JIHOČESKÁ UNIVERZITA V ČESKÝCH BUDĚJOVICÍCH

PEDAGOGICKÁ FAKULTA

KATEDRA INFORMATIKY

Mgr. Václav Šimandl

Kompetence učitelů ICT v oblasti technické e-bezpečnosti

Disertační práce

Vedoucí práce: doc. PaedDr. Jiří Vaníček, Ph.D.

Studijní obor: Informační a komunikační technologie ve vzdělávání

ČESKÉ BUDĚJOVICE 2016

UNIVERSITY OF SOUTH BOHEMIA IN ČESKÉ BUDĚJOVICE

FACULTY OF EDUCATION

DEPARTMENT OF INFORMATICS

Mgr. Václav Šimandl

The competence of ICT teachers in the area of technical e-safety

Thesis

Supervisor: doc. PaedDr. Jiří Vaníček, Ph.D.

Field of study: Information and communication technology in education

ČESKÉ BUDĚJOVICE 2016

Bibliografická identifikace

Jméno a příjmení autora: Mgr. Václav Šimandl

Název disertační práce: Kompetence učitelů ICT v oblasti technické e-bezpečnosti

Název disertační práce anglicky: The competence of ICT teachers in the area of technical e-safety

Studijní program: Specializace v pedagogice

Studijní obor: Informační a komunikační technologie ve vzdělávání

Školitel: doc. PaedDr. Jiří Vaníček, Ph.D.

Školitel specialista: -

Rok obhajoby: 2016

Klíčová slova v češtině: e-bezpečnost, učitelé ICT, kompetence učitelů

Klíčová slova v angličtině: e-safety, ICT teachers, competence of teachers

ABSTRAKT

Aktuálním tématem je v současné době e-bezpečnost dětí a mládeže, na jejichž kompetence v oblasti e-bezpečnosti může mít značný vliv edukace. Nespornou roli zde hrají příslušné kompetence učitelů, které doposud nebyly uspokojivě zkoumány. Proto jsme realizovali kvalitativní výzkum, který se zabýval kompetencemi učitelů ICT v oblasti e-bezpečnosti. Cílem výzkumu bylo zmapování současných odborných kompetencí učitelů ICT, identifikování determinantů, ovlivňujících tyto kompetence, a vytvoření modelu jejich utváření. Sběr dat pro naplňování těchto cílů probíhal formou hloubkových rozhovorů s učiteli ICT, data byla analyzována pomocí otevřeného kódování a technik na něj navazujících.

E-bezpečnostní kompetence učitelů ICT ovlivňují kromě vnějších a vnitřních vlivů vztahy k pravidlům e-bezpečnosti, jako předpokládaným zdrojům bezpečného chování, a překážky ochrany v mysli učitele, které mu naopak brání se chovat bezpečně. Jako významný faktor (formující e-bezpečnostní návyky učitelů) byla identifikována předchozí negativní zkušenost učitele. Vytvořený model popisuje kauzální a intervenující vztahy mezi popsanými kategoriemi. V tomto modelu je důraz kladen na roli posouzení dat z pohledu e-bezpečnosti jakožto faktoru působícího na konkrétní způsoby ochrany jedince v určité situaci.

Na základě vytvořeného modelu jsme realizovali pedagogický experiment, jehož vliv na změnu postojů učících se osob v oblasti technické e-bezpečnosti jsme zjišťovali pomocí sémantického diferenciálu. V rámci experimentu jsme použili dva různé pedagogické přístupy vyplývající z výzkumu a vedoucí k zážitku negativní zkušenosti. První z nich byl založen na simulaci e-bezpečnostní hrozby s přímým zážitkem negativní zkušenosti, druhý na prožití negativní zkušenosti zprostředkovaně přednáškou externího odborníka. Přínosem této fáze výzkumu je ověření platnosti té části uvedeného modelu, která se zabývá vlivem negativní zkušenosti.

ABSTRACT

The e-safety of children and youngsters, whose e-safety knowledge and routines can be significantly influenced by education, is currently a highly up-to-date issue. What seems to be of paramount importance is whether teachers, who have not yet been satisfactorily researched, have appropriate knowledge and routines. For that reason, our study has carried out qualitative research to look into ICT teachers' e-safety knowledge and routines. The aim of the research was to map ICT teachers' current professional knowledge and routines to identify the determinants that influence their knowledge and routines and to develop a model of formation. To achieve these goals, data was collected through in-depth interviews with ICT teachers. Open coding and other associated techniques were subsequently used to analyse the data.

Besides being affected by external and internal influences, ICT teachers' e-safety knowledge and routines are also determined by their attitude to e-safety rules (whether they adopt them as guidelines for safe behaviour) and by the barriers to protection in teachers' minds which prevent them from behaving in a safe way. Teachers' previous negative experiences have also been identified as a significant factor (in forming teachers' e-safety habits). The created model describes causal and intervening relationships between given categories. In this model, an emphasis has been placed on the role of data interpretation from the point of view of e-safety as a factor affecting an individual's choice of specific method of protection for a certain situation.

The created model provided the basis for our pedagogical experiment, using the semantic differential to investigate its influence on learners' changes in attitude as far as technical e-safety is concerned. Two differing pedagogical approaches identified in the research as leading to the occurrence of a negative experience were used for the experiment. The first one was based on the simulation of an e-safety threat with the occurrence of a direct negative experience. The second was based on encountering a negative experience through a lecture given by an external specialist. This phase of the research is beneficial as it verifies the part of the given model that concerns the effects of a negative experience.

Poděkování

Chtěl bych tímto poděkovat svému školiteli panu docentu Jiřímu Vaníčkovi za četné rady a doporučení v průběhu zpracování této práce. Dále bych chtěl poděkovat panu doktoru Michalu Šerému za pomoc při analýze dat pomocí sémantického diferenciálu a panu magistru Václavu Dobiášovi za kritické připomínky při analýze dat pomocí metod zakotvené teorie.

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

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

V Českých Budějovicích dne 15. 4. 2016 …….

OBSAH

SEZNAM OBRÁZKŮ

SEZNAM TABULEK

SEZNAM POUŽITÝCH SYMBOLŮ A ZKRATEK

CD	Kompaktní disk
DUM	Digitální učební materiál
DVD	Digitální víceúčelový disk
EU	Evropská unie
ICT	Informační a komunikační technologie
JČU	Jihočeská univerzita v Českých Budějovicích
NAS	Síťové úložiště dat
OS	Operační systém
PC	Osobní počítač
SD	Sémantický diferenciál
USB	Univerzální sériová sběrnice
VŠTE	Vysoká škola technická a ekonomická v Českých Budějovicích

1 ÚVOD

Aktuálním problémem při používání digitálních technologií je bezpečnost uživatele a ochrana jeho dat. Zájem výzkumníků i široké veřejnosti je zaměřen především na e-bezpečnost dětí a mládeže, jejichž kompetence v oblasti e-bezpečnosti je možné zlepšovat prostřednictvím školní edukace. Klíčovými osobami v této problematice se jeví být učitelé, především pak učitelé ICT. Při výuce této problematiky je potřebné, aby učitelé dokázali u žáků pěstovat vhodné kompetence, podstatné je též, aby učitelé samotní byli v této oblasti odborníky. Od této odbornosti se navíc v některých případech odvíjí příslušná e-bezpečnostní politika školy. Z výše uvedených okolností vyplývá, že je potřeba porozumět tomu, jaké jsou kompetence učitelů ICT v této oblasti a jaké jsou determinanty těchto kompetencí. Protože je však téma e-bezpečnosti velice široké, my se zaměříme na problematiku spamu a hoaxu, malware, havárií počítačů, počítačových hesel a krádeží identity a na oblast sdílení osobních dat. Pro naše potřeby budeme tyto oblasti označovat souborným označením technická e-bezpečnost; širší souvislosti tohoto vymezení uvádíme v kapitole 2.

2 SOUČASNÝ STAV STUDOVANÉ PROBLEMATIKY

V rámci této kapitoly v podkapitole 2.1 prezentujeme vymezení základních pojmů této práce, podkapitoly 2.2 a 2.3 jsou věnovány znalostem, návykům a zkušenostem dětí, mládeže i dospělých uživatelů v oblasti technické e-bezpečnosti. Podkapitola 2.4 obsahuje rešerši literatury týkající se role školy a učitelů ICT při výuce e-bezpečnostních témat, požadavky kladené na odborné kompetence učitelů v této oblasti jsou diskutovány v podkapitole 2.5 a dosavadními poznatky, které se týkají kompetencí učitelů v oblasti e-bezpečnosti, se zabýváme v podkapitole 2.6. Podkapitola 2.7 je věnována e-bezpečnostním kompetencím, které u absolventů škol očekávají české i mezinárodní kurikulární dokumenty.

Jednotlivé výňatky z rešerší, které prezentujeme v této kapitole, jsme již publikovali v článcích, jejichž seznam je uveden v sekci Publikační činnost. Zatímco v jednotlivých článcích jsme se zabývali pouze rešeršemi vztahujícími se ke konkrétní části problematiky, v této publikaci prezentujeme jejich ucelenější přehled.

2.1 Vymezení terminologie

2.1.1 Kompetence

Pojem kompetence lze v pedagogickém pojetí chápat jako schopnost, dovednost, způsobilost úspěšně realizovat nějaké činnosti, řešit určité úkoly zejména v pracovních a jiných životních situacích (Průcha et al., 2009), chovat se určitým způsobem, plnit určité funkce a sociální role (Kolář et al., 2012). Veteška a Tureckiová (2008a) se domnívají, že kompetence znamená jedinečnou schopnost člověka úspěšně jednat a dále rozvíjet svůj potenciál na základě integrovaného souboru vlastních zdrojů, a to v konkrétním kontextu různých úkolů a životních situací, spojenou s možností a ochotou (motivací) rozhodovat a nést za svá rozhodnutí odpovědnost. Pod těmito zdroji přitom chápou soubor veškerých informací, znalostí (teoretických poznatků a vědomostí), dovedností a dřívější zkušenosti jedince, znalost postupů řešení problémů a složitějších konceptů a modelů (Veteška a Tureckiová, 2008a).

Kompetence se projevuje zásadně v chování (které může být součástí kompetence), respektive v průběhu a výsledku nějaké činnosti (dosažení cíle), a je v ní obsažen rozvojový potenciál (Veteška, 2010). Kompetence je získávána a rozvíjena v procesech vzdělávání

a učení (Veteška, 2010), přičemž zvládnutí kompetence v požadované míře je posuzováno úspěšností chování jedince v různých životních situacích (Veteška a Tureckiová, 2008b).

2.1.2 Učitel ICT

Pod pojmem učitel ICT v této práci rozumíme učitele, který vyučuje na základní či střední škole předměty zaměřené na výuku ICT a informatiky. Jak uvádí Naske (2011), výuka ICT se zabývá rozvíjením základních uživatelských dovedností při práci s digitálními technologiemi[1], znalostí a dovedností poučeného uživatele ICT techniky. Výuku informatiky lze považovat za úvod do algoritmizace a informatiky jako oblastí propojených s poučeným způsobem využití ICT (Naske, 2011). Tyto předměty jsou zpravidla označovány jako ICT, Informatika, Informační technologie, Informační a komunikační technologie, Výpočetní technika a podobně.

2.1.3 E-bezpečnost a technické e-bezpečnost

E-bezpečnost (v angličtině e-safety) se zabývá ochranou uživatele a jím používaných digitálních technologií před negativními jevy, které se vyskytují při využívání digitálních technologií (Barrow a Heywood-Everett, 2006). Tato rizika tvoří značně nehomogenní celek, a proto vznikla během let celá řada definic e-bezpečnosti a systémů členění rizik, jimiž se zabývá (Chou a Peng, 2011). Důraz je přitom kladen především na rizika při práci na Internetu (Chou a Peng, 2011). Komplexní pohled na tuto problematiku dávají Livingstone a Haddon (2008), kteří rizika, jimiž se e-bezpečnost zabývá, rozdělují do čtyř základních kategorií:

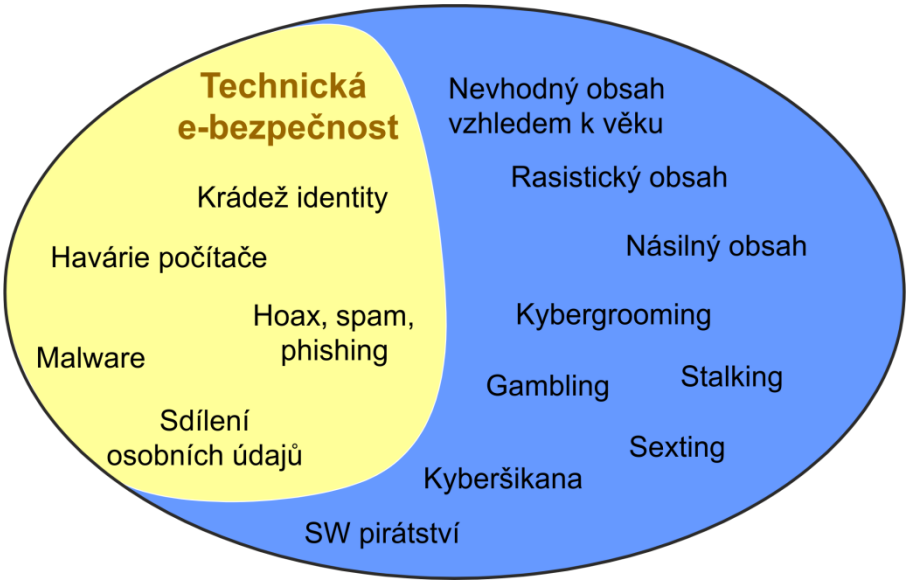
- rizika obsahová
- rizika kontaktní
- rizika komerční
- rizika spojená se soukromím

Mezi obsahová rizika začleňují např. vystavení se nelegálnímu nebo potenciálně škodlivému obsahu, sexuálním, násilným, rasistickým a nenávistným materiálům; jako rizika kontaktní zmiňují kyberšikanu a kontakt s neznámými osobami. Mezi komerční rizika

[1] Abychom odlišili pojem ICT označující vědní obor (zejména příslušný vyučovací předmět) od ICT jako prostředků pro komunikaci a práci s informacemi, budeme v následujícím textu prostředky pro komunikaci a práci s informacemi nazývat digitálními technologiemi.

řadí reklamní zneužívání, ilegální stahování dat a gambling; mezi rizika spojená se soukromím začleňují zneužívání počítačů, narušování soukromí a zveřejňování osobních informací.

Pojem technická e-bezpečnost se týká především té části e-bezpečnosti, která se zabývá interakcí uživatele s technikou. Případní další uživatelé a vztahy s nimi jsou zde vnímáni spíše na pozadí a dopředu vystupuje technická stránka věci. Pokud bychom použili kvalifikaci e-bezpečnostních rizik podle Livingstone a Haddon (2008), patří sem rizika spojená se soukromím, tj. problematika malware, sdílení osobních dat, počítačových hesel a s nimi spojených krádeží identity. Kromě těchto oblastí pod pojem technická e-bezpečnost zahrnujeme z důvodu blízkosti s ostatními tématy i negativní jevy při e-mailové komunikaci (spam, hoax, phishing) a havárie počítačů. Na Obrázku 1 jsou znázorněny vybrané jevy, kterými se zabývá e-bezpečnost, přičemž ve žlutě označené oblasti jsou umístěny jevy, které začleňujeme pod pojem technická e-bezpečnost.



Obrázek 1: Jevy, kterými se zabývá e-bezpečnost, s vyznačením jevů, které řadíme pod technickou e-bezpečnost

2.2 Kompetence dětí v technické e-bezpečnosti

Kompetence dětí a mládeže v oblasti e-bezpečnosti se staly předmětem zájmu mnoha českých i zahraničních výzkumů. Strategie, jak se chránit před nebezpečím, jsou u žáků prvního stupně základních škol vzhledem k věku málo propracované a rizika špatně pochopená (Cranmer et al., 2008), žákům druhého stupně chybí schopnost chápat a kriticky hodnotit online obsah a řídit své chování online (Byron, 2008). Byron (2008) uvádí, že

v některých skupinách rodin jsou zřejmé mezery ve vědomostech, porozumění a dovednostech týkajících se e-bezpečnosti a také v samotném uvědomění, co může být nebezpečím. K podobnému závěru dospěl v českém prostředí na základě rozhovorů se středoškolskými učiteli i Beránek. Podle něj jsou si žáci vědomi reálnosti e-bezpečnostních hrozeb, ale chybí jim základní e-bezpečnostní pravidla a nechtějí akceptovat „pravidla dospělých“ (Beránek, 2009). Toto zřejmě souvisí s názorem, že pro problematiku technické e-bezpečnosti je typické přesvědčení uživatelů, že jim se problémy zcela jistě vyhnou (Lang et al., 2009).

Jak uvádí Aytes and Conolly (2004, cit. podle Teer et al., 2007), snížení míry riskování při používání počítačů je možné díky zlepšení povědomí o této problematice a vhodnému tréninku. Podle organizace Ofcom (2015) mluvily se svými dětmi ve věku 8 až 15 let o zvládání online rizik asi čtyři pětiny britských rodičů, podobný podíl rodičů pak věří, že jejich děti používají digitální technologie bezpečným způsobem (Ofcom, 2011; Ofcom, 2015). Sebedůvěru ohledně bezpečného používání Internetu mají téměř dvě třetiny žáků ve vyšších ročnících středních škol, avšak jen čtvrtina žáků prvního stupně (Eynon, 2009). Nabízí se však otázka, zda žáci dokáží své kompetence správně ohodnotit. Podle výzkumu Huclové a Vrbíka (2011) chtěla v roce 2011 pouze čtvrtina oslovených žáků 2. stupně základních škol získat nové informace z oblasti e-bezpečnosti, zbylí žáci považovali toto téma za zbytečné. Autoři výzkumu nicméně žáky podrobili výuce zaměřené právě na e-bezpečnost a po skončení výuky všichni žáci uvedli, že se dozvěděli mnoho nových informací. Tento příklad ukazuje, že ne všichni žáci dokáží své kompetence dobře odhadnout, a proto v následujícím textu uvádíme konkrétní zjištění, jaké chování a zkušenosti mají děti a mládež v jednotlivých oblastech technické e-bezpečnosti.

V oblasti problematiky malware bezpečnostní firma Symantec Corporation (2010; 2011a) ve svých výzkumech zjistila, že třetina dětí si stáhla do počítače malware, naopak téměř dvě třetiny dětí jsou obezřetné při otevírání e-mailových příloh, dvě pětiny dětí říkají, že se mají na pozoru před příliš výhodnými online nabídkami, a asi třetina dětí je ostražitá před pop-up okny. Lauri et al. (2015) uvádí, že dvě pětiny dětí se již potýkaly s viry, sedmina zažila hackerský útok a téměř polovina dětí se setkala s pop-up okny. Třetina dětí se domnívá, že nejnebezpečnějším jevem v Internetu jsou hackerské útoky, a podle pětiny dětí je nejnebezpečnějším jevem nákaza malware (Lauri et al., 2015). Jak uvádí Eynon (2009), z počítačových virů má přinejmenším nějaké obavy přibližně polovina žáků; tyto obavy jsou

nejméně časté u žáků na prvním stupni základní školy a se zvyšujícím se věkem se stávají častějšími.

Komplexní pravidelně měněné bezpečnostní heslo užívá podle společnosti Symantec Corporation (2010) celosvětově méně než polovina dětí a podle studie provedené mezi dětmi v New Yorku použila cizí heslo bez svolení majitele účtu asi šestina respondentů (McQuade a Sampat, 2008 cit. podle OECD, 2011). Sdělování počítačových hesel mezi mladými lidmi je považováno nejen za projev důvěry, ale také za jednoduchou cestu, jak mít kontrolovanou e-mailovou schránku (resp. účet na sociální síti) v době nepřítomnosti (OECD, 2011).

Svůj profil na sociálních sítích nechává přístupný zcela veřejně nebo pro přátele přátel asi šestina dětí (Ofcom, 2015). Nastavení viditelnosti příspěvků na sociálních sítích pro přátele přátel nemusí být dostatečně bezpečné, medián počtu přátel přátel na sociální síti Facebook je asi 31 000 (Hampton et al., 2012). Děti navíc často mylně předpokládají, že osobní informace poslané online nepřekročí hranice, kam byly poslány (OECD, 2011).

Podle výzkumné zprávy společnosti AVG již děti ve věku 10 až 13 let provozují na Internetu podobné aktivity jako dospělí lidé, a proto „jsou vehnány do komplexních společenských situací, které vyžadují uvažování dospělého člověka – a to mnohem dříve, než jsou na to vůbec připraveny“ (Zouzalová a Malyon, 2011).

V kompetencích dětí a mládeže lze spatřovat určité nedostatky, a proto je potřeba děti o e-bezpečnostních rizicích poučit. Protože to činí ve velké míře jejich rodiče, nabízí se otázka, jaké jsou jejich e-bezpečnostní kompetence. V následujícím textu se proto budeme zabývat e-bezpečnostními kompetencemi dospělých osob.

2.3 Kompetence dospělých v technické e-bezpečnosti

Nebližšími osobami, na které se děti obracejí s žádostí o pomoc či radu, jsou jejich rodiče. Ti však často znají digitální technologie jako pracovní nástroj (Kapoun et al., 2011) a cítí se být nevybaveni pomoci dětem ve světě digitálních technologií (Byron, 2008). Podle organizace Ofcom (2011) se například dvě třetiny rodičů domnívají, že jejich děti ve věku 12 až 15 let mají lepší povědomí o Internetu než oni.

