a pojetím. Vždy by ale měly být dodržovány základní principy těchto metod (např. postup rozdělování žáků do skupin pro jednotlivé aktivity). Bez ohledu na zvolenou metodu je nutné dodržovat obecné didaktické zásady, mezi které patří především princip přiměřenosti a individuálního přístupu (ohled na vzdělávané), uvědomělosti a cílevědomosti (vzdělávaný rozumí tomu, co a proč se učí, směřuje k danému cíli), posloupnosti a systematičnosti (látka navazuje), aktivnosti, názornosti a spojení teorie s praxí (snaha o co nejpřímější poznávání), trvalosti, vědeckosti a zpětné vazby.

Žádná z metod nevede k úspěchu za všech podmínek, je vhodné neomezovat se na několik málo metod, ale reflektovat obsah učiva, předpokládaný charakter učení, organizační limity (čas, prostor, materiální vybavení), znalosti žáků a zkušenosti pedagoga a především výukový cíl. Přestože mluvíme o fázích výuky a různých výukových metodách, které se v nich uplatňují, je nutné stále myslet na to, že se jedná o výukový celek, kdy všechny fáze a metody směřují k naplnění stejného konkrétního a dosažitelného cíle. „*Cílem vyučování chápeme zamýšlený a očekávaný výsledek, k němuž učitel v součinnosti se žáky směřuje. Tento výsledek je vyjádřen ve změnách* (...) *ve vědomostech, dovednostech, vlastnostech žáků, v utváření hodnotové orientace i v jejich osobnostním rozvoji*.“[380] Jak zdůrazňuje Skalková, i když zvažujeme cíle vyučovací hodiny, je nutné je konkretizovat a zvažovat s ohledem na celou hierarchii cílů, je tedy nutné zohlednit cíle školy, předmětu a ročníku (v návrhu koncepce spojeno pomocí RVP, v praxi vhodné spojit s ŠVP) a tématu (postupně rozvíjeno v rámci celé koncepce i v souvisejících předmětech ve výuce ve škole)[381]. Výukové cíle můžeme dělit podle různých kritérií, známé je například dělení kognitivních výukových cílů podle Bloomovy taxonomie, případně Niemierkovy taxonomie, kdy snahou je neomezit výuku na nižší úrovně myšlení, ale naopak usilovat o vyšší úrovně (viz vymezení aktivního učení v kap. 3.1.1).

Stanovený cíl je nutné mít na paměti při návrhu výukových aktivit v rámci každé výukové fáze. Cíl i aktivity, které k jeho dosažení vedou, by měly být lekto-

378 GRECMANOVÁ 2000, s. 34–38.

379 Podrobněji např. MAŇÁK 2003, SKALKOVÁ 2007, specificky zaměřené na metody aktivního učení viz GRECMANOVÁ 2000, SITNÁ 2013.

380 SKALKOVÁ 2007, s. 119.

381 SKALKOVÁ 2007, s. 120.

rem jasně vysvětleny, aby se podpořila motivace žáků i jejich volba vhodné strategie dosažení tohoto cíle[382]. Žáci by si měli uvědomovat, co se naučí, i z jakých předchozích kompetencí mohou vycházet, jaká jsou kritéria úspěchu. Jejich uvědomění si nejen obsahu výuky, ale i možných postupů učení rozvíjí nejen kognitivní, ale i metakognitivní úroveň. Žáci také musí cíle vnímat jako dosažitelné a ideálně je přijmout za vlastní, což lze podpořit tím, že si látku spojí s vlastním životem. Cíle mají ale i hodnotící funkci, protože právě vzhledem ke kvalitě jejich dosažení může lektor hodnotit žáky i vlastní výukový výkon.[383]

První fáze lekce v tříúrovňovém modelu učení – evokace má vzdělávanému připomenout jeho již dříve nabyté poznatky k tématu, což podporuje motivaci, protože navazuje na známé a představitelné pro využití ve vlastním reálném životě. Nestačí, že tyto poznatky existují, je nutné je aktivitou zapojit do lekce, uvědomit si různé související znalosti k tématu. „*Cílem této fáze je tedy žáky aktivizovat, motivovat, vzbudit v nich vnitřní zájem problém řešit.*“[384] Vybavením si předchozích kompetencí si žák vytváří základ struktury, kterou v rámci lekce obohacuje, nové informace řadí do známého kontextu, čímž je podpořeno jejich trvalé uchování[385]. Současně ale může konfrontací s pedagogem a spolužáky dojít i k identifikaci nejasností a chybných názorů. Učitel tedy může do projevů žáků vstupovat, tyto zásahy by ale měly být minimální, spíše by měl žáky povzbuzovat k myšlení. Přílišné zásahy by mohly omezit aktivizaci a zájem žáků o téma, které patří mezi hlavní úkoly této fáze. Vhodné je, aby si žáci sami formulovali otázky, na které by v lekci chtěli získat odpověď. Při takto definovaném záměru lekce se v otázkách odrazí různé druhy motivace, mezi které lze zařadit praktické využití znalostí, potřeba získat kvalifikaci, posilování sebevědomí (úspěchem v učení), potřebu pochvaly, obavu z neúspěchu nebo radost z učení[386]. V tradiční výuce lze evokaci přirovnat k opakování učiva, případně formálnímu diagnostikování vstupní úrovně znalostí žáků pomocí testů, které ale slouží jen učiteli, aby nastavil přiměřenou náročnost nové látky. Proti tomu neformální diagnostika v rámci evaluace plní podobnou funkci vůči učiteli, ale má výše jmenovaná pozitiva i pro studenta, příprava testu je také náročnější než neformální diagnostikování, ale přináší přesnější výsledky[387]. Z toho důvodu byly v rámci testování koncepce zařazeny také pretesty a posttesty pro žáky.

Uvědomění si významu je druhou fází vzdělávacího rámce, kdy dochází k předání nových poznatků. I zde může být využito aktivního učení, ale může se jednat

382 SKALKOVÁ 2007, s. 126.

383 PASH 2005, s. 93.

384 HANSEN ČECHOVÁ 2006, s. 30.

385 GRECMANOVÁ 2000, s. 26.

386 SITNÁ 2013, s. 18–24.

387 PASH 2005, s. 106–108.

také o tradiční frontální výuku[388], pokud je vhodná pro téma lekce a skupinu vzdělávaných. Také v tomto případě je dobré proložení drobnými aktivizačními metodami pro udržení pozornosti a zájmu žáků. Vedle předání nových znalostí ve spojení s předchozími se pedagog snaží také o vedení žáků k tomu, aby sledovali proces učení (metakognitivní úroveň), zda nové informaci rozumí a jak souvisí s jejich předchozími znalostmi, případně si ujasňovali problematická místa s podporou spolužáků nebo učitele[389]. I když se jedná o jádro výuky, není možné lekci omezit na tuto fázi a počítat s tím, že ostatní vzdělávaný zvládne sám bez vedení.

Závěrečnou fázi představuje reflexe, která slouží ke zhodnocení získaných zkušeností a poznatků, ověření, že došlo k správnému pochopení a k hlubšímu zakotvení informací ve znalostní struktuře. Klíčové je, aby vzdělávaný vyjádřil své myšlenky vlastními slovy (podpora argumentace) a aby došlo k výměně názorů mezi žáky pro srovnání možných odlišných pohledů. V rámci reflexe dochází také ke shrnutí poznatků, kdy jsou vyzdviženy nejpodstatnější prvky nově naučené látky. V tradiční výuce si tuto fázi lze z části přiblížit zkoušením, které také slouží oběma stranám ve výuce k ověření, že došlo k správnému přenosu poznatků. V případě reflexe je toto zjištění pouze informativní a je nezbytné tuto fázi realizovat ihned po fázi uvědomění, protože slouží k upevnění poznání před zapomenutím. Známky a produkt učení se při reflexi stávají sekundárními, vzdělávaní si často uvědomují, že důležitější je pro ně proces učení, kdy získávají zpětnou vazbu od ostatních, ne od vzdělávajícího[390]. Klíčové přitom je, aby se při reflexi dostala vzdělávanému také zpětná vazba od vyučujícího, nestačí sebehodnocení vlastního výkonu.[391] I sebehodnocení je ale podstatnou složkou reflexe, žák by si měl uvědomit, jak se změnilo jeho myšlení, hodnoty apod.[392] Cílem reflexe je také motivovat k dalšímu učení v řešené problematice tím, že student bude zaujat aktivitami a také si bude vědom dosažení výukových cílů, projeví se tedy pozitivní emoce v podobě spokojenosti s vlastním výkonem[393].

Výhody aktivního učení a výukového rámce E-U-R, které byly představeny v posledních dvou kapitolách, mohou posílit vzdělávací roli knihovny a zaujmout nejen pro předmět lekce, ale také budovat pozitivní vztah vzdělávaného k samotné instituci. I když je nutné brát v úvahu také limity těchto přístupů, jak bylo výše diskutováno, v prostředí knihoven jsou omezené právě specifiky neformálního učení v tomto prostředí. Proto jsou aktivní učení i struktura evokace – uvědomě-

388 GRECMANOVÁ 2000, s. 27.

389 GRECMANOVÁ 2000, s. 27–28.

390 KASÍKOVÁ 1997, s. 91.

391 PIHT 2012.

392 GRECMANOVÁ 2000, s. 28.

393 PIHT 2012.

ní – reflexe využity v dále popsané koncepci vzdělávání o informační bezpečnosti pro knihovny.

3.2 Lekce o informační bezpečnosti a zkušenosti z jejich realizace

Podobně jako v běžné výuce je nutné nastavit předávané informace podle jejich příjemce[394]. Vzhledem k tomu, že tato publikace přináší nové řešení, navržená koncepce je jen prvním krokem komplexní nabídky vzdělávání o informační bezpečnosti, které mohou zprostředkovat knihovny. Na ni by mělo navazovat vzdělávání dalších cílových skupin. Knihovny jsou přitom jen primárním prostředím s ohledem na zaměření této publikace, lekce je možné realizovat i v dalších institucích neformálního vzdělávání (např. volnočasová centra) a za určitých podmínek i formálního (při zohlednění způsobu a obsahu výuky ve škole). Lekce jsou propojeny se základním vzděláváním (kurikulární spojení jsou konkretizována v rámci popisu jednotlivých lekcí), je zde tedy potenciál oslovit celou populaci, pro kterou jsou určeny.

Koncepce je navržena tak, že pro každý z devíti ročníků základní školy je určena jedna lekce. Zaměření na práci s informačními zdroji a bezpečnou komunikaci se pravidelně střídají. Lekce je možné s drobnými úpravami využít i pro jiné ročníky, je ale nutné zvážit odlišné potřeby. Lekce volně navazují, postupně jsou rozvíjeny znalosti, dovednosti a postoje žáků s ohledem na jejich věk a problémy, se kterými se s větší pravděpodobností mohou setkávat (viz kap. 1.2.3). Lze je ale realizovat také samostatně, pokud žáci mají dostatečné znalosti pro zvládnutí problematiky. Koncepce v následujících kapitolách je určena především učícím knihovníkům, kteří lekce budou realizovat ve své knihovně, čemuž odpovídá forma a obsah návrhu.

Popis každé lekce je složen z těchto částí: anotace, výukové cíle, spojení s RVP a NIQUES, materiální zajištění, osnova (jednotlivé aktivity a jejich význam pro lekci, ukázky pracovních materiálů jsou obsahem přílohy 2) a zkušenosti lektora. Pro návrh lekcí byly využity zdroje uvedené v této publikaci (odborné poznatky shrnuje kap. 1) a konzultace s učícími knihovníky a po realizovaných lekcích i s učiteli daných tříd. Klíčové výsledky konzultací s učiteli jsou popsány v rámci zkušeností z lekcí u každé z nich, tyto subkapitoly ale primárně staví na výsledcích zúčastněného pozorování. Byly zařazeny do koncepce jako upozornění na klíčové prvky lekce pro její efektivitu (proto nejsou součástí kap. 3.3, přestože tvoří složku akčního výzkumu, který je předmětem jmenované kapitoly). Metodologie a souhrnné poznatky z pozorování jsou předmětem kap. 3.3.3.

394 ČÁP 1993; FONTANA 1997; VÁGNEROVÁ 2005.

Dále představená koncepce byla prezentována na seminářích pro knihovníky[395], na základě toho byla vyžádána pro nasazení ve vlastních aktivitách desítkami knihoven různých velikostí (např. Jihočeská vědecká knihovna v Českých Budějovicích, Knihovna Jiřího Mahena v Brně, Krajská knihovna Františka Bartoše ve Zlíně, Městská knihovna a infocentrum Dolní Bousov, Městská knihovna Pelhřimov, Městská knihovna Třinec, Městská knihovna v Praze a další). O lekci v souladu s cíli této publikace projevily zájem i další organizace (např. Skaut). Od knihovníků byla při sdílení žádána zpětná vazba pro upravení koncepce. Veškeré reakce knihovníků i žáků byly pozitivní, ukázalo se ale, že nezbytnou součástí koncepce je vymezení neformálního vzdělávání, aktivního učení a rámce evokace – uvědomění – reflexe (viz kap. 3.1.2), protože někdy nebyla dodržena didaktická pravidla a tím byl omezen vzdělávací efekt lekce. Materiály lze šířit při uvedení autorky, lze je i upravit, další šíření ale musí obsahovat i původní verzi. Všechny materiály k lekcím v aktuální podobě jsou dostupné na Google Drive (https://goo.gl/bHjGfU – přístup bude udělen na vyžádání).

Všechny lekce mají společné následující charakteristiky:

- Časová dotace 90 minut (dvě vyučovací hodiny) zahrnuje i 10 minut jako rezervu pro přesuny, lze jí prodloužit fázi uvědomění. Časová náročnost aktivit je popsána v osnově lekcí.
- Lekce jsou určeny vždy pro jednu třídu, tj. 20–30 dětí.
- Pro každý ročník je navržena jedna lekce, ročník odpovídá pořadí lekce v seznamu.
- Na straně dětí nejsou potřebné předchozí kompetence nad rámec jejich běžné zkušenosti v daném ročníku.
- Součástí lekcí je kooperace, která podporuje zapojení i méně zdatných žáků.
- Lekce rozvíjí i klíčové kompetence dle RVP (komunikativní, sociální a personální a občanské) a průřezová témata (osobnostní a sociální výchova, výchova demokratického občana a mediální výchova) – více viz kap. 2.1.2.
- Lekce jsou navrženy s co nejmenšími požadavky na technické vybavení, většina probíhá bez počítačů.
- Struktura lekce odpovídá výukovému rámci E-U-R (viz kap. 3.1.2). Aktivity se mohou zdát jednoduché při zvážení, co vše by měly děti znát. S ohledem na časovou dotaci, záživnost a hlubší pochopení je vhodné zůstat na stanovené úrovni a předat sice jen základy, ale kvalitně.
- Na konci každé osnovy je *Pět otázek s dospělými*, které by každé dítě mělo po lekci

395 Kdo je za monitorem a mnoholičný lektvar (Workshop Informační vzdělávání v knihovnách – Jak na to kreativně 2013), Bezpečná internetová komunikace akademika s dětmi v městské knihovně (Národní seminář informačního vzdělávání 2013), Bezpečnost dětí na internetu v knihovnách (Nebezpečný internet v KJM 2013), Kdo je za monitorem? (Seminář Informační vzdělávání uživatelů ve veřejných knihovnách 2014) a další.

dostat pro diskuzi s rodiči v nejbližších dnech. Úmyslně jsou zařazeny otázky, které jsou využity i u předchozí nebo následující lekce pro jejich návaznost.
- K diskuzi jsou po lekci vyzváni i učitelé. Jako podklad slouží materiály, které si žáci odnáší po lekci, protože vytváření pevných struktur může trvat déle, což je v souladu se stanovenými postupy pro aktivní učení[396]. Jedná se většinou o produkty z fáze reflexe. Při nedostatku času může aktivita ve fázi reflexe proběhnout ve škole s diskuzí s učitelem, vhodnější je ale uskutečnit ji v knihovně a ve škole navázat jen další diskuzí nad výsledky.

3.2.1 Výhody a nevýhody digitálních zařízení

Anotace: Cílem lekce je především zvýšení motivace a seznámení dětí s možnostmi a limity různých digitálních zařízení. Snahou je sdílení zkušeností dětí a uvědomění si výhod a nevýhod použití jednotlivých typů zařízení (smartphone, tablet, 2v1, stolní počítač, notebook, čtečka). Děti zkusí nad zařízením přemýšlet na základě návodných otázek.
Cílová skupina: 1. třída ZŠ
Materiální vybavení: Psací potřeby a volné papíry pro žáky, puzzle (jedny pro skupinu), pracovní list Analýza věcných rysů (jeden pro skupinu), vhodné každé z řešených zařízení
Výukové cíle – Žák je po lekci schopen...:
- vybrat nejvhodnější typ zařízení pro určené využití;
- vyjmenovat některé klady a zápory jednotlivých zařízení;
- vysvětlit osobní potřebu a zájem v rozvoji v oblasti IT.

Spojení s RVP: ČJL-3-1-02, ČJL-3-1-03, ICT-5-1-02, klíčové kompetence a průřezová témata
Spojení s NIQUES (informační gramotnost): Formulace problému, plánování postupu řešení, hardware, každodenní život s technologiemi
Výukové aktivity dle E-U-R:
- evokace: Puzzle zařízení,
- uvědomění: Analýza věcných rysů,
- reflexe: Kreslení nejvýhodnějšího zařízení.

Osnova
Puzzle zařízení
Časový plán: 15 minut
Lekce je zahájena představením jejího cíle, který spočívá v uvědomění si toho, jaká pozitiva může přinést využití digitálních zařízení pro různé aktivity, ale také jaké

396 *STEELOVÁ 2007c*, s. 15.

jsou jejich limity. Přitom s ohledem na současnou popularitu tabletů jsou výhody i limity představeny právě pomocí jejich srovnání s dalšími typy zařízení. Žáci by si měli uvědomit, proč se o tato zařízení chtějí či nechtějí zajímat s ohledem na účel využití. Nadřazené a podřazené pojmy (digitální zařízení a jejich druhy), stejně jako výhody a limity každého druhu jsou přiblíženy připodobněním k rostlinám – kaktus i pampelišku lze označit jako rostliny, výhoda kaktusu je v malé potřebě zalévání, problém v jeho ostnech, pampeliška může být léčivá, ale může obarvit ruce.

Žáci jsou rozdělení do šesti skupin tak, že si vylosují lísek s číslem a najdou ostatní žáky se stejným číslem. Tak vzniknou skupiny 3–4 žáků, kdy se každá skupina věnuje jednomu typu zařízení. V případě, že nejsou v knihovně k dispozici všechna uvedená zařízení, je možné, aby více skupin mělo stejné zařízení. Každá skupina dostane obálku s dílky puzzle, cílem je poskládat obrázek a pojmenovat daný typ zařízení. Jedná se o stolní počítač, notebook, 2v1, tablet, smartphone a čtečku e-knih. Po seskládání obrázku jsou žáci vyzváni, aby se podívaly na zařízení ostatních skupin a poté každá skupina pojmenovala své zařízení. Při neznalosti nebo špatné odpovědi jsou o pomoc požádány ostatní skupiny.

Analýza věcných rysů
Časový plán: 45 minut: 15 min. pro vyplnění, 30 min. pro diskuzi
Následně je skupinám představen pracovní list pro analýzu věcných rysů a postup aktivity. Lektor postupně čte a vysvětluje otázky a nabídnuté odpovědi a žáci list po diskuzi ve skupině vyplňují. Před zahájením vyplňování dostane každá skupina svůj pracovní list a zařízení, kterého se týká, přičemž zařízení je zaheslované a žáci jsou upozorněni, že je to úmyslně a nemají se snažit uhodnout heslo. Jinak ale zařízení mohou zkoušet (především rozsvítit).

Poté, co je vyplněn celý list, lektor znovu prochází otázky, kdy ale jsou žáci vedeni k tomu, aby zařízení srovnávali. Po položení otázky jsou proto prezentovány odpovědi ke každému zařízení. Otázky tentokrát nejsou čteny, ale právě pro srovnání jsou přeformulovány, např. na velikost je položena otázka: „*Kdo si myslí, že jeho zařízení je nejmenší? A která skupina má naopak to největší? Ostatní skupiny mají všechny zvolenu střední variantu, nebo jinou?*“ Tímto postupem dochází nejen ke srovnání, ale i udržení pozornosti všech skupin (kterákoli může být na řadě v odpovědi) a k časové úspoře. V případě nesprávné odpovědi jsou k diskuzi vyzváni všichni žáci a lektor na správnou odpověď navádí ukázkou práce s daným zařízením.

Kreslení nejvýhodnějšího zařízení
Časový plán: 15 minut: 10 min. kreslení, 5 min. prezentace
Žáci dostanou prázdný papír a pastelky, fixy apod. se zadáním, aby namalovali zařízení, které je podle nich nejlepší, a přemýšleli, proč je nejlepší a jaká jsou naopak

jeho omezení. Během kreslení lektor žáky obchází a ptá se jich právě na výhody a limity. Po uplynutí času jsou žáci seznámeni s tím, že si obrázky odnesou, takže je budou moci dokončit ve škole. Ještě před odchodem z lekce ale zájemci obrázek ukáží ostatním a řeknou, proč je dané zařízení podle nich nejlepší a kde je jeho omezení. Tím dojde k zopakování si základu lekce, tedy že zařízení mohou být pro určité účely výhodná, ale je nutné si uvědomovat, že každé má svá omezení.

Pět otázek s dospělými

1. Jaké jsou druhy počítačů?
2. V čem ti může pomoct použití počítače?
3. Který druh počítače ti může nejvíc pomoct při přípravě do školy?
4. Jaké má výhody a nevýhody tablet proti stolnímu počítači?
5. Co tě nejvíc baví a nepoužíváš k tomu žádný druh počítače?

Zkušenosti lektora

V případě prvních tříd se často ukázalo, že řada dětí má velmi malé zkušenosti s počítači, ale v každém třídním kolektivu se našel někdo, kdo měl velké zkušenosti, byť jen s některými zařízeními a účely využití. Tento žák byl obvykle dominantní a od počátku bylo nutné upozornit ho na slabiny jeho znalostí a povzbuzovat ostatní k diskuzi s ním. To neznamená, že by měl být ponižován, ale jen deskriptivně upozorněn na limity jeho znalostí a zkušeností a na to, že i on se může v lekci něco nového naučit. V případě citlivého přístupu to nevedlo k tomu, že by se žák přestal zapojovat, ale byl stále aktivní a nadále přispíval svými zkušenostmi. Méně zkušení žáci by se měli přestat lekce obávat tím, že lektor konstatuje, že to pro lekci není problém. Naopak budou vědět, kde jsou pozitiva a negativa zařízení, až bude čas, kdy s nimi budou pracovat, takže na to budou dobře připraveni a s menší pravděpodobností se setkají s problémem při jejich využití.

V rámci evokace není v případě nedostupnosti některých typů zařízení vhodné vytvářet větší skupiny, protože to omezuje interakci žáků. Místo toho je možné, aby se více skupin věnovalo stejnému zařízení. V každém případě by měly být řešeny stolní počítače, tablety a smartphony. Vzhledem k tomu, že s nimi při lekci žáci nepracují, ale praktické ukázky jsou v rukou lektora, může se jednat o jeho osobní zařízení. Upozornění na heslo bylo důležité, v opačném případě věnovali mnoho času právě snaze o odemknutí zařízení a zkoušení různých aplikací. V případě nastavení pravidla s heslem žáci omezení respektovali. Některá zařízení žáci znají dobře, jiná ne, především zařízení 2v1 budilo velký zájem, protože ho většinou i zkušenější žáci viděli poprvé, což zvyšovalo zájem žáků. Spokojeny byly především skupiny pracující s tabletem.

Rozpočítání do skupin bylo dobré proto, že se k sobě častěji dostali různě znalí žáci. I když v prvním okamžiku, kdy byla oznámena skupinová práce, žáci projevovali, s kým chtějí být a s kým ne, rychle akceptovali odlišné určení, pokud

viděli jeho náhodnost (co si sami vylosovali, ne že k nim byl přidán lektorem člen, se kterým pracovat nechtěli). Skládání puzzle s více než 20 kousky bylo pro žáky náročné na čas i dovednosti, většinou potřebovali asistenci lektora nebo učitele. Problémy byly v počtu puzzle, ne v obrázku. Puzzle z tvrdého papíru byla opakovatelně využitelná.

V rámci představování pracovního listu pro analýzu věcných rysů není vhodné vysvětlovat otázky dopředu, ale až postupně při vyplňování, protože žáci si je nezapamatují a mají problém se čtením zadání. Čtení otázek a jejich opakované vyjádření jinými slovy je potřebné pro to, aby žáci byli schopni najít správné odpovědi a neměli problém s tím, že nerozumí zadání. I když se jedná o žáky v druhém pololetí, i krátké věty čtou poměrně dlouho a mají problém se čtením s pochopením. Podobně jako bylo potřeba usnadnit zadání čtením otázek, tak bylo klíčové dát možnost jen zakroužkovat správnou variantu, protože žáci měli ještě problém s psaním. To by mělo být omezeno na minimum a lektor by měl být k dispozici pro pomoc s tím, jak se píše konkrétní písmeno. Většina skupin postupovala stejně rychle, v případě, že byli žáci rychlejší, sami se snažili o čtení a odpovídání na následující otázky. Pokud žáci mají zařízení v ruce, i když ho nemohou plnohodnotně používat, zvyšuje to jejich motivaci a usnadňuje vyplňování. I s omezeným využitím je vhodné v rámci vyplňování pomoci, např. ukázat, jak lze zařízení rozsvítit (to bez asistence měli problém žáci zjistit především u čtečky, ale i u některých tabletů a 2v1).

Pokládání otázek pro vyhodnocení je klíčové. Procházet jedno zařízení po druhém, stejně jako v pevně daném pořadí skupin není vhodné kvůli udržení pozornosti všech. Žáci se soustředí jen v okamžiku, kdy jsou na řadě, jinak diskutují ve skupinách a nevěnují pozornost ostatním, ale naopak je svou diskuzí ruší. Pokud mohou být na řadě kdykoli, sledují lektora a současně se zapojují do diskuze třídy. Jako nejvhodnější postup se proto ukázalo spíše řízení diskuze tím, že při každé otázce byly žáci dotázáni na krajní hodnoty a následně na středové, jak je popsáno v osnově lekce. Odpověď nemusí být nutně správně jedna konkrétní, důležité je, jak ji žáci vysvětlí, např. velikost může být správná prostřední při srovnání se stolním počítačem, ale největší při srovnání se smartphonem. V případě dominantního člena skupiny (např. „*Já jsem dal…*“) je důležité zapojit ostatní členy („*Co by dali ostatní?*“ nebo „*Co si o tom myslíš ty, slečno?*“), ale také žáky z jiných skupin, a to nejen v případě špatné odpovědi dané skupiny. Zapojování ostatních skupin není nutné při každé otázce, ale vede k podpoře pozornosti v průběhu celé diskuze.

Během řešení odpovědí a pro podporu srovnání je klíčové daný aspekt prakticky ukazovat, např. při srovnání velikosti položit zařízení vedle sebe a pak otázku zopakovat, aby odpověď nedával lektor, ale stále žáci. Lektor jim jen pomáhá položením zařízení vedle sebe snáz správnou odpověď identifikovat. Je důležité opravdu srovnání, tj. praktické ukázky na minimálně dvou různých zařízeních.

V případě otázek zaměřených na využívání zařízení je důležité, aby lektor zařízení odblokoval a ukázal diskutované funkce. Například v jedné třídě žákyně řekla, že na stolním počítači si může prohlížet hvězdy, ale na tabletu ne, proto lektorka vzala tablet a ukázala aplikaci Night Sky, což žáky zaujalo tak, že se všichni seskupili, aby na displej viděli, včetně toho, že prolézali lektorce pod nohama. Diskuze při nesprávné odpovědi nebylo nutné vyvolávat lektorem, žáci spontánně projevovali nesouhlas a uváděli vlastní zkušenosti, které je vedly k odlišné odpovědi.

I při zadání reflexe je důležitá formulace zadání. Je nevhodné položit otázku typu: „*Které zařízení byste si nejvíc přáli?*" Tato odpověď vede žáky k omezenému uvažování, je často ohraničeno využitím pro hry, ne například pro přípravu do školy, která ještě v tomto ročníku obvykle nevyžaduje samostatnou práci s počítačem. Současně je takto formulovaná otázka negativně hodnocena učiteli, kteří to vnímají jako nátlak na rodiče, kdy žáci po lekci za nimi přijdou s tím, že je lekce navedla k tomu, že jim mají zařízení koupit. V případě sdílení výsledků reflexe se lektor na nevýhody ptá, nepřichází s nimi sám (např. problém s hraním her pro omezování jejich aktivit, kdy by se raději měli věnovat tradičnímu hraní s přáteli). Během sdílení se ukázalo jako klíčové především to, jaké funkce byly ukázány na zařízeních. Právě praktická ukázka, která byla u každé třídy odlišná s ohledem na vývoj diskuze, byla často uváděná u výhod i nevýhod daného zařízení, výrazně častěji než ostatní srovnávané parametry a funkce. To ukazuje význam praktických ukázek, a že právě na ně by lektor měl klást důraz v tom, co především chce žáky naučit.

3.2.2 Desatero bezpečného internetu

Anotace: Lekce si klade za cíl seznámit žáky se základními bezpečnostními principy použití internetu v podobě desatera bezpečného internetu s pomůckou ve formě připodobnění k použití mobilního telefonu a ke komunikaci ve fyzickém prostředí. Vedle toho, že tato pravidla jsou určena k ochraně dětí, jsou žáci upozorněni, že podobně by měli reflektovat vlastní aktivity, protože je tato regulace vyžadována netiketou a v některých případech i zákonem.
Cílová skupina: 2. třída ZŠ
Materiální vybavení: Psací potřeby a volné papíry pro žáky, tabule a fixy, herní plán, barevné magnety (5 různých barev), hrací kostka, pracovní list Komiks pro reflexi desatera bezpečného internetu (jeden pro každého žáka)
Výukové cíle – Žák je po lekci schopen...:

- aplikovat základní bezpečnostní principy při použití internetu;
- vysvětlit důvody omezení při použití internetu pro prevenci ohrožení sebe nebo ostatních.

Spojení s RVP: ČJL-3-1-01, ČJL-3-1-02, ČJL-3-1-03, ČJL-3-1-07, ICT-5-1-02, ICT-5-1-03, klíčové kompetence a průřezová témata

Spojení s NIQUES (informační gramotnost): Formulace problému, posouzení pravdivosti informací, modelování a simulace, plánování postupu řešení, komunikace, vytváření digitální identity, bezpečnost, uplatňování právních norem, každodenní život s technologiemi

Výukové aktivity dle E-U-R:

- evokace: Vennův diagram k činnostem na různých zařízeních,
- uvědomění: znalostní hra,
- reflexe: komiksy.

Osnova

Vennův diagram k činnostem na různých zařízeních

Časový plán: 15 minut: 5 min. tvorba grafu, 10 min. diskuze

Cíl lekce, který je v úvodu žákům představen, spočívá v přiblížení bezpečného chování na internetu při využití libovolného typu zařízení. Cílem je seznámení žáků s jejich právy i povinnostmi při využití internetu, aby si uvědomili vhodné reakce na konkrétní situace, se kterými se mohou na internetu setkat. Podobně jako v případě předchozí lekce je nutné žáky upozornit na to, že mohou vycházet ze svých zkušeností, ale i pokud je nemají, budou se mít čím do aktivit zapojit, protože si mohou podobné situace představit při použití mobilního telefonu nebo při komunikaci s cizími lidmi na ulici.

Následně je žákům představena aktivita, kdy jsou na tabuli namalovány dvě kružnice, které se z části protínají. Každá kružnice má jinou barvu, střední, společná část, má třetí barvu. Ke každé kružnici je odpovídající barvou připsán typ zařízení (tablet a smartphone společně k jedné kružnici, počítač k druhé). Žáci jmenují možná využití, ten, kdo první dané využití uvede, rozhodne, kterou barvou, tj. do jaké části grafu, ho má lektor připsat. Žákům lektor připomíná, že pokud s umístěním nesouhlasí, budou mít možnost to vyjádřit po dokončení obrázku.

V průběhu diskuze nad výsledným diagramem jsou šipkami ukázány změny, které z diskuze vzešly, přitom se ukazuje, že většina aktivit by měla být umístěna ve střední části grafu. Diskuze je uzavřena konstatováním tohoto výsledku a toho, že většina činností se odehrává v prostředí internetu, ke kterému zařízení zprostředkovávají přístup. Internet je označen jako důležitá pomůcka pro řadu aktivit, nejen zábavných, ale třeba i pro komunikaci s přáteli a pro učení, proto není řešením bezpečnostních problémů se ho člověk vzdát, ale být na ně připravený a vědět, jak v typických situacích reagovat, což je předmětem následující aktivity.

Znalostní hra typu Člověče, nezlob se

Časový plán: 40 minut

Druhá aktivita je přiblížena pomocí připodobnění ke hře Člověče, nezlob se. Pro tuto aktivitu jsou žáci rozděleni do pěti skupin podle toho, jak sedí. Každá skupina dostane herní figurku odlišné barvy. Ze skupiny postupně chodí jednotliví žáci, hodí

kostkou a posunou figurku o daný počet polí. Následně dostanou otázku, kdy pro odpověď mohou využít pomoc své skupiny, odpověď ale musí vždy říct žák, který házel. Každá otázka je jiná, přičemž skupiny odpovídají na otázku ze série odpovídající postupně pravidlům v desateru bezpečného internetu. Mezi otázkami lektor přibližuje možné reálné situace. Pokud skupina odpoví správně, postoupí o další pole vpřed, pokud na něm stojí figurka, tak ji vyhodí. V případě, že je odpověď špatná, nebo ji skupina nezná, vrací se o pole zpět. V případě, že na něm stojí jiná figurka, tak jsou vyhozeni. Vyhozené figurky musí začít znovu na startu na herním plánu. Vyhrává skupina, které se v časovém limitu pro hru podaří dostat nejdál. Výhrou je výhoda do následující aktivity, kdy si žáci vyberou komiks, který se jim líbí.

Komiksová rada kamarádovi
Časový plán: 20 minut: 10 min. doplnění, 10 min. prezentace
Skupiny si podle pořadí v soutěži chodí vybírat komiksy. Připraveno je 10 hromádek, na každé je jeden typ komiksu, který odpovídá jednomu pravidlu z desatera bezpečného internetu. Poté, co má každý žák svůj komiks (již nepracují ve skupině), lektor představí cíl aktivity. Tím je napsat do poslední části nebo na druhou stranu komiksu, jak by žák poradil svému kamarádovi, kdyby se mu stalo to, co chlapci v příběhu. Poté, co budou mít radu napsanou, mohou si obrázky vybarvit. Následně lektor vždy představí podstatu jednotlivých příběhů a ti, kteří ho měli, uvádí možné rady. Pak lektor přečte odpovídající pravidlo z desatera bezpečného internetu.

Pět otázek s dospělými
1. Jaké má výhody a nevýhody tablet proti stolnímu počítači?
2. Co tě nejvíc baví a nepoužíváš k tomu žádný druh počítače?
3. Co můžeš a co nemůžeš poslat někomu, s kým ses seznámil na internetu?
4. Jak ti může někdo lhát na internetu?
5. Jak ti mohou rodiče pomoci, když se ti na internetu stane něco nepříjemného?

Zkušenosti lektora
Lekce navazuje na předchozí tím, že ukazuje na bezpečné chování žáků při práci s různými typy zařízení. Na to jsou žáci upozorněni pomocí první aktivity, jejímž cílem je ukázat, že stolní počítač či notebook je možné využít pro podobné aktivity jako tablet nebo smartphone. O možnosti zapojení do všech aktivit v lekci bez ohledu na předchozí zkušenosti je důležité žáky ujistit připodobněním k mobilnímu telefonu a reakcím na cizí osoby na ulici. Toto ujištění je vhodné opakovat na začátku lekce i při přechodu na další aktivitu.

Brainstorming přinesl vždy velké množství činností jmenovaných dětmi, i když někdy je nutné jej podpořit otázkami (např. „*Co třeba na počítači dělají vaši rodiče?*“).

Objevovaly se nejen činnosti, se kterými mají žáci osobní zkušenost, jak ukazuje např. uvedení vyplňování faktur. To bylo pozitivní pro rozšíření pohledu žáků nad rámec toho, co jim může internet nabídnout v tomto věku, ale také v čem jim může pomoci v budoucnosti. Jen výjimečně byly uváděny konkrétní služby, opakovaně např. YouTube, Facebook, Google, Skype, příp. funkce, např. Bluetooth. V takovém případě je nutné žáka, který danou službu uvedl, nechat specifikovat, jak funguje. Toto vysvětlení by nemělo narušit brainstorming, ale následovat až po něm v rámci diskuze. Při diskuzi je pro další aktivitu důležité najít spojení s e-mailem, aby mohlo být vysvětleno, jak funguje e-mail a jeho přílohy, což je připodobněno k posílání dopisu prarodičům, ke kterému mohou děti přiložit svůj obrázek. V případě, že žáci diskutují příliš dlouho o umístění služby, přebírá po krátké výměně názorů slovo lektor, který vysvětlí, proč by měla být v určité části.

Rozhodně je nutné vyvarovat se konstatováním typu „*všichni víte...*". Žáci se často obávali vyjádřit svou neznalost internetu, případně když ji vyjádřili, tak se cítili zesměšňováni těmi, kdo tuto znalost měli. Důležité je, aby lektor vyjádřil, že se nejedná o problém, ale přitom potřebnou informaci vysvětlil. V případě, že se některé dítě vyjádří posměšně vůči jinému, je vhodnou reakcí lektora tomuto žákovi pokládat doplňující otázky k tomu, jak daná služba funguje, až narazí na znalostní hranici, což oběma žákům ukáže, že stále je co se učit a není problémem něco nevědět, ale nenaučit se to v okamžiku, kdy je to vhodné.

Při přechodu mezi prvními dvěma aktivitami je důležité upozornit, že internet není lektorem prezentován jako něco negativního, i když se na negativa soustředí. Vysvětleno je to tak, že výhody jsou mnohem lépe patrné, ale s bezpečnostními opatřeními je vhodné pomoci. Například stejně jako přes počítač i přes mobilní telefon nebo na ulici je možné, že žáky kontaktuje člověk, který jim chce ublížit, a rodiče a učitelé je na to připravují tím, že jim vysvětlují, jak by měli reagovat.

V rámci seznamování s desaterem bezpečného internetu formou typických situací bylo nejdříve na vyžádání učitelů využito dramatické výchovy. Problémem ale bylo zadání scény, kdy i v případě čtyřřádkového popisu měli žáci problém s přečtením a pochopením. I přes tento problém učitelé u metody chtěli zůstat i za cenu omezeného dopadu, až po urgenci lektorky souhlasili se změnou na znalostní soutěž, kdy nejsilnějším argumentem byla kvantita znalostí, které bylo možné zahrnout (bez ohledu na to, že se jednalo jen o více variací na malé množství pravidel, které byly součástí scének).

Člověče, nezlob se je dětem dobře známé, výjimky, které hru neznají, ji rychle pochopí, k čemuž pomáhají ostatní členové jejich skupiny. Je vhodné, aby lektor měl dopředu napsané pořadí barev, aby se nepletl. Původně bylo vytvořeno 50 otázek, pro každou skupinu jedna otázka z každé série odpovídající pravidlu v desateru bezpečného internetu. Ukázalo se ale nereálné projít takové množství otázek, proto jsou v jejich seznamu (Příloha 2.2) ponechány otázky, které by měly být položeny, a zbývající jsou zařazeny do seznamu náhradních otázek v případě časové rezervy.

Přestože je většina otázek zjišťovacích, ukázalo se, že rozhodně nebyly pro žáky bezproblémové. Přesto, že odpověď hledala celá skupina, se přibližně jednou, někdy i dvakrát během každého kola objevila špatná odpověď. Soutěž proto neprobíhá jen pokládáním otázek a odpovědí, ale také krátkými vstupy lektora, který po odpovědi (každé nesprávné a některých správných) doplní další informace a příklady reálných situací. Například u otázek k léčení malwaru může být uvedena paralela k tomu, kdy je žák nemocný, což mohou řešit rodiče, pokud je to lehčí nemoc, v případě většího problému jdou k expertovi, který ho vyléčí – podobně je tomu u nákazy počítače. Nesprávné odpovědi ukazují, že i když žáci mají zkušenosti s počítači a internetem, je dobré je s bezpečnostními pravidly seznamovat.

Žákům z každé skupiny je během prvního kola vhodné zopakovat možnost poradit se se skupinou, toho pak žáci dobře a aktivně využívají. Pohyb mezi herním plánem a skupinou ukazoval motivaci žáků, protože téměř všichni běhali (pokud jim to prostor umožnil). Silný vliv mělo vyhazování figurek, každé vyhození vyvolávalo bouřlivou reakci žáků, jejichž figurka se vracela na start, i ostatních skupin, které se radovaly ze zlepšení svého pořadí. Kompetice mezi skupinami byla patrná nejen z těchto reakcí, ale i z toho, že při poradách skupin nad odpovědí se žáci snažili, aby je zástupci ostatních skupin neslyšeli.

Při výběru komiksu jsou sice skupiny posílány postupně, lektor ale nečeká, až si vyberou všichni jejich členové, protože často je tento výběr dlouhý. Po krátkém okamžiku proto byla poslána k výběru další skupina, i když u nabídky komiksů ještě byli žáci z předchozí skupiny. To pomohlo urychlení výběru. Při samostatné práci žáků bylo důležité mezi nimi procházet a připomínat jim, že nejdříve mají vymyslet radu, až pak kreslit. Pokud žák řekl, že přemýšlí nad radou a během toho kreslí, měl by jej lektor pomocí diskuze navést k odpovědi. V rámci tohoto návodu je vhodné připomínat odpovědi z předchozí aktivity. Sdílení bylo bouřlivé, problém byl v okamžiku, kdy každý chtěl říct svou radu. Proto je vhodné před zahájením sdílení upozornit, že ke každému příběhu bude dán prostor jen pro rady tří dětí, které se přihlásí nejrychleji.

Z komentáře učitelů všech ročníků 2. tříd z jedné školy, který byl zaslán po lekci, vyplývá, že učitelé viděli zájem žáků, což je samotné vede k pozitivnímu hodnocení lekce. Učitelé po skončení lekce pozitivně hodnotili její obsah, který byl dle jejich názoru přizpůsoben věku žáků, a také formu, kterou považují za zábavné procvičování získaných informací.

3.2.3 Digitální stopy v síti

Anotace: Lekce představuje základní principy fungování internetu, které se odrážejí do problematiky dostupnosti digitálních stop a jejich šíření. Řešeny jsou otázky, jak se informace na internet dostávají a jak se mohou šířit ať už prostým

kopírováním souboru nebo sdílením na sociálních sítích a také jaké důsledky může mít nevhodné nakládání s digitálními stopami, včetně možnosti zjistit autora daných informací, i když použije přezdívku. Klíčovou složkou je upozornění na možnosti, jak šíření digitálních stop omezit. Následně jsou žáci seznámeni s neustálým vývojem spojeným se zánikem žádoucích informací na internetu, ale i možným zachováním těch nežádoucích a je vytvořena časová kapsle toho, co dnes považují na internetu za nejvíce hodné zachování.

Cílová skupina: 3. třída ZŠ

Materiální vybavení: Psací potřeby a volné papíry pro žáky, tabule a fixy, papírová krabička nebo obálka na časovou kapsli, komiks (jeden pro každého žáka), možné rekvizity na scénky (klobouk, paruka...)

Výukové cíle – Žák je po lekci schopen...:

- uvědomit si omezené možnosti zachování nebo smazání digitální stopy;
- vyjmenovat různé způsoby šíření informací na internetu, včetně šíření přes sociální vazby;
- popsat praktické příklady možných důsledků nevhodného sdílení informací na internetu,
- vysvětlit význam pozitivní digitální stopy a uvést příklady možných informací v jejím rámci.

Spojení s RVP: ČJL-3-1-01, ČJL-3-1-02, ČJL-3-1-03, ČJL-3-1-07, ČJL-3-1-11, ICT-5-1-02, ICT-5-1-03, ICT-5-2-03, klíčové kompetence a průřezová témata

Spojení s NIQUES (informační gramotnost): Formulace problému, posouzení pravdivosti informací, modelování a simulace, plánování postupu řešení, komunikace, vytváření digitální identity, bezpečnost, uplatňování právních norem, etika zacházení s informacemi a netiketa, každodenní život s technologiemi

Výukové aktivity dle E-U-R:

- evokace: šibenice s pojmy z internetu,
- uvědomění: hraní příběhů,
- reflexe: časová kapsle.

Osnova

Šibenice s pojmy z internetu

Časový plán: 20 minut

Lekce je zahájena již s připraveným zadáním šibenice, na tabuli rozdělené na tři části jsou pole pro všechna tři slova pro každou skupinu. Po představení tématu lekce jsou žáci rozděleni na tři skupiny podle toho, kde sedí, aby se nemuseli přesouvat a skupiny byly stejně velké. Následně je položen dotaz na to, kdo zná hru šibenice. Žák, který se první přihlásí, je vyzván k představení pravidel. Lektor doplní, že před tipem písmene se má skupina poradit, protože první, které zazní, je vyhodnoceno, ať ho řekne kdokoli ze skupiny. Současně jsou žáci vyzváni, aby se radili nad písmenem, když hádají ostatní, aby mohli písmeno zkusit hned, jak

bude jejich skupina na řadě. Také by se ale měli dívat na ostatní slova, která jim mohou napovědět, z jaké oblasti bude jejich slovo.

Tipovaná písmena lektor zapisuje na tabuli, aby je žáci netipovali znovu. Pro každé kolo se tvoří nová šibenice. Když se zvyšuje náskok některé skupiny, nebo se blíží konec aktivity, dostává skupina od lektora nápovědy („*Zkoušeli jste všechny samohlásky?*“ nebo „*Vidíte slovo jiné skupiny, tak co by mohlo být to vaše?*“). Poté, co jedna skupina vyhraje, ostatní slova lektor dopíše na tabuli, nečeká se na dokončení všech.

Slova musí mít podobnou obtížnost pro stejná kola:

1. kolo: video, fotka, profil;
2. kolo: WhatsApp, YouTube, Facebook;
3. kolo: kamarádi, učitelka, kdokoliv.

Když jsou všechna slova napsaná na tabuli, lektor vysvětlí jejich význam pro lekci. První řádek je zaměřen na to, co může být o člověku na internetu, druhý uvádí služby, kde mohou být informace dostupné, a třetí, kdo se k nim může dostat. Přitom neplatí, že by byly spojené jen pojmy v rámci sloupců, naopak vše může být kombinováno se vším, např. k fotce na Facebooku se může dostat i paní učitelka. Kdo se k danému obsahu dostane, může být omezeno, ale jen částečně, protože přátelé mohou bez souhlasu sdílet obsah s dalšími lidmi. Proto člověk nikdy nemá jistotu, kdo všechno se k informaci může dostat ani že je možné zpětně ji zcela z internetu odstranit. Vítězná skupina získává výhodu v tom, že si první losuje obálku do další aktivity.

Hraní příběhů

Časový plán: 45 minut: 15 min. příprava, 30 min. scénky s diskuzí

Každá skupina z první aktivity se dle své volby rozdělí na poloviny a vylosuje si obálku, ve které je pro každého člena stejný komiks. Žáci mají za úkol zahrát scénku, která je zachycena v komiksu. Ten mohou, ale nemusí číst. Příběh si také podle svého zájmu mohou upravit. Doporučeno je, aby využili vlastní zkušenosti z práce s internetem. Poté, co jsou spokojeni s přípravou v rámci času, se mohou bavit o tom, co mělo dítě v příběhu dělat jinak.

Poté, co skupina zahraje svůj příběh, lektor zopakuje podstatu příběhu a vyzve všechny žáky (nejen skupinu, která hrála), aby řekli, co bylo v příběhu špatně a co by bylo správné udělat. Po diskuzi žáků opět shrne základní bezpečnostní opatření:

1. Člověk, o kterém si nejsi jistý, že ho znáš opravdu dobře a ne jen z internetu, by neměl nikdy dostat tvou fotku, video ani adresu a telefonní číslo. Nevíš, kdo se skrývá za monitorem.
2. Když na internetu něco sdílíš, přemýšlej, jestli nemůžeš mít problém z toho, že někdo uvidí, že se ti líbí něco špatného. Když na internetu něco napíšeš, není tě u toho vidět. Přemýšlej, jestli to někdo nemůže pochopit jinak, než jsi to myslel.

3. Než o někom na internetu něco napíšeš, sdílíš s ním fotku nebo video, přemýšlej, jestli by ti nevadilo, kdyby totéž někdo sdílel o tobě nebo o někom, na kom ti záleží. Každému může ublížit něco jiného.
4. I když na internetu není těžké lhát a vytvořit si falešný profil, specialisté třeba u policie přesto dokážou zjistit, kdo na internetu něco psal nebo nahrál fotku nebo video.
5. Když něco na internetu uděláš, vždycky to někdo může zkopírovat nebo sdílet s dalšími lidmi a nikdy nemůžeš mít jistotu, že se k tomu dostane jen ten, kdo chceš, nebo že jsi to smazal všude, kam se to dostalo.
6. Přemýšlej nad tím, že na fotce nebo videu s tebou může být to, co za 10 let může vidět kdokoli. Co je na internetu se totiž může objevit i po letech, i když si myslíš, že už je to zapomenuté.

Časová kapsle
Časový plán: 5 minut příprava, 5 min. sdílení
Poslední scénka v předchozí aktivitě vede v rámci diskuze k přemýšlení nad budoucností. Na to je zaměřena i poslední aktivita, odráží se ale v ní i témata ostatních příběhů, např. že by žáci nechtěli, aby zůstalo na internetu, jak si dělají legraci z někoho jiného. Cílem poslední aktivity je, aby se žáci zamysleli nad tím, co je nebo by o nich mohlo být aktuálně na internetu, a co z toho by si přáli, aby tam bylo nebo naopak nebylo i za 10 let. Vyjádřit to mohou tak, že to napíší, nakreslí nebo jakkoli jinak zaznamenají, aby to při otevření kapsle poznali. Žáci jsou srozuměni s tím, že jejich výsledky budou umístěny do časové kapsle, kterou si odnese paní učitelka, a tato kapsle bude otevřena až ve chvíli, kdy budou opouštět školu.

Diskuze je zahájena konstatováním, že internetu a osobním informacím na něm se nelze vyhnout, jde ale o uvážlivost před tím, než jsou na něj informace nahrány. Žáci jsou vyzváni ke sdílení svých produktů s tím, aby vysvětlili, proč vybrali právě dané informace.

Pět otázek s dospělými

1. Co můžeš a co nemůžeš poslat někomu, s kým ses seznámil na internetu?
2. Jak ti může někdo lhát na internetu?
3. Kdo se může dostat k tomu, co pošleš přes internet?
4. Jak můžeš smazat něco, co jsi jednou nahrál na internet?
5. Jak ti mohou rodiče pomoci, když se ti na internetu stane něco nepříjemného?

Zkušenosti lektora

Přesto, že sociální sítě by měly být využívány až staršími dětmi, jak ukazují výzkumy (kap. 1.2.1) pracují s nimi i mladší děti. I pokud je žáci nevyužívají, cílem lekce je připravit je na práci s těmito službami, ideálně ještě před jejím zahájením. Současně téma lekce, sociální sítě a digitální stopy, jejich vznik, šíření a omezené smazání,

vzešlo z požadavku z první zapojené školy (Masarykova základní škola v Poličce). Přípravu na budoucí činnosti na internetu a Facebook (resp. obecně sociální sítě) jako potenciálně využitelnou službu, ne službu, kterou by měli již znát, je vhodné zdůraznit na začátku lekce jako její cíl.

Při šibenici je důležité značit nesprávně hádaná písmena, jinak je žáci stále opakují. Stejně tak popsané pomůcky při rostoucím rozdílu mezi skupinami jsou důležité, protože při překročení určité úrovně žáci ztrácí motivaci. Pro její udržování je také vhodné připomínat, že každá skupina má některé slovo o trochu náročnější než ostatní. Současně by ale žáci neměli mít pocit většího rozdílu z hlediska zadání, slova by měla být stejně dlouhá (delší maximálně o jedno písmeno) a rozdíly v náročnosti by měly být co nejmenší. Význam řádků není vhodné vysvětlovat před aktivitou, ale až v rámci diskuze po ní. Dokud žáci slova nevidí, vysvětlovaný význam si nezapamatují a zopakování je již nebaví. Po vítězství jedné skupiny není dobré pokračovat, protože ti, kteří již soutěž dokončili, nevěnují ostatním pozornost. Doplnění zbývajících slov lektorem také sníží časovou náročnost aktivity. V rámci komentáře lektora spojujícího první a druhou aktivitu je vhodné upozornit na to, že nejde jen o to, s kým dané informace samy děti sdílí, ale že toto sdílení mohou iniciovat i jiní lidé.

Příběhy byly nejdříve zadány dětem tak, že každý dostal krátký text s verzí příběhu pro svou postavu, následně pak krátký text (cca 4–5 řádků) stejný pro každého pro představení podstaty příběhu. Obě varianty byly ale pro děti příliš náročné pro převedení do scénky. Po zvážení velkého zájmu učitelů o formát dramatické výchovy byly vyzkoušeny komiksy, kdy děti mohou jen zopakovat to, co vidí. Tento způsob se ukázal jako efektivní, i když některé skupiny měly i s tímto drobné problémy a v rámci přípravy potřebovaly asistenci lektora, který jim pomohl pochopit podstatu příběhu a přečíst jejich repliky. Zásah lektora byl někdy potřebný i při domlouvání, kdo bude mít kterou roli.

Komiks je nutné vytisknout dost velký, aby děti neměly problémy se čtením malých písmen. Každý komiks by měl být o velikosti stránky A4. Čísla u komiksů uvádí jejich pořadí, které lektor vždy vysvětlí. Vyzdvižení podstaty příběhu a základního bezpečnostního opatření lektorem je také klíčové, protože ne vždy je to ze scénky patrné a žáci, kteří příběh hrají, se více soustředí na hraní, příp. čtení než na obsah. V rámci hraní je možné postavy podpořit rekvizitami. U menších tříd je pro každý příběh ve skupině malé množství herců, jedno dítě pak zastává více rolí. Při hraní je ale změna postavy špatně identifikovatelná diváky, kteří příběh neznají. Současně žáci, pokud nemají zkušenosti z dramatického kroužku, mají problém s přizpůsobením příběhu, takže dodržují například i pohlaví postav, takže chlapci hrají dívky a naopak. Řada dětí to zvládla vtipně a bavila tím i spolužáky, méně zdatní žáci ale jen těžce předčítali to, co měli uvedeno v zadání, a ostatní je brzy přestali sledovat. Proto je důležité, aby příběhy byly co nejkratší.

Při zadání časové kapsle je důležité upozornit na možnost pozitivní digitální stopy, která může prezentovat jejich kvality. Vhodné je žákům uvést několik příkladů informací, které o nich na internetu mohou být, např. jejich fotka po výhře soutěže v kroužku, video na téma moje rodina, které vytvořili do školy, profil v jejich oblíbené hře apod. Na dětech pak je jen rozhodnutí, zda danou informaci chtějí umístit do sektoru, co na internetu má být nebo co tam být nemá. Samozřejmě si mohou vymyslet i vlastní informaci, kterou na pracovní list zaznamenají. Žáci musí mít dostatek času na dokončení svých produktů, jinak to vnímají negativně, že musí odevzdat do kapsle list, se kterým nejsou spokojení. V případě, že větší množství žáků chce dál na produktu pracovat, lektor učiteli předá nezalepenou obálku (časovou kapsli) s informací, do kdy musí žáci produkty dokončit a odevzdat učiteli, který obálku zalepí a uschová. I nedokončená díla odnáší paní učitelka, aby nedošlo k tomu, že se některé ztratí. Krabička se dětem jako kapsle líbí více, pokud je ale problém s jejím získáním, funkci může dobře splnit i větší obálka. Protože produkty jsou uzavřeny, je vhodné pro další práci ve třídě dát paní učitelce vytisknutý seznam pravidel bezpečného chování, která byla předmětem jednotlivých scének.

Učitelé i tuto lekci hodnotili pozitivně, především vítali „*velice zajímavé a přínosné modelové situace*“. Současně se ale potvrdil vliv prostředí na hodnocení lekce, které bylo poznamenáno chladem v místnosti během výuky. To se více promítlo do názoru učitelů než žáků, ale i ti tento nedostatek v rámci pozorování uváděli.

3.2.4 Bezpečnost osobních informací (Kdo je za monitorem?)

Anotace: Komunikace přes internet je běžnou součástí života dospělých, ale mnohem více dětí a dospívajících, proto jsou někdy označováni jako net generation. Stejně jako v reálném prostředí se i v tom elektronickém seznamují s novými lidmi. S ohledem na malou životní zkušenost ale hůře rozeznávají varovné signály v komunikaci s internetovým známým. Proto jsou náchylnější k problémům, které mohou zasáhnout i dospělé. Lekce pomůže s využitím individuální soutěže pochopit základní problémy komunikace přes internet s neznámými lidmi a vyzkoušet si vhodné reakce při komunikaci s internetovým známým. Cílem je upozornit na obvyklé postupy pro zjišťování zneužitelných osobních informací, zejména těch, které vedou k identifikaci ve fyzickém prostředí.
Cílová skupina: 4. třída ZŠ
Materiální vybavení: Psací potřeby a volné papíry pro žáky, tabule a fixy, dvě místnosti (ne vzdálené), placky nebo lístky pro identifikaci v soutěži (jedna pro každého žáka), pracovní list Tabulka zjištěných identit (jeden pro každého žáka), pracovní list Když se mě někdo zeptá... (pro skupiny), seznam pravidel v soutěži (zavěšený nebo promítaný v každé místnosti), možné lístky s obvyklými komunikačními službami

Výukové cíle – Žák je po lekci schopen...:

- rozpoznat obvyklé postupy zjišťování osobních informací v komunikaci na internetu;
- kategorizovat informace podle úrovně možného zneužití, zejména ve vztahu k fyzické identitě;
- formulovat vhodné odpovědi na osobní otázky od internetového známého, včetně odmítnutí sdělit zneužitelnou informaci o sobě či jiném.

Spojení s RVP: ČJL-5-1-03, ICT-5-1-02, ICT-5-1-03, ICT-5-2-03, ČJS-5-2-01, ČJS-5-2-02, klíčové kompetence a průřezová témata

Spojení s NIQUES (informační gramotnost): Formulace problému, získání informací, posouzení relevance a úplnosti informací, posouzení pravdivosti informací, analýza získaných informací, modelování a simulace, plánování postupu řešení, vytváření originálního díla, komunikace, vytváření digitální identity, bezpečnost, uplatňování právních norem, etika zacházení s informacemi a netiketa, každodenní život s technologiemi

Výukové aktivity dle E-U-R:

- evokace: brainstorming,
- uvědomění: soutěž v odhalování identity a přednáška,
- reflexe: Když se mě někdo zeptá.

Osnova

Brainstorming

Časový plán: 15 minut: 5 min. způsoby komunikace na internetu, 10 min. vyhodnocení

Na začátku lekce jsou děti povzbuzeny, aby se podělily o to, co znají. Uvolní se tak obavy a děti se zapojí do lekce, vytváří si ji do značné míry samy. Je nutné, aby lektor dodržoval pravidla brainstormingu. Brainstorming je zahájen otázkou: Jakými způsoby se můžete s někým bavit pomocí internetu? Poznamenává či dává na tabuli připravené názvy na lístcích bez komentářů. Shromáždí vše, co děti jmenují, že používají nebo vědí, že to někdo v jejich blízkosti používá. Pokud se děti kritizují, lektor komunikaci usměrní a povzbuzuje do jmenování dalších služeb. Pokud se neobjevují další nápady, dodá nápovědu směřující k připraveným typům (ale nejmenuje je), např. pokud chce slyšet videohovory, tak se zeptá, jestli děti znají něco, pomocí čeho by přes internet s někým mohly mluvit a současně ho vidět. Není nutné, aby se na tabuli objevilo vše připravené, základní kategorie by ale měly být zastoupeny.

Po určeném časovém limitu převezme slovo lektor. Zeptá se žáků, které ze služeb někdo nezná. Ten, kdo ji uvedl v brainstormingu poté vysvětlí, jak služba funguje. Následně lektor s dětmi služby kategorizuje a kategorie pojmenovává (např. Instant Messaging, sociální sítě...) s vysvětlením toho, jakou formu komunikace každá kategorie umožňuje. Pomůckou jsou barvy nápisů. Děti si touto formou uvě-

domí, co vše znají, a současně si doplní nebo opraví své znalosti. Nakonec lektor upozorní na paralelu s reálným prostředím, kdy na internetu, stejně jako na ulici či v kroužku, je možné poznávat nové lidí. Většina služeb umožňuje komunikaci lidí, kteří se dříve neznali, a současně se obvykle navzájem nevidí. Podobnou situaci bude simulovat soutěž ve fázi evokace.

Soutěž v odhalování identity internetového známého
Časový plán: 25 minut: max. 5 min. vysvětlení pravidel, 20 min. soutěž se simulací komunikace na internetu pro poznání druhého člověka
Po vysvětlení pravidel jsou děti rozděleny losováním na dvě skupiny. Každé dítě si vylosuje jedno číslo či písmeno, které by nikdo jiný neměl vidět. Žáci s čísly se přesunou do druhé místnosti. Hra spočívá v posílání dotazů a odpovědí mezi jednotlivci, kdy cílem je zjistit identitu co nejvíce dětí z druhé skupiny (za každou správnou získá bod), a současně chránit vlastní identitu před odhalením (za každé odhalení ztratí bod). Dopravu zpráv mezi skupinami zajišťuje lektor, ideálně s jedním pomocníkem (učitel, knihovník).

Aby hra fungovala, jsou představena pravidla komunikace, která jsou během celé soutěže viditelně napsána v obou místnostech, spolu s příklady možných otázek (např. *Jsi kluk nebo holka? Jaký je tvůj oblíbený zpěvák? Co hraješ na internetu?*). Děti se označují vylosovaným číslem či písmenem (prezentováno jako jejich „nick" či přezdívka), jsou zakázána veškerá jména, a to nejen dětí samotných. Není možné položit otázku např. na jméno nejlepšího kamaráda. Protože v elektronickém prostředí plní podobnou funkci jako jméno e-mailová adresa, ze které je navíc často jméno rozeznatelné, jsou zakázány i tyto informace. Další pravidlo je v příkazu, že je nutné odpovídat pravdu, a to na každou otázku. Při nepravdě či neposkytnutí odpovědi by totiž hra neměla smysl, protože by nebylo možné nikoho odhalit.

Aby bylo možné rozlišit, kdo si s kým píše (v prezentaci k dětem: „*komu má internet doručit zprávu a odpověď*"), je každá komunikace nadepsána odpovídajícím číslem a písmenem, např. 1A, tedy dítě 1 si píše s dítětem A. Pro zjednodušení každé dítě dostane první papír ke komunikaci nadepsaný, čísla píší písmenům na stejné pozici v abecedě (1-A), písmena číslům o jedno vyšším (A-2). Při zahájení má tedy každé dítě dva komunikační partnery, v případě lichého počtu žáků má jedno dítě tři a jedno jednoho. To se vyrovnává tím, že následně je možné zahájit libovolný počet komunikací, podobně jako na internetu. Přitom je nutné upozornit na omezený čas pro soutěž, tedy omezené množství položených otázek. Pokud tedy žák píše více než 3–4 partnerům, obvykle jim nestihne položit tolik otázek, aby zjistil, o koho se jedná. Dětem je při prvních dvou kolech opakováno, že mají vždy napsat odpověď a jednu vlastní otázku. Lektor a pomocník, kteří zprávy přenáší, od dveří vyhlašují písmena či čísla, pro která mají zprávu, pohyb dětí je žádoucí. Současně je lektor k dispozici pro řešení problémů a nejasností. Pokud si komunikující myslí, že toho druhého poznali, stále nepíší jméno, ale *znám tě*, ko-

munikace končí, až si toto napíší oba. Aby nezapomněli, koho odhalili pod jakým označením, zapisují si jména do tabulky (viz pracovní materiál *Tabulka zjištěných identit*).

Děti jsou na začátku upozorněny, že soutěží každý za sebe, nesmí si tedy prozrazovat zjištěné identity (lektor vysvětlí dětem, že si samy kazí hru). Není ale dětem bráněno v komunikaci v rámci skupin, pokud sdílí tipy na otázky a odpovědi. V průběhu aktivity i bez zásahu lektora pokládají děti otázky, které znají z internetového prostředí. Také si samy, nebo díky jiným členům skupiny uvědomí, jaké informace je prozradí a jak odpovídat, aby k tomu nedošlo (např. při otázce na bydliště odpoví ČR, ne adresu). Lektor otázky (mimo ukázek), ani odpovědi nenapovídá. Přibližně 5 minut před koncem lektor upozorní, že nese poslední otázky, na které dostanou jejich odesilatelé odpovědi. Po doručení posledních odpovědí si děti doplní tabulky identit podle svého přesvědčení a sejdou se opět v jedné místnosti.

Vyhodnocení s přednáškou pro komparaci s prostředím internetu

Časový plán: 20 minut: 10 min. vyhodnocení, 10 min. interaktivní přednáška k pravidlům

Soutěž je vyhodnocena tak, že lektor postupně říká všechna čísla a písmena. Komu patří, ten řekne své jméno. Následně se přihlásí ti, kteří mají v tabulce správné jméno u správného označení, aby bylo jasné, kolik bodů se odečítá za odhalení. Děti se třemi nejvyššími počty bodů získají drobnou odměnu (placky s motivy IT, např. tablet, zavináč, logo Facebooku).

Po vyhodnocení lektor stručně připomene, jaká byla pravidla pro soutěž a proč. Přitom každé pravidlo postaví do protikladu s internetem i fyzickým prostředím a upozorní tak děti na to, co poznaly v soutěži jako problém, a jak se mu mohou v praxi vyhnout. V souladu s principy aktivního učení jsou podporovány vstupy dětí se sdílením jejich zkušeností ze soutěže i z reálného života.

Pravidlo zákazu jmen a e-mailů lze spatřovat v jejich identifikační funkci. V tradičním i internetovém prostředí je s nimi snazší dohledat další informaci či přímo člověka (např. s využitím telefonního seznamu či profilu na Facebooku) nebo se na další informace zeptat (např. jiná reakce na internetu i ve škole bude, pokud se zeptám na jméno nebo pokud se zeptám na přezdívku s tím, že třeba má rád kočky). Jména a e-mailové adresy propojují profily na různých službách internetu, proto je dobré si dávat pozor, jaké informace je s nimi možné spojit. Další pravidlo, které spočívalo v nutnosti říkat pravdu, neplatí v tradičním i internetovém prostředí. Současně je na internetu mnoho komunikace veřejné, proto může kdokoli vysledovat způsob komunikace a témata mezi dětmi a s jejich využitím si budovat důvěru a zjišťovat další informace. Nelze spoléhat na pravdu od internetového kamaráda, internet totiž umožňuje mnohem snazší lhaní i v tom, co je ve fyzickém prostředí zjevné, např. věk. Na závěr je pozitivně ukončeno neplatností posledního

pravidla, a to nutnosti odpovídat. Dětem je dobré zdůraznit, že nikdo je nemůže nutit sdělit informaci, kterou poskytnout nechtějí. Současně existují situace, kdy je zjevné, že něco není v pořádku. Mnoho z nich lze připodobnit k tomu, co děti rodiče učí s ohledem na setkání s neznámým člověkem na ulici (co mu neříkat, nikam s ním nechodit apod.).

Setkání na ulici a soutěž v lekci by měly dát dětem nápovědu, jakou informaci mohou poskytnout. Pokud se jich internetový známý na něco zeptá, měly by si říct, jestli by je odpověď odhalila v soutěži a jestli by ji poskytly neznámému člověku na ulici. Pozor by si měly dávat především na to, co je může pomoci najít ve fyzickém prostředí, např. adresa školy, jméno učitele, telefonní číslo, fotky, celé jméno. Důležité je také si uvědomit, že stejný přístup by měl být zachován, ať je předmětem dotazování člověk sám nebo jeho známý. Rozhodování si děti vyzkouší v rámci reflexe v klidu a bezpečí knihovny.

Když se mě někdo zeptá
Časový plán: 15 minut: 5 min. vyplňování, 10 min. sdílení s diskuzí
Každá skupina po 3–4 dětech dostane jeden pracovní list *Když se mě někdo zeptá*. Společně do tabulky udělají šipky od každé otázky v prostředním sloupci ve směru podle toho, jestli danou informaci odmítnou sdělit, nebo ji poskytnou. Lektor by měl vybrat min. tři otázky pro demonstraci toho, že na většinu lze odpovědět obecně (např. bydlím na Moravě), ale ne konkrétně (např. adresa). Upozorní také na otázky, které by děti měly varovat (např. Jsi doma sám/sama?).

Pět otázek s dospělými
1. Jak se bavíš s jinými lidmi přes internet?
2. S kým se tak bavíš?
3. Co chceš, aby o tobě hodně lidí vědělo (např. díky zdi na Facebooku)?
4. Jak by ses bavil přes internet s člověkem, kterého jsi nikdy neviděl?
5. Když se ti ozve někdo známý s novým profilem, jak zjistíš, že je to opravdu ten, kdo myslíš?

Zkušenosti lektora
Lekci se osvědčilo zahájit otázkou: „*Kdo z vás nikdy nebyl na internetu?*“ Většina žáků se zasměje, vytvoří se pozitivní a otevřená atmosféra, kdy děti samovolně začnou uvádět své zkušenosti. Současně se ale téměř ve všech třídách objevil někdo, kdo ještě nikdy na internetu nebyl, příp. S ním má minimální zkušenosti. To je způsobeno jak finančními důvody, tak i zákazy rodičů, kteří nechtějí, aby děti v tomto věku trávily volných čas na internetu, ale vedou je k jiným činnostem. Rozhodně proto není možné v žácích nastavit pocit, že lekce pro ně bude problémová, naopak je vhodné vyzdvihnout, že na tom není nic špatného, protože mohou získat plno krásných zážitků, které by je jinak minuly. Současně je ale dobré, aby i oni

byli připraveni na to, že jednou s internetem budou pracovat, minimálně ve škole, proto je dobré si teď vyzkoušet, jak se na něm vhodně chovat. Také díky práci ve skupině jim určitě některý kamarád pomůže, aby lekci zvládli bez problémů.

Pro fázi evokace je důležitá lektorova orientace v nejpoužívanějších službách internetové komunikace, zejména v online hrách. Hry a komunikační možnosti populární v době přípravy lekce jsou uvedeny v materiálu *Mapa komunikace*, nejpozději po půl roce je vhodná aktualizace. Pokud nemá lektor možnost zjistit trendy v této oblasti, může se nechat poučit dětmi. Toto poučení nesníží jeho odbornost, pokud projeví zájem a obecnou orientaci (např. dobře zná některé služby, i když ne všechny). Děti často způsob komunikace nedemonstrovali obecným popisem, ale svou osobní zkušeností (např. „*Když hraju Minecraft, tak si vždycky povídám s kámošem ... přes Skype*."). Orientace lektora je patrná pro děti také tím, že má služby připravené na lístcích. Jejich použití je také časově výhodnější. Lístky zvyšují motivaci dětí, pokud mezi nimi najdou oblíbenou hru (dříve Minecraft) nebo službu (aktuálně WhatsApp). Důležité bylo i upozornění, že není nutné jmenovat jen to, co používají, ale i co znají od rodičů nebo sourozenců, proto se děti nemusely bát jmenovat nástroje, u kterých cítí, že by je používat neměly, např. Facebook, kde je věková hranice pro uživatele 13 let. Sdílení zkušeností v dětech povzbudí komunikaci a učení se navzájem. Vždy je totiž součástí třídního kolektivu někdo, kdo s řadou služeb nemá zkušenosti. Návodné otázky se v některých třídách ukázaly jako potřebné, zejména pokud děti dříve nepřišly na možnost jmenovat online hry. Po uvedení několika z nich byl vždy nutný zásah lektora, že her už je dost, ať zkusí i jiné služby.

V souladu s postupy interaktivní hry[397] jsou reprodukovány v hlavní části lekce situace ze skutečného života dětí pro porozumění a nalezení možných scénářů jednání s ověřením jejich důsledků. Pomáhalo říct, že lektor a učitel jsou internet, žáci to pak i komentovali („*dneska je ten internet nějak pomalej*"), a tuto symboliku držet v průběhu celé aktivity (např. pokud někdo zapomněl napsat označení žáka v druhé skupině, tak zprávu odnést a vrátit s tím, že ji e-mail taky vrátí, když není zadaná adresa příjemce). V pravidlech původně nebyly uvažovány e-maily, ale první realizace lekce ukázala, že děti si opravdu spojují aktivitu se zkušenostmi z internetu, protože celý běh byl ovlivněn zjištěním jmen právě z e-mailů. Při zahájení aktivity je vhodné dopsat k pravidlům, jaká čísla a písmena byla zadána (např. 1–13 a A–M), aby bylo jasné, s kým je možné zahájit novou komunikaci (tedy existuje žák s daným označením).

Často žáci nevěděli, jak komunikaci začít, a měli problém s tím, že jim nejsou jasná pravidla. Osvědčilo se spojit je do menších skupinek pro vzájemnou pomoc a dát jim pokyn, ať zkusí poslat zprávu s vzorovou otázkou. Po dvou kolech soutěže již byla pravidla zřejmá. Skupinky téměř vždy vznikly i bez intervence lektora,

397 BELZ 2001, s. 101.

obvykle ve velikosti 2–6 osob, která je vhodná pro interakci[398]. V rámci skupin žáci sdíleli vhodné otázky a odpovědi (např. ukázka z rozhovoru žáků: „*Když se tě zeptaj na bydliště, tak tam dej byt.*“ „*Nebo bydlím v domě.*“ „*Bydlím nedaleko školy*.“) Lektor sloužil i jako rádce, kterého se děti doptávaly, jestli je nově vymyšlená otázka v souladu s pravidly. Často se chodily ptát na otázky, které považovaly za dobře vymyšlené, aby se pochlubily. Děti tak samy přišly na to, jaké postupy je vedou ke stanovenému cíli – odhalení cizí identity a uchování vlastní a sdílely to se spolužáky. Tento tzv. aha-moment přitom kromě efektu učení vede také ke vzbuzení radosti a pocitu, že učení je příjemná věc[399]. Zásadní zjištění tedy nepřišlo od lektorky, ale od vrstevníků, bylo pak zvažováno při vlastní aktivitě. Objevilo se ve všech skupinách, někdy přeneseně z druhé skupiny, když si někdo naopak stěžoval, že určitá otázka či odpověď mu překazila snažení.

V 5. třídě ve srovnání s nižším ročníkem děti více sledovaly jazykové prohřešky. Ve škole byla soutěž tímto poznamenána více a docházelo ke zpomalení komunikace, protože děti strávily více času přemýšlením nad formou než nad obsahem. V knihovně byla soutěž uvolněnější, pomohl tomu také papír A4 bez linek. V 5. třídě se také objevil problém s identifikací ne podle informací, ale podle písma, někteří si to uvědomili již na počátku aktivity a dotazovali se lektorky, jak to vyřešit, přičemž sami nabízeli vlastní řešení – že si zprávy nechají psát někým jiným. Při doručování zpráv se pro označení dětí osvědčily placky, které měly mít připíchnuté viditelně. Současně je na rozdíl od papírků bylo možné využít opakovaně. Žáci 4. tříd ve srovnání s vyššími ročníky byli aktivnější při očekávání zpráv, obvykle běhali po místnosti, aby byli co nejdříve u rozdávání a stihli poslat co nejvíce zpráv. U starších ročníků se více stávalo, že se žák (většinou jen jeden) rozhodl, že mu postačují dvě komunikace, které dostal při zahájení, a nechtěl si přes výzvu lektora vzít prázdný papír a začít psát někomu dalšímu.

Při počítání bodů se osvědčilo mít v ruce tabulku s čísly a písmeny a postupně je překrývat, aby někdo nebyl vynechaný. I když odměna vítězům byla jen symbolická, žáci ji hodnotili pozitivně, pokud se jednalo o placky spojené s IT, ne s knihovnou, ale i o sladkosti[400]. V rámci komentáře po soutěži, jehož funkce je z lekce nejpodstatnější, je zásadní střízlivý přístup ke zneužitelnosti informací. Neměl by být ani příliš striktní, ani benevolentní, aby děti viděly, že bezpečnost v komunikaci lektor bere vážně, ale nesnaží se jim zakázat pro ně nezbytnou součást společenského života, která přispívá k budování jejich postavení v kolektivu a pozitivní digitální stopy. Lektor by měl dále mít přehled o stylu běžné komunikace dětí na internetu, tedy co a komu jsou ochotny sdělit. To lze vysledovat ve veřejné komunikaci dětí anebo zjistit z výzkumů, např. EU Kids Online nebo e-Bezpečí (viz kap. 1.2.1). Srovnání

398 KASÍKOVÁ 1997, s. 38.

399 STEELOVÁ 2007b, s. 9.

400 Vhodnost odměny při aktivním učení zdůrazňuje PETRESS 2008.

s fyzickým prostředím učitelé hodnotili pozitivně, ne výjimečně do výkladu v tomto okamžiku vstoupili a připomněli dětem, že se tomu věnovali v dřívější výuce.

Při reflexi byl zkoušen materiál, kde děti měly samy dopsat informace do polí: Když ode mě někdo chce vědět...:

- ... přestanu se s ním bavit a řeknu to dospělému.
- ... řeknu, že mu to nepovím.
- ... tak mu to řeknu.

Tento způsob byl ale pro žáky příliš náročný, problémem bylo zejména vymyslet informace, ne zařadit je do správného pole. Proto byla vytvořena návodnější tabulka, kde byly informace připraveny a šlo jen o správou reakci, navíc zjednodušenou na dvě varianty. Důležité je při zadání aktivity zdůraznit, že cílem je určit, zda odpovědět (ne jak). To, že lze odpovědět různě, většinou vyjádří samy děti v diskuzi („*Můžu mu říct, že chodím plavat, ale on neví kam*."). Jen výjimečně potřebovaly nápovědu od lektora. Děti ve 4. třídě a některé i v 5. ještě viděli možnost nepoužívat komunikaci přes internet (např. reakce „*Lepší je se s nikým cizím nebavit.*"), s vyšším věkem jim toto řešení ale připadalo stále méně reálné, což potvrdil i akční výzkum (viz kap. 3.3.4). Pro lekci bylo pozitivním zjištěním, že děti se odkazovaly při volbě odpovědi na předchozí aktivitu, kterou proto lze označit za efektivní. Přestože se jednalo o aktivitu, která ukončovala více než sedmdesátiminutový program, děti se soustředily na její průběh a po celou určenou dobu se bavily o otázkách na papíře.

Soutěž pozitivně hodnotili i učitelé, pro které právě tato aktivita je základním přínosem lekce, kterou označili jako zpracovanou adekvátně věku žáků. Lekce, zejména soutěž, byla pozitivně hodnocena i 5. a 6. třídou, včetně realizace místní knihovnicí v Městské knihovně Pelhřimov pro speciální základní školu (dle e-mailové komunikace s Lenkou Havlovou ze dne 19. 2. 2014). Při soutěži často v okamžiku, kdy lektorka upozornila na blížící se konec, chtěly děti pokračovat, případně se ptaly učitelky, zda si soutěž nemohou později zahrát ve škole.

3.2.5 Práce s informačními zdroji

Anotace: Lekce primárně vede žáky k vyzkoušení základních postupů hodnocení informačních zdrojů a k lepší orientaci v elektronických i tradičních informačních zdrojích. Žáci se seznámí s omezeními vybraných typů informačních zdrojů (kniha, časopis, Wikipedie a odborná webová stránka) a základními evaluačními kritérii. Sekundárně jsou rozvíjeny znalosti v aktuálních tématech z informační bezpečnosti, protože při lekci žáci pracují s texty na témata: závislost na informačních technologiích, virální videa, kyberšikana a sociální inženýrství.
Cílová skupina: 5. třída ZŠ
Materiální vybavení: Psací potřeby a volné papíry pro žáky, tabule a fixy, kniha a časopis k řešeným tématům a dva počítače, zadání rychlých špiónů, týmové role

(jedna pro každého žáka), analyzovaný text (jeden pro každého žáka), pracovní list I.N.S.E.R.T. (pro skupinu), pracovní list Hledání informací (jeden pro skupinu), možný plakát s hodnotícími kritérii

Výukové cíle – Žák je po lekci schopen...:

- srovnat výhody a omezení různých typů informačních zdrojů, především s ohledem na jejich důvěryhodnost;
- použít pomůcky pro orientaci v základních typech informačních zdrojů;
- zdůvodnit potřebu hodnocení informací a jejich zdrojů;
- zhodnotit základní charakteristiky důvěryhodnosti informačního zdroje.

Spojení s RVP: ČJL-5-1-01, ČJL-5-1-02, ČJL-5-1-03, ČJL-5-1-04, ICT-5-1-02, ICT-5-1-03, ICT-5-2-01, ICT-5-2-02, ČJS-5-2-01, ČJS-5-2-02, ČJS-5-2-03, ČJS-5-2-04, klíčové kompetence a průřezová témata

Spojení s NIQUES (informační gramotnost): Formulace problému, určení typu informace, získání informace, posouzení relevance a úplnosti informací, posouzení pravdivosti informací, analýza získaných informací, modelování a simulace, plánování postupu řešení, vytváření originálního díla, bezpečnost, ochrana zdraví, uplatňování právních norem, etika zacházení s informacemi a netiketa, každodenní život s technologiemi

Výukové aktivity dle E-U-R:

- evokace: Rychlí špioni,
- uvědomění: I.N.S.E.R.T. a analýza informací v informačních zdrojích,
- reflexe: brainwriting.

Osnova

Rychlí špióni (aktivity)

Časový plán: 10 minut

Lekce je zahájena představením jejího cíle. Ten spočívá v uvědomění si výhod a nevýhod jednotlivých typů informačních zdrojů a zvažování, nakolik jsou informace, které tyto zdroje nabízí, vhodné pro využití právě žáky. Témata, která jsou předmětem řešených textů, uvedena nejsou, protože jejich zaměření je předmětem první aktivity v lekci. Ta spočívá ve variaci na hru Aktivity, resp. výukovou aktivitu Rychlí špióni. Žáci jsou rozdělení na čtyři skupiny. Každá skupina si zvolí svého špióna pro každé kolo, kdy první spočívá v malování („mobilní telefon“), druhé v pantomimě („šikana“) a třetí slovním vyjádření slova bez jeho použití („video“). Lektor stojí před třídou a špiony, kteří k němu doběhnou, seznamuje postupně s hádanými slovy. Způsob vyjádření a hádané slovo jim ukazuje na vytištěném lístku, přičemž lístky pro další kola by špión dopředu vidět neměl.

Poté, co první skupina uhádne všechna tři slova, je hra ukončena. Vítězná skupina zopakuje uhádnutá slova a celá třída je vyzvána, aby na jejich základě definovala, čeho se budou týkat texty v následující aktivitě. Lektor upřesní, že i když předmětem textů jsou různé problémy spojené s internetem a dětmi, klíčovou

složkou lekce je přemýšlení nad zdroji informací, a že obě témata informační bezpečnosti spolu těsně souvisí především právě v hodnocení důvěryhodnosti.

I.N.S.E.R.T.
Časový plán: 20 minut: 5 min. čtení textu, 5 min. vyplňování pracovního listu, 10 min. diskuze
Jako odměna pro vítěznou skupinu je, že si první vybírají obálku. Z každé obálky vysypou žáci nejdříve malé lístky s týmovými rolemi, ideálně aby neviděli, co je na nich napsáno. Každý žák si jednu vylosuje. Poté jsou jednotlivé role vysvětleny. Všichni ve skupině budou číst stejné texty, ale hledač informací se při zpracování soustředí na nalezení odpovědí na položené otázky na pracovních listech. Zapisovatel výsledky značí, ale hledači mohou pomáhat. Prezentující po aktivitě představuje výsledky ostatním, i on může pomáhat při zpracování úkolu, hlavně se ale domlouvá se zapisovatelem, aby z jeho poznámek byl schopný výsledek prezentovat.

Po vysvětlení rolí jsou žáci vyzváni, aby si každý z obálky vzal svůj text (všichni ve skupině mají stejný) a sám si jej přečetl. Nakonec z obálky vytáhnou pracovní list I.N.S.E.R.T., do kterého společně vyplní, co už o tématu věděli, co z článku pochopili, i když to pro ně bylo nové, čemu z textu nerozumí a čemu nevěří. Prezentující pak postupně představí výsledky zpracování a lektor okomentuje to, co zaznělo u částí „nerozumíme“ a „nevěříme“.

Analýza informací v informačních zdrojích
Časový plán: 35 minut: 20 min. vyplňování pracovního listu, 15 min. diskuze
Fáze uvědomění si významu pokračuje prací v různých informačních zdrojích:

Typ zdroje	**Téma**	**Zdroj pro hledání**
kniha	kyberšikana	Bezpečnost dětí na internetu (Eckertová a Dočekal)
časopis	sociální inženýrství	Počítač pro každého čísla č. 12/2014 a 15/2015
web	internetová závislost	Online adiktologická poradna
Wikipedie	virální videa	Wikipedie

S konkrétním zdrojem informací jsou žáci seznámeni lektorem při zadání aktivity, přičemž jsou upozorněni, že při práci na počítači musí pracovat výhradně na uvedených stránkách. Cílem všech skupin je, aby co nejkompletněji vyplnily pracovní list Hledání informací, kdy před zahájením práce jsou jednotlivé položky na listu žákům představeny. Během aktivity lektor prochází kolem skupin a pomáhá jim, když neví, jak postupovat. Po vypršení časového limitu se žáci vrací s pracovními listy na přednáškové místo, aby představili výsledky svého hledání. Po prezentaci každé skupiny následuje diskuze o hodnotících kritériích pro daný zdroj ve vztahu k hledaným parametrům (stáří, autor apod.). Otázky lektor směřuje tak, aby žáci vyjádřili silné a slabé stránky jednotlivých typů zdrojů z hlediska důvěryhodnosti.

Brainwriting
Časový plán: 10 minut: 5 min. brainwriting, 5 min. tvorba seznamu
V reflexi jsou žáci vyzváni, aby se pomocí individuálního brainwritingu zamysleli znovu nad předchozí aktivitou a zkusili sepsat vše, co je podle jejich názoru důležité zohlednit u každého informačního zdroje pro posouzení jeho využitelnosti (především důvěryhodnosti) informací v návaznosti na předchozí aktivitu. Poté jsou žáci vyzváni, aby se podívali na sepsaný výsledek a společně definovali pět nejdůležitějších prvků, na které by se měli zaměřit u každého zdroje, a aby vysvětlili, proč je právě toto kritérium zásadní. Definované prvky jsou sepisovány lektorem na velký papír. Vytvořený seznam dostane učitel po lekci, příp. knihovník může vytvořit vlastní plakát, který srovná při reflexi s vytvořeným seznamem a následně jej dá učiteli pro zavěšení ve třídě.

Pět otázek s dospělými

1. Co je závislost na internetu a jak se jí dá předcházet?
2. Může být kyberšikana, i když si jen děláš legraci z kamaráda?
3. Můžeš si být jistý, že z internetu smažeš video, které jsi tam někdy nahrál?
4. Jaké jsou výhody knížek proti internetu, když děláš referát do školy?
5. Čeho si všímáš na zdroji informací, abys mohl říct, že je pro tebe dobrý?

Zkušenosti lektora
Lekci je vhodné realizovat v prvním pololetí 5. třídy, protože v druhém se postupně snižuje motivace žáků a více se projevuje jejich sebevědomí v práci na internetu, což vede k nižší ochotě zapojení. V rámci evokační aktivity je vhodné ji prezentovat jako hru a využít oba názvy. Aktivity většina žáků zná, ale vždy byli ve třídě jednotlivci, kteří s touto hrou zkušenosti neměli. Proto bylo dobré nechat žáky jejich spolužákům vysvětlit princip hry s tím, že lektor jen doplnil, že proběhnou tři kola, kde každé má formu jiné aktivity a ta je zadána pro všechny skupiny stejně. Důležité je, které skupině se podaří slova uhodnout nejrychleji, což vede k názvu Rychlí špióni. Žáci si název většinou přeloží tak, že je nutné, aby se špión pohyboval rychle, jen výjimečně mezi skupinou a lektorem neběžel. V rychlém pohybu jej také většinou povzbuzovali ostatní členové skupiny. Zda bude pro každé kolo využitý jiný nebo stejný špión, většinou rozhodl lektor až při zadávání aktivity s ohledem na to, jak žáci reagovali na představení hry. Ve většině tříd mělo zájem stát se špiónem více dětí, tak jim to bylo umožněno, v jiných třídách naopak projevovali více komentáře typu „*já to teda nebudu*“. Role evokace je také motivační, proto byla zvolena varianta právě s ohledem na zájem žáků.

V průběhu aktivity je důležité sledovat skupiny, které ji, i když byla prezentována jako hra, vnímaly jako soutěž, proto se snažily odposlechnout skupiny, které byly ve hře dál, a na základě odposlechnutých tipů najít hledané slovo. To by měl lektor korigovat a připomínat, že při tipování mají skupiny pracovat potichu.

Pokud nezasáhne, stěžují si žáci, že ostatní podvádějí, a chybějící vstup lektora má negativní vliv na jejich motivaci.

Při hádání tematického zaměření textů žáci obvykle zůstávají u pojmu šikana, který je jim známý a představuje směr, který je pro ně představitelný jako téma, ve kterém učitelé a lektoři prosazují osvětu. Současně obvykle ví od učitele, že lekce souvisí s internetem, proto často tipovali šikanu na internetu. Přestože na začátku lekce byli seznámeni s cílem spočívajícím v práci s informačními zdroji, spojení s internetem pro ně bylo zajímavější. Pro správné nastavení pozornosti bylo vhodné jim podstatu toho, čemu se budou věnovat, připomenout. Současně byli žáci upozorněni na spojení obou tematických zaměření v informační bezpečnosti, kdy jak v případě nevhodného přístupu ke zdroji, tak i v komunikaci a sdílení na internetu, mohou být poškozeni, i když třeba jen tím, že si z nich ostatní budou dělat legraci kvůli jejich důvěře v chybnou informací.

Aktivita I.N.S.E.R.T. by mohla sloužit také jako evokace. Lekce je pro žáky ale poměrně náročná v množství textu, který mají přečíst, a (ve srovnání s dalšími lekcemi v koncepci) také menší hravostí aktivit. Již začít lekci čtením textu, i když ne dlouhého, na děti nemá dobrý motivační účinek. Vhodnější je aktivizovat je pro lekci pohybem a krátkou a jednoduchou hrou, kdy současně začne spolupracovat skupina, která zůstává ve stejném složení i ve fázi uvědomění si významu. Losování rolí je důležité, žáci se často snaží některé roli vyhnout, v případě losování tuto nežádanou roli musel někdo vykonávat a byl zkrácen čas, kdy skupina diskutovala, jaká bude role kterého z nich. Současně se ale v některých skupinách žáci domluvili na výměně role (bez pokynu lektora). V tom případě je vhodné nezasahovat, protože žáci se v dané pozici cítí lépe, současně je ale dodrženo, aby každou roli někdo zastával. Přitom nerozhoduje lektor, ale žáci sami náhodným losováním. V případě, že se v některé skupině déle někdo snaží přesvědčit ostatní, aby si s ním roli vyměnili, a oni nesouhlasí, teprve vstupuje lektor s pokynem, že má být zahájena aktivita s rolemi, jak byly vylosovány. Při menším počtu žáků jsou před lekcí odstraněny duplicitní role (nejdříve prezentující, pak zapisovatel, nakonec hledač informací).

Čtené texty musí být stejně dlouhé, aby se některá skupina necítila znevýhodněná. Klíčový je i jejich výběr, který by měl odpovídat tomu, co žáci považují za diskutované téma pro jejich osobní kontext. Témata byla zvolena z oblasti informační bezpečnosti s ohledem na podporu provázanosti obou částí koncepce, lekci je ale možné upravit i pro jiná témata. Ta by měla být co nejvíce různorodá (ne např. různé variace kyberšikany). Po zkušenosti z realizace byly texty zkráceny na rozsah 800–900 znaků. Upravena byla i jejich volba, aby se jednalo o texty pochopitelné a tematicky známé dětem, ale také aby v nich byl prvek odborného textu a mohla tak být vyplněna celá tabulka pro I.N.S.E.R.T. I když lektor reflektoval neznámé nebo nepochopitelné informace z textu, jeho cílem bylo nechat některé otázky otevřené s tím, že odpovědi si žáci sami najdou v navazující aktivitě.

Hlavní část lekce založená na práci s informačními zdroji vždy vedla k emotivnímu vyjádření zájmu pracovat na počítači. Zejména skupiny, které hledaly informace v časopisech, nebyly s přiděleným zdrojem spokojeny. Vhodné bylo připomenout jim, že si téma losovaly. Tyto skupiny pak bylo také častěji nutné podporovat tím, že lektor chvíli pracoval s nimi a snažil se je podpořit při vyplňování pracovního listu. Naopak skupiny, které pracovaly na počítači, vyžadovaly spíše rychlé zásahy lektora, kdy jim připomínal, že musí zůstávat výhradně na přidělené webové stránce, případně korigoval, když se žáci postrkovali u počítače a každý jej chtěl ovládat. I když bylo ve skupině více hledačů, kvůli spolupráci hrálo velkou roli to, kolik počítačů nebo výtisků mohli využít. Při rozdělení bylo vyhledávání méně efektivní a docházelo k výrazně nižší kooperaci žáků. Na druhou stranu bylo důležité umístění vybavení při práci s počítači. Pokud byl počítač v rohu místnosti, na monitor vidělo jen několik žáků. Když byla skupina větší a chvíli některý člen na monitor neviděl, případně se cítil při hledání nevyužitý, přestal se zapojovat. Pak bylo vhodné dát mu k dispozici potřebný materiál, aby se mohl opět na aktivitě podílet.

V rámci diskuze po prezentaci hledání informací je cílem lektora navést žáky na silné a slabé stránky jednotlivých informačních zdrojů. K tomu přispívá, že žáci ve skupinách s tradičními zdroji projevují svůj zájem o ty elektronické („*Vy jste byli na počítači? To ti závidím*."). Lektor by měl mít připravené doplňující otázky pro diskuzi, z nichž si vybírá pro různé typy zdrojů takové, které upozorní i na druhou stranu hodnocení využitelnosti zdroje (obvykle je nutné lektorem iniciovat nevýhody elektronických a výhody tradičních zdrojů). Např. v rámci stáří informace lektor navazuje otázkami, jak dlouho trvá daný zdroj vytvořit a jaké jsou možnosti aktualizací, jaké mohou být následky toho, když jsou využity zastaralé informace, případně jestli se žáci někdy setkali s problémem nefunkčních odkazů ve webovém prostředí. V případě řešení původce informací je možné upozornit na to, kdo se může stát autorem daného zdroje, jak je to náročné, jak důležitá je jeho odbornost, zda si uvědomují komerční a redakční vstupy apod. Při řešení správnosti, platnosti a objektivity informací je důležité nezůstat jen u odpovědi ano nebo ne, ale žádat po dětech zdůvodnění a příklady, proč zdroj hodnotí daným způsobem. Důležitým faktorem je porozumění s upozorněním, že ne všechny informace jsou určeny pro každého, takže někdy je i dobrý zdroj pro žáky nepoužitelný, třeba když je příliš odborný.

Ve fázi reflexe je možné z časových důvodů přeskočit brainwriting a rovnou žáky vyzvat, aby se zamysleli nad předchozí diskuzí a vybrali a zdůvodnili základní prvky, kterých by si při hodnocení každého zdroje měli všimnout, ať půjde o Wikipedii nebo o knihu. Právě z časových důvodů obvykle není možné vytvořit graficky pěkný seznam, který by mohl být dlouhodobě pověšený ve třídě, např. pro připomínku při referátech studentů. Z toho důvodu knihovník může mít dopředu připravený plakát (ideálně ve formátu A3), který srovná s vytvořeným seznamem. Tento plakát může být také některým z testů pro hodnocení důvěryhodnosti zdro-

je (viz kap. 1.1.2), například matice C.R.A.P. testu od McKenzie, kterou je možné i přeložit díky licenci CC BY-NC 3.0[401].

3.2.6 Sociální inženýrství a silná hesla (Mnoholičný lektvar)

Anotace: Žáci druhého stupně základní školy jsou již často uživateli mnoha služeb internetu, z nichž významnou část tvoří komunikace a služby vázané na osobní profil. S jejich užíváním jsou ale spojeny různé hrozby, se kterými se žáci mohou setkat a jejichž důsledky mohou být silně negativní. Proto je vhodné vybudovat v nich zdravou nedůvěru v toho, s kým komunikují na internetu, především s ohledem na sociální inženýrství a krádež identity. Pro lepší uvědomění si těchto problémů je do lekce zařazena simulace problematické komunikace na internetu. Klíčovou roli v souvislosti s tím hrají autentizační údaje, nejčastěji ve formě hesel, proto jsou představeny zásady práce s bezpečnými hesly.
Cílová skupina: 6. třída ZŠ
Materiální vybavení: Psací potřeby a volné papíry pro žáky, dvě místnosti (ne vzdálené), lístky s názvy hrozeb (jeden pro skupinu), pracovní list Tabulka pravosti identit (jeden pro každého žáka), pracovní list Hesla (pro každého žáka), seznam pravidel v soutěži (zavěšený pro skupinu nebo promítaný), vhodná tabule a fixy a anglicko-české slovníky
Výukové cíle – Žák je po lekci schopen...:

- popsat možné způsoby podvržení identity při komunikaci na internetu;
- identifikovat typické postupy sociálního inženýrství;
- aplikovat zdravou nedůvěru na internetovou komunikaci;
- vysvětlit význam autentizace;
- vytvořit silné heslo a bezpečně ho používat.

Spojení s RVP: ČJL-9-1-02, ČJL-9-1-07, ČJL-9-2-03, ICT-9-1-01, VO-9-1-07, VO-9-4-05, VO-9-4-08, VO-9-4-10, VZ-9-1-01, VZ-9-1-14, VZ-9-1-16, klíčové kompetence a průřezová témata
Spojení s NIQUES (informační gramotnost): Formulace problému (vynikající), určení typu informace (vynikající), určení typu informace (standardní), posouzení relevance a úplnosti informací (vynikající), posouzení pravdivosti informací (vynikající), analýza získaných informací (standardní), modelování a simulace (standardní), plánování postupu řešení (minimální), komunikace (standardní), vytváření digitální identity (vynikající), bezpečnost (vynikající), uplatňování právních norem (vynikající), etika zacházení s informacemi a netiketa (vynikající), každodenní život s technologiemi (minimální)

401 MCKENZIE 2013.

Výukové aktivity dle E-U-R:
- evokace: definování internetových hrozeb,
- uvědomění: soutěž a interaktivní přednáška,
- reflexe: brainstorming.

Osnova

Definování internetových hrozeb

Časový plán: 20 minut: 5 min. definice, 15 min. prezentace s přednáškou

Po zahájení lekce s představením jejího zaměření na hrozby komunikace na internetu jsou žáci vyzváni, aby se rozdělili se do skupin po 3–4. Cílem evokace je nejen nasměrovat uvažování žáků k tématu, ale především je motivovat v zapojení do lekce poukázáním na jejich znalostní nedostatky, které je schopen lektor doplnit. Během pěti minut má každá skupina vytvořit krátkou definici pojmu, který si vylosuje. Žáci definují pojmy: krádež identity, kyberšikana, slovníkový útok, kybergrooming, hacking, kyberstalking, happy slapping, sexting, malware. Pojmy jsou řazeny podle významu pro lekci, do losování je zařazeno tolik pojmů, aby vyšel na každou skupinu jeden. Protože řada pojmů vychází z anglického termínu, jako pomůcky slouží anglicko-české slovníky, které si skupiny mohou, ale nemusí půjčit. Definici mají skupiny vytvořit jakkoli, pokud pojem neznají, mají si ji zkusit odvodit z významu slov.

Následně skupina přednese své vymezení pojmu. Ostatní žáci mohou tuto definici reflektovat. Pokud není správná, po vyjádření ostatních žáků je vymezení upřesněno lektorem. Současně lektor doplní informace o rozšířenosti daného problému pomocí výsledků výzkumů, příp. grafů (viz kap. 1.2) a možné maximální sankce v českém prostředí. Při přechodu mezi jednotlivými definicemi pojmů upozorní na jejich vazby, zejména uplatnění krádeže identity v hrozbách při komunikaci na internetu, a to s neznámými lidmi, ale i známými, za které se může vydávat někdo jiný. Pro simulaci, jak je jednoduché převzít cizí identitu a současně těžké odhalit tuto krádež, je určena následující hra.

Soutěž v odhalování pravosti či krádeže identity

Časový plán: 30 minut: 5 min. vysvětlení pravidel, 20 min. soutěž, 5 min. vyhodnocení

Formát hry je podobný lekci pro 4. třídu, proto je zde vymezení stručnější. Losováním čísel a písmen, kterými se ve hře žáci označují místo jmen, jsou opět vytvořeny dvě skupiny, které se po vysvětlení pravidel rozdělí do dvou místností, mezi kterými lektor s pomocí učitele přenáší vzkazy žáků. Cílem zde ale není zjistit totožnost komunikačního partnera, ale zda je komunikace s ním pravdivá (s reálnou identitou) či lživá (s ukradenou identitou) a současně zmást toho druhého ohledně své role z hlediska pravdivosti komunikace. Za každé správné odhalení přístupu je získán bod, za každé odhalení vlastního ztracen bod.

Pravidla komunikace ve hře jsou viditelně napsána v obou místnostech. Po rozchodu skupin se v každé místnosti postaví polovina žáků k pravé ruce lektora (nebo učitele), druhá polovina k levé ruce. Následně lektor ukáže, ve které ruce měl červený lístek značící falešnou identitu a ve které zelený pro pravou identitu pro průběh celé aktivity. Pravé identity musí psát výhradně pravdu (výjimkou jsou soukromá tajemství), falešné se po celou dobu vydávají za jednoho člověka ze své skupiny, aby nebyli odhaleni už při představení se ukradenou identitou. Jména je možné používat, jen pro označení subjektů komunikace (adresátů zpráv) je nutné označení číslem a písmenem. První komunikace je nadepsaná podle stejného klíče jako u lekce pro 4. třídu. Opět je možné vést libovolný počet komunikací s rizikem malého množství odpovědí, totožný je i způsob komunikace, kdy je zapsána odpověď a následně položena vlastní otázka před odesláním zprávy zpět. Pokud si žák myslí, že poznal identitu druhého, opět použije formulku *už vím*, ale komunikace končí až při jejím zapsání oběma komunikujícími žáky. Pro zaznamenání pravosti identity je použita podobná tabulka jako u předchozí lekce (viz materiál *Tabulka pravosti identit*). Pro zahájení komunikace děti dostanou příklady možných otázek, např. *Jak se jmenuješ? Jaký je tvůj oblíbený zpěvák? Jaký děláš sport?*. Lektor opět radí při nejasnostech a zasahuje jen v podobných případech jako u předchozí lekce, hlídá čas a 5 minut před koncem dá výzvu k posledním otázkám.

Po ukončení hry se skupiny sejdou v jedné místnosti a vyhodnocení probíhá stejně jako u předchozí lekce, kdy jsou postupně odříkána všechna písmena a čísla a k nim správná odpověď na to, zda říkali pravdu nebo lhali.

Interaktivní přednáška reflektující soutěž
Časový plán: 10 minut
Po ukončení hry lektor připodobní simulaci reálnému prostředí a upozorní žáky na to, co poznali v soutěži jako problém, a jak se mu mohou vyhnout. Klíčová je při komunikaci na internetu snadnost krádeže identity či vytvoření a užívání falešné (pro lekci jsou obě situace označovány zjednodušeně jako krádež identity). Nikdo si nemůže být zcela jistý, že komunikuje opravdu s tím, s kým si myslí, pokud toho druhého nezná z fyzického prostředí a nekomunikuje s ním v reálném čase přes webkameru, což ale není typická forma komunikace s přáteli na internetu.

Vodítko pro odhalení charakteristik či identity druhého nemůže dát ani forma komunikace. Mnoho jí totiž na internetu probíhá veřejně, proto není těžké zjistit si pro konkrétní skupinu uživatelů obvyklou formu i obsah komunikace a napodobit je. V případě krádeže identity může útočník paralelně navázat komunikaci i s tím, za koho se vydává. Potom není problém se zeptat na informace, které potřebuje pro komunikaci se zamýšlenou obětí. Při závažnějších problémech, jako je např. grooming, často dochází k dlouhodobému budování důvěry a tzv. zrcadlení, kdy komunikující vyjadřuje stejné zájmy a názory jako ten druhý a tím vyvolává pocit *spřízněné duše*, tedy získává důvěru.

I v případě, že člověk přes internet komunikuje jen s těmi, které zná, nemůže si být jistý, že se nejedná jen o ukradené identity. Lektor vybídne k zamyšlení a vlastnímu vyhodnocení, jak by žák reagoval na situace, které popisují různé možnosti krádeže identity v praxi (falešný profil, prolomené heslo, žádosti o přátelství od neznámých lidí). Poté jsou žáci vyzváni, zda někoho napadá možné odhalení ukradené identity, když se zamyslí nad úspěšnými strategiemi v předchozí hře. Při řešení lektor upozorní na možnost využít informace, kterou zná jen osoba, jejíž identita je ověřována, jako v sérii knih a filmů o Harrym Potterovi. Jedná se v podstatě o autentizační údaj, podobně jako heslo. Význam hesla také naznačil jeden z výše popsaných scénářů, proto se poslední aktivita zaměřuje na to, jak používat heslo, aby bylo silné a odolalo útokům.

Brainstorming
Časový plán: 15 minut: 5 min. sběr nápadů, 10 min. tvorba bezpečného hesla
Metodou brainstormingu žáci společně vytvoří soubor pravidel pro tvorbu, formu a použití hesel, aby byla dostatečně bezpečná. Lektor nezasahuje, pouze zapisuje nápady a ukončí brainstorming, pokud již nepřináší nové myšlenky. Následně dá každému žáku pracovní list *Hesla* a představí obsah horní poloviny (formát a způsob využívání hesla). Potom je vyzve, aby během tří minut vytvořili ve dvojici bezpečné heslo a zapamatovali si ho a současně poznamenali na pracovní list. Několik žáků poté napíše na tabuli své heslo a lektor na pracovním listu zkontroluje, že bylo zapamatováno.

Když se žáci vyjádří k tomu, zda heslo splňuje stanovená pravidla, doplní svůj názor také lektor a upozorní na průměrnou rychlost prolomení dané formy podle pracovního listu. Následně popíše možná řešení použití silného hesla bezpečně i k zapamatování (správce hesel, několikaúrovňová politika a algoritmus tvorby) a služby pro kontrolu bezpečnosti hesla, které jsou také uvedeny na pracovním listu. Na závěr jsou žáci opět vyzváni k vytvoření bezpečného hesla, jehož kvalitu si v některé z uvedených služeb ověří.

Pět otázek s dospělými

1. Jak jste se bavili přes internet s člověkem, kterého jste nikdy neviděli?
2. Když se vám ozve někdo známý s novým profilem (e-mailem, facebookovým profilem, Skype účtem atd.), jak zjistíte, že je to opravdu ten, kdo myslíte?
3. Jak si vytváříte heslo a kde se snažíte, aby bylo co nejbezpečnější?
4. Když s někým komunikujete přes internet, jak si ověřujete, jestli říká pravdu?
5. Dokážete popsat alespoň tři situace, ke kterým by mohlo dojít při komunikaci s člověkem, který chce zneužít internet proti vám?

Zkušenosti lektora

S ohledem na obvyklé charakteristiky dospívajících v tomto věku projevují pro lekci menší nadšení než mladší děti. Internet ale chtějí znát, proto se do aktivit zapojí a nebudou projevovat tolik revoltu vůči autoritám, mezi které patří i knihovna (i když mnohem méně než škola) pokud je lektor přesvědčí o přínosu lekce pro jejich znalosti. Důležitá je pro to evokace. Většina řešených pojmů je žákům známá, ale nejsou schopni jasně popsat podstatu a řešení problémů. Je také důležité přiblížení rozsahu problému, protože další z častých reakcí žáků je, že se tak hloupě nechovají, aby mohli být oběťmi jmenovaných problémů. Podobné vyjádření často projevil některý z žáků a ti, jejichž chování je rizikové, se nevyjadřovali. Zde se již výrazněji projevují rozdíly mezi žáky z hlediska jejich znalostí i chování, kdy někteří se výrazně lépe v problematice orientují, ale ostatní nechtějí ukázat svá omezení v tomto směru, protože internet považují za běžnou součást života. Pro komentář lektora je důležité, aby se orientoval v pojmech a měl informace o rozsahu hrozeb založené na výzkumech, které již žáci jsou schopni přijmout, zejména pokud jsou procentuální hodnoty převedeny na to, kolik žáků z jejich třídy odpovídá danému množství. Nejvíce žáky ale upoutaly maximální sazby v trestním zákoníku, příp. v jiných zákonech, které silně komentovali, že jim připadají nízké nebo naopak vysoké.

Pokud budou některé aktivity nahrazeny, je nutné myslet na to, že i přes téma, které žáky zajímá, je lekce poměrně náročná na soustředění. Proto je důležité proložení výkladu herní aktivitou s pohybovou složkou. Žáci 6. třídy již neprojevují tolik nadšení jako 4. třídy v podobně nastavené aktivitě, ale přesto se většina do hry aktivně zapojila. Toto zapojení bylo výraznější u tříd, které absolovaly právě lekci pro 4. třídu. I když si na ni na začátku nevzpomněli, hra jim to připomněla a vzpomněli si i na to, jak je bavila. Při zahájení hry děti projevovaly zájem především o roli lhářů, proto bylo nutné cíleně rozdělit žáky v obou místnostech na pravdomluvné a lháře losováním. Také tip pro lháře, aby se po celou aktivitu vydávali za stejného člověka, byl důležitý, jinak si v druhé místnosti řeknou, že jednou se prezentoval jedním jménem a potom druhým, takže je jasně lhář. Dalším důležitým prvkem byl pro lháře zákaz ptát se toho, za koho se vydávali, na vhodné odpovědi, směli se ptát jen ostatních spolužáků ve skupině.

Stěžejní fáze uvědomění si významu je interaktivní přednáška. Ta je v případě této lekce delší a měla by obsahovat příklady těsně spojené s reálnými činnostmi žáků na internetu. V případě krádeže identity lze využít zamyšlení žáků, jak by reagovali na následující situace:

- Když se označím na Facebooku jako Justin Bieber, vyjadřuji se jako on a mám vytvořen profil s informacemi, které odpovídají této osobě, jak zjistíte, že lžu?
- Přišlo by vám divné, kdybych vám poslala zprávu z profilu podobného, jako má vaše kamarádka zařazená na sociální síti mezi přátele s tím, že toto je

nový profil, který je mimo kontrolu matky, a že ten starý musím občas používat, aby nepoznala, že mám nějaký bez jejího dohledu, takže na ten starý nemůžete nic k novému napsat?

- Jste si zcela jistí, že někdo neuhádl nebo neprolomil heslo vašeho kamaráda k účtu, se kterým komunikujete? Nebo se jen nezapomněl odhlásit či nenechal uložené heslo na počítači, ke kterému má přístup i někdo jiný, třeba v knihovně? Potom byste mluvili s účtem, který máte prověřený, ale se zcela jinou osobou, než myslíte. Přitom tato osoba má přístup i k celé historii komunikace, takže o vás i vašem dorozumívání ví mnoho a dokáže to napodobit.
- Jste si jistí, že znáte dobře všechny vaše přátele na Facebooku a jejich přátele, kteří mají přístup k vašim informacím zveřejněným v této službě?

Reálnost popsaných scénářů je snadno představitelná. Jaké jsou možnosti řešení nebo alespoň omezení těchto situací? A nepřipomínají krádeže identity něco? Zde lektor odkazuje na předposlední a poslední díl série o Harrym Potterovi, kdy smrtijedi používali mnoholičný lektvar právě pro krádež identity, aby narušili odboj proti Voldemortovi. A opět se nabízí otázka pro žáky: Jak se Fénixův řád bránil? I na internetu je jednou z možností (mimo již uvedené ověření webkamerou) využít sdíleného tajemství. Při tom je nutné pracovat s informací, kterou opravdu nezná nikdo jiný, a obě strany ví, že ji nesmí prozrazovat nikomu dalšímu a samozřejmě nelze nikde zveřejnit nic, co by ji prozradilo. Jedná se o autentizační údaj, podobně jako heslo. Význam hesla také naznačil jeden z výše popsaných scénářů, proto se poslední aktivita v lekci zaměřuje na to, jak používat heslo, aby bylo silné a odolalo útokům. Opět je nutný vyvážený přístup ke sdílení informací, který by měl vést žáky k budování pozitivní digitální stopy a k uvážlivému chování na internetu s uvědomováním si důsledků vlastního chování a snadnosti realizace představených problémů.

Hesla používají všichni žáci. Reflexe je proto zaměřena na konfrontaci reálně používaných a silných hesel. Autentizace představuje jádro bezpečného užívání mnoha elektronických služeb. Je tedy vhodné věnovat jí dostatečný prostor. První část reflexe, kdy žáci vytváří bezpečné heslo, je obvykle pro žáky opakování, většina z nich má povědomí o tom, jak by heslo mělo vypadat a jak s ním pracovat. Klíčový moment představuje ukázka, nakolik jsou schopni reálně se silným heslem pracovat. Proto následují opět praktické příklady pro vysvětlení možných nástrojů pro silná hesla, která jsou zároveň prakticky využitelná:

- Správce hesel je obvykle zvláštní software, do kterého se uživatel přihlásí, a program sám za něj doplní heslo pro příslušnou službu, takže nutné je zapamatovat si jen jediné silné heslo pro správce. Příklady programů jsou uvedeny na pracovním listě, takže žáci si je při zájmu mohou snadno najít.
- Několikaúrovňová politika hesel spočívá ve stanovení kategorií důležitosti služeb, které heslo chrání. Podle toho jsou pak hesla silná. Je ale nutné si uvědomit, že jednoduché heslo může být prolomeno, proto by mělo být

použito jen tam, kde uživateli nebude vadit, když dojde ke krádeži profilu, příp. identity přes něj.
- Algoritmus tvorby znamená, že postup je stále stejný, ale generuje vždy jiné a silné heslo. Např. věta „*Toto je moje heslo, které mám na Facebooku v lednu.*" vytvoří heslo *Tjmh,kmnFv1.* – je použito vždy první písmeno z každého slova, ponechána čárka a tečka ve větě, leden jako první měsíc je nahrazen číslicí 1. Tuto větu lze použít i pro další služby, kdy Facebook je nahrazen jejím názvem, heslo tedy bude odlišné a přitom postup stejný.

Nástroje se mění, proto je dobré se s nimi před lekcí seznámit a stručně je následně představit a doporučit k vyzkoušení. Vhodné je zkontrolovat jejich funkčnost těsně před lekcí (zejména ty uvedené v pracovním listu *Hesla*).

3.2.7 Autorský zákon na internetu (Up and download)

Anotace: Žáci vyhledávají a užívají cizí autorská díla, ale také vytváří vlastní. Lekce si klade za cíl rozšíření povědomí o možnostech a omezeních v autorském zákoně v elektronickém prostředí. Důraz je kladen na zákonnou úpravu využití cizího díla ve vlastní práci i pro osobní užití se snahou zdůvodnit etické aspekty této úpravy. Součástí lekce je upozornění žáků na možné sankce a reálné případy dle mediálních sdělení.

Cílová skupina: 7. třída ZŠ

Materiální vybavení: Psací potřeby a volné papíry pro žáky, tabule a fixy, citace ze zákona (jedna pro každého žáka), mediální zpráva (jedna pro každého žáka), pravidla třífázového rozhovoru k zavěšení pro třídu (příp. promítané)

Výukové cíle – Žák je po lekci schopen...:
- vysvětlit význam autorských práv a povinností pro vlastní i cizí tvorbu;
- aplikovat zákonná omezení na nejběžnější způsoby nakládání s cizími autorskými díly v elektronickém prostředí;
- srovnat rozdíly v možnostech nakládání s různými typy děl.

Spojení s RVP: ČJL-9-1-07, ČJL-9-1-08, ICT-9-2-03, ICT-9-2-04, VO-9-4-05, VO-9-4-08, VO-9-4-10, VZ-9-1-01, VZ-9-1-16, klíčové kompetence a průřezová témata

Spojení s NIQUES (informační gramotnost): Formulace problému (vynikající), určení typu informace (vynikající), posouzení relevance a úplnosti informací (standardní), posouzení pravdivosti informací (vynikající), zpracování textu (minimální), analýza získaných informací (minimální), modelování a simulace (standardní), vytváření originálního díla (vynikající), uplatňování právních norem (vynikající), etika zacházení s informacemi a netiketa (vynikající), každodenní život s technologiemi (minimální)

Výukové aktivity dle E-U-R:
- evokace: scénky ze života,

- uvědomění: rozbor mediálních zpráv,
- reflexe: patero licenčních podmínek pro práci na internetu.

Osnova

Scénky ze života

Časový plán: 30 minut: 5 min. čtení, 10 min. práce skupin, 15 min. prezentace
Lekce se zaměřuje na seznámení žáků s pravidly autorského zákona, která jsou často porušována při jejich používání internetu. Podstatou lekce tedy není ochrana dětí proti tomu, aby se nestaly oběťmi, ale naopak aby samy nebyly pachateli protizákonného jednání. Evokace se opět snaží žáky upozornit na situace snadno představitelné v jejich reálném životě, kdy mohou porušovat autorský zákon. Aktivita směřuje na slabiny v jejich chování, protože i když mají povědomí o tom, co je správné a co ne v oblasti nakládání s autorskými díly v elektronickém prostředí, mají jen omezené povědomí o zákonných specifikacích.

Po zahajovacím seznámení žáků s tím, co všechno jsou autorská díla chráněná zákonem a proč je důležité dodržovat autorský zákon, se třída rozdělí na 6 skupin, kde každá skupina dostane stručně popsanou situaci. Každý žák si text přečte samostatně a následně společně nacvičí popsanou scénku. Postupně scénku sehrají, lektor shrne její podstatu a žáci z celé třídy jsou vyzváni, aby řekli, co bylo správně a co bylo porušením zákona. Scénka je uzavřena krátkým vstupem lektora, který spojí situaci s úpravou v zákoně, kterou podrobněji nerozebírá, uvede jen obecné vymezení zákonných práv a povinností.

Rozbor mediálních zpráv

Časová dotace: 35 minut: 5 min. čtení, 10 min. pracovní list, 20 min. prezentace
Navazující aktivita se soustředí na možné dopady porušení autorského zákona na základě mediálních zpráv. Cílem je upozornit žáky na možné sankce, které nejsou hypotetické, ale možné.

V praktických situacích se často střetávají různé části zákona, kdy to, která bude upřednostněna, často závisí na domluvě dotčených stran, např. toho, kdo dílo sdílí na internetu a kolektivního správce autorských práv. Roli hraje i povědomí jednotlivých stran o jejích právech, kdy kolektivní správci jsou odborníci v problematice, což může vést k tomu, že právě jejich výklad je upřednostněn. V případě, že se strany nedomluví, je řešením sporu soud. Ten rozhoduje podle pravidel v zákoně, kdy obvykle rozhodnutí odpovídá způsobu, jak byly podobné spory řešeny jiným soudem v minulosti. Proto mediální zprávy mohou být poučením, jakým by soud v daném případě rozhodl. Každá skupina dostane jednu mediální zprávu, která by měla být zkrácena do rozsahu necelé strany A4. Pro lekci byly využity tyto zprávy:

- VENTUROVÁ, Jitka a ČTK. Nejvyšší soud se zastal piráta. Za sdílení filmů měl platit miliony. *iDnes* [online]. 2015 [cit. 2017-02-25]. Dostupné z:

http://zpravy.idnes.cz/nejvyssi-soud-se-zastal-pirata-za-stahovani-filmu-mel-platit-miliony-12e-/krimi.aspx?c=A150105_101746_krimi_jpl
- VŠETEČKA, Roman, Jan KUŽNÍK a Vladan RÁMIŠ. Konec beztrestného stahování. Kopírovat půjde pouze z legálních zdrojů. *Technet.cz* [online]. 2014 [cit. 2017-02-25]. Dostupné z: http://technet.idnes.cz/kopirovat-na-prazdna-media-lze-pouze-z-legalnich-zdroju-rozhodl-soud-1jt-/sw_internet.aspx?c=A140410_151806_sw_internet_vse
- ČTK. Dávat na web odkazy na stažení filmů zdarma je trestné, rozhodl Ústavní soud. *Novinky.cz* [online]. 2013 [cit. 2017-02-25]. Dostupné z: https://www.novinky.cz/krimi/315915-davat-na-web-odkazy-na-stazeni-filmu-zdarma-je-trestne-rozhodl-ustavni-soud.html
- MIM. Muž nabízející stažení filmů dostal u soudu podmínku. Česká televize [online]. 2012 [cit. 2017-02-25]. Dostupné z: http://www.ceskatelevize.cz/ct24/archiv/1169649-muz-nabizejici-stazeni-filmu-dostal-u-soudu-podminku
- VÁCLAVÍK, Lukáš. Exkluzivně: Video od BSA je autentické. Pirát si jím může vykoupit část trestu. *CNews* [online]. 2015 [cit. 2017-02-25]. Dostupné z: https://www.cnews.cz/exkluzivne-video-od-bsa-je-autenticke-pirat-si-jim-muze-vykoupit-cast-trestu/
- HORÁK, Jan. „Pirát" vyhrál soud o poplatky za hudbu z rádia. Pouští místní kapely. *iDnes* [online]. 2014 [cit. 2017-02-25]. Dostupné z: http://usti.idnes.cz/klub-vyhral-soud-o-poplatky-za-licencni-smlouvy-s-intergramem-pb2-/usti-zpravy.aspx?c=A140129_2027865_usti-zpravy_alh

Po přečtení textů je vysvětlena samotná aktivita. Skupina má za cíl společně vyplnit pracovní list, který žáky navádí, čeho si mají v textu všímat. Žáci jsou seznámeni s tím, že výsledek budou prezentovat jen s podkladem v jejich vlastních poznámkách na pracovním listu. Vstupy lektora propojují řešené případy a zákonnou úpravu z první části lekce. Upozorňuje, jaká část zákona byla porušena a za jakých podmínek by bylo nakládání s cizími autorskými díly legální.

Patero licenčních podmínek pro práci na internetu

Časový plán: 10 minut

Závěrečná aktivita je opět skupinová, kdy žáci dostanou zadání, aby každá skupina připravila vlastní seznam pěti bodů, které by pro ně definovaly, co mohou a nemohou dělat s autorskými díly v elektronickém prostředí. Doporučeno je, aby aktivitu zahájili brainstormingem a následně zkusili dát dohromady kategorie, které spolu souvisí, a určili pořadí důležitosti. Na závěr jsou seznamy vyvěšeny a žáci jsou vyzváni, aby si prohlédli produkty ostatních a hlasovali o tom, čí seznam je nejlepší. Všechny produkty si pak odnesou žáci do školy pro možné navázání ve výuce.

Pět otázek s dospělými

1. Za jakých podmínek můžeš stahovat filmy z internetu? A software?

2. Jaké problémy jsou z hlediska autorského zákona při využívání torrentů?
3. Můžeš poskládat referát z odstavců, které jsi našel na různých stránkách na internetu?
4. Jaké a komu hrozí sankce, když porušíš na internetu autorský zákon?
5. Proč by rodiče měli vědět o tom, co nahráváš na internet nebo z něho stahuješ?

Zkušenosti lektora

V rámci evokace žáci obvykle nebyli příliš motivováni zapojit se do lekce po seznámení s jejím tématem, které se zaměřuje na dodržování autorského práva v elektronickém prostředí. V souladu s výzkumy (viz kap. 1.1.1) si jsou často vědomi toho, co je protizákonné, ale stejně tak se tím často neřídí. Klíčovou součástí evokace jsou proto praktické příklady aplikace dané zákonné úpravy, aby si žáci uvědomili, proč by pro ně téma lekce mělo být zajímavé. V celé lekci je apelováno zejména na obavu z možného trestu, která je u dětí v tomto věku poměrně dobrým motivačním faktorem. Důležité je ale ukázat jim, že i když jsou jen dospívající a jednotlivci, tak i ti bývají v České republice postiženi, pokud autorský zákon poruší (viz druhá aktivita). Pro přiblížení zákonné úpravy reálným situacím je možné využít tyto komentáře k jednotlivým částem zákona:

- Právo dílo užít a sdělování veřejnosti: Tato část se týká mj. všeho, co je zprostředkováno přes internet. Jde o jediný typ užití díla bez spojení s hmotným nosičem, takže do sdělování veřejnosti spadá např. streamování, ukládání a následné stahování z internetu, ať jde o jakékoli dílo. Podstatné je, že vždy musí mít ten, kdo s dílem nakládá, jasný souhlas autora (uvedený v licenčních podmínkách). Při sdílení přes internet se nemůže jednat o půjčování, protože to je dle autorského zákona spojeno s hmotným nosičem.
- Volná užití: Týká se použití fyzickou osobou výhradně pro ni, např. stažení knížky z internetu a čtení doma bez dalšího šíření. Důležité je, že není při stahování možné současně sdílet, pak už jde o porušení zákona, což je problém u torrentů. Důležité také je, že se osobní užití netýká softwaru a není možné nahrát si vysílaný film, třeba v kině nebo v televizi.
- Technické ochrany děl: Autorský zákon zakazuje jakékoli obcházení technické ochrany díla, např. použití keygenerátoru pro neoprávněné použití softwaru (např. hry), hackování softwaru nebo informačního systému, šíření softwaru pro kopírování DVD bez ochrany výrobce apod. Problém je ale podle také držení zařízení, které toto umožňuje, např. i když je keygenerátor jen stažený do osobního počítače.
- Elektronické informace o právech: § 44 navazuje na předchozí bod, tedy když někdo technickou ochranu neobešel, ale podporuje šíření díla s odstraněnou ochranou. Sem patří veškeré sdílení i odkazů díla ke stažení, kdy si je člověk vědom nelegálnosti, takže formulace typu „nejde o můj upload“

nic nemění na nelegálnosti. Dále je popsána situace odstranění DRM např. u e-knihy – také je nelegální, ať už ji někdo provede, nebo takto změněné dílo šíří nebo zastírá, že k něčemu takovému došlo. V této části lektor může upozornit na licence Creative Commons, kdy autor dává možnost dalšího šíření díla, přičemž ale nespojuje dílo s žádnou technickou ochranou.

- Oprávněné užití softwaru: V § 66 je popsáno to, co je legální, např. že v pořádku je, když někdo získá rozmnoženinu programu, aby ho používal, ale nesmí ji dál šířit. V zásadě je nelegální třeba prodat počítačovou hru, když ji někdo dohraje, pokud si ji po zakoupení stáhl, ale je možné prodat originální nosič (rozdíly v distribuci od prodejce ovlivňují další možnosti nakládání s dílem). Jinak, než používat software jen pro svou potřebu a nijak dál ho nešířit ani nepřevést, je možné, jen když je to výslovně uvedené v licenčních podmínkách programu. Zákon také dává možnost udělat si kopii softwaru pro vlastní užívání, což je vlastně i nainstalování.
- Citace: Pokud jde o běžnou citaci, třeba když ji žáci chtějí něco dát do referátu, tak to musí být jen malá část díla, nesmí zkopírovat celý text, který našli. Vždy to musí být s uvedením autora a zdroje. Pokud vydávají za svůj referát text, který našli na Wikipedii, tak porušují autorský zákon a mohou být potrestáni i finančně. Celé dílo je možné využít jen krátké a jen pro kritiku či recenzi nebo pro ilustraci ve výuce. Není proto možné nahrát celý text knížky nebo článku na internet s uvedením autora a odkazovat se na citaci. Ve škole to možná takový problém nebude a budou jen pokáráni, ale kdyby něco takového udělali na internetu, třeba si stáhli písničku a dali ji do videa, které pak nahrají na YouTube, tak už by se k tomu snadno mohl dostat někdo, kdo chrání práva autora. Tímto se zabývají speciální organizace, kterým se říká kolektivní správci.

Původně byla testována aktivita, kdy žáci výše popsané poznávali na základě analýzy citací ze zákona. Tím mělo dojít také k rozvoji dokumentové gramotnosti, aby si žáci uvědomili, že sami mají problém zákonnou úpravu pochopit, ale jaké jak nad právním textem přemýšlet. Tato aktivita se ale ukázala jako příliš náročná a pro žáky demotivující. Na rozdíl od využívání komunikačních služeb na internetu žáci více pociťují své omezené znalosti autorského zákona a pro evokaci je proto nejdůležitější, aby si dokázali uvědomit, proč by je měl obsah lekce zajímat. Proto byla aktivita nahrazena scénkami, které mají těsný vztah k jejich každodennímu životu.

Druhá aktivita navazuje na evokaci obsahovým zaměřením, ale jiným způsobem podání. Jsou využity mediální zprávy, které přibližují zákonnou úpravu v reálných podmínkách se zaměřením na možné sankce. Texty je nutné zkrátit nejen z časových důvodů, ale také pro udržení pozornosti žáků, pro které je text delší než jedna strana příliš dlouhý na to, aby byli ochotni mu věnovat potřebnou pozornost. I analýza textů se ukázala jako náročná, pro její usnadnění proto byl vytvořen pracovní list, který pomáhá žákům identifikovat prvky, na které by se měli soustředit.

Přestože z hlediska informační nosnosti je aktivita zařazená do evokace silnější než práce s mediálními sděleními, není vhodné obracet jejich pořadí, protože mediálně řešené případy jsou pro žáky mnohem hůř spojitelné s jejich reálným životem. V rámci diskuze žáci často argumentovali tím, že pro policii jsou svými porušeními zákona málo zajímaví a policie nemá možnost, jak jejich aktivity identifikovat. Proto je nutné je upozornit, že zprávy ukazují, kam až může jejich jednání zajít, a že i menší problémy jsou řešeny, jen se tak často nedostávají do médií. Vhodné je také být připraven doložit možné způsoby využití digitálních stop pro identifikaci člověka, resp. IP adresy počítače, který porušuje zákon. Podobně jako u lekce pro 6. třídu je uvědomění si výše sankce silným motivačním faktorem pro akceptaci řešených pravidel.

Závěrečná aktivita je svou formou blízká předchozím lekcím. Díky tomu je možné řízení zpracování ponechat na skupinách, čímž je více podpořena kooperace a také rozvoj týmové práce, která je důležitá pro tvůrčí aktivitu nejen v internetovém prostředí. S následným hlasováním o nejlepším produktu by žáci měli být seznámeni před aktivitou, protože to zvyšuje jejich motivaci pro tvorbu.

3.2.8 Internetové hrozby pro dospívající (Detektivky na Facebooku)

Anotace: Žáci blížící se konci základní školní docházky jsou již seznámeni s možnostmi internetu. Dospívající bývají jeho častými uživateli, mají povědomí o hrozbách s ním pojenými, ne výjimečně ale na obecné bázi, bez představy o tom, jak by mohla daná situace zasáhnout i je. Pomocí reálných případů je žákům zprostředkován právě tento pohled na problematiku. Řada problémů je spojena s nevhodným nastavením soukromí a zabezpečení (nejen) komunikačních služeb. V závěru lekce je proto simulována registrace a nastavení uživatelského účtu, vzhledem k rozšířenosti na příkladu sociální sítě Facebook.
Cílová skupina: 8. třída ZŠ
Materiální vybavení: Psací potřeby a volné papíry pro žáky, pracovní list Diamant (pro každého žáka), nastříhané příběhy (jeden pro každého žáka), pracovní list FB registrace (pro skupiny), vhodné tabule a fixy
Výukové cíle – Žák je po lekci schopen...:

- aplikovat zdravou nedůvěru na internetovou komunikaci;
- identifikovat obvyklé varovné signály nejčastějších hrozeb v internetové komunikaci;
- definovat možná bezpečnostní opatření proti těmto hrozbám;
- spravovat nastavení soukromí a zabezpečení uživatelského účtu;
- vysvětlit možné důsledky zvoleného nastavení.

Spojení s RVP: ČJL-9-1-02, ČJL-9-1-07, ČJL-9-1-08, ICT-9-1-01, VO-9-1-06, VO-9-1-07, VO-9-1-08, VO-9-1-09, VO-9-4-05, VO-9-4-08, VO-9-4-10, VZ-9-1-01, VZ-9-1-12, VZ-9-1-14, VZ-9-1-16, klíčové kompetence a průřezová témata
Spojení s NIQUES (informační gramotnost): Formulace problému (vynikající), určení typu informace (vynikající), posouzení relevance a úplnosti informací (vynikající), posouzení pravdivosti informací (vynikající), modelování a simulace (standardní), plánování postupu řešení (standardní), komunikace (standardní), vytváření digitální identity (vynikající), bezpečnost (vynikající), uplatňování právních norem (vynikající), etika zacházení s informacemi a netiketa (vynikající), každodenní život s technologiemi (minimální)
Výukové aktivity dle E-U-R:

- evokace: Diamant pro pozitiva a negativa internetu,
- uvědomění: Analýza příběhů založených na skutečných událostech,
- reflexe: Simulace registrace a nastavení v sociální síti Facebook.

Osnova lekce *Detektivky na Facebooku*
Diamant pro pozitiva a negativa internetu
Časový plán: 15 minut: 5 min. vyplnění, 10 min. sdílení
Diamant v evokační fázi vychází z toho, že žáci již mají zkušenosti s internetem, jeho pozitivy i negativy. Ta sice znají, ale uvědomují si především přínosy, které jim internet nabízí a negativa jsou pro ně více teoretická, jsou přesvědčeni, že se jich dotýkají minimálně. Diamant pomáhá, aby si žáci sami uvědomili obě stránky internetu a to, nakolik těžké je přemýšlet nad tímto nástrojem nejen ve smyslu využití, ale i zneužití.

S pomocí diamantu jsou žáci vedeni k tomu, aby vytvořili na daný počet slov pozitivní i negativní charakteristiky internetu (viz pracovní materiál *Diamant*). Obrazec vytváří jednotlivci samostatně, kdy postupují od nejkratších polí střídavě nahoře a dole směrem do středu, čímž se jim spojují pozitiva a negativa na stejných úrovních. Současně by si měli uvědomit, nakolik je pro ně těžké či lehké daný řádek vyplnit. Vyplnění by nemělo přesáhnout 5 minut, po 3. minutě lektor upozorní na blížící se konec. Následně nejdříve přečte vlastní vyplněný diamant a vyzve žáky, aby se také podělili o to, co vytvořili. Pokud žáci nereagují, postupuje se stejně jako při vyplňování, ale žáci nahlas říkají různé varianty pro daná pole.

Lektor by měl diamanty sledovat a najít v nich pojítko na další aktivitu. Obecně lze vždy přejít přes to, že negativa si tolik neuvědomují, přestože se s nimi mohou setkat při použití služeb, které jsou s identitami často spojeny, např. pro komunikaci s blízkými lidmi. A právě k problémům, které zahájila komunikace na internetu, se váže aktivita ve fázi uvědomění.

Analýza příběhů založených na skutečných událostech
Časový plán: 30 minut: 5 min. čtení, 10 min. diskuze ve skupině, 15 min. prezentace
Aktivita je založena na příbězích, které vznikly spojením několika reálných případů, jež skončily tragicky a kvůli tomu se jim dostalo silného mediálního ohlasu. Příběh je vždy rozdělen na pasáže klíčových okamžiků. Odstavce jsou seřazeny abecedně a úkolem žáků je poskládat do správného pořadí jednotlivé části (puzzle). Žáci si samostatně čtou příběh a následně je úkolem skupiny poskládat logicky příběh. Poté mají definovat předpoklady a možné důsledky dané hrozby a opatření, která je možné využít pro prevenci nebo řešení daného problému v kterékoli jeho části. Nakonec skupiny prezentují svůj příběh a diskutované okolnosti (pořadí částí, předpoklady, důsledky a možná obranná opatření proti dané hrozbě). Žáci se tak seznámí se všemi příběhy, přitom u každého aktivita rozvíjí schopnost naslouchání i komunikace. Správné pořadí částí příběhu je:

- Martina (kyberšikana): AEDFBC
- Monika (stalking): DCAFEB
- Petra (sexting): BACDFE
- Matěj (grooming): DAFEBC
- Mirek (krádež identity): CBAEFD

Každý z pěti příběhů se věnuje jinému tématu, ale všechny spojuje, že jsou založeny na hrozbách komunikace na internetu. Příběhy lze libovolně obměňovat, je ale vhodná právě tematická šíře a odkaz na skutečné případy. Právě skutečnost by měla být přiblížena žákům po shrnutí příběhu v rámci prezentace skupin. Reálný průběh a důsledky případu by měly být obohaceny o typický průběh, v tomto věku žáků doplněný i podložením výsledky výzkumů. Důležité je upozornit žáky na prevenci proti útokům, která spočívá především v důsledné ochraně soukromí a zdravé nedůvěře v komunikaci s čistě internetovými známými.

Simulace registrace a nastavení v sociální síti Facebook
Časový plán: 15 minut: 10 min. vyplnění, 5 min. sdílení
Z příběhů je patrné, jak silné postavení může mít Facebook nejen pro komunikaci žáků s jejich přáteli, ale také pro internetové hrozby. Jedním ze základních bezpečnostních opatření je vhodné nastavení soukromí. Facebook umožňuje upravit dostupnost množství informací o uživateli, často se ale stává, že toho není využito. Může se jednat o pohodlnost, ale také neznalost. V obou případech může pomoci aktivita při reflexi, která ukáže žákům, jaké možnosti nastavení soukromí Facebook aktuálně nabízí. I pokud jich nevyužijí, jedná se čistě o jejich rozhodnutí, klíčové je, že si jsou možností vědomi. S ohledem na předchozí aktivitu by si to měli uvědomit ve chvíli, kdy jsou seznámeni s možnými důsledky benevolentního přístupu k soukromí na internetu.

V rámci aktivity si žáci ve skupinách po třech až čtyřech projdou formulář registrace a nastavení soukromí (viz pracovní materiál *Registrace na Facebooku*)

a vyplní jej pro fiktivní osobu. Zadání zní, aby poradili kamarádovi, který se chce na Facebook registrovat, aby byl v bezpečí, ale mohl službu dobře využívat. Po 10 minutách lektor vyzve žáky, aby společně prošli jednotlivá pole. V případě, že některá skupina bude mít odlišnou reakci nebo jmenovaná nastavení nebudou vhodná, lektor doplní komentář k možným důsledkům jednotlivých variant.

Pět otázek s dospělými
1. Když s někým komunikujete přes internet, jak si ověřujete, jestli říká pravdu?
2. Dokážete popsat alespoň tři situace, ke kterým by mohlo dojít při komunikaci s člověkem, který chce zneužít internet proti vám?
3. Slyšeli jste o někom, komu byly zneužity jeho osobní informace zveřejněné na internetu nebo komunikované s internetovým známým?
4. Co děláte pro to, aby se něco podobného nestalo vám?
5. Jak si nastavujete různé internetové služby pro ochranu svého soukromí?

Zkušenosti lektora
V tomto věku je již nepochybné, že všichni žáci na lekci mají poměrně rozsáhlé, i když často jen dílčí zkušenosti s internetem a mají o něm vytvořenou jasnou představu. Současně již není nutné je tolik přesvědčovat o smyslu tématu a uklidňovat jejich sklony k revoltě vůči lektorovi. Ten by měl vystupovat v roli partnera a průvodce, nikoliv nezpochybnitelné autority. Při zpracování diamantu byli žáci po představení diamantu lektora více ochotní se podělit o vlastní zpracování – sice ne všichni, ale vždy minimálně tři zpracování byla prezentována. I z vyplněných pracovních listů zanechaných po lekci žáky bylo patrné, že synonymem pro internet je pro většinu z nich Facebook, což dokládá vhodné nastavení navazujících aktivit. Současně se potvrdilo, že mnohem snažší je pro žáky vyplnění pozitivní části diamantu, zatímco u negativních aspektů je často nenapadala vhodná slova. Ve střední části diamantu (věta o čtyřech slovech) převažoval pozitivní názor na internet, opakovala se vyjádření typu: „*Internet je super/dobrá/užitečná věc.*“, jen výjimečně byly věty negativní, např. „*Bere nám hodně času.*“ Vždy zazněly formulace, které umožňovaly lektorovi navázat druhou aktivitou přes spojení internetu s komunikací, která je podstatou všech řešených případů.

V případě, že se podaří diamant uzavřít včas a je dostupné technické vybavení, je dobrým úvodem pro příběhy promítání videa Let‘s Fight It Together (dostupné z YouTube), které natočila organizace Childnet International pro ilustraci kyberšikany a jejích možných důsledků. Video je sice v angličtině, mluví se v něm ale minimálně. Při zařazení je nutné myslet na časovou náročnost, i při rychlém komentáři vyžaduje min. 10 minut. Použití videa ale může urychlit fázi vysvětlení pravidel následující aktivity, protože je využito práce s příběhem. Po zhlédnutí videa je vhodné vyzdvihnout základní poznatky o kyberšikaně:

- Začíná obvykle nevinným pošťuchováním, ale graduje do neúnosnosti.

- Terčem se může stát i dříve oblíbený žák.
- Jsou využívány nejrůznější způsoby komunikace, pomocí kterých je oběť napadána, zesměšňována apod.
- Problém může zahnat oběť na hranici sil, pak jsou i řešení extrémní, v případě videa to bylo zapojení policie, která přišla pro šikanující dívky.

Příběhy byly původně testovány ve formě čtení s předvídáním. To se ale ukázalo jako časově velmi náročné a pro žáky nezábavné. Formát puzzle se ukázal v obou těchto směrech jako výrazně vhodnější. Současně došlo k přejmenování jednoho ze subjektů příběhu, aby nebyla ve dvou příbězích podobná jména (Petr a Petra), protože to vedlo k problémům při diskuzi. Důležitá se ukázala role pohlaví představitelů příběhů, kdy zájem vzbudilo u některých tříd například to, že obětí kybergroomingu může být i chlapec. K tomu bylo důležité doplnění, že právě toto pohlaví odpovídá reálnému případu.

Právě z toho důvodu, je důležité, aby se lektor orientoval v reálných útocích řešeného typu. Základem je minimálně znalost případů, které jsou uvedeny u zadání aktivity. Dále by měl být seznámen s výsledky výzkumů související s řešenými hrozbami, které jsou zakomponovány také do lekce pro 6. třídu. Lekce je náročnější na znalosti lektora, měl by znát kazuistiky v řešené oblasti a také by měl mít přehled o bezpečnostních opatřeních a důvodech jejich aplikace. Stejně jako u předchozí lekce je nutný vyvážený přístup ke sdílení informací, který by měl vést žáky k budování pozitivní digitální stopy, a k uvážlivému chování na internetu s uvědomováním si důsledků jednání a snadnosti realizace představených problémů.

Pořadí částí příběhů bylo až na výjimky vždy správně. Protože lekce byla testována i na vyšších ročnících, než pro které je doporučena, ukazoval se význam zařazení právě pro 8. třídu pro předcházení problému. Ve vyšších ročnících se výrazně častěji objevovaly zkušenosti žáků s danými hrozbami. Na jedné škole žáci dokonce sami upozornili na to, že v předchozím roce jedna dívka byla známá všem ve škole právě tím, že se snažila nabízet spolužákovi, který se jí líbil, zasíláním fotek, které byly typickou ukázkou sextingu, což v podstatě vedlo ke kyberšikaně této dívky. Hrozby je proto nutné žákům představit ještě v době, kdy je možné je připravit na problém, který pro ně zatím není příliš reálný, aby si v okamžiku, kdy zvažují rizikové chování, byli vědomi možných důsledků.

Poslední aktivita se ukázala jako pozitivní v tom, že se žáci často poprvé seznámili s možnostmi nastavení, které jim Facebook nabízí, i když ho často využívají. Podle sdílených zkušeností jsou většinou přesvědčeni o tom, že přednastavení služby je správné a není nutné zabývat se jeho úpravami. Někteří žáci uvedli, že jim profil zakládali rodiče, kteří také upravovali nastavení, a žáci od té doby necítili potřebu na něm něco měnit. Někteří byli překvapeni, jaké možnosti Facebook nabízí a komentovali, že si ověří, nakolik jejich zájmy odpovídají aktuálnímu nastavení.

Při diskuzi nastavení se ukázalo u tříd, které neabsolvovali lekci pro 6. třídu, že je časově náročná již registrace, kdy žáci diskutovali o vhodném formátu hesla. To podporuje význam koncepčního řešení informační bezpečnosti, kdy by bylo možné odkázat se na předchozí lekci. V případě vlastního nastavení se ukázalo jako časově i logicky výhodné dotázat se, co by mělo být nastaveno na jednotlivé formy dostupnosti, např. co by mělo být dostupné jen uživateli samotnému, nebo co by mělo být dostupné jen přátelům (tedy ne naopak jak by měly být nastaveny dané informace). Žáci následně diskutovali, jestli by omezení nemělo být přísnější. V rámci vyplňování profilových informací bylo žákům připomenuto, že pole nejsou povinná, takže pokud dané informace nechtějí sdílet s někým, kdo je nezná, je zbytečné je vyplňovat. Tím totiž vytváří další možné riziko, kdy někdo informaci může zjistit, např. pokud Facebook změní politiku přístupu k informacím (např. podle čeho je možné vyhledávat uživatele).

Lekce byla hodnocena pozitivně především pedagogy, podle kterých lekci děti dobře hodnotily a diskutovaly o ní i v následujících dnech, což lze interpretovat splněním cíle v zamyšlení nad řešenými problémy. Vhodnost hlavní aktivity založené na reálných případech i potřebu znalostí těchto případů potvrzuje i zkušenost Aleny Srovnalové (Městská knihovna Rožnov pod Radhoštěm, e-mailová komunikace ze dne 18. 6. 2014), kdy žáci vyjadřovali již dostatečné znalosti obecných informací, ale právě doplnění výzkumnými zjištěními a kazuistikami z českého prostředí přidávalo obsahu na zajímavosti. Současně tato knihovnice upozorňovala na problém náročnosti čtení s předvídáním, což potvrzuje vhodnost úpravy aktivity na puzzle. Knihovnice také uváděla, že diamant bylo někdy problém zahájit, osvědčilo se navést žáky k pozitivním slovesům (3. řádek). Pozitivní zkušenost měla i se zařazením alternativního videa mezi diamantem a příběhy, konkrétně *Hnusná držka* (dostupné na YouTube) bez komentářů odborníků. Reflexe byla realizována metodou *poslední slovo patří mně*.

3.2.9 Život mediální zprávy

Anotace: Lekce směřuje k mediální výchově, kde snahou je přiblížit žákům postupy pro hodnocení a srovnání informací ve zpravodajství k aktuálnímu kontroverznímu tématu (zde je řešena uprchlická krize, možné jsou ale obměny pro jiné téma např. Romové, volby prezidenta...). Snahou je upozornit žáky na fungování médií a možnosti zkreslení informace vlivem různých subjektů, které ovlivňují proces tvorby zprávy. Následně jsou žáci seznámeni s postupy pro hodnocení důvěryhodnosti informací se zaměřením na mediální zprávy.
Cílová skupina: 9. třída ZŠ

Materiální vybavení: Psací potřeby a volné papíry pro žáky, tabule a fixy, pracovní list SMELL test (pro každého žáka), mediální zpráva (jedna pro každého žáka), pracovní list Analýza článků (pro skupiny), vhodný počítač s projektorem
Výukové cíle – Žák je po lekci schopen...:

- vyjmenovat základní postupy při tvorbě mediální zprávy;
- uvědomovat si potřebu komparace informací z různých zdrojů s vyvozením vlastních závěrů;
- hodnotit důvěryhodnost mediálního sdělení dle základních kritérií.

Spojení s RVP: ČJL-9-1-01, ČJL-9-1-02, ČJL-9-1-03, ČJL-9-1-07, ČJL-9-1-08, ICT-9-1-01, ICT-9-2-02, ICT-9-2-04, VO-9-1-05, VO-9-1-08, VO-9-1-09, VO-9-4-05, VZ-9-1-14, VZ-9-1-16, klíčové kompetence a průřezová témata
Spojení s NIQUES (informační gramotnost): Formulace problému (vynikající), určení typu informace (vynikající), určení typu informace (standardní), posouzení relevance a úplnosti informací (vynikající), posouzení pravdivosti informací (vynikající), zpracování textu (minimální), analýza získaných informací (vynikající), modelování a simulace (standardní), plánování postupu řešení (minimální), vytváření originálního díla (vynikající), uplatňování právních norem (vynikající), každodenní život s technologiemi (minimální)
Výukové aktivity dle E-U-R:

- evokace: brainstorming,
- uvědomění: přednáška a analýza mediálních zpráv,
- reflexe: SMELL test.

Osnova
Brainstorming
Časový plán: 10 minut: 5 min. generování nápadů, 5 min. vyhodnocení
Jako cíl lekce je žákům prezentováno hodnocení mediálních sdělení, která vědomě i nevědomě ovlivňují jejich pohled na svět. Především je lekce zaměřena na zpravodajství, jehož podstatou by mělo být objektivní představení aktuální události nebo tématu, které jsou široce diskutovány. Protože tato sdělení formují přesvědčení lidí, je zvažování jejich důvěryhodnosti a kritické myšlení důležité.

Cíl lekce je následně připodobněn k internetovým hoaxům nebo řetězovým zprávám. Na nich je patrné, že ne vše, co je na internetu napsané, je pravda. Po položení otázky žákům, podle čeho určují, že obsahu e-mailu věří, nebo ne, lektor zdůvodní obsah lekce. U mediálních zpráv, stejně jako u jmenovaných typů e-mailů mohou být ty nedůvěryhodné na první pohled rozeznány tím, že si je čtenář vědom typických rysů, které snižují důvěryhodnost sdělení, případně že dojde k porovnání obsahu sdělení z různých nezávislých zdrojů.

Aby si žáci uvědomili, co vše lekce pokrývá, je první aktivitou brainstorming, kde žáci mají jmenovat různá média, která používají, nebo znají. Následně jsou

v rámci vyhodnocení vyškrtána ta, která nenabízí zpravodajství, a naopak jsou vyzdviženy základní kanály, tj. televize, rádio (rozhlas), tisk a internet.

Přednáška o mediální manipulaci
Časový plán: 15 minut
Přednáška navazuje na předchozí aktivitu společnými rysy všech jmenovaných médií, kdy mezi jejich funkce patří informování, učení, ovlivňování a zábava. V rámci jednotlivých pořadů se tyto funkce mísí, ale určitý typ vždy akcentuje jednu ze jmenovaných rolí. Primární funkcí zpravodajství by mělo být informování, a to co nejvíce objektivní, ne ovlivněné názorem reportéra. Následně jsou žáci upozorněni na vliv různých subjektů na obsah mediovaných sdělení (vlastník média, PR a tiskové agentury, komerční sféra a reklama, ale především občanské žurnalistiky) a způsobu vzniku zprávy, která bývá založena na vyprávění příběhu. Ten z časových důvodů musí být redukován, omezená je také možnost ověřování informací, protože příjemci chtějí sdělení co nejrychleji (což je jeden z faktorů, který vede k převaze internetového zpravodajství nad tradičním). Dále jsou žákům představeny různé způsoby úmyslné i neúmyslné manipulace v médiích se zaměřením na obrazové informace. Navazuje upozornění na to, že argumenty, jejichž cílem je přesvědčit o pravdivosti sdělení, by měly být podloženy důvěryhodným zdrojem informací, a naopak jsou žáci upozorněni na argumentační fauly, se kterými se mohou setkat. Vhodné je s ohledem na využívanost zpravodajství přirovnávat ho k činnostem youtuberů a influencerů na sociálních sítích, se kterými mají dospívající častěji osobní zkušenost.

Analýza mediálních zpráv
Časový plán: 20 minut: 5 min. čtení, 5 min. skupinová práce, 10 min. prezentace
Pro hlavní aktivitu je nutné zvolit kontroverzní téma, které je žákům známé. Buď se proto musí jednat o problematiku, která se jich samotných dotýká nebo která je dlouhodobě diskutována v celé společnosti. Pro lekci byla vyzkoušena kauza možného zkreslení uprchlické krize v televizi Prima v roce 2016, kdy údajně jeden z uprchlíků prohlásil, že v přemalovaném kravínu bydlet nebude. Toto zaměření bylo zvoleno proto, aby byl jasně prezentován vliv médií na formování masového názoru na určitou problematiku a také aby byl problematizován rozšířený negativní názor české veřejnosti na uprchlickou krizi. Lekce se nesnaží o boj proti xenofobii, jen upozorňuje na to, že černobílý pohled na situaci není tak jednoduchý, protože oba názory mají oprávněné, ale i manipulativní postupy pro obhajobu svého přesvědčení. Žákům bylo zdůrazněno, že předmětem zpráv není hodnocení toho, zda uprchlíci jsou dobří nebo špatní, ale jak výše uvedená kauza byla prezentována televizí Prima.

Při zadání aktivity je vytvořeno šest skupin žáků a dvě vždy dostanou stejnou mediální zprávu, kterou analyzují. Všechny zprávy se týkají stejné problematiky,

ale jedna je manipulativní v jednom směru, druhá v opačném a třetí nabízí oba úhly pohledu na řešenou kauzu. Pro lekci byly zvoleny tyto zprávy:

- Manipulace: Reportáž TV Prima o iráckých uprchlících. *HateFree Culture* [online]. 2016 [cit. 2017-02-25]. Dostupné z: http://www.hatefree.cz/blo/hoaxy/1412-prima-uprchlici-irak
- Kauza „Byty jako přemalovaný kravín" má pokračování: Uprchlíci stále nejsou spokojeni a chtějí pryč z ČR. *Pravý prostor* [online]. 2016 [cit. 2017-02-25]. Dostupné z: http://pravyprostor.cz/kauza-byty-jako-premalovany-kravin-ma-pokracovani-uprchlici-stale-nejsou-spokojeni-a-chteji-pryc-z-cr/
- Kravín, měl říct o bytě podle televize uprchlík z Iráku. Šlo o manipulaci, brání se fond. *Lidovky.cz* [online]. 2016 [cit. 2017-02-25]. Dostupné z: http://www.lidovky.cz/premalovany-kravin-mel-rict-o-byte-podle-televize-uprchlik-z-iraku-slo-o-manipulaci-gzg-/zpravy-domov.aspx?c=A160212_170034_ln_domov_sk

Každý žák dostane svůj výtisk zprávy, aby se s ní mohl seznámit, každá skupina má ale jeden pracovní list, který vyplňuje pro analýzu sdělení. Formou otázek jsou žáci navedeni k tomu, aby se zamysleli nad různými faktory, které ovlivňují důvěryhodnost sdělení. Následně skupiny prezentují jim přidělený způsob podání kauzy, kdy se dvě skupiny se stejným článkem doplňují. Lektor upozorní na protichůdnost názorů, která dokládá potřebu srovnání informace z více různých zdrojů, kdy si každý může sám zhodnotit, které argumenty byly nejsilnější. Podstatné je, aby se rozhodl na základě dostatečného množství různě zaměřených informací.

SMELL test

Časový plán: 10 minut: 5 min. vyplnění, 5 min. prezentace

Poté, co jsou žáci seznámeni s různými pohledy na kauzu, dostanou zadání SMELL testu, který je zaměřený právě na hodnocení kvality mediálních sdělení. Vedle obecného pojmenování sledovaného faktoru jsou opět žákům přiblíženy oblasti k zamyšlení formou otázek. Rozdíl proti předchozí aktivitě je ten, že tentokrát vyplňují pracovní list individuálně a mohou reflektovat názory, které byly uvedeny i v jiných zprávách než jen v té, kterou sami četli.

Zkušenosti lektora

Téma lekce je pozitivně přijímáno učiteli, ale pro žáky je důležité od počátku přiblížit problematiku tomu, co odpovídá jimi pociťované potřebě. Jak se ukázalo již ve fázi evokace, pro žáky je základním médiem internet. Uvědomují si sice existenci jiných médií, jsou to ale pro ně zdroje, se kterými mají minimální osobní zkušenost, spíše z nich přebírají informace filtrované jejich rodiči. Pozitivní vliv na přiblížení problematiky mělo srovnání s e-mailovými zprávami typu hoax nebo řetězové zprávy, protože to jsou informace, se kterými mají žáci přímou zkušenost. Při brainstormingu žáci naráželi na problém, že řada internetových služeb slouží

stejně jako média i jako komunikační kanál, zejména sociální sítě. Evokace se proto ukázala jako podstatná pro vymezení toho, na co se mají soustředit v rámci dalších aktivit.

Prezentace v prvním testování lekce představovala mediální gramotnost podrobněji, žáci ale přibližně po 15 minutách ztráceli pozornost. Velmi je ale zaujaly praktické příklady manipulace, zejména obrazové. Proto při dalším testování byla prezentace zkrácena a zaměřena na základ lekce a praktické příklady. I když hodnocení grafů není snadné, manipulace s nimi vyvolala mezi žáky největší zájem, i když bylo nutné ji dostatečně okomentovat, aby si uvědomili, že graf v podstatě vyjadřuje informaci správně, ale způsob zpracování vede k tomu, že na první pohled je interpretován odlišně (podseknutá osa, 3D graf apod.).

Při práci s mediálními sděleními se ukázalo jako důležité zkrátit sdělení maximálně na rozsah dvě normostrany, protože delší texty byly žáky již při zadání hodnoceny tak, že to nejsou ochotni číst, a to i v případě, že písmo bylo příliš malé. Při čtení žáci často ignorovali formální zpracování a měli problém akceptovat vytištěný text jako internetové zpravodajství (např. negativně hodnotili, že je tam množství videí, když si je nemohou pustit, i když není jasné, kolik z nich by to udělalo, pokud by měli zprávu k dispozici v elektronické formě).

Žáci také často projektovali do aktivit svůj názor na uprchlíky i přes upozornění, že aktivita spočívá v tom, jak bylo vyjádření jednoho z uprchlíků ovlivněno prezentací ve zpravodajství televize Prima. V rámci diskuze proto byly důležité vstupy lektora, které upozornily žáky na slabiny jejich argumentace, např. že činí závěry z názorů uvedených v textu, ne z podložených tvrzení, které sice byly obsahem článku, ale následně byly relativizovány názorem reportéra. Velký problém měli žáci s tím, aby se zamysleli nad problémy, které by mohlo způsobit nekritické přijetí obsahu článku. Jako pozitivní se ukázalo, že když lektor přiblížil alternativní pohledy na problematiku, následující skupiny zahrnuly toto řešení do své prezentace, což znamená, že pochopily jeho sdělení. Lektor ale musí být schopen oprostit se od vlastního názoru a mít připraveny argumenty, aby zastával pozici „ďáblova advokáta“, tedy aby bez ohledu na vlastní přesvědčení byl schopný žáky vést k argumentaci podporující jejich názory, kdy se obvykle ukázalo, že pro své názory nedokáží formulovat objektivní důvody. Právě v tom okamžiku žáci často argumentovali tím, že se jedná o názor jejich rodiny, který nekriticky přijímají.

Důležitým aspektem v zadání se ukázalo formulování sledovaných kritérií ve formě otázek. Při testování lekce byly nejdříve použity heslovité formulace, aby zadání nebylo demotivující množstvím textu. Žáci ale měli problém s pochopením toho, nad čím mají přemýšlet. Otázky pro ně byly výrazně lépe pochopitelné. Pomohlo také jejich představení před tím, než žáci článek četli, takže dopředu věděli, na které části materiálu se mají zaměřit.

Po testování lekce také bylo sníženo množství zpráv, kdy původně měla každá skupina jiný text. Pro podporu zapojení více žáku a omezení vlivu dominantních

členů skupiny se ukázalo jako vhodné snížit množství žáků ve skupinách. Dominantní členové skupiny byli často motivovaní se projevovat v průběhu celé lekce, i když je lektor upozornil na nesprávné řešení položených otázek. Ostatní členové skupiny dominantnímu žákovi oponovali v rámci prezentace u několika prvních otázek, následně ale na svou aktivitu rezignovali. Právě to byl jeden z důvodů většího množství skupin s méně žáky. V rámci lekce se ukázalo jako pozitivní také zapojení učitele do jedné ze skupin, kdy žáci viděli, že i učitel má subjektivní názor na problematiku, ale je ochotný vyslechnout protiargumenty a diskutovat o nich.

Při zadání SMELL testu žáci neměli problém s pochopením sledovaných faktorů, ale spíše s tím, jestli mají test aplikovat na článek, který řešili ve skupině, nebo na celou problematiku. Bylo nutné jim zdůraznit, že i když hodnotí text, který četli, měli by zvážit, co v něm nebylo, ale mohlo by být, protože to slyšeli v rámci prezentace ostatních skupin.

Při hodnocení již první, pilotní realizace lekce bylo pozitivně komentováno téma a směr uvažování (Vyjádření učitele: „*Jinak se mi to líbilo, hlavně myšlenka "nebýt hloupou ovcí"*."), stejně jako využití pretestu a posttestu. Podobně jako lektor i učitel hodnotil negativně snahu předat příliš velké množství informací (část přednášky i délka mediálních sdělení, která byla žáky analyzována), což bylo následně upraveno. Výsledkem bylo i výrazně pozitivnější hodnocení lekce lektorem, učitelem i žáky.

3.3 Akční výzkum

Akční výzkum slouží k úpravám lekcí, kdy výzkumník spolupracuje se subjekty výzkumu při diagnostikování problému a tvorbě jeho řešení. Smyslem je akcí změnit stav, vyřešit lokální problém s empirickými podklady a umožnit opakování výzkumu v nových podmínkách, tj. přenositelnost pro řešení stejného problému v jiné lokalitě[402]. Výzkum měl smíšenou formu, pomocí kvalitativního pozorování a rozhovorů s různými subjekty byly zjišťovány názory na vzdělávání v knihovnách v informační bezpečnosti obecně i k navržené koncepci, kvantitativně formou smilesheetů byla zjišťována spokojenost žáků s lekcemi. Zapojení všech zúčastněných subjektů je možné označit jako 360° zpětnou vazbu. V souladu s možnostmi a cíli kvalitativního výzkumu jsou představeny reálné názory, se kterými se lze setkat. Nelze je zobecňovat, ale jedná se o východisko pro vytvoření nové teorie v oblasti názorů na problematiku této publikace.

Chevalier a Buckles[403] specifikují současné oblasti aplikace akčního výzkumu: organizace, psychologie, zdraví, gramotnost, vzdělání, pracoviště, komunitní roz-

402 HENDL 2008.

403 CHEVALIER 2013.

voj, zemědělské systémy, meziproduktové technologie, environmentální studia a zapojení veřejnosti (např. v politické sféře). Uplatnění zmiňují i v knihovnách, ale podrobněji jej nerozvádí. Uplatnitelnosti akčního výzkumu v knihovnách se více věnuje např. Civallero[404], který ho vidí jako paralelní proces pro knihovnictví založené na důkazu, který je stále silněji diskutován jako potřebný. S tím se ztotožňuje i Pickard, která uvádí, že *„akční výzkum se rychle stává jednou z nejpopulárnějších výzkumných metod v informačním a komunikačním výzkumu mezi lidmi v praxi.“*[405]

Akční výzkum je přístupem, který může nabývat různých forem, např. experimentální akční výzkum, induktivní akční výzkum, participační akční výzkum, participační akční výzkumná praxe a dekonstrukční akční výzkum. Zde je preferován induktivní akční výzkum, kdy je nejdříve identifikován pozorováním problém, po kterém následuje akce a reflexe. Tomuto přístupu odpovídá definice Lewina, kdy akční výzkum: *„[p]ředstavuje flexibilní, vědecký přístup k plánované změně, která postupuje přes spirálu kroků, z nichž každý se skládá z cyklu plánování, akce a zjišťování faktů o výsledcích akce.“*[406] Jedná se o spirálovitý proces, který nikdy nekončí, každá výzkumná fáze je následována akcí a evaluací, změna se pak promítá do nového cyklu výzkumu, který vede k novým akcím a evaluacím. I přesto je možné výsledky akčního výzkumu hodnotit, pokud se ukáže efektivita (v tomto případě vzdělávací) akce a její přijatelnost pro všechny dotčené cílové skupiny.

Akční výzkum je ve vzdělávání používán pro profesní vzdělávání učitelů, zkvalitňování kurikula nebo zlepšování edukační praxe[407]. Protože cílem je změna praxe v komunitě[408], je nutné, aby komunita přijala výzkumníka i výzkum. To vyžaduje zapojení (ne akademický odstup) při řešení výzkumu, při vyhodnocování výzkumu je nutné toto zapojení zohlednit a usilovat o co nejvyšší objektivitu a současně reálnost (ideálně ověřením správnosti pochopení zjištění u zkoumané komunity). Rozdíl přirozeného vývoje a akčního výzkumu je právě v striktním dodržení pravidel výzkumu.

K základním charakteristikám akčního výzkumu patří úzké spojení s praxí. Tomu odpovídá preference kvalitativního výzkumu[409], proto nelze výsledky zobecňovat. Protože k požadavkům na akční výzkum patří publikování výsledků[410], musí být popsány i se specifiky prostředí, kde byl výzkum realizován. Tak si následovníci, kteří jej budou chtít přenést do vlastní praxe, mohou zvážit míru společných

404 CIVALLERO 2007.

405 PICKARD 2013, s. 157.

406 LEWIN, K. Resolving Social Conflicts; Selected Papers on Group Dynamics. In: CHEVALIER 2013, s. 11.

407 PICKARD 2013, s. 157–158.

408 HENDL 2008, s. 136.

409 HENDL 2008, s. 136.

410 ZUBER-SKERRITT 2007, s. 415.

a odlišných charakteristik a tím také míru přenositelnosti. Další kritéria hodnocení kvality realizovaného akčního výzkumu jsou popsána v jeho závěru.

Prezentovaný akční výzkum představuje explorativní případovou studii. Byl realizován pro řešení praktických problémů a jako ukázka možné změny zahrnutím knihoven do vzdělávání o internetové bezpečnosti v praxi. Cílem výzkumu bylo prezentovat specifický přístup ke vzdělávání s použitím metod neformálního vzdělávání a aktivního učení s minimem materiálních požadavků a ukázat akceptaci všemi klíčovými osobami. V lekcích si děti pomocí aktivního učení samy vytvoří nové poznatky o rizikových formách komunikace, vhodného přijímání publikovaných informací a možných příčinách a důsledcích informačních hrozeb v prostředí internetu. Lektor působí jen jako průvodce dětí aktivitami a upozorňuje na získané poznatky. Vzhledem k cíli lekcí byl pro hodnocení efektivity zvolen Kirkpatrickův čtyřúrovňový model[411], který umožňuje sledovat krátkodobý i dlouhodobý vliv, jak z hlediska dojmu z lekce, tak zlepšení znalostí a dovedností.

Nejdříve je pozornost zaměřena na zúčastněné pozorování, v jehož rámci je popsán kompletní průběh lekcí v praxi. Pozorování se soustředí na společné poznatky platné pro všechny lekce, specifická zjištění pro konkrétní lekci byla jako zjištění lektora uvedena v kap. 3.2. Smilesheety, tedy jednoduchá zpětná vazba od žáků na to, jak se jim lekce líbila, a zúčastněné pozorování ukazují evaluaci na první úrovni Kirkpatrickova modelu. Ta se soustředí na aktuální reakce na lekci (spokojenost s prostředím, lektorem apod.). Pozorování ale také pokrývá druhou úroveň, tedy studijní výsledky (získané kompetence). S odstupem několika týdnů až měsíců po lekci byly uskutečněny rozhovory, jejichž dílčím cílem bylo zhodnocení dlouhodobého vlivu lekce na chování vzdělávaných, což představuje třetí úroveň Kirkpatrickova modelu. Čtvrtá úroveň modelu je určena k hodnocení přínosů lekce pro okolí (např. při dalším vzdělávání ve firmách), tato úroveň byla opět pokryta rozhovory s lidmi, kteří jsou v dlouhodobém kontaktu se vzdělávanými žáky. Protože se jedná o jeden výzkum, je nezbytné výsledky všech úrovní a metod (všechny použité metody uvádí Pickard[412] mezi základními pro akční výzkum) propojit a tím komplexně zhodnotit efektivitu navržené koncepce.

V rámci celého šetření byla uvažována etika výzkumu, která je v tom akčním složitější kvůli úzkému spojení s konkrétní praxí, kdy je problematická především anonymita. Protože ale šetření probíhalo několik let a ve spolupráci se dvěma knihovnami a čtyřmi školami, jsou konkrétní subjekty vzdělávání neidentifikovatelné. Současně měli všichni možnost neúčastnit se lekce, příp. se jí účastnit, ale neposkytnout data (mluvení tiše, odnesení produktů lekce), čehož ale využilo jen několik jednotlivců. V případě vzniku audiozáznamů byli žáci, jejich rodiče i uči-

411 KIRKPATRICK 1996.

412 PICKARD 2013, s. 165.

telé dopředu informováni prostřednictvím školy a byl od nich získán souhlas. Pokud se jej nepodařilo pro třídu získat, byla data z pozorování zaznamenávána jen pomocí terénních deníků. V rámci rozhovorů bylo s ohledem na nemožnost anonymizace zvoleno neanonymní řešení, se kterým všichni dotázaní souhlasili udělením poučeného souhlasu (viz příloha 1.4).

3.3.1 Prostředí výzkumu

Primární prostředí akčního výzkumu představovala Městská knihovna v Poličce. Ta byla vybrána díky zájmu knihovníků o internetovou bezpečnost[413]. Jednalo se o účelový výběr s využitím extrémního případu s ohledem na požadavek akčního výzkumu spočívající v nutnosti zájmu spolupracující komunity a v důvěře a společném cíli mezi autorem výzkumu a jeho subjekty. Výběr eliminoval problémy s nezájmem knihovny či školy se zachováním reálného (ne laboratorního) prostředí. Smyslem šetření bylo ověřit účinnost navržené koncepce s důrazem na uplatnění aktivního učení (viz kap. 3.1.1). Tato případová studie může sloužit jako ukázka, jak pozitivní mohou být výsledky zapojení knihovny do vzdělávání o internetové bezpečnosti s aplikací prvků aktivního, neformálního učení a nakolik pozitivní může být jeho hodnocení různými zúčastněnými stranami.

Polička je město s asi 9000 obyvateli a dvěma základními školami. Knihovna zprostředkovala kontakt s jednou z nich – Masarykovou základní školou. Tato škola vzdělává žáky z města a blízkých vesnic. Učitelé z obou stupňů školy jsou již několik let zvyklí navštěvovat s třídami lekce v knihovně, a to pravidelně několikrát do roka. Před realizací lekcí popsaných v této publikaci však měli zkušenost spíše s lekcemi zaměřenými na práci s textem, a to v tradiční i elektronické podobě. Právě v druhém případě se lekce zaměřená na hodnocení informací často dotýkala problémů internetové komunikace. I z toho důvodu učící knihovnice, vedení knihovny i školy pociťovaly zájem více téma rozvinout v samostatných lekcích. Iniciovali proto vstup knihovny do případové studie. Knihovnice a zástupkyně školy pro 1. stupeň představují pro výzkum tzv. gatekeepers[414].

Od počátku byl plánován koncepční přístup, kdy budou vzděláváni žáci všech ročníků, vždy jednou za rok, v tématu internetové bezpečnosti. Lekcím v Poličce předcházel kontakt s vyučujícími, protože ti rozhodují, zda se se svou třídou lekce zúčastní a propojí ji se svou aktivitou při formálním vzdělávání. Cílem setkání tedy bylo vybudovat si pozitivní vztah s touto cílovou skupinou akčního výzkumu. Byla diskutována významnost problematiky internetové bezpečnosti, klíčová témata

413 Jak již bylo uvedeno u vymezení akčního výzkumu, zájem cílové skupiny o změnu je podstatným předpokladem pro provedení akčního výzkumu, viz např. PICKARD 2013, s. 163.

414 PELIKÁN 2011, s. 234.

pro jednotlivé ročníky a také omezené znalosti pedagogů v této oblasti. Zájem učitelů o téma i realizaci v knihovně byl překvapivě pozitivní, a to při jejich vlastním vzdělávání i ochotě zúčastnit se lekce se svou třídou.

Pro ověření dopadů koncepce byly sekundárně lekce realizovány pro vybrané třídy v Knihovně na Křižovatce ve spolupráci se ZŠ Křídlovická, Brno, dále pak v ZŠ Pomezí (okres Svitavy), ZŠ a MŠ Blažkova, Brno a Taneční konzervatoři Brno. Všechny školy se do výzkumu po nabídce zapojily s velkým zájem. Ten vycházel z jimi deklarovaného významu tématu a omezeného řešení v současných podmínkách škol. Na školách nebyla realizována vždy celá koncepce, ale vybrané lekce po domluvě s učiteli a vedením škol a také pod vlivem potřeb revize lekcí (především po významnějších změnách).

- ZŠ Křídlovická byla zapojena podobnou formou jako Masarykova základní škola v Poličce. Lekce byly realizovány v knihovně jako rozšíření dlouhodobé spolupráce na vzdělávání žáků v informační gramotnosti. Rozdíl spočíval především v socio-demografii, jedná se o školu v krajském městě.
- Podobně velkou brněnskou školou je ZŠ Blažkova, která se nachází v okrajové čtvrti Brna. Lekce byly realizovány přímo na této škole pro ověření vlivu prostředí.
- ZŠ Pomezí proti tomu představuje malou školu v obci s přibližně 1200 obyvateli, která se nachází nedaleko Poličky. Spolupracuje tedy s knihovnou, kdy ale knihovnice často realizuje lekce přímo na této škole s ohledem na dopravu žáků. Na škole je vždy jedna třída v každém ročníku na 1.a 2. stupni.
- Poslední škola v akčním výzkumu, Taneční konzervatoř, představuje menší školu se specifickými zájmy žáků. Jedná se o víceletou střední školu. Lekce byly testovány jak pro nižší stupeň odpovídající 2. stupni základní školy, tak i pro starší žáky pro ověření vhodného nastavení věku cílové skupiny lekcí.

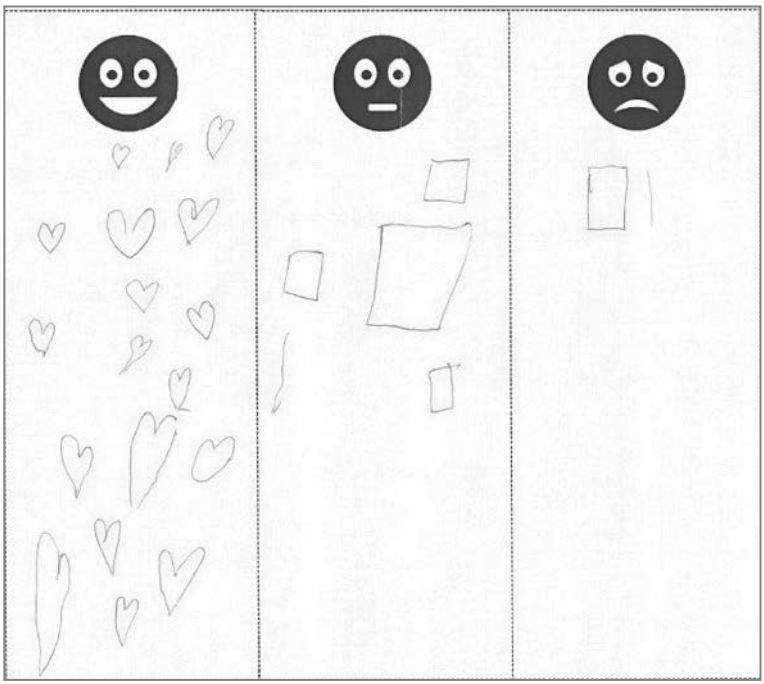
Omezení závěrů případové studie by v budoucnu měla být redukována využitím v odlišných prostředích a jinými lektory, což ale není předmětem této publikace. Příkladem takového ověření může být diplomová práce Jany Skládané[415].

3.3.2 Smilesheety

Od roku 2013 byly pro hodnocení lekcí využívány smilesheety. Ty měly formu jednoduchého dotazníku, kde pod tři emotikony s různými emocemi měl každý žák udělat jednu čárku. Pokyn k označení hodnocení žáci dostali vždy ihned po skončení lekce před jejich odchodem z místnosti, kde probíhala. Formulář ležel na stole v dostatečné vzdálenosti od lektora i učitele, aby žáci necítili obavu vyjádřit své hodnocení.

415 SKLÁDANÁ 2017.

Přesto někteří žáci, zejména na prvním stupni, chodili lektorovi nebo učiteli sdělovat, jaké hodnocení zaznamenali. Zájem o vyplnění hodnocení byl poměrně zřejmý. Na druhém stupni se však později ukázalo, že žáci necítili obavu v udělení hodnocení vůči lektorovi a učiteli, ale vůči spolužákům, zejména pokud chtěli uvést pozitivnější hodnocení než oni, jak později komentovali někteří učitelé. Z toho důvodu by v budoucnu pro druhé stupně mělo být využito odlišného přístupu, kdy smilesheety budou mít podobu malých individuálních formulářů s žádostí o komentář k udělenému hodnocení. Tento přístup byl již otestován jako vhodný v diplomové práci navazující na obsah této publikace[416]. Jak ilustruje Obrázek 3, některé třídy přistoupily k vyplnění kreativně. V jiných třídách ale docházelo k situaci, že alespoň jeden z žáků udělil více hodnocení. V případě, že počet hodnocení převyšoval počet žáků ve třídě, byl celý list z hodnocení vyřazen.



Obrázek 3 Ukázka vyplněného smilesheetu

Výsledky hodnocení jednotlivých lekcí ukazuje Tabulka 8. Lekce pro první stupeň byly vzhledem k snazší organizaci a s tím souvisejícímu zájmu učitelů realizovány vícekrát než lekce pro druhý stupeň. Hodnocení jsou seřazena podle data

416 SKLÁDANÁ 2017, s. 42–43.

realizace lekcí, kde je patrné mírně se zvyšující hodnocení při úpravách vzešlých z výsledků pozorování. Současně byly patrné negativní vlivy realizace lekcí za odlišných podmínek, než jsou doporučeny, např. v prostorách školy místo knihovny. Vliv těchto faktorů je popsán v rámci výsledků pozorování (kap. 3.3.3).

Tabulka 8 Výsledky smilesheetů pro jednotlivé lekce

Ročník	Název lekce	Datum	Prostředí	Pozitivní	Neutrální	Negativní
1	Výhody a nevýhody počítačů	9. 3. 2016	knihovna	16	2	2
		23. 3. 2016	knihovna	16	2	0
		18. 1. 2017	knihovna	14	2	1
		18. 1. 2017	knihovna	14	4	1
		27. 1. 2017	knihovna	24	5	1
		27. 1. 2017	knihovna	10	0	0
				94	15	5
2	Desatero bezpečného internetu	18. 11. 2015	knihovna	19	2	5
		18. 11. 2015	knihovna	28	1	2
		6. 4. 2016	knihovna	15	4	5
		13. 4. 2016	knihovna	24	6	4
		13. 4. 2016	knihovna	18	5	2
		7. 12. 2016	knihovna	17	1	2
		7. 12. 2016	knihovna	15	3	1
		8. 12. 2016	knihovna	13	6	2
				149	28	23
3	Digitální stopy v síti	30. 9. 2015	knihovna	24	0	0
		30. 9. 2015	knihovna	18	8	1
		7. 10. 2015	knihovna	16	4	3
		11. 5. 2016	knihovna	24	2	0
				82	14	4
4	Kdo je za monitorem	27. 5. 2014	knihovna	15	1	2
		9. 4. 2015	škola	13	18	0
		9. 4. 2015	škola	29	4	0
		7. 10. 2015	knihovna	19	1	0
		14. 10. 2015	knihovna	21	0	0
				97	24	2
5	Práce s informačními zdroji	2. 12. 2015	knihovna	16	5	1
		9. 12. 2015	knihovna	5	10	1
		10. 12. 2015	knihovna	13	10	1
				34	25	3
6	Mnoholičný lektvar	30. 5. 2013	škola	23	1	0
		30. 5. 2013	škola	21	2	0
		21. 5. 2014	knihovna	17	4	0
		21. 5. 2014	knihovna	20	0	2
		25. 5. 2016	knihovna	19	1	0

Ročník	Název lekce	Datum	Prostředí	Pozitivní	Neutrální	Negativní
		25. 5. 2016	knihovna	12	4	0
				112	12	2
7	Up and Download	20. 3. 2017	knihovna	0	5	20
		20. 3. 2017	knihovna	0	18	5
				0	23	25
8	Detektivky na Facebooku	9. 11. 2015	škola	13	19	11
9	Život mediální zprávy	8. 2. 2017	knihovna	3	3	8
		13. 2. 2017	knihovna	4	21	1
				7	24	9

Pro lekci pro 7. třídu sice nebylo získáno pozitivní hodnocení, ukazuje se ale výrazné zlepšení hodnocení po zjednodušení obsahu lekce. Po druhém testování došlo ještě k dalšímu zjednodušení obsahu, které je již zapracováno do kap. 3.2.7. Z pozorování i reakcí učitelů je patrné, že hodnocení by již při druhé realizaci bylo pozitivní, kdyby se žáci navzájem nesledovali při vyplňování smilesheetu, kdy pociťovali potřebu vyjádřit odstup k lektorovi, i když je evidentně lekce bavila. Hodnocení pro 8. třídu je ovlivněno získáním výsledků jen z jedné realizace lekce, která proběhla v prostředí školy, kdy žáci negativně reflektovali to, že nebyla dodržena přestávka ve výuce. Negativní hodnocení lekce pro 9. třídu je významně ovlivněno první realizací, po které byla lekce výrazně upravena.

Hodnocení lekcí pro 2. stupeň je poznamenáno zařazením také prvních testovacích běhů lekcí, po kterých došlo k úpravám na základě pozorování. Uvedené komentáře k sníženému hodnocení v smilesheetech vychází z komentářů žáků a učitelů během lekce a po jejím skončení. Proto je hodnocení lekcí pro druhý stupeň s ohledem na výše uvedené považováno za pozitivní i vzhledem ke konzervativnějšímu přístupu žáků k řešeným tématům. Limitem výsledků je také nutnost vyřazení formulářů celých tříd při nevhodném vyplnění opakovaně stejnými žáky. Výsledky smilesheetů tedy pokrývají na rozdíl od pozorování v následující kapitole jen část realizovaných lekcí.

3.3.3 Zúčastněné pozorování lekcí

Zúčastněné pozorování je často součástí akčního výzkumu. Jeho prostřednictvím dochází ke sledování efektivity zvoleného přístupu a na základě vyhodnocení stavu k úpravám lekce. K této metodě patří omezená možnost zaznamenání veškerých podnětů, zejména při paralelním výskytu. Proto v souladu s doporučeními[417] bylo vedle pozorování využito smilesheetů (kap. 3.3.2) a rozhovorů (kap. 3.3.4).

417 Např. PELIKÁN 2011, s. 209–210.

Cílem zúčastněného pozorování bylo potvrzení akceptace navržených lekcí o informační bezpečnosti žáky a učiteli. Proto bylo sledováno především to, jak žáci reagují na postupy neformálního vzdělávání i konkrétních typů aktivit a jejich přijetí simulace reálné online komunikace. Šetření probíhalo v letech 2013 až 2017. Opakování potvrdilo saturaci vzorku a možnost uzavřít akční výzkum v této fázi, protože zúčastněné pozorování nepřinášelo nové výsledky, přestože kolektivy tříd byly velmi odlišné a poslední lekci realizovaly místní knihovnice, výzkumnice byla přítomna v roli pozorovatele a pomocníka.

Všechny lekce proběhly v čase běžné výuky, jako alternativní náplň dvou vyučovacích hodin. Po každé lekci byl diskutován její průběh (fáze akce) s knihovnicí zkušenou ve vzdělávání a byly formulovány požadavky na úpravy v návaznosti na pozorované reakce dětí a stručný komentář učitelů po lekci. Definované úpravy byly zavedeny v následujícím běhu. Každá lekce prošla odlišným počtem testování:

1. Výhody a nevýhody počítačů: 7 pozorování (124 žáků)
2. Desatero bezpečného internetu: 9 pozorování (238 žáků)
3. Digitální stopy v síti: 8 pozorování (193 žáků)
4. Kdo je za monitorem: 15 pozorování (366 žáků)
5. Práce s informačními zdroji: 4 pozorování (82 žáků)
6. Mnoholičný lektvar: 8 pozorování (190 žáků)
7. Up and download: 2 pozorování (48 žáků)
8. Detektivky na Facebooku: 4 pozorování (115 žáků)
9. Život mediální zprávy: 2 pozorování (42 žáků)

Bylo nezbytné založit lekci na znalostech a zkušenostech žáků (fáze evokace), proto jejich zapojení bylo primárním ukazatelem, zda je lekce vhodně postavená. Hlavní cíl lekce spočívá v tom, že si děti samy, aniž by jim to někdo řekl, uvědomí, jaké činnosti v informačním prostředí jsou rizikové a jakými postupy mohou hrozby nebo negativní dopady útoku omezit (fáze uvědomění). To by mělo být přeneseno po lekci do jejich reálné aktivity na internetu. Tu si v lekci žáci vyzkouší ve fázi reflexe, jejímž smyslem je ukotvení poznání z předchozí aktivity. Zásadním výsledkem pozorování tedy bylo ověřit, že děti reagují na aktivity uvedeným způsobem, a to nejen na úrovni znalostí, ale také formou reakcí na postupy aktivního učení. Pokud tomu tak nebylo, v rámci následujícího cyklu akčního výzkumu došlo k úpravě lekce a jejímu opakování pro ověření nově nastavených činností.

Pozorování bylo vyhodnocováno na základě otevřeného kódování terénních poznámek a audiozáznamů lekce (ty vznikly jen k první sérii lekcí, kdy bylo zjišťováno nejvíce podnětů, proto by bylo náročné zachycení jen pomocí terénních poznámek). Vliv změny učitele bude patrný i při běžném nasazení lekce v knihovnách, kdy lekci nevede učitelka, ale knihovnice, tedy osoba, která děti vzdělává výjimečně, čímž je omezen tzv. Hawthornský efekt[418]. Pomocí záznamových technik

418 MAŇÁK 2005.

byly kvalitativně vyhodnocovány výskyty sledovaných jevů[419]. Podrobnější informace k zpracování dat jsou popsány v původní dizertační práci[420].

Výsledek pozorování je v souladu s principy etnografického přístupu prezentován formou analytického interruptu v podobě chronologie[421]. V rámci této kapitoly jsou shrnuty základní poznatky, které byly patrné při realizaci celé koncepce. Jejím cílem je upozornit na společné rysy pro všechny navržené lekce, ale také změny v přístupu, které byly zjištěny především s přelomem v 5. třídě, kdy žáci změnili přístup k různým aspektům realizovaných lekcí. Analýzou bylo definováno pět tematických okruhů: místo realizace lekcí, osoba učitele (základní školy), forma lekcí, práce jednotlivých žáků (včetně žáků se specifickými výukovými potřebami) a volba tématu. Tyto výsledky se proto spíše zaměřují na organizační než obsahové aspekty lekcí, obsah z hlediska pozorování byl již předmětem popisu v kap. 3.2 (části Zkušenosti lektora).

3.3.3.1 Knihovna jako místo realizace lekcí

Lekce byly testovány ve třech školách a ve dvou knihovnách (každá pak v rámci spolupráce s jednou školou). V rámci školy se žáci více soustředili na dodržování režimu, na který jsou v tomto prostředí zvyklí, např. z hlediska délky lekce a přestávek, omezené aktivity a především spolupráce mezi žáky, i pokud byly aktivity skupinové. Vliv místa byl zřejmý v tom, že jakmile žáci slyšeli ve škole zvonění, trvali na přestávce a její nedodržení výrazně negativně ovlivňovalo jejich motivaci, naopak v knihovně byl čas vnímán výrazně odlišně a žáci neměli problém soustředit se při vhodném nastavení aktivit v průběhu celé lekce, která bez přestávky pokrývala dvě vyučovací hodiny.

Pokud lekce probíhaly v knihovně, žáci byli uvolněnější, aktivnější a méně se obávali vyjádřit svůj názor nebo odpověď, u které si nebyli jisti správností. Situováním lekce do knihovny bylo také omezeno sledování charakteristik projevů nerelevantních pro téma lekce. I přesto starší děti (od 5. třídy), zejména dívky, poměrně často upozorňovaly na jazykové nedostatky v písemných projevech spolužáků. Podobně je tomu s výzvou k uvolnění projevů žáků, které jsou základem aktivního učení. Při něm je vítán jakýkoli příspěvek žáků, třeba i nesprávný, protože může vést k zamyšlení, kde je jeho problém. Již osoba učitelky toto do určité míry omezovala, což bylo patrné i na tom, že před vstupem do místnosti či do knihovny učitelky upozornily žáky, že se mají chovat tiše a mluvit až na vyzvání, což je proti principům aktivního učení. To se v knihovně po krátkém čase vždy

419 Dle PELIKÁN 2011, s. 210–211.

420 KOVÁŘOVÁ 2015.

421 PELIKÁN 2011, s. 234–235.

podařilo odbourat, opět ale ve škole děti významněji setrvávaly v zažitých požadovaných stylech chování.

Situování lekcí do knihovny může být přínosné nejen s ohledem na průběh lekce, ale může sloužit i pro navázání vztahu mezi žáky a touto institucí. Pomocí lekce knihovna žákům ukazuje, že jim může nabídnout něco, co je pro ně osobně přínosné a zajímavé. Po lekcích se žáci často dotazovali knihovnice, co je potřeba, aby mohli využívat služeb knihovny, někteří z nich si odnášeli domů registrační formulář, který si sami vyžádali.

S volbou místa jsou spojena ale i určitá negativa. Předně je pro realizaci lekcí nutné materiální a prostorové vybavení, byť jsou lekce úmyslně navrženy tak, aby tyto požadavky byly co nejmenší. Přesto se při lekcích někdy objevily organizační nedostatky, které by zřejmě ve škole nebyly, např. nedostatek místa pro židle žáků tak, aby všichni dobře viděli na tabuli a promítanou prezentaci. Problémem může být také čas, který žáci potřebují pro přesun mezi školou a knihovnou, což může narušit výuku. I v případě blízkosti obou institucí je většinou čas pro přesun odečten z časové dotace pro lekci, která pak netrvá 90 min. (dvě vyučovací hodiny), ale v případě výuky v prostorách knihovny se lekce zkracovaly obvykle na 70–80 minut. Tento časový limit klade na lektora vysoké nároky v řízení aktivit v rámci daného času, aby vždy bylo dostatek prostoru pro klíčové části lekce.

3.3.3.2 Osoba učitele

Akceptace lekcí učitelem je důležitým předpokladem pro jejich efektivitu. Názor učitele žáci často vycítí, což ovlivní jejich vlastní postoj k lekci. Současně pozitivní názor vede k návaznosti na lekci v běžné výuce, což podporuje její dopad. Při dlouhodobé spolupráci se ukázalo, že v rámci školy se přenáší mezi učiteli zájem o lekce vlivem zkušenosti i s jinými lekcemi v koncepci. To ukazuje na způsob, jak koncepci rozšířit do prostředí celé školy. Není nutné trvat na tom, aby se všechny třídy lekcí účastnily, ale naopak spíše začít s motivovaným pedagogem, jehož názor ovlivní ostatní. Ti se necítí donuceni lekce navštívit, dojde k tomu na základě jejich vlastního přesvědčení.

Osoba učitele se ukázala jako silný faktor pro průběh lekce. Během některých lekcí se učitel po předání dětí vzdálil a vrátil se po skončení lekce, v jiných třídách se zapojil do realizovaných aktivit, v jednom případě třídu nedoprovázela učitelka, ale vychovatelka, v ostatních případech učitel přihlížel lekci. Při účasti vychovatelky se děti chovaly uvolněně, a to i na úkor pozornosti. Také necítily takové zábrany v projevech šikany dívky, která již na lekci přišla s pláčem, protože ji uhodil spolužák, a následně se odmítla zapojit do aktivit v lekci. Proti tomu v případě, že učitel na lekci nebyl přítomný, ale děti na ni přivedl, nebo se dokonce do aktivit zapojil, se děti chovaly srovnatelně jako při pasivní účasti učitele.

V rámci úprav byl vždy po lekci učitel požádán o rychlou zpětnou vazbu, než se žáci připraví k odchodu. Učitelé lekce hodnotili velmi pozitivně, často i v případě, kdy si lektor uvědomoval slabiny daného testu. Učitelé oceňovali aktivní a kooperativní učení, výukové hry a také méně časté výukové metody (např. dramatickou výchovu). Z hlediska obsahu byl patrný primární zájem učitelů o negativní aspekty internetu, i když ne vždy se shodli, které z těchto negativ jsou podle nich pro žáky v daném ročníku nejdůležitější. Učitelé usilovali o přesvědčení žáků, že by proti internetu měli upřednostňovat jiné činnosti:

> *„Učitelka mi pak říkala, že děti ve škole říkají hodně věcí, a že třeba FB je pro děti přeci zakázaný a když to řeší s rodiči, tak že rodiče „zatloukají" [sic!] protože nemají čas děti a internet řešit. (...) Chtěli by nějakou „odpočinkovou" lekci pro druháky, ve kterých [sic!] by se děti dozvěděly o tom, že na FB by být neměly, ještě víc jim zdůraznit výhody toho, proč není nezbytné mít v 7 letech net, smartphone atp., protože tam byly 2 holčičky, které na netu nikdy nebyly (protože mají rodiče, kteří jim věnují čas a lítají s nimi venku...)*" (e-mailová komunikace s knihovnicí z 8. 12. 2016)

Proti tomu žáci projevovali větší spolupráci s lektorem, pokud jim internet neprezentoval jako něco negativního, ale spíše se snažil o objektivní přístup s poukázáním na klady i zápory tohoto nástroje a možnosti, jak internet mohou využívat, aby možná rizika omezili.

3.3.3.3 Volba tématu a náročnosti

Při zahájení lekce se děti posadily vždy odděleně chlapci a dívky. Na téma reagovaly nižší ročníky s nadšením, starší s pozitivním odstupem, zejména když jim bylo oznámeno, že v knihovně nebudou číst, ale věnovat se internetu. Děti ve všech třídách vnímaly jako přirozené, že do knihovny téma patří, protože vidí, že do ní patří také počítače a internet. Nálada se nezměnila ani v okamžiku uvědomění, že nebudou pracovat se samotným internetem, ale budou se jen o něm bavit a simulovat jej. Žáci od nízkých ročníků projevovali poměrně obsáhlé znalosti, zejména pokud se jednalo o komunikační služby. Učitelé byli často rozsahem těchto znalostí překvapeni. Proti tomu se ale ukázalo, že žáci často měli problém při řešení tématu nad rámec stereotypního využití několika málo služeb.

V případě některých bezpečnostních opatření si žáci uvědomovali, že je mohou využít sami, ale ne tolik, že jich může využít někdo jiný. To opět ukazuje, že žáci mají poměrně dobré znalosti, ale jejich aplikace na reálné situace již tak dobrá není. Např. možnost uvádění nepravdivých informací byla dětmi jmenována ve všech 4. třídách. Tento postup často děti viděly u sebe, ale obvykle si ho již nespojily s druhou stranou komunikace, protože po aktivitě tato možnost ochrany identity oproti blokování jiných uživatelů nebyla uváděna dětmi, ale doplňována lektorkou.

Volba tématu lekce pro konkrétní ročník je důležitá, aby byly řešené situace již pro žáky představitelné z hlediska jejich praktických aktivit, ale současně aby byli seznámeni s vhodnými postupy ještě dříve, než se většina z nich s daným problémem setká. Jako východiska byly použity výzkumy chování žáků na internetu, témata definovaná pro jednotlivé stupně v RVP a konzultace s učiteli na základní škole. I přesto byly některé lekce po vyzkoušení zhodnoceny jako pro žáky nevhodné z důvodu jejich přílišné náročnosti (pro 2. třídu základní principy fungování internetu a pro 3. třídu základní služby internetu) a byly v koncepci vynechány a nahrazeny jinými. Přestože stejně jako ostatní lekce byly i tyto založeny na herních a praktických aktivitách, žáci měli problém v samostatné práci, protože nemohli navazovat na předchozí znalosti a zkušenosti, a to např. i pokud se jednalo o vyhledávání informací na internetu (3. třída). To potvrzuje sice dobré, ale jen úzce zaměřené znalosti žáků o internetu.

3.3.3.4 Forma lekcí

Všechny realizované lekce byly založeny na metodách RWCT Reading and Writing for Critical Thinking (čtením a psaním ke kritickému myšlení), což zasazovalo problematiku do aktivit knihoven a také do informační gramotnosti. Forma lekce založená na výukovém rámci E-U-R (evokace, uvědomění, reflexe) byla učitelům ve většině zapojených škol známá z předchozích lekcí ve spolupráci s knihovnou, nové bylo ale téma informační bezpečnosti.

V souladu s teorií[422] se po prvním odbourání bariér zapojením několika málo jedinců do aktivity podařilo aktivizovat většinu třídy. Lze tedy konstatovat, že až na výjimky došlo k naplnění cílů fáze evokace, kdy si žáci z chaotických a roztříštěných zkušeností zformovali vědomostní základ již známého pro následující činnosti, které jej rozvíjí a tímto spojením dochází k dlouhodobějšímu zvnitřnění (interiorizaci) a hlubšímu porozumění[423]. Současně došlo k učení, když byly zjištěny a opraveny chybné názory a znalosti. Vlivem navázání na existující znalosti by mělo dojít k dalšímu klíčovému důsledku evokace, vzbuzení vnitřního zájmu žáků řešit stanovenou problematiku, protože si jsou vědomi jeho smyslu a dokáží se s ním ztotožnit[424]. Jak ukazuje popis zkušeností lektora z lekcí (kap. 3.2), došlo ke strukturování poznatků navázáním nových na staré, např. že si žáci uvědomovali, proč by aktuálně na internetu postupovali daným způsobem[425].

V rámci aktivit se ukázalo u nižších i vyšších ročníků jako pozitivní, pokud byly do lekce zapojeny pohybové aktivity. Zejména pokud mělo dojít k nějaké interakci

422 GRECMANOVÁ 2000, s. 31.

423 STEELOVÁ 2007a, s. 24.

424 STEELOVÁ 2007a, s. 24.

425 STEELOVÁ 2007a, s. 19.

s lektorem, bylo to pro něj usnadněním činnosti (např. nemusel se po místnosti pohybovat sám, aby při hře Člověče, nezlob se, distribuoval kostku skupinám), ale současně to vedlo k většímu zapojení dětí, vyšší motivaci a také udržení pozornosti. Většina aktivit je kooperativních s cílem umožnit každému žáku využít pro výsledek činnosti své silné stránky a v případě těch slabých využít podpory ostatních členů skupiny.

Z hlediska zvolené formy je důležité, aby lektor přijal své postavení jako průvodce žáků v tématu a jeho zapojení nebylo řízením dětí. Lekce jsou nastaveny tak, aby žáci došli sami k uvědomění základních poznatků. Lektor jen doplňuje nebo upřesňuje vyjádření dětí na základě jejich zkušeností a aktivit, které si v lekci vyzkoušely. Důležité je také citlivé hodnocení žáků (např., i když se jedná o soutěž, tak neříkat „*tady ti dva pracovali pěkně*“, když všichni pracovali v rámci okolností tak, jak byli schopni). Někdy ale pochvaly jednotlivců byly naopak cílené, např. pro vyzdvižení výsledku slabého žáka ve třídě (tuto pochvalu někdy vyjádřil lektor, jindy učitel). V lekcích je snahou spíše reagovat na výkon žáků pozitivně, kdy v případě ne zcela správné odpovědi je žák pochválen, ale současně lektor upřesní správnou odpověď, neuzavře otázku nepřesným sdělením.

Žáci se do lekcí zapojovali aktivně, i když tato aktivita byla výrazně vyšší u nižších ročníků. V případě vyšších ročníků byl patrný odstup vůči lektorovi, ale i tak žáci jen výjimečně neakceptovali nastavené aktivity. Aktivně se zapojili téměř všichni, vždy po celou dobu lekce. Pokud došlo k zaměření pozornosti jiným směrem, bylo velmi krátké (v řádu vteřin), např. při objevení zajímavé knihy v regále. Užitečné postupy žáci spontánně vykřikovali a vzájemně komentovali (u nižších ročníků více, ale tyto projevy byly patrné až do 9. třídy).

Individuální i skupinové aktivity jsou podkladem pro sdílení v rámci celé třídy. I zde se ukázaly postupné změny v přístupu žáků. Zatímco na prvním stupni bylo často nutné limitovat, kolik produktů bude sdíleno, protože téměř každý chtěl ukázat výsledek své činnosti, případně doplnit k řešenému tématu zkušenosti vlastní nebo zprostředkované (např. k chování rodičů na internetu, někdy i nevhodným způsobem, např. když žáci poukazovali na to, jak vypadá silné heslo tím, že řekli, jaké heslo využívá jejich rodič). Proti tomu již v 5. třídě byl patrný opačný problém, kdy žáci vnímali spíše negativně, pokud se měli podělit o výsledky své aktivity. Proto bylo nutné, většinou náhodně, určit, kdo bude mít roli prezentujícího. Náhodnost omezovala pocit nespravedlnosti, že se ostatní této aktivitě mohli vyhnout.

Pro mladší děti mohla představovat problém aktivita založená na písemném projevu, který je pro tyto děti namáhavý a časově náročný. Množství čtení a psaní bylo nastaveno v rozsahu, který byl pro většinu žáků daného ročníku zvládnutelný, což bylo ověřeno testováním. Naopak starší žáky bylo nutné přesvědčit o kompetencích lektora a o smyslu předmětu lekce, protože téma internetu mohou považovat za zvládnuté, podléhají přesvědčení, že knihovník jim k tématu

nemá co říci. Tento zlom v motivaci byl patrný mezi prvním a druhým stupněm základní školy, přechod bylo ale možné sledovat již v druhém pololetí 5. třídy.

3.3.3.5 Práce jednotlivých žáků

Sdílení poznatků dětí neprobíhalo jen s lektorkou, ale také mezi dětmi samotnými, lze tedy vysledovat tzv. peer teaching, který patří k základním prvkům aktivního učení[426]. Při přijetí nastavené formy aktivního učení je zásadní odbourání omezení se na základě kvality či kvantity činnosti. Klíčová je jakákoli aktivita, která je následně otestována, a dítě samo získá vědomí úspěšnosti zvoleného postupu. To ještě při zapojení sociální interakce a principu tzv. „*lešení*" zvyšuje efektivitu učebního procesu[427]. Vzhledem k tomu, že poznatky staví na znalostech a dovednostech jednotlivců, kteří sice prochází stejnou aktivitou, ale různým způsobem, je naplněna i podmínka individualizace učení a podpořeno zapojení vnitřní motivace žáků, protože poznávají nové informace v oblasti, která je pro ně zajímavá a je součástí každodenního života[428].

Přestože v rámci týmových aktivit se často (zejména ve vyšších ročnících) někteří žáci nezapojovali, jen výjimečně celou aktivitu za tým provedl jeden dominantní člen. V takových případech se mu ostatní pokoušeli oponovat. Pak záleželo na zásahu lektora i motivaci členů skupiny, zda kooperativní práce bude naplněna nebo dominantní člen prosadí své názory i přes nesouhlas ostatních. Přestože aktivity obvykle nejsou podávány jako soutěž, žáci z nižších ročníků je tak často vnímali a usilovali o lepší výsledek než ostatní, příp. o korekci podle nich nesprávného názoru spolužáků na řešené téma. Proti tomu ve vyšších ročnících byla častěji patrná vzájemná podpora jednotlivých skupin, které spolu nesoutěžily (spíše se argumentačně vyhraňovaly vůči lektorovi než proti sobě).

Osobní zkušenosti se ukázali jako nejčastěji sdílená informace ve všech třídách. Žáci právě na základě nich definovali faktické informace (např. jaké činnosti internetová služba umožňuje) i postoje („*nikdy se mi to nestalo, takže to podle mě není takový problém, abych to musel řešit*"). Právě ztotožnění se s předávanými poznatky mělo výrazný vliv na hodnocení lekce. Zejména u vyšších ročníků proto byla klíčová argumentace lektora, kdy musel předložit dostatek důkazů o svých tvrzeních, aby narušil pevné přesvědčení dospívajících o řešené problematice. Proti tomu mladší žáci akceptovali autoritu lektora, kdy nebylo nutné tolik akcentovat důkazy, ale spíše předávané informace uvádět na praktických příkladech pro menší požadavky na abstrakci.

426 HANSEN ČECHOVÁ 2006, s. 25.

427 STEELOVÁ 2007a, s. 16–17.

428 STEELOVÁ 2007a, s. 18–19.

V rámci ztotožnění se s řešenými informacemi se ukázaly u některých tříd pozitivní reakce, kdy žáci v rámci diskuze naváděli právě přes své osobní zkušenosti k problémům, se kterými se setkali, a měli velký zájem diskutovat podrobnosti protiopatření na velmi konkrétní situace. Děti se snažily zjistit, jak řešit problémové situace, které znají (např. „*A co mám dělat, když mi začne nadávat?*"). V tomto případě po odpovědi lektorky někdy žák ještě několikrát konkretizoval situaci, pro kterou hledá řešení. Tento přechod k řešení reálných problémů žáků byl zcela neřízený lektorkou, v souladu s aktivním učením děti rozhovor iniciovaly samy. To podporuje nastavení lekcí, které se dotýkají možných problémů dětí v prostředí internetu ve věku, pro který byly určeny jednotlivé lekce.

Z hlediska zapojení žáků se ukázala jako důležitá příprava na práci žáků se specifickými vzdělávacími potřebami a poruchami učení. Zejména na prvním stupni tito žáci pozorovali intenzivní aktivitu spolužáků, které nebyli schopni. To často vedlo k jejich neochotě zapojit se do práce se spolužáky, proto jim byla nabídnuta alternativní, individuální aktivita v tématu, kterou přijali. Jen jednou na tuto změnu reagovala negativně učitelka, protože se jednalo o autistické dítě a ona nechtěla podporovat jeho vyloučení. V jiném případě dokonce učitelka i při nevhodném zásahu lektora (vzhledem k problému žáka) do toho nevstoupila a až po lekci lektorku seznámila s diagnózou. Její včasná znalost by přitom vedla k výrazně jiné práci s tímto žákem. Z toho vyplývá co nejvyšší snaha lektora o to, aby mu včas byly oznámeny specifické nároky žáků, i když vždy záleží na ochotě učitelů tyto informace sdělovat. Protože i přes upozornění, aby specifické nároky žáků učitelé oznamovali předem, tak se to až na výjimky nestalo a tento faktor musel lektor reflektovat až po zjištění na lekci (viz například dvě výše uvedené situace). Naopak inkluze žáků, nejčastěji původem cizinců s dosud omezenými znalostmi jazyka, ale i zdravotně znevýhodněných žáků byla podpořena skupinovými aktivitami, kdy si žáci běžně bez vyzvání pomáhali.

3.3.3.6 Shrnutí průběhu lekcí

Zúčastněné pozorování splnilo svůj cíl, došlo k potvrzení teorie aktivního učení v rámci navržených lekcí, a to ve všech fázích. Současně se potvrdil edukační cíl lekcí. K těmto výsledkům došlo i přes to, že třídní kolektivy se velmi lišily, a to jak na úrovni žáků, ze kterých byly složeny, tak také ve skupinové dynamice. Tím je potvrzena přenositelnost lekcí s udržením dosažitelných cílů lekce navzdory mnoha specifikům kolektivu, je ale v budoucnosti nutné ověřit přenositelnost i do odlišných prostředí.

Mezi faktory ovlivňujícími osvětu v informační bezpečnosti patří velikost obce, kde bylo šetření realizováno. Menší město umožnilo intenzivnější kontakt mezi výzkumnicí a subjekty výzkumu, z hlediska výsledků pozorování ale nebyl vliv velikosti obce patrný. Jak ale ukázalo pozorování ve školách, místo výuky neovlivňuje

tolik průběh lekce, jako spíše možnost navazujících aktivit (např. poradenství o internetové bezpečnosti). Silnější dopad lekcí byl pozorován u škol, pro které lekce v knihovně probíhají pravidelně a jsou vedeny knihovnicí, ne učitelkou, současně je dětem i učitelům známý formát lekce založený na aktivním učení a rámci evokace – uvědomění – reflexe. V opačném případě bylo nutné déle navazovat vztahy založené na důvěře a otevřenosti mezi všemi skupinami, jejichž význam pro průběh a výsledek lekce byly popsány v kap. 3.1. Tyto prvky prostředí byly vnímány již při plánování výzkumu a výběru prostředí, je nutné je zvážit pro přenositelnost do jiných prostředí.

Pomocí pozorování bylo možné potvrdit právě to, zda nastavení lekcí odpovídá postupu a výsledku aktivního učení. Především zda dochází k získání nových poznatků v řešené oblasti pomocí realizovaných aktivit. Interakce různých členů lekce staví na předchozích znalostech a na nich jsou postaveny nové znalostní struktury, které jsou systematicky ukotvené pomocí reflexe. Všechny tyto cíle lekcí sledované pozorováním se podařilo naplnit.

3.3.4 360° zpětná vazba formou rozhovorů

Existují různé názory na to, zda by knihovna měla vzdělávat v informační bezpečnosti, přičemž se objevují také přesvědčení, jak na to pohlíží zástupci primárně i sekundárně dotčených cílových skupin. Tato přesvědčení často vychází se subjektivního pocitu spíše než podložení empirickými daty. Cílem kvalitativních rozhovorů není zobecnitelný, ale možný pohled různých subjektů na knihovny jako instituce vzdělávající v informační bezpečnosti.

Kvalitativní polostrukturované rozhovory byly zvoleny, protože umožňují zjistit postoje a jejich zdůvodnění[429]. Rozhovory se jevily jako nejvhodnější přístup, protože nebyl zjišťován jen současný stav, ale i minulost a vnitřní názory k tématu, a protože mezi subjekty dotazování existují mocenské vztahy vylučující skupinový sběr dat.

Cílem výzkumu bylo ukázat deklarovaný i skutečný postoj zástupců klíčových skupin k otázce, zda by knihovna měla vzdělávat v informační bezpečnosti. Pro dosažení tohoto cíle byly formulovány čtyři dílčí výzkumné otázky:

- VO1: Jaké pozitivní důvody a důsledky realizace lekcí v knihovnách o informační bezpečnosti si dotazovaní uvědomují?
- VO2: Jak hodnotí dotazovaní vliv realizované lekce v knihovně o informační bezpečnosti?
- VO3: Jaké možné bariéry realizace lekcí v knihovnách o informační bezpečnosti, které mohou omezit efektivnost nebo zcela zamezit jejich realizovatelnosti, dotazovaní identifikují?

429 PICKARD 2013.

– VO4: Jaká řešení bariér realizace lekcí v knihovnách o informační bezpečnosti informanti na základě vlastní zkušenosti navrhují?

Výzkumné otázky se snaží zachytit kombinaci pozitivních a negativních aspektů (předpokladů a důsledků) lekce s obecným a konkrétním (na lekci založeným) postojem k lekcím. Příloha 1.4 obsahuje scénář pro polostrukturovaný rozhovor. Byl zjišťován obecný postoj k tomu, aby knihovna vzdělávala v informační bezpečnosti a faktory, které k němu vedly, včetně vlivu realizované lekce (se zaměřením na 4. třídu s ohledem na výběr žákyně a její matky). Právě tato část rozhovorů je podstatnou součástí akčního výzkumu, protože umožňuje potvrzení vlivu lekce na děti, ale i další osoby, udržitelnost výsledku akčního výzkumu a, dle Kirkpatrickova modelu, dlouhodobý efekt lekce jak z pohledu změny chování žáka (3. úroveň), tak i návazně důsledky pro okolí dětí (4. úroveň).

Výběr dotazovaných byl účelový pro zachycení zástupců všech identifikovaných klíčových skupin ve vztahu k navrženým lekcím, jedná se tedy o přístup nazývaný 360° zpětná vazba. Protože byly jasně dány některé klíčové subjekty pro výzkum, jejichž postavení je jedinečné, ale také odlišné, byl zvolen účelový výběr (maximálně variantní případy). Vzhledem k nastavení koncepce se formují tři skupiny, kterých se lekce dotýkají a jejichž názory jsou proto z hlediska šetření podstatné: knihovna jako realizátor, škola pro kontakt mezi knihovnou a žáky a nakonec cílová skupina vzdělávání, tj. děti a sekundárně i jejich okolí, především rodina. Vzniklo celkem šest rozhovorů vždy se dvěma různými zástupci jmenovaných skupin:

– knihovna: ředitel knihovny rozhodující o přidělení zdrojů (čas, materiál a lidské zdroje) pro vzdělávání a knihovnice vzdělávající přibližně 3 roky děti od předškolního věku po ukončení sekundárního vzdělávání na systematické a opakované úrovni (přes spolupracující školy každý ročník min. jednou za rok), knihovnice lektoruje i semináře o vzdělávání v knihovnách pro knihovníky,
– škola: zástupkyně ředitele školy (po realizaci rozhovoru jmenovaná ředitelkou), pro kterou byla realizována většina navržených lekcí, a učitelka, která na této lekci se svou 4. třídou byla, učitelé a vedení školy zajišťují přítomnost primární cílové skupiny vzdělávání v době výuky a musí být tedy schopni obhájit smysl této spolupráce s knihovnou; vzhledem k pracovním pozicím je nutné zdůraznit, že většina zjištění týkajících se školy platí pro 1. stupeň, jen omezeně i pro 2. stupeň,
– rodina: žákyně 4. třídy, která se lekce zúčastnila, a její matka, která pracuje jako úřednice na Městském úřadě v Poličce a má přímé informace o jednání mezi zřizovatelem a vedením knihovny; pro dodržení etiky výzkumu rozhovor s žákyní probíhal za přítomnosti matky.

Spojení dotazovaných s realizovanou lekcí je podstatné proto, že rozhovory jsou součástí akčního výzkumu. Dalším kritériem výběru informantů je jejich pozitivní vztah k tématu, který sice může mít vliv na výsledky, ale je nezbytným

předpokladem pro formulaci akce v cyklu akčního výzkumu (viz kap. 3.3). Názory různých nedotazovaných klíčových skupin jsou částečně pokryty dotazy na známé reakce, primárním účelem rozhovorů ale bylo spíše najít argumenty a možnosti k tomu, co je možné realizovat a co je efektivní.

Rozhovory se uskutečnily v létě a na podzim 2013, tj. několik týdnů až měsíců po lekci, která umožňovala reakci. Knihovnice byla dotazována po prvních čtyřech cyklech lekce, ředitel knihovny a obě zástupkyně školy po pěti, přičemž učitelka čtyři týdny po lekci s její třídou, žákyně a její matka s odstupem 24 týdnů (rozhovory byly odloženy kvůli letním prázdninám a podruhé kvůli volbám na úřadě, kde je matka zaměstnána). Časový odstup slouží k odbourání okamžitého dojmu ve prospěch dlouhodobého vlivu (Kirkpatrick[430] doporučuje 3 měsíce). Jedná se v každé kategorii o zastoupení přímého účastníka lekce a nadřazené pozice. Rozhovory lze tedy považovat za výsledky 3. a 4. úrovně Kirkpatrickova modelu. Pro 4. úroveň je interval odstupu na spodní hranici, ale s ohledem na organizaci a zájmy dotazovaných byl snížen na stejnou délku pro všechny.

Pro dodržení etiky výzkumu byl dotazovanými udělen poučený souhlas (formulář je uveden v Příloze 1.4). Vzhledem ke specifičnosti subjektů byly dopředu výsledky rozhovorů sjednány jako neanonymní, ale pro ochranu dotazovaných je omezena identifikace označováním v textu výhradně zástupnými pojmenováními (ředitel, knihovnice, zástupkyně, učitelka, matka a žákyně). Pro přesný záznam rozhovorů vznikly videozáznamy[431], z nich pak byly vytvořeny přepisy. Po zpracování výsledků do publikace byl text poskytnut dotázaným k autorizaci a vyznačení úseků, které měly být ze zpracování vyřazeny pro ochranu dotazovaného nebo jeho okolí, případně kvůli nesprávné interpretaci jejich sdělení. Podrobněji je postup analýzy popsán v původní dizertační práci[432].

Na základě kategorií vzniklých v analýze rozhovorů jsou dále popsány názory informantů, které vycházejí z jejich přesvědčení, ale i ze zkušenosti, a to jak s informační bezpečností samotnou, tak i s lekcí v knihovně. Nejdříve je pozornost věnována kontextu dalších zjištění, základem je předchozí postoj k informační bezpečnosti a vysvětlení dále využívaných pojmů pro předcházení chybné interpretaci a postoje k mediačním strategiím se zaměřením na vzdělávání. Následně je pozornost zaměřena na samotnou knihovnu, od jejích výchozích možností pro realizaci lekcí o informační bezpečnosti, až po důsledky, které jí přijetí či nepřijetí této funkce přinese. Stranou nezůstává škola podporující vzdělávání dětí knihovnou. Vyzdviženy jsou klíčové okamžiky, které ovlivnily přijetí lekcí, vč. možnosti řešení tématu přímo školou. Navazuje sféra rodiny, tedy primární a sekundární cílové skupiny. Kromě přístupu k vzdělávání dětí je popsáno řízení informační bezpeč-

430 KIRKPATRICK 1971.

431 Vliv na dotázané by vzhledem k běžnosti použití neměl být velký – viz CHRÁSKA 2007, s. 184.

432 KOVÁŘOVÁ 2015.

nosti v rodině na úrovni znalostí a zkušeností, na což navazuje potřeba vzdělávání dospělých i názory dotazovaných na přijetí nabídky vzdělávání o problematice knihovnou pro jejich potřeby. Pro všechny subjekty je základem konkretizace náplně jednotlivých lekcí v rámci koncepce. Evaluace lekce v akčním výzkumu je zařazena na závěr, přestože navazuje na předchozí dvě šetření, protože se jedná o rozšíření a zacílení na specifickou situaci všech předchozích uvedených názorů, v jejichž kontextu je nutné evaluaci lekce vnímat.

3.3.4.1 Vliv prostředí participantů

Pro další řešení tématu je nutné popsat kontext, do kterého mají být lekce začleněny. Knihovny jsou stále vnímány jako instituce reprezentující hodnoty považované za podstatné, služby jsou ale vnímány omezeně, především na půjčování knih, což vyjádřila i učitelka, která s třídou navštěvuje lekce v knihovně. To vede k tomu, že veřejnost často necítí potřebu knihovnu navštěvovat, takže lekce slouží i jako osvěta, co vlastně knihovna je, protože rodiče ji dětem ne vždy zprostředkují. Osvěta je vnímána jako výrazně vhodnější forma prezentace knihovny ve srovnání s předchozí zkušeností školy v podobě tradičního představení instituce (exkurze).

V době realizace rozhovorů knihovna spolupracovala se školskými institucemi od mateřské školy po gymnázium, tj. vzdělávala děti ve věku přibližně rok a půl až osmnáct let. K tomu byl využit úvazek o velikosti 0,6, což je výrazná část ve sledované knihovně. Ředitel zdůrazňuje neobvyklost tohoto přístupu. Přitom za vhodné by považoval nastavení spolupráce škol a knihoven ve vzdělávání ze strany ministerstva, ale až v okamžiku, kdy na to knihovny budou především personálně připraveny, a s nezbytným vysvětlením nastavení spolupráce jejím realizátorům, což je z jeho zkušenosti problém.

Tradice spolupráce se sledovanou školou je přibližně tříletá, 1. třídy chodí do knihovny na pasování na čtenáře, lekcí se účastní od 2. třídy, kdy již umí číst, třídy na 1. stupni se lekcí účastní opakovaně v půlročních tematicky zaměřených celcích, na 2. stupni navštěvují lekce jednou za rok, primárně v hodinách češtiny, kdy přínos lekce je spatřován v tom, že literatura je podána záživněji a tím je i lépe zapamatována. Učitelé, resp. žáci, na 1. stupni si volili podle zájmu z připravených přibližně dvaceti lekcí podle toho, které téma je zajímá.

V pozitivním hodnocení spolupráce školy s dalšími místními organizacemi, ať už s kulturním centrem, muzeem nebo třeba s hasiči, se shodli všichni dotázaní. Přínos je spatřován na různých úrovních: pro děti, které si látku oživí a lépe zapamatují a naučí se přístupu vzdělávat se nejen ve škole; pro školu, která může využít dostupných expertů v oblastech, které by musela dostudovávat; pro město, jehož obyvatelé jsou vzdělanější a uvědomují si potřebnost všech institucí i efektivitu struktury městských organizací; a pro navštívenou instituci, které škola pomůže navázat s dětmi vztah. Pokud tedy škola s dalšími místními institucemi spolupra-

cuje, nejedná se jen o vyplnění času nebo náhradu při plnění vlastních povinností, ale strategii přínosnou pro všechny přímo i nepřímo dotčené.

Vedle vzdělávání se mezi zmiňovanými mediačními opatřeními pro řešení informační bezpečnosti objevilo nastavení zákonných pravidel, protože řešení na nižších úrovních je v současnosti omezené. Přestože jsou vnímána omezení při vzniku právních aktů (viz kap. 1.3.1), je jejich role považována za zásadní, a to jak pro represivní řešení incidentů, tak nastavení hranic společensky správného chování na internetu. Matka zdůraznila přísnost zákonů především u krádeže identity kvůli jejím negativním důsledkům i v situaci, kdy se ji podaří řešit. Z vyjádření je evidentní, že tento problém ji oslovil a představoval by pro ni lákavý obsah v nabídce vzdělávání.

Protože se má jednat o pravidla na úrovni celé společnosti, je akceptován pozitivní přínos nadnárodních organizací (Evropská unie), které mohou prosadit vznik řešení i ve státech, které problematice věnují omezenou pozornost. Stanovení pravidel chování v zákonech představuje formu kultivace prostředí, která je vnímána jako klíčová po příchodu jakékoli technologie. Je logické, že se vyvíjí, ale nelze rezignovat na jejich nastavení. Kultivační role je vnímána jako zásadní, protože nespočívá jen v dílčích úpravách, jak je v současnosti časté, ale v zavedení hodnot. Přitom se nacházíme v době změny, kdy je nutné zvažovat nejen aktuální situaci, ale také to, jak formovat pravidla práce na internetu pro budoucnost, ve které již internet bude běžnou součástí života celé populace.

Ve vyjádření ředitele knihovny se objevilo přesvědčení, že v oblasti praktického vzdělávání v knihovnách není vhodné operovat s termínem digitální stopy, protože se jedná o akademické označení, ostatní dotazovaní ale toto nepotvrdili, spíše naopak. Nicméně tento názor vedl ředitele k využívání označení informační bezpečnost spíše než bezpečnost digitálních stop, ale výslovně ujistil, že jej používá primárně v kontextu významu tohoto pojmu. Termín digitální stopy byl dotazovanými definován poměrně jednotně, jako jakýkoli digitální záznam bez ohledu na zařízení, které bylo využito k jeho vzniku, tím může být např. digitální fotoaparát. Digitální stopy nejsou vnímány na úrovni určité obsahové náplně, ale spíše ve formě zaznamenané informace, přičemž vznik digitálních stop je v současné společnosti nevyhnutelný. Z toho vyplývá přesvědčení, že téma se týká všech, na druhou stranu nelze omezovat problematiku na něco výhradně negativního, protože existuje možnost pozitivní digitální stopy. Z hlediska formy se již omezení v definicích někdy objevily, a to na prostředí internetu či webu, přestože digitální stopa může vznikat i na počítači nepřipojeném do sítě (např. dočasné soubory). Mezi příklady formátů byly jmenovány jen aktivní digitální stopy, ale tvořené člověkem, o kterém vypovídají, i někým jiným, přičemž někdy je jejich vypovídající hodnota podle matky až překvapivá.

3.3.4.2 Knihovna

Ředitel knihovny vyjádřil přesvědčení, že celé informační vzdělávání v knihovně bude školami vítáno, což potvrzuje to, že učitelka vyjádřila obavu, že rozšíření cílové skupiny lekcí realizovaných knihovnicí sníží její vlastní možnosti navštěvovat je se třídou. Ve sledovaném prostředí došlo k zavedení lekcí o informační bezpečnosti vlivem knihovnou pociťované poptávky od škol a veřejnosti. Ředitel knihovny tuto poptávku vnímal dlouhodobě, nebyl si vědom konkrétního zlomového okamžiku v přesvědčení o významu tématu, pouze zesílení pocitu po jeho vstupu na sociální síť Facebook. Zahrnutí informační bezpečnosti do lekcí knihovny spojoval s řešením témat, která jsou důležitá, ale školou nepokrytá. Původně řešení spatřoval, podobně jako zástupkyně školy, v absolventech pedagogických fakult, což se ale v řádu let nepodařilo (viz kap. 3.3.4.3). Zařazení informační bezpečnosti do aktivit knihovny tedy představovalo manažerské rozhodnutí vedení knihovny, které bylo zprostředkováno do školy, kde bylo přijato zástupkyní pro první stupeň za jí stanovených podmínek.

Informační bezpečnost do lekcí v knihovně byla začleňována postupně. Přestože i knihovnice si uvědomovala potřebu jejího řešení, s ohledem na své znalosti si potřebovala vytvořit zázemí před zakomponováním tohoto pro ni omezeně známého tématu. Při tom přispělo nastavení spolupráce se školou v tématech, kde si byla knihovnice jistá, a nalezení experta na informační bezpečnost, který by ji ujistil ve správnosti postupu a poskytl možnost konzultací odborné stránky lekce.

Schopnost kvalitně pokrýt téma, a to bez zaměstnání nového a neověřeného pracovníka, byla základním předpokladem zahájení lekcí i pro ředitele knihovny. Tuto schopnost podle ředitele má každá knihovna vzhledem k oborové blízkosti a považuje za pravděpodobné, že se situace v tomto směru bude zlepšovat působením propagátorů informační bezpečnosti i elektronických služeb spojených s knihovnami, a také přítomností vzdělaných knihovníků v právě jmenovaných tématech. Předpoklad existence člověka v knihovně, který může pomoci radou v internetové bezpečnosti, vyjádřila i matka, kdy navíc knihovnu vnímá jako bezpečné prostředí pro použití internetu seniorkou v její rodině. Na druhou stranu upozorňuje na snižování důvěry kvůli nezabezpečenému Wi-Fi připojení nabízenému knihovnou a významnou neaktuálností obsahu webových stránek knihovny, které si všimla s dcerou. Pro udržení důvěryhodnosti je tedy nezbytný rozvoj knihovny ve všech směrech jejích činností souvisejících s digitálním prostředím.

V oblasti připravenosti knihoven realizovat informační vzdělávání jsou dotazovaní zástupci knihovny skeptičtí. Problém vidí v chybějící pozici lektora v knihovně, a to i ve větších knihovnách. Pokud má být koncepčně řešeno informační vzdělávání, musí být tato pozice nastavena. V praxi lze ale pozorovat zadání informačního vzdělávání vedením bez zajištění potřeb pro knihovníka – lektora. Knihovníci mohou být odborně připraveni, ale i když nepotřebují doplnit zna-

losti, jsou příprava i přizpůsobení převzaté lekce časově náročné. Čas je spojen s realizací, což pociťuje škola při domluvě termínů vyhovujících institucím i lidem. Lekce je nutné v klidu kanceláře připravit, mohou být náročné materiálně, není nutné vždy IT vybavení, ale i bez něj je náročná příprava třeba na tradiční výukové pomůcky. To vše jsou zdroje, se kterými knihovník nemůže nakládat libovolně, musí se zodpovídat z jejich efektivního vynaložení nadřízenému, který disponuje omezeným rozpočtem. Podle ředitele jsou ale tyto náklady přínosné pro knihovnu i zdůvodnitelné u zřizovatele.

Kromě materiálního zázemí je otázka připravenosti knihovníků vzdělávat i na úrovni schopností v oblasti pedagogiky. Ta je podle knihovnice omezená, i když se změnami v kurikulu oboru ISK zlepšuje. Znalosti ale podle ní nejsou tak podstatné jako zkušenosti se vzděláváním, proto doporučuje zavedení praxe pro přípravu studentů, ať už v knihovnách nebo školách, alespoň na úrovni náslechů, podobně jako je tomu u studentů učitelství. To by odbouralo také v současnosti pozorovaný strach absolventů učit děti. Knihovnice považuje pedagogické znalosti za zásadní, protože na témata informační gramotnosti i bezpečnosti jsou podle ní studenti připraveni nebo jsou naučeni si znalostní deficit doplnit. Tuto schopnost doplnění zadaného tématu knihovnicí vyjádřily i obě zástupkyně školy, ale s omezením na knihovnici v místě. Vyjádřily obavu, že ne každý učící knihovník je takto univerzální, ochotný zabývat se různými tématy. S knihovnicí příliš nesouhlasil ředitel knihovny, především pro oblast informační bezpečnosti považoval za podstatnější expertízu lektora, na druhou stranu sám vyjádřil názor, že expert v knihovně na informační bezpečnost a lektor mohou být dvě různé osoby, pokud budou lekce probíhat jen jednou ročně v rozsahu dvou hodin. Je ale problém, pokud se lektor sám nechová bezpečně, jak ukázala zkušenost ředitele s egosurfingem nově přijímané učící knihovnice. Zástupkyně školy sice souhlasily s významem formy lekce, význam didaktické přípravy ale vnímaly nižší, potřebné kvality spatřovaly spíše v osobnosti lektora a jeho schopnosti děti zaujmout, i když pedagogická průprava toto podporuje.

Důraz na osobnost lektora nejen pro téma byl vyjádřen oběma zástupkyněmi školy i rodiny. Bylo pro ně jen těžce představitelné, že by lekce ve stejném formátu probíhaly i při změně lektorky, což se později v roce stalo. Lekce probíhají i nadále, i když jak vyjádřila žákyně *„už by to nebylo prostě ono“*. Je možné, že se situace v budoucnosti stabilizuje na dřívější úroveň, pokud se nově učící knihovnici podaří dosáhnout stejné úrovně hodnot, které akcentovaly zástupkyně školy. Zdůrazňovaly pěkný vztah k dětem s pochopením jejich mentality a přizpůsobení lekce této mentalitě i jejich aktuální náladě, s čímž souvisí schopnost děti zaujmout a bavit, což obvykle není možné čistě frontální výukou, ale současně udržet autoritu, nebýt příliš kamarádský, udržet určité hranice chování při lekci. Důležité je získat důvěru dětí a dokázat, aby se otevřely lekci, což při vhodném přístupu není těžké, protože se otevřít chtějí, jak ukazuje zkušenost se sdílením rizikových činností při

lekci s policistkou. Z toho vyplývá, že při vzdělávání dětí je nezbytná fyzická, ne virtuální osoba lektora, který je přiměje o tématu přemýšlet, jak opakovaně vyjádřil ředitel knihovny.

Jak bylo uvedeno, knihovnice vidí jako základní předpoklad realizace lekce zvládnutou didaktiku, např. pomocí e-learningu, resp. blended learningu, bez které je navržená koncepce jen těžce aplikovatelná. Poté ale považuje koncepci za potřebnou, protože podobně jako ona i ostatní knihovníci považují problematiku za zásadní, ale chybí jim opora pro její řešení, což knihovnice tvrdí na základě jejích zkušeností ze seminářů pro knihovníky, které lektorovala. Koncepce by měla být stručná, ale komplexní, protože současné nárazové řešení lekcí založené na nalezení pracovního listu a přečtení populárně naučné četby je nedostatečné. Znalostní připravenost v oblasti bezpečnosti digitálních stop je vnímaná jako omezená s tím, že mladší generace knihovníků k ní má blíž, především v prostředí sociálních sítí, a má také zažitý postup dovzdělávání se v potřebných oblastech, u starších knihovníků je připravenost a příprava výrazně omezenější. Podobné problémy ale existují i u ostatních kulturních a vzdělávacích lokálních institucí, knihovna má proti nim výhodu v oborové blízkosti.

Dotazovaní se shodují, že s jistými omezeními jsou v knihovně lidé schopní po doplnění určitých znalostí a získání podpory vedení vzdělávat o informační bezpečnosti. Ředitel považuje vzdělávání za roli, která udrží význam knihovny i v digitální budoucnosti. Shoda panovala v tom, že informační vzdělávání je přínosem pro knihovnu i pro vzdělávané, přičemž zahrnovat by mělo tradiční i elektronické zdroje, včetně informační bezpečnosti, a to pro děti i dospělé se zdůrazněním seniorů. Ve všech těchto tématech by měla knihovna budovat svou pozici kontaktního místa pro řešení problémů. Podle dotazovaných by bylo logické, kdyby knihovny toto téma v lekcích nabízely, protože je nerozlučně spojeno s informacemi, které zase patří do knihovny víc než do jiné místní organizace.

To vede k vyjádření možnosti řešení problematiky v alternativní instituci proti knihovně. To je vnímáno jako reálné, ale jen nouzové řešení, když se knihovna rozhodne tématu neujmout. Dotazovaní totiž považují za nutné obojí vzdělávání a kontaktní bod, nejblíže k tomu vidí knihovnu, ale ta nepředstavuje jedinou možnost. Mezi jmenovanými alternativami byly uvedeny: síť prevence na městském úřadě, dům dětí a mládeže, informační centrum pro mládež, kulturní centrum a muzeum, příp. při dotacích od města nebo ve velkém městě komerční subjekt (nebo projekt). Dotazovaní tedy považují za jisté, že centrum řešení informační bezpečnosti v místě vznikne, pokud ho nebude zajišťovat knihovna, tak to udělá jiná instituce. Jedná se tedy o výzvu pro knihovny, zda se této příležitosti chopí, nebo ji přenechají někomu jinému.

Podpora vedení knihovny je nezbytná při systematickém řešení nejen tohoto tématu, ale i ostatních složek informační gramotnosti. Prvním krokem je rozhodnutí managementu, zda bude podporovat vzdělávací funkci knihovny a tím dá

k dispozici část svých zdrojů. Proto musí knihovník doložit smysluplnost lekcí, což je u informační bezpečnosti možné společenskou poptávkou. Právě to byl zásadní argument ředitele knihovny. Pokud jsou lekce efektivní, knihovna podle něj získává vysokou přidanou hodnotu a má smysl je podporovat i na úkor jiných činností. Efektivita lekce je pak argumentem i ke zřizovateli. Pokud se knihovna rozhodne kvalitně využít této příležitosti, vytvoří na úrovni zřizovatele i veřejnosti pozitivní obraz řešením zásadního společenského problému. Informační bezpečnost je podle ředitele knihovny tématem informačního vzdělávání, které je pro okolí knihovny nejsnáze představitelné s průniky do praktického života každého občana. Výhodou knihovny je především lokálnost a dostupnost pro řešení problému, která je již v místě šetření potvrzena praxí.

3.3.4.3 Škola

Knihovnice vyjádřila přesvědčení, že školy nabídku knihoven v lekcích o informační bezpečnosti přivítají, protože škola toto téma potřebuje zajistit. Skeptičtější přístup vyjádřil ředitel knihovny, podle kterého se objeví reakce pozitivní i negativní. Není možné vyvodit, které budou převažovat, protože na plošnější úrovni diskuze o zavedení spolupráce neexistuje. Zástupkyně školy komentovaly především vlastní pozici. Výběr lekcí v knihovně pro jednotlivé třídy vychází z jejich aktuálních potřeb, a to pro školní vzdělávací program i život v současné společnosti, ať se jedná o autora literárního díla, koloběh vody v přírodě nebo informační bezpečnost. Právě informační bezpečnost je dle učitelky zásadní, především v 4.–5. třídě, aby si žáci ujasnili, co dělají na internetu. Ten jim totiž není možné zakázat a děti by si ho ani zakázat nenechaly, proto by škola měla zařídit, aby se děti seznámily s tím, jak se zde vhodně chovat. Potřebnost je tak veliká, že by učitelka uvítala i dvě lekce o informační bezpečnosti za rok, jednu zaměřenou na bezpečnou komunikaci a druhou na autorství na internetu a kritický přístup k informacím. Ještě silnější přijetí lekcí v knihovně o informační bezpečnosti je podle zástupkyň školy možné očekávat v menších obcích, kde je problém s odborníky na toto téma ve školách, v případě větších měst se postoj neodvážily odhadnout.

Přestože se škola neomezila na očekávání nabídky, ale sama se zapojila do přípravy a nasazení koncepčního vzdělávání v informační bezpečnosti (což byl také důvod jejího výběru do akčního výzkumu), ani ona neiniciovala toto řešení, spíše vyjádřila nadšení a přijetí nabídky knihovny. Impulz pro zahájení řešeného typu spolupráce proto musí vyjít z knihovny, nelze očekávat opačný směr. Školu motivovalo i její zapojení do grantu, ve kterém se problematika částečně objevila tím, že škola musela řešit práci s autorskými díly podle zákona. Jako prvořadý byl ale opakovaně uváděn zájem dětí o informační bezpečnost, který učitelky pozorovaly na jejich dotazech a který se věkem posiloval. Tento zájem vedl i k tomu, že učitelky na 1. stupni cítily vzrůstající potřebu samy se v informační bezpečnosti vzdělávat.

Pro nastavení spolupráce knihovny a školy v lekcích o informační bezpečnosti byla podle všech dotázaných (kromě žákyně, která se k tomu nevyjádřila) nezbytná osobní komunikace a srozumitelné vysvětlení, co přinese škole a co knihovně, a s jakým obsahem budou děti seznámeny. Tato fáze představuje nalezení společných zájmů obou institucí ve prospěch dětí, její výsledek je ale spojen nejen s obsahem, ale také s tím, jak jsou tito lidé ochotní a schopní domluvit se. I nejlepší obsah nemusí vést k úspěchu, pokud mezi zástupci institucí nebudou dobré mezilidské vztahy. Pokud je domluva možná, měl by být dostatečně vysvětlen obsah i forma lekce, aby se učitelky nemusely obávat, že se děti v knihovně naučí rizikovému chování, které ještě neznaly, k čemuž podle zástupkyň školy v realizované lekci nedošlo, takže se tato obava po zkušenosti rozptýlila. Bez této fáze je také možné navázat spolupráci, pokud si jsou obě strany vědomy významu tématu, ale ne s tak dobrými výsledky a s vyšším rizikem, že spolupráce neproběhne bezproblémově. Je také otázkou, zda bude o lekce mít zájem každá třída nebo jestli dojde k příkazu od vedení školy, což není vhodná varianta, protože učitelé a knihovníci by se ve vzdělávacím obsahu měli vzájemně podporovat. Protože se jedná o osobní kontakt, je kritickým okamžikem změna osoby na jedné straně, která může vést k potřebě nového budování důvěry opakováním jednání o koncepci vzdělávání.

Knihovna by měla být prostředníkem i pro vzdělávání učitelů. K tomu by na základní úrovni mělo dojít již při zahájení vzdělávání dětí, aby učitelé chápali, proč se mají lekce účastnit. Lekce by měly sloužit k budování dle slov knihovnice *tandemu*, kdy učitel má blíže k dětem a formě vzdělávání a knihovník k obsahu informační bezpečnosti, takže si mohou vzájemně pomoci správně nastavit lekci pro děti i na ni navázat ve škole. Zástupkyně školy ale poznamenávají, že knihovník může být inspirací pro učitele i ve formě vzdělávání, pokud využívá metod aktivního učení. Postupně by podle knihovnice mělo vzdělávání dětí o technické stránce bezpečnosti přecházet z knihovny na učitele, ale knihovna to musí zahájit a podporovat. Knihovna by si pak měla udržet oblast bezpečného chování na internetu, která je jí nejblíže, a v ideálním nastavení by děti procházely vzděláváním o informační bezpečnosti ve škole i v knihovně.

Je samozřejmé, že škola má možnost řešit problematiku informační bezpečnosti bez zapojení knihovny, i v tomto případě se ale podle dotazovaných hledá zástupné řešení. To může představovat interní zaměstnanec školy z 2. stupně, kdy ale škola musí řešit suplování a náhrady hodin a ne vždy se i učitel informatiky zaměřuje na bezpečné chování, přičemž pro děti je to ještě méně známá osoba než knihovnice. Jinou variantu představuje externí přednášející, který ale neřeší potřebu kontaktního bodu v případě informačního incidentu. Není tedy důvod, proč by externím expertem neměl být knihovník, který je navíc dobře dostupný, a děti se s ním setkávají i v jiných lekcích informační gramotnosti.

Vzdělávání o tématu ve škole před zavedením lekcí bylo spíše nárazové, zástupkyně školy i žákyně si vybavily především preventistu, který po ukázce videí Seznam se

bezpečně s dětmi o problému diskutoval. Zajímavým zjištěním v rozhovorech bylo, že děti si v prvních letech školní docházky povinně zakládaly e-mail pro komunikaci se školou, ale nebyly poučeny o jeho bezpečném použití, proto většinou obsahoval jméno a příjmení a byl dětmi využíván běžně při různých činnostech na internetu. Kromě e-mailu škola děti podporuje v používání internetu pro jejich vzdělávání. Před zavedením lekcí v knihovně se objevily okamžiky, kdy učitelka musela řešit informační incident na podnět matky, příp. při problematických záběrech školy na YouTube. Bez těchto neignorovatelných podnětů se ale s dětmi tématu informační bezpečnosti na 1. stupni nevěnovala. To ukazuje nedostatečnost řešení tématu i ve škole, která je mu nakloněna, ale zajišťuje si jej vlastními silami. Systematičtěji se o něm nemluví, aby se děti naučily stabilně přemýšlet o bezpečném chování při použití internetu. To, že sice ve škole je osoba, u které se materiály a informace o problematice shromažďují, považuje za nedostatečné i učitelka, podle ní by bylo dobré, aby základní informace o bezpečnosti na internetu měl každý.

Při hodnocení vzdělávání dětí v informační bezpečnosti školou a knihovnou byly v rozhovorech uvedeny určité nevýhody školy ve prospěch knihovny. Jen část z nich je spojena s nedostatečnými znalostmi učitelek v oblasti práce s počítačem, roli hraje i omezení vlivem školy jako instituce formálního vzdělávání. Pro řešení informačních problémů a vzdělávání v tomto směru může být pro školu omezením, že děti se zde cítí pod dohledem, a to jak autority učitele, tak i stálého kolektivu, chybí zde zdravá anonymita, aby se dítě uvolnilo a svěřilo s problémem. Ve škole je těžší říct, že dítě neví, jak se bránit, protože ve škole má prokázat znalost, ne neznalost. Důsledků odlišného vztahu mezi dítětem a učitelem nebo knihovníkem, příp. jiným externím odborníkem ve prospěch řešení tématu informační bezpečnosti mimo školu si jsou vědomy i zástupkyně školy.

Silný vliv při navazování spolupráce i při hodnocení lekcí měla návaznost lekcí na výuku ve škole, proto jsou základní pomůckou pro práci s lekcemi pro knihovníka školní dokumenty, což si uvědomují všechny strany, které se tohoto jednání v minulosti zúčastnily. Žákyně sice soudila, že knihovna slouží především v návaznosti na předmět český jazyk, vyplývalo to z její zkušenosti, protože na látku z informatiky lekce v knihovně navázané necítila. Proti tomu knihovnice a obě zástupkyně školy uváděly spojení se svým školním vzdělávacím programem v rámci mezipředmětových vztahů zahrnujících český jazyk vzhledem ke čtení a psaní při aktivním učení v lekcích, ale především přírodovědu, protože do ní patří oblast zdraví, tím i bezpečnost a také informační bezpečnost, vč. Linky důvěry. Zařazení tématu do tohoto dokumentu zavazuje učitele látku s dětmi probrat, ale podle knihovnice i pracovnic školy uvítají, pokud se jí chopí knihovna, protože se v ní učitelky necítí příliš jisté. Lekce se tak stává součástí školní výuky, není proto problém vyčlenit na ni požadované hodiny.

Po získání představy o navržené koncepci zástupkyně školy i knihovnice vyjádřily přesvědčení o vhodnosti zahájit ji již s dětmi od 2. třídy, nejpozději od 4., příp.

začátku 5. třídy. Tento věk by měl odpovídat tomu, kdy děti používají samostatně počítač, protože pak by se měly také samostatně rozhodovat o svém chování na internetu. Koncepční přístup je hodnocen jako klíčový, tj. že lekce jsou naplánovány pravidelné a na sebe navazující, jsou přizpůsobeny obsahově i formálně věku tak, že jsou pro děti přijatelné a zábavné. Přestože se koncepce do praxe zavádí postupně, je vhodné mít stanoven cíl, který je sledován a prezentován zúčastněným. Pestré, aktivní učení je dobře hodnoceno všemi dotazovanými, kdy se děti nenásilnou formou dozvědí něco nového, co ale již částečně bylo probráno ve škole. Toto nastavení lekce je pro učitelku zásadní – pokud má jistotu určité úrovně znalostí, není důležité, o kolik větší je jeden expert, když jiný dokáže potřebný obsah dětem lépe předat. Všichni dotázaní hodnotili pozitivně, že lekce neprobíhala ve škole, ale v knihovně, což omezuje důraz na sumativní hodnocení výsledku ve prospěch formativního hodnocení, děti se soustředí více na to, co má být naučeno, než na formu, např. pravopis, který se v knihovně řeší výrazně méně než ve škole. Pro výsledné hodnocení lekce je proto zásadní forma i obsah.

Přes to, jaký obsah a forma jsou před lekcí prezentovány, učitelky nehodnotí lekci do doby, než s ní mají zkušenost. Až ta je tedy zásadní pro dlouhodobé přijetí či nepřijetí lekce, ovšem nemusí se jednat o přímou zkušenost každé učitelky, ale jedné z nich, hodnocení poté sdílí. Reakci následně lze pozorovat na zvyšujícím se nebo snižujícím zájmu navštívit lekce. Může se tak stát, že i učitelka, která původně o lekci neměla zájem, vlivem pozitivního hodnocení kolegyň se se třídou do lekce zapojí. V případě, že knihovna využije hosta a škole lekci zprostředkuje, očekávají učitelky standard, jako jsou u knihovny zvyklé, pokud není splněn, má to vliv nejen na hodnocení externího lektora, ale celého vzdělávání v knihovně.

V případě, že je učitel s lekcí spokojen, měl by na ni navázat s dětmi ve vlastní výuce, což je dobré podpořit poskytnutím materiálu, od kterého by učitel mohl začít. Dle knihovnice i zástupkyň školy ale vliv spokojenosti vede také k přenesení znalostí i zprostředkování kontaktu přes učitele k rodičům. Škola tedy sebe vnímala spíše jako prostředníka pro navázání kontaktu, aby knihovna vzdělávala nejen děti, ale i rodiče, k tomu je dokonce ochotná nabídnout svůj prostor a hodnocení kvalit vzdělávání o tématu v knihovně na rodičovských sdruženích a dalších místech kontaktu s rodiči.

3.3.4.4 Rodina

Žáci na připravenou lekci o informační bezpečnosti šli až na výjimky (dle žákyně se v její třídě jednalo o jediného žáka) s nadšením a očekáváním. To ukazuje pozitivní postoj dětí k řešení tématu ve vzdělávání knihovnou. Kladně hodnotí oživení tématu s doplněním nových informací. Současně žákyně projevila zájem o lekci (v rozsahu 90 minut) nabídnutou knihovnou i mimo školu s tím, že by se nesměla křížit s jejími volnočasovými prioritami a musela by mít jistotu, že jí přinese něco

nového. Zástupkyně školy k tomu doplnily přesvědčení, že se jedná o záležitost 1. stupně, a to jak z hlediska přínosu, kdy si děti v tomto věku budují postoje, tak i zájmu se zapojit. V postoji venkovských a městských dětí podle nich ve směru přístupu k aktivitám i k tématu není v současnosti rozdíl.

Pohled rodičů na vzdělávání dětí v knihovně ve sledovaném tématu se opět nikdo z dotázaných neodvážil zobecňovat, vyjádřili ale svorně přesvědčení, že by převažoval pozitivní postoj. Někteří by uvítali, že děti slyší i od někoho jiného to, co sami rodiče říkají, což byl případ dotazované matky. Jiní by mohli uvítat, že lektor s dětmi řeší závažné téma, které je pro ně samotné vzdálené, i když je možné, že by si ho spíše spojovali se školou, protože rodiče mají méně přímý kontakt se vzděláváním v knihovně než učitelé a děti. Ne výjimečný by podle ředitele byl i postoj neutrální, protože *„který rodiče zajímá všechno, co je, co je ve škole učí.“* Matka připomíná, že knihovna nemusí šířit osvětu jen lekcemi, mohla by připravit různé letáčky a nálepky pro děti s připomínkami bezpečného chování na internetu, osvěta také nemusí směřovat jen k dětem, protože ohroženou skupinou jsou například i senioři.

Odkaz matky na seniora vycházel z její zkušenosti ve vlastní rodině. Uvedla příklady dvou příbuzných, z nichž jeden je vášnivý čtenář s omezeným zájmem cokoli dělat na internetu, přestože by mu to usnadnilo čtení, druhý získal od rodiny registraci do knihovny především pro řešení zájmu používat internet, primárně pro komunikaci se známými. Bezpečnost seniorky na internetu by proto matka také uvítala s podporou knihovny, toto vzdělávání by podle ní mohlo navazovat na osvětu seniorů, která probíhala pro jejich ochranu proti nepoctivým prodejcům. Dotazovaná žákyně je silnou uživatelkou internetu, ale v době rozhovorů ho využívala spíše k hrám než ke komunikaci (s půlročním odstupem matka uvedla změnu se značným nárůstem komunikace, což odpovídá výzkumům). Omezenou komunikaci vedla především přes e-mail, o další typy služeb neměla zájem, protože *„prostě každej den to kontrolovat, jako jestli mi něco nepřišlo a tak, jako to podle mě je nuda“*. Vyjádřila přesvědčení, že i její spolužáci, kteří používají Facebook, zde komunikují zejména v rámci třídy (což potvrdila i matka s odkazem na internetovou činnost spolužaček při častých návštěvách), sama necítila informační deficit tím, že profil na Facebooku nemá.

V rámci rozhovorů matka i žákyně odkazovaly na své znalosti v oblasti informační bezpečnosti. Žákyně především směřovala k práci s fotografiemi obličeje, které by se na internet neměly dávat, a problém s jejich stažením. Druhou opakovaně uváděnou oblastí byla bezpečná hesla, ke kterým se vyjadřovala i na úrovni zkušeností založených na práci s hesly u jejích známých. Matka se proti tomu zamýšlela spíše nad veřejnými rejstříky, do značné míry opět díky zkušenostem z jejího zaměstnání, a také nad připojením k internetu a využití IP adresy, které si uvědomila až při přípravě na rozhovor. I dříve se ale zamýšlela nad některými způsoby využití digitálních stop, např. po nákupu v e-shopu. Současně dodává, že

se její přístup za dobu používání internetu změnil k důkladnějšímu uvažování nad důsledky poskytnutí informací, uvědomuje si ale, že chyba, kterou mohla udělat před mnoha lety, se může objevit v budoucnosti, aniž by s tím v současnosti mohla cokoli udělat. Sama se ale naučila využívat digitální stopy, a to nejen v zaměstnání, ale třeba i pro zjištění, kdo je současná přítelkyně jejího syna. Přes Facebook našla i nevhodné fotky dcery její kamarádky, kterou upozornila i přes obavu, že bude považována za drzou, ale s potěšením zjistila, že dívka uznala svou chybu a fotky stáhla. Přemýšlení o digitálních stopách u matky i žákyně vedlo k tomu, že zvažují poskytnutí informací o sobě přes internet, např. v registracích, proto když je nutné některý údaj uvést a je to možné, vymyslí si jej.

Z hlediska mediačních strategií dotazovaní nebyli příliš nakloněni restriktivním opatřením, především pokud se spoléhá výhradně na ně, spíše se přikláněli k aktivní mediaci, protože výhody spojené s použitím internetu podle nich výrazně převažují nevýhody. I rodiče, kteří mají určité povědomí o informační bezpečnosti, se jen málokdy cítí v této oblasti dostatečně pevně nebo vnímají potřebu problematiku řešit, takže se s dítětem snaží bavit, ale jejich ponaučení jsou omezována na případy ve zpravodajství nebo dílčí témata. Opakovaně v rozhovorech zaznělo, že internet a materiály k tématu na něm jsou dobrým zdrojem osvěty, ale nestačí, je nutné děti (ale i rodiče a učitele) vést k přemýšlení o tématu a umožnit jim diskuzi s fyzickou osobou, a to při lekci i v návaznosti na ni, když cítí tuto potřebu. Podle zástupkyně se to možná časem bude měnit, nová generace bude v oblasti informační bezpečnosti poučenější, alespoň u vysokoškolsky vzdělané části populace. Méně vzdělaní a starší lidé ale stále budou potřebovat podporu, otázka je, zda o ni budou mít zájem.

Z toho vyplývá, že v rodině jsou udržovány základní znalosti a dovednosti práce s digitálními stopami jak vlastními, tak cizími, i přesto byl vyjádřen zájem o lekce v knihovně pro různé členy rodiny. Ukázalo se také, že matka i dcera mají poměrně bohaté zkušenosti s digitálními stopami, jak přímými, tak zprostředkovanými, často ale jednají intuitivně. Zamýšlení se nad možnými důsledky zkušenosti je vhodné ještě podpořit, např. materiálem dodaným rodině po lekci, který by matka pro tento účel podle vlastních slov uvítala.

Přesvědčení, že by postupně mělo dojít k zapojení rodičů do řešení informační bezpečnosti, se objevilo u zástupců školy a knihovny. Je ale nutné je nejdříve nějakým způsobem aktivizovat, protože jejich vnímání problému je omezené. K tomu škola může využít např. rodičovské sdružení, podle zástupkyně může rodiče aktivizovat strach o jejich dítě, je proto nutné je upozornit na možné negativní důsledky informačních útoků formou kazuistik. Ředitel knihovny, který v místě téma informační bezpečnosti prosazuje, uvádí, že se setkává s žádostmi o radu od dětí nebo učitelů, ale od rodičů je ještě nezažil. Spoléhat se na neorganizované vzdělávání rodičů není správná cesta, stejně jako očekávat, že si sami najdou cestu do knihovny. Opět je nutný impulz od samotné knihovny, který může podpořit škola.

Informální vzdělávání dětí probíhá v kontaktu se staršími členy rodiny při společném použití počítače a v diskuzi s vrstevníky, k rodičům se ale z těchto směrů příliš informací nedostává. Rodiče se informálně v informační bezpečnosti mohou vzdělávat v zaměstnání, jako v případě dotazované matky při prováděných kontrolách informací od klientů, ale to je případ jen omezeného množství rodičů. Druhým zdrojem pro informální vzdělávání jsou média, zejména zpravodajství, kde dotazovaní upozorňovali na krádeže identity. Zprávy se ale objevují nahodile, chybí systematický akcent, proto je zástupkyně přesvědčena, že média na podporu tématu nejsou připravena, i když jinak by představovala vhodný zdroj pro osvětu veřejnosti. Při uvědomění si zájmu rodičů vzdělávat se v tomto směru je možné sebeřízené vzdělávání, kde je využíváno především televizních pořadů a obsahu na internetu, což je ale podle matky časově náročné, důvodem může být, že má omezenou představu, co hledá, a nezná specializované zdroje pro osvětu v této problematice, nebo jí nevyhovují.

Ze zkušenosti školy vyjádřily její zástupkyně přesvědčení, že sice se objeví nezájem i negativní reakce rodičů na vzdělávání v informační bezpečnosti v knihovně, nebudou ale příliš časté. Zástupkyně ale upozornila na problém, že o vzdělání budou mít zájem spíše rodiče, kteří se dítěti na internetu věnují a zabývají se také jeho ochranou, výrazně horší to bude s rodiči, kteří to berou na lehkou váhu, a proto by lekce potřebovali více. Zástupkyně školy upozorňují, že je nutný citlivý přístup ve vzdělávání rodičů i v jejich informování o obsahu vzdělávání dětí, důraz by měl být kladen na to, že obsahem lekce je ochrana proti útokům. Pasivita v řešení informačních hrozeb i vlastního vzdělávání je podle zástupkyň školy spojena s tím, že si rodiče nedovedou představit možné důsledky chování jejich dětí na internetu i reálnost problémů, dokud k nim nedojde. Jsou přesvědčeni, že o potřebách svého dítěte toho ví dost. Toto se neobjevuje jen u informační bezpečnosti, ale i u jiných problémů dětí. Někteří rodiče dokonce sami ohrožují dítě, především matky malých dětí jsou příliš otevřené na internetu ve sdílení informací, jak upozornila knihovnice, proto by rodiče měli být vzdělávaní ještě před narozením potomka. Přestože rodiče pravděpodobně neprojeví silnější zájem o lekce v knihovně o informační bezpečnosti, je podle učitelky podstatné s nimi začít a věřit, že se při trpělivém opakování osvědčí a rozšíří.

3.3.4.5 Obsah a forma lekce

Podle knihovnice se knihovny informační bezpečností zabývají, ale spíše v oblasti autorského práva a etiky, téma digitálních stop je v praxi pokryto minimálně. Jak je uvedeno v kap. 3.3.4.3, informační bezpečnost řadí škola do přírodovědy pod oblast obecné bezpečnosti. To odpovídá názoru ředitele knihovny, že informační bezpečnost patří spíše do občanské vybavenosti, v případě vědních oborů do základů společenských věd než do informatiky, a přesvědčení knihovnice, že škola

by měla v informatice pokrývat technická řešení bezpečnosti a knihovna bezpečné chování na internetu. Od toho se odvíjí přesvědčení ředitele o jednoduché podstatě sdělení v lekci, ať už vzdělává děti, učitele, rodiče nebo nejširší veřejnost: „*ona celá internetová bezpečnost je relativně dost banální, ono to není nic jinýho, než, než jako nemluv s cizími lidmi.*“ S tím souhlasila i učitelka, která srovnávala potřebu uvažování nad digitálními stopami před jejich vznikem s rozhlížením před vstupem do vozovky. K tomu je ale potřeba upozornit na iluze (např. vzdálenosti mezi lidmi vedoucí k nemožnosti útoku) a specifika bezpečnosti v internetovém prostředí. Pozitivní je podle dotazovaných již otevření diskuze nad tématem, aby se člověk zamyslel, co zná teoreticky a co dělá. To není samozřejmé, naopak jednoduché propojení vnímají informanti jako něco, co může velmi pomoci. Nejde tolik o přenesení odborných znalostí, např. definic termínů nebo pouček, ale spíše postojů a přemýšlení o digitálních stopách dřív, než je člověk vytvoří, příp. domýšlení možných důsledků jejich vzniku. K přenesení tohoto postoje nepomohou materiály zveřejněné na internetu různými projekty, je nutná osobní diskuze, jak vyjádřili shodně dotazovaní. Součástí sdělení lekcí by také podle nich mělo být nabídnutí se knihovny jako kontaktního bodu pro řešení problémů v informační bezpečnosti.

Při konkretizaci informací, které by se v lekcích měly objevit, uvedli informanti řízení vzniku digitálních stop, které nevede k omezení použití internetu s jeho výhodami, a možnosti nápravy digitální stopy. Silný důraz byl kladen na kritické myšlení a prevenci v chování spíše než spoléhání se na fungování služeb a jejich bezpečnostní principy. To lze přenést i na vzdělávání o netiketě, protože podle ředitele knihovny tato pravidla vzniknou přirozeně při dodržování základních etických principů, jako je zlaté pravidlo nebo kategorický imperativ. Ředitel knihovny přitom zdůrazňuje, že není možné příliš vycházet z obsahu vzdělávání o tématu v západních zemích, protože tam se uživatelé na internetu chovají méně rizikově, ale také je téma již výrazně více řešeno. Z hlediska důsledků, které je vhodné vyzdvihnout při vzdělávání, uvádí matka ztrátu soukromí a kriminální čin v podobě krádeže identity. Se zástupkyněmi školy se shodla, že vhodné je předání poznatků o možných důsledcích formou kazuistik, ne obecnými přednáškami, a to opět při vzdělávání nejen dětí. V jejich případě se podle matky i dcery není nutné obávat strachu vedoucího k omezení používání internetu, protože je pro ně příliš důležitý, dokáží se s informacemi vyrovnat.

Z hlediska formy lekce pro děti by mělo jít o koncepční přístup přibližně od 3. třídy vzhledem k používání internetu dětmi, byl doporučen minimální rozsah 90 minut za rok, učitelka by uvítala lekce na začátku i na konci školního roku, které by na sebe navazovaly. Lekce by měly být učitelům známé všechny (a ideálně více lekcí s odlišným pojetím problematiky), aby mohli s knihovníkem zvolit, která z nich je vhodná pro konkrétní třídu. Pro děti by měla být účast na těchto lekcích povinná v rámci školní docházky zařazením do školního vzdělávacího programu. Lekce by měla být pestrá, rozhodně ne na úrovni pouhé před-

nášky, a kvalitní, děti musí mít jistotu, že lektor obsahu rozumí, ale současně je dokáže zaujmout. Matka s dcerou uváděly zájem o lekce, při kterých společnou tvorbou knihovníka a dětí vznikne nějaký materiál, může se jednat o zápisky, obal na sešit s informacemi o problematice nebo např. komiks. Produkt po lekci by měl sloužit nejen k udržení informací v paměti dítěte, ale knihovník by měl podpořit učitele v návaznosti na lekci tím, že mu také poskytne nějaký materiál, např. jednoduchý pracovní list.

Obsah lekcí pro děti by měl navazovat na lekce v knihovně k informační gramotnosti, kde děti zjistí, jak s informací pracovat, především u dětí na 2. stupni je nutné informační bezpečnost prohlubovat v souvislostech mezi těmito tématy přes dokumentovou gramotnost. Informanti se shodují, že základem obsahu jsou informace o řešení internetových problémů (spíše než samotné tyto problémy, i když i ty by se měly v lekcích objevit, jak již bylo uvedeno, zejména formou kazuistik), především preventivní na úrovni chování, jak již bylo popsáno výše při vymezení obsahu lekcí pro libovolnou cílovou skupinu. V prvním kroku je nutné doplnit povědomí o fungování internetu, následně by pozornost měla být zaměřena na omezení sdílení osobních informací, zejména fotek a videí, netiketu, krádež identity a kyberšikanu.

Aby mohli učitelé na lekci v knihovně navázat, musí vědět, co bylo jejím obsahem, a také mít znalosti pro jeho rozvedení při vlastním kontaktu s dětmi, o který na této úrovni učitelky podle zástupkyň školy projevily zájem (a při kontaktu výzkumnice se všemi učitelkami z 1. stupně při zahájení akčního výzkumu). Proto dotazovaní, především zástupci školy, zdůrazňovali potřebnost vzdělávání učitelů knihovnou. Současní učitelé, ale i absolventi pedagogických fakult, pokud se nespecializují na informatiku, nemají v rámci odborného vzdělávání příliš příležitostí rozvíjet se v informační bezpečnosti. Toto vzdělávání je pak obvykle omezeno na přednášky bez praktické složky, které podle slov zástupkyň školy za sebou mají všechny učitelky, ale výsledky nepovažuje nikdo z nich za dostatečné. Výjimečná práce s kazuistikami ukázala, že je tato forma mnohem efektivnější, proto je vhodné jí využít i při kontaktu s učitelkami. Jejich vzdělávání knihovnou v informační bezpečnosti by mělo probíhat na dobrovolné úrovni formou prezenční interaktivní lekce, protože podle učitelky si poskytnuté materiály k tématu projde málokdo, spíše je jejich obsah jen povrchně mezi učiteli sdílen. Za vhodnou není považována ani technika webinářů, kterou by mohli přijmout knihovníci, ale učitelé spíše projevují zájem o fyzický kontakt při svém vzdělávání. Učitelé i knihovníci by při vzdělávání mohli být podle knihovnice podpořeni e-learningovým kurzem, základem ale je fyzické setkání, ideálně formou workshopu, jak dodávají zástupkyně školy, vzhledem k omezenému zapamatování toho, co si ihned nevyzkouší, s aktivním, příp. dramatickým učením, protože to aktivizuje nejen děti, ale i učitele. Tyto lekce by sice měly sloužit k předání znalostí, ale na takové úrovni, kterou učitelé opravdu potřebují a s ujištěním, že téma zvládnou.

Pokud si knihovna dokáže vybudovat postavení instituce pro osvětu v informační bezpečnosti, podaří se jí získat přístup k veřejnosti, jejíž zájem o vzdělávání nejen v této problematice je v současnosti omezený. Dotazovaní vyjádřili přesvědčení, že má smysl směřovat i k tomuto cíli a věřit, že se po osvědčení lekce pro veřejnost rozšíří. Pro tuto skupinu, z níž knihovna může zaujmout z počátku jen omezenou část, je proto schůdné využít elektronické formy osvěty, např. matka doporučuje sekci o informační bezpečnosti pro dospělé na webových stránkách knihovny. Nemusí se jednat jen o materiály vytvořené knihovnou, ale i o rozcestník na ověřené informační zdroje, které jsou podle matky špatně dostupné. Ředitel zmiňuje i možnost webinářů pro tuto cílovou skupinu, především v malých knihovnách, protože nevěří v návštěvnost fyzických lekcí, které by jinak preferoval on i knihovnice.

3.3.4.6 Evaluace lekce

Názory uvedené v předchozích kapitolách představují obecný přístup dotazovaných k problematice. Je možné předpokládat, že je ovlivnila zkušenost s realizovanou lekcí. Pro akční výzkum je ale klíčový výsledek evaluace s tím, že vlivy jsou kontrolovány triangulací dat.

Průběh lekce byl i s odstupem hodnocen velmi pozitivně, dotazovaní sami upozornili na potvrzení většiny teoretických východisek zohledněných při tvorbě lekce (viz kap. 3.1–3.2). Forma aktivního učení přispěla k tomu, že i méně motivovaní jedinci se zapojili a o tématu diskutovali na lekci i po ní, nechali se strhnout ostatními. Již při lekci se děti ptaly na navazující vzdělávání v rámci školy. V efektech aktivního učení podle knihovnice hrála roli zkušenost dětí s lekcemi podobného formátu v knihovně. Efekt by se objevil, i kdyby neproběhly, ale nebyl by tak silný. Učitelka i žákyně hodnotily pozitivně délku i obsahovou vyplněnost, které vedly k zapojení dětí v průběhu celé lekce. Učitelka vyjádřila silnou spokojenost s formou lekce, která byla pro ni i pro děti v tomto tématu nová, toto hodnocení ji vedlo k projevům zájmu rozšířit její využití i pro další ročníky ve škole.

Dotazovaní vyjadřovali přesvědčení o uplatnění simulačního efektu ve fázi uvědomění si významu v lekci (i když s omezením odhadu identity dle rukopisu), který dětem umožnil, aby si samy uvědomily žádané poznatky v bezpečí knihovny. Knihovnice pouze doporučila, aby při efektivním průběhu nebyla aktivita ukončována z časových důvodů, dokud děti zjišťují nové skutečnosti. Lekce ukázala, že některé děti mají poměrně dobré znalosti v informační bezpečnosti, ale jiné o ní téměř netuší. Oběma skupinám dětí ale lekce otevřela téma, nad kterým by měly přemýšlet, což často nedělají, i když znalosti k tomu mají. Bylo tedy dosaženo stanoveného i požadovaného cíle podle všech dotazovaných dospělých.

Z hlediska 3. úrovně Kirkpatrickova modelu byly uváděny i dlouhodobé pozitivní důsledky lekce u dětí. Všichni dotazovaní vyjádřili, že lekce s odstupem několika měsíců sice nevedla k tomu, aby děti dokázaly odříkat představená pravidla,

ale při řešení vzniku digitální stopy se zamyslí, poskytnou nebo neposkytnou ji vědomě se zvážením důsledků, a tím je jejich chování častěji bezpečné, než kdyby lekce neproběhla, i když si to třeba neuvědomují. Jedná se o postoj vžitý praktickým nácvikem na lekci. Samozřejmě to nezaručí, že negativní digitální stopu děti nevytvoří, jsou si ale vědomy, co je správné, a když se podle toho nechovají, tak úmyslně. Současně je z vyjadřování matky i žákyně evidentní, že digitální stopu vnímají i na její rovině pozitivní, pokud prezentuje znalosti a dovednosti (např. blog nebo umělecká videa).

V konkrétních případech práce s digitálními stopami byly dcerou a matkou uváděny podle nich vhodné postupy při registraci k různým službám, především k Facebooku, dále pravidla pro silnou autentizaci a práci s fotkami v elektronickém prostředí, které byly vztahovány k poznatkům řešeným na lekci. Při registraci žákyně nyní postupuje obezřetně, registruje se jen v případě, že je to opravdu nutné. Pokud zváží, že není, tak je ochotná si i odepřít obsah, o který měla zájem, ani se nepodívá na požadované údaje. V případě, že k registraci chce přistoupit, tak vkládá falešné údaje, kde je to možné. Žákyně vyjádřila názor, že když je v registraci zadán e-mail, je tím prozrazeno i jméno, i když uživatelské jméno je falešné, nezvažovala možnost e-mailu ve tvaru bez jména.

V případě, že by žákyně chtěla vytvořit skutečný profil např. na Facebooku pro komunikaci se spolužáky, kde musí uvést určité informace pravdivé, zdůrazňovala uvedení jen nezbytně nutných údajů, tj. jen křestní jméno, ne příjmení, fotku by nepoužila vlastní, ale své kočky. V žádné představitelné službě by nebyla ochotná udat např. rodné číslo a e-mailovou adresu. To je totožný postup, jako zná od své kamarádky, a podobný jako u kamaráda, který je sice na fotce sám, ale v kapuci bez viditelného obličeje a s kytarou v ruce. Z hlediska zpřístupňování fotografií žákyně uvedla odstranění fotky ze svého e-mailového účtu, protože na ní byla rozpoznatelná. V případě používání sociální sítě popsala význam autorizace a také několik pravidel pro silná hesla, která ilustrovala na podobě hesla její kamarádky, které žákyně zčásti znala.

Poslední úroveň Kirkpatrickova modelu směřuje k dopadům lekce na okolí vzdělávaných. Zde dotazovaní popisovali především vliv na prostředí školy a rodiny a také zahájení diskuze o tématu mezi dětmi, která podle učitelky probíhala několik dní po lekci spontánně z podnětů dětí. Dospělí dotazovaní vyjádřili přesvědčení, že lekce vedla k diskuzi dosti velké části dětí s rodiči o bezpečnosti digitálních stop iniciované dětmi. Přestože tento výsledek nebude u všech dětí, podle učitelky: „*i kdyby, já nevím, čtvrtina, jo, to s těma rodičema probrala, tak si myslím, že i to je veliká zásluha*“. Současně vyjádřila přesvědčení, že vlivem této diskuze byla zahájena i kontrola a zamezení rizikovým činnostem v oblasti digitálních stop. Matka toto přesvědčení zčásti potvrdila, omezení diskuze podle ní bylo vlivem toho, že se zamyslela nad činnostmi žákyně na internetu a posoudila je jako dostatečně bezpečné. Diskuzi podle ní výrazně více vyvolaly otázky, které dostala pro přípravu

k rozhovoru, podobný materiál by proto uvítala po lekci, aby na ni mohla navázat i ona v rodině, a to jak v komunikaci s žákyní, tak i pro ujasnění přístupu k bezpečnosti vlastních digitálních stop. Vlivem lekce tedy může dojít k sekundárnímu předání poznatků rodičům a také k zjištění na jejich straně, že tu knihovna je k dispozici i pro toto téma, což se stalo u dotazované matky. Pokud bude lekce kvalitní, tak zejména na malém městě se to dle dotázaných rozšíří, a tím se ovlivní názory rodičů, ať už původně byly jakékoli.

Rozhovory přinesly poznatky také o vlivu lekce směrem ke škole. Jak již bylo uvedeno v kap. 3.3.4.3, před lekcí se objevovaly obavy na straně učitelek z pojetí tématu. I přesto se na ni přihlásily, aby si ji vyzkoušely a následně hodnotily pozitivně její nastavení. Podobně jako pro matku i pro učitele by podle dotazovaných prospělo k přenesení výsledků lekce do jejich prostředí poskytnutí materiálu knihovníkem, bez kterého bylo řešení problematiky ve škole omezené na diskuzi s dětmi nad materiálem z reflexe v lekci a nad informačními incidenty, které se v poslední době ve škole objevily. Učitelka dále uvedla, že důsledky lekce doznívaly v diskuzích několik dní, nicméně by uvítala, kdyby na lekci mohla s dětmi navázat ještě týž den ve škole. Současně, stejně jako matka, pozitivně hodnotí vliv lekce i na své vlastní znalosti, především poznání toho, co všechno děti v této oblasti znají a dělají.

Spokojenost zástupkyň školy s lekcí se odráží v jejich přímém hodnocení. Lekce se jim líbila zejména proto, že se líbila dětem, současně byla přínosná a obsah odpovídal plnění několika cílů stanovených ve školním vzdělávacím programu. Spokojenost se ale projevuje i v tom, že nechtěly na lekci nic měnit. Naopak ji chtěly nabídnout i dalším ročníkům ve škole, s případným drobným přizpůsobením pro jiný věk, než pro jaký je aktuálně určena. Toto rozšíření si učitelka i knihovnice dokázaly představit pro mladší děti (učitelka až od 2. třídy), ne pro starší věk, kdy už děti nejsou tolik otevřené, jak je potřebné pro soutěž. Silný důraz učitelka kladla na zajištění udržitelnosti lekce i dalších lekcí pro jiné ročníky, aby došlo k zajištění opravdu koncepčního přístupu, kdy každý rok budou děti navštěvovat navazující lekci v knihovně o informační bezpečnosti. V nejbližší době by učitelka uvítala lekci pro 3., 4. a 5. třídu, případně s jiným lektorem, pokud to bude jediná možnost udržení lekce v nabídce. Informanti ze školy jsou tedy s pojetím lekcí informační bezpečnosti v knihovně spokojeni, proto je podporují a iniciativně se snaží o udržení a rozšíření nastaveného standardu ve frekvenci a cílových skupinách vzdělávání nejen o informační gramotnosti v tradičním pojetí, ale se zahrnutím informační bezpečnosti.

3.3.5 Limity akčního výzkumu

Pro snížení limitů výzkumu byla uplatněna triangulace metod. Součástí akčního výzkumu byly smilesheety pro žáky, zúčastněné pozorování na lekcích a rozhovory

s různými subjekty ve vztahu k lekci, tj. učící knihovnice, ředitel knihovny, učitelka, zástupkyně ředitele, žákyně a její matka. Rozhovory také sloužily pro omezení subjektivity zúčastněného pozorování. K tomu bylo využito především informací od knihovnice a učitelky, které se zúčastnily lekcí.

Omezením akčního výzkumu je nemožnost jeho vztažení k širší populaci, je pevně svázán s prostředím, ve kterém je realizován. Jeho cílem ale není potvrzení obecně platných závěrů. Jak bylo konstatováno již v úvodu akčního výzkumu, jeho smyslem je představit funkčnost a možné přínosy realizace navržené koncepce vzdělávání v informační bezpečnosti. Pro zobecnění výsledků by bylo nutné použít jiné výzkumné metody a také cíl šetření by byl odlišný, jde již nad rámec této práce. Limit přenositelnosti byl z části omezen ověřením lekcí ve spolupráci s více školami. Validace výsledků opakováním lekcí v dalších prostředích je žádoucí, a to z hlediska velikosti obce i množství zkušeností škol s vzděláváním dětí v knihovnách, zvažováno je také ověření aplikovatelnosti lekce do jiných vzdělávacích institucí, a to v rámci formálního i neformálního vzdělávání. Toto srovnání by mělo ukázat, do jaké míry jsou výsledky průkazné pro doložení potenciálu neformálního vzdělávání nejen v knihovnách pro zvyšování internetové bezpečnosti dětí. Rozšíření realizace koncepce se bude pohybovat v řádech let a je pro něj nezbytné doložení, že se jedná o dobrou praxi, kterou je vhodné vyzkoušet i ve vlastní knihovně.

S ohledem na specifika akčního výzkumu se autoři shodují[433], že při hodnocení jeho důvěryhodnosti je nutné aplikovat jiná kritéria než v tradičním kvalitativním výzkumu. K hodnocení realizovaného akčního výzkumu je použito klasifikace validity[434]:

- Demokratická validita: Kritérium lze považovat za naplněné, ke kolaboraci výzkumníka a participantů ve všech fázích cyklu akčního výzkumu došlo. Formování lekce probíhalo na základě reakcí a činností žáků a učitelů a průběžných konzultací s knihovníkem přítomným na lekcích. Menší, ale stále vliv na úpravy lekce měly také dvě konzultace s ředitelem knihovny a dvě se zástupkyní ředitele, nejmenší zásahy vzhledem k nejslabšímu zapojení do lekce měly podněty od matky žákyně. Vlivy subjektů jsou popsány v rámci všech tří šetření, každé totiž představovalo jeden nebo více cyklů akčního výzkumu.
- Výstupní validita: Realizované intervence se vždy ukázaly jako pozitivní v dalším cyklu, někdy se ale zásahem objevily nové problémy. Například doplnění pravidel při identifikaci nevhodného postupu, který se ve třídě rozšířil, takže se neprojevil jiný, po zásahu vedl k objevení odlišného ne-

433 PICKARD 2013, s. 163.

434 HERR, Kathryn a Gary L. ANDERSON. The action research dissertation: a guide for students and faculty. In: PICKARD 2013, s. 163–164.

vhodného postupu. Poslední cykly již ale ukázaly saturaci výzkumu, kdy významnější intervence nebyly nutné.

- Procesní validita: Toto kritérium je obvykle zajišťováno triangulací metod sběru dat, která byla využita. Cílem je podpořit to, že výstup je efektem realizovaných procesů. Triangulace v popsaném výzkumu skutečně vedla k vzájemnému potvrzování výsledků.
- Katalytická validita: V rámci výsledků jednotlivých výzkumů byla snaha co nejlépe popsat a triangulací potvrdit, že proces akčního výzkumu opravdu vedl ke změně u všech zúčastněných vlivem jejich vlastního přispění. Přijetí vlastní role v akčním výzkumu si byli vědomi dospělí, u dětí se výzkumem nepodařilo prokázat, svůj přínos pro změnu si pravděpodobně příliš neuvědomovaly.
- Dialogová validita: Kritérium akcentuje vliv na intervence nejen na základě názorů jednotlivých účastníků, ale i vliv komunikace mezi vrstevníky (resp. ostatních ve stejné pozici, např. učitelů, v angličtině *peer review*). Ten se prokázal na straně dětí a školy v rozhovorech, v případě rodičů a knihovníků tento typ validity není zjištěn.

Existuje více dalších přístupů k hodnocení validity akčního výzkumu, které ale akcentují podobná kritéria, není nutné se vyjadřovat k více různým klasifikacím. Podstatným společným rysem hodnocení akčního výzkumu je především přínos pro participanty. Akční výzkum vznikl v místě realizace na základě podnětu od participantů, konkrétně ředitele knihovny a knihovnice, jak se ukázalo v rozhovorech, původ podnětu byl ještě před tím u zástupkyně ředitele školy. Výsledky smilesheetů, pozorování a rozhovorů dále ukazují, že všichni přímo dotazovaní a většina subjektů pozorování, jsou přesvědčeni o pozitivních důsledcích lekcí nejen v době jeho provádění, ale také následně po převzetí knihovnicí vzdělávající ve zkoumané knihovně v příštích letech. V tom se spojuje i dostatečné naplnění kritérií hodnocených v bodech výše.

3.3.6 Závěry akčního výzkumu

Cílem akčního výzkumu bylo ukázat kvalitu nastavené koncepce vzdělávání v knihovně o informační bezpečnosti, která odpovídá reálným podmínkám současných knihoven a staví na možných pozitivních vlivech při řešení těchto lekcí. V průběhu šetření došlo k několika cyklům změn v koncepci, nejvíce problémů bylo odstraněno v rámci zúčastněného pozorování, které sloužilo k přímému hodnocení efektivity lekce. Po dostatečných úpravách proběhlo několik cyklů potvrzujících, že další změny v metodice nejsou potřebné, jen je nutné lekci vždy přizpůsobit konkrétní třídě, což odpovídá pedagogickým principům. Hodnocení vlivem pozorování bylo srovnáváno s výsledky zpětné vazby studentů pomocí smilesheetů.

Poslední realizované šetření v akčním výzkumu směřovalo na hodnocení chování a výsledků po lekci, které bylo spojeno se zjišťováním názorů klíčových subjektů ve vztahu k lekci na to, že by knihovna měla vzdělávat v informační bezpečnosti, protože *„v současnosti je vzdělávání nejlepší legální cestou jak vštípit dětem kulturu online bezpečnosti.“* [435]

Rozhovory přinesly zajímavá zjištění, a to v pozitivním i negativním aspektu, převládaly ale kladné dopady lekce, které ani nebyly předpokládány, když např. matka žákyně uvedla, že lekce ji přiměla k diskuzi s dcerou i k zamyšlení jí samé o různých stránkách rizikové komunikace. Ze strany knihovny i školy bylo hodnocení tak pozitivní, že obě instituce trvaly na minimálně opakování, v ideálním případě i rozšíření lekcí. Všichni dotazovaní se shodli, že knihovna má své místo ve vzdělávání v informační bezpečnosti, a to nejen při vzdělávání dětí.

Šetření ukázalo pohledy různých klíčových osob ve vztahu ke vzdělávání v knihovně o informační bezpečnosti, které byly spíše podobné než rozdílné. Byly identifikovány určité slabiny realizace lekcí, ale i možnosti řešení, které jsou ověřeny z jejich vlastní praxe. Tím byly definovány argumenty využitelné při diskuzi ohledně bariér na různých úrovních, které brání realizaci lekce jinde.

Dotazovaní sice identifikovali možné bariéry, ale poskytli ke všem také vodítka pro možná řešení. Znalostní bariéry knihovníků je vhodné řešit pomocí blended learningu a dostupností experta pro konzultace. Časové, provozní a materiální podmínky pro realizaci lekcí musí vytvořit vedení knihovny, které za to může získat hodnocení efektivity vzdělávání pro prezentaci zřizovateli při žádosti o podporu této činnosti. Dalším argumentem ke zřizovateli i veřejnosti může být řešení vážného společenského problému knihovnou tam, kde se toho dosud nechopila jiná instituce. Bariéry na straně školy mohou odstranit oba právě uvedené argumenty, zásadní je především dobrá komunikace a vysvětlení, co škole lekce přinesou, včetně přizpůsobení výukovým cílům školy stanoveným v jejích školních dokumentech. To je pro učitele podstatné. Vedle toho ale vyžadují, aby lekce byla pro děti přínosná a aby je dokázala zaujmout. Kvalita obsahu i formy vedoucí k zaujetí dítěte je řešením některých bariér i na této úrovni. Děti internet zajímá, motivace je zde tedy velká, klíčové je ale na ni správně reagovat. I když je motivace slabší, tak ji lze zvýšit nastavením aktivního učení a strhnutím dítěte zájmem ostatních. Pokud dítě odejde z lekce spokojené, je nejlepším šiřitelem spojení vzdělávání v knihovně a informační bezpečnosti nejen mezi vrstevníky, ale především v rodině, kde může otevřít diskuzi s rodiči a případně je přesvědčit, aby se sami nechali knihovnou vzdělat.

Představeny byly názory různých subjektů na to, co a proč funguje, kde byly jejich obavy, problémy i jejich řešení. Argumenty jsou rozvedeny ve výsledcích výzkumu výše, jejich základy lze shrnout pomocí SWOT analýzy v tabulce 9.

435 CHANG 2010, s. 527.

Tabulka 9 SWOT analýza vzdělávání v knihovně o informační bezpečnosti dle rozhovorů

Silné stránky	**Slabé stránky**
– Lokální instituce nejvíce zaměřená na informace, média a IT. – Životní zkušenost v práci s IT. – Sdílený pocit potřeby vzdělávat o informační bezpečnosti, hl. o digitálních stopách. – Návaznost na již realizované vzdělávání (informační gramotnost). – Připravenost knihovníků mladší generace dovzdělat se, základní znalosti v informační bezpečnosti z vysokoškolského studia. – Záživnější řešení témat vedoucí k lepšímu zapamatování. – Existence ověřené koncepce vzdělávání respektující specifika současných knihoven. – Již existující spolupráce knihoven a škol. – Stálá dostupnost v lokalitě (možný kontaktní bod). – Vyvolání větší otevřenosti pro hledání řešení rizikových a problémových situací na internetu. – Hodnocení více jako sumativní než formativní.	– Knihovny jako reprezentace hodnot, služby omezeny na půjčování knih. – Ne vždy kvalitní elektronické služby. – Personální nepřipravenost koncepčně vzdělávat v potřebném rozsahu (pozice lektora, pedagogické schopnosti). – Omezený rozpočet vedoucí k omezeným lidským zdrojům (úvazek na vzdělávání omezením jiné práce). – Obava z řešení nedostatečně známého tématu s dětmi, které IT rozumí více než většina knihovníků.
Příležitosti	**Hrozby**
– Aktuální situace společenské poptávky, kdy se očekává subjekt, který ji bude řešit. – Lekce i jako osvěta o knihovně samotné. – Omezení mediace právními předpisy. – Nedostatečnost aktivní mediace u rodičů a učitelů. – Budování expertní pozice v lokalitě pro práci s informacemi a IT. – Navázání vztahu s perspektivními uživateli knihovny (dětmi). – Řešení tématu v rámcovém vzdělávacím programu. – Doplnění poznatků o informační bezpečnosti předávaných rodiči a učiteli pro rozšíření množství dětí dotčených tématem (každému může vyhovovat jiná forma).	– Pokrytí tématu jinou místní organizací, když se jej neujme knihovna, např. síť prevence na městském úřadě, dům dětí a mládeže, informační centrum pro mládež, kulturní centrum a muzeum, příp. při dotacích od města nebo ve velkém městě komerční subjekt (nebo projekt).

Témata, která participanti pro vzdělávání dětí v knihovně vyzdvihli, odpovídají nejčastějším problémům v praxi[436]. Podobně odpovídá odborným doporučením[437] zájem o zaměření na principy bezpečného chování, ne tolik o technické či právní aspekty informační bezpečnosti. Ve výzkumu se potvrdilo, že knihovna je u dětí

436 LIVINGSTONE 2011.

437 RANGUELOV 2010; MARTIN 2012.

jedním ze zdrojů pomoci, ale není tolik pro tento účel využívána rodiči[438]. Předchozím výzkumům odpovídá i shoda participantů, že spolupráce školy a knihovny ve vzdělávání v informační bezpečnosti může mít pozitivní dopady na všechny zúčastněné[439].

Součástí rozhovorů byla také poslední fáze evaluace realizované lekce, opět ji ukázala jako efektivní. Pozitivně ji hodnotili všichni dotazovaní, drobné připomínky k průběhu lekce byly zohledněny v úpravách navržené koncepce v kap. 3.2. Lekce splnily stanovený cíl v dlouhodobém postoji v oblasti informační bezpečnosti dětí, které nyní ví, jak by měly postupovat, jejich činnost je pak dána vědomým a uváženým rozhodnutím. Vedle toho ale lekce zapůsobily i na okolí dětí, tj. učitelku a rodinu, kde následovala diskuze z podnětů dětí, jejímž výsledkem bylo zvýšení aktivní a někdy i restriktivní mediace v domácím použití internetu dítětem. Materiály poskytnuté v lekci (fáze reflexe a Pět otázek s dospělými) a scénář rozhovoru ale vedly i k zamyšlení dospělých o jejich vlastní činnosti na internetu a o znalosti práce dětí při tvorbě a správě digitálních stop.

Přestože se bariéry mohou objevit, není možné dopředu je očekávat a věřit v jejich nepřekonatelnost. Výzkum prokázal reálnost praktické aplikace navrženého konceptu v této publikaci. Právě ukázka fungování nasazené koncepce s pozitivními důsledky pro všechny strany by měla vést k přesvědčení dalších knihoven, že není důvod nezkusit to i ve vlastní instituci a využít výhod, které tato spolupráce ve vzdělávání přináší.

Z dílčích výsledků je možné vyvodit, že se podařilo dosáhnout stanoveného cíle akčního výzkumu a upravit a ověřit efektivitu navržené lekce a do určité míry i celé koncepce, kterou tato lekce reprezentovala. Na lekci děti dospěly k žádoucím poznatkům vlastní činností, k čemuž bylo využito metod aktivního učení. Pomocí pozorování se podařilo prokázat výskyt požadovaných efektů aktivního učení ve všech aktivitách v lekci, ale také edukační efekt lekcí. Přestože nebylo možné zcela prokázat simulační efekt jádrové aktivity v lekci, nebylo ho ani možné vyvrátit a v navazujících rozhovorech všichni dotazovaní vyjádřili přesvědčení, že k němu došlo.

Rozhovory ukázaly, že všichni dotazovaní považují řešení tématu této práce v praxi za přínosné pro všechny strany. Vycházejí přitom z vlastní zkušenosti s realizovanou lekcí. Díky tomu mohou posoudit, co bylo správně, a to jak při samotné lekci, tak při nastavování spolupráce i v celé navržené koncepci vzdělávání. Část rozhovorů sloužila pro evaluaci lekce, takže výsledkem byla i mírná úprava koncepce (především doplnění části otázek pro rodiče), většina zjištění ale spíše směřovala k argumentům, proč by knihovny měly vzdělávat v informační bezpečnosti, a to primárně děti, v druhé řadě učitele a nakonec i rodiče a širokou

438 LIVINGSTONE 2011.

439 MARTIN 2012.

veřejnost. Rozhovory potvrdily, že východiska popsaná v teoretické části této práce jsou reálná, i když v některých místech nemusí vše proběhnout tak snadno jako u zapojených institucí, protože ty byly vybrány kvůli zvýšenému zájmu o toto řešení. Je ale pravděpodobné, že získané argumenty i ověřená efektivita lekcí povedou k rozšíření zájmu a aplikaci do praxe i v jiných místech. Je možné, že koncepce nebude některou ze stran přijata, ale jak ukazuje tento výzkum, je jisté, že alespoň někde přijata bude.

Je tradiční rolí knihoven, že učí rozlišovat mezi důvěryhodnými a nedůvěryhodnými informačními zdroji, a to jak v případě dokumentů, tak i lidí. A právě toto je základem mnoha informačních hrozeb i jejich vhodného řešení, které by mělo spočívat především v uvážlivém chování po posouzení důvěryhodnosti zdroje a možných důsledků nakládání s informací. Knihovny by proto měly pokračovat v této dlouhodobé činnosti a rozšířit ji o problematiku řešenou v této práci, protože tím budou reflektovat současné potřeby společnosti. Samozřejmě nejen knihovny by měly vzdělávat o tomto tématu, neměly by ale spoléhat na jeho pokrytí učiteli nebo rodiči, protože knihovna může podpořit jejich činnost vzhledem ke svému potenciálu představenému v kap. 2.3. Jak učitelé a rodiče, tak i knihovny mohou přinést potřebné poznatky z různých pohledů, takže zasáhnou větší množství dětí, vhodná je také jejich spolupráce pro pomoc dětem v oblasti znalostí i řešení informačních incidentů. Dítě, ale i dospělý pak má možnost vybrat si instituci, člověka i přístup, který mu pro lekci i řešení problému nejvíce vyhovuje, což je v tomto citlivém tématu vhodné. Akční výzkum ukázal, že spolupráce mezi školou, knihovnou a rodinou je nejen možná, ale pro všechny strany i přínosná.

ZÁVĚR

S rostoucím významem informací, informačních technologií a internetu pro potřeby společnosti v různých využitích od fungování kritických infrastruktur státu po volnočasové aktivity jedince, roste také význam informační bezpečnosti. Pro její efektivní aplikaci je nutné řešit jak technickou, tak uživatelskou stránku práce s informacemi, kdy především druhá jmenovaná oblast je blízká činnosti knihoven, které se dlouhodobě věnují podpoře uživatelů při práci s informacemi.

Obrana proti informačním hrozbám je nejefektivnější v rámci prevence, je proto nutné věnovat se osvětě v informační bezpečnosti. Jak je prezentováno podrobně v teoretickém ukotvení problematiky, toto téma spadá do informační gramotnosti, k jejímuž rozvoji se knihovny hlásí. Právě ony mají významný potenciál kterak přispět ke zvýšení povědomí veřejnosti prostřednictvím vzdělávání formou lekcí i poradenství v případě vzniku problému. Tento potenciál je z části specifický pro Českou republiku, většina definovaných východisek je ale rozšiřitelná i na jiná prostředí. Proto je možné se částečně inspirovat zkušenostmi zahraničních, především anglo-amerických knihoven, které se vzdělávání v oblasti informační bezpečnosti v současnosti již silně věnují. Zaměřují se na jednu stranu na bezpečnostní rizika s nimi spojená, ale současně i na budování tzv. pozitivní digitální stopy, jejímž smyslem je vytvářet prezentaci člověka, která jej podporuje a je jen omezeně zneužitelná, slouží především k předvedení jeho schopností a osobnosti jeho okolí, ať už přátelům nebo zaměstnavateli. Tento trend nezmizí, proto je spolu s představeným potenciálem českých knihoven pravděpodobné, že i v současnosti spíše nahodilé formy vzdělávání v knihovnách o informační bezpečnosti se budou postupně rozšiřovat a usazovat v nabídce především pro školy. Knihovny současně přestávají mít význam pouhého zprostředkovatele informací, kterých je s internetem dostatek. Jejich role je ale stále v řízení zprostředkování a předávání této schopnosti, což odpovídá i předmětu této práce.

Knihovny jsou ve vztahu k bezpečnosti dětí na internetu ve složité situaci, protože musí vyvažovat svobodný přístup k informacím a ochranu dětí. Technické prostředky jsou omezeně využitelné ne tolik kvůli jejich finanční náročnosti, jako spíše kvůli tomu, že vedou právě k omezení svobodného přístupu k informacím. V knihovnách je problematická také mediace na úrovni monitoringu, protože knihovny musí zachovávat informační soukromí dětí, nemohou proto sledovat vše, co se objevuje na monitoru nejen dětem, ale třeba i dospělým, kteří sedí na počítači vedle dítěte. V současnosti proto mediace v knihovnách představuje nevyřešenou otázku, ke které se přistupuje různě a ne vždy vhodně, přestože se knihovny snaží postupovat co nejlépe v rámci svých možností. Z toho vyplývá, že nejschůdnější formou, a podle výzkumů také nejefektivnější[440], je aktivní mediace formou učení dětí, jak se vhodně chovat při práci s elektronickými informacemi.

Omezené řešení tématu ve vzdělávání v knihovnách může být způsobeno obavami z toho, že by knihovníci ztratili své postavení autority a experta, protože děti mají často lepší znalosti informačních technologií než oni, proto není snadné se je pokoušet něco v tomto směru učit. Jak ale vyplývá z této práce, obava není zcela na místě, protože i přesto, že děti mají často rozsáhlé znalosti internetu, ty mohou být omezeny jen na část problematiky, která obvykle vychází z toho, co je baví. Nelze popřít, že i v informační bezpečnosti děti znalosti mají, slabší je to ale podle výzkumů[441] s jejich dovednostmi a postoji. České děti se chovají dosti rizikově. Proto by je knihovníci měli podpořit tím, že je dovedou k revizi postoje, především zprostředkováním životní zkušenosti s informačními technologiemi, ale i bezpečností obecně, protože informační bezpečnost vychází ze stejných základů, které jen rozšiřuje o specifika své formy. Knihovníci proto mohou využít svých specifických znalostí, především v hodnocení a třídění informací a zdrojů, ve kterých spočívá i bude spočívat jejich přínos.

Didaktické testování prokázalo, že knihovníci mají určité znalosti v problematice, které jsou obvykle dostatečné pro lekce v požadovaném rozsahu na základní škole. Pro navazující práci se staršími studenty a dospělými je ale vhodné je dále podpořit. Jak bylo možné očekávat vzhledem k zaměření služeb knihovny, znalosti knihovníků jsou vyšší v oblasti bezpečného chování než v technických možnostech, což odpovídá i očekávání uživatelů knihovny. Podle výsledků všech tří výzkumů mapujících situaci v českých knihovnách v řešeném zaměření není knihovníkům nutné vysvětlovat význam problematiky, ale spíše ji přenést do reálných možností jejich práce.

Možností podpory knihovníků je i nabídka koncepce lekcí o informační bezpečnosti pro žáky všech tříd základních škol a odpovídajících ročníků středních škol. Pro co nejširší využitelnost jsou lekce vytvořeny s co nejnižšími požadavky

440 DUERAGER 2012.

441 Např. LIVINGSTONE 2011.

na vybavení. Jsou postaveny na formátu aktivního učení, aby podpořily specifika knihoven pro vzdělávání a současně byly co nejefektivnějším doplněním vzdělávání ve škole nabídkou alternativního přístupu k potřebnému tématu, které podle rámcových vzdělávacích programů musí být nějakým způsobem školou řešeno. Součástí koncepce je také materiál, který by měl sloužit pro zahájení diskuze o řešeném tématu ve škole i rodině žáka, aby došlo k sekundárnímu přenosu znalostí i aktivní mediace také do ostatních prostředí klíčových pro dítě. Do koncepce byly také zahrnuty zkušenosti lektorů s realizací lekcí a materiály doporučené případným lektorům pro vlastní vzdělání, aby tímto byli podpořeni s omezením požadavků na lidské zdroje.

Pro ověření nastavení koncepce bylo využito akčního výzkumu, který se pro ověření výsledků triangulací dat skládal ze dvou větších šetření: zúčastněného pozorování a rozhovorů s klíčovými osobami ve vztahu k lekci, doplněním pak byly výsledky jednoduché zpětné vazby žáků formou smilesheetů. Tato šetření potvrdila, že lekce využívá možností aktivního učení, které děti baví a současně je pro ně přínosné, protože děti při něm samy získají potřebné znalosti a zkušenosti díky činnosti vlastní i ostatních spolužáků, dochází tedy k tzv. *peer teaching*, které je pro české děti nejpřijatelnější formou v oblasti informační bezpečnosti[442]. K ověření tohoto vlivu i dalších výsledků byly využity rozhovory realizované s odstupem po lekci, které prokázaly efektivitu lekce hodnocenou pozitivně všemi zúčastněnými subjekty.

Vedle toho také rozhovory sloužily k zjištění obecného postoje dotčených osob na vzdělávání v knihovnách o informační bezpečnosti. I v tomto směru jsou výsledky pozitivní, což je do určité míry ovlivněno výběrem dotazovaných. Na základě zjištění sice není možné zobecňovat, že všichni tuto roli knihoven přijmou s nadšením. Je ale možné konstatovat, že se mohou vyskytnout na různých stranách zavádění koncepce do praxe různé bariéry, ty ale jsou překonatelné. V případě, že dojde k nasazení koncepce, může přinést pozitivní důsledky pro všechny zúčastněné, nejen děti, které se chovají bezpečněji. Obsah lekce pro děti v knihovně se může přenést i na sekundární cílové skupiny, tj. učitele a rodiče, a vybudovat u nich jak určitou úroveň znalostí, tak také změnit přístup ke službám a potřebnosti knihovny. Lekce o informační bezpečnosti mohou být nejsilněji pociťovanou potřebou pro řešení, která v současnosti v lokalitách mimo velká města není řešena. Mohou se jí ujmout knihovny a získat tak přidanou hodnotu, ale pokud to neudělají, jsou dotazovaní přesvědčení, že se této společenské poptávky chopí jiná instituce. Je totiž nezbytné, aby se problematika v místě reflektovala, a to nejen lekcemi, ale i zajištěním kontaktního bodu pro řešení problémů. Otázkou tedy zůstává, zda se této funkce knihovny rozhodnou chopit a pokusí se takto o upra-

442 LIVINGSTONE 2011, s. 123–129.

vení své činnosti, aby více odpovídala potřebám společnosti v oblasti, která patří k jádru služeb knihovny.

Internet by měl být vnímán jako nástroj, s čímž je spojená možnost jeho využití i zneužití. Může tedy dětem přinést mnoho výhod, ale také je ohrozit. Při rozvoji dětí v práci s internetem je proto vhodné podporovat oba tyto směry. Většina zkušeností dětí s internetem je a pravděpodobně bude pozitivních, ale útoky mohou mít natolik negativní vliv, že je vhodné se jim věnovat, i když by mohly zasáhnout jen omezenou část dětí, protože není možné říct, která část z nich to bude. Je proto dobré stavět především na prevenci, ukázat, že vše má možné řešení a že pro dítě jsou k dispozici lidé, kteří mu pomohou. Vzdělávání je výrazně efektivnější než řešení právní nebo technickou cestou, jak bylo doloženo v první části publikace, restrikce by měla být menší, aby dítě nemělo obavu se svěřit, protože porušilo nějaké pravidlo, ale také aby znalo vhodnou reakci, protože bude připraveno, že problémová situace může nastat. Současně lekce formou aktivního učení, které rozvíjejí zkušenosti dětí v této oblasti, podpoří jejich schopnost rozpoznat problém a nalézt řešení. Je proto vhodné děti především vzdělávat pro zvýšení jejich informační bezpečnosti a knihovny v tom mohou významně přispět.

Problém informační bezpečnosti je do značné míry postaven na nevhodném zhodnocení důvěryhodnosti šířených informací. Jedná se tedy o problém starý stovky let, s jehož řešením knihovny dlouhodobě pomáhaly. Nyní se jen dostal do nové formy v digitálním prostředí, ale zůstává stejně vážný, ne-li vážnější vzhledem k informační společnosti. Digitální stopy, jejich užití a odpovědné budování by měly být řešeny knihovnami z mnoha důvodu popsaných v této práci. Podstatné je, že všechny tyto činnosti nejsou o ničem jiném než o vyhledávání, zpracování a sdílení informací, a to je to, co knihovny dělají a umí nejlépe. Proto by měly reagovat na tuto společenskou poptávku a do své odpovědi vložit vlastní expertízu, což ukáže, že knihovny nejsou překonané instituce, ale jsou klíčové pro podporu digitálního občanství, kterému se stále přibližujeme.

SUMMARY

Information Safety of Primary School Pupils Lessons in Libraries

Responsible behaviour is essential to prevent information attacks. It is a necessary complement to the technical and legal instruments to ensure information safety. Safety on the Internet and also when working with non-electronic information is part of the Framework Educational Programme for Primary Schools, but it is implemented inadequately. At the same time, it is a sensitive subject in which libraries can provide education with a number of advantages over other institutions. They have often already established cooperation with elementary schools and give lessons in the use of information and IT. Adding information safety to the range of topics is therefore just another step for mutually beneficial cooperation with the local community. However, the lessons have to develop the competencies in an appropriate and conceptual way.

The publication presents the reasons for and appropriate ways of setting a framework for information safety lessons. The pivotal part of the publication presents the conception of education that is useful not only in libraries. All classes use active learning and they build on each other freely. The conception contains a total of nine lessons (one for each grade), which mainly cover topics of authorship and evaluating information, and safe behaviour when working with information, focusing on communication on the Internet. Two questionnaires and didactic testing of librarians were used in developing the conception. The results show that the information safety lessons build on already implemented activities of libraries and that librarians have sufficient skills to carry out lessons included in the proposed conception.

The conception was revised based on action research conducted from 2012 to 2017. The results were obtained through observation during lessons (carried out by a researcher, a teaching librarian and the teacher of the class, a teaching librarian and a library director were interviewed). Lessons were piloted in the Municipal Library in Polička in cooperation with the Masaryk Elementary School; effectiveness of the lessons was confirmed by other three schools (Primary School Pomezí, district Svitavy, Primary School and Kindergarten Blažkova, Brno and Dance Conservatory, Brno) and one library (Library at the Crossroads in cooperation with Křídlovická in Brno). Based on action research, lessons were adapted into the form published in this work.

SEZNAM POUŽITÉ LITERATURY

Monografie a kapitoly v knihách

(Part IV) Marketing & Promotion: (Chapter 17) Behavioral Targeting. 2007. *Entertainment, Media & Advertising Market Research Handbook*. Loganville: Richard K. Miller & Associates, s. 117–121. ISBN 9781577831068.

BELZ, Horst a Marco SIEGRIST. 2001. *Klíčové kompetence a jejich rozvíjení: východiska, metody, cvičení a hry*. Vyd. 1. Praha: Portál, 375 s. ISBN 8071784796.

BJØRNÅVOLD, Jens a Aviana BULGARELLI. 2008. *Validation of non-formal and informal learning in Europe: a snapshot 2007*. Luxembourg: Office for Official Publications of the European Communities, 48 s. ISBN 92-896-0509-X. Dostupné z: http://www.cedefop.europa.eu/EN/Files/4073_en.pdf

BOTT, Ed a Carl, SIECHERT. 2004. *Mistrovství v zabezpečení Microsoft Windows 2000 a XP*. 1. vyd. Brno: Computer Press, 696 s. ISBN 80-722-6878-3.

BYČKOVSKÝ, Petr. 1982. *Základy měření výsledků výuky: tvorba didaktického testu.* Praha: ČVUT.

CIVALLERO, Edgardo. 2007. Action-Research application in Evidence-Based practice for libraries. In: *IFLA Conference Proceedings* [online]. s. 1–7 [cit. 2014-08-30]. Dostupné z: EBSCOhost

COX, Christopher N. A Elizabeth Blakesley LINDSAY. 2008. *Information literacy instruction handbook*. Chicago: Association of College and Research Libraries, 236 s. ISBN 978-083-8909-638.

ČÁP, Jan. 1993. *Psychologie výchovy a vyučování*. 1. vyd. Praha: Univerzita Karlova, 415 s. ISBN 80-706-6534-3.

EEMEREN, F. H. van a R. GROOTENDORST. 2004. A *systematic theory of argumentation: the pragma-dialectical approach*. New York: Cambridge University Press. ISBN 05-215-3772-X.

FISH, Tony. 2009. *My digital footprint: a two-sided digital business model where your privacy will be someone else's business!*. London: Futuretext, v, 191 s. ISBN 978-095-5606-984.

FONTANA, David. 1997. *Psychologie ve školní praxi: Příručka pro učitele*. 1. vyd. Praha: Portál, 383 s. ISBN 80-717-8063-4.

Global Media and Information Literacy Assessment Framework: country readiness and competencies. 2013. Paris: UNESCO. ISBN 978-92-3-001221-2. Dostupné také z: http://unesdoc.unesco.org/images/0022/002246/224655e.pdf

GRAYSON, Robert. 2011. *Managing your digital footprint*. 1st ed. New York: Rosen Central. ISBN 14-488-1319-0.

GRECMANOVÁ, Helena, Eva URBANOVSKÁ a Petr NOVOTNÝ. 2000. *Podporujeme aktivní myšlení a samostatné učení žáků*. Vyd. 1. Olomouc: Hanex, 159 s. Edukace. ISBN 80-857-8328-2.

HANSEN ČECHOVÁ, Barbara. 2006. *Nápadník pro rozvoj klíčových kompetencí ve výuce*. Praha: SCIO, 177 s. ISBN 80-869-1053-9.

HENDL, Jan. 2006. *Přehled statistických metod zpracování dat: analýza a metaanalýza dat*. Vyd. 2., opr. Praha: Portál, 583 s. ISBN 80-736-7123-9.

HENDL, Jan. 2008. *Kvalitativní výzkum: základní teorie, metody a aplikace*. 2., aktualiz. vyd. Praha: Portál, 407 s. ISBN 978-80-7367-485-4.

CHEVALIER, Jacques M. A Daniel BUCKLES. 2013. *Participatory action research: theory and methods for engaged inquiry*. 1st ed. London: Routledge, xxi, 469 s. ISBN 9780415540322.

CHRÁSKA, Miroslav. 1999. *Didaktické testy*. Vyd. 1. Brno: Paido, 1999, 91 s. ISBN 80-859-3168-0.

CHRÁSKA, Miroslav. 2007. *Metody pedagogického výzkumu: základy kvantitativního výzkumu*. Vyd. 1. Praha: Grada, 265 s. ISBN 9788024713694.

JANKOVCOVÁ, Marie, Jiří KOUDELA a Jiří PRŮCHA, 1989. *Aktivizující metody v pedagogické praxi středních škol*. Praha: Státní pedagogické nakladatelství. Pedagogická teorie a praxe. ISBN 80-04-23209-4.

KASÍKOVÁ, Hana. 1997. *Kooperativní učení, kooperativní škola*. Vyd. 1. Praha: Portál, 147 s. ISBN 8071781673.

KIRKPATRICK, Donald L. 1971. A *practical guide for supervisory training and development*. Reading, Mass: Addison-Wesley, ISBN 978-020-1037-463.

KOPECKÝ, Kamil a René SZOTKOWSKI. 2017. *Sexting a rizikové seznamování českých dětí v kyberprostoru (výzkumná zpráva)*. Olomouc: Pedagogická fakulta, Univerzita Palackého v Olomouci. Dostupné z: https://www.e-bezpeci.cz/index.php/ke-stazeni/doc_download/96-.

KOPECKÝ, Kamil, René SZOTKOWSKI a Veronika KREJČÍ. 2012. *Nebezpečí internetové komunikace III*. Olomouc: Pedagogická fakulta, Univerzita Palackého v Olomouci. ISBN 978-80-244-3087-4. Dostupné z: http://www.e-bezpeci.cz/index.php/ke-stazeni/doc_download/39-nebezpei-internetove-komunikace-3-2011-2012

KOPECKÝ, Kamil. 2015. *Rizikové formy chování českých a slovenských dětí v prostředí internetu*. Olomouc: Univerzita Palackého v Olomouci. ISBN 978-80-244-4861-9.

KOVÁŘOVÁ, Pavla a Gabriela ŠIMKOVÁ. 2014. Evidence-Based Learning Approach in Evaluation of Information Literacy Education. In: KURBANOĞLU, Serap, Esther GRASSIAN, Diane MIZRACHI, Ralph CATTS a Sonja ŠPIRANEC (eds.). *Information Literacy: Lifelong Learning and Digital Citizenship in the 21st Century, Ecil 2014, Dubrovnik, Croatia, October 20-23, 2014*. Revised selected papers. Switzerland: Springer, s. 560-569. ISBN 978-3-319-14136-7. https://doi.org/10.1007/978-3-319-14136-7. Dostupné z: https://link.springer.com/book/10.1007%2F978-3-319-14136-7.

KOVÁŘOVÁ, Pavla a Iva ZADRAŽILOVÁ. 2013. The Influence of Technological Changes on the Definition of Information Literacy. In: KURBANOĞLU, Serap, Esther GRASSI-

AN, Diane MIZRACHI, Ralph CATTS a Sonja ŠPIRANEC (eds.). *Worldwide Commonalities and Challenges in Information Literacy Research and Practice European Conference, Ecil 2013, Istanbul, Turkey, October 22–25, 2013*. Revised selected papers. Cham: Springer, s. 118–125. ISBN 9783319039183. https://doi.org/10.1007/978-3-319-03919-0_14. Dostupné z: http://link.springer.com/10.1007/978-3-319-03919-0_14.

KOVÁŘOVÁ, Pavla. 2012a. *Trendy v informačním vzdělávání*. 1. vyd. Zlín: VeRBuM. ISBN 978-80-87500-18-7.

KOVÁŘOVÁ, Pavla. Information Literacy Education and the Educational Needs of Teaching Librarians: The Czech Republic in Comparison with the Other Visegrad Four Countries. KURBANOĞLU, Serap, Joumana BOUSTANY, Sonja ŠPIRANEC, Esther GRASSIAN, Diane MIZRACHI, Loriene ROY a Tolga ÇAKMAK, ed. *Information Literacy: Key to an Inclusive Society [online]. Cham: Springer International Publishing*, 2016, 2016-01-29, s. 644-654 [cit. 2018-02-13]. Communications in Computer and Information Science. https://doi.org/10.1007/978-3-319-52162-6_63. ISBN 978-3-319-52161-9. Dostupné z: http://link.springer.com/10.1007/978-3-319-52162-6_63.

KRÁL, Mojmír. 2006. *Bezpečnost domácího počítače: prakticky a názorně.* 1. vyd. Praha: Grada, 334 s. ISBN 80-247-1408-6.

LATTA, Sara L. 2011. *Cybercrime: data trails do tell tales*. Berkeley Heights (NJ): Enslow, 104 s. True forensic crime stories. ISBN 15-984-5361-0.

LEEDER, Chris. 2014. Pilot-testing an Online Credibility Evaluation Learning Tool. In: *IConference 2014 Proceedings* [online]. iSchools, 2014-03-01 [cit. 2014-08-30]. https://doi.org/10.9776/14058. Dostupné z: https://www.ideals.illinois.edu/handle/2142/47296.

LIVINGSTONE, Sonia M. A Leslie HADDON. 2009. *Kids online: opportunities and risks for children*. Portland (OR): Policy Press, xix, 272 s. ISBN 978-184-7424-389.

LLOYD, Annemaree. 2010. *Information literacy landscapes: information literacy in education, workplace and everyday contexts*. 1st pub. Oxford: Chandos Publishing, xvi, 192 s. Chandos information professional series. ISBN 978-184-3345-077.

LYON, David. 1994. *The electronic eye: the rise of surveillance society*. Minneapolis: University of Minnesota Press, 270 s. ISBN 08-166-2515-8.

MACDONALD, Scot. 2007. *Propaganda and information warfare in the twenty-first century: altered images and deception operations*. New York: Routledge. Contemporary security studies. ISBN 04-157-7145-5.

MAŇÁK, Josef, 1999. *Nárys didaktiky*. Brno: Masarykova univerzita. ISBN 80-210-1661-2.

MAŇÁK, Josef a Vlastimil ŠVEC. 2003. *Výukové metody*. Brno: Paido. ISBN 80-7315-039-5.

MAŇÁK, Josef, Vlastimil ŠVEC a Štefan ŠVEC. 2005. *Slovník pedagogické metodologie*. 1. vyd. Brno: Paido, 134 s. Pedagogický výzkum v teorii a praxi, sv. 3. ISBN 80-731-5102-2.

MATĚJKA, Michal. 2002. *Počítačová kriminalita*. Vyd. 1. Praha: Computer Press, x, 106 s. ISBN 80-722-6419-2.

MCLUHAN, Marshall. 2008. *Člověk, média a elektronická kultura: reprezentativní výbor z celoživotního díla proroka a mága elektrického věku a elektronické revoluce.* Dotisk 1. vyd. Brno: Jota, 415 s. ISBN 9788072171286.

MITNICK, Kevin. 2003. *Umění klamu*. HELION S.A., 348 s. ISBN 83-7361-210-6.

MÜLLER, Hans Jörg, Florian ALT a Daniel MICHELIS. 2011. *Pervasive advertising*. London: Springer, ix, 364 s. ISBN 978-085-7293-510.

NIXON, Paul G, Vassiliki N. KOUTRAKOU a Rajash RAWAL. 2010. *Understanding e-government in Europe: issues and challenges*. New York: Routledge, xxviii, 322 s. ISBN 02-038-6609-6.

NOVOTNÝ, Oto. 1997. *Trestní právo hmotné*. 3. přepracované vyd. Praha: Codex. ISBN 80-859-6324-8.

NOVOTNÝ, Petr. 2002. Výukový proces z pohledu současné školní didaktiky. *Vybrané kapitoly ze školní pedagogiky*. Brno: Masarykova univerzita, Filozofická fakulta, s. 17–28. ISBN 80-210-3020-8.

PASCH, Marvin, 2005. *Od vzdělávacího programu k vyučovací hodině*. Vyd. 2. Praha: Portál. ISBN 80-736-7054-2.

PELIKÁN, Jiří. 2011. *Základy empirického výzkumu pedagogických jevů*. Praha: Karolinum. ISBN 978-80-246-1916-3.

PICKARD, Alison Jane. 2013. *Research methods in information*. 2nd ed. London: Facet. ISBN 978-185-6048-132.

POŽÁR, Josef. 2005. *Informační bezpečnost*. Plzeň: Aleš Čeněk, 309 s. Vysokoškolské učebnice (Aleš Čeněk). ISBN 80-868-9838-5.

PRŮCHA, Jan, Jiří MAREŠ a Eliška WALTEROVÁ. 2003. *Pedagogický slovník*. 4. aktualiz. vyd. Praha: Portál. ISBN 80-7178-772-8.

ŘÍČAN, Pavel. 1990. *Cesta životem*. 1. vyd. Praha: Panorama, 435 s. ISBN 80-703-8078-0.

SEIDELIN, Susanne a Stuart HAMILTON (eds.). 2005. *Libraries, national security, freedom of international laws and social responsibilities*.. Copenhagen: IFLA/FAIFE Office, 406 s. World Report Series, vol. v. ISBN 87-988-0136-8. Dostupné z: http://www.ifla.org/files/assets/faife/publications/world-report-2005.pdf.

SITNÁ, Dagmar, 2013. *Metody aktivního vyučování: spolupráce žáků ve skupinách*. Vyd. 2. Praha: Portál. ISBN 978-80-262-0404-6.

SKALKOVÁ, Jarmila, 2007. *Obecná didaktika: vyučovací proces, učivo a jeho výběr, metody, organizační formy vyučování*. Praha: Grada. Pedagogika (Grada). ISBN 978-80-247-1821-7.

SMEJKAL, Vladimír. 2001. *Internet a §§§*. 2. aktualiz. a rozš. vyd. Praha: Grada, 284 s. ISBN 80-247-0058-1.

SNYDER, Lawrence. c2011. *Fluency with information technology: skills, concepts*. 4th ed. Boston: Addison-Wesley, xviii, 795 s. ISBN 01-360-9182-2.

STEELOVÁ, Jeannie L., Kurtis S. MEREDITH, Charles TEMPLE a Scott WALTER. 2007a. *Co je kritické myšlení (vymezení pojmů a rámce E-U-R)*. Příručka 1. Praha: Kritické myšlení.

STEELOVÁ, Jeannie L., Kurtis S. MEREDITH, Charles TEMPLE a Scott WALTER. 2007b. Čtením a psaním ke kritickému myšlení. Příručka 3. Praha: Kritické myšlení.

STEELOVÁ, Jeannie L., Kurtis S. MEREDITH, Charles TEMPLE a Scott WALTER. 2007c. *Čtení, psaní a diskuse ve všech předmětech*. Příručka 4. Praha: Kritické myšlení.

SZOTKOWSKI, René, Kamil KOPECKÝ a Veronika KREJČÍ. 2013. *Nebezpečí internetové komunikace IV*. Olomouc: Univerzita Palackého v Olomouci. ISBN 978-80-244-3911-9.

ŠÁMAL, Pavel. 2010. *Trestní zákoník II.: § 140 až 421: komentář*. 1. vyd. Praha: C. H. Beck, 2. v. ISBN 97880740017892.

ŠIMÍČKOVÁ-ČÍŽKOVÁ, Jitka. 2003. *Přehled vývojové psychologie*. 2. nezměn. vyd. Olomouc: Univerzita Palackého, 175 s. ISBN 80-244-0629-2.

ŠTEFEK, Tomáš. 2012. Bezpečné městečko na dlani. In: FRIEDLOVÁ, Zdeňka a Pavla GAJDOŠÍKOVÁ. *Knihovny současnosti 2012: sborník z 20. konference, konané ve dnech 11.–13. září 2012 v Pardubicích*. 1. vyd. Ostrava, s. 70–74. ISBN 978-80-86249-65-0.

ŠVAŘÍČEK, Roman a Klára ŠEĎOVÁ. 2007. *Kvalitativní výzkum v pedagogických vědách*. Vyd. 1. Praha: Portál, 377 s. ISBN 9788073673130.

TOULMIN, Stephen. 2003. *The uses of argument*. Updated ed. Cambridge, U.K: Cambridge University Press. ISBN 978-051-1062-711.

VÁGNEROVÁ, Marie. 1999. *Psychopatologie pro pomáhající profese: variabilita a patologie lidské psychiky*. Vyd. 1. Praha: Portál, 444 s. ISBN 8071782149.

VÁGNEROVÁ, Marie. 2000. *Vývojová psychologie: dětství, dospělost, stáří*. Vyd. 1. Praha: Portál, 522 s. ISBN 8071783080.

VÁGNEROVÁ, Marie. 2005. *Vývojová psychologie*. Vyd. 1. Praha: Karolinum, 467 s. ISBN 978-802-4609-560.

VALIŠOVÁ, Alena a Hana KASÍKOVÁ, 2007. *Pedagogika pro učitele*. Praha: Grada. Pedagogika (Grada). ISBN 978-80-247-1734-0.

VANÍČKOVÁ, Eva, Kamil PROVAZNÍK a Zuzana HADJ-MOUSSOVÁ. 1997. *Sexuální zneužívání dětí*. 1. vyd. Praha: Karolinum, 82 s. ISBN 80-718-4479-9.

VANÍČKOVÁ, Eva. 1999. *Sexuální násilí na dětech: výskyt, podoby, diagnostika, terapie, prevence*. Vyd. 1. Praha: Portál, 118 s. ISBN 80-717-8286-6.

VANÍČKOVÁ, Eva. *Dětská prostituce*. Praha: Grada, 2005. Psyché (Grada). ISBN 8024711389.

WESTIN, Alan. 1967. *Privacy and Freedom*. New York: Atheneum.

WILSON, Carolyn, Alton GRIZZLE, Ramon TUAZON, Kwame AKYEMPONG a Chi Kim CHEUNG. 2011. *Media and information literacy curriculum for teachers*. Paris: UNESCO, 192 s. ISBN 978-923-1041-983. Dostupné také z: http://unesdoc.unesco.org/images/0019/001929/192971e.pdf.

Základní statistické údaje o kultuře v České republice 2012. III. díl, Knihovny a vydavatelská činnost. 2013. Praha: NIPOS – Centrum informací a statistik kultury, 67 s. ISBN 978-80-7068-274-6. Dostupné také z: http://www.nipos-mk.cz/wp-content/uploads/2013/05/Statistika_kultury_2012_III.KNIHOVNY_web.pdf.

Základní statistické údaje o kultuře v České republice 2016. III. díl, Knihovny a vydavatelská činnost. 2017. Praha: NIPOS – Centrum informací a statistik kultury, 65 s. ISBN 978-80-7068-321-7. Dostupné také z: http://www.nipos-mk.cz/wp-content/uploads/2013/05/Statistika_2016_III.KNIHOVNY_VYDAVATELE_web.pdf.

ZURKOWSKI, Paul G. 1974. *The Information Service Environment Relationships and Priorities.* Related Paper No. 5. Washington (D.C.). Dostupné z: http://files.eric.ed.gov/fulltext/ED100391.pdf

Články v periodikách

AALTONEN, Mikko a Venla SALMI. 2013. Versatile Delinquents or Specialized Pirates? a Comparison of Correlates of Illegal Downloading and Traditional Juvenile Crime. *Journal of Scandinavian Studies in Criminology and Crime Prevention*. 14(2), 188–195. https://doi.org/10.1080/14043858.2013.837267. ISSN 1404-3858. Dostupné také z: http://www.tandfonline.com/doi/abs/10.1080/14043858.2013.837267.

ÁLVAREZ, M., A. TORRES, E. RODRÍGUEZ, S. PADILLA a M.J. RODRIGO. 2013. Attitudes and parenting dimensions in parents' regulation of Internet use by primary and secondary school children. *Computers* [online]. Roč. 67, s. 69–78 [cit. 2014-08-28]. https://doi.org/10.1016/j.compedu.2013.03.005. Dostupné z: http://linkinghub.elsevier.com/retrieve/pii/S0360131513000833.

ANDERSON, Karen a Frances A. MAY. 2010. Does the Method of Instruction Matter? An Experimental Examination of Information Literacy Instruction in the Online, Blended, and Face-to-Face Classrooms. *The Journal of Academic Librarianship* [online]. 36(6), 495–500 [cit. 2018-02-05]. https://doi.org/10.1016/j.acalib.2010.08.005. ISSN 00991333. Dostupné z: http://linkinghub.elsevier.com/retrieve/pii/S0099133310002132.

BECHMANN, Anja. 2014. Non-informed Consent Cultures: Privacy Policies and App Contracts on Facebook. *Journal of Media Business Studies*. Roč. 11, č. 1.

DOMBROVSKÁ, Michaela, Hana LANDOVÁ a Ludmila TICHÁ. 2004. Informační gramotnost – teorie a praxe v ČR. *Národní knihovna: knihovnická revue* [online]. Roč. 15, č. 1, s. 7–18 [cit. 2014-07-24]. ISSN 1214-0678. Dostupné z: http://knihovna.nkp.cz/nkkr0401/0401007.html.

DÖRING, Nicola. 2014. Consensual sexting among adolescents: Risk prevention through abstinence education or safer sexting?. *Cyberpsychology: Journal of Psychosocial Research on Cyberspace* [online]. Roč. 8, č. 1 [cit. 2014-08-28]. https://doi.org/10.5817/CP2014-1-9. Dostupné z: http://cyberpsychology.eu/view.php?cisloclanku=2014031401.

EKE, Helen Nneka. 2012. Creating a digital footprint as a means of optimizing the personal branding of librarians in the digital society. *Webology*. Roč. 9, č. 2, s. 31–40.

GALLAGHER, Frank a Kat STEWART. 2011. Information literacy beyond the library: Cable in the Classroom. *College & Undergraduate Libraries* [online]. 2011-03-10, roč. 18, č. 1, s. 111–118 [cit. 2014-08-28]. https://doi.org/10.1080/10691316.2011.550537. Dostupné z: http://www.tandfonline.com/doi/abs/10.1080/10691316.2011.550537.

GINSBERG, Jeremy, Matthew H. MOHEBBI, Rajan S. PATEL, Lynnette BRAMMER, Mark S. SMOLINSKI a Larry BRILLIANT. 2008. Detecting influenza epidemics using search engine query data. *Nature* [online]. 2008-11-19, roč. 457, č. 7232, s. 1012–1014 [cit. 2014-08-28]. https://doi.org/10.1038/nature07634. Dostupné z: http://www.nature.com/doifinder/10.1038/nature07634.

HARRIS, Amy. 2010. Active learning for the Millennial Generation. *Georgia Library Quarterly* [online]. Fall 2010, roč. 47, č. 4, s. 13–14 [cit. 2014-08-30]. ISSN: 2157-0396. Dostupné z: EBSCOhost.

HARRIS, Margaret S. G. 2012. Fulfilling a European Vision through Flexible Learning and Choice. *European Journal of Education* [online]. Roč. 47, č. 3, s. 424–434 [cit. 2014-08-30]. https://doi.org/10.1111/j.1465-3435.2012.01535.x. Dostupné z: http://doi.wiley.com/10.1111/j.1465-3435.2012.01535.x.

HERRINGTON, Kim. 2010. Now is the Time! Teen Tech Week in a School Library. *Young Adult Library Services* [online]. Winter 2010, roč. 8, č. 2. s. 9–10 [cit. 2014-08-30]. ISSN 15414302. Dostupné z: http://search.proquest.com/docview/217697643.

HUSSAIN, Mohammed Ali a Sarath Babu DUGGIRALA. 2012. Secure Anonymous Route Discovery Protocol for Ad Hoc Routing in Ad Hoc Wireless Networks. *International Journal of Computer Technology and Applications* [online]. Jan 2012, roč. 3, č. 1. s. 495–501 [cit. 2014-08-30]. Dostupné z: ProQuest Technology Collection.

CHANG, Charlotte. 2010. Internet Safety Survey: Who will protect the children. *Berkeley Technology Law Journal* [online]. Roč. 25, č. 501, s. 501–527 [cit. 2014-08-30]. Dostupné z: http://www.btlj.org/data/articles/25_1/0501-0528%20Chang_Web.pdf.

CHESTER, Jeff a Kathryn MONTGOMERY. 2008. No escape: Marketing to kids in the digital age. *Multinational Monitor* [online]. Roč. 29, č. 1 [cit. 2014-08-30]. Dostupné z: http://www.multinationalmonitor.org/mm2008/072008/chester.html.

CHOI, Wonchan a Besiki STVILIA. 2015. Web credibility assessment: Conceptualization, operationalization, variability, and models. *Journal of the Association for Information Science and Technology* [online]. 66(12), 2399–2414 [cit. 2017-02-16]. https://doi.org/10.1002/asi.23543. ISSN 23301635. Dostupné z: http://doi.wiley.com/10.1002/asi.23543.

JANSSEN, José, Adriana J. BERLANGA a Rob KOPER. 2011. Evaluation of the Learning Path Specification. *Journal of Educational Technology & Society* [online]. Roč. 14, č. 3, s. 218–230 [cit. 2014-08-30]. ISSN 1176-3647. Dostupné z: http://search.proquest.com/docview/1287031475.

JOINER, Richard, Jeff GAVIN, Jill DUFFIELD, Mark BROSNAN, Charles CROOK, Alan DURNDELL, Pam MARAS, Jane MILLER, Adrian J. SCOTT a Peter LOVATT. 2005. Gender, Internet Identification, and Internet Anxiety: Correlates of Internet Use. *CyberPsychology* [online]. Roč. 8, č. 4, s. 371–378 [cit. 2014-08-30]. https://doi.org/10.1089/cpb.2005.8.371. Dostupné z: http://www.liebertonline.com/doi/abs/10.1089/cpb.2005.8.371.

JUVONEN, Jaana a Elisheva F. GROSS. 2008. Extending the School Grounds?-Bullying Experiences in Cyberspace. *Journal of School Health* [online]. Roč. 78, č. 9, s. 496–505 [cit. 2014-08-30]. https://doi.org/10.1111/j.1746-1561.2008.00335.x. Dostupné z: http://doi.wiley.com/10.1111/j.1746-1561.2008.00335.x.

KATZ, Irvin R., 2007. Testing Information Literacy in Digital Environments: ETS's iSkills Assessment. *Information Technology and Libraries* [online]. Roč. 26, č. 3, s. 3–12 [cit. 2018-02-13]. https://doi.org/10.6017/ital.v26i3.3271. ISSN 2163-5226. Dostupné z: http://ejournals.bc.edu/ojs/index.php/ital/article/view/3271.

KIM, Won, Ok-Ran JEONG, Chulyun KIM a Jungmin SO. 2011. The dark side of the Internet: Attacks, costs and responses. *Information Systems* [online]. Roč. 36, č. 3, s. 675–705 [cit. 2014-07-25]. https://doi.org/10.1016/j.is.2010.11.003. Dostupné z: http://linkinghub.elsevier.com/retrieve/pii/S0306437910001328.

KIRKPATRICK, Donald. 1996. Great Ideas Revisited: Revisiting Kirkpatrick's Four-Level Model. Training and Development [online]. Roč. 50, č. 1, s. 54–57 [cit. 2014-08-30]. Dostupné z: EBSCOhost.

KOVÁŘOVÁ, Pavla, Martin HÁJEK, Lenka KVAPILOVÁ, Lucie MÁJKOVÁ, Lenka MATUŠKOVÁ, Radek MEZULÁNÍK a Hana SLOUPENSKÁ. 2012b. Vzdělávání k informační bezpečnosti v českých knihovnách. ProInflow [online]. Roč. 4, č. 2 [cit. 2017-02-20]. ISSN 1804-2406. Dostupné z: http://www.phil.muni.cz/journals/index.php/proinflow/article/view/800/930.

LANDOVÁ, Hana a Zdeňka CIVÍNOVÁ. 2010. Aktivity vysokoškolských knihoven v oblasti informačního vzdělávání: vývoj v letech 2006–2010 na veřejných vysokých školách v ČR. ProInflow [online]. Roč. 2, č. 2 [cit. 2014-07-24]. ISSN 1804–2406. Dostupné z: http://pro.inflow.cz/aktivity-vysokoskolskych-knihoven-v-oblasti-informacniho-vzdelavani-vyvoj-v-letech-2006-2010-na-vere.

LEANDER, Lina, Sven Å CHRISTIANSON a Pär Anders GRANHAG. 2008. Internet-initiated sexual abuse: adolescent victims' reports about On – and Off -line sexual activities. *Applied Cognitive Psychology* [online]. Roč. 22, č. 9, s. 1260–1274 [cit. 2014-07-26]. https://doi.org/10.1002/acp.1433. Dostupné z: http://doi.wiley.com/10.1002/acp.1433.

LI, Lili a Lori LESTER. 2009. Rethinking Information Literacy Instructions in the Digital Age. *The International Journal of Learning* [online]. Roč. 16, č. 11, s. 569–577 [cit. 2014-08-30]. ISSN 1447-9494. Dostupné z: EBSCOhost.

Majority of Youth Understand Copyright but Continue to Download Illegally. 2004. *The Reading Teacher*. International Reading Association, 58(1). ISSN 0034-0561. Dostupné z: JSTOR Journals.

Manifest IFLA o přístupu k Internetu. 2002. *Bulletin SKIP* [online]. Č. 2 [cit. 2014-08-30]. Dostupné z: http://wwwold.nkp.cz/o_knihovnach/konsorcia/skip/Bull02_23.htm.

MARCOUX, Elizabeth. 2010. Cybersecurity a school libraries. *Teacher Librarian* [online]. Roč. 67, č. 2, s. 67–68 [cit. 2014-08-30]. Dostupné z: http://search.proquest.com/docview/846786568.

MARTIN, Nigel a John RICE. 2012. Children's cyber-safety and protection in Australia: An analysis of community stakeholder views. *Crime Prevention and Community Safety* [online]. Roč. 14, č. 3, s. 165–181 [cit. 2014-08-30]. https://doi.org/10.1057/cpcs.2012.4. Dostupné z: http://www.palgrave-journals.com/doifinder/10.1057/cpcs.2012.4.

METZGER, Miriam J. A Andrew J. FLANAGIN. 2013. Credibility and trust of information in online environments: The use of cognitive heuristics. *Journal of Pragmatics*. 59, 210–220. https://doi.org/10.1016/j.pragma.2013.07.012. ISSN 03782166. Dostupné také z: http://linkinghub.elsevier.com/retrieve/pii/S0378216613001768.

MOORE, Shelley C. 2012. Digital Footprints on the Internet. *International Journal of Childbirth Education* [online]. Roč. 27, č. 3, s. 86–91 [cit. 2014-08-30]. Dostupné z: http://search.proquest.com/docview/1039291547.

MORENO, Megan A., Katie G. EGAN, Kaitlyn BARE, Henry N. YOUNG a Elizabeth D. COX. 2013. Internet safety education for youth: stakeholder perspectives. *BMC Public Health* [online]. Roč. 13, č. 1, s. 543– [cit. 2014-08-30]. https://doi.org/10.1186/1471-2458-13-543. Dostupné z: http://www.biomedcentral.com/1471-2458/13/543.

Na internetu bezpečně. 2014. *Tišnovské noviny: příloha Tišnovských novin* [online]. Roč. 24, č. 4, s. 6 [cit. 2014-08-30]. Dostupné z: http://tisnov.cz/soubor/tisnovske_noviny_2014-04_web_priloha-kam.pdf.

O'NEILL, Brian. 2012. Trust in the information society. *Computer Law* [online]. Roč. 28, č. 5, s. 551–559 [cit. 2014-08-30]. https://doi.org/10.1016/j.clsr.2012.07.005. Dostupné z: http://linkinghub.elsevier.com/retrieve/pii/S0267364912001409.

OGROCKÁ, Eva. 2013. Nebezpečný internet aneb Co dělají vaše děti právě teď? *Inflow* [online]. 30. 11. 2013 [cit. 2014-08-30]. Dostupné z: http://www.inflow.cz/nebezpecny-internet-aneb-co-delaji-vase-deti-prave-ted.

OHM, Paul. 2009. Broken promises of privacy: Responding to the surprising failure of anonymization. *UCLA Law Review* [online]. Roč. 57, č. 1701 [cit. 2014-08-30]. Dostupné z: http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1450006.

OOLO, Egle a Andra SIIBAK. 2013. Performing for one's imagined audience: Social steganography and other privacy strategies of Estonian teens on networked publics. *Cyberpsychology: Journal of Psychosocial Research on Cyberspace*, vol. 7, issue 1. https://doi.org/10.5817/CP2013-1-7. Dostupné z: http://www.cyberpsychology.eu/view.php?cisloclanku=2013011501.

PETRESS, Ken. 2008. What Is Meant by "Active Learning?". *Education* [online]. Summer 2008, roč. 128, č. 4, s. 566–569 [cit. 2014-08-30]. ISSN: 0013-1172. Dostupné z: EBSCOhost.

PIHT, Sirje, Piret LEHISTE, Rea RAUS a Mariliis LAZAREV. 2012. The relevance of evocation and reflection cards in the learning process. *Problems of Education in the 21st Century*. Č. 41, s. 61–74.

PINTO, Caro. 2013. Teaching Librarians & Project Management: New Expectations for the Digital Age. *Archive Journal* [online]. Č. 3 [cit. 2014-08-30]. Dostupné z: http://www.archivejournal.net/issue/3/notes-queries/teaching-librarians-project-management-new-expectations-for-the-digital-age/.

POLING, Devereaux A. A Julie M. HUPP. 2009. Active Learning Through Role Playing: Virtual Babies in a Child Development Course. *College Teaching* [online]. Fall, 2009, roč. 57, č. 4, s. 221–228 [cit. 2014-08-30]. ISSN 8756-7555. Dostupné z: http://search.proquest.com/docview/848215353.

Polovina dětí reaguje na internetu na zprávy od cizích lidí – ze zvědavosti. 2010. *HN Tech* [online]. 9. 2. 2010 [cit. 2014-08-30]. Dostupné z: http://tech.ihned.cz/c1-40440600-polovina-deti-reaguje-na-internetu-na-zpravy-od-cizich-lidi-rodice-je-prilis-nechrani.

PORADA, Viktor a Roman RAK. 2006. Teorie digitálních stop a její aplikace v kriminalistice a forenzních vědách. *Karlovarská právní revue* [online]. Roč. 2, č. 4, s. 1 – 21 [cit. 2014-08-30]. Dostupné z: http://www.sinz.cz/archiv/docs/si-2005-01-3-23.pdf.

PRENSKY, Marc. 2001. Digital Natives, Digital Immigrants. *On the Horizon* [online]. Roč. 9, č. 5 [cit. 2014-05-04]. ISSN 1085-4959. Dostupné z: http://www.marcprensky.com/writing/Prensky%20-%20Digital%20Natives,%20Digital%20Immigrants%20-%20Part1.pdf.

RABUŠICOVÁ, Milada, Klára ŠEĎOVÁ, Kateřina TRNKOVÁ a Vlastimil ČIHÁČEK. 2004. K otevřenosti škol vůči rodičům a veřejnosti. In: *Studia paedagogica: Sborník prací filozofické fakulty brněnské univerzity* [online]. s. 59–72 [cit. 2014-08-30]. ISSN 2336-4521. Dostupné z: http://www.phil.muni.cz/journals/index.php/studia-paedagogica/article/view/395/551.

RANGUELOV, Stanislav. 2010. Summary Report Education on Online Safety in Schools in Europe. *New Horizons in Education* [online]. Roč. 58, č. 3, s. 149–163 [cit. 2014-08-30]. ISSN-1683-1381. Dostupné z: http://files.eric.ed.gov/fulltext/EJ966666.pdf.

SALTZMAN, Marc. 2008. Identity thieves 'phishing' the Internet. *Star – Phoenix* [online]. Sep 20, 2008, E.14 [cit. 2014-08-29]. ISSN 0832-4174. Dostupné z: http://search.proquest.com/docview/348892935.

SAVOLAINEN, Reijo. 2011. Judging the quality and credibility of information in Internet discussion forums. *Journal of the American Society for Information Science and Technology* [online]. 62(7), 1243–1256 [cit. 2017-02-16]. https://doi.org/10.1002/asi.21546. ISSN 15322882. Dostupné z: http://doi.wiley.com/10.1002/asi.21546.

SMART, K. L., C. WITT a J. P. SCOTT. 2012. Toward Learner-Centered Teaching: An Inductive Approach. *Business Communication Quarterly* [online]. 7. 11. 2012, roč. 75, č. 4, s. 392–403 [cit. 2014-08-30]. https://doi.org/10.1177/1080569912459752. Dostupné z: http://bcq.sagepub.com/cgi/doi/10.1177/1080569912459752.

SMEJKALOVÁ, Kateřina, 2014. K pojetí konstruktivismu jakožto modernímu paradigmatu vzdělávání. *Paideia: philosophical e-journal of Charles University* [online]. Praha, 11(1) [cit. 2018-08-08]. ISSN 1214-8725.

SOLON, Olivia. 2012. How much data did Facebook have on one man? 1,200 pages of data in 57 categories. *Wired* [online]. 28. 12. 2012 [cit. 2014-08-28]. Dostupné z: http://www.wired.co.uk/magazine/archive/2012/12/start/privacy-versus-facebook.

STASIUNAITIENE, Egle a Lina KAMINSKIENE. 2009. Qualitative Parameters for Evaluation Procedures of Non-Formal and Informal Learning Achievements. *Quality of Higher Education* [online]. Č. 6, s. 117–140. ISSN-1822-1645. Dostupné z: http://files.eric.ed.gov/fulltext/EJ870192.pdf.

TAMBAUM, Tiina. 2010. Expectations of the elderly for the Internet as an influencing

factor for the internet teaching. *Problems of Education in the 21st Century* [online]. Roč. 22 [cit. 2014-08-30]. Dostupné z: EBSCOhost

TAYLOR, Arthur a Heather A. DALAL. 2014. Information Literacy Standards and the World Wide Web: Results from a Student Survey on Evaluation of Internet Information Sources. *Information Research: An International Electronic Journal* [online]. 19(4) [cit. 2017-02-17]. Dostupné z: http://www.informationr.net/ir/19-4/paper645.html#.WKbbzvJDQ2Z.

TERESEVIČIENĖ, Margarita, Vaiva ZUZEVIČIŪTĖ a Monika IVOŠKAITĖ. 2008. Assessment and Recognition of Achievements of Non-Formal and Informal Learning – Function in Context of Lifelong Learning, Achievements and Challenges. *Socialiniai tyrimai (Social Research)* [online]. Roč. 11, č. 1, s. 67–73 [cit. 2014-08-30]. ISSN 1392-3110. Dostupné z: http://etalpykla.lituanistikadb.lt/fedora/get/LT-LDB-0001:J.04~2008~1367164334343/DS.002.1.01.ARTIC.

THOMPSON, Samuel T. C. 2013. Helping the hacker? Library information, security, and social engineering. *Information Technology and Libraries* [online]. Roč. 25, č. 4, s. 222–225 [cit. 2014-08-30]. Dostupné z: http://ejournals.bc.edu/ojs/index.php/ital/article/viewFile/3355/2966.

TUOMAITE, Virginija and Vaiva ZUZEVICIUTE. 2008. Validation and Recognition of Non-Formal and Informal Learning of Employees as Prerequisite of Lifelong Learning. *Organizacijø Vadyba: Sisteminiai Tyrimai* [online]. Č. 45, s. 99–113 [cit. 2014-08-30]. ISSN 1392-1142. Dostupné z: http://search.proquest.com/docview/222760897.

WALRAVE, Michel, Ini VANWESENBEECK a Wannes HEIRMAN. 2012. Connecting and protecting? Comparing predictors of self-disclosure and privacy settings use between adolescents and adults. *Cyberpsychology: Journal of Psychosocial Research on Cyberspace* [online]. Roč. 6, č. 1 [cit. 2014-08-30]. https://doi.org/10.5817/CP2012-1-3. Dostupné z: http://www.cyberpsychology.eu/view.php?cisloclanku=2012051201.

WEAVER, Anne. 2010. Facebook and Other Pandora's Boxes. *Access*. Roč. 24, č. 4, s. 24–32.

WEAVER, Stephen D. A Mark GAHEGAN. 2007. Constructing, visualizing, and analyzing a digital footprint. *Geographical Review*. Roč. 97, č. 3, s. 324–350. https://doi.org/10.1111/j.1931-0846.2007.tb00509.x.

WEEDEN, Shalynn, Bethany COOKE a Michael MCVEY. 2013. Underage Children and Social Networking. *Journal of Research on Technology in Education* [online]. Roč. 45, č. 3, s. 249–262 [cit. 2014-08-30]. https://doi.org/10.1080/15391523.2013.10782605. Dostupné z: http://www.tandfonline.com/doi/abs/10.1080/15391523.2013.10782605.

WOLD, Thomas. 2010. Protection and access: To regulate young people's internet use. *International Journal of Media and Cultural Politics* [online]. Roč. 6, č. 1, s. 63–79 [cit. 2014-08-30]. https://doi.org/10.1386/macp.6.1.63/1. Dostupné z: http://www.ingentaconnect.com/content/intellect/mcp/2010/00000006/00000001/art00005.

WOOLLEY, Darryl. 2015. The association of moral development and moral intensity with music piracy. *Ethics* [online]. 17(3), 211–218 [cit. 2017-02-16]. https://doi.org/10.1007/s10676-015-9376-7. ISSN 13881957.

ZUBER-SKERRITT, Ortrun a Margaret FLETCHER. 2007. The quality of an action research thesis in the social sciences. *Quality Assurance in Education* [online]. Roč. 15, č. 4, s. 413–436 [cit. 2014-08-30]. https://doi.org/10.1108/09684880710829983. Dostupné z: http://www.emeraldinsight.com/10.1108/09684880710829983.

Webové zdroje

Akce – kyberšikana. 2014. *Základní škola Dačice: Komenského 7* [online]. 24. 4. 2014 [cit. 2014-08-28]. Dostupné z: http://www.zsdacice.eu/fotogalerie.php?typgalerie=99&typakce=1436.

ANGWIN, Julia a Jennifer VALENTINO-DEVRIES. 2010. The Information That Is Needed to Identify You: 33 Bits. In: *Digits* [online]. 4. 8. 2010 [cit. 2014-08-28]. Dostupné z: http://blogs.wsj.com/digits/2010/08/04/the-information-that-is-needed-to-identify-you-33-bits/.

Aukro nápověda: komentáře a hodnocení prodeje. [b.r.]. *Aukro* [online]. [cit. 2014-08-28]. Dostupné z: http://napoveda.aukro.cz/18967/18959/20205/system-komentaru-hodnoceni-prodeje-na-aukru.

Barevný svět poznání. 2014. *Masarykova veřejná knihovna Vsetín* [online]. 9. 6. 2014 [cit. 2014-08-28]. Dostupné z: http://www.mvk.cz/knihovna/vsetin/barevny-svet-poznavani/.

BAUEROVÁ, Marta. 2014. Kyberšikana. *Městská knihovna ve Svitavách* [online]. 11. 2. 2014 [cit. 2014-08-28]. Dostupné z: http://www.booksy.cz/?p=2099.

Big6 Skills Overview. c2013. *The Big6* [online]. [cit. 2014-08-28]. Dostupné z: http://big6.com/pages/about/big6-skills-overview.php.

Březen měsíc Internetu 2008: Akce pro veřejnost v Knihovně města Plzně, p. o. 2008. In: *Knihovna města Plzně, p. o.* [online]. [cit. 2014-08-28]. Dostupné z: http://www.knihovna.plzen.eu/aktuality/bmi08.rtf.

BONWELL, Charles C. a James A. EISON, 1991. Active Learning: Creating Excitement in the Classroom. *ERIC Digest* [online]. [cit. 2018-08-09]. Dostupné z: https://files.eric.ed.gov/fulltext/ED340272.pdf.

Certifikáty a ocenění e-shopů. c2014. *Ověř si to* [online]. [cit. 2014-08-28]. Dostupné z: http://www.oversito.cz/uzitecne-informace/certifikaty-a-oceneni-e-shopu/.

Citizenship in the Digital Age: Sample Lesson Plans for Grades 1-12. 2012. In: *New York City School Library System* [online]. 4. 4. 2012 [cit. 2014-08-28]. Dostupné z: http://schools.nyc.gov/NR/rdonlyres/3CA0188D-66A2-490C-9E90-1EFCADA92F8C/0/Citizenshipinthedigitalage.pdf.

DANIELISOVÁ, Tereza, Michal DENÁR a Pavla KOVÁŘOVÁ. 2018. Ochrana osobních údajů – Příručka pro knihovny. *Informace pro knihovny* [online]. 7. 2. 2018 [cit. 2018-02-13]. Dostupné z: http://ipk.nkp.cz/legislativa/01_LegPod/ochrana-osobnich-udaju/ochrana-osobnich-udaju-prirucka-pro-knihovny.

Davis Elementary Internet Safety Month Lesson Plans. c2002–2014. *Davis Library* [online]. [cit. 2014-08-28]. Dostupné z: http://cfbportal.schoolwires.net/Page/25483.

Dětské oddělení. [b.r.]. *Městská knihovna Pelhřimov* [online]. Pelhřimov: Městská knihovna Pelhřimov [cit. 2014-08-28]. Dostupné z: http://www.knih-pe.cz/index.php/detske-oddeleni

Digital Footprint. 2014. *Manheim Township High School Library* [online]. [cit. 2014-08-28]. Dostupné z: http://hs.mtwp.libguides.com/content.php?pid=363642&sid=3320865.

DUERAGER, Andrea a Sonia LIVINGSTONE. 2012. How can parents support children's internet safety?. In: *LSE Research Online* [online]. London: EU Kids Online [cit. 2014-08-28]. Dostupné z: http://eprints.lse.ac.uk/42872/1/How%20can%20parents%20support%20children%E2%80%99s%20internet%20safety%28lsero%29.pdf.

Egosurf. c2014. *Oxford Dictionaries* [online]. [cit. 2014-08-28]. Dostupné z: http://www.oxforddictionaries.com/definition/english/egosurf.

FINDAHL, Olle. 2009. Preschoolers and the Internet: will children start to use the Internet when they start walking? In: *London School of Economics & Political Science* [online]. [cit. 2014-08-28]. Dostupné z: http://www.lse.ac.uk/media@lse/research/EUKidsOnline/EU%20Kids%20I%20%282006-9%29/Conference%20Papers%20and%20abstracts/Emerging%20Issues/Findahl.pdf.

FISHER, Clarence. 2010. Stalking in English Class. *Remote Access even from here* [online]. [cit. 2014-08-28]. Dostupné z: http://www.evenfromhere.org/2010/10/13/stalking-in-english-class/.

Framework for Information Literacy for Higher Education. 2015. In: *American Library Association* [online]. [cit. 2017-02-10]. Dostupné z: http://www.ala.org/acrl/standards/ilframework.

GÉBLOVÁ, Alena. 2013. Síť veřejných knihoven máme nejhustší na světě. Český statistický úřad [online]. [cit. 2014-08-28]. Dostupné z: http://www.czso.cz/csu/2013edicniplan.nsf/c/EA002B5940.

Get your Data!: Make an Access Request at Facebook! [b.r.]. *Europe versus facebook* [online]. [cit. 2014-08-26]. Dostupné z: http://europe-v-facebook.org/EN/Get_your_Data_/get_your_data_.html.

HARRIS, Robert. 2015. Evaluating Internet Research Sources. *VirtualSalt* [online]. [cit. 2017-02-16]. Dostupné z: http://www.virtualsalt.com/evalu8it.htm.

HEMBREE. 2013. Thinking about Digital Footprints. *Bulldog Reader Blog* [online]. 6. 10. 2013 [cit. 2014-08-28]. Dostupné z: http://bellbulldogreaders.edublogs.org/2013/10/06/thinking-about-digital-footprints/.

CHRÁSTKOVÁ KNÍŘOVÁ, Michaela. 2013. Kyberšikana v dětských kolektivech. *Město Březová u Sokolova* [online]. 23. 5. 2013 [cit. 2014-08-28]. Dostupné z: http://mu-brezova.cz/?article_id=11846.

IFLA/UNESCO Public Library Manifesto. 1994. In: *IFLA* [online]. [cit. 2014-08-28]. Dostupné z: http://www.ifla.org/publications/iflaunesco-public-library-manifesto-1994.

In the fishbowl. 2013. *COETAIL* [online]. 21. 4. 2013 [cit. 2014-08-28]. Dostupné z: http://www.coetail.com/bqdressler/tag/digital-footprint-2/.

Information Literacy Competency Standards for Higher Education. 2000. In: *American Library Association* [online]. [cit. 2014-08-28]. Dostupné z: http://www.ala.org/acrl/sites/ala.org.acrl/files/content/standards/standards.pdf.

Information literacy skills. 2012. In: *CILIP* [online]. [cit. 2014-08-28]. Dostupné z: http://www.cilip.org.uk/sites/default/files/documents/Information%20literacy%20skills.pdf.

Information literacy standards for student learning: Standards and indicators. 1998. In: *Innovative Library Initiatives Promotion Group* [online]. [cit. 2014-08-28]. Dostupné z: http://www.ilipg.org/sites/ilipg.org/files/bo/InformationLiteracyStandards_final.pdf.

IRGENS, Morten. 2013. What does it all mean? *The Business of Better* [online]. 1. 8. 2013 [cit. 2014-08-26]. Dostupné z: http://www.businessofbetter.com/?p=2057.

ISTE Standards: Students. c2007. In: *International Society for Technology in Education* [online]. [cit. 2014-08-28]. Dostupné z: http://www.iste.org/docs/pdfs/20-14_ISTE_Standards-S_PDF.pdf.

Jelly Bean 4.2: a new and improved Jelly Bean. [2012]. *Android* [online]. [cit. 2014-08-26]. Dostupné z: http://www.android.com/versions/jelly-bean-4-2/.

KASÍK, Pavel. 2009. Češi Facebooku nebezpečně věří. Falešné krasavici naletělo 60 procent. In: *Technet* [online]. 19. 11. 2009 [cit. 2014-08-28]. Dostupné z: http://technet.idnes.cz/

cesi-facebooku-nebezpecne-veri-falesne-krasavici-naletelo-60-procent-112-/sw_internet.aspx?c=A091117_171036_sw_internet_pka.

KOVÁŘOVÁ, Pavla. 2011. *Ohrožení dětí na internetu: teorie a doporučení pro vzdělávání* [online]. [cit. 2017-02-15]. Dostupné z: https://is.muni.cz/auth/th/136790/ff_r/.

KOVÁŘOVÁ, Pavla. 2015. *Zneužití digitálních stop uživatelů ICT: vzdělávání v knihovnách jako prevence narušení soukromí* [online]. [cit. 2017-02-15]. Dostupné z: https://is.cuni.cz/webapps/zzp/detail/105358. Vedoucí práce Martin Souček.

LEYDEN, John. 2005. Americans are pants at password security. In: *The Register* [online]. 6. 5. 2005 [cit. 2014-08-28]. Dostupné z: http://www.theregister.co.uk/2005/05/06/verisign_password_survey/.

LIBRARIANTIFF. 2014. Digital Citizenship at CMS. *Mighty Little Librarian* [online]. 27. 2. 2014 [cit. 2014-08-28]. Dostupné z: http://www.mightylittlelibrarian.com/?p=1081.

Library lessons calendar. c2002-2014. *C.S. Porter Middle School* [online]. [cit. 2014-08-28]. Dostupné z: http://www.mcpsmt.org/Page/6273.

LIVINGSTONE, Sonia, Leslie HADDON, Anke GÖRZIG a Kjartan ÓLAFSSON. 2011. Risks and safety on the internet: The perspective of European children. Full Findings. In: *London School of Economics & Political Science*. London: LSE, 168 s. ISSN 2045-2551. Dostupné z: http://www2.lse.ac.uk/media@lse/research/EUKidsOnline/EU%20Kids%20II%20(2009-11)/EUKidsOnlineIIReports/D4FullFindings.pdf.

LochyProduction. 2013. Česká Televize | Na Stopě | Metin 2 | Krádež Účtu. In: *YouTube* [online]. 7. 2. 2013 [cit. 2014-08-28]. Dostupné z: https://www.youtube.com/watch?v=d-7bo5gQSZhI.

MADDEN, Mary. 2007. Digital Footprints: Online identity management and search in the age of transparency. In: *Pew Internet & American Life Project* [online]. [cit. 2014-08-28]. Dostupné z: http://www.pewinternet.org/files/old-media/Files/Reports/2007/PIP_Digital_Footprints.pdf.pdf.

MADDEN, Mary. 2012. Privacy management on social media sites. In: *Pew Internet & American Life Project* [online]. 24. 2. 2012 [cit. 2014-08-28]. Dostupné z: http://www.pewinternet.org/2012/02/24/privacy-management-on-social-media-sites/.

Manifest IFLA pro digitální knihovny. 2010. In: *Portál Knihovnického institutu Národní knihovny ČR* [online]. Prosinec 2010 [cit. 2014-08-26]. Dostupné z: http://knihovnam.nkp.cz/docs/IFLA/IFLA_Manifesto_for_Digital_Libraries_201012cz.pdf.

MAREK, Tomáš. 2015. Tvorba efektivních grafů: Doporučení pro diplomovou práci. In: *IS MU* [online]. Brno, s. 1–25 [cit. 2017-02-17]. Dostupné z: http://is.muni.cz/th/362075/ff_m/tvorba-efektivnich-grafu.pdf.

MARTÍNEZ-CABRERA, Alejandro. 2010. Erasing all digital footprints 'impossible'. In: *SFGate* [online]. 6. 7. 2010 [cit. 2014-08-28]. Dostupné z: http://www.sfgate.com/business/article/Erasing-all-digital-footprints-impossible-3259754.php.

MCCANDLESS, David a Marek PICHA. 2012. Argumentační fauly. MASARYKOVA UNIVERZITA. *Centrum občanského vzdělávání* [online]. Brno [cit. 2017-02-17]. Dostupné z: http://www.obcanskevzdelavani.cz/work/ke-stazeni/argumentacni-fauly-A3-barva.pdf.

MCKENZIE, Dianne. 2013. The C.R.A.P. test rubric. *Library grits blog* [online]. [cit. 2017-02-16]. Dostupné z: http://librarygrits.blogspot.cz/2013/12/the-crap-test-rubric.html.

Městská knihovna Přerov – březen 2014. 2014. *Přerov* [online]. Březen 2014 [cit 2014-08-28]. Dostupné z: http://prerov.nejlepsi-adresa.cz/akce-kalendar/mista/Mestska-knihovna-Prerov-Zerotinovo-namesti-36-Prerov/2014/3/31.

MINELLE, Bethany. 2018. US military to review security amid Strava fitness app fears. *SkyNews* [online]. 29 January 2018 [cit. 2018-02-07]. Dostupné z: https://news.sky.com/story/us-military-to-review-security-amid-strava-fitness-app-fears-11228045.

Mobile/Tablet Operating System Market Share. 2017. In: *NetMarketShare* [online]. [cit. 2017-02-09]. Dostupné z: https://www.netmarketshare.com/operating-system-market-share.aspx?qprid=8&qpcustomd=1.

MORRIS, Kathleen. 2013. Teaching Children About Digital Footprints. *Primary Tech* [online]. 22. 2. 2013 [cit. 2014-08-28]. Dostupné z: http://primarytech.global2.vic.edu.au/2013/02/22/teaching-childre-about-digital-footprints/.

Nabídka knihovnických lekcí a besed na školní rok 2012 – 2013. 2012. In: *Regionální knihovna Karviná* [online]. Karviná: Regionální knihovna Karviná [cit. 2014-08-28]. Dostupné z: http://www.rkka.cz/KVC/KVC2013.pdf.

Nabídka pro školy. [2014]. *Knihovna města Plzně* [online]. Plzeň: Knihovna města Plzně, Obvodní knihovna Doubravka [cit. 2014-08-28]. Dostupné z: http://www.knihomol.wz.cz/skoly.php.

Nabídka tematických besed pro školy pobočka Jungmannova 2014/2015 pro 1. stupeň ZŠ. c2009 – 2014. *Knihovna města Olomouce* [online]. [cit. 2014-08-28]. Dostupné z: http://www.knihomol.wz.cz/skoly.php.

Nabídka vzdělávání pro střední školy a gymnázia. [2014]. *Městská knihovna Prostějov* [online]. Prostějov: Městská knihovna Prostějov [cit. 2014-08-28]. Dostupné z: http://knihovnapv.webnode.cz/pro-skoly/ss/.

Nástrahy v online světě: beseda pro 6. – 9. třídy ZŠ. 2014. *Knihovna města Ostravy* [online]. Ostrava: Knihovna města Ostravy [cit. 2014-08-28]. Dostupné z: http://cms.kmo.cz/www/cl-900/297-knihovnicke-lekce-a-besedy/?akce=240.

NIKOS, Askitas a Klaus F. ZIMMERMANN. 2009. Google Econometrics and Unemployment Forecasting. *IZA Discussion Paper No. 4201* [online]. [cit. 2012-08-20]. Dostupné z: http://ssrn.com/abstract=1415585.

Operating System Market Share. 2018. In: *NetMarketShare* [online]. [cit. 2018-02-13]. Dostupné z: https://netmarketshare.com/operating-system-market-share.aspx?id=platformsMobile.

Operating System Share by Version. 2018. In: *NetMarketShare* [online]. [cit. 2018-02-13]. Dostupné z: https://netmarketshare.com/operating-system-market-share.aspx?id=platformsDesktopVersions.

Overview. [b.r.] *Do Not Track: Universal Web Tracking Opt Out* [online]. [cit. 2014-08-28]. Dostupné z: http://donottrack.us/.

PC učebna. 2013. *Městská knihovna Litvínov* [online]. Litvínov: Městská knihovna Litvínov, 18. 2. 2013 [cit. 2014-08-28]. Dostupné z: http://www.knihovna-litvinov.cz/sluzby/pc-ucebna.

PINTÉR, Josef. V havířovské Městské knihovně o hororové literatuře. 2014. *Karvinský deník* [online]. 18. 2. 2014 [cit. 2014-08-30]. Dostupné z: http://karvinsky.denik.cz/kultura_region/v-havirovske-mestske-knihovne-o-hororove-literature-20140218.html.

Plán ZŠ Aloisina výšina na měsíc říjen 2012. *Základní škola, Liberec: Aloisina výšina* [online]. Liberec: Základní škola Aloisina výšina [cit. 2014-08-28]. Dostupné z: http://www.zs-aloisinavysina.cz/?D=186.

POTÁČEK, Jiří. 2003–. Informační bezpečnost. In: *KTD: Česká terminologická databáze knihovnictví a informační vědy (TDKIV)* [online]. Praha: Národní knihovna ČR [cit. 2014-

08-28]. Dostupné z: http://aleph.nkp.cz/F/?func=direct&doc_number=000000074&local_base=KTD.

Presidential Committee on Information Literacy: Final Report. 1989. *Association of College and Research Libraries* [online]. Chicago: American Library Association, 10. 1. 1989 [cit. 2014-08-28]. Dostupné z: http://www.ala.org/acrl/publications/whitepapers/presidential.

Preventivní programy. c2014. *ZŠ Blansko Erbenova* [online]. Blansko: ZŠ Blansko, Erbenova [cit. 2014-08-28]. Dostupné z: http://www.erbenova.cz/detail-historie-clanky/560.html

Přednáškový blok: Digitální stopy (25. 2. 2014). 2014. *Novinkový systém SR FF UK* [online]. 22. 2. 2014 [cit. 2014-08-28]. Dostupné z: http://sml.strada.ff.cuni.cz/novinka/629/.

Přístup k osobním údajům na Facebooku: Kde na Facebooku najdu své údaje? c2014. *Facebook* [online]. [cit. 2014-08-28]. Dostupné z: https://www.facebook.com/help/405183566203254.

QUICK, Susannah, Gillian PRIOR, Ben TOOMBS, Luke TAYLOR a Rosanna CURRENTI. 2013. In: Názory uživatelů na přínosy informačních a komunikačních technologií ve veřejných knihovnách v České republice: Závěrečná zpráva [online]. TNS – Bill&Melinda Foundation [cit. 2013-11-02]. Dostupné z: http://www.ikaros.cz/images/201308/Cross-European_Libraries_Survey_CZE.pdf#.

RÁBLOVÁ, Romana. 2014. Lapeni v síti. In: *SDRUK* [online]. Ostrava: Sdružení knihoven ČR [cit. 2014-08-28]. Dostupné z: http://www.sdruk.cz/data/xinha/sdruk/2014/rablova_prezentace.pdf.

Rámcové vzdělávací programy. c2013-2014. *Ministerstvo školství, mládeže a tělovýchovy* [online]. Praha: Ministerstvo školství, mládeže a tělovýchovy [cit. 2014-08-28]. Dostupné z: http://www.msmt.cz/vzdelavani/skolstvi-v-cr/skolskareforma/ramcove-vzdelavaci-programy.

REID, Kate. 2014. Digital Citizenship – What does it mean to you?. *The Hutchins school library lions* [online]. 12. 5. 2014 [cit. 2014-08-28]. Dostupné z: http://blogs.hutchins.tas.edu.au/librarylions/2014/05/12/digital-citizenship-what-does-it-mean-to-you/.

Riding the Waves or Caught in the Tide?: Insights from the IFLA Trend Report. 2013. In: *IFLA Trend Report* [online]. Hague: IFLA [cit. 2014-08-28]. Dostupné z: http://trends.ifla.org/files/trends/assets/insights-from-the-ifla-trend-report_v3.pdf.

Safer Internet for Children: Qualitative study in 29 European countries – summary report. 2007. In: *European Commission* [online]. [cit. 2014-08-28]. Dostupné z: http://ec.europa.eu/public_opinion/archives/quali/ql_safer_internet_summary.pdf.

Scope & Sequence. 2012. *Common Sense Media* [online]. [cit. 2014-08-28]. Dostupné z: https://www.commonsensemedia.org/educators/scope-and-sequence.

SKLÁDANÁ, Jana. Efektivita lekcí informační bezpečnosti pro 4. ročníky ZŠ – srovnávací analýza. Brno, 2017. 95 s. Diplomová práce. Masarykova univerzita, Filozofická fakulta, Ústav české literatury a knihovnictví, Kabinet informačních studií a knihovnictví. Vedoucí práce PhDr. Pavla Kovářová, Ph.D. Dostupné z: https://is.muni.cz/th/415312/ff_m/DIPLOMKA_final.pdf.

Statistika kultury. c2007. *Ministerstvo kultury* [online]. Praha: Ministerstvo kultury [cit. 2014-08-28]. Dostupné z: http://www.mkcr.cz/scripts/detail.php?id=5018.

STOWER, Helen. 2013. Online = Public...a lesson for students in taking care of your digital footprint. *EduBlogs* [online]. 16. 1. 2013 [cit. 2014-08-28]. Dostupné z: http://sallytilley.edublogs.org/2013/01/16/online-public-a-lesson-for-students-in-taking-care-of-your-digital-footprint/.

SUJA, Miroslav. 2011. CIA sleduje sociální sítě. *Czech Free Press* [online]. [cit. 2017-02-27]. Dostupné z: http://www.czechfreepress.cz/amerika/cia-sleduje-socialni-site.html.

SULLIVAN, Laurie. 2011. Behavioral Targeting For Facebook. *MediaPost Publications* [online]. 16. 3. 2011 [cit. 2014-08-26]. Dostupné z: http://www.mediapost.com/publications/article/146799/behavioral-targeting-for-facebook.html.

SULLIVAN, Nancy. [b.r.]. iPad Lessons. *Madison High School Library* [online]. [cit. 2014-08-28]. Dostupné z: https://sites.google.com/site/madisonhslibrary/class-connections/ipad-lessons.

SWALLOW, Erica. 2011. How Recruiters Use Social Networks to Screen Candidates: Infographic. *Mashable: The Social Media Guide* [online]. October 23, 2011 [cit. 2014-08-26]. Dostupné z: http://mashable.com/2011/10/23/how-recruiters-use-social-networks-to-screen-candidates-infographic/.

SWETNAM, Lorena. 2013. Digital Citizenship, Digital Footprint & Digital Literacy. *It all started in the library...* [online]. 29. 8. 2013 [cit. 2014-08-28]. Dostupné z: http://lswetnam.blogspot.cz/2013/08/digital-citizenship-digital-footprint.html.

Sylaby a moduly. [2014]. *ECDL Czech Republic* [online]. [cit. 2014-08-28]. Dostupné z: http://www.ecdl.cz/zakladni_moduly.php.

Školy. [2014]. *Městská knihovna Litomyšl* [online]. Litomyšl: Městská knihovna Litomyšl [cit. 2014-08-28]. Dostupné z: http://www.litomysl.cz/knihovna/skoly.

The Role of Libraries in Lifelong Learning: Final report of the IFLA project under the Section of Public Libraries. 2003. In: *IFLA* [online]. [cit. 2014-08-28]. Dostupné z: http://archive.ifla.org/VII/s8/proj/Lifelong-LearningReport.pdf.

VÁLEK, Jiří. 2009. Elektronizace zdravotnictví (e-Health). *Zdraví a Zdravotnictví* [online]. [cit. 2014-08-26]. Dostupné z: http://www.zdrav.cz/modules.php?op=modload&name=News&file=article&sid=8963.

Využití internetu dětmi ve věku od 12 do 17 let: Safeinternet-Gemius Ad-hoc. 2006. In: *Národní centrum bezpečnějšího internetu* [online]. Praha: Národní centrum bezpečnějšího internetu [cit. 2014-08-26]. Dostupné z: www.ncbi.cz/category/5-dokumenty?download=21.

Web 2.0 suicide machine [online]. [b.r.]. [cit. 2018-02-13]. Dostupné z: http://suicidemachine.org/.

What is a digital footprint?. c2010. *Dear librarian* [online]. [cit. 2014-08-28]. Dostupné z: http://www.dearlibrarian.com/2010/11/what-is-a-digital-footprint/.

XNOTION. 2010. How to Unblock Facebook. In: *HubPages* [online]. 7. 6. 2010 [cit. 2014-08-28]. Dostupné z: http://xnotion.hubpages.com/hub/How-to-Unblock-Facebook.

ZADEMBSKÁ, Marika a Martin ČADRA. 2014. V pavučině sítí. In: *SDRUK* [online]. Ostrava: Sdružení knihoven ČR [cit. 2014-08-28]. Dostupné z: http://www.sdruk.cz/data/xinha/sdruk/2014/zadembska_cadra_prezentace.pdf.

Zapojené organizace. 2017. *Saferinternet CZ* [online]. [cit. 2017-02-10]. Dostupné z: http://www.saferinternet.cz/sid-2017/730-zapojene-organizace.html.

ZAŤKO, Igor. 2014. Zkušenosti s informačním vzděláváním na ZŠ Gorkého v Havířově v předmětu Informatika. In: *SDRUK* [online]. Ostrava: Sdružení knihoven ČR , 24. 4. 2014 [cit. 2014-08-28]. Dostupné z: http://www.sdruk.cz/data/xinha/sdruk/2014/Informacni_vzdelavani_na_ZS_Gorkeho.pdf.

ZAZANI, Eleni. 2013. Lesson plan: Who am I? In: My digital footprint. In: *Birkbeck University of London* [online]. 25. 10. 2013 [cit. 2014-08-28]. Dostupné z: http://eprints.bbk.ac.uk/8667/3/8667.pdf.

ZVONKOVÁ, Lenka. 2009. Lekce děti upozorní na nebezpečí internetu. *Region Valašsko* [online]. 31. 3. 2009 [cit. 2014-08-28]. Dostupné z: http://www.regionvalassko.cz/aktuality_zobraz.php?lang=1&id=198&akt=2552&page=4.

Právní a paraprávní dokumenty (všechny ve znění k 1. 2. 2018)

Antitrust: Commission probes allegations of antitrust violations by Google. 2010. IP/10/1624. 30. 11. 2010. Dostupný z: http://europa.eu/rapid/press-release_IP-10-1624_en.htm?locale=en.

Commission staff working paper impact assessment: Accompanying document to the Proposal for a Council Recommendation on the validation of non-formal and informal learning. 2012. SWD/2012/0252 final. 5. 9. 2012. Dostupný z: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2001:0678:FIN:EN:PDF.

Communication from the Commission of the European communities: Making a European Area of Lifelong Learning a Reality. 2001. Brussel, COM(2001) 678 final. 21. 11. 2001. Dostupné z: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2001:0678:FIN:EN:PDF.

DELORS, Jacques. 1996. Learning: The treasure within: Report to UNESCO of the International Commission on Education for the Twenty-first Century. Dostupné z: http://unesdoc.unesco.org/images/0010/001095/109590eo.pdf.

Dlouhodobý záměr vzdělávání a rozvoje vzdělávací soustavy ČR (2011–2015). 2011. Dostupné z: http://www.vzdelavani2020.cz/images_obsah/dokumenty/knihovna-koncepci/dlouhodoby-zamer-reg/dzcr_2011.pdf.

Federal Trade Commission Decision and Order from Dec. 14, 2011, Docket No. C-4344, File No. 102–3185. Dostupné z: http://www.ftc.gov/sites/default/files/documents/cases/2011/12/111221scanscoutdo.pdf.

Implementace Koncepce rozvoje knihoven v ČR na léta 2017–2020. 2016. Dostupné z: http://files.ukr.knihovna.cz/200000231-e59a2e694a/pril1Implementace.pdf.

Koncepce rozvoje knihoven ČR na léta 2011 – 2015 včetně internetizace knihoven: Knihovny pro EVROPU 2020. 2012. Dostupné z: http://www.mkcr.cz/assets/literatura-a-knihovny/Koncepce_rozvoje_knihoven_2011-2015.pdf.

Koncepce rozvoje knihoven v České republice na léta 2004 – 2010. 2004. Dostupné z: http://knihovnam.nkp.cz/docs/Koncepce04_10.doc.

Metodický pokyn Ministerstva kultury k zajištění výkonu regionálních funkcí knihoven a jejich koordinaci na území České republiky. 2011. Dostupné z: knihovnam.nkp.cz/docs/MetPokynMK05.doc.

Metodika pro hodnocení rozvoje čtenářské gramotnosti. 2015, čj. ČŠIG-2928/15-G2. Dostupné z: http://www.niqes.cz/Niqes/media/Testovani/KE%20STA%c5%bdEN%c3%8d/V%c3%bdstupy%20KA1/%c4%8cG/Metodika-pro-hodnoceni-rozvoje-CG.pdf.

Metodika pro hodnocení rozvoje informační gramotnosti. 2015, čj. ČŠIG-2981/15-G2. Dostupné z: http://www.niqes.cz/Niqes/media/Testovani/KE%20STA%c5%bdEN%c3%8d/V%c3%bdstupy%20KA1/IG/Metodika-pro-hodnoceni-rozvoje-IG.pdf.

Metodika pro hodnocení rozvoje sociální gramotnosti. 2015, čj. ČŠIG-2950/15-G2. Dostupné z: http://www.niqes.cz/Niqes/media/Testovani/KE%20STA%c5%bdEN%c3%8d/V%c3%bdstupy%20KA1/SG/Metodika-pro-hodnoceni-rozvoje-SG.pdf.

Nález Ústavního soudu ze dne 22. 3. 2011, spis. zn. N 52/60 SbNU 625. Dostupné z: http://nalus.usoud.cz/Search/GetText.aspx?sz=Pl-24-10_1.

Příloha č. 1 k Opatření ministryně školství, mládeže a tělovýchovy, kterým se mění Rámcový vzdělávací program pro základní vzdělávání, čj. MSMT-28603/2015. Dostupné z: www.nuv.cz/uploads/RVP_ZV_2016.pdf.

Příloha č. 2 Soubor indikátorů procesu rozvoje informační gramotnosti. 2015. Dostupné z: http://www.niqes.cz/Niqes/media/Testovani/KE%20STA%c5%bdEN%c3%8d/V%c3%bdstupy%20KA1/IG/Priloha-c-2.pdf.

Příloha č. 5 Soubor indikátorů dosažné úrovně informační gramotnosti. 2015. Dostupné z: http://www.niqes.cz/Niqes/media/Testovani/KE%20STA%c5%bdEN%c3%8d/V%c3%bdstupy%20KA1/IG/Priloha-c-5.xls.

Rozsudek Soudního dvora (velkého senátu) ze 13. května 2014, spis. zn. C-131/12. Dostupný z: http://curia.europa.eu/juris/document/document.jsf?text=&docid=152065&doclang=cs.

Směrnice Evropského parlamentu a Rady 2009/136/ES, kterou se mění směrnice 2002/22/ES o univerzální službě a právech uživatelů týkajících se sítí a služeb elektronických komunikací, směrnice 2002/58/ES o zpracování osobních údajů a ochraně soukromí v odvětví elektronických komunikací a nařízení (ES) č. 2006/2004 o spolupráci mezi vnitrostátními orgány příslušnými pro vymáhání dodržování zákonů na ochranu zájmů spotřebitele. Dostupné z: http://eur-lex.europa.eu/legal-content/CS/TXT/HTML/?uri=CELEX:02009L0136-20091219.

Směrnice Evropského parlamentu a Rady 95/46/ES ze dne 24. října 1995 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů. Dostupné z: http://eur-lex.europa.eu/legal-content/CS/TXT/HTML/?uri=CELEX:01995L0046-20031120.

Státní informační politika – cesta k informační společnosti. 1999. Dostupné z: http://www.vlada.cz/cz/clenove-vlady/historie-minulych-vlad/statni-informacni-politika—cesta-k-informacni-spolecnosti—dokument-2089/.

Strategie digitální gramotnosti ČR na období 2015 až 2020. 2015. Dostupné z: https://www.mpsv.cz/files/clanky/21499/Strategie_DG.pdf.

Struktury systémů vzdělávání a odborné přípravy v Evropě: Česká republika 2009/10. 2009. Praha: Ministerstvo školství, mládeže a tělovýchovy [cit. 2014-08-29]. Dostupné z: http://www.msmt.cz/uploads/VKav_200/Eu_CZ_2010/educz_0910.pdf.

Usnesení č. 2/1993 Sb., o vyhlášení Listiny základních práv a svobod jako součásti ústavního pořádku České republiky. Dostupné z: http://portal.gov.cz/app/zakony/zakonPar.jsp?idBiblio=40453.

Zákon č. 101/2000 Sb., o ochraně osobních údajů. Dostupné z: http://portal.gov.cz/app/zakony/zakonPar.jsp?idBiblio=49228.

Zákon č. 121/2000 Sb., o právu autorském, o právech souvisejících s právem autorským a o změně některých zákonů (autorský zákon). Dostupné z: https://portal.gov.cz/app/zakony/zakonPar.jsp?idBiblio=49278.

Zákon č. 257/2001 Sb., o knihovnách a podmínkách provozování veřejných knihovnických a informačních služeb (knihovní zákon). Dostupné z: http://portal.gov.cz/app/zakony/zakonPar.jsp?idBiblio=51517.

Zákon č. 273/2008 Sb., o Policii České republiky. Dostupné z: http://portal.gov.cz/app/zakony/zakonPar.jsp?idBiblio=67272.

Zákon č. 40/2009 Sb., trestní zákoník. Dostupné z: https://portal.gov.cz/app/zakony/zakonPar.jsp?idBiblio=68040.

Zákon č. 561/2004 Sb., o předškolním, základním středním, vyšším odborném a jiném vzdělávání (školský zákon). Dostupné z: http://portal.gov.cz/app/zakony/zakonPar.jsp?idBiblio=58471.

SEZNAM ZKRATEK

AAP	American Academy of Pediatrics
ACRL	Association of College & Research Libraries
AKM	Archivy, knihovny, muzea (konference)
AKVŠ	Asociace knihoven vysokých škol
ANOVA	Analysis of variance
APEK	Asociace pro elektronickou komerci
CILIP	Chartered Institute of Library and Information Professionals
ČIS	Česká informační společnost, o. s.
DS	Digitální stopy
EU	Evropská unie
E-U-R	Evokace – uvědomění – reflexe
FIT	Fluency with Information Technology
HR	Řízení lidských zdrojů
HTTP	Hypertext Transfer Protocol
ICT	Informační a komunikační technologie
IFLA	International Federation of Library Associations
INEBE	Informační nebezpečí (projekt)
IP	Internet Protocol
ISK	Informační studia a knihovnictví
ISTE	International Society for Technology in Education
IT	Informační technologie
IVIG	Odborná komise pro informační vzdělávání a informační gramotnost
IVU SDRUK	Informační vzdělávání uživatelů Sdružení knihoven
K12	Kindergarten – 12 grade
KJM	Knihovna Jiřího Mahena
MKP	Městská knihovna v Praze

MZK	Moravská zemská knihovna
NCBI	Národní centrum bezpečnějšího internetu
NETS	National Educational Technology Standards
NIPOS	Národní informační a poradenské středisko pro kulturu
OS	operační systém
PRVoK	Centrum prevence rizikové virtuální komunikace Pedagogické fakulty Univerzity Palackého v Olomouci
RVP ZV	Rámcový vzdělávací program pro základní vzdělávání
SKIP	Svaz knihovníků a informačních pracovníků České republiky
SSL/TLS	Secure Sockets Layer / Transport Layer Security
ŠVP	Školní vzdělávací program
TOR	The Onion Router

SEZNAM OBRÁZKŮ

SEZNAM TABULEK

SEZNAM GRAFŮ

PŘÍLOHA 1 POUŽITÉ VÝZKUMNÉ NÁSTROJE

Příloha 1.1 Vzdělávání v knihovnách k bezpečnosti na internetu

Představení

Vážené kolegyně a vážení kolegové,
jmenuji se Pavla Kovářová a jsem doktorandka na ÚISK FF UK a odborná pracovnice na KISK FF MU, kde se mj. zabývám informační bezpečností. Ráda bych Vás tímto požádala o spolupráci formou vyplnění krátkého dotazníku, jehož cílem je zmapování vzdělávání na téma bezpečnosti na internetu, především v knihovnách a se zaměřením na děti, ale i souvisejícího širšího kontextu. Výsledky dotazníku poslouží i k přizpůsobení několika plánovaných seminářů pro knihovníky na obdobná témata. Dále budou představeny na mezinárodní konferenci EU Kids Online (http://www2.lse.ac.uk/media@lse/research/EUKidsOnline/Conference.aspx) i v českých odborných periodikách.

Dotazník je složen z 10 otázek. Pokud je u některé možný výběr více odpovědí, budete na toto u ní upozorněni. Vyplnění by Vám nemělo zabrat déle než 10 minut.

Děkuji za spolupráci Pavla Kovářová

1. V jaké jste zaměstnán/a instituci (vyberte nejkonkrétnější možnost)? *
   - školní knihovna
   - akademická knihovna
   - veřejná knihovna, která podle knihovního zákona není specializovaná knihovna
   - jiná knihovna
   - instituce školství mimo školní knihovnu

- instituce veřejné správy
- soukromá firma

2. Organizuje tato instituce vzdělávací aktivity (ne pro zaměstnance samotné instituce)? *
   - ano
   - ne (přejděte na otázku č. 8)

Vzdělávací aktivity v instituci

3. Jaké je obsahové zaměření vzdělávacích aktivit Vaší instituce? (možno více odpovědí)
   - zkvalitnění zpracování informací bez ohledu na jejich zdroj (např. využití softwaru, online nástrojů, informační služby, informační etika, publikační činnost atd.)
   - zkvalitnění práce s tradičními informačními zdroji
   - zkvalitnění práce s elektronickými informačními zdroji
   - kulturní akce
   - jiné (uveďte jedno nejvýznamnější)
4. Víte o tom, že by se někdy některá/některé z nich věnovaly bezpečnosti na internetu? (možno více odpovědí)
   - ano, jako samostatnému tématu (do pole poslední možnosti této otázky uveďte, zda pravidelně/nepravidelně a kolikrát během Vámi stanoveného časového období)
   - ano, v rámci jiných témat je zmiňován aspekt bezpečnosti na internetu (do pole poslední možnosti této otázky uveďte, zda pravidelně/nepravidelně a kolikrát během Vámi stanoveného časového období)
   - ne, ale podle mého názoru by měly
   - ne, podle mne to nemá smysl
   - pokud ano, jak často
5. Považujete děti za jednu z klíčových primárních cílových skupin vzdělávacích aktivit ve Vaší instituci (tj. vzdělávací akce pořádáte přímo pro ně a to minimálně 6 v roce)?
   - ano
   - ne (přejděte na otázku č. 8)

Vzdělávací aktivity pro děti

6. Jaké je obsahové zaměření vzdělávacích aktivit orientovaných na děti jako primární cílovou skupinu? (možno více odpovědí)
   - zkvalitnění zpracování informací bez ohledu na jejich zdroj (např. využití softwaru, online nástrojů, informační služby, informační etika, publikační činnost atd.)
   - zkvalitnění práce s tradičními informačními zdroji

- zkvalitnění práce s elektronickými informačními zdroji
- čtenářství
- kulturní akce
- doplnění výuky ve škole bez zaměření na aktivity knihovny (např. kreslení, fyzikální experimenty...)
- jiné (uveďte jedno nejvýznamnější)

7. Víte o tom, že by se někdy některá/některé z nich věnovaly bezpečnosti na internetu? (možno více odpovědí)
   - ano, jako samostatnému tématu (do pole poslední možnosti této otázky uveďte, zda pravidelně/nepravidelně a kolikrát během Vámi stanoveného časového období)
   - ano, v rámci jiných témat je zmiňován aspekt bezpečnosti na internetu (do pole poslední možnosti této otázky uveďte, zda pravidelně/nepravidelně a kolikrát během Vámi stanoveného časového období)
   - ne, ale podle mého názoru by měly
   - ne, podle mne to nemá smysl
   - pokud ano, jak často

Doplňující informace

8. Myslíte si, že by se knihovny měly v rámci svých vzdělávacích aktivit věnovat bezpečnosti dětí na internetu? *
   - ano
   - ne
9. Jaké znáte online vzdělávací projekty k tématu bezpečnosti dětí na internetu (nejsou myšleny jednorázové kampaně)? (možno více odpovědí) *
   - Bezpecne-online.cz
   - E-Bezpečí
   - E-Nebezpečí
   - Internet Hotline
   - Nebuď oběť
   - Pomoconline.cz
   - Protišikaně.cz
   - Saferinternet CZ
   - Žádný
   - Jiný (uveďte jeden nejvýznamnější)
10. Chcete k tématům v dotazníku něco dodat? Pokud chcete být informováni o umístění publikovaných výsledků tohoto dotazníku, uveďte kontaktní e-mailovou adresu.

    Vaše odpovědi byly úspěšně odeslány, děkuji za vyplnění dotazníku.

Příloha 1.2 Rozšiřující deskripce vzdělávání

Dobrý den, jsme projekt iNeBe – informační (ne)Bezpečí, podporovaný Kabinetem informačních studií a knihovnictví Masarykovy univerzity v Brně. Chtěli bychom Vás požádat o vyplnění dotazníku zaměřeného na tématiku informační bezpečnosti, který nám pomůže zjistit, jaký zájem mají knihovny o vzdělávání v této oblasti. Vyplnění dotazníku Vám zabere přibližně 8 minut. V případě, že máte jakýkoliv dotaz nebo zájem o spolupráci, pište na e-mail: inebe@seznam.cz. Děkujeme za Váš čas!

1. Prosím uveďte název města, ve kterém se nachází Vaše knihovna: *
2. Zde prosím vyplňte název Vaší knihovny: *
3. Organizuje Vaše knihovna vzdělávací aktivity pro veřejnost? *
   - Ano
   - Ne
   - Nevím
4. Je některá z těchto aktivit zaměřená na počítačovou gramotnost nebo práci s počítačem/internetem? *
   - Ano
   - Ne
   - Nevím
5. Věnujete se v rámci některé vzdělávací aktivity problematice informační bezpečnosti? *
   - Ano
   - Ne
   - Nevím
6. Myslíte si, že je důležité vzdělávání v oblasti informační bezpečnosti? *
   - Určitě ano
   - Spíše ano
   - Spíše ne
   - Určitě ne
   - Nevím / nemohu odpovědět
7. Chtěli byste se vy osobně vzdělávat v oblasti informační bezpečnosti? *
   - Určitě ano
   - Spíše ano
   - Spíše ne
   - Určitě ne
   - Nevím
8. Měli byste zájem o přednášku či kurz na téma informační bezpečnosti ve Vaší knihovně?*

- Určitě ano
- Spíše ano
- Spíše ne
- Určitě ne
- Nevím / nemohu odpovědět

9. Pokud by vám byla nabídnuta možnost vzdělávat se v problematice informační bezpečnosti, jaká forma výuky by Vám vyhovovala?

	Vyhovovala	Spíše vyhovovala	Spíše nevyhovovala	Nevyhovovala
E-learningový kurz *				
Klasické přednáškové lekce v rozsahu 5-10 lekcí *				
Jednorázový intenzivní workshop ve Vaší knihovně *				
Výuka ve virtuálním světě, např. SecondLife *				
Samostudium materiálů *				
Individuální školení s lektorem (max. 3 osoby) *				

10. Byli byste ochotni na výuku dojíždět? *

	Ano	Ne
Praha *		
Brno *		
nejbližší krajská knihovna *		

11. Kolik času týdně byste byli ochotni věnovat takovému kurzu? *
    - Maximálně hodinu
    - 1-2 hodiny
    - 2-3 hodiny
    - 3-4 hodiny
    - 4 hodiny a více
12. Vyberte témata, která by Vás zajímala v kurzu: * Můžete vybrat více možností
    - problematika sociálních sítí
    - nevyžádané zprávy (spam)
    - malware (viry, červy, trojské koně...)
    - zneužití osobních informací (vč. kyberšikany)
    - autorské právo
    - pornografie
    - nevhodný a nelegální obsah (agresivita a násilí)
    - specifičtí uživatelé (děti, firmy, stát...)

- šifrování (hesla, elektronický podpis...)
- prevence (jak svá data chránit)
- jiné (napište prosím jaké)

13. Měli byste zájem o metodické materiály, které by vám umožnily orientaci v problematice tak, abyste sami mohli ve Vaší knihovně přednášet na téma informační bezpečnosti? *
    - Ano
    - Ne
14. Jakou formu výukových materiálů preferujete? *
    - podcasty (zvukové nahrávky)
    - teoretické texty
    - brožurky/letáčky
    - videa
    - zábavná forma (hry, komiksy, křížovky...)
    - teorie s možností ověření znalostí (test)
    - jiné (napište prosím jaké)
15. V případě, že máte zájem o spolupráci, výukové nebo propagační materiály, vyplňte prosím Vaši e-mailovou adresu:
16. Místo pro Vaše vyjádření nebo připomínky, a to ať už k dotazníku nebo problematice:

    Děkujeme za Váš čas strávený vyplňováním dotazníku!

Příloha 1.3 Didaktické testování

Dobrý den,
prosím o vyplnění dotazníku, jehož cílem je porovnat znalosti studentů oboru informační studia a knihovnictví a knihovníků o problematice digitálních stop. Výsledky budou použity pro tvorbu dizertační práce.
Vzhledem k cíli šetření prosím netipujte odpovědi, ale vyberte variantu „nevím“, pokud danou znalost nemáte. Vyplnění může být časově náročnější (přibližně 20 minut), výsledky ale budou o to přínosnější nejen pro publikování, ale také pro to, jaké vzdělávací aktivity Vám budou v budoucnu v souvisejících tématech nabízeny. Proto věřím, že vynaložený čas bude prospěšný i pro Vás.
Velmi děkuji za ochotu se tímto šetřením zabývat.
Pavla Kovářová
Kabinet informačních studií a knihovnictví, FF MU
Ústav informačních studií a knihovnictví, FF UK

1. Co jsou digitální stopy? (více možných odpovědí)*
   - *Historie vyhledávání, záznamy e-komerce (registrace, objednávky)*
   - *Informace s vypovídací hodnotou, uložená či přenášená v digitální podobě, tedy dokumenty, „otisky“ činností technologického zařízení pracujícího s daty, metadata obsahující informace o daném souboru apod.*
   - *Informace zpřístupněné vědomým nahráváním a sdílením samotným uživatelem i zpřístupněné online bez záměrného přičinění uživatele*
   - *Jakákoliv digitální data, která mohou prokázat spáchání trestného činu nebo mohou poskytnout vazbu mezi trestným činem a jeho obětí či jeho pachatelem*
   - *Profily, které reklamním společnostem umožňují doručovat personifikovaná reklamní sdělení, vytvořené nejčastěji na základě sledování klíčových slov zadávaných do vyhledávačů a sledování pohybu napříč navštívenými webovými stránkami*
   - *Soubor informací, které za sebou uživatel zanechává (ať již vědomě, či nevědomě) během využití informačních technologií*
   - *Záznamy komunikace přes mobil, tablet i GPS a podobná zařízení*
   - Nevím
2. Ve které oblasti si dokážete představit legální využití a ve které nelegální zneužití digitálních stop?*

	využití	**zneužití**	**bez vlivu**	**nevím**
hacking		X		
kriminalistika	X			
management (kontrola a monitoring)	X	X		
marketing	X	X		
mezilidská komunikace, např. zprávy i zeď na Facebooku	X	X		

	využití	zneužití	bez vlivu	nevím
personalistika	X	X		
správa informačních systémů a sítí	X	X		
státní správa	X			

3. Jak silně zneužitelné jsou informace, které je za určitých okolností možné zjistit z digitálních stop? (označte jednu možnost pro každý řádek)* (1 silně zneužitelné – 5 samostatně nezneužitelné)

	1	2	3	4	5	Nevím
cestovní plány		X				
citlivé údaje s potenciálem diskriminace (náboženství, přestupky proti zákonu...)	X					
číselné identifikátory a autentizační údaje (rodné číslo, uživatelské jméno a heslo...)	X					
dokumenty k osobě (vlastní i oblíbené cizí výtvory, fotky s ním...)			X			
identifikační údaje pro stát či firmy (jméno, příjmení, datum a místo narození, adresa trvalého pobytu...)	X					
informace o denní rutině (pravidelný dopravní spoj, zájmová sdružení, rozvrh...)		X				
navštívené webové stránky			X			
osobní informace možná za hranicí soukromí (podrobnosti přátelství a partnerství, nahé fotky v kojeneckém věku...)		X				
podrobnosti o movitém či nemovitém majetku			X			
povolání					X	
přibližná výše platu					X	
telefonní číslo, e-mailová adresa			X			
věk				X		
zájmy (koníčky, zdroje, názory...)			X			
zaměstnavatel, vzdělání				X		

4. Co je výsledkem deaktivace účtu na Facebooku? Vyberte jednu nejpřesnější odpověď.*
   - Informace vyprodukované uživatelem, který účet deaktivuje, budou odstraněny
   - *Účet bude neaktivní, ale vše zaznamenané na Facebooku zůstane, dokud nebudou podniknuty komplexnější kroky ke smazání*
   - Účet nebude přístupný, dokud ho uživatel znovu neaktivuje přes daný postup (např. potvrzení e-mailem, když byl účet deaktivován kvůli prozrazení přístupových údajů)
   - Všechny informace spojitelné s uživatelem budou odstraněny

- Nevím

5. Jaké nástroje jsou využívány pro automatický pasivní (bez uživatelovy aktivity) sběr digitálních stop? (více správných odpovědí)*
   - CAPTCHA
   - *cookies*
   - crawler
   - *historie v prohlížeči*
   - hotspot
   - link farma
   - PageRank
   - *plugin v prohlížeči*
   - *sociální síť*
   - *vyhledavač*
   - *webbug (pixelový tag)*
   - jiný (doplňte)
6. Zhodnoťte upotřebení digitálních stop v problémech uvedených v tabulce. Pokud je pro realizaci digitální stopu nezbytné využít, zatrhněte pole „vyžaduje". Pokud digitální stopa jen přispívá k úspěšnosti, ale není nezbytná, zatrhněte pole „podporuje". Pokud problém s digitální stopou nepracuje, zatrhněte „bez vlivu". Pokud pojem neznáte, zatrhněte „nevím". (označte jednu či více možností)*

	Vyžaduje	**Podporuje**	**Bez vlivu**	**Nevím**
Krádež identity	X			
Kyberšikana		X		
Kyberstalking	X			
Kybergrooming	X			
Sexting	X			
Vydírání	X			
Malware		X		
Spam			X	
Scam		X		
Hoax			X	
Phishing		X		
Prolamování hesel		X		

7. Jaká varování mohu předznamenávat to, že se Vás někdo snaží zmanipulovat? (více možných odpovědí)*
   - *„ohánění se" autoritou (nadřízený, známá organizace...) a znalostí bez kontextu*
   - *časový limit, naléhavost*
   - *formální (jazykové, typografické) chyby*
   - *napodobení očekávaného vzhledu (např. webu, adresy, vizuálu...)*

- *nebezpečí (finanční či jiné)*
- *nemožnost či omezení ověření*
- *symboly pro zvýšení pozornosti (velká písmena, vykřičníky, $$$...)*
- *útok na emoce (vina, soucit, ego přes flirtování či lichocení...)*
- *vybuzení zájmu (zvědavost, finanční či jiný zisk s malými náklady)*
- nic z uvedeného
- jiné

8. Jaká preventivní opatření ve vlastním chování proti vytváření a využití digitálních stop znáte a která používáte?*

	znám a používám	**znám, ale nepoužívám**	**neznám**
Bezpečné používání silných hesel			
Čtení certifikátů, licenčních podmínek, varování, potvrzení...			
Egosurfing (vyhledání informací o konkrétním člověku)			
Nedůvěra k deklarované identitě (uvědomění si možností změny identity, např. spoofing, falešné údaje v registraci...)			
Nezjednodušování si práce na úkor bezpečnosti (např. pamatování hesel v prohlížeči)			
Prověřování aplikacemi typu antivir všeho staženého z internetu (soubory, e-maily...)			
Při neobvyklé žádosti (o informace, činnost...) ověřit oprávněnost			
Sledování aktuálních problémů a bezpečnostních řešení			
Šifrování (e-mailů, spojení...) či elektronický podpis, kde je to možné			
Uvážlivá práce s uživatelskými účty, především v operačním systému			
Uvážlivé publikování fotografií, videí a osobních údajů			
Vhodné nastavení soukromí u všech služeb, zejména sociálních sítí (např. nastavení aktualizací)			
Vhodné nastavení prohlížeče (např. správa cookies)			
Nejsou navštěvovány weby a stahovány soubory s nevhodným a nelegálním obsahem			
Využití více přihlašovacích jmen (přezdívek)			
Zamýšlení se nad možnými negativními i pozitivními důsledky a jejich zhodnocení před aktivitou			

9. Co znamená anonymní mód (InPrivate apod.) v prohlížeči? Vyberte jednu nejpřesnější odpověď.*
   - Nejsou ukládány nikam žádné informace o uživateli a zařízení, které využívá
   - Nejsou ukládány informace spojitelné s konkrétním uživatelem, ale jen obecné (např. preferovaný jazyk)
   - *Jsou ukládány informace jako při běžném použití prohlížeče, ale po ukončení jsou smazány záznamy (historie, cookies apod.), kromě stažených souborů*
   - Nevím
10. Jakou anonymizaci umožňují webové proxy servery? Vyberte jednu nejpřesnější odpověď.*
   - Úplné skrytí veškerých technických informací o uživatelově zařízení, díky čemuž webové stránky mohou zjistit jen technické informace o proxy serveru
   - Úplné skrytí IP adresy za adresu proxy serveru, o zařízení uživatele mohou weby zjistit jen obecné technické informace (např. rozlišení obrazovky pro správné zobrazení)
   - *Skrytí IP adresy, které je ale neúčinné, pokud nejsou blokovány HTTP hlavičky nebo není důvěryhodný správce*
   - Nevím
11. Jak fungují služby založené na onion routingu (např. TOR, JonDonym)? Vyberte jednu nejpřesnější odpověď.*
   - *IP adresa a další údaje jsou skryty za údaji několika proxy serverů, navíc lze přenos šifrovat a použít pluginy pro šifrovaný přenos a blokování Flash a Java skriptů*
   - Dostatečná anonymizace je zajištěna skrytím veškerých technických informací o uživatelově zařízení několikanásobným zašifrováním (jako vrstvy cibule), jiné funkce by službu nevhodně zpomalovaly
   - Různé pakety jsou přes různé uzly sítě (rating), proto žádný uzel nezíská kompletní informaci o uživatelově zařízení či osobě
   - Nevím
12. Co se stane při zablokování cookies s úmyslem zamezit vzniku digitální stopy? Vyberte jednu nejpřesnější odpověď.*
   - *Některé služby nebudou správně fungovat, zejména pokud jsou spojeny s uživatelským účtem.*
   - Služby nebudou moci shromažďovat žádné informace o uživateli, takže mu nebudou moci zasílat cílenou reklamu.
   - Nezobrazí se některé části stránky (např. interaktivní, Flash videa apod.).
   - Zvýší se bezpečnost uživatele, ale použití internetu to neovlivní, je to pro něj transparentní opatření.
   - Nevím.
13. Jaké specializované nástroje proti vytváření a využití digitálních stop znáte a které používáte? (označte jednu možnost pro každý řádek)*

	znám a používám	znám, ale nepoužívám	neznám
Anonymizér			
Antiphishingový nástroj			
Antirootkit			
Antispam			
Antispyware			
Antivirus			
Filtry obsahu			
Firewall			

14. Co jsou osobní údaje, které chrání český zákon a jeho evropské obdoby díky směrnici EU? Vyberte jednu nejpřesnější odpověď.*
    - *Informace, které jednoznačně identifikují konkrétní fyzickou osobu ve fyzickém prostředí (např. jméno, příjmení, adresa trvalého pobytu, datum narození)*
    - Informace, které jednoznačně identifikují konkrétní osobu ve fyzickém i v elektronickém prostředí (např. přístupové údaje)
    - Informace, které jednoznačně identifikují konkrétní fyzickou nebo právnickou osobu (např. IČO, vedení organizace)
    - Informace, které chce konkrétní člověk uchovat v soukromí (např. společenské vztahy, sociální vazby)
    - Nevím
15. Když někdo přinese počítač na opravu, může se technik legálně podívat na data v počítači? Vyberte jednu nejpřesnější odpověď.*
    - Ano, pokud je jeho úkolem i zálohovat data
    - Ano, protože co mu zákon nezakazuje, to má povoleno a toto mu zákon nezakazuje
    - Ne, pokud by musel nějak neoprávněně proniknout do systému (uhodnout heslo, využít bezpečnostní mezery informačního systému atp.); v opačném případě ano
    - Ne, ale musí mu to zákazník výslovně zakázat
    - *Ne, jde o narušení soukromí zákazníků a to není legálně možné*
    - Nevím
16. Jste:*
    - muž
    - žena
17. V jaké fázi vysokoškolského vzdělávání v oboru informační studia a knihovnictví se nacházíte? (jedna odpověď)*
    - studuji bakalářský stupeň
    - studuji navazující magisterský stupeň
    - studuji doktorský stupeň

- studuji jiný obor než informační studia a knihovnictví
- mám již dostudován obor informační studia a knihovnictví a pracuji nebo chci pracovat v knihovně
- mám již dostudován jiný obor než informační studia a knihovnictví a pracuji nebo chci pracovat v knihovně
- jiné

18. Jak byste popsal/a svůj zájem o téma digitálních stop? Vyberte jednu nejpřesnější odpověď.*
    - vůbec mne to nezajímá a myslím, že nemá smysl tomu věnovat čas
    - nezajímá mne to, ale myslím, že má smysl v této oblasti vzdělávat
    - zajímá mne to jako běžného uživatele
    - zajímá mne to a chci se této problematice věnovat hlouběji než běžný uživatel nebo o ní chci vzdělávat ostatní
19. Přiřaďte rozsah vzdělávání v tématu digitálních stop (nebo obecněji informační bezpečnosti), který jste absolvoval/a. (označte ve vybraném řádku jednu či více možností)*

	Žádné vzdělání	**1–3 přednášky**	**Více přednášek**	**Samostatný předmět či seminář**
před vysokou školou				
na vysoké škole mimo obor ISK				
na vysoké škole v rámci oboru ISK				
po vysoké škole mimo akce určené pro knihovníky				
po vysoké škole v rámci akce určené pro knihovníky				

20. Přiřaďte varianty vyjadřující Váš názor, jak by se mělo vzdělávat o digitálních stopách na ZŠ, VŠ a v knihovně. Vzdělávat by se...
    a) nemělo.
    b) mělo několika přednáškami nezaměřenými na informační bezpečnost, ale souvisejícími.
    c) mělo několika přednáškami o digitálních stopách v předmětech/vzdělávacích cyklech nezaměřených na informační bezpečnost.
    d) mělo celým předmětem zaměřeným na informační bezpečnost.*

Základní škola _____
Vysoká škola _____
Knihovna _____

Příloha 1.4 Rozhovory v akčním výzkumu

Poučený souhlas

Tímto uděluji PhDr. Pavle Kovářové, r. č. , poučený souhlas k neanonymnímu publikování autorizovaných výsledků rozhovoru v její disertační práci. Cílem publikovaných informací bude popsat názory a argumenty k vzdělávání v knihovnách o tématu digitálních stop a jejich zneužívání s důrazem na spolupráci škol a knihoven při tomto vzdělávání. Ke zpracování dojde na základě polostrukturovaného rozhovoru zaznamenaného ve formě videa pro potřeby vyhodnocení zjištění. Videozáznamy nebudou publikovány, po zpracování budou uchovány jen pro potřeby pozdějšího přezkoumání.

Jméno:

Pozice pro výzkum:

Podpis:

Seznam otázek pro rozhovor: Aktuální pohled na knihovnu a informační bezpečnost

1. Jak byste definoval/a digitální stopy a jaké problémy jsou s nimi spojeny?
2. Má podle Vás smysl vzdělávat v oblasti digitálních stop a (proti) jejich zneužití?

3. Jak byste popsal/a svůj aktuální názor na to, jestli knihovny mají vzdělávat v tématu digitálních stop a (proti) jejich zneužití?
4. Jak se na spojení vzdělávání o digitálních stopách v knihovnách podle Vás dívají obecně knihovníci/školy/veřejnost či její určité části?

5. Jaká subtémata by se měla při tomto vzdělávání v knihovnách řešit?
6. Pro koho by měla být nabízena?
7. A jakou formou?
8. Při srovnání s jinými tématy, co by měla knihovna upřednostnit (knihy X internet; témata v rámci internetu; v subtématech digitálních stop)?

9. Dokážete si Vy osobně představit, že by se toto téma řešilo v každé knihovně?
10. Co by pro to muselo být zajištěno?
11. Proč myslíte, že dnešní aktivní knihovníci jsou či nejsou připraveni vzdělávat v této problematice?
12. Vzdělávají podle Vás střední, vyšší a vysoké školy budoucí knihovníky, aby toto téma mohli řešit?
13. Co by tyto školy měly dělat, aby to jejich absolventi mohli řešit?
14. Co by měli absolventi pro to znát a jak hluboce?

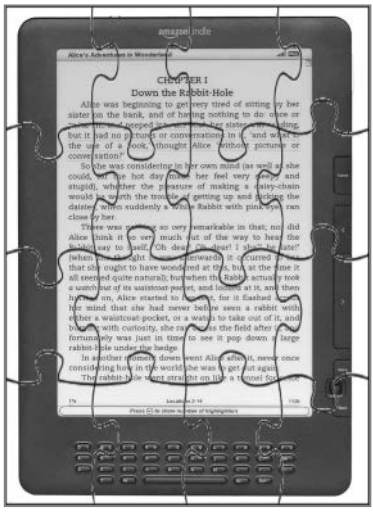
15. Jak jste dříve pohlížel/a na to, že by knihovny vzdělávaly v problematice digitálních stop?
16. Kdy a čím se to měnilo?
17. Jakou jste měl/a představu o možnosti lekcí a jejich reálnosti?
18. Bylo nějak téma digitálních stop řešeno dřív v nějaké lekci knihovny?
19. Jak to vypadalo?
20. Jak byste popsala stav před lekcí, tj. do jakého prostředí byla implementována, co mohlo ovlivnit její realizaci?
21. Co podle Vás přesvědčilo knihovnu pustit se do realizace lekce?
22. A co přesvědčilo školu (paní učitelky)?

23. Co si myslíte o uskutečněné lekci?
24. Změnila nějak právě ona Vaše názory? V čem?
25. Mělo by se podle Vás něco v uskutečněné lekci změnit?
26. Jaké pozitivní či negativní výsledky podle Vás má a na koho?
27. Myslíte, že je rozšiřitelná na další prostředí (školy, knihovny, věk cílové skupiny...)?
28. Na jaká a za jakých podmínek?
29. Co si myslíte, že si z ní děti odnesly?
30. Myslíte si, že by se na ni mělo navázat? Jak?

PŘÍLOHA 2 UKÁZKY MATERIÁLŮ V NAVRŽENÉ KONCEPCI

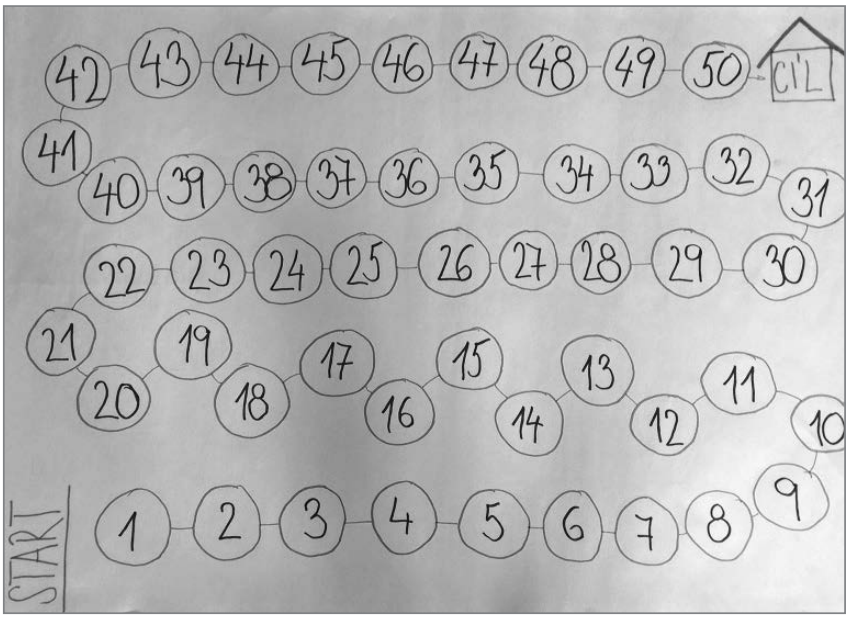
Všechny materiály v aktuální podobě jsou dostupné ve sdílené složce na Google Drive https://goo.gl/bHjGfU. Přístup bude udělen na vyžádání. Uživatelé těchto materiálů, kteří si přístup vyžádali, mohou být osloveni pro zpětnou vazbu na řešenou koncepci i dílčí materiály.

Příloha 2.1 Typy zařízení



Obrázek 4 Puzzle a pracovní list Vlastnosti počítače

Příloha 2.2 Desatero bezpečného internetu



Obrázek 5 Herní plán Člověče, nezlob se

Základní otázky

1. Může ti poslat e-mail nebo SMS člověk, kterého neznáš?
2. Poznáš, kolik let je tvému internetovému kamarádovi, se kterým ses seznámil při hraní na internetu?
3. Poznáš, jestli ti tvůj internetový kamarád říká vždycky pravdu, nebo lže?
4. Je v pořádku, když svému internetovému kamarádovi řekneš adresu, kde bydlíš?
5. Je v pořádku, když svému internetovému kamarádovi řekneš adresu, kam chodíš do školy?
6. Když máš třeba ve hře nebo jinde na internetu svou fotku, co na ní může být, aby to bylo bezpečné?
7. Když chceš svému internetovému kamarádovi o sobě něco říct, co nesmíš říct, aby to bylo bezpečné?
8. Když by ti chtěl ublížit někdo, kdo má tvou fotku, co by s ní mohl udělat?
9. Komu můžeš říct své heslo k počítačové hře?
10. Když ti někdo pošle zprávu, kde ti nadává, měl bys mu na to odpovědět, že to není správné dělat?

11. Když ti někdo pošle zprávu, kde ti nadává, měl bys mu odpovědět a nadávat mu ještě víc?
12. Když ti někdo pošle zprávu, kde ti nadává, měl bys to říct mámě, tátovi, paní učitelce nebo jinému dospělému?
13. Když ti někdo pošle zprávu, kde ti nadává, může máma nebo táta něco v počítači nastavit, aby ti už žádná zpráva od toho člověka nepřišla?
14. Když ti někdo pošle hodně sprostou zprávu, video nebo obrázek, mohou to tvoji rodiče řešit s policií?
15. Když se chceš potkat s někým, koho znáš jen z internetu, je to bezpečné?
16. Když potkáš cizího člověka, který chce, abys s ním šel někam, protože nezná cestu, můžeš s ním jít?
17. Co bys měl udělat, když ti najednou při hraní on-line hry vyskočí sprostý obrázek?
18. Když náhodou při prohlížení videí na internetu narazíš na nějaké, co tě vydělsí, co bys měl udělat?
19. Vyjmenuj tři typy informací, které můžeš hledat na internetu.
20. Jaké informace bys neměl hledat na internetu, i když tam jsou, protože se pro tebe nehodí?
21. Když na internetu vidíš nějaké opravdu sprosté video nebo obrázek, mohou to tvoji rodiče řešit s policií?
22. Je bezpečné podívat se na přílohu e-mailu od někoho, koho neznáš?
23. Jak se chová počítač nakažený virem?
24. Když je počítač nakažený virem, může to tvůj táta nebo máma vyléčit?
25. Můžeš na internetu napsat něco, co není pravda?
26. Je všechno, co najdeš napsané na internetu, pravda?
27. Když najdeš na internetu nebo ti někdo pošle fotku, mohl ji před tím někdo změnit, takže neukazuje to, co se doopravdy stalo?
28. Když ti někdo, kdo je na tebe sprostý, pošle zprávu, měl bys mu odpovědět?
29. Když ti někdo, koho znáš jen proto, že hrajete stejnou počítačovou hru, pošle zprávu, měl bys mu odpovědět?
30. Když si máma nebo táta neví rady, jak ti na internetu pomoct, kdo může pomoct jim?

Doplňkové otázky

1. Když se s někým na internetu nechceš bavit, ale on ti pořád píše, co bys měl udělat?
2. Když ti někdo, koho neznáš, pošle zprávu, měl bys mu odpovědět?
3. Když najdeš na internetu nebo ti někdo pošle video, mohl ho před tím někdo změnit, takže neukazuje to, co se doopravdy stalo?
4. Když si nejsi jistý tím, co je na internetu napsané, jak zjistíš, jestli je to pravda?
5. Co to je e-mail?

6. Když je v e-mailu příloha, co v ní může být?
7. Když na internetu narazíš na video nebo obrázek, které tě vyděsí, může máma nebo táta něco v počítači nastavit, aby se ti to stejné už neukázalo?
8. Když na internetu narazíš na video nebo obrázek, které tě vyděsí, může máma nebo táta něco v počítači nastavit, aby se ti podobné video nebo obrázek už neukázaly?
9. Co bys měl udělat, když ti při prohlížení videí na internetu s kamarádem řekne ten kamarád, že se bojí? Třeba když se díváte na videa s vlaky a mezi nimi je strašná nehoda, kde je plno lidí mrtvých a od krve.
10. Když se opravdu chceš potkat s někým, koho znáš jen z internetu, a řekneš to jen svému kamarádovi, je to v pořádku?
11. Když se opravdu chceš potkat s někým, koho znáš jen z internetu, co bys měl dělat?
12. Když se ti na internetu někdo hodně snaží ublížit, třeba když ti slibuje, že ti ublíží, až tě potká, mohou to tvoji rodiče řešit s policií?
13. Kam si můžeš napsat své heslo k počítačové hře, e-mailu nebo k telefonu?
14. Co třeba ti může udělat někdo, kdo zná tvoje heslo k e-mailu nebo k telefonu?
15. Myslíš, že se na tebe může tvůj nejlepší kamarád někdy rozzlobit tak, že by ti chtěl udělat něco nepěkného?
16. Komu můžeš říct své heslo k e-mailu nebo k telefonu?
17. Když chceš svému internetovému kamarádovi o sobě něco říct, co můžeš říct, aby to bylo bezpečné?
18. Je v pořádku, když svému internetovému kamarádovi pošleš svou fotku?
19. Je v pořádku, když svému internetovému kamarádovi řekneš svoje telefonní číslo?
20. Poznáš, jestli je tvůj internetový kamarád kluk nebo holka?

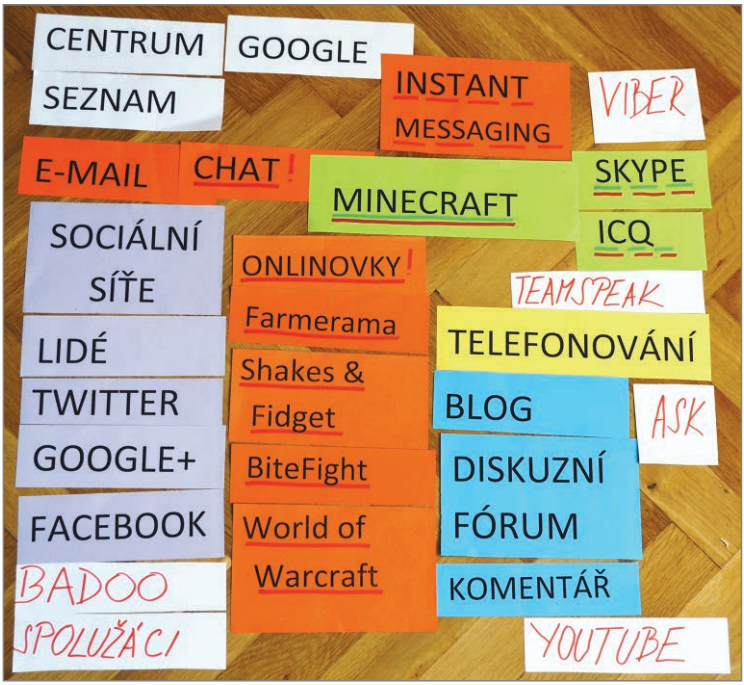
Obrázek 6 Komiks pro reflexi desatera bezpečného internetu

Příloha 2.3 Digitální stopy v síti

Obrázek 7 Komiks pro scénky

Obrázek 8 Časová kapsle

Příloha 2.4 Kdo je za monitorem?



Obrázek 9 Připravené názvy komunikačních služeb

Moje číslo:
Moje jméno:

Na druhé straně:

	Jméno	Body
A		
B		
C		
D		
E		
F		
G		
H		
I		
J		
K		
L		
	Celkem odhaleno spolužáků	
	Minusové body za odhalení	
	Celkem	

Moje písmeno:
Moje jméno:

Na druhé straně:

	Jméno	Body
1		
2		
3		
4		
5		
6		
7		
8		
9		
10		
11		
12		
	Celkem odhaleno spolužáků	
	Minusové body za odhalení	
	Celkem	

Obrázek 10 Tabulka zjištěných identit

Když se mě někdo, koho znám jen online, zeptá: ...

Co dělá tvůj tatínek?
Co máš na sobě?
Co rád (ráda) posloucháš za hudbu?
Dáš si mne do přátel na Facebooku?
Chodíš na nějaké kroužky?
Jak vypadáš?
Jaká je tvoje oblíbená barva?
Jaké je tvoje číslo na mobil?
Jakou máš e-mailovou adresu?
Jakou onlinovku teď hraješ?
Jsi doma sám (sama)?
Jsi kluk nebo holka?
Kam chodíš do školy?
Kam chodíš na kroužky?
Kde bydlíš?
Kde máš počítač?
Kolik máš sourozenců?
Máš doma nějaké zvíře?
Nechceš se potkat?
Pošleš mi svou fotku?

http://us.123rf.com/400wm/400/400/candyman/candyman0706/candyman070600089/1158082-do-not-speak.jpg

… nepovím mu to.

http://static5.depositphotos.com/1002927/449/i/450/dep_4490852-Communication-Problem.jpg

… tak mu to řeknu.

Obrázek 11 Reakce na dotazy od internetového kamaráda

Příloha 2.5 Hodnocení informací

Kresli	Ukaž bez mluvení	Vysvětli bez hledaného slova
		
Mobilní telefon	Šikana	Video

Obrázek 12 Zadání pro rychlé špióny

Závislost na informačních technologiích

Webová stránka Online adiktologická poradna (http://poradna.adiktologie.cz/)

Jaké tři závislosti na internetu jsou nejčastější?	
Jak může vypadat špatný vliv závislost na internetu na váš život?	
Kdy jsou lidé nejvíc ohrožení závislostí na internetu?	
Když se chce někdo zbavit závislosti na internetu, musí ho přestat do konce života používat?	
Jak jste našli správné místo s odpověďmi?	
Kde jste našli, jak je stránka stará a kdo ji napsal?	
Rozumíte většině vět?	
Vypadá stránka profesionálně?	
Snaží se autor uvádět různé názory na téma?	
Je jasné, odkud autor vzal to, co je napsané?	

Obrázek 13 Otázky k analýze článků

Příloha 2.6 Mnoholičný lektvar

Moje číslo:
Moje jméno:

Na druhé straně:

	Uváděné jméno	Pravda √	Lež ×	Body
A				
B				
C				
D				
E				
F				
G				
H				
I				
J				
K				
L				
M				
N				
O				
P				
Celkem odhaleno spolužáků				
Minusové body za odhalení				
Celkem				

Moje písmeno:
Moje jméno:

Na druhé straně:

	Uváděné jméno	Pravda √	Lež ×	Body
1				
2				
3				
4				
5				
6				
7				
8				
9				
10				
11				
12				
13				
14				
15				
16				
Celkem odhaleno spolužáků				
Minusové body za odhalení				
Celkem				

Obrázek 14 Tabulka pravosti identit

Bezpečná hesla

Typy útoků na hesla

Typ útoku	**Rychlost**	**Přibližná úspěšnost**
Útok uhodnutím (přenesením)	Minuty	30%
Slovníkový útok	Hodiny	70%
Útok hrubou silou	Až tisíce let	100%

Délka prolomení hesla (testování 100 hesel za sekundu, s ohledem na pravděpodobnost zjištění v 1. polovině obvykle interval dělen dvěma)

Počet znaků	**4**	**5**	**6**	**7**	**8**
0-9	2 minuty	16 minut	3 hodiny	1 den	11 dní
0-9, a-z	5 hodin	7 dní	8 měsíců	25 let	900 let
0-9, a-z, A-Z	2 dny	3 měsíce	18 let	1 000 let	70 000 let
0-9, a-z, A-Z, @*!	6 dní	1 rok	120 let	10 000 let	800 000 let

Formát bezpečného hesla

- více než 8 znaků, ideálně 12
- velká i malá písmena, číslice a speciální znaky (např. *+)
- nerozeznatelné smysluplné slovo (ani s vloženým písmenem či zvláštním znakem)

- není posloupností (např. 123456 nebo „asdfgh“ - písmena vedle sebe na klávesnici)

Bezpečné používání hesla

- žádná shoda se zjistitelnou informací (např. datum narození, jméno domácího mazlíčka, ani shoda s přihlašovacím jménem)
- neopakují se v různých službách
- pravidelně měněno, na důležitých místech do 90 dní, na běžných do půl roku
- nikomu neprozrazovat (ani nejlepšímu kamarádovi, stejně jako nepůjčíte kartáček na zuby), nezapisovat

Automatizace správy hesel

- správce hesel: Sticky Password, Password Depot, Password Corral, KeyWallet, Aha Password, Správce hesel, lastpass, a další
- náročnost hesla podle významu služby
- stejný postup, jiné heslo, např. Toto je moje heslo, které mám na Facebooku v lednu. => „Tjmh,kmnFv1.“ (první písmeno z každého slova, ponechána čárka a tečka ve větě, leden jako první měsíc nahrazen číslicí 1)

Kontrola bezpečnosti hesla

- Test Your Password (http://www.testyourpassword.com/) – v angličtině, ale velmi jednoduché, heslo se zadá do levého sloupce a čím víc vyskočí pod tím, tím lepší
- Tester síly hesla Password meter (http://www.paracom.cz/password.html) – poví všechno, kde jsou silné a slabé stránky hesla
- Změření odolnosti hesla (https://security.ics.muni.cz/kontrola-hesla) – hodně informací i to, za jak dlouho by bylo heslo prolomeno

Pro mne bezpečné heslo

.....

Příloha 2.7 Autorský zákon na internetu

Zadání scénky pro evokaci

Paní učitelka zadala třídě referát na knihu Krakatit. Honza si řekl, že se mu to číst nechce, raději referát udělá z filmu podle knihy, i když už je z roku 1948, je to lepší, než něco číst. Starší bratr mu poradil, jak si film pustit na internetu. Honza se na něho podíval a sepsal referát. Říkal si, že když je film podle knížky, bude obsah úplně stejný. Aby byl jeho referát zajímavější, rozhodl se, že spolužákům pustí kousek, co se mu líbil. Protože ale je ve škole slabý internet, tak si film stáhl. Ukázku pak samozřejmě ve třídě pustil.

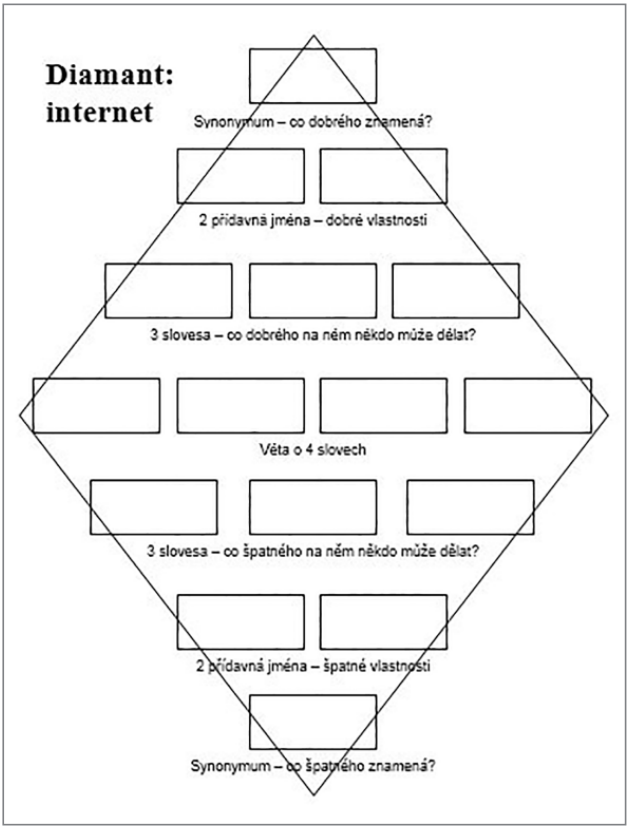
Pracovní list pro analýzu článků

Rozbor mediální zprávy

Kdy byl článek zveřejněný?	
Kdo měl být potrestaný?	
Za co měl být trest?	
Jaký byl trest?	
Jak se bránil ten, kdo porušil autorský zákon?	
Zaujalo vás něco?	

Obrázek 15 Analýza mediální zprávy

Příloha 2.8 Detektivky na Facebooku



Obrázek 16 Diamant

Příběhy útoků

MARTINA A

Martina se smutně rozhlédla po pokoji. Na stěnách viděla fotky, kde se smála se svou nejlepší kamarádkou, pár obrázků z posledního třídního výletu, kytku, co si naposled natrhala u přehrady, když s pár dalšími lidmi chtěli využít teplého letního večera. Pak dala do kufru posledních pár kousků oblečení a zaklapla ho. Ten zvuk jí ukázal, že stěhování už je tady a celý její život končí a bude muset začít jinde znovu. Jak ji asi vezmou v půlce školního roku?

MARTINA B

Martina změnila školu, ale tím její starost neskončila. Už je sice neviděla ve škole, ale něco je stále spojovalo. Když se přihlásila na Facebook, opět se na ni vyřítila

dávka sprostých slov spolu s odpornými obrázky, do kterých byla vložena její fotka. Mezi mnoha byla na její zdi básnička od „vzorné žačky" z bývalé třídy: „Vypadá jako hnida/ ale je velká pinda/anglicky umí jen i miss you, i love you/ Ale na to jí říkám jen Fuck you." Vyvrcholilo to na Nový rok, kdy dostala „přání": „Přeju ti vše nejhorší do nového roku. Smrt, mor, syfilis, tuberu, láskou nezamaskuješ žádný hemeroidy, hnidy. A dostaneš přes hubu hned na Nový rok." Ta hrůza z ponížení před milióny lidí pro ni byla nesnesitelná. Martina se zhroutila. Odmítala jíst.

MARTINA C

Naštěstí opět zasáhla máma. Šla do Martininy bývalé školy a přesvědčovala učitelku, že je nutné něco udělat. Když se jí to stále nedařilo, obrátila se na policii, která případ začala řešit a došlápla si na ty, kdo Martině ubližovali. Skončilo to záznamem do prospěchu v chování a pokáráním. Snad to postačí, aby stejný zájem nevěnovali někomu dalšímu, když Martina už jejich cílem být nemohla.

MARTINA D

Pak přišel konec školního roku a Martina doufala, že dvouměsíční pauza situaci uklidní. Ale po začátku školního roku to vypadalo spíš na to, že ostatní chtěli dohnat, co zameškali. Smáli se jí, když byla před tabulí. Zesměšňovali ji. Útoky zesilovaly. Vyvrcholilo to tím, že natočili shora kabinku záchodu, když měla průjem. A video kolovalo třídou... všichni se svíjeli smíchy, až na Martinu. Už nevěděla jak dál, tak se svěřila učitelce. Ta jí ale nevěřila a říkala, že to k jejich věku patří, že občas „rýpnou". A že to je určitě jen jednorázový problém. Styděla se to říct doma, tak svůj problém jen naznačovala a doufala, že se objeví pomoc. Ta nepřicházela, proto jednou napsala na Facebook, že takový život nezvládne a musí ho skončit.

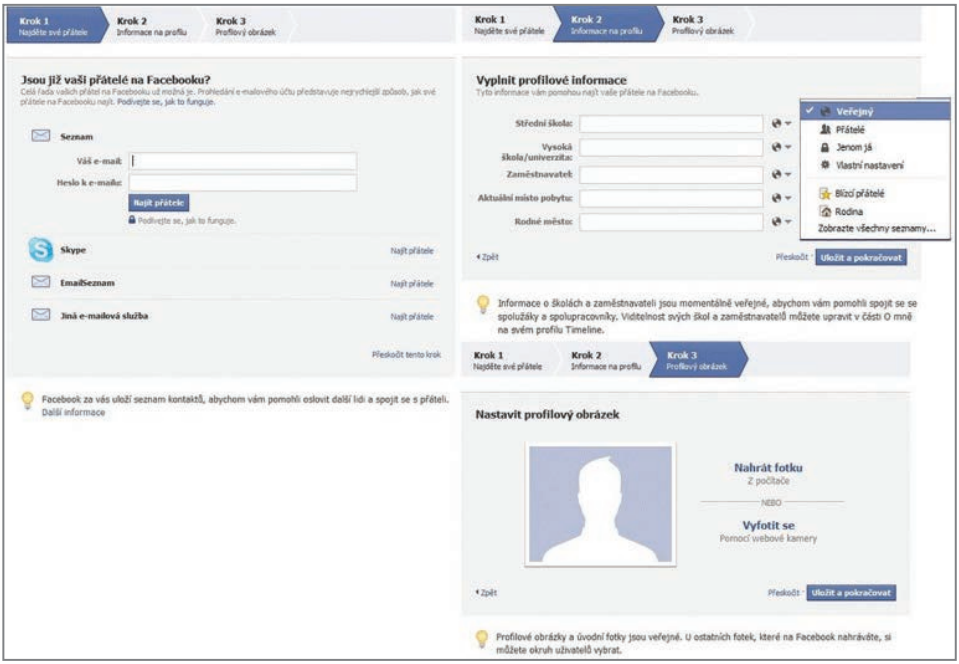
MARTINA E

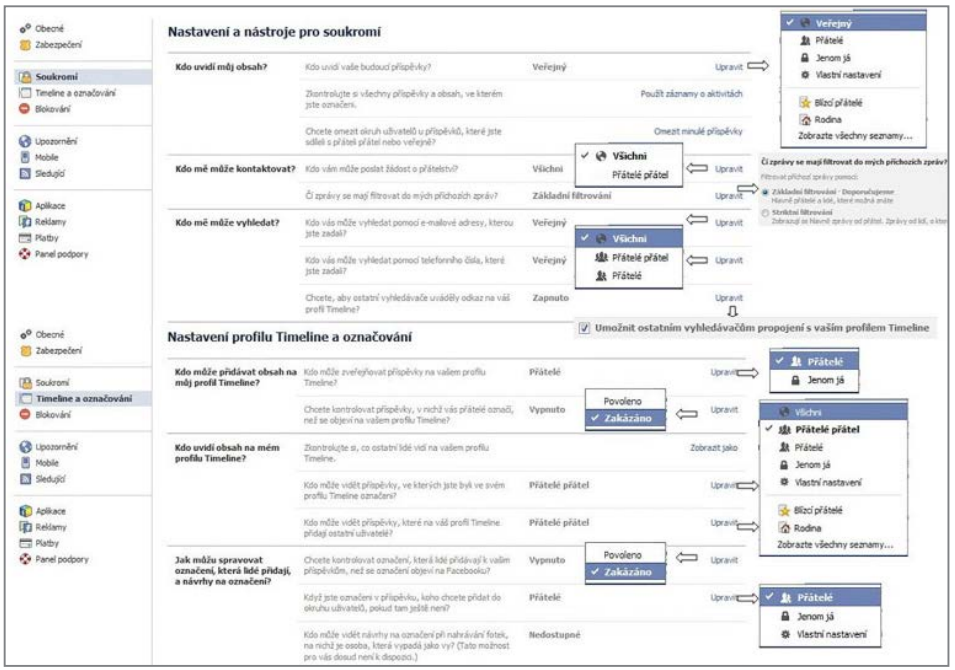
S přicházejícím jarem už odpověď na otázku při stěhování znala, ale byla horší, než si kdy představovala i v nejhorších snech. Pošťuchování, kterým to začalo, ještě čekala. Navzájem se s ostatními tipovali, co jsou zač. Postupně to ale začalo přecházet v něco, co už nemohla označit jako pošťuchování, protože jí to bylo nepříjemné. Neustálé narážky na její původ na vesnici, nemoderní oblečení, nenamalovaný obličej nabývaly na agresivitě i sprostosti.

MARTINA F

Stěhování ale nezabilo její předchozí přátelství, takže za pár minut zvonil Martině mamce telefon a nejlepší kamarádka její dcery jí řekla, co Martina chystá. Martina to myslela vážně, ale včasný příchod její maminky zajistil včasnou pomoc.

Kyberšikana
Skutečnost: NEJEZCHLEBOVÁ, Lenka. SMS pro hnidu a video ze záchoda. Tak vypadá kyberšikana. IDnes [online]. 5. března 2009 [cit. 2013-07-21]. Dostupné z: http://zpravy.idnes.cz/sms-pro-hnidu-a-video-ze-zachoda-tak-vypada-kybersikana-p1l-/domaci.aspx?c=A090304_130312_domaci_nel
WYNTER, Nadia. Parents of Holly Grogan, 15, blame Facebook for teen's suicide. The New York times. Monday, September 21, 2009. ISSN 0362-4331. Dostupné z: http://articles.nydailynews.com/2009-09-21/news/17933131_1_facebook-social-networking-bully
KOPECKÝ, Kamil, René SZOTKOWSKI a Veronika KREJČÍ. Nebezpečí internetové komunikace III. 1. vyd. Olomouc: Pedagogická fakulta, Univerzita Palackého v Olomouci, 2012, 60 s. ISBN 978-80-244-3088-1. Dostupné z: http://e-bezpeci.cz/index.php/ke-stazeni/doc_download/39-nebezpei-internetove-komunikace-3-2011-2012





Obrázek 17 Registrace na Facebook

Příloha 2.9 Život mediální zprávy

Najděte ve svém článku:

Název webu:

Jaké sledoval autor cíle, když psal článek? Chtěl informovat, přesvědčit, pobavit, ovlivnit? O čem?	
Na jaké zdroje informací se autor zprávy odkazuje? Jsou jednostranné, nebo nabízí různé pohledy na téma?	
Co v textu může být manipulace? Jaké z toho mohou čtenáři vzniknout problémy, když celé zprávě uvěří?	
Vyberte si v článku jednu dílčí informaci. Co k ní autor poskytuje, aby doložil, že byste jí měli věřit?	

Obrázek 18 Pracovní list pro analýzu článků

SMELL test

John McManus

Source	Kdo poskytl informace? Kdo je autorem? Odkud sám vzal informace?	
Motivation	Proč mi to říkají? Je patrný nějaký soukromý zájem? Snaží se mne přesvědčit, nebo informovat?	
Evidence	Jaké důkazy jsou dodány pro zobecnění? Jak ví to, co tvrdí? Umožňují mi ověřit si tvrzení?	
Logic	Odpovídá to tomu, co už o tématu vím? Vedou fakta logicky k uvedeným závěrům?	
Left out	Co chybí, co by mohlo změnit interpretaci informací? Nejsou zamlčeny pohledy některých zúčastněných stran?	

Obrázek 19 SMELL test

PŘÍLOHA 3 OBSAHOVÉ VAZBY TÉMAT V KONCEPCI

Příloha 3.1 Rozvíjené kompetence v lekcích dle RVP ZV a NIQUES

Bezpečnost při získávání a hodnocení informací

RVP ZV[1] (Vzdělávací oblast – obor: číslo výstupu (období a stupeň vzdělávání)	**NIQUES[2]**
Jazyk a jazyková komunikace – Komunikační a slohová výchova: ČJL-3-1-01 a 02 (1. období 1. stupeň), ČJL-5-1-01, 02, 03 a 06 (2. období 1. stupeň), ČJL-9-01, 03 a 08 (2. stupeň) – Jazyková výchova: ČJL-9-2-03 (2. stupeň) Informační a komunikační technologie – Vyhledávání informací a komunikace: ICT-5-2-01 a 02 (1. stupeň) a ICT-9-1-01 (2. stupeň) – Zpracování a využití informací: ICT-9-2-02 až 04 (2. stupeň) Člověk a jeho svět – Lidé kolem nás: ČJS-5-2-04 (2. období 1. stupeň) Člověk a společnost – Výchova k občanství: VO-9-1-05 a 09, VO-9-4-05, 08 a 10 (2. stupeň) Člověk a zdraví: – Výchova ke zdraví: VO-9-1-14 (2. stupeň)	Informační gramotnost – indikátory dosažené úrovně informační gramotnosti – Identifikovat a specifikovat potřebu informací v problémové situaci: formulace problému, určení typu informace – Najít, získat, posoudit a vhodně použít informace s přihlédnutím k jejich charakteru a obsahu: získání informací, posouzení relevance a úplnosti informací, posouzení pravdivosti informací, zpracování textu – Používat vhodné pracovní postupy (algoritmy) při efektivním řešení problémů: analýza získaných informací, modelování a simulace, plánování postupu řešení – Účinně spolupracovat v procesu získávání a zpracování informací s ostatními: vytváření originálního díla – Při práci dodržovat etická pravidla, zásady bezpečnosti a právní normy: uplatňování právních norem, etika zacházení s informacemi a netiketa – Využívat potenciálu digitálních technologií: vývoj technologií a společnost

1 Příloha č. 1 (...) 2015.

2 Příloha č. 5 Soubor indikátorů dosažné úrovně informační gramotnosti 2015.

Průřezová témata – Osobnostní a sociální výchova: seberegulace a sebeorganizace – Mediální výchova: kritické čtení a vnímání mediálních sdělení, interpretace vztahu mediálních sdělení a reality, stavba mediálních sdělení, vnímání autora mediálních sdělení, fungování a vliv médií ve společnosti	**Čtenářská gramotnost** – Zaměření na samotný text: práce s textem z různých médií, uvědomění si autora, záměru i adresáta textu, rozpoznání a vyhodnocení jejich vlivu při interpretaci textu
klíčové kompetence: k učení, k řešení problémů a občanské (zejména spojení s autorskými právy)	

Digitální stopy a riziková komunikace

RVP ZV	NIQUES
Jazyk a jazyková komunikace – Komunikační a slohová výchova: ČJL-3-1-03 (1. období 1. stupeň), ČJL-9-02 a 07 (2. stupeň) **Informační a komunikační technologie** – Základy práce s počítačem ICT-5-1-02 a 03 (1. stupeň) – Vyhledávání informací a komunikace: ICT-5-2-03 (1. stupeň) a ICT-9-1-01 (2. stupeň) **Člověk a jeho svět** – Lidé kolem nás: ČJS-5-2-01 a 03 (2. období 1. stupeň) **Člověk a společnost** – Výchova k občanství: VO-9-1-07, VO-9-4-05, 08 a 10 (2. stupeň) **Člověk a zdraví** – Výchova ke zdraví: VO-9-1-01, 12, 14 a 16 (2. stupeň)	**Informační gramotnost – indikátory dosažené úrovně informační gramotnosti** – Najít, získat, posoudit a vhodně použít informace s přihlédnutím k jejich charakteru a obsahu: posouzení pravdivosti informací – Používat vhodné pracovní postupy (algoritmy) při efektivním řešení problémů: analýza získaných informací, modelování a simulace, plánování postupu řešení – Účinně spolupracovat v procesu získávání a zpracování informací s ostatními: komunikace – Vhodným způsobem informace i výsledky práce prezentovat a sdílet: vytváření digitální identity – Při práci dodržovat etická pravidla, zásady bezpečnosti a právní normy: bezpečnost, ochrana zdraví, etika zacházení s informacemi a netiketa – Využívat potenciálu digitálních technologií: každodenní život s technologiemi
Průřezová témata – Osobnostní a sociální výchova: mezilidské vztahy, komunikace, řešení problémů a rozhodovací dovednosti, hodnoty, postoje, praktická etika – Multikulturní výchova: lidské vztahy	

Příloha 3.2 Srovnání charakteristik lekcí

	Název	Výukové cíle – Žák je po lekci schopen…	Spojení s RVP ZV	Spojení s NIQUES (informační gramotnost)	Materiální vybavení	Aktivity E-U-R
1	Výhody a nevýhody počítačů	– srovnat různé typy digitálních zařízení z hlediska jejich využití; – uvést klady a zápory jednotlivých zařízení; – uvědomovat si potřebu osobního rozvoje v oblasti IT a svůj zájem v této oblasti; – vyjádřit vlastní názor na problémovou situaci, aplikovat prezentační dovednosti a aktivní naslouchání, obhájit a kritizovat názory ve skupině.	ČJL-3-1-02, ČJL-3-1-03, ICT-5-1-02, klíčové kompetence a průřezová témata	Formulace problému, plánování postupu řešení, hardware, každodenní život s technologiemi	Psací potřeby a volné papíry pro žáky, puzzle (jedny pro skupinu), pracovní list Analýza věcných rysů (jeden pro skupinu), vhodné každé z řešených zařízení	Puzzle – Analýza věcných rysů (výhody a omezení) – Malování nejvýhodnějšího zařízení
2	Desatero bezpečného internetu	– aplikovat základní bezpečnostní principy při použití internetu; – rozumět důvodům omezení při použití internetu pro prevenci ohrožení sebe nebo ostatních; – vyjádřit vlastní názor na problémovou situaci, aplikovat prezentační dovednosti a aktivní naslouchání, obhájit a kritizovat názory ve skupině.	ČJL-3-1-01, ČJL-3-1-02, ČJL-3-1-03, ČJL-3-1-07, ICT-5-1-02, ICT-5-1-03, klíčové kompetence a průřezová témata	Formulace problému, posouzení pravdivosti informací, modelování a simulace, plánování postupu řešení, komunikace, vytváření digitální identity, bezpečnost, uplatňování právních norem, každodenní život s technologiemi	Psací potřeby a volné papíry pro žáky, tabule a fixy, herní plán, barevné magnety (5 různých barev), hrací kostka, pracovní list Komiks pro reflexi desatera bezpečného internetu (jeden pro každého žáka)	Vennův diagram (počítač a telefon) – Člověče, nezlob se (desatero bezpečnosti) – Komiks (rada kamarádovi)
3	Digitální stopy v síti	– vysvětlit omezené možnosti zachovat nebo smazat informaci zpřístupněnou na internetu; – rozlišovat možné způsoby šíření informací na internetu přes společenské vazby; – uvést praktické příklady možných důsledků nevhodného sdílení informací na internetu; – vyjádřit vlastní názor na problémovou situaci, aplikovat prezentační dovednosti a aktivní naslouchání, obhájit a kritizovat názory ve skupině.	ČJL-3-1-01, ČJL-3-1-02, ČJL-3-1-03, ČJL-3-1-07, ČJL-3-1-11, ICT-5-1-02, ICT-5-1-03, ICT-5-2-03, klíčové kompetence a průřezová témata	Formulace problému, posouzení pravdivosti informací, modelování a simulace, plánování postupu řešení, komunikace, vytváření digitální identity, bezpečnost, uplatňování právních norem, etika zacházení s informacemi a netiketa, každodenní život s technologiemi	Psací potřeby a volné papíry pro žáky, tabule a fixy, papírová krabička nebo obálka na časovou kapsli, komiks (jeden pro každého žáka), možné rekvizity na scénky (klobouk, paruka…)	Šibenice – Scénky podle komiksu – Časová kapsle

	Název	Výukové cíle – Žák je po lekci schopen…	Spojení s RVP ZV	Spojení s NIQUES (informační gramotnost)	Materiální vybavení	Aktivity E-U-R
4	Kdo je za monitorem?	– identifikovat obvyklé postupy zjišťování zneužitelných osobních informací v komunikaci na internetu; – kategorizovat informace podle úrovně možného zneužití, zejména ve vztahu k fyzické identitě; – formulovat vhodné odpovědi na osobní otázky od internetového známého, včetně odmítnutí sdělit zneužitelnou informaci o sobě či jiném; – vyjádřit vlastní názor na problémovou situaci, aplikovat prezentační dovednosti a aktivní naslouchání, obhájit a kritizovat názory ve skupině.	ČJL-5-1-03, ICT-5-1-02, ICT-5-1-03, ICT-5-2-03, ČJS-5-2-01, ČJS-5-2-02, klíčové kompetence a průřezová témata	Formulace problému, získání informací, posouzení relevance a úplnosti informací, posouzení pravdivosti informací, analýza získaných informací, modelování a simulace, plánování postupu řešení, vytváření originálního díla, komunikace, vytváření digitální identity, bezpečnost, uplatňování právních norem, etika zacházení s informacemi a netiketa, každodenní život s technologiemi	Psací potřeby a volné papíry pro žáky, tabule a fixy, dvě místnosti (ne vzdálené), placky nebo lístky pro identifikaci v soutěži (jedna pro každého žáka), pracovní list Tabulka zjištěných identit (jeden pro každého žáka), pracovní list Když se mě někdo zeptá… (pro skupiny), seznam pravidel v soutěži (zavěšený pro skupinu nebo promítaný), možné lístky s obvyklými komunikačními službami	Brainstorming (komunikační služby) – Soutěž v odhalování identit – Když se mne někdo zeptá…
5	Práce s informačními zdroji	– uvést výhody a omezení jednotlivých typů informačních zdrojů, především s ohledem na jejich důvěryhodnost; – použít pomůcky pro orientaci v různých typech informačních zdrojů; – rozumět potřebě hodnocení informací a jejich zdrojů; – aplikovat základní evaluační kritéria pro informační zdroje; – vyjádřit vlastní názor na problémovou situaci, aplikovat prezentační dovednosti a aktivní naslouchání, obhájit a kritizovat názory ve skupině.	ČJL-5-1-01, ČJL-5-1-02, ČJL-5-1-03, ČJL-5-1-04, ICT-5-1-02, ICT-5-1-03, ICT-5-2-01, ICT-5-2-02, ČJS-5-2-01, ČJS-5-2-02, ČJS-5-2-03, ČJS-5-2-04, klíčové kompetence a průřezová témata	Formulace problému, určení typu informace, získání informace, posouzení relevance a úplnosti informací, posouzení pravdivosti informací, analýza získaných informací, modelování a simulace, plánování postupu řešení, vytváření originálního díla, bezpečnost, ochrana zdraví, uplatňování právních norem, etika zacházení s informacemi a netiketa, každodenní život s technologiemi	Psací potřeby a volné papíry pro žáky, tabule a fixy, kniha a časopis k řešeným tématům a dva počítače, zadání rychlých špiónů, týmové role (jedna pro každého žáka), analyzovaný text (jeden pro každého žáka), pracovní list I.N.S.E.R.T. (pro skupinu), pracovní list Hledání informací (jeden pro skupinu), možný plakát s hodnotícími kritérii	Rychlí špióni (aktivity) – Analýza textů (I.N.S.E.R.T., obsah a forma) – Soupis hodnotících kritérií

	Název	Výukové cíle – Žák je po lekci schopen…	Spojení s RVP ZV	Spojení s NIQUES (informační gramotnost)	Materiální vybavení	Aktivity E-U-R
6	Mnoholičný lektvar	– popsat možné způsoby podvržení identity při komunikaci na internetu; – identifikovat obvyklé postupy sociálního inženýrství; – aplikovat zdravou nedůvěru na internetovou komunikaci; – vysvětlit význam autentizace a způsoby bezpečného použití hesla; – vytvořit bezpečné heslo; – vyjádřit vlastní názor na problémovou situaci, aplikovat prezentační dovednosti a aktivní naslouchání, obhájit a kritizovat názory ve skupině.	ČJL-9-1-02, ČJL-9-1-07, ČJL-9-2-03, ICT-9-1-01, VO-9-1-07, VO-9-4-05, VO-9-4-08, VO-9-4-10, VZ-9-1-01, VZ-9-1-14, VZ-9-1-16, klíčové kompetence a průřezová témata	Formulace problému (vynikající), určení typu informace (vynikající), určení typu informace (standardní), posouzení relevance a úplnosti informací (vynikající), posouzení pravdivosti informací (vynikající), analýza získaných informací (standardní), modelování a simulace (standardní), plánování postupu řešení (minimální), komunikace (standardní), vytváření digitální identity (vynikající), bezpečnost (vynikající), uplatňování právních norem (vynikající), etika zacházení s informacemi a netiketa (vynikající), každodenní život s technologiemi (minimální)	Psací potřeby a volné papíry pro žáky, dvě místnosti (ne vzdálené), lístky s názvy hrozeb (jeden pro skupinu), pracovní list Tabulka pravosti identit (jeden pro každého žáka), pracovní list Hesla (pro každého žáka), seznam pravidel v soutěži (zavěšený pro skupinu nebo promítaný), vhodná tabule a fixy a anglicko-české slovníky	Definice pojmů (hrozby) – Soutěž v odhalování lhářů – Brainstorming (bezpečné heslo)
7	Up and download	– uvědomovat si význam autorských práv a povinností pro vlastní i cizí tvorbu; – aplikovat zákonná omezení na nejběžnější způsoby nakládání s cizími autorskými díly v elektronickém prostředí; – definovat rozdíly v možnostech nakládání s různými typy děl; – vyjádřit vlastní názor na problémovou situaci, aplikovat prezentační dovednosti a aktivní naslouchání, obhájit a kritizovat názory ve skupině.	ČJL-9-1-07, ČJL-9-1-08, ICT-9-2-03, ICT-9-2-04, VO-9-4-05, VO-9-4-08, VO-9-4-10, VZ-9-1-01, VZ-9-1-16, klíčové kompetence a průřezová témata	Formulace problému (vynikající), určení typu informace (vynikající), posouzení relevance a úplnosti informací (standardní), posouzení pravdivosti informací (vynikající), zpracování textu (minimální), analýza získaných informací (minimální), modelování a simulace (standardní), vytváření originálního díla (vynikající), uplatňování právních norem (vynikající), etika zacházení s informacemi a netiketa (vynikající), každodenní život s technologiemi (minimální)	Psací potřeby a volné papíry pro žáky, tabule a fixy, citace ze zákona (jedna pro každého žáka), mediální zpráva (jedna pro každého žáka), pravidla třífázového rozhovoru k zavěšení pro třídu (příp. promítané)	Učíme se navzájem (citace zákona) – Třífázový rozhovor (mediální zprávy) – Brainstorming a patero do licenčních podmínek

	Název	Výukové cíle – Žák je po lekci schopen…	Spojení s RVP ZV	Spojení s NIQUES (informační gramotnost)	Materiální vybavení	Aktivity E-U-R
8	Detektivky na Facebooku	– aplikovat zdravou nedůvěru na internetovou komunikaci; – identifikovat obvyklé varovné signály nejčastějších hrozeb v internetové komunikaci; – definovat možná bezpečnostní opatření proti těmto hrozbám; – spravovat nastavení soukromí a zabezpečení uživatelského účtu, včetně uvědomění si možných důsledků zvoleného nastavení; – vyjádřit vlastní názor na problémovou situaci, aplikovat prezentační dovednosti a aktivní naslouchání, obhájit a kritizovat názory ve skupině.	ČJL-9-1-02, ČJL-9-1-07, ČJL-9-1-08, ICT-9-1-01, VO-9-1-06, VO-9-1-07, VO-9-1-08, VO-9-1-09, VO-9-4-05, VO-9-4-08, VO-9-4-10, VZ-9-1-01, VZ-9-1-12, VZ-9-1-14, VZ-9-1-16, klíčové kompetence a průřezová témata	Formulace problému (vynikající), určení typu informace (vynikající), posouzení relevance a úplnosti informací (vynikající), posouzení pravdivosti informací (vynikající), modelování a simulace (standardní), plánování postupu řešení (standardní), komunikace (standardní), vytváření digitální identity (vynikající), bezpečnost (vynikající), uplatňování právních norem (vynikající), etika zacházení s informacemi a netiketa (vynikající), každodenní život s technologiemi (minimální)	Psací potřeby a volné papíry pro žáky, pracovní list Diamant (pro každého žáka), nastříhané příběhy (jeden pro každého žáka), pracovní list FB registrace (pro skupiny), vhodné tabule a fixy	Diamant (internet) – Puzzle příběhu a předpoklady a důsledky hrozby – Simulace registrace na Facebook
9	Život mediální zprávy	– vyjmenovat základní postupy při tvorbě mediální zprávy; – uvědomovat si potřebu komparace informací z různých zdrojů s vyvozením vlastních závěrů; – hodnotit důvěryhodnost mediálního sdělení dle základních kritérií; – vyjádřit vlastní názor na problémovou situaci, aplikovat prezentační dovednosti a aktivní naslouchání, obhájit a kritizovat názory ve skupině.	ČJL-9-1-01, ČJL-9-1-02, ČJL-9-1-03, ČJL-9-1-07, ČJL-9-1-08, ICT-9-1-01, ICT-9-2-02, ICT-9-2-04, VO-9-1-05, VO-9-1-08, VO-9-1-09, VO-9-4-05, VZ-9-1-14, VZ-9-1-16, klíčové kompetence a průřezová témata	Formulace problému (vynikající), určení typu informace (vynikající), určení typu informace (standardní), posouzení relevance a úplnosti informací (vynikající), posouzení pravdivosti informací (vynikající), zpracování textu (minimální), analýza získaných informací (vynikající), modelování a simulace (standardní), plánování postupu řešení (minimální), vytváření originálního díla (vynikající), uplatňování právních norem (vynikající), každodenní život s technologiemi (minimální)	Psací potřeby a volné papíry pro žáky, tabule a fixy, pracovní list SMELL test (pro každého žáka), mediální zpráva (jedna pro každého žáka), pracovní list Analýza článků (pro skupiny), vhodný počítač s projektorem	Brainstorming (média) – Přednáška a analýza manipulace ve zpravodajství – SMELL test

Informační bezpečnost žáků základních škol
Lekce v knihovnách

Pavla Kovářová

Vydala MASARYKOVA UNIVERZITA, Žerotínovo nám. 617/9, 601 77 Brno
v edici **Spisy Filozofické fakulty Masarykovy univerzity** / číslo 489

Odpovědná redaktorka / doc. Mgr. Jana Horáková, Ph.D.
Výkonná redaktorka / doc. Mgr. Katarina Petrovićová, Ph.D.
Ediční referentka / Mgr. Vendula Hromádková
Grafická koncepce edice a návrh obálky / Mgr. Pavel Křepela
Sazba / Dan Šlosar

Vydání první / 2019
Náklad / 200 výtisků
Tisk a knihařské zpracování / Reprocentrum, a.s., Bezručova 29, 678 01 Blansko

ISBN 978-80-210-9270-9
ISBN 978-80-210-9271-6 (online : pdf)
ISSN 1211-3034
https://doi.org/10.5817/CZ.MUNI.M210-9271-2019

#**489**