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.

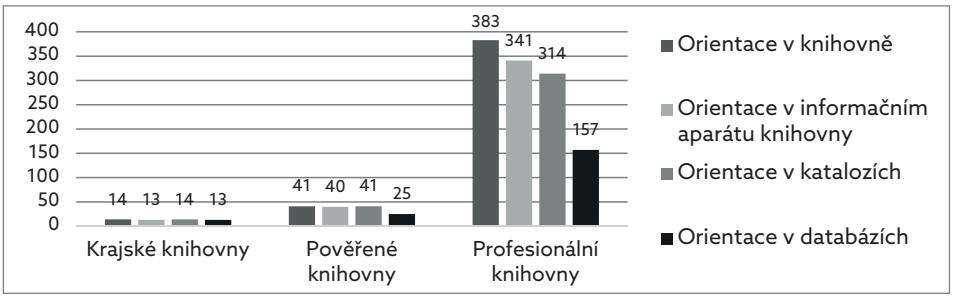
235 DOMBROVSKÁ 2004.

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.

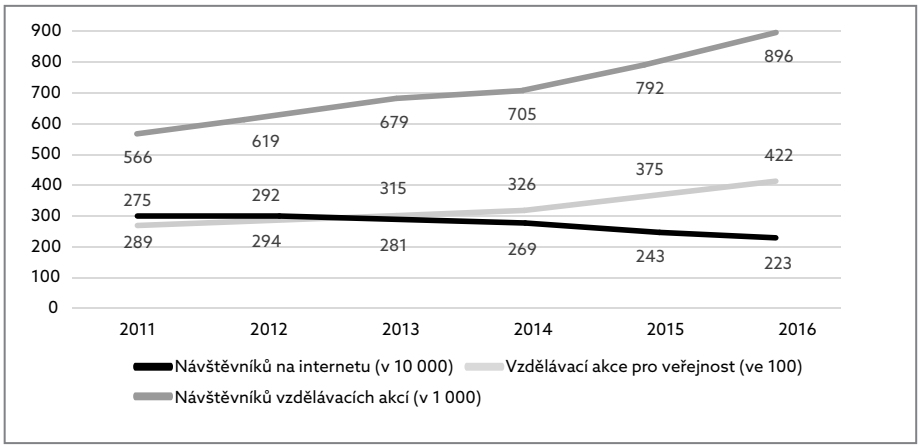
300 QUICK 2013, s. 8.

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.

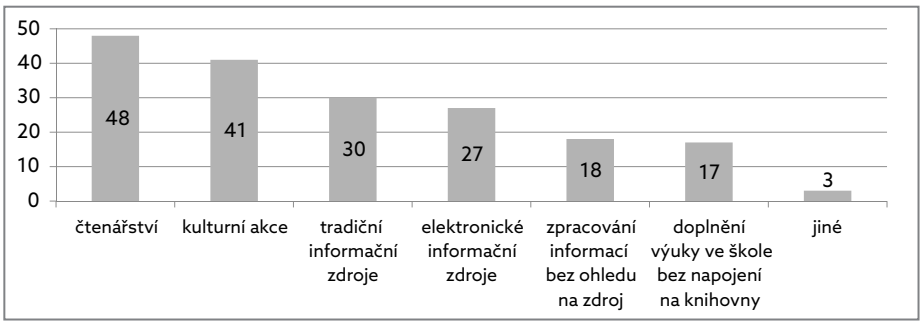
308 Základní statistické údaje o kultuře (...) 2013.

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.



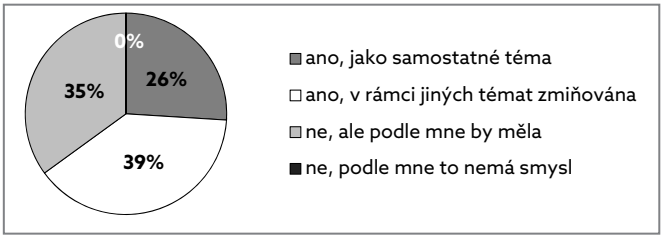
Graf 4 Základní kategorie obsahu vzdělávání dětí v knihovnách

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).



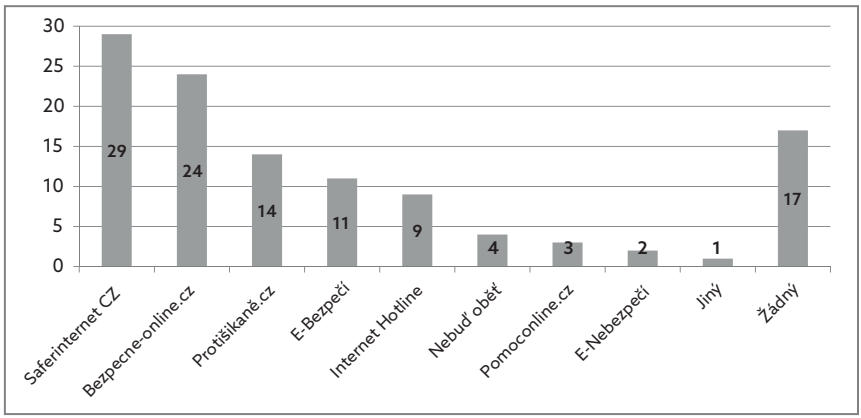
Graf 5 Zařazení bezpečnosti na internetu do lekcí pro děti

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.

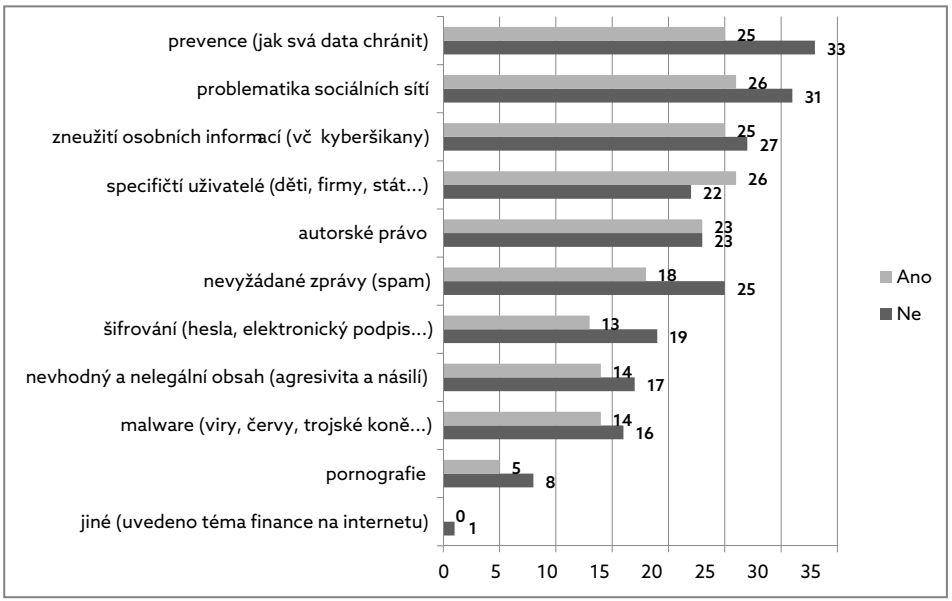
Známé internetové zdroje k informační bezpečnosti (Graf 6) byly zjišťovány proto, že na nich je možné najít materiály pro výuku o této problematice a také je možné na ně odkazovat zájemce o další informace. Řádově méně zastoupené proti projektům Saferinternet CZ byly iniciativy Centra PRVoK, přestože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

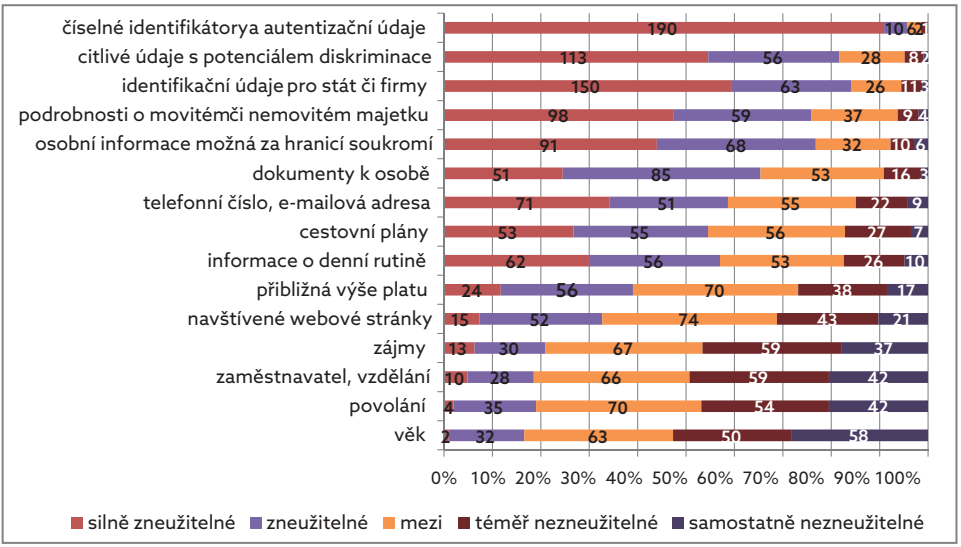
První otázka byla zaměřena na vymezení pojmu digitální stopy. Přestože byla v zadání uvedena možnost volby více odpovědí a všechny nabídnuté byly správné, ve výsledcích převažuje jediná. 93,4 % respondentů označilo jako správnou odpověď „*Soubor informací, které za sebou uživatel zanechává (ať již vědomě, 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.



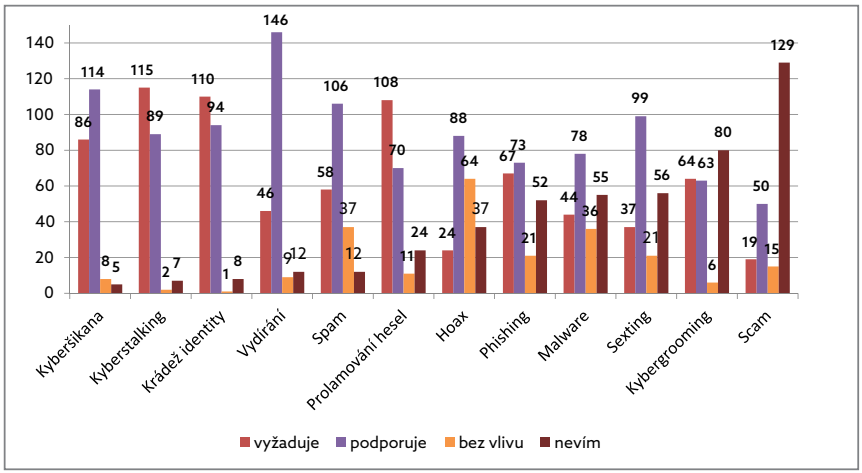
Graf 8 Síla zneužitelnosti informací z digitálních stop[321]

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

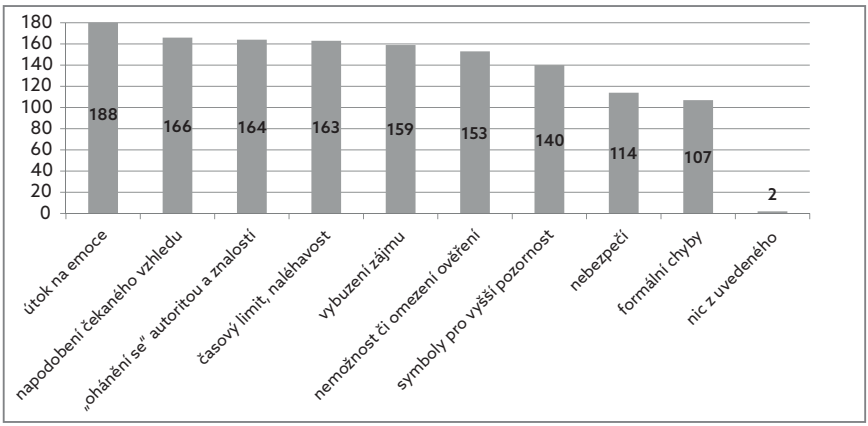
321 Řazeno dle průměrné zneužitelnosti, škála je zleva doprava od nejvíce po nejméně zneužitelné informace, středová hodnota je označena zelenou barvou.

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.

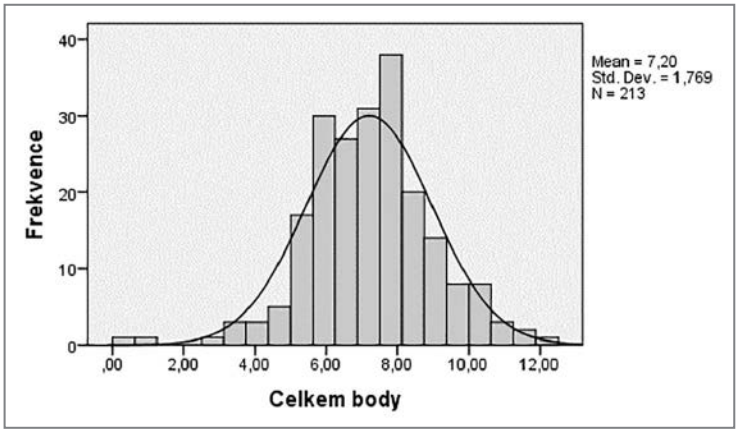
Další série otázek se zaměřila na znalost technických možností ochrany soukromí (anonymní mód v prohlížeči, proxy server a onion routing). Všechny měly více než 70 % špatných odpovědí, většina nulových ohodnocení byla udělena vlivem označení odpovědi *nevím*. Limity blokování Cookies si uvědomuje většina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

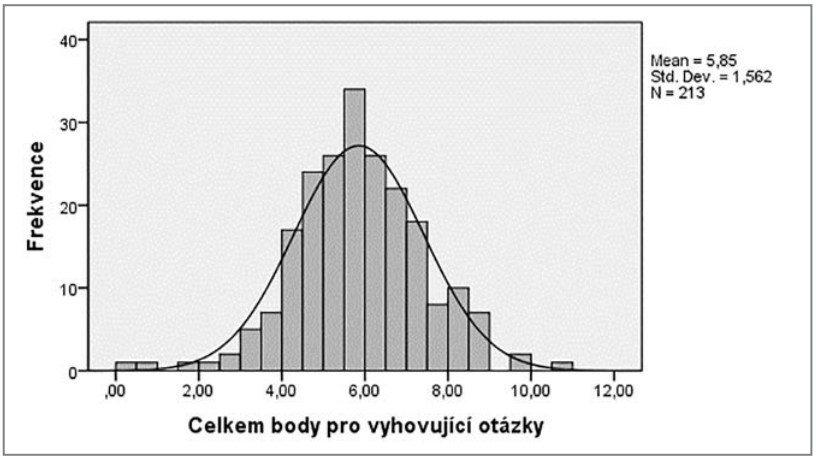
Tabulka 5 Obtížnost a citlivost testových úloh

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).

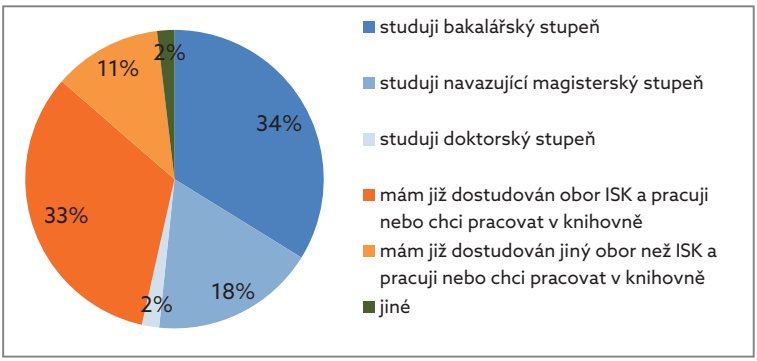
323 CHRÁSKA 1999, s. 49–51.

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).



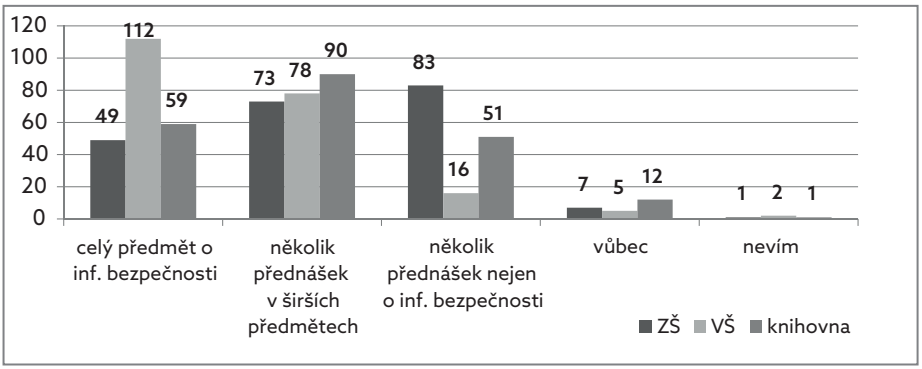
Graf 13 Pozice respondentů v systému školství a knihovnictví

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.