Ačkoliv si většina dospělých na rozdíl od dětí rizika spojená s používáním digitálních technologií uvědomuje, mnozí z nich nemají dostatečné e-bezpečnostní znalosti a návyky a neznají postupy, jak se vyrovnat s nebezpečím. Pocit plné kontroly nad svou online bezpečností má asi sedmina dospělých uživatelů (Symantec Corporation, 2015) a třetina

uživatelů by podle svého vyjádření věděla, jak se zachovat v případě, že by se stali obětí kybernetického zločinu (Symantec Corporation, 2015). Terčem kybernetického útoku se přitom za svůj život staly přibližně tři pětiny dospělých uživatelů (Symantec Corporation, 2013; Symantec Corporation, 2011a; Get Safe Online, 2009). Dvě pětiny uživatelů se za poslední rok potýkaly s útokem malware, polovina uživatelů zažila finanční hrozbu (zejména ve formě phishingu), krádeži identity byla vystavena třetina uživatelů a čtvrtina uživatelů zažila pokus o prolomení účtu (Kaspersky Lab, 2015). Kompetencemi dospělých uživatelů digitálních technologií s ohledem na jednotlivé oblasti technické e-bezpečnosti se budeme zabývat v následujícím textu.

Používáním softwarových bezpečnostních prvků se zabývalo několik zahraničních průzkumů. Z nich vyplývá, že antivir používá asi devět desetin uživatelů osobních počítačů (Kaspersky Lab, 2015; Get Safe Online, 2010). Zatímco v osobních počítačích se antivir stal běžnou součástí vybavení, antivirová aplikace je nainstalována asi v polovině chytrých telefonů s operačním systémem Android a asi ve třetině telefonů iPhone (Kaspersky Lab, 2015).

Svá počítačová data zálohuje přibližně polovina uživatelů osobních počítačů (Lang et al., 2009; Symantec Corporation, 2009), podobný podíl uživatelů přiznává též navštěvování nedůvěryhodných stránek (Symantec Corporation, 2009) a asi sedmina uživatelů připouští otevírání příloh e-mailových zpráv od neznámých odesílatelů (Get Safe Online, 2009). Výzkum provedený softwarovou společností Steganos GmbH (2008) mezi uživateli v USA a Velké Británii zjistil, že čtyři pětiny uživatelů nešifrují informace v důvěrných e-mailových zprávách. Asi třetinu chytrých telefonů s operačními systémy Android nebo Microsoft Windows Phone jejich uživatelé nechrání pomocí hesla, telefony iPhone nejsou heslem chráněny asi v šestině případů (Kaspersky Lab, 2015).

Své bezpečnostní heslo od e-mailové schránky si změnila za poslední rok asi polovina jejich uživatelů v EU, podobný podíl uživatelů si změnil své heslo k účtu na některé sociální síti (TNS Opinion & Social, 2015). Podle irské studie čtyři pětiny studentů používají jedno heslo pro více služeb (Lang et al., 2009). Jak autoři studie uvádějí, tato činnost je potenciálně nebezpečná v případech, kdy uživatel zadá svou e-mailovou adresu při registraci k některé online službě a přitom použije stejné heslo, jaké používá pro přístup ke své e-mailové schránce. Garrison a Posey (2006) zmiňují, že dvě pětiny uživatelů přiznaly používání snadno odhadnutelného hesla, a asi pětina uživatelů sdílí některá svá hesla s další osobou (Symantec Corporation, 2015). Polovina uživatelů uchovává svá bezpečnostní hesla

rizikovým způsobem (například uložené v prohlížeči, v emailové schránce, v určitém souboru na disku nebo napsané na papíře) (Kaspersky Lab, 2015).

Čtyři pětiny dospělých uživatelů sociálních sítí mají svůj profil přístupný jen pro uzavřený okruh osob (Get Safe Online, 2010), asi čtvrtina osob sdílí na Internetu svá osobní data – např. telefonní číslo, e-mail (Get Safe Online, 2010). Téměř polovina z veřejně přístupných profilů na MySpace obsahuje kontroverzní informace, jako jsou fotografie zachycující uživatele při požívání alkoholu a drog nebo nevhodné explicitní komentáře (Moreno et al., 2007).

Tyto informace mohou být pro uživatele poměrně nebezpečné, neboť devět desetin amerických personalistů během přijímacího řízení prohlíží veřejné profily uchazečů o zaměstnání (Zouzalová a Madrová, 2012) a sedm desetin amerických firem připouští, že aspoň jednou odmítly uchazeče o zaměstnání na základě informací získaných o jeho osobě na Internetu (Cross-Tab, 2010). Tato problematika se týká především mladých lidí, neboť podle průzkumu společnosti AVG se asi polovina personalistů domnívá, že mladí lidé ve věku 18–25 let si neuvědomují potřebu zodpovědného chování na Internetu (Zouzalová a Madrová, 2012). Zajímavý je též názor mladých Australanů ve věku 15 až 25 let – tři čtvrtiny z nich se domnívají, že technologie jsou hrozbou pro jejich soukromí (Dooley et al., 2009). Podle anglické studie mladí lidé ve věku 16 až 24 let sdílí osobní údaje častěji než starší lidé, a proto je důležité je poučit o e-bezpečnosti (Get Safe Online, 2010).

Z výše uvedeného textu lze dovodit, že kompetence dospělých osob v technické e-bezpečnosti nejsou zcela ideální. Lze očekávat, že rodiče jsou schopni poradit dětem se základními e-bezpečnostními otázkami, avšak s pokročilými problémy by dětem měly být nápomocny odborně vzdělané osoby. Těmito osobami mohou být například učitelé, a proto se v následujícím textu budeme zabývat rolí školy při eliminaci e-bezpečnostních rizik hrozících dětem.

2.4 Role školy při předcházení e-bezpečnostním rizikům

Podle Byron (2008) nelze spoléhat, že edukaci dětí v problematice e-bezpečnosti zajistí sami rodiče, ačkoliv právě vzdělávání a trénink je základní podmínkou eliminace e-bezpečnostních rizik (Becta, 2006). Za nejlepší místo k učení dětí digitálním dovednostem potřebným k maximalizaci příležitostí a minimalizaci rizik označují Livingstone a Haddon (2009) školu. Ta by se měla zaměřit na edukaci k bezpečnosti a odpovědnosti při užívání digitálních technologií (Byron, 2008; Evropská komise, 2012) a měla by nést hlavní

zodpovědnost za vedení žáků ke kritickému myšlení a vhodnému chování, které je bude chránit před riziky při používání Internetu (Becta, 2005; Becta, 2007). Žáci potřebují pomoc školy též v rozpoznávání a eliminaci nebezpečí a tvorbě odolnosti vůči němu (South West Grid for Learning, 2009). Byron (2008) dále upozorňuje na šanci předávat prostřednictvím školy e-bezpečnostní informace všem dětem bez rozdílu.

Že k bezpečnějšímu používání Internetu dětmi a mládeží přispěje výuka ve škole, se domnívá v průměru sedm osmin rodičů v EU (The Gallup Organisation, 2008) a téměř všichni řečtí učitelé základních a středních škol (Papavasiliou, 2009). Trénink v technické e-bezpečnosti považuje za důležitý pro zlepšení svých kompetencí i většina dospělých uživatelů digitálních technologií (Gordon et al., 2004 cit. podle Teer et al., 2007).

Ve Velké Británii získávají vzdělání v e-bezpečnosti asi dvě třetiny žáků (Ofcom, 2015), někteří autoři nicméně upozorňují na skutečnost, že zejména mladší žáci vyučované problematice nerozumí (Cranmer et al., 2009). Ačkoliv většina škol hodnotí realizovaný e-bezpečnostní trénink jako pro žáky přínosný, v mnoha případech nejsou školy schopny toto tvrzení podložit konkrétními důkazy (Ofsted, 2010). K podobnému závěru došli i Livingstone a Bulger (2013), podle jejichž názoru sice existuje velké množství e-bezpečnostních iniciativ, avšak jen málo z nich bylo evaluováno z hlediska jejich efektivity.

Některé školy ve snaze o eliminaci e-bezpečnostních rizik regulují přístup žáků k Internetu, například využívají software pro blokování nevhodných webových stránek a sociálních sítí (Sharples et al., 2009). Jak však uvádí Valcke et al. (2007), takovéto intervence školy nemají vliv na rozvoj adekvátních e-bezpečnostních kompetencí žáků. Podobná restriktivní opatření mohou navíc způsobovat omezení při výuce (Sharples et al., 2009; Purcell et al., 2013), přičemž podle Steeves (2012) tímto škola znemožňuje žákům potkat příležitosti potřebné ke kritickému hodnocení obsahu. Podle vyjádření Federal Communication Comission (2012) sociální sítě nespadají mezi stránky, které by bylo potřeba blokovat, a je třeba naopak žáky vést k vhodnému využívání těchto technologií. Sociální sítě jsou některými výzkumníky přímo považovány za technologie vhodné ke vzdělávání či podpoře vzdělávání (Maranto a Barton, 2010; Lim a Richardson, 2016).

Na základě výše uvedeného textu je patrné, že důležitější než používání blokovacího software je edukace žáků. Papavasiliou (2009) ve svém šetření zjišťoval, kdo a v jakých předmětech by měl vyučovat e-bezpečnost a jaké oblasti e-bezpečnosti by měly být zahrnuty do této výuky. Tři čtvrtiny oslovených učitelů se domnívají, že o e-bezpečnosti by měli

vzdělávat učitelé ICT, a jako nejvhodnější předmět byl nejčastěji označen předmět zaměřený na výuku ICT. Podle britského výzkumu se v tomto předmětu e-bezpečnost vyučuje na devíti z deseti škol (Barrow a Heywood-Everett, 2006). Výsledky, jaké oblasti e-bezpečnosti by měly být vyučovány podle řeckých učitelů, jsou zobrazeny pomocí grafu v Obrázku 2. V kontrastu oproti tomu čeští učitelé ICT, kteří byli ve stejné době dotazováni na důležitost témat ve výuce ICT, problematiku technické e-bezpečnosti mezi tématy výuky vůbec nezmínili (Rambousek et al., 2007)[2].

Obrázek 2: Důležitá témata výuky e-bezpečnosti dle řeckých učitelů podle Papavasiliou (2009)

2.5 Požadavky kladené na učitele v oblasti e-bezpečnosti

Jako klíčová se pro zajištění technické e-bezpečnosti dětí jeví role učitele. Na učitele jsou v rámci této problematiky kladeny požadavky nejen v oblasti vzdělávací, ale také výchovné. Od učitelů se tak očekává, že budou žákům dobrým příkladem v oblasti ochrany svého soukromí, zálohování dat, antivirové ochrany nebo dodržování autorských práv (Buettner et al., 2002; International Society for Technology in Education, 2008). Bez speciální přípravy však učitelé patrně nebudou mít významně vyšší kompetence než běžní uživatelé digitálních technologií – proto by nositeli e-bezpečnostní gramotnosti na školách měli být nově dostudovaní učitelé a stávající učitelé by měli být v problematice vhodně

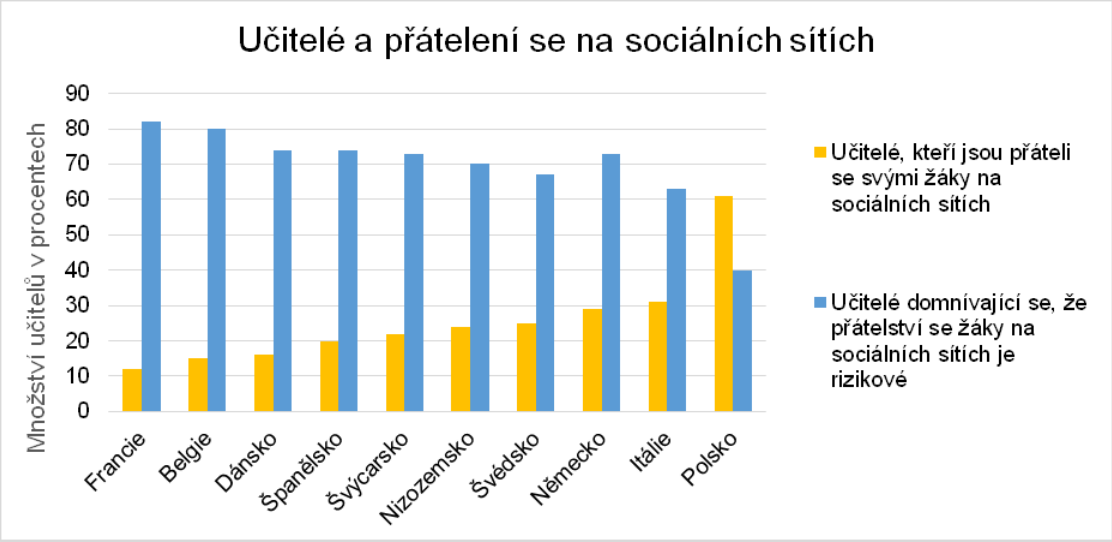
[2] Ačkoliv jde vesměs o osm až deset let staré výzkumy, kdy na e-bezpečnost nebyl v České republice kladen takový důraz jako dnes, je zde vidět rozdíl v přístupu k tomuto tématu u nás a v zahraničí.

proškoleni (Byron, 2008). Pro zajištění dostatečných kompetencí v této oblasti by měli studenti pedagogických škol projít tréninkem zaměřeným na problematiku e-bezpečnosti a toto téma by se mělo pro ně stát součástí povinného ICT testu (Byron, 2008).

2.6 Stav aktuálního poznání kompetencí učitelů v oblasti e-bezpečnosti

I přes důraz kladený na učitele nebyly kompetence učitelů v oblasti e-bezpečnosti doposud nijak výrazněji zkoumány. Je potřeba realizovat výzkumy zaměřené právě na učitelovu e-bezpečnostní gramotnost (Livingstone a Haddon, 2008) a na jeho schopnost o těchto tématech vyučovat (Spielhofer, 2010). Důležité je též objasnit, jakou podporu učitelé k výuce tohoto tématu potřebují (Spielhofer, 2010). Výzkumy, které se učiteli zabývaly, jsou směřovány především do problematiky působení učitelů na sociálních sítích.

Část učitelů nemá v problematice ochrany soukromí online dostatek osobní zkušenosti, neboť například nikdy nenavázali vztah s jinými uživateli v online prostoru (Chou a Peng, 2011). Svůj profil na sociálních sítích mají přibližně tři čtvrtiny učitelů (Seaman a Tinti-Kane, 2013; Purcell et al., 2013) a asi dvě pětiny učitelů využívají sociální sítě ve své výuce (Seaman a Tinti-Kane, 2013). Podle celosvětového průzkumu firmy Symantec Corporation (2011a) se v roce 2011 na sociálních sítích přátelila se svými žáky asi třetina učitelů, přátelství mezi žáky a učiteli na sociálních sítích vnímaly jako rizikové dvě třetiny učitelů (Symantec Corporation, 2011a). Situace mezi jednotlivými státy byla však značně odlišná; údaje pro evropské státy jsou zobrazeny na Obrázku 3.



Obrázek 3: Učitelé a přátelení se se žáky na sociálních sítích (podle Symantec Corporation 2011b)

Učitelé se mohou v online prostředí stát oběťmi urážek či napadání. Podle Phippen (2011) se asi třetina učitelů vyjádřila, že oni nebo někdo z jejich kolegů zažil takový útok. Ve dvou třetinách útoků byli do tohoto jednání zapojeni žáci, v pětině rodiče a v desetině kolegové učitele (Phippen, 2011). Podle Sharples et al. (2009) negativní zkušenost způsobenou žáky při používání Web 2.0 zažil často jeden učitel z dvaceti, občas pětina učitelů a zřídka čtvrtina učitelů.

Během času byly dokumentovány případy, kdy byl na učitelově sociálním profilu či jeho webových stránkách objeven nevhodný obsah – nevhodné komentáře, fotografie zachycující jej při požívání alkoholu a podobně (Maranto a Barton, 2010; O'Connor a Schmidt, 2015). Řada učitelů byla v důsledku podobných situací a v důsledku nevhodného přátelení se se žáky na sociálních sítích propuštěna ze svého zaměstnání (O'Connor a Schmidt, 2015). Americká učitelská organizace Ohio Education Association svým členům nařídila zrušit veškeré osobní profily na sociálních sítích jako je MySpace a Facebook, neboť by mohly být použity jako důkaz v případném disciplinárním řízení proti osobě daného učitele (Simpson, 2008).

Z výše uvedeného textu je patrné, že učitelé mají při používání sociálních sítí odlišné postavení než zbytek populace. Jako problematické se jeví především přátelení se se žáky a odhalování soukromí. Z uvedených výzkumů však není patrné, jaké důvody učitele k tomuto chování vedou. Stejně tak není známo mnoho informací o gramotnosti učitelů v ostatních oblastech e-bezpečnosti, ačkoliv jsou na ně v tomto ohledu kladeny značné požadavky.

2.7 Technická e-bezpečnost v kurikulárních dokumentech

Výuka e-bezpečnosti je též zakotvena v dokumentech týkajících se výuky ICT. Protože je však problematika e-bezpečnosti poměrně rozsáhlá, omezíme se v následujícím textu pouze na technickou e-bezpečnost. Organizace UNESCO uvádí Sociální a etické záležitosti jako jeden z devíti základních modulů výuky ICT, v jehož rámci by studenti měli porozumět problematice počítačových zločinů a podvodů, duševního vlastnictví, soukromí nebo počítačové bezpečnosti, jako jsou krádeže, hacking nebo počítačové viry (Buettner et al., 2002).

Požadavky z oblasti technické e-bezpečnosti klade na uchazeče o certifikaci také koncept ECDL. Jeho modul M1 předpokládá, že uchazeč by měl být schopen „uvědomovat si důležité bezpečnostní problémy spojené s používáním počítačů“ a „uvědomovat si

důležité právní problémy týkající se autorského práva a ochrany dat spojené s používáním počítačů“ (ECDL Foundation Ltd., 2007a). Modul M7 předpokládá, že uchazeč by měl být schopen „uvědomovat si některá bezpečnostní hlediska při používání Internetu“ a „uvědomovat si etická a bezpečnostní hlediska při používání elektronické pošty na Internetu“ (ECDL Foundation Ltd., 2007b); tyto obecné kompetence jsou v sylabech ECDL dále podrobně rozepsány.

Informace o problematice technické e-bezpečnosti lze nalézt též v českých kurikulárních dokumentech. Rámcový vzdělávací program pro gymnázia mezi očekávanými výstupy uvádí, že žák „organizuje účelně data a chrání je proti poškození či zneužití“, „posuzuje tvůrčím způsobem aktuálnost, relevanci a věrohodnost informačních zdrojů a informací“ a „využívá informační a komunikační služby v souladu s etickými, bezpečnostními a legislativními požadavky“ (Balada et. al., 2007). Požadavky uvedené v rámcových vzdělávacích programech jsou poměrně obecné, konkrétnější požadavky je možno nalézt v návrzích katalogů požadavků k maturitní zkoušce z informatiky z roku 2010, především pak v tematickém celku Člověk, společnost a počítačové technologie (CERMAT, 2010). Zde jsou společně s předpokládanými praktickými dovednostmi (např. „žák dovede chránit svá data před ztrátou, zálohovat svá data“) uvedeny také očekávané teoretické znalosti (např. „žák dovede vysvětlit potřebu aktualizací operačního systému a aplikačních programů“).

2.8 Shrnutí

Vzhledem k významnosti tématu technické e-bezpečnosti, požadavkům kladeným na školu (a tedy učitele, zejména učitele ICT) v této oblasti a neustálému vývoji v ní se ukazuje jako nutnost, aby byl učitel ICT v této problematice odborníkem. V České republice je však ve svém oboru vysokoškolsky vzdělána méně než třetina učitelů ICT působících na druhém stupni základních škol (Zatloukal et al., 2014). Protože právě učitelé ICT jsou klíčovými osobami v edukaci žáků v této problematice a protože edukace je nejlepší cestou k zajištění adekvátních technických e-bezpečnostních kompetencí dětí a mládeže, je nezbytné zkoumat kompetence učitelů ICT v oblasti technické e-bezpečnosti. Konkrétně by bylo potřeba zjistit, jaké jsou současné kompetence učitelů ICT v oblasti technické e-bezpečnosti, jak jsou tyto kompetence utvářeny a jaké jsou možnosti jejich zvyšování. Tyto otázky přitom nebyly doposud nijak výrazněji zkoumány.

3 CÍLE DISERTAČNÍ PRÁCE

Na základě prostudování výše uvedené literatury jsme stanovili výzkumný problém, který zní: Jak probíhá proces utváření odborných kompetencí učitelů ICT v oblasti technické e-bezpečnosti?

Konkrétním rozpracováním uvedeného výzkumného problému byly stanoveny celkem tři základní výzkumné cíle:

1. Zmapování stávajících odborných kompetencí učitelů ICT v oblasti technické e-bezpečnosti a vlivů, které na ně působí.
2. Analýza významných faktorů, které uvedené kompetence učitelů ICT determinují, a objasnění procesu utváření uvedených kompetencí.
3. Návrh, vytvoření a evaluace nástroje, jehož účelem je zvyšovat uvedené kompetence a který bude vycházet z přechozích zjištění výzkumu.

K jednotlivým výzkumným cílům byly dále definovány výzkumné otázky:

ad 1: Jak jsou učitelé ICT s technickým e-nebezpečím srozuměni? Jaké mají v této oblasti návyky? Do jaké míry si dokáží s nebezpečím poradit? Jaké jsou zásadní vlivy na kompetence učitelů ICT v problematice technické e-bezpečnosti? Proč se učitelé ICT snaží získávat o problematice technické e-bezpečnosti nové informace?

ad 2: Jak jednotlivé faktory ovlivňující kompetence učitelů ICT v problematice technické e-bezpečnosti vzájemně interagují? Které vlivy přispívají k tomu, aby se učitelé ICT chovali podle daných e-bezpečnostních pravidel, a které vlivy tomuto chování naopak brání? Existují-li rozdíly mezi znalostmi učitelů ICT v této problematice a jejich chováním, čím jsou způsobeny? Jakou roli hrají stávající e-bezpečnostní návyky učitele ICT v utváření jeho kompetencí budoucích?

ad 3: Do jaké míry vedou nalezené postupy skutečně ke zvyšování cílových kompetencí? V jakém ohledu je vytvořený optimalizační nástroj účinnější než jiné formy výuky? Jaká jsou případná negativa tohoto nástroje?

K výzkumným cílům byly též vymezeny očekávané výstupy:

- Popis stávajících technických e-bezpečnostních kompetencí učitelů ICT a vlivů, které na ně působí.
- Teorie, jak a čím jsou uvedené kompetence determinovány.
- Ověření této teorie a také samotný optimalizační nástroj.

4 METODY ZPRACOVÁNÍ A ZPŮSOB ŘEŠENÍ

V této kapitole se zabýváme metodologickými otázkami výzkumu; kapitola je členěna podle cílů, ke kterým popisované postupy vedou. Jelikož postupy, vedoucí k naplnění prvních dvou cílů výzkumu, proběhly do jisté míry současně, uvádíme je v rámci této kapitoly společně.

4.1 Zmapování stávajících kompetencí a objasnění procesu jejich utváření

4.1.1 Volba kvalitativního nebo kvantitativního přístupu

Základním rozhodnutím v návrhu metodologie naplňování prvních dvou cílů výzkumu byla volba, zda použít kvalitativní, kvantitativní nebo smíšený přístup. Jak uvádí Ferjenčík (2000, s. 245), kvantitativní výzkum je obvykle konfirmatorní a mívá deduktivní charakter, zatímco kvalitativní výzkum je spíše exploratorní a heuristický s induktivním zaměřením. Protože jsme nenalezli žádné teorie o formování kompetencí v problematice technické e-bezpečnosti (o nedostatku vědeckých poznatků v této oblasti se zmiňují i některé zahraniční studie – viz kapitola 2.6), rozhodli jsme při naplňování prvních dvou vytčených výzkumných cílů pro kvalitativní přístup.

4.1.2 Výzkumný design

V rámci zvoleného kvalitativního přístupu jsme se dále rozhodovali, jaký použít výzkumný design. Výstup naplňující první cíl výzkumu jsme navrhli jako popisný a z tohoto důvodu jsme se přiklonili k realizaci deskriptivního výzkumu. Výstupem naplňujícím druhý cíl výzkumu je nová teorie, a proto jsme jako základní design této části výzkumu zvolili zakotvenou teorii, jež je určena právě k vytváření teorií induktivně vzniklých ze zkoumání jevů (Šeďová, 2007c, s. 84). Objasňování procesu utváření uvedených kompetencí tedy nechápeme jako popis jednotlivých jevů, ale jako vytváření obecnější teorie, která je tzv. zakotvena v datech a která postihuje vztahy mezi proměnnými (Šeďová, 2007c, s. 86).

Ačkoliv je proces sběru a analýzy dat popisovaný v této kapitole 4.1 vylíčen jako čistě lineární, použili jsme cirkulární postup výzkumu. Po sběru dat zacíleném na první část účastníků výzkumu následuje analýza těchto dat, na což navazuje další sběr dat atd. Cílem tohoto cirkulárního cyklu je možnost porovnávat nově sesbíraná data s předcházejícími a na

základě této komparace vybírat další účastníky výzkumu, případně modifikovat metody sběru dat či jejich analýzy (Šeďová, 2007b, s. 51).

4.1.3 Vzorek účastníků

Sběr dat pro naplnění prvních dvou cílů výzkumu proběhl současně, a proto je identický též vzorek účastníků, jimiž jsou samotní učitelé ICT. Tento vzorek jsme konstruovali především s ohledem na použitý design zakotvené teorie, kdy počet účastníků má reflektovat požadavek nasycenosti dat pro naplnění druhého výzkumného cíle (Šeďová, 2007c, s. 88). Výběr jednotlivých účastníků výzkumu jsme navrhli nejprve jako apriorně determinovaný, později jsme využili graduálního výběru (Šeďová, 2007b, s. 73). Mezi apriorní determinanty výběru řadíme věk, pohlaví, aprobovanost v ICT, vzdělávací stupeň školy (druhý nebo třetí stupeň), délka praxe, velikost školy a velikost obce.

Za účastníky výzkumu jsme celkově vybrali 15 učitelů ICT ze čtyř okresů, které leží ve dvou krajích České republiky. Tři z těchto učitelů byli původně vybráni jako účastníci ověřování metod sběru dat (o němž se zmiňujeme dále), vzhledem k relevantnosti získaných informací jsme se je rozhodli zařadit i do samotného výzkumu. Těmito účastníky se stali absolventi Pedagogické fakulty JČU, kteří jsou aprobovanými učiteli ICT pro střední školy a mají poměrně krátkou praxi ve školství (v době realizace ověřovací fáze tři až pět let). Další dva účastníky výzkumu jsme vybrali z okruhu známých osob na základě graduálního výběru, neboť tito učitelé prodělali negativní zkušenost v oblasti technické e-bezpečnosti[3]. Sekundárním důvodem jejich výběru byl odlišný přístup k sebevzdělávání se v oboru ICT a krátká praxi ve výuce ICT (jeden rok resp. tři roky)[4].

Další účastníky jsme vybrali mimo okruh kolegů či známých, kdy jsme aplikovali apriorně determinovaný výběr účastníků. Dva účastníky jsme vybrali z absolventů studia celoživotního vzdělávání ICT koordinátoři, který se konal na Pedagogické fakultě JČU. Tyto

[3] Informace, že tito učitelé prodělali určitou negativní zkušenost, jsme získali poměrně náhodně. V případě prvního učitele se nám o této zkušenosti (ztrátě dat) mimochodem zmínil sám učitel při nahodilém setkání. V případě druhého učitele jsme tuto informaci (o nákaze PC malwarem) obdrželi od jeho kolegy, který příběh spojený s celou situací vyprávěl svým přátelům.

[4] Tyto informace jsme v případě prvního učitele věděli, protože jsme daného učitele znali. V případě druhého učitele jsme se tyto informace dozvěděli v rámci příběhu uvedeném v předchozí poznámce pod čarou.

účastníky jsme vybrali jako sice neaprobované, ale dlouholeté středoškolské učitele ICT se zájmem o obor a další vzdělávání v něm[5].

Vzhledem k povaze výzkumu, který předpokládá značnou rozmanitost vstupních dat, jsme se rozhodli zaměřit na učitele základních škol. Oslovili jsme dva učitele, se kterými jsme již dříve spolupracovali v rámci krátkodobých školení. Společným znakem obou učitelů je výuka ve škole v menším městě. Dalšího účastníka výzkumu jsme zvolili z důvodu, že zároveň působil jako ředitel školy[6]. Následně jsme vzorek účastníků doplnili o tři učitele neaprobované v ICT, u kterých nebyly informace o navštěvování kurzů či školení týkajících se ICT. Tyto účastníky jsme zvolili především na základě jejich věku, který se pohyboval od cca 35 let do cca 65 let[7].

Poslední dva účastníky výzkumu jsme vybrali na základě graduálního výběru na základě jejich otevřenému vztahu k sociálním sítím a přátelení se se žáky v online prostředí[8].

4.1.4 Sběr dat a triangulace zdrojů dat

Sběr dat pro naplnění prvních dvou cílů výzkumu proběhl od dubna 2013 do dubna 2015. Sběr dat spočíval v individuálním setkání s každým účastníkem výzkumu, kdy jsme s každým účastníkem realizovali polostrukturovaný hloubkový rozhovor, v jehož rámci jsme účastníka požádali o vyplnění didaktického testu. Setkání jsme realizovali po dohodě s účastníkem v místě jeho působení, nejčastěji tedy ve škole, kde vyučuje. Délka každého rozhovoru činila přibližně 50–70 minut bez započtení neformálních částí na začátku a na konci setkání.

Na úvod setkání v souladu s doporučeními, která uvádí Švaříček (2007a, s. 163), proběhlo představení výzkumníka a realizovaného projektu, ujištění o anonymitě, žádost o participaci na výzkumu a žádost o souhlas s nahráváním rozhovoru na diktafon. Následovaly tzv. úvodní otázky (Švaříček, 2007a, s. 163), které byly zaměřeny na účastníkův

[5] Tyto učitele jsme požádali o účast ve výzkumu z důvodu, že podle svých slov zajišťovali výuku ICT mnoho let a měli v oblasti ICT rozsáhlé zkušenosti. Tito učitelé tak představovali protiklad k dosavadním účastníkům výzkumu, které lze označit jako spíše méně zkušené.
[6] Tuto informaci jsme zjistili při cíleném prohlížení webových stránek jednotlivých základních škol. Daný učitel byl na webových stránkách své školy uveden nejen jako učitel ICT, ale i jako ředitel školy.
[7] Seznam možných kandidátů na účastníky výzkumu jsme získali od našich přátel, kterých jsme se ptali, jací učitelé vyučovali ICT na základní škole, kde sami působili nebo kterou dříve navštěvovali.
[8] Tipy na vhodné učitele jsme získali od našich přátel, kterých jsme se na vhodné účastníky výzkumu ptali. Tyto osoby se s danými učiteli přátelily na sociální síti Facebook, a tudíž měly o jejich virtuálním životě dostatečné informace.

postoj k technické e-bezpečnosti. Hlavním smyslem těchto otázek bylo navození tématu setkání a překonání případné bariéry mezi účastníkem a výzkumníkem. Obvyklá úvodní otázka zněla: „*Co si myslíte o důležitosti problematiky bezpečnosti na Internetu?*“ Na úvodní otázky navazoval didaktický test.

Didaktický test jsme navrhli jako předstupeň rozhovoru, přínosem tohoto testu byl především počáteční vhled do kompetencí účastníka výzkumu v problematice technické e-bezpečnosti, na jehož základě jsme vedli samotný rozhovor. Vedlejším efektem testu bylo seznámení účastníka se strukturou a oblastmi e-bezpečnosti, jichž se týkal následný rozhovor. Test se skládal z osmi znalostních otázek z oblasti technické e-bezpečnosti (viz Příloha A). Jednotlivé otázky jsme navrhli jako uzavřené s jednou správnou odpovědí ze dvou až pěti nabízených. Doba vyplňování testu činila obvykle asi deset minut, odpovědi účastníka jsme okamžitě po vyplnění zkontrolovali, avšak znalosti daného účastníka jsme explicitně nehodnotili. Ačkoliv by bylo možné data vzešlá z tohoto testu kvantifikovat, vzhledem k poměrně malému vzorku účastníků jsme samostatné využití takto získaných dat odmítli. Přestože tento test lze považovat za přínosný pro počáteční vhled do kompetencí účastníků výzkumu, riziko jeho použití spočívalo v možnosti, že účastníci výzkumu mohli získat pocit zkoušení jejich znalostí. Z tohoto důvodu jsme účastníkům zdůrazňovali, že u některých situačních otázek neexistuje jednoznačně jedna správná odpověď, ale že je spíše na základě znalostí problematiky potřeba se rozhodnout pro nějakou reakci.

Po didaktickém testu následoval samotný rozhovor, vedený podle základní osnovy (viz Příloha B), která je tvořena tzv. hlavními otázkami (Švaříček, 2007a, s. 164) a která reflektuje první dva cíle výzkumu. Jak uvádí Švaříček (2007a, s. 164), hlavní otázky by měly mít deskriptivní podobu, měly by pokrývat zájem výzkumníka a zároveň by neměly omezovat nebo předurčovat odpovědi účastníků. V souladu s názorem Švaříčka (2007a, s. 168) jsme nepožívali všechny otázky během každého rozhovoru. Důvodem byl především fakt, že uvedená osnova hlavních otázek uvažovala různé varianty vedení rozhovoru, přičemž ne vždy bylo možné vzhledem ke směřování rozhovoru dané otázky využít. Kromě hlavních otázek jsme během rozhovoru vytvářeli a kladli tzv. navazující otázky, které podle Švaříčka (2007a, s. 168) dodávají rozhovoru hloubku. Tyto otázky by měly pomáhat badateli pochopit význam řečeného nebo jsou vedeny k myšlenkám a jevům, jež badatel na začátku výzkumu neočekával (Švaříček, 2007a, s. 168). Na závěr setkání jsme kladli tzv. ukončovací otázky, které dávaly účastníkovi možnost vyjádřit se k tématu, o kterém by ještě chtěl mluvit (Švaříček, 2007a, s. 169). Rozhovory jsme (s nezbytným souhlasem účastníka rozhovoru)

zaznamenali na digitální diktafon, ve formě počítačového souboru je přenesli do počítače a přepsali do textové podoby pro následnou analýzu. Celková doba nahrávek činila 782 minut, což po přepsání do textové podoby znamenalo asi 296 normostran textu.

Jako součást setkání jsme zařadili také pasáž, kdy jsme nechali učitele reagovat na simulovanou situaci. Učiteli jsme předložili vytištěnou e-mailovou zprávu – hoax (viz Příloha C) a jeho úkolem bylo prakticky ukázat či alespoň slovně popsat, jak by na tuto zprávu reagoval.

Protože rozhovor samotný přináší pouze jeden pohled na zkoumanou skutečnost, rozhodli jsme se začlenit do sběru dat koncept triangulace. Jak uvádí Švaříček (2007c, s. 206), při kombinaci rozhovoru s pozorováním dochází k poznání, jak se slova učitele konkrétně projevují v praxi. Jelikož se náš výzkum primárně nezaměřoval na pedagogickou činnost učitele, ale na jeho uživatelské chování, pravděpodobně by pozorování učitele při výuce (a to i výuce témat technické e-bezpečnosti) vzhledem k časové náročnosti neznamenalo výrazný posun při hledání odpovědí na výzkumné otázky. Místo toho jsme se zabývali možnostmi, jak ověřit cílové kompetence učitele mimo vyučování. Jednou z cest bylo použití výše zmíněného didaktického testu, který pomáhal zjišťovat znalosti daného učitele, a pozorování reakce učitele na nevyžádanou zprávu. Taktéž věříme, že učitelé po absolvování testu neměli tendenci své e-bezpečnostní kompetence během rozhovoru zveličovat.

V rámci triangulace výpovědí učitelů jsme též vyhledávali veřejně dostupné informace o učitelově „virtuálním životě“ na Internetu, zejména pak na sociální síti Facebook. Zaměřovali jsme se na to, zda je učitel registrován na sociální síti Facebook, jaké zde veřejně prezentuje informace a zda má žáky mezi svými přáteli. Na základě zjištěných dat jsme do rozhovoru s konkrétním učitelem začleňovali tzv. konfrontační otázky, které mohou pomoci vysvětlit případný rozpor mezi zjištěným chováním a učitelovou výpovědí během rozhovoru. Pokud se nám nepodařilo před samotným rozhovorem daného učitele na sociální síti Facebook nalézt a během rozhovoru se učitel vyjádřil ve smyslu, že je na sociální síti aktivní, snažili se jej na sociální síti Facebook dohledat alespoň následně.

4.1.4.1 Ověření metod sběru dat předvýzkumem

V březnu a dubnu 2013 jsme realizovali ověřovací fázi výzkumu (předvýzkum), která měla za cíl ověřit srozumitelnost didaktického testu a jasnost a jednoznačnost otázek kladených v rámci rozhovoru. Jak jsme již uvedli výše, během předvýzkumu jsme postupně

oslovili tři absolventy Pedagogické fakulty JČU, kteří jsou aprobovanými učiteli ICT s poměrně krátkou praxí ve školství.

Jednotliví účastníci nejprve vyplnili didaktický test a poté proběhla krátká diskuze nad tímto testem. Účastníky jsme požádali, aby se vyjádřili ke svým odpovědím a určili, zda váhali nad správnou odpovědí a případně z jakého důvodu. Jejich komentáře jsme rozdělili do dvou kategorií: na komentáře týkající se formulace otázek a odpovědí a na připomínky týkající se jednoznačnosti výběru správné odpovědi. Zatímco konstruktivní komentáře zaměřené na formulaci otázek a odpovědí jsme zapracovali v plném rozsahu, připomínky týkající se jednoznačnosti výběru správné odpovědi u situačních otázek jsme nezapracovávali. Dospěli jsme k názoru, že tento test není klasickým didaktickým testem, ale vzhledem k situační povaze některých úloh se blíží dotazníku předkládajícímu účastníkovi hypotetické situace a očekávajícímu adekvátní reakce. Pokud účastník vybral odpověď, která nás zaujala, během následného rozhovoru jsme se jej dotázali, proč zvolil právě tuto odpověď. Domníváme se, že tímto přístupem jsme byli schopni získat hlubší vhled do účastníkových kompetencí než v případě didaktického testu sestaveného pouze z otázek s jednou jednoznačně správnou odpovědí.

Jeden z účastníků při vyplňování didaktického testu „přemýšlel nahlas“, jakou odpověď zvolit, čímž byla eliminována potřeba se dodatečně ptát, proč danou odpověď zvolil. Na základě této zkušenosti jsme další účastníky výzkumu začali povzbuzovat, že pokud chtějí během vyplňování didaktického testu „přemýšlet nahlas“, je to pro nás žádoucí.

Otázky kladené účastníkům během vlastního rozhovoru byly pro účastníky srozumitelné a jejich odpovědi se týkaly témat, na která byly dané otázky zaměřeny. V odpovědích účastníků na výzkumné otázky jsme identifikovali dva faktory, které je ovlivňovaly ve smyslu bezpečného chování v jednotlivých oblastech technické e-bezpečnosti. Jedním z nich byla negativní zkušenost při nedodržení e-bezpečnostních pravidel a druhým byla určitá nedůvěřivost jedince vůči neznámým jevům v reálném i virtuálním světě. Jelikož byly tyto dva faktory velice obecné, zkoumali jsme jejich povahu a vliv formou doplňujících otázek i u dalších účastníků výzkumu.

Část rozhovoru založená na předložení poplašné zprávy nás překvapila názorem některých účastníků, že na pravdivosti této zprávy nezáleží. Tento postoj souvisel s obsahem zprávy: Domnívali se totiž, že zdravotním rizikům, která s sebou nese používání průmyslových výrobků, se nelze bránit, a proto je ověřování pravdivosti této zprávy bezpředmětné. Abychom přesto zjistili, jak by tito účastníci pravdivost poplašných zpráv

ověřovali, vypracovali jsme druhou variantu zadání této úlohy. Ta je založena na předpokladu, že o ověření pravdivosti této zprávy účastníka požádal někdo blízký, jenž se popisovaných zdravotních rizik obává.

Provedený předvýzkum splnil podle našeho názoru svůj cíl, spočívající v otestování nástrojů, které jsme posléze použili při sběru dat v samotném výzkumu. Po proběhnutí této fáze jsme provedli reflexi, na jejímž základě jsme precizovali otázky v didaktickém testu i otázky kladené v rámci rozhovoru (například jsme upravili znění výše uvedené úlohy týkající se poplašné zprávy) a následně jsme zahájili sběr dat samotného výzkumu.

4.1.5 Analýza dat

Analýzu zjištěných dat jsme založili na metodě otevřeného kódování. Jak doporučuje Šeďová (2007a, s. 212–214), analyzovaný text jsme rozdělili na jednotky (slova, sekvence slov, věty) a těmto jednotkám jsme přidělili kód, který vystihuje určitý typ vyjádření a odlišuje jej od ostatních. Při volbě kódu bylo klíčové se rozhodnout, jaký jev či jaké téma daná pasáž reprezentuje, a to s ohledem na danou výzkumnou otázku. Aby bylo možno s kódy efektivně pracovat, některé ad hoc vytvářené kódy jsme redefinovali tak, aby stejnou skutečnost nevyjadřovalo více vzájemně zaměnitelných kódů (Šeďová, 2007a, s. 216).

Obrázek 4: Otevřené kódování v software Atlas.ti

Při analýze dat jsme využili software Atlas.ti; způsob kódování dat v tomto programu zobrazuje Obrázek 4. Celkem jsme tímto způsobem vytvořili 434 kódů (jejich seznam je uveden v Příloze D), které jsou zakotveny v 2443 úryvcích textu.

Kódy ze vzniklého seznamu jsme následně seskupovali do kategorií podle podobnosti nebo jiné vnitřní souvislosti (Šeďová, 2007a, s. 221). K tomuto účelu jsme využili vytištěný seznam kódů vzniklý analýzou dat od několika prvních účastníků výzkumů a tento vytištěný seznam jsme rozstříhali na jednotlivé kódy. Ty jsme seskupovali na oddělené hromádky, jež utvořily základ budoucích kategorií. Následně jsme v software Atlas.ti vytvořili jednotlivé kategorie a přiřadili do nich příslušné kódy. Nové kódy vzniklé analýzou dat od dalších účastníků výzkumu jsme přiřazovali ke kategoriím obdobným způsobem. Během této fáze analýzy bylo nutné průběžně měnit význam některých kategorií, aby odpovídal i nově zařazených kódům, případně část původně kódů obsažených v určité kategorii přesunout do jiných kategorií, dvě původně různé kategorie sloučit do jediné nebo naopak jednu kategorii rozdělit na dvě odlišné. Tímto postupem jsme vytvořili výsledných 20 kategorií, které posloužily jako základ další analýzy.

4.1.5.1 Vyložení karet

Postup následující po otevřeném kódování se lišil podle výstupu, k jehož realizaci směřoval. Protože výstup naplňující první cíl výzkumu jsme navrhli jako deskriptivní, využili jsme zde techniku „vyložení karet“ (Šeďová, 2007a, s. 226). Tehdy by kategorie vzniklé skrze otevřené kódování měly být uspořádány do určité struktury a na jejím základě by měl být sestaven výsledný text, který je deskriptivním obrazem obsahu jednotlivých kategorií (Šeďová, 2007a, s. 226). V našem případě jsme nejprve jednotlivé kategorie rozčlenili na menší části (například dimenze kategorie), a bylo-li to možné, kódy spadající do těchto částí jsme uspořádali podle určitého klíče (například podle četnosti prováděné činnosti od nejčastějšího po nejméně častou). Každá kategorie pak vytvořila jednu podkapitolu kapitoly 5.1, jejímž obsahem je popis a interpretace kódů spadajících do dané kategorie (Šeďová, 2007a, s. 227).

4.1.5.2 Zakotvená teorie

Postupy vedoucí k naplnění druhého výzkumného cíle naopak předpokládaly použití designu zakotvené teorie, a proto na otevřené kódování navázalo axiální kódování. Jeho cílem bylo vytvářet spojení mezi kategoriemi a subkategoriemi pomocí paradigmatického modelu, který je popsán v (Šeďová, 2007a) na str. 232–233. Jednotlivým položkám tohoto

modelu, označeným jako Příčinné podmínky, Jev, Kontext, Intervenující podmínky, Strategie jednání a interakce, Následky, jsme přiřazovali kategorie vzešlé z otevřeného kódování. Vztahy v takto vytvořeném modelu jsme okamžitě ověřovali, zda jsou skutečně obsaženy v datech, tj. zjišťovali jsme, zda lze kódy náležící do příslušných kategorií nalézt v datech v takových souvislostech, jak je popisuje vytvářený model. Jestliže se v datech tyto souvislosti v dostatečné míře nepotvrdily, příslušný model jsme zamítli a poupravili jej tak, aby byl v datech skutečně zakotven.

Původní paradigmatický model podle Strausse a Corbinové jsme během výzkumu opustili, neboť svým charakterem neodpovídal zjištěným vazbám, a místo něj jsme navrhli nový kauzální model[9]. Je třeba poznamenat, že toto opuštění paradigmatického modelu znamenalo pouze určitou volnost při vytváření struktury modelu, metody naší práce se i nadále opíraly o design zakotvené teorie podle Strausse a Corbinové.

Během axiálního kódování jsme jednotlivé kategorie rozvíjeli z hlediska jejich vlastností a dimenzí (Strauss a Corbinová, 1999, s. 79), kdy jsme vyhledávali různé varianty jevu popisovaného v dané kategorii, a hledali jsme vztah mezi kategoriemi vytvářeného modelu na dimenzionální úrovni (tj. například že určitý typ příčinných podmínek vyvolává určitou variantu základního jevu). Prvotní důraz jsme přitom kladli na hledání rozdílů v chování a znalostech podle věku, pohlaví a aprobovanosti učitelů v ICT, vzdělávacího stupně a velikosti obce, kde působí. Posléze jsme tuto myšlenku opustili a zaměřili se na hledání rozdílů v chování a znalostech zejména ve vztahu k příčinným kategoriím identifikovaným během otevřeného kódování.

Následně jsme provedli selektivní kódování, kdy jsme vybrali centrální kategorie, k níž jsme vztáhli ostatní kategorie (Strauss a Corbinová, 1999, s. 92). Za tuto centrální kategorií jsme zvolili kategorii, která nejlépe vyhovovala z hlediska výzkumného cíle a byla v rámci výzkumu dobře propracována z hlediska svých vlastností a dimenzí. Během selektivního kódování jsme pokračovali v hledání a ověřování pravidelností mezi kategoriemi kauzálního modelu (Strauss a Corbinová, 1999, s. 97), k čemuž jsme využili systém analytických poznámek (viz dále). Důraz jsme kladli na identifikaci a analýzu procesu ve vznikající teorii,

[9] O možnosti opustit paradigmatický model vytvořený podle Strausse a Corbinové hovoří i Šeďová (2007a, s. 235).

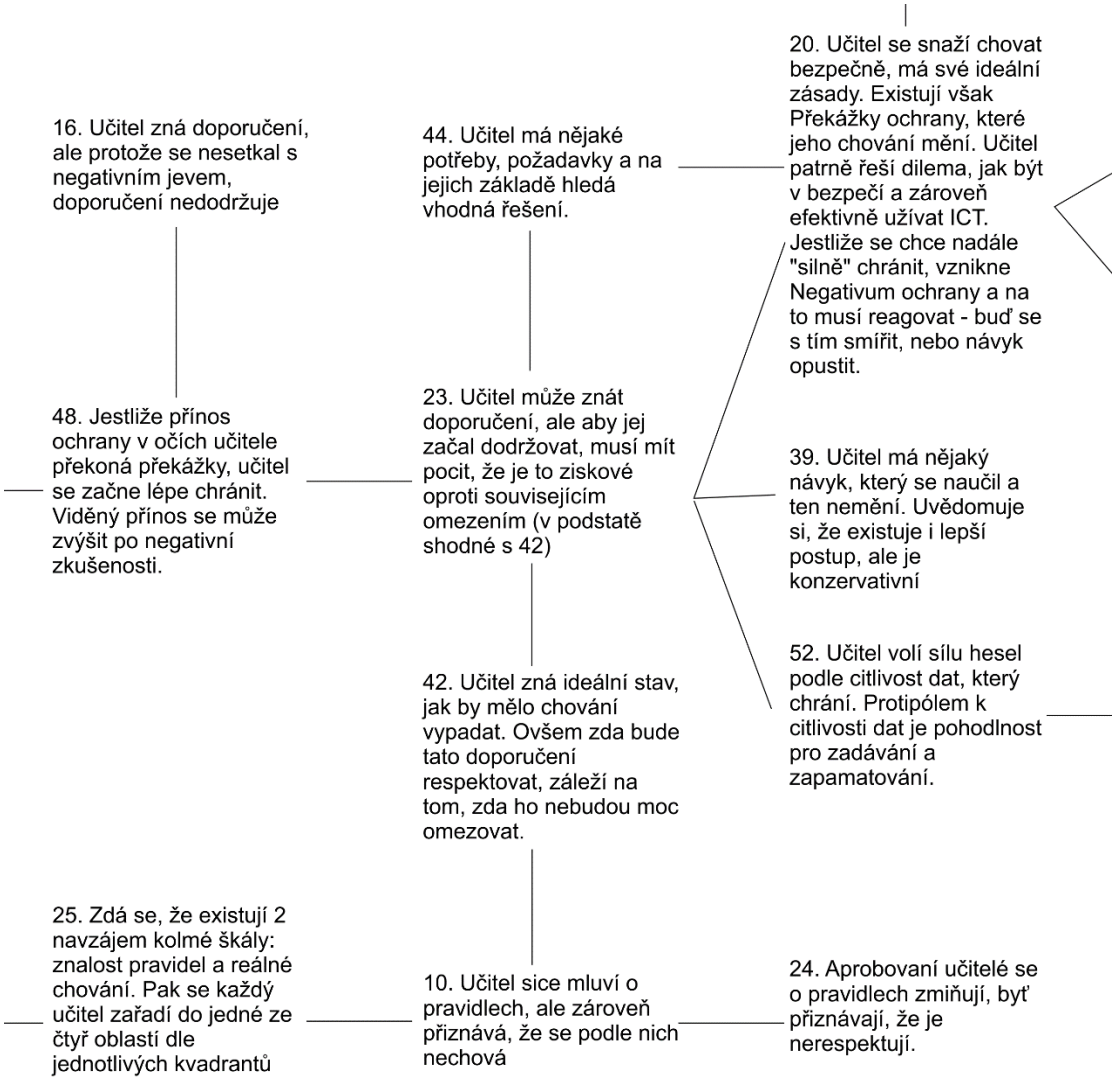
přičemž jsme se přiklonili k pojetí procesu jako neprogresivního pohybu (Strauss a Corbinová, 1999, s. 116).

Proces analýzy dat jsme podpořili tvorbou analytických poznámek (mem), které jsme vytvářeli v průběhu otevřeného, axiálního i selektivního kódování. Tyto poznámky zprvu vyjadřovaly postřehy o zajímavých vztazích mezi kódy, které jsme u daného účastníka zaznamenali (například: „*Tento učitel začal zálohovat svá data, když prodělal ztrátu dat*“). Postupně jsme je upravovali do podoby tvrzení o vztazích mezi kategoriemi, přičemž se stále vztahovaly pouze k danému účastníkovi (například: „*Učitel začne hledat lepší řešení, když původní postup zklame – prodělá nějakou negativní zkušenost*“). Během třídění jsme některé poznámky odmítli jako neověřitelné či neodpovídající cílům výzkumu, platnost ostatních jsme ověřovali v datových zdrojích vztahujících se k ostatním účastníkům.

Během této fáze analýzy jsme zjišťovali rozdíly mezi jednotlivými případy a hledali případy, které vytvořeným tvrzením odporovaly. Na základě takových případů jsme tvrzení upravovali, aby bylo možno takové případy integrovat (například: „*Učitel začne hledat lepší řešení, když původní postup zklame – prodělá nějakou negativní zkušenost. Tato změna návyků však nemusí proběhnout vždy*“). Seznam analytických poznámek z této fáze analýzy uvádíme v Příloze E.

Z revidovaných tvrzení jsme (za použití mentálních map – viz Obrázek 5) sestavili kostru analytického příběhu, která obsahuje popis jednotlivých kategorií a vztahů mezi nimi (Šeďová, 2007a, s. 239) a která vytvořila základ samotné teorie. Tu jsme dále propracovávali hledáním dalších případů v datových zdrojích a jejich ověřováním; její výslednou podobu prezentujeme v kapitole 5.2.1. Ostatní tvrzení, která by vytvořenou teorii příliš rozmělňovala, jsme uspořádali do vedlejších soustav poznatků, které prezentujeme v kapitole 5.2.2, nebo jsme je integrovali do kapitoly 5.1.

Do průběhu analýzy dat jsme začlenili princip konstantní komparace, kdy jsme se snažili provádět porovnávání v co nejvíce rovinách práce s daty, jak je uvedeno v (Šeďová, 2007a) na str. 223–224. Jak uvádí Šeďová (2007a, s. 224), dodržení tohoto principu by mělo vést nejen ke kontrole konzistence jednotlivých případů, ale též k vytvoření typologie případů a k rozpoznání podmínek, které vedou ke vzniku odlišných typů případů.



Obrázek 5: Výsek z mentální mapy, sloužící pro tvorbu kostry analytického příběhu (vytvořeno v CorelDraw)

4.1.6 Zajištění kontroly kvality výzkumu

Kromě určení metod sběru dat a jejich následné analýzy jsme definovali též postupy pro zajištění kvality výzkumu.

Při výzkumu jsme usilovali o dodržení následujících postupů:

- Využití triangulace při získávání dat – tuto techniku diskutujeme v kapitole 4.1.4.
- Vedení deníku výzkumníka, ve kterém jsme zachycovali metainformace o realizovaných dílčích částech výzkumu, pro zajištění pravdivosti a platnosti výzkumu (Švaříček, 2007b, s. 35). Zaznamenávali jsme zde především, co nás vedlo k výběru daného účastníka výzkumu, s jakými očekáváními jsme realizovali dané setkání a jak nás toto setkání ovlivnilo v dalším směřování výzkumu. Ve fázi analýzy

dat jsme deník výzkumníka nahradili systémem analytických poznámek; k jejich staršímu znění je možné se vracet prostřednictvím archivovaných verzí datových souborů projektu v software Atlas.ti.

- Zajištění transparentního výběru účastníků výzkumu (Švaříček, 2007b, s. 34) – tento výběr diskutujeme v kapitole 4.1.3.
- Zaznamenání veškerých realizovaných rozhovorů (se souhlasem daného účastníka) na diktafon a následný přepis do písemné podoby pro zajištění spolehlivosti výzkumu (Švaříček, 2007b, s. 41).
- Udržení konzistence otázek kladených účastníkům výzkumu, v čemž nám pomáhal písemný seznam těchto otázek (viz Příloha B).
- Reflexe, zda účastníci významu kladených otázek rozumí.
- Udržení konzistence při kódování dat. Jak upozorňuje Švaříček (2007b, s. 42), kódování dat provedené na počátku výzkumu může být odlišné oproti pozdější době – pro naplnění požadavku konzistence při kódování jsme tak provedli částečné opětovné kódování několika prvních rozhovorů.

4.2 Návrh, vytvoření a evaluace optimalizačního nástroje

Jako třetí cíl výzkumu jsme na základě teorie, která byla definována jako výstup naplňující druhý cíl výzkumu, navrhli a vytvořili optimalizační nástroj, jehož účelem je zvyšovat kompetence učitelů ICT v oblasti technické e-bezpečnosti. Během výzkumu jsme zjistili, že učitelé ICT obvykle potřebné e-bezpečnostní znalosti mají, avšak je v řadě případů nedodržují (viz kapitola 5.2.1.4). Dle našeho názoru by proto hlavním cílem optimalizačního nástroje nemělo být navyšování znalostí učitelů ICT, ale ovlivnění jejich postojů tak, aby e-bezpečnostní zásady skutečně dodržovali.

Jelikož dle vytvořené teorie má na e-bezpečnostní chování učitelů ICT významný vliv prodělaná negativní zkušenost, v návrhu optimalizace byla právě negativní zkušenost chápána jako jeden ze základních mechanismů pro zlepšování kompetencí. Vytvořený optimalizační nástroj bylo potřeba taktéž evaluovat z hlediska efektivity, čili bylo nutné následně provést sumativní evaluaci nástroje (Hendl, 2005, s. 293). Vzhledem k použité metodě evaluace nástroje pomocí sémantického diferenciálu (viz kapitola 4.2.2), kdy se jako důležitý jeví požadavek na velký počet respondentů zahrnutých do výzkumu, kterého bychom nebyli schopni při výzkumu zaměřeném na stávající učitele ICT nebo studenty učitelství ICT zdaleka dosáhnout, jsme se rozhodli evaluaci nástroje provést na skupině studentů neučitelského vysokoškolského studia.

4.2.1 Návrh optimalizačního nástroje

Negativní zkušenosti jakožto vlivu zprostředkovávajícího zlepšení chování učitelů ICT v problematice technické e-bezpečnosti jsme v rámci optimalizačního nástroje využili dvěma způsoby. První varianta byla založena na osobní negativní zkušenosti, kdy vyučující zprostředkoval učícímu se jedinci určitý negativní zážitek, který se jej přímo dotýkal. Druhá varianta pak pracovala s přenesenou negativní zkušeností, kdy pozvaný odborník realizoval přednášku o rizicích spojených s technickou e-bezpečností, a během této přednášky byly na konkrétních případech zachyceny příběhy lidí, s nimiž se učící se jedinec mohl ztotožnit. Zatímco první variantu jsme využili v rámci **Zážitkové výuky**, na druhé variantě byla založena **Přednáška odborníka**.

Kromě těchto dvou typů výuky založených na výsledcích výzkumu jsme pro srovnání s tradičními metodami výuky navrhli výuku technické e-bezpečnosti pomocí dalších dvou typů výuky, **Skupinové výuky** a **Frontální výuky**, a jednotlivé typy výuky jsme porovnávali v rámci následné evaluace.

Společným požadavkem na všechny typy výuky byla možnost realizace v běžné počítačové učebně na skupině deseti studentů či více, délka výuky by neměla přesáhnout dvě vyučovací hodiny, tj. 90 minut. V rámci jednotlivých typů výuky byla sice realizována rozdílná forma výuky, ale se stejným edukačním obsahem a stejný byl i cíl výuky. Tímto cílem bylo takové ovlivnění e-bezpečnostních postojů absolventů výuky, které podpoří jejich bezpečné chování při používání digitálních technologií a dodržování adekvátních e-bezpečnostní pravidel. Výuka byla zaměřena na následující témata:

- Malware, ochrana před ním
- Krádež identity, počítačová hesla
- Havárie počítačů, zálohování
- Hoax, spam, phishing a ochrana před nimi
- Sdílení osobních údajů
- SW pirátství, legalita stahování dat z Internetu
- Specifická rizika spojená s používáním mobilních zařízení

V následujících podkapitolách popíšeme návrh jednotlivých typů výuky.

4.2.1.1 Zážitková výuka

Zážitková výuka předpokládala, že student v rámci výuky podlehne předem připraveným e-bezpečnostním hrozbám, načež prožije určitou negativní zkušenost. Zatímco v případě skutečného e-bezpečnostního incidentu je jeho účinek umocněn jeho dlouhodobými následky, v případě námi připravených hrozeb jsme naopak dbali na vyloučení dlouhodobých následků, které by mohly ohrozit uživatele, jeho data či jím používané digitální technologie. Inspirovali jsme se Kolbovým modelem zkušenostního učení (Hanuš a Chytilová, 2009), podle něhož má po konkrétní zkušenosti následovat ohlédnutí a reflexe. V rámci výuky jsme tak dbali nejen na zprostředkování negativního zážitku, ale také na následnou analýzu prožité situace a jejích skutečných i potenciálních důsledků.

Připravili jsme dvě situace, které simulovaly e-bezpečnostní hrozby, s nimiž se měli studenti vyrovnat. Obě situace jsme vytvořili tak, aby student měl možnost si všimnout určitých rizikových znaků, na které by zareagoval a nebezpečí se tak vyhnul. Tento požadavek považujeme za důležitý nejen z etického hlediska, ale i proto, aby si student

uvědomil možnost volby a přijal určitou míru zodpovědnosti za to, že hrozbě podlehl. V následujícím textu popíšeme jednotlivé připravené situace.

Situace: Riziková registrace

Vytvořili jsme web nabízející materiály pro usnadnění studia (například poznámky z hodin či testy z uplynulých let). Web byl svým názvem Pirate VŠTE, vzhledem (viz Obrázek 6) i povahou materiálů zaměřen přímo na studenty, na nichž jsme realizovali pilotní ověření výuky. Zatímco několik materiálů bylo možno získat přímo, pro zpřístupnění dalších sekcí webu se měl návštěvník registrovat. Během registrace uživatel zadal svou e-mailovou adresu, zvolil nějaké heslo a odsouhlasil Podmínky používání webu. Pro dokončení registrace měla být zaslána na uvedenou e-mailovou adresu aktivační e-mailová zpráva. Ta však již zasílána nebyla a registraci tak nebylo možno dokončit.

Obrázek 6: Úvodní stránka námi vytvořeného webu Pirate VŠTE

Data uvedená při registraci se ukládala do databáze – e-mailová adresa v čitelné podobě, heslo v šifrované podobě (nejprve byl k heslu přidán určitý sufix a posléze byl z celého řetězce vytvořen hash pomocí algoritmu MD5)[10].

Studentům byla několik dnů před plánovanou výukou rozeslána jménem fiktivního studenta[11] e-mailová zpráva, ve které byli informováni, že existuje web obsahující materiály pro usnadnění studia na škole. Ve zprávě byl uveden odkaz na tento náš web.

Student si při čtení zaslané e-mailové zprávy a prohlížení webu mohl všimnout následujících rizikových znaků:

- Odesilatel e-mailu. Jako jméno odesilatele e-mailu jsme použili jméno neexistujícího studenta. Příjemce zprávy si v informačním systému školy mohl ověřit, zda daný student existuje. Určité pochybnosti mohla budit také e-mailová adresa odesilatele borec.novak@email.cz.
- Podmínky používání webu. V nich bylo uvedeno, že uživatel si je vědom, že na webu nejsou po registraci dostupné žádné další materiály k výuce. Tyto Podmínky musel během registrace každý uživatel odsouhlasit.

Situace: Nebezpečné uvádění osobních údajů

Vytvořili jsme web, který svým vzhledem napodoboval školní informační systém IS. Studentovi se po přihlášení na web zobrazila stránka, na které byl informován, že je mu nabízeno Vánoční stipendium, pro jehož získání je potřeba zadat rodné číslo (viz Obrázek 7).

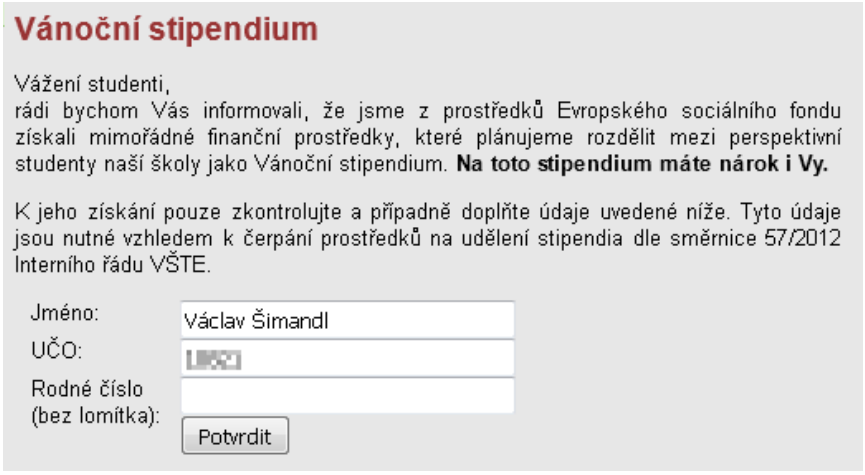
Jestliže student zadal platné rodné číslo, zobrazilo se hlášení o úspěšném provedení akce. Po několika vteřinách však byla automaticky zobrazena další stránka, na které jsme studenta varovali, že navštívená stránka je pravděpodobně podvodná[12] (viz Obrázek 8).

---

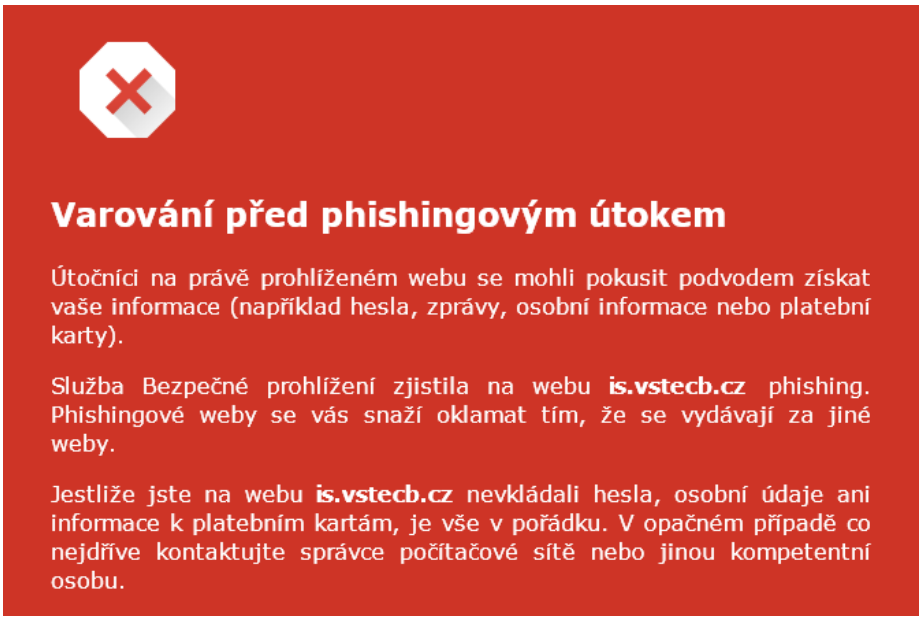
[10] Pro hashe hesel vytvořených pomocí algoritmu MD5 existují slovníky, které obsahují textové řetězce a k nim vytvořené hashe. Útočník tak může porovnat získaný hash se záznamy ve slovníku a odvodit původní heslo. Abychom tomuto postupu zabránili, přidávali jsme k heslu určitý sufix (o délce 8 znaků), aby vzniklý řetězec nebyl ve slovnících uveden. Protože vzniklý řetězec nedává smysl, nebude patrně uveden ve slovnících běžných hesel. Vzhledem k minimální délce řetězce 13 znaků (minimálně 5 znaků hesla a 8 znaků sufixu) by se takový řetězec neměl vyskytovat ani v duhových tabulkách. Funkčnost našeho opatření jsme otestovali na několika triviálních heslech (např. 12345, 12345678, password, heslo), jejichž hashe jsme zadali do specializovaných dekodérů MD5 hashů. Ani v jednom případě jsme původní řetězec nezískali a námi realizovaný postup šifrování tak považujeme za bezpečný.

[11] Že žádný takový student na dané škole nestuduje a ani nikdy v minulosti nestudoval, jsme si předem ověřili v informačním systému školy.

[12] Tato stránka svým obsahem i vzhledem napodobovala stránku, prostřednictvím které prohlížeč Google Chrome varuje uživatele před phishingovými útoky.



Obrázek 7: Výzva k zadání rodného čísla



Obrázek 8: Námi vytvořená stránka napodobující varování před podvodným webem

Z technického hlediska byla celá situace vytvořena tak, že v počítačové učebně, kde měl proběhnout tento typ výuky, byly upraveny konfigurace počítačů, aby po zadání URL adresy informačního systému školy byl uživatel přesměrován na námi vytvořený web. Zde se přihlásil pomocí přihlašovacích údajů používaných standardním informačním systémem. Ze zadaných údajů jsme ověřovali pouze uživatelské jméno, s uživatelským heslem jsme nijak nepracovali (tedy jsme jej ani neověřovali, ani např. neukládali). Uživatelské jméno bylo ověřováno proti námi vytvořené databázi studentů zařazených do daného typu výuky, čímž bylo zamezeno, aby se k webu přihlásil jakýkoliv jiný uživatel. Jestliže student vyplnil po přihlášení pole s rodným číslem, platnost tohoto rodného čísla byla ověřena na straně klienta

pomocí JavaScriptu[13]; na straně serveru nebylo s tímto číslem nijak manipulováno (tedy nebylo např. ukládáno).

Student si při práci s webem mohl všimnout několika rizikových znaků:

- Nezabezpečené připojení. Zatímco přihlašovací stránka standardního informačního systému je zabezpečená a je využíván protokol https (uživateli se v adresním řádku prohlížeče zobrazí před URL adresou název protokolu a symbol zámku), námi vytvořená stránka používala protokol http (kde název protokolu a symbol zámku chybí).
- Přidělování peněz prostřednictvím avizovaného stipendia. Nabízí se otázka, proč by student prvního ročníku, který ještě nesložil žádné zkoušky, a není tudíž evidence o jeho studijních úspěších, měl získat mimořádné stipendium. O získání stipendia by byl student pravděpodobně vyrozuměn písemně či alespoň e-mailem. Student si mohl ověřit, zda směrnice uvedená v textu existuje (tato směrnice pochopitelně neexistuje) a jaké je její případné znění.
- Požadavek na zadání rodného čísla. Rodné číslo škola od studenta získala již při zápisu do studia, je patrně zaneseno ve studentově dokumentaci, a není tak objektivní důvod jej požadovat znovu.

Návrh vyučování

V úvodu vyučování učitel studenty požádal, aby se přihlásili do školního informačního systému. Studenti se na základě upravené konfigurace počítačů v učebně přihlásili k námi vytvořenému webu, kde někteří z nich zadali své rodné číslo (čímž podlehli této hrozbě), načež jim bylo zobrazeno námi vytvořené varování před podvodnou stránkou. Učitel na vzniklou situaci reagoval, ptal se studentů na jejich činnost vedoucí k zobrazení tohoto varování a podpořil domněnku, že se jedná o phishingový útok, kdy útočníci mohli získat jejich rodná čísla. Posléze však studentům oznámil, že se nejednalo o reálný phishingový útok, ale o simulaci, při níž žádná jejich osobní a citlivá data (zejména rodná čísla) nebyla zneužita. Následovala reflexe prožité situace, při níž učitel vysvětlil princip phishingového útoku a společně se studenty na příkladu prožité situace definoval znaky, které by je od

[13] Testovali jsme, zda je zadaný textový řetězec číslem a zda je toto číslo dělitelné jedenácti beze zbytku.

zadání požadovaných dat měly odradit (tyto znaky diskutujeme výše). Na tuto fázi výuky navazoval výklad učitele o technické e-bezpečnosti.

Během výkladu učitel využíval elektronickou prezentaci, která mu sloužila jako osnova a kterou mohli studenti sledovat. Základní linie prezentace byla doplněna o nadstavbové grafické a audiovizuální materiály (snímky obrazovky, grafy a diagramy, ukázky webových stránek), které se týkaly aktuálních e-bezpečnostních problémů či hrozeb. Učitel do výkladu začleňoval prvky zpětné vazby, například kladl aktivizační otázky.

Výklad pokračoval až k oblasti počítačových hesel, kdy učitel povzbudil studenty k definování několika způsobů, jak by jiná osoba mohla odhalit jejich hesla. Poté učitel studentům zobrazil web Pirate VŠTE a stručně připomněl, že jim patrně přišla e-mailová zpráva informující o tomto webu a že se někteří z nich na webu registrovali. Následně zobrazil tabulku zadaných e-mailových adres a zašifrovaných hesel (viz Obrázek 9).

email	heslo	precetl
wertykal@	06a0545f07d42e3da845d51ada372	1
ss-h@	29f99bdeb080f4d3f0aecfdd8f81a	0
S.Hoblinka@	36aa9b12a485fcc15f549371c4812	0
Standa009@	3771eda218a9073757b9a00591acd	0
Filikarow@	3aaadec6fc32275022b1339250b07	0
Filokarow@	3aaadec6fc32275022b1339250b07	0
vincekzbytecnosti@	5350a9323a313b6429d5046512243	1
myska44444@	7d68d78fb3b0a5d0405e132cfc1ca	0
xoilx@	8ec0ac678087d11fa272149a67b78	0
certicek007@	8f72877cb586d33e90d0ab95bc170	0
poky007@	93d46433e28ae5321567714699e0b	1
17145@	983a42f2c5ae582b292a67e380875	0
Londoran@	9d0e7e5ed3d362fb7add2add2aee5	0
sramcice@	ab00902c9c97d042a97d93a4f6ba8	0
Petr1302@	ace4b3556124d1275075206031771	0
j.a.n.a.1.4@	ad3f0a7a897a51b90b1db1d96b184	0
pinzezna@	b33eb36429c1e4b4361f740342199	0
riicik@	c9dcf0b01635d6146c06b6985a2bc	1
pouzynka@	d2277f0fae7886d20ff3e5cdad4d8	0
adam.krat@	dfa301d50b93c56b3e6167b8f7529	0
BNikca3@	ffd9ddbe968070454095979739e14	0

Obrázek 9: Tabulka zadaných e-mailových adres a hashů hesel získaných z pilotního ověření výuky

Studentům vysvětlil, že tyto údaje byly získány na základě registrace na webu (tedy na základě podlehnutí této hrozbě) a oznámil jim, že zadaná hesla byla sice zašifrovaná (a nelze je dešifrovat), ale že by tato hesla mohla být sbírána v původní podobě a že by mohla být zneužita k útoku mířenému proti jejich osobě. Následovala společná reflexe a nástin zásad chování, aby se potenciální útočníci nemohli k důležitým heslům uživatele dostat. Poté následoval výklad učitele o technické e-bezpečnosti podobným způsobem, jak je popsáno výše.

Při probírání problematiky online služeb se učitel zaměřil na souhlas uživatele s podmínkami využívání služby. Vrátil se přitom k tabulce z Obrázku 9, kdy oznámil, že kolegové uvedení v tabulce se sběrem údajů souhlasili, neboť v rámci Podmínek používání webu Pirate VŠTE bylo toto uvedeno. Upozornil je, že souhlas s těmito Podmínkami studenti vyjádřili při registraci na webu nehledě na to, zda si znění Podmínek používání webu přečetli. Učitel přitom poukázal na poslední sloupec zobrazené tabulky, kde je zapsáno, kdo si stránku s Podmínkami zobrazil (hodnota 1) a kdo nikoliv (hodnota 0). Poté až do konce hodiny opět následoval výklad.

Etické otázky

Při návrhu situací simulujících e-bezpečnostní hrozby i při návrhu vyučování jsme se zabývali etickými otázkami vytvářeného řešení. Jsme si vědomi, že do určité míry došlo k oklamání studentů, kteří se tohoto typu výuky zúčastnili a stali se „oběťmi“ připravených hrozeb. Naším cílem nicméně nebylo studenty poškodit či dokonce se na nich obohatit, ale sledovali jsme pouze pedagogické a výzkumné cíle.

Se studenty byl během výuky realizován debriefing zaměřený na analýzu obou prožitých situací simulujících e-bezpečnostní hrozby. Studenti byli informováni, že se jednalo o simulace reálných útoků a byli ujištěni, že žádná jimi zadaná data nebyla, nejsou a nebudou zneužita. Dále jim byl ponechán prostor k vyjádření či dotazům nad proběhlou situací.

Obě simulované hrozby byly připraveny tak, aby při jakémkoli způsobu práce s vytvořenými weby nebyla nijak ohrožena citlivá data uživatelů.

Do obou připravených situací jsme se snažili situací zanést prvky, které měly studenty upozornit, že se jednalo o pokus o e-bezpečnostní útok (viz popis rizikových znaků jednotlivých situací).

V případě webu Pirate VŠTE byli studenti v rámci Podmínek používání webu informováni, že na webu po registraci nebudou dostupné žádné další materiály a provozovatelé webu mohou sbírat informace o uživatelích webu. Tyto Podmínky přitom uživatelé odsouhlasili během registrace.

O připravovaných situacích simulujících e-bezpečnostní hrozby jsme informovali garanta předmětu, který vzal náš experiment na vědomí, a oddělení informačních systémů školy, které s experimentem souhlasilo[14].

4.2.1.2 Frontální výuka

Návrh **Frontální výuky** vycházel z běžného pojetí této výukové metody, kdy učitel vykládá látku a studenti jej poslouchají. Během výuky učitel využíval elektronickou prezentaci, která mu sloužila jako osnova pro jeho vlastní výklad. Prezentaci zároveň mohli sledovat studenti, kterým tím bylo umožněno vnímat sdělované informace nejen sluchem, ale i zrakem. Základní linie prezentace byla doplněna o nadstavbové grafické a audiovizuální materiály (snímky obrazovky, ukázky webových stránek, grafy a diagramy, krátká videa), které se týkaly aktuálních e-bezpečnostních problémů či hrozeb a měly za cíl výklad učitele oživit a narušit tak relativně stereotypní běh hodiny.

Výuku učitel nepojal čistě jako svůj monolog, ale začlenil do ní prvky zpětné vazby a dialogu. Studenům kladl aktivizační otázky, jak se v problematice e-bezpečnosti chovají (např. kolik používají bezpečnostních hesel), a podněcoval je, aby sami definovali některá e-bezpečnostní pravidla (např. jaká kritéria by mělo splňovat bezpečnostní heslo) a případně o nich krátce diskutovali.

4.2.1.3 Přednáška odborníka

Přednáška odborníka byla založena na vyprávění odborníka o problematice technické e-bezpečnosti. Důraz byl kladen na neformálnost výuky, kdy studenti mohli odborníka kdykoliv přerušit, zeptat se jej na nějakou podrobnost, říci vlastní zkušenost týkající se vysvětlované tématiky a podobně. Odborník pojal svou přednášku co nejvíce popularizačně a zaměřil se na nejzávažnější hrozby a jejich typické projevy. Naopak se nesnažil

[14] S tímto oddělením jsme při realizaci simulace hrozby založené na napodobení školního informačního systému spolupracovali – jeho úkolem bylo dočasně upravit konfiguraci počítačů v učebně, kde se konala výuka.

vyjmenovávat přesné definice pojmů, předávat studentům co nejvíce faktů nebo klasifikovat všechny varianty hrozby a jejich následky.

Během své přednášky odborník používal příběhy ze své zkušenosti, kdy se zaměřil nejen na příčiny a projevy dané situace, ale také na její důsledky. Tím se snažil navodit atmosféru, ve které by se studenti mohli s postavami vyprávěných příběhů ztotožnit a v ideálním případě se z jejich chyb sami poučit. Zároveň se studenty diskutoval, z kterých projevů dané situace je možné odvodit, že se jedná o rizikovou situaci, a jak se při zpozorování těchto projevů zachovat.

Příkladem výše uvedeného přístupu budiž využití dat získaných v rámci **Zážitkové výuky** z webu Pirate VŠTE. Tehdy studenty stručně uvedl do situace, ukázal jim úvodní stránku webu (viz Obrázek 6) a tabulku získaných e-mailů a šifrovaných hesel (viz Obrázek 9). Osoby, které se na webu registrovaly, přitom nezesměšňoval a mírnil i případné posměšky studentů. Cílem příkladu bylo studenty varovat, jak snadné je podlehnout takovému útoku a nechat studenty uvědomit si, jak by se ve stejné situaci zachovali oni.

Odborník studenty aktivizoval pomocí otázek, jak se v určité oblasti e-bezpečnosti studenti sami chovají (např. jak zálohují svá data) či zda mají s probíranými riziky vlastní zkušenost (např. zda někdy ztratili svá data). Podle reakcí studentů přizpůsoboval svůj další výklad a případně nechal studenty o tématu krátce diskutovat s následným shrnutím nejdůležitějších informací.

Odborník během své přednášky nepoužíval elektronickou prezentaci, neboť by jej omezovala v možnosti zaměřovat se na témata, na která studenti reagovali pozitivně (viz předchozí odstavec), a naopak se jen stručně zmínit o tématech, která studenty očividně nezaujala. Pro klíčové okamžiky své přednášky měl připraveny adekvátní materiály (ukázky webů, které mohou pomoci zvládnout hrozbu, snímky obrazovky zachycující rizikové situace a podobně), které promítal.

Důraz byl kladen na vstup odborníka do výuky, kdy jej obvyklý vyučující představil jako odborníka na e-bezpečnost, který přišel studentům povyprávět o problematice a zároveň je ochoten s nimi diskutovat či zodpovídat jejich dotazy. Sám odborník po

představení uvedl jako důvod své návštěvy určitou aktuální hrozbu[15], na základě které přišel studenty poučit o problematice.

4.2.1.4 Skupinová výuka

Při návrhu **Skupinové výuky** jsme úzce spolupracovali s vyučujícím, který později realizoval pilotní ověření jednotlivých typů výuky. Tento učitel již měl se skupinovou metodou výuky dřívější zkušenosti, a tak postupy práce uvedené v této kapitole jsou spíše jeho know-how než naše.

Skupinová výuka byla navržena tak, aby studenti byli po většinu výuky aktivní – například vyhledávali informace na Internetu, zpracovávali je a výstup této analýzy prezentovali ostatním studentům. Tím se tento typ výuky odlišoval od ostatních navržených typů výuky, kdy byli studenti po většinu času pasivní.

Na začátku výuky učitel studenty informoval, že tento výukový blok bude věnován problematice počítačové bezpečnosti. Posléze proběhl brainstorming, během kterého měli studenti uvést příklady oblastí, které lze do této problematiky zařadit. Učitel nápady zapisoval na tabuli a následně ve spolupráci se studenty proběhla selekce, které oblasti skutečně do cílové problematiky patří. Jestliže byla některá oblast opomenuta, učitel ji do vzniklého seznamu doplnil.

Poté byli studenti rozděleni do skupin po třech až čtyřech členech a každé skupině bylo přiděleno jedno téma z problematiky e-bezpečnosti (například Hoax, phishing a spam – odhalení, reakce; PC hesla – výběr, uchovávání, změna; Zálohování dat – výhody, způsoby, četnost), o kterém měla vytvořit krátkou ústní prezentaci, s níž následně vystoupila před ostatními studenty. Na práci bylo vyhrazeno přibližně 45 minut času, studenti mohli využívat Internet a hledat zde patřičné zdroje podle svého uvážení. Učitel obcházel jednotlivé skupiny, podněcoval je ke spolupráci, pomáhal studentům, kteří si nevěděli rady, a případně je naváděl správným směrem, odklonili-li se zjevně ve svém snažení od zadaného tématu. Samotné vyhledání zdrojů a zpracování informací však nechal na studentech.

Následovala prezentace témat zpracovaných jednotlivými skupinami, kdy na prezentaci každého tématu bylo vyhrazeno asi 5 až 10 minut. Skupiny měly možnost využít při

[15] V případě pilotního ověření výuky to bylo asi týden staré napadení školní počítačové sítě virem CryptoLocker, které způsobilo omezení ve výuce.

prezentování i dataprojektor a předpokládalo se, že do prezentování tématu se zapojí každý člen skupiny. Učitel posléze doplnil důležité informace, které daná skupina opomněla zmínit, a uvedl vybrané zajímavosti či novinky vztahující se k tématu s cílem téma odlehčit.

4.2.2 Evaluace optimalizačního nástroje

Navržený a vytvořený evaluační nástroj, jehož účelem bylo zvyšovat kompetence učících se osob v technické e-bezpečnosti, jsme evaluovali z hlediska jeho efektivity. Během evaluace jsme se zaměřili změny postojů učících se osob v oblasti technické e-bezpečnosti.

4.2.2.1 Design evaluace

V rámci evaluace optimalizačního nástroje z hlediska jeho efektivity jsme se rozhodli pro pedagogický experiment. Za nezávisle proměnnou v tomto experimentu (Ferjenčík, 2000, s. 87) jsme považovali určitý typ výuky problematiky technické e-bezpečnosti a za závisle proměnnou postoj respondentů k této problematice[16]. Jako výzkumný nástroj jsme použili sémantický diferenciál, pomocí něhož jsme měřili vnímání vybraných pojmů týkajících se technické e-bezpečnosti.

Během experimentu jsme kromě experimentálních skupin, kde proběhla výuka technické e-bezpečnosti pomocí vybraného typu výuky, vytvořili kontrolní skupinu respondentů (Ferjenčík, 2000, s. 90), kde výuka technické e-bezpečnosti neproběhla. Experimentální skupiny byly následující:

- Skupina se **Zážitkovou výukou**
- Skupina s **Přednáškou odborníka**
- Skupina se **Skupinou výukou**
- Skupina s **Frontální výukou**

V každé skupině byl realizován nejprve pretest, následovala případná výuka a poté posttest. Samotné zjišťování působení experimentu bylo založeno na identifikaci rozdílů ve vnímání klíčových slov u respondentů experimentálních skupin před výukou (tj. v pretestu) a po ní (tj. v posttestu), přičemž bylo ověřováno, zda podobná změna ve vnímání daných klíčových slov neproběhla u respondentů kontrolní skupiny.

[16] Během experimentu jsme se záměrně vyhnuli měření vlivu výuky na znalosti respondentů, protože i přes znalost určitých e-bezpečnostních zásad se jedinec podle těchto zásad nemusí chovat (blíže viz kapitola 5.2.1.3).

Abychom lépe zachytili změny postojů u respondentů, kteří podlehli některé z námi připravených e-bezpečnostních hrozeb v rámci **Zážitkové výuky**, analyzovali jsme navíc data pro tyto podskupiny respondentů. Za podlehnutí hrozbě označujeme následující okamžiky reagování na připravené hrozby:

- Nebezpečné uvádění osobních údajů: Zadání svých přihlašovacích údajů do přihlašovacího formuláře na webu napodobujícím školní informační systém, zadání validního **rodného čísla** na tomto webu a následné spatření varování, že web je podvržený
- Riziková registrace: Registrace na námi vytvořeném webu Pirate VŠTE

4.2.2.2 Sémantický diferenciál

Sémantický diferenciál (SD) je určen k měření individuálních, psychologických významů určitých pojmů u jednotlivých osob na základě umístění těchto pojmů v tzv. sémantickém prostoru (Chráska, 2007, s. 221) a lze jej využít i k měření posunu v chápání významu těchto pojmů (Chráska, 1995). Jak uvádí Pelikán (2004, s. 144), za pomocí této metody lze pracovat i se skupinami respondentů a zjišťovat, zda existuje určitý společný jmenovatel pro pojetí vybraných pojmů danou skupinou respondentů, případně zda se od sebe určité skupiny v tomto směru liší.

4.2.2.3 Tvorba dotazníku SD

Pro měření individuálních významů pojmů jsme využili dotazníky SD, jejichž základem bylo celkem dvanáct sedmibodových posuzovacích škál (Chráska, 2007, s. 221) s krajními body určenými dvojicí přídavných jmen protikladného významu (bipolárních adjektiv). Na škálách respondenti zaznamenávali svůj postoj k patnácti posuzovaným pojmům výběrem určitého bodu na těchto škálách (Chráska, 2007, s. 221), čímž každý pojem dostal individuální význam v pojetí posuzujícího subjektu (Pelikán, 2004, s. 145).

Při výběru posuzovaných pojmů jsme se zaměřili na pojmy, které se týkají výzkumného problému (Kerlinger, 1972, s. 550), v našem případě problematiky technické e-bezpečnosti. Primárně jsme hledali takové ICT výrazy, které se nevztahují k určité konkrétní hrozbě a jsou spíše obecného charakteru. Jako tyto pojmy jsme zvolili následující výrazy:

- Soukromí
- E-mail
- Zálohování

- Heslo
- Ulož.to
- Facebook

Tento seznam jsme doplnili o dva pojmy, které se odkazují na e-bezpečnostní hrozby – Vir a Ztráta.

Abychom mohli porozumět konotativnímu významu výše uvedených pojmů v širším kontextu, rozšířili jsme seznam o ty pojmy, které přesahují problematiku technické e-bezpečnosti a jistým způsobem charakterizují samotného respondenta (Šerý, 2013, s. 20). Tyto pojmy se týkají respondenta samotného, jeho pohledu na společensky uznávané hodnoty a vzdělávání. Při jejich výběru jsme se inspirovali podobně zaměřeným výzkumem Pöschla (2005). Jako tyto pojmy jsme zvolili následující výrazy:

- Já
- Strach
- Znalost
- Život
- Práce
- Peníze
- Učitel

Při volbě bipolárních adjektiv jsme vycházeli z povahy posuzovaných pojmů (Chráska, 2007, s. 225). Jako výchozí vodítko posloužil původní seznam 50 posuzovacích škál C. Osgooda (Chráska, 2007, s. 225), který jsme doplnili adjektivy z podobně zaměřeného výzkumu M. Šerého (Šerý, 2013, s. 28). Volili jsme přitom takové dvojice adjektiv, aby dominantní faktorové náboje Hodnocení, Potence a Aktivity byly rovnoměrně zastoupeny. Zvolené dvojice adjektiv jsou následující:

- dobrý – špatný
- užitečný – neužitečný
- nezbytný – zbytečný
- jednoduchý – složitý
- těžký – lehký
- problémový – bezproblémový

- tlustý – tenký
- silný – slabý
- dynamický – statický
- horký – studený
- rychlý – pomalý
- aktivní – pasivní

4.2.2.4 Analýza dat z dotazníků SD

Předzpracování a analýzu dat získaných z dotazníkového šetření SD jsme realizovali ve spolupráci s M. Šerým při využití jím vyvinutých softwarových nástrojů. Jelikož nástroj pro analýzu dat (Šerý, 2013) obsahuje řadu voleb a nastavení, popíšeme v následujícím textu metodu práce s tímto nástrojem – byť veškeré uvedené výpočty prováděl tento nástroj automatizovaně.

Automatizovaně prováděná část analýzy dat

Analýza dat byla založena na metodě globálního hodnocení podobnosti pojmů, která podle Ferjenčíka (2000, s. 194) umožňuje posouzení, do jaké míry je možné pojmy považovat za sémanticky podobné či odlišné. Při výpočtu této tzv. D-statistiky (Kerlinger, 1972, s. 556) byla použita klasická Eukleidovská vzdálenost. Vzdálenost D_{ij} mezi pojmy i a j tak byla vypočítána podle vzorce

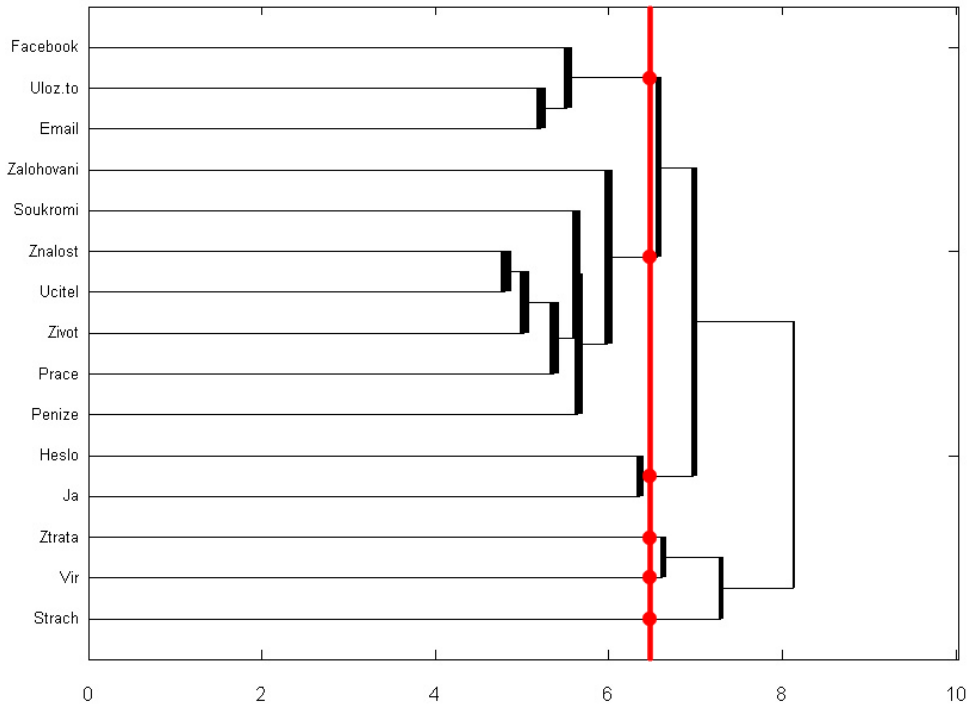
$$D_{ij} = \sqrt{\sum_{k=1}^{12} \left(x_i(k) - x_j(k)\right)^2},$$

kde $x_i(k)$ je hodnota k-té škály (tj. vybraná hodnota u k-té dvojice adjektiv) u pojmu i (podle Kerlinger, 1972, s. 556; Šerý, 2013, s. 21). Platí přitom, že čím menší je vzdálenost D_{ij}, tím jsou si dané pojmy i a j bližší svým významem a naopak (Kerlinger, 1972, s. 557). Vypočítané hodnoty vzdálenosti D byly posléze zaznamenány do symetrické D-matice (Chráska, 2007, s. 224). Při výpočtu globálního hodnocení pojmů skupinou respondentů byla vypočítána příslušná D-matice pro každého respondenta zvlášť a poté byla vytvořena výsledná D-matice s průměrnými vzdálenosti (Šerý, 2013, s. 49).

Jak uvádí Šerý (2013, s. 25), analýza globální podobnosti pojmů představuje jistou formu shlukové analýzy. Tehdy lze za objekty určené ke shlukování považovat pojmy posuzované v SD a za vlastnost, podle níž jsou objekty shlukovány, vzdálenosti v D-matici. Během analýzy byla použita metoda aglomeračního shlukování (Meloun a Militký, 2006, s. 342), kdy je na počátku algoritmu každý objekt chápán jako shluk. V každém dalším kroku jsou dva nejbližší shluky[17] spojeny v jeden jediný, čímž se postupně všechny objekty seskupí do jednoho velkého shluku (Meloun a Militký, 2006, s. 342). Tento proces postupného shlukování je graficky vyjádřen pomocí tzv. dendrogramů (Šerý, 2013, s. 25). Vytvořením dendrogramů byla zakončena část analýzy dat, prováděná pomocí softwarových nástrojů, a další analýza již byla založena na individuální práci výzkumníka.

Ručně prováděná část analýzy dat

Samotná analýza podobnosti pojmů byla založena na sledování, s jakými dalšími pojmy se vybrané pojmy z oblasti technické e-bezpečnosti ve vytvořených dendrogramech shlukují při určitém počtu shluků (ukázku pro šest shluků uvádíme v Obrázku 10).

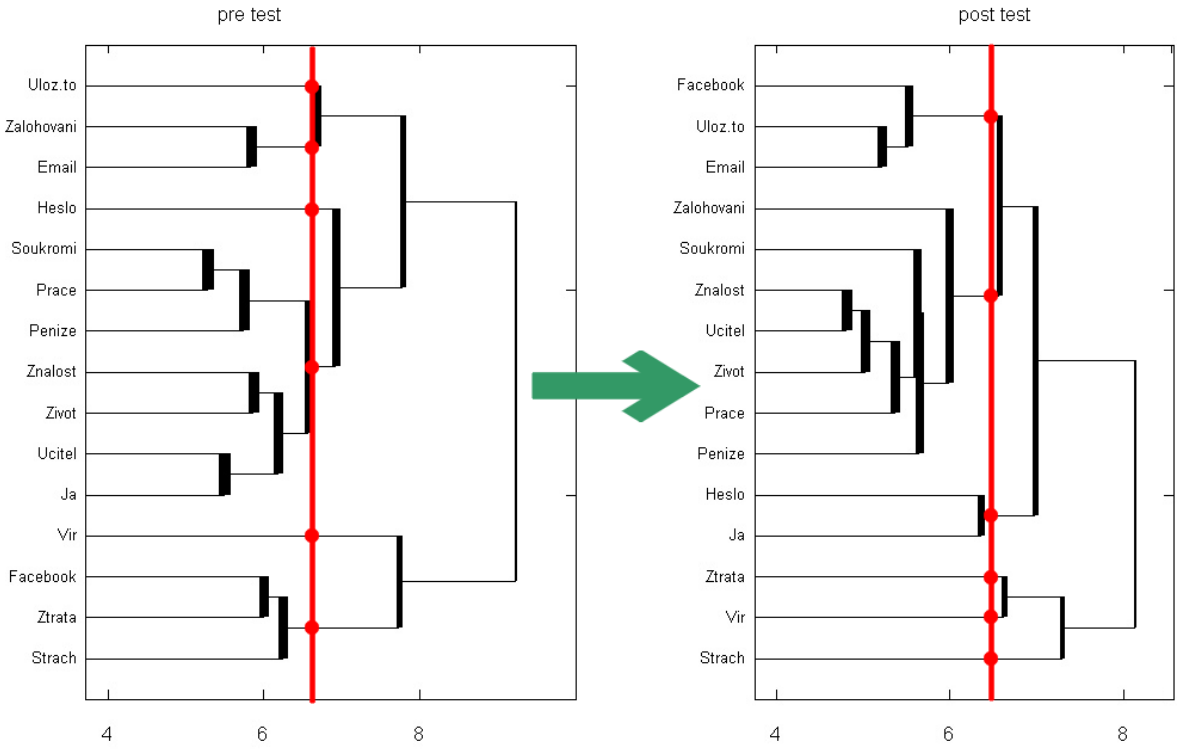


Obrázek 10: Ukázka hledání, s jakými dalšími pojmy se v dendrogramu shlukují jednotlivé pojmy při šesti shlucích. Například: Pojem Heslo se shlukuje s pojmem Já; Pojem Facebook se shlukuje s pojmy Ulož.to a Email; Pojem Vir tvoří samostatný shluk.

[17] Pro výpočet vzdálenosti dvou shluků byla použita metoda skupinového průměru (Šerý, 2013, s. 49).

Abychom byli schopni určit změnu ve vnímání pojmu, srovnávali jsme dendrogram pretestu určité skupiny respondentů s dendrogramem posttestu této skupiny, kdy jsme sledovali případné přesuny jednotlivých pojmů mezi shluky. Přesunem pojmů mezi shluky přitom nazýváme následující situace:

- V dendrogramu pretestu jsou určité pojmy při určitém počtu shluků ve stejném shluku, ale v dendrogramu posttestu jsou při stejném počtu shluků v různých shlucích.
- V dendrogramu pretestu jsou určité pojmy při určitém počtu shluků v různých shlucích, ale v dendrogramu posttestu jsou při stejném počtu shluků v jednom shluku (viz ukázka v Obrázku 11).



Obrázek 11: Přesun pojmů Heslo a Já mezi shluky při počtu šesti shluků. Zatímco v dendrogramu pretestu jsou tyto pojmy v různých shlucích, v dendrogramu posttestu jsou v jednom shluku

Pro odlišení případů, kdy k přesunu pojmů mezi shluky nedošlo vlivem výuky, ale následkem jiných faktorů (zejména přirozeného zrání respondentů), jsme vytvořený seznam přesunů pojmů pro experimentální skupiny respondentů porovnali s přesuny pojmů u kontrolní skupiny. Tehdy jsme sledovali, zda k témuž přesunu pojmů nedošlo i u kontrolní skupiny. Jestliže k přesunu u kontrolní skupiny došlo, daný přesun jsme ze seznamu přesunů u experimentální skupiny vyřadili.

Následně jsme provedli identifikaci přesunů pojmů mezi shluky, ke kterým pravděpodobně nedošlo vlivem výuky, ale vlivem abnormalit v experimentální skupině. Tehdy jsme vyhledávali přesuny, u kterých byl počáteční stav v experimentální skupině odlišný než v kontrolní skupině. Šlo o přesuny, u kterých byly při určitém počtu shluků v dendrogramu pretestu experimentální skupiny sledované pojmy v jednom shluku, ale v dendrogramu pretestu kontrolní skupiny byly tyto pojmy při stejném počtu shluků v odlišných shlucích. Analogicky šlo o přesuny, u kterých byly při určitém počtu shluků v dendrogramu pretestu experimentální skupiny sledované pojmy v různých shlucích, ale v dendrogramu pretestu kontrolní skupiny byly tyto pojmy při stejném počtu shluků v jednom shluku. Tyto přesuny jsme opět ze seznamu odstranili.

Pro vyhledání přesunů pojmů mezi shluky, ke kterým zřejmě nedošlo vlivem výuky, ale vlivem abnormalit v experimentální skupině, jsme využili ještě další postup. V tomto případě jsme vyhledávali přesuny, jejichž výsledný stav u experimentální skupiny byl stejný jako u kontrolní skupiny. Šlo o přesuny, u kterých byly při určitém počtu shluků sledované pojmy v dendrogramu posttestu v různých shlucích nejen u experimentální skupiny, ale také u kontrolní skupiny. Analogicky šlo o přesuny, u kterých byly při určitém počtu shluků sledované pojmy v dendrogramu posttestu v jednom shluku nejen u experimentální skupiny, ale také u kontrolní skupiny. Tyto přesuny jsme opět ze seznamu odstranili.

Tímto postupem jsme dosáhli stavu, kdy výsledný seznam přesunů pojmů mezi shluky obsahoval pouze přesuny, kdy počáteční rozvržení sledovaných pojmů mezi shluky bylo stejné jako u kontrolní skupiny a zároveň výsledné rozvržení sledovaných pojmů mezi shluky bylo odlišné než u kontrolní skupiny. Za přesuny ukazující na splnění cílů výuky označujeme takové přesuny pojmů mezi shluky, které dávají naději, že změny postojů v nich obsažené povedou k bezpečnějšímu chování v oblasti technické e-bezpečnosti.

4.2.3 Pilotní nasazení

Pilotní nasazení optimalizačního nástroje a jeho evaluace byly realizovány na Vysoké škole technické a ekonomické v Českých Budějovicích (VŠTE) v rámci předmětu Informatika I, který je určen studentům prvního semestru studia. Tato škola byla vybrána vzhledem k použité metodě sémantického diferenciálu, kdy se jako důležitý jeví požadavek na velký počet respondentů zahrnutých do výzkumu, kterého bychom nebyli schopni při výzkumu zaměřeném na stávající učitele ICT nebo studenty učitelství ICT zdaleka dosáhnout.

4.2.3.1 Výběr respondentů a určení skupin

Výzkum jsme naplánovali tak, abychom za respondenty mohli získat všechny prezenční studenty navštěvující předmět Informatika I. Vzhledem k tomu, že je tento předmět povinný pro všechny studenty prvních ročníků, teoreticky se měli výzkumu zúčastnit všichni prezenční studenti prvního ročníku školy (cca 750 až 800 studentů)[18].

Jelikož jsou studenti předmětu rozděleni do seminárních skupin, další práce se studenty probíhala v rámci těchto skupin. V každé seminární skupině byla naplánována výuka pomocí jednoho vybraného typu výuky (s výjimkou seminárních skupin zařazených do kontrolní skupiny, kde výuka tématu neproběhla). Počty seminárních skupin, které vytvořily jednotlivé experimentální skupiny resp. kontrolní skupinu, jsou uvedeny v Tabulce 1.

Tabulka 1: Počty seminárních skupin respondentů podle použitého typu výuky

Typ výuky	Počet skupin
Zážitková výuka	7
Přednáška odborníka	7
Skupinová výuka	6
Frontální výuka	5
Kontrolní vzorek	7
Celkem	32

Důležitým požadavkem pro zajištění vnitřní validity výzkumu je podle Ferjenčíka (2000, s. 84) vyrovnanost experimentálních skupin a kontrolní skupiny. Tento požadavek byl při našem výzkumu dodržen implicitně, neboť podle vyjádření Studijního oddělení VŠTE jsou studenti do seminárních skupin předmětu Informatika I vybíráni náhodně.

4.2.3.2 Sběr dat pretestu a posttestu

Sběr dat pretestu byl proveden přibližně v polovině zimního semestru 2014/2015. V následujících dvou týdnech po prvním dotazníkovém šetření proběhla samotná výuka a s odstupem dvou týdnů po ní proběhlo dotazníkové šetření pro posttest.

Sběr dat pretestu a posttestu proběhl vždy na počátku vyučovací hodiny. Studenti byli požádáni o participaci při vyplňování dotazníku a byli seznámeni s principem jeho

[18] Tohoto cíle v praxi nebylo možno dosáhnout, neboť řada studentů se výuky předmětu Informatika I nezúčastnila – i přes to, že je účast na výuce předmětu povinná.

vyplňování. Zejména byli upozorněni na skutečnost, že neexistuje žádná správná či špatná odpověď a že dotazníky nebudou sloužit k jejich hodnocení. Vyplňování dotazníků probíhalo na předtištěných formulářích (viz Příloha F), studenti prací strávili přibližně 20 minut.

4.2.3.3 Průběh výuky

Jeden vyučující. Abychom eliminovali vliv osoby učitele na výsledky výzkumu, byla veškerá výuka (mimo výuky založené na **Přednášce odborníka**) vedena jedním vyučujícím, kterým však nebyl sám výzkumník. Tohoto vyučujícího jsme seznámili s cílem výzkumu a požádali jej, aby se na všechny použité typy výuky připravil se stejnou pečlivostí a aby žádný typ výuky nepovažoval a priori za lepší či efektivnější, čímž jsme se snažili vyhnout sebesplňující předpovědi.

Role odborníka při výuce založené na **Přednášce odborníka** se ujal sám výzkumník. Pro toto řešení jsme se rozhodli zejména proto, že role externího odborníka se nemohl ujmout samotný učitel, kterého studenti znají. Domníváme se však, že případný důraz výzkumníka na důležitost problematiky, který by mohl ovlivnit výsledky výzkumu, je akceptovatelný. Odborník na určitou oblast zpravidla dle našeho názoru mívá v této oblasti hlubší znalosti než všeobecněji zaměřený učitel, považuje ji za důležitou a svým zaujetím pro problematiku si získává své publikum.

Hospitace nezávislého pedagoga. Abychom získali na výuku pohled nezávislý na učiteli či výzkumníkovi a zajistili tak určitou triangulaci výzkumu, pozvali jsme do vybraných seminárních skupin na hospitaci nezávislého pedagoga. Tento pedagog byl přítomen výuce pomocí každého typu výuky v jedné seminární skupině. Jeho úkolem bylo pozorovat dění během výuky, vytvořit o něm zápis a také upozornit výzkumníka na případnou nevyváženost ve snažení učitele při výuce pomocí různých typů výuky. Tento pedagog zůstal pro studenty v utajení – vcházel do učebny společně se studenty, vyučující na něj studenty nijak neupozorňoval a je tak pravděpodobné, že si jeho přítomnosti studenti nevšimli či jej (i vzhledem k jeho věku) považovali za svého spolužáka.

Hospitační zápis po skončení veškeré výuky si kromě samotného výzkumníka prostudoval i vyučující, kterého jsme požádali o vyjádření k proběhlé výuce z jeho pohledu. V následujících podkapitolách popíšeme průběh výuky v hospitovaných hodinách. Vycházíme přitom z hospitačního zápisu a z výpovědi samotného učitele. Originální znění hospitačního zápisu uvádíme v Příloze G.

Zážitková výuka

Studenti se v úvodu výuky podle pokynů učitele chtěli přihlásit do školního informačního systému, avšak byli přesměrováni na náš podvržený web, kde někteří z nich zadali své rodné číslo. Na stránku s varováním, že se stali obětí phishingu, reagovali slovy: „dnes IS nefunguje“ nebo „měl jsem radost, že jsem dostal stipendium“. Následnou informací, že stránka byla podvržena, učitel konfrontoval studenty se závažností celé situace. Po krátké reflexi zážitku učitel začal svou připravenou přednášku o možném zneužití dat, studenti byli zaujati.

Během výkladu pozornost postupně upadala, zlepšení nastalo při promítnutí tabulky e-mailových adres a zašifrovaných hesel získaných z databáze webu Pirate VŠTE. Podle zápisu si nikdo ze studentů nechtěl přiznat, že hrozbě podlehl a je v seznamu uveden.

V průběhu následující části hodiny pozornost studentů kolísala, zvýšila se při změně stylu výuky (např. při promítnutí videa, zobrazení grafu nebo aktivizačních dotazech učitele), naopak při výkladu bez interaktivních prvků klesala.

Učitel se během hodiny snažil oživovat výklad vlastními zkušenostmi, reálnými příběhy a aktualitami. Většinu času učitel věnoval výkladu, otázky studentům kladl občas a reagovalo na ně obvykle jen několik aktivnějších studentů.

Frontální výuka

Učitel na začátku hodiny studentům sdělil, že počítačová síť školy byla napadena virem CryptoLocker. Zatímco několik studentů tuto motivační část sledovalo, ostatní zůstali pasivní. Učitel využíval elektronickou prezentaci, avšak pozornost studentů se měnila podle stylu výuky. Při zobrazení videa či interaktivního grafu se zvýšila, během pasáží prezentace bez názorných grafických prvků naopak upadala. Výjimku tvořil výklad o rizicích spojených se sítí Facebook, kdy učitel studenty zaujal samotných tématem. Učitel se snažil výklad oživovat vlastními zkušenostmi a reálnými příběhy, avšak studenti jej mnohdy nesledovali. Na aktivizační dotazy si musel učitel obvykle odpovídat sám. Ke konci výuky se pozornost při výkladu o hrozbách spojených s mobilními zařízeními zlepšila.

Podle vyjádření učitele nelze výše uvedené poznatky generalizovat na všechny skupiny vyučované pomocí tohoto typu výuky, neboť sledovaná seminární skupina byla nejpasivnější a nejméně spolupracující ze všech. V ostatních skupinách byla podle jeho slov pozornost a aktivita studentů lepší, výuku ve sledované skupině označil za velmi nepodařenou.

Skupinová výuka

Učitel výuku začal brainstormingem, při němž měli studenti vymyslet seznam rizik spojených s používáním digitálních technologií. Následně studenty rozdělil do skupin a přidělil jim témata, o nichž měli vytvořit prezentaci. Ve většině skupin probíhala aktivní spolupráce, avšak někteří studenti byli pasivní a spoléhali, že práci odvedou ostatní členové týmu. Ve většině skupin probíhala diskuze k tématu, vyhledávání dalších informací na Internetu a vzájemné dotazy mezi studenty.

Veřejné prezentování výsledků práce činilo některým studentům potíže; žádná skupina nevyužila možnost projekce. Ostatní studenti obvykle dávali pozor, většinou nevyrušovali. Případné vyrušování učitel toleroval, nelze však určit, zda diskuze probíhala k tématu. Učitel po prezentaci doplňoval k tématu další informace, vlastní zkušenosti a aktuality.

Učitel během reflexe nehodnotil výuku tak pozitivně jako hospitující pedagog. Podle jeho slov studenti během brainstormingu v úvodu výuky vymysleli pouze čtyři témata týkající se e-bezpečnosti, zbytek musel doplnit sám. Během skupinové práce podle jeho názoru ve většině případů studenti nepracovali ve skupinách společně, ale v rámci skupin si práci rozdělili a každý zpracoval část tématu.

Přednáška odborníka

Odborník (dále označen jako učitel) byl na začátku semináře stálým vyučujícím představen studentům a bylo objasněno téma výuky. Učitel začal svůj výklad informací, že počítačová síť školy byla napadena virem CryptoLocker, a toto napadení uvedl jako důvod své návštěvy. Studenti byli změnou učitele zaujati, po několika minutách však přišla vlna rozptýlení, na kterou učitel reagoval aktivizačními dotazy. Jeden ze studentů byl v problematice znalejší než ostatní, měl odborné dotazy, na které se učitel snažil odpovídat. Současně s tím však klesala pozornost ostatních studentů a tato ztráta pozornosti někdy přetrvala po zodpovězení dotazu a navrácení se k původnímu tématu výkladu. I přes výše uvedenou občasnou ztrátu pozornosti přišla na konci vyučovací hodiny řada dotazů, zdálo se, že téma studenty zaujalo.

Učitel se během hodiny snažil oživovat výklad vlastními zkušenostmi, reálnými příběhy a aktualitami, kladl aktivizační dotazy. Studenti podle zápisu nad tématem přemýšleli a s učitelem diskutovali.

4.2.3.4 Počty respondentů

Celkový počet studentů, kteří byli zapsáni na předmět Informatika I byl přibližně 780. Protože se však řada z těchto studentů seminářů nezúčastňovala, počet respondentů zahrnutých do výzkumu byl 507. Při analýze dat jsme pokládali za členy experimentálních skupin ty studenty, kteří vyplnili pretest i posttest a zúčastnili se výuky tématu. Za členy kontrolní skupiny jsme považovali všechny studenty, kteří vyplnili pretest nebo vyplnili posttest a zároveň se nezúčastnili výuky tématu. Kromě studentů kontrolních seminárních skupin jsme sem tedy zařadili i studenty, kteří byli sice zařazeni do určité experimentální seminární skupiny, ale neabsolvovali některou z částí pretest – výuka tématu – posttest[19]. Počet respondentů v jednotlivých skupinách podle použitého typu výuky je uveden v Tabulce 2.

Tabulka 2: Počet respondentů v jednotlivých skupinách podle použitého typu výuky

Typ výuky	Počet respondentů pretest	Počet respondentů posttest
Zážitková výuka	58	58
Přednáška odborníka	34	34
Skupinová výuka	30	30
Frontální výuka	21	21
Kontrolní vzorek	262	142
Celkem	405	285

Počty respondentů, kteří absolvovali **Zážitkovou výuku** a zároveň podlehli námi vytvořeným hrozbám, uvádíme v Tabulce 3.

Tabulka 3: Počet respondentů, kteří podlehli námi vytvořeným hrozbám

Hrozba	Počet respondentů
Nebezpečné uvádění osobních údajů	26
Riziková registrace	15[20]
Celkem	58

[19] Z výzkumu byli vyřazeni respondenti, kteří neabsolvovali pretest, ale absolvovali výuku tématu a posttest. Ty jsme se rozhodli nezařazovat do experimentálních skupin, ale zároveň jsme je nemohli zařadit ani do kontrolní skupiny, neboť jejich posttest byl ovlivněn výukou. Počet těchto respondentů byl 38.

[20] Protože jsme nechtěli automaticky přiřazovat e-mailové adresy zadané do registračního formuláře ke konkrétním respondentům, jsou zde zahrnuti pouze respondenti, které se nám podařilo zpětně identifikovat (například se přihlásili na naši výzvu, kdo se na webu Pirate VŠTE registroval).

5 VÝSLEDKY, ANALÝZA VÝSLEDKŮ A DISKUZE

5.1 Odborné kompetence učitelů ICT v oblasti technické e-bezpečnosti a vlivy na ně působící

Na základě analýzy rozhovorů jsme identifikovali několik kategorií, které se týkají aktuálních kompetencí učitelů v oblasti technické e-bezpečnosti a procesu jejich utváření. Tyto kategorie uvádíme v abecedním pořadí:

- ***Hodnocení druhých***
- ***Konkrétní způsoby ochrany a návyky***
- ***Negativa ochrany***
- ***Posouzení dat***
- ***Překážky ochrany***
- ***Příčiny chování na sociálních sítích***
- ***Subjektivní hodnocení kompetencí***
- ***Vnější vlivy***
- ***Vnitřní vlivy***
- ***Výstupy ochrany***
- ***Vztah k e-bezpečnostním pravidlům***
- ***Vztah k ICT***
- ***Znaky nebezpečí***

Kategorie ***Konkrétní způsoby ochrany a návyky*** pak byla ještě dále rozdělena na podkategorie podle dotčené oblasti. Vznikly tak následující podkategorie:

- Průřezové způsoby ochrany
- Zálohování
- Malware a nefunkční OS
- Zabezpečení účtů
- Ochrana před nevyžádanou poštou
- Soukromí v online prostředí a používání sociálních sítí

V následujících podkapitolách se budeme zabývat popisem jednotlivých kategorií; přehled kódů vztažených k jednotlivým kategoriím uvádíme v Příloze D.

5.1.1 Vnější vlivy

Na kompetence učitelů ICT působí vlivy, které mají přímý vztah k vnějšímu světu. Rozdělujeme je do oblastí zkušenost, samostudium, organizovaná výuka a upozornění správců.

Zkušenost. Významným faktorem ovlivňujícím učitele v oblasti technické e-bezpečnosti je dřívější zkušenost, zejména osobní negativní zkušenost při nedodržení pravidel: „*Strašně mne vytrestalo to, že jsem prostě přišel o jedinečný dílo, který už nikdy zpátky dohromady nedám a do dneška neexistuje, a prostě tak jsem se začal tímhlenstím způsobem opravdu bránit. Asi kdyby se mi to nestalo, tak bych tak důslednej nebyl...*". Kromě osobní zkušenosti mohou učitele ovlivnit problémy, které se stanou blízké nebo známé osobě, nebo situace řešené při výkonu povolání, například při vykonávání funkce správce školní počítačové sítě: „*To už jsem tady zažil taky několik bezesných nocí, kdy jsem odcházel ze školy v pět ráno a myslel jsem si, že už mám všechny počítače vyčištěný, ráno to všichni zapnuli a bylo to (zavirované) znova. (...) Takže se bojím*".

Samostudium. Učitelé ICT se v oblasti technické e-bezpečnosti vzdělávají v hojné míře sami. Důležitým zdrojem jsou pro ně učebnice ICT, odborná ICT literatura a Internet, kde navštěvují odborné stránky s cílem porozumět určité problematice nebo vyřešit konkrétní problém. Jestliže nemají na toto studium dostatek času nebo se jim nepodařilo problému porozumět, nechají si někteří z nich problematiku vysvětlit od zkušenějších kolegů nebo známých ICT odborníků: „*Jednak čerpám hodně z Internetu a jednak mám okolo sebe lidi, který tomu rozuměj (...), tak se snažím ty věci pochopit sám a v nějaký fázi když nevím, oslovím třeba je*".

> **Exkurz 1.** Impulzem k bezpečnějšímu chování může být příchod nové technologie. Učitel může zjistit, že používání této technologie je cestou, jak být více v bezpečí, a začne ji vhodným způsobem používat. Následující citace ukazuje, jak učitel začal po pořízení NASu zálohovat: „*Ten NAS už mám asi čtyři roky. Předtím jsem asi nezálohoval. Možná jsem zálohoval… V zásadě asi nezálohoval, nebo jsem si to nahrál na flashku … Asi jsem nezálohoval*".

Výuka. Učitele v oblasti technické e-bezpečnosti ovlivňuje organizovaná výuka. Řada učitelů neaprobovaných v ICT si uvědomuje přínos školení a kurzů při zaměstnání, jak dokládá následující citace: „*(...) opravdu jsem si tak nějak zapsal za uši z těch různejch instruktážních přednášek a toho, že čím častěji měním heslo, tím menší pravděpodobnost, že se mi někdo do toho dostane*“. Učitelé aprobovaní v ICT se zmiňují o vlivu vysokoškolské výuky spíše okrajově, jejich výpovědi nejsou přesvědčivé a zdá se, že případná výuka tématu splynula s dalšími informačními zdroji.

> **Exkurz 2.** U jedné ze začínajících učitelek aprobovaných v ICT nás překvapilo, jak rychle a přesně vyjmenovala pravidla pro tvorbu počítačových hesel. Dotázali jsme se jí, zda tyto znalosti načerpala během středoškolského nebo vysokoškolského studia, načež učitelka uvedla: „*Ne, to jsem vyčetla až v učebnici, kterou jsem si pořídila, když jsem začala informatiku učit*“.

Jeden z učitelů aprobovaných v ICT vliv vysokoškolské výuky v této oblasti explicitně odmítl. Na náš dotaz, zda měla vysoká škola nějaký podíl na jeho současných kompetencích, uvedl: „*Rozhodně ne. (...) zrovna k tomuhle tématu, nějak si nemyslím, že by tam bylo nějak znatelný*“.

Na základě těchto zjištění se nabízí otázka, zda výuka technické e-bezpečnosti není při přípravě budoucích učitelů ICT na některých vysokých školách podceňována či přehlížena. V tom případě by tito vystudovaní učitelé ICT, stejně jako jejich kolegové v ICT neaprobovaní, byli nuceni problematiku technické e-bezpečnosti studovat dodatečně.

Upozornění správců. Jako podněty k bezpečnému chování vnímají někteří učitelé výzvy k provedení určité akce. Tyto výzvy pocházejí od správce počítačové sítě, operačního systému nebo administrátorů používaných online služeb. Jeden z učitelů například uvedl: „*Občas přijde nějaká hláška (ať si změním heslo) přímo ze školy (...), tak to provedu všude. Když už to dělám*“. Zatímco jedna část učitelů obsah těchto výzev akceptuje a snaží se podle nich chovat (viz výše uvedená citace), jiní sice výzvu uposlechnou, ale vnitřně s ní nesouhlasí: „*Třeba co se týče účtů ve škole k počítači, tak tam je automatická aktualizace (požadavek na změnu hesla) každej rok. Tam to prostě zahlásí a tam si nevyberete*“.

Náhodné příležitosti. Někteří učitelé k získání znalostí a inspirace, jak zůstat co nejvíce v bezpečí, využívají náhodných příležitostí. Příkladem jsou zprávy v médiích: „*Jsou to takový informace z médií (...) nebo v televizi řeknou, že tohle je nebezpečný, nebo i na Facebooku tam několikrát přišlo, že něco teď rozesílá policie, nějakou zprávu (...)*“. Jiným

příkladem jsou předem neplánované debaty se známými ICT odborníky. Na straně druhé však může být takovou příležitostí také výzkumný rozhovor, jak ukazuje Exkurz 3.

> **Exkurz 3.** V rámci výzkumu jsme se setkali s učitelem, který byl během rozhovoru zvídavý a na naši otázku, zda si vypracoval strategii obrany proti spamu, vypověděl: „*(...) strategii obrany nemám, protože mne to netíží. A když mne to netíží, tak to neřeším. Ale jestli něco takovýho existuje, tak povězte*“.

5.1.2 Vnitřní vlivy

Na chování učitelů ICT působí vlivy vycházející z jejich osobnosti a pohledu na svět. Při rozhodování se projevuje zejména opatrnost, důvěřivost resp. nedůvěřivost, strach, pragmatičnost či zásadovost, přemýšlivost a ohled na roli učitele, kterou nesou.

Opatrnost. Učitelé se při používání digitálních technologií snaží být opatrní, tedy nevystavovat se zbytečnému riziku. Tato opatrnost úzce souvisí s obavou z následků – učitelé se snaží chovat opatrně, aby předešli případnému incidentu. Opatrnost může působit přímo: „*Doopravdy si netroufnu mít to jedno heslo všude, ať už je to Facebook, internetová banka a tak dále*“ nebo se projevovat ve formě nedůvěřivosti: „*(Stane se, že) se dostane člověk do neznámých obchodů (...) Najde si tam kontakt, to dělám, že vjedu do kontaktů a i se podívám, jestli mají kamennej obchod (...) Takže ty beru jako důvěryhodnější (...)*“.

Obava z následků. Motivem k bezpečnému chování je obava z následků případného incidentu při nedodržení pravidel. Tato obava je u jednotlivých učitelů různě silná, zatímco někteří si dané riziko pouze uvědomují: „*Prostě tak se to stane (že se zaviruje počítač) a je potřeba nějakým způsobem se toho zbavit*“, u jiných se projevuje strach: „*I když jsem třeba zvědavej, co by tam mohlo bejt, tak to překonám. Když je tam obrázek ve formátu jpg, tak proč bych se nepodíval, ale v exe ne. To se bojím*“.

Někteří učitelé se obávají zneužití dat uveřejněných na Internetu: „*Myslím si, že tohleto člověk musí brát s tím rizikem, že můžou všechny informace, který tam (na zdi Facebooku) uvede, bejt použitý proti němu*“ a prolomení svého soukromí při neuváženém sdílení informací na Internetu: „*Nechci, aby cizí lidi viděli moje soukromí (...) Možná mám nějakou fóbii, ale nechci, aby si mne byl schopen kdokoliv najít a tam vidět, jak vypadám, jaký mám jméno, kde bydlím, jak vypadá můj barák. Nechci prostě*“. Příčinou těchto situací může být podle učitelů nejen jejich neuvážené jednání, ale také chybné zabezpečení dat proti nepovolaným osobám (proti ostatním uživatelům i hackerům) ze strany poskytovatele služby: „*Nevěřím tomu, že by to (sociální sítě) bylo natolik zabezpečený, že co tam dám*

a budu to chtít mít, aby se mi tam někdo nedostal, že skutečně se nedostane“. Výše uvedené obavy jsou zintenzívněny rolí učitele, kdy se část učitelů obává nesnází ve vztahu k žákům: „*Myslím si, že by se to (k žákům) mohlo dostat. Protože nedám to tam (na zeď Facebooku) třeba já, ale dá to tam známej známého a jeho známého a takhle*“.

U některých učitelů se projevuje obava z prolomení hesel a krádeže identity, ztráty dat uchovávaných v počítači, působení viru v počítači nebo finančního podvodu na Internetu: „*(Internetové obchody nepoužívám), jedině jsem používala z rádia Proglas a televize Noe, protože to vím, to jsou poctiví lidi a to kdyžtak jde na charitu ty výtěžky… Tam vím, že mne nepodfouknou. Jinak se toho bojím*“.

Důvěřivost vs. nedůvěřivost. Učitelé jsou často nedůvěřiví vůči neznámým subjektům (službám, webovým stránkám i osobám) v Internetu, kdy se obávají možného nebezpečí; na straně druhé obvykle důvěřují subjektům, se kterými mají pozitivní zkušenost. Nedůvěra vůči neznámým subjektům se projevuje například v neochotě důvěřovat informacím poskytovaným na neznámém webu nebo se zde registrovat výměnou za poskytnutí určitých dat. Tuto nedůvěru jsou mnohdy ochotni překonat, pokud jim osoba z jejich okolí poskytne o dané službě pozitivní reference: „*Pokud byste s tím měl zkušenost, že opravdu Vám to dali, a že Vás potom neotravovali (...), tak bych asi do toho šel*“ nebo jestliže se provozovatel dané služby akceptovatelným způsobem zavazuje k ochraně osobních dat: „*Věřím tomu, když tam napíšou, že účty potřebujou pouze právě pro ty svoje účely a že je neposkytnou třetím stranám*“.

Někteří učitelé jsou částečně nedůvěřiví i k renomovaným službám, přičemž se obávají o kvalitu jejich zabezpečení a možného zneužití svěřených dat: „*Neukládala bych si tam (do cloudu) osobní údaje, protože stejně tak, jako jsem si z Facebooku pokusila odstranit téměř všechny fotografie a mám tam fakt jenom omezený počet, tak stejně tak bych na Google nebo Microsoftu prostě celkově nedávala vůbec žádný data*”. Na straně druhé většinou těmto službám důvěřují v tom smyslu, že svěřená data jsou ochráněna proti ztrátě či poškození.

V důvěře v technickou ochranu počítače před hrozbami (antivir, antispyware a podobně) se učitelé liší. Zatímco jedni věří, že tato ochrana případnou hrozbu zastaví: „*Důvěřuju tomu, že kdyby v tom byl nějaký virus, tak se ten antivirus prostě ozve*“, druzí jsou opatrnější a na technické řešení nechtějí bezmezně spoléhat.

Část učitelů je obezřetná i v případě neobvyklé online komunikace ze strany jejich přátel či blízkých osob, kdy se obávají podvržení či krádeže identity odesilatele: „*I kdyby mi přišel*

od nějakýho známýho exe soubor a já ho nečekal, tak napřed mu to třeba zavolám, co to je (...)“, a při využívání digitálních technologií (počítačů, počítačových sítí), které jsou spravovány neznámými osobami: „*Mám zásadu nepřipojovat se nebo nechodit na internetový bankovnictví v nějakejch sítích, který neznám (...)*“.

Role učitele. Učitelé obvykle přizpůsobují své chování tak, aby bylo adekvátní jejich učitelské profesi, což se projevuje zejména při používání sociálních sítí. Tehdy je u mnohých učitelů zřetelná snaha udržovat určitý odstup od žáků. Motivem je obava ze ztráty autority: “*Když tam uvidí ten student tam ty tvoje fotky nebo když ti může něco komentovat, tak řekněme ten odstup jakoby mizí, úplně se stírá*” a snaha oddělit práci a soukromý život: “*Nemám potřebu si s nima klábosit ve volným čase. Prostě moje práce je tady učit, tak učím, ale pořád je to jenom práce (...)*”. Zaznamenali jsme však také názor opačný, kdy se učitel snažil ke svým žákům prostřednictvím sociálních sítí co nejvíce přiblížit: „*Rád se s nimi (s žáky) bavím, chci poznat, jak se dneska v tomhle věku chovaj, jak přemejšlej. Takže (se snažím) proniknout mezi ně. To je moje taková učitelská strategie*“.

> **Exkurz 4.** Během rozhovorů jsme se setkali s učitelem, který odmítá uveřejňovat na sociálních sítích informace o své osobě. Důvodem tohoto chování je podle jeho slov obava, že by se zde publikované informace mohli dozvědět jeho žáci nebo rodiče těchto žáků – a to aniž by měl tyto osoby mezi svými přáteli. Lze říci, že tento učitel sdílí názor Ohio Education Association požadující nezveřejňování osobních informací učiteli na sociálních sítích (Simpson, 2008). Postoj tohoto učitele si zaslouží srovnání s učitelem, který na sociální síti informace ze svého soukromí zveřejňuje a zároveň se na této sociální síti přátelí se svými žáky (viz Exkurz 13).

Vědomí role pedagoga se u některých učitelů projevuje i v jejich pohledu na žákovské profily na sociálních sítích. Jsou si vědomi, že akceptováním přátelství se žáky by začali mít přímější přístup k obsahu jejich profilů s nejrůznějšími statusy. Část z nich se této situace obává kvůli možné přítomnosti nevhodných statusů, které by z pozice učitele museli začít řešit: “*On má něco napsáno na Facebooku, tak když to začnu nějak řešit, tak si mne odebere a je to stejný, jako když jsem si ho nepřidávala, a když to řešit nebudu, tak si myslím, že to není úplně v souladu s tím, kdo ten učitel je. Že ten učitel by měl ty žáky i vychovávat.*” Další učitelé tuto situaci jako problematickou nevnímají a domnívají se, že by žáci obsah svých profilů včas vhodně přizpůsobili: “*Ti studenti, když si tam dávají ty učitele, tak si uvědomí, že jsou jaksi pod kontrolou. Že ty jejich příspěvky tam někdo potom vidí (...)*”. Během

výzkumu jsme se setkali s příkladem učitele, který zjistil na profilech některých svých žáků nepřijatelné statusy, jak ukazuje Exkurz 5.

> **Exkurz 5.** V rámci zkoumání jsme se setkali s učitelem, který se na Facebooku přátelil se svými žáky, jimž je třídním učitelem. Jak učitel vypověděl, postupem času začali někteří žáci publikovat statusy s nevhodným obsahem: "*(...) i když o tom věděli, že jsme v přátelích, tak tam psali věci, o kterých mohli vědět, nebo spíš si myslím, že věděli, že neskousnu, hlavně co se týče školy a plánovali různý věci, co se bude dít na horách (...) a já nevím co*". Protože podle učitele byla záležitost závažná, odmítl ji ignorovat, čímž si tyto žáky značně znepřátelil. Zároveň se rozhodl většinu žáků z přátel odebrat. Jak učitel uvedl, řešením věci rozdělil třídu na dvě části – zatímco jedna část jeho postup akceptovala, zbylá část se začala chovat „brutálně". Na náš dotaz, jak tuto záležitost s odstupem hodnotí, odpověděl: "*Za tu zkušenost rozhodně děkuju a myslím si, že je to dobrá věc, protože (...) aspoň vím, co se všechno může stát a je to prostě pro mne ponaučení, že si musím dávat bacha s kým se, co se týče žáků, dávám dohromady*".

Role učitele se však neprojevuje jen při používání sociálních sítí. Někteří učitelé se snaží být obezřetní před svými žáky z obavy, že případná hrozba by mohla pocházet právě od těchto žáků: „*Bojím se (...) a zvlášť ve škole, protože naši současní studenti jsou hackeři. Dostanou se do hodně věcí a věřím, že i do e-mailu by se mi mohli dostat, kdyby chtěli*".

Okamžik, kdy učitel začíná poprvé učit ICT (bez ohledu na to, zda učitel vstupuje do praxe nebo doposud vyučoval jiné předměty), je pro řadu učitelů důvodem, proč se v oblasti technické e-bezpečnosti zdokonalovat: „*Když jsem začala učit, tak jsem to studovala nebo půjčila jsem si takovou bichli, snažila jsem se něco do sebe nahltit*", a toto zdokonalování průběžně během jejich praxe pokračuje: „*(...) občas mám pocit, že mám něco učit. A pokud mám něco učit, tak chci o tom něco vědět. Pak ty informace vyhledávám*". Motivací je pro ně nejen snaha porozumět určité problematice do té míry, aby byli schopni o ní vyučovat (viz předchozí citace), ale také pocit, že jako učitelé ICT by určité problematice měli rozumět: „*Samozřejmě je to pro mne motivace, abych si to dohledal, protože jsem učitel informatiky*". Specifickým projevem této potřeby rozumět určité problematice je zájem o nové trendy: „*Facebook jsem vyzkoušela jenom proto, když jsem chtěla vědět… když jsem začala učit před pár lety tu informatiku, tak abych věděla, co to obnáší*". Pro úplnost dodejme, že někteří učitelé se snaží získávat informace v problematice technické e-bezpečnosti nejen kvůli výuce či v případě řešení nějakého problému (viz kapitola 5.1.9),

ale i čistě ze zvídavosti a zájmu o problematiku: „(…) *ale i mne to baví, tak i sama, aniž vím, že to budu třeba potřebovat v tý hodině, tak si to sama zjišťuju nebo dohledávám*“.

Pragmatičnost vs. zásadovost. Zatímco někteří učitelé přiznávají, že se chovají pragmaticky, jiní tvrdí, že se chovají zásadově. Příkladem budiž registrace k neznámým online službám, kdy jedni jsou podle svých slov ochotni zadat nepravdivé údaje o své osobě: „*Tak asi kdybych ho (nějaký dokument) potřeboval, tak bych se registroval nějakým vymyšleným jménem (...)*“, zatímco druzí takové chování odmítají: „*(...) spíš si rozmejšlím, jestli vůbec tu registraci potřebuju udělat nebo ne. A když je to fakt nutný, tak většinou uvádím reálný informace (...)*“.

Přemýšlivost. Učitelé o svém jednání většinou nerozhodují formálně na základě obecně platných pouček, ale snaží se o konkrétním problému přemýšlet: „*Samozřejmě je tam ten zdravej rozum. Člověk přemejšlí, když něco dělá, na jaký stránky jde, když se ho někdo na něco ptá, tak proč se ho na to ptá (...)*“ *a* hledají svou vlastní cestu, jak naplnit své potřeby či požadavky okolí a zároveň zůstat v bezpečí: „*Třeba kolega tam (veřejně na Google+) taky dává alba z cest. Na tom mi zase nepřijde nic špatnýho, ale je to třeba si nějak rozlišit, najít si nějakou hranici*“. Mnozí učitelé zvažují také rizika svého potenciálního jednání a berou v potaz i očekávaný přínos tohoto jednání: „*Člověk musí vyhodnotit, že zadání těch údajů, speciálně telefonu, že se mu to vyplatí, za to, co dostane. (...) Že ten předpokládanej zisk je větší než předpokládanej náklad. A to, že nechám někde telefon, je náklad, protože mi může někdo zavolat (...)*“. Toto přemýšlení o určitém problému či situaci úzce souvisí se subjektivním posouzením dat, o němž se zmiňujeme v kapitole 5.1.4.

Ohled na druhé. Závěrem popisu této kategorie poznamenejme, že někteří učitelé také zohledňují potenciální dopady svého jednání na druhé osoby: *„(...) nemusím otravovat ostatní lidi věcma, který je vůbec nemusí zajímat (...)*“ nebo „*(Stalo by se, že by ten hoax) člověka nějakýho vylekal, skutečně natolik, tak by to člověk ještě vzal, jako že za to může on. Ne ten, kdo napsal tu zprávu. Prostě poslal jsem to kamarádovi a něco se přihodilo, tak to je takový těžký (...)*“.

5.1.3 Příčiny chování na sociálních sítích

Kategorie ***Příčiny chování na sociálních sítích*** se zabývá okolnostmi, které učitelé zohledňují při rozhodování, zda a jak používat sociální sítě. Patří sem zejména přínosy a překážky používání sociálních sítí v osobním životě učitele, využitelnost sociálních sítích

ve výuce, obava z rizik při používání sociálních sítí a postoj učitele. Poslední dva zmíněné faktory jsme diskutovali v předchozí kapitole ***Vnitřní vlivy***.

Přínosy používání sociálních sítí. Mezi důvody, proč používat sociální sítě, patří podle učitelů možnost soukromé komunikace, zejména pak s přáteli či příbuznými. Sociální sítě umožňují učitelům získávat informace o lidech, se kterými nejsou ve spojení: „*Když už jsem o nějakým člověku dlouho neslyšela, tak se kouknu na ten jeho profil, jestli tam o sobě nepíše něco zajímavýho*". Tento přístup někteří učitelé používají i u svých bývalých žáků: „*Vím, kde (mí bývalí žáci) jsou a když se jim narodí děti, vím, jak vypadají jejich děti a takový. Je to takový jako sraz pořád. (...)*". Část učitelů používá sociální sítě jako zdroj zábavy nebo zájmových informací: „*Já se často třeba zapojuju do diskuzí třeba tady po kraji (= v okolí) a takový. Protože tam lidi publikujou zajímavý materiály (...)".*

Skepse vůči sociálním sítím. Za hlavní překážku bránící učitelům používat sociální sítě lze označit skepsi učitelů vůči těmto technologiím. Učitelé, kteří nepoužívají sociální sítě, obvykle uvádějí jako důvod nízký zájem o tuto službu: „*Já nepotřebuju se prezentovat na Internetu. Když má někdo potřebu, tak prosím*". Někteří jsou však vůči nim značně skeptičtí, jako negativní vnímají například velkou časovou náročnost jejich používání: „*Ty děti v podstatě tráví na tom Facebooku takovýho času… Myslím, že je to na škodu, a když si myslím, že je to na škodu, tak já to nebudu používat*". Dále jsme zaznamenali názory kritizující neosobnost sociálních sítí, uveřejňování nepravdivých informací uživateli, povrchní komunikaci a nedostatek spolupráce mezi nimi. Jeden učitel například vypověděl: „*Myslím si, že ty sociální sítě neplní to, k čemu vlastně jakoby ta myšlenka prvotní byla, k tý spolupráci. Když se podíváte na ty sociální sítě, co se tam odehrává, tak si tam (uživatelé) akorát povídají (...)*".

Využitelnost ve výuce. V názoru na využitelnost sociálních sítí ve výuce se učitelé značně liší. Část z nich se domnívá, že sociální sítě by ve škole pro podporu výuky nevyužili: „*Mám pocit, že jako učitel, když se každej tejden s těma studentama vidím, tak to (sociální sítě) nepotřebuju*". Jiní spatřují v sociálních sítích komunikační nástroj, umožňující jim být dostupnými pro jejich žáky: „*(Žáci) se mne ptali na něco třeba ohledně testu, že po víkendu budeme psát písemku, tak se zeptali na podrobnosti (...)*" nebo „*Hlavně nám to sloužilo pro takovou tu komunikaci, jakože zejtra nepřijde do školy, že se omlouvá (...)*".

5.1.4 Posouzení dat

Kategorie ***Posouzení dat*** se zabývá subjektivním hodnocením cennosti a citlivosti dat, která mají být chráněna nebo jsou vystavována potenciálnímu riziku, a důvěryhodností subjektu, se kterým učitel interaguje.

Cennost dat vystihuje míru nepostradatelnosti určitých dat pro daného učitele a je obvykle vztažena k riziku ztráty těchto dat: „*(...) ty fotky z dovolenejch, ty už v životě nikdy nebude mít. To je to nejdůležitější, co jako má z toho. To je to, co má cenu prostě chránit*".

Citlivost dat vyjadřuje míru důvěrnosti určitých dat pro daného učitele a je obvykle vztažena k riziku vyzrazení těchto dat nepovolaným osobám. Učitelé o citlivosti dat uvažují především vzhledem k údajům, které jsou ochotni o sobě na Internetu uvést: „*Jméno, příjmení (bych dal) taky, ale už bych neudával třeba datum narození, telefonní číslo nebo adresu, rodný číslo vůbec ne*", a při nakládání s hesly k internetovým službám: „*Se může stát, že mi někdo zjistí heslo, tak to vyzkouší i jinde. (...) Takže u těch důležitejch služeb mám ty hesla jiný*".

Učitelé svá data poměrně často označují jako málo citlivá popř. jako málo cenná: „*Kdybych měl pocit, že tam (v e-mailové schránce) mám něco choulostivého, tak asi jo. Ty moje věci ale nejsou takovýho rázu, že kdyby to někdo četl, že by se zboural svět*".

Důvěryhodnost subjektu popisuje, jak silně je učitel ochoten danému internetovému zdroji, internetové službě nebo osobě v online prostředí důvěřovat. Učitelé obvykle o důvěryhodnosti zdroje uvažují při rozhodování, zda pro ně, jimi používané digitální technologie či jejich data daný subjekt nepředstavuje nějaké nebezpečí – např. zda není infiltrován malwarem, nehrozí zde zneužití či vyzrazení svěřených dat, neobsahuje nepravdivá data apod.: „*Když (...) za prvý ty stránky vypadají dobře, a za druhý ten řádek tý adresy opravdu sedí, tak pak asi jsem schopen zadat ten svůj novej nebo školní mail. Pokud mám pocit, že to tam k tomu není, tak zadávám ten svůj spamovej mail*".

5.1.5 Vztah k ICT

Kategorie ***Vztah k ICT*** vyjadřuje postoj učitele k výuce ICT předmětů a k digitálním technologiím jako takovým. Je zde diskutováno, jak se daný učitel stal učitelem ICT, jak svou roli vnímá a jakým způsobem používá digitální technologie mimo výuku.

Vztah k výuce ICT. V rámci našeho výzkumu jsme oslovovali učitele aprobované i neaprobované v ICT. Učitelé neaprobovaní v ICT obvykle uvedli, že ICT začali vyučovat,

neboť na škole nebyl vhodnější kandidát: „*A protože to bylo třeba na škole taky učit, ženský k tomu většinou takovej vztah nemají, tak nějak jsem si to studoval a dostal jsem se k tomu*“. Zatímco většina z nich se s výukou ICT sžila: „*Byla jsem do toho (výuky ICT) nahnána. Strašně jsem se toho bála, ale baví mne to*“, nalezli jsme i příklad učitele, který svou roli učitele ICT chápe jen jako povinnost: *„Informatik nejsem, nejsem naprosto aprobovanej a není to můj koníček, ani se v tom nevyznám, ale učím informatiku, učím vlastně uživatelskou kancelářskou informatiku Word a Excel*“.

Názor na to, zda je vysokoškolské ICT studium přínosné pro orientaci v problematice technické e-bezpečnosti a pro schopnost toto téma učit, se u učitelů neaprobovaných v ICT liší. Někteří z nich se domnívají, že absence vysokoškolského ICT vzdělání pro ně není v této oblasti hendikepem a kompenzaci vidí například v dlouhé praxi v oboru: „*Asi protože jsem tím prošel od začátku, tak si myslím, že možná ano (mám výhodu), že dokážu víc v souvislostech mluvit (...)*“. Jiní s tímto názorem nesouhlasí: „*Já si myslím, že v tý škole do Vás nahustí opravdu to množství poznatků a toho všeho, že určitě byste byl lepší kantor, co se týká odbornosti* (…)“ a mají pocit nevýhody: „*Tak ti (nově vystudovaní učitelé aprobovaní v ICT) určitě mají větší přehled v tomhle. Protože ti to dělají od píky, od takovejch těch základů a mají co nejaktuálnější informace. Zatímco my se to dozvídáme tak nějak pozpátku (...)*“.

Vztah ke správě a používání digitálních technologií. Vztah ke správě digitálních technologií se mezi učiteli, které jsme v rámci výzkumu oslovili, liší. Zatímco jedni se o správu svého počítače a související techniky starají sami, jiní uvádějí, že nejsou správci svého počítače, ale jen uživateli. Rozdíly lze nalézt také ve vztahu ke správě digitálních technologií ve škole. Zatímco jedni mají podle svých slov správu digitálních technologií ve škole na starost, jiní učitelé uvedli, že se této činnosti nevěnují a digitální technologie ve škole spravují jiné osoby.

Intenzita používání digitálních technologií mimo výuku je u učitelů značně rozdílná. Část učitelů podle svých slov Internet využívá spíše málo: „J*á si na Internetu vybírám jen to, co potřebuji a nejsem ten, co by na něm brouzdal celý den. (...) Je pravda, že teď třeba si hodně si stahujou lidi filmy a takhle, tyhle věci mne vůbec nezajímají*“ a komunikace pomocí digitálních technologií u nich není silnou stránkou, jiní využívají celé řady internetových služeb: „*Samozřejmě já při těch všech přihlašování bych těch hesel musela mít v hlavě nejmíň dvacet* (…)“ a uvědomují si, že jejich způsob využívání Internetu se během času

mění: „*(...) ty stránky, který nepoužívám, tak ty účty se pokouším zrušit. Pak na to člověk zapomene a už neví, kde všude má e-maily a jaký e-maily*“.

5.1.6 Překážky ochrany

Na chování učitelů v problematice e-bezpečnosti působí vlivy, které jim brání být v bezpečí v maximální možné míře. Tyto vlivy vycházejí z vnějšího prostředí, z jejich osobnosti a nedostatku odborných znalostí a schopností.

Nedostatek odborných znalostí a schopností nedovoluje některým učitelům rozhodnout se v konkrétní situaci fundovaně. Jejich interpretace problému není přesná, což může vést k vystavení se riziku nebo naopak k nadměrně opatrnému chování. Příkladem vystavení se riziku budiž citace týkající se infikování učitelova počítače virem: *„(...) protože tam bylo nějaký (okno), chcete zobrazit obsah, já jsem na něco kliknul a už to jelo. Čili asi vlastně tím pádem (to vir) byl, protože místo toho, aby to zobrazilo nějaký obsah, to začalo dělat něco v počítači*“. Tendence k nadměrně opatrnému chování v důsledku nedostatku znalostí je zachycena v citaci: *„(...) druhá věc je ta, že nevím, jak ty internetový formuláře jsou viditelný pro ostatní uživatele. Když tady objednávám zboží a dává tam člověk tu adresu, tak na kolik si někdo tu adresu nemůže vzít*“.

O nedostatku odborných znalostí a schopností může svědčit nepřesně používaná terminologie (například „*ten odklikávací křížek je tam někdy falešnej*“) a také explicitní vyjádření učitelů: „*Sám se do toho nepouštím, protože vím, že toho nejsem schopen*“.

Vnější překážky. Řada učitelů vnímá překážky, které vycházejí z vnějšího prostředí a se kterými jsou konfrontovány jejich e-bezpečností zásady. Mezi tyto překážky patří tlak okolí na zveřejňování údajů o dané osobě; typickým příkladem je nutnost uvádět e-mailovou adresu na stránkách školy: „*(moje e-mailová adresa) je uvedená na stránkách školy. (...) tenhleten oficiální e-mail mám bohužel uvedenej na víc stránkách, hlavně teda školních. Na střední a na gymplu (v předchozím zaměstnání) jsem ho měla taky (...)*“, při registraci k internetovým službám i při sjednávání smluv mimo online prostředí: „*(...) dneska bohužel plno věcí, abych něco mohla získat, tak ten e-mail musím uvést, takže zase ho uvádím na spousty různejch podepisování papírů a takhle, takže holt s tímhle víc jako neudělám*“. Někteří učitelé se kvůli potřebě rychlé komunikace se žáky rozhodli opustit svou zásadu nevytvářet na sociálních sítích přátelství se žáky: „*většinou (jsem uzavřela přátelství) kvůli nějaký soutěži, protože jsme se potřebovali dorozumět a nechtěla jsem, aby mi volali. Takže jsem zvolila Facebook, že to budeme řešit přes Facebook (...)*“.

Exkurz 6. Během našeho zkoumání jsme se setkali s učitelem, který podle svých slov musel čas od času sdělit heslo k určité online službě (typicky e-mailové schránce) další osobě. Jak učitel uvedl, toto sdělení hesla bylo nutné kvůli provedení nějaké akce uvnitř účtu, kterou nemohl provést sám. I toto okolnostmi vynucené sdělení hesla další osobě lze považovat za překážku ochrany.

Někteří učitelé pociťují zahlcenost daty, které je způsobeno velkým množstvím dat, jež mají chránit (např. zálohováním) nebo jež jsou jim nabízena (např. e-mailem: „*já mám problém se tím (doručenými e-maily) ráno prokousat, protože mi ráno, když sem přijdu, trvá čtvrt hodiny, než smažu to, co smazat mám*“).

Část učitelů vnímá nedokonalost technických řešení a možnost selhání používaných prostředků ochrany. Jeden z učitelů toto shrnul výrokem, že „*Jakejkoliv stroj je vždycky jenom stroj a má spoustu chyb*“.

Vnitřní překážky. Učitelům v co nejbezpečnějším používání digitálních technologií brání překážky, které vycházejí z jejich osobnosti, momentálního rozpoložení a časových možností. Učitelé se mohou dostat do rizikových situací kvůli spěchu či únavě, kdy podle svých slov ztrácí pozornost: „*Když jsem unavená, tak už pak nějak moc nepřemejšlím a už člověk dělá něco automaticky, tak se nejspíš může udělat chyba*“.

Někteří učitelé opouštějí ideální způsoby ochrany kvůli své pohodlnosti a nedostatku času: „*Ta ostatní hesla mám taková z důvodu jednoduchosti na psaní, abych tam nemusel vyťukávat abecedu plus dvanáct čísel (...)*“. Obdobnou překážkou ochrany je náročnost na zapamatování, která se projevuje například v nedodržení pravidel týkajících se počítačových hesel: „*(...) úplně systém číslic a písmen, to ne, to bych v životě nedal. To si zapamatujou děti malý (...), ale já už ne*“.

Někteří učitelé odmítají změnit své způsoby ochrany, neboť jsou konzervativní a raději používají méně bezpečné způsoby ochrany, než by své návyky změnili: „(*Virtuální počítač) nepoužívám. To samý jako když si nainstaluješ nějakou aplikaci, tak si ji nainstaluješ v tom… jenom na zkoušku… To taky nedělám, asi bych měl, ale prostě nedělám*“.

Řada učitelů přestává být obezřetná v případě, kdy potenciální hrozba pochází od blízké osoby. Příkladem budiž výrok učitele o otevření podezřelé přílohy: „*Známejm a kamarádům v tomhle věřím, když mi něco pošlou*“.

Za specifickou vnitřní překážku ochrany lze považovat rezignaci učitele na plnou ochranu, kdy se učitel odmítá maximální ochranou vůbec zabývat: „*Já vím, že kdybyste chtěl,*

tak se na mojí wifi stejně nabouráte. Takže je mi to úplně jedno. Mám ji nějak zabezpečenou, aby ti nejblbější se tam nějak nedostali, ti inteligentnější se tam nějak dostanou".

5.1.7 Vztah k e-bezpečnostním pravidlům

Vlivem působícím na chování učitelů v problematice technické e-bezpečnosti je jejich postoj k e-bezpečnostním pravidlům, přičemž tento postoj se mezi učiteli liší[21]. Někteří učitelé podle svých slov e-bezpečnostní pravidla respektují: „*Ono se nedoporučuje (zálohovat data) na jeden, doporučuje se na střídačku aspoň na dva, tak to střídám*" a případně jejich naplňování prosazují i u své rodiny či přátel: „*Snažím se teda říct doma »zálohujte si, zálohujte si«, abych se o to já nemusel starat*". Jiní učitelé sice e-bezpečnostní pravidla znají (a případně o nich poučují své žáky), přiznávají však, že je sami nedodržují: „*Samozřejmě, učím o tom, že by se ty hesla měly střídat, měly by bejt nějak dlouhý, ale mám pocit, že to nějak nedodržuju. I když to teoreticky vím*".

E-bezpečnostní pravidla učitelé nechápou jako neporušitelné dogma, spíše je používají jako inspiraci, jak by se měli chovat, a zároveň jako reflexi, jak se ve skutečnosti chovají: „*Takže tam jsem jako uznala, jo, to jsou dobrý důvody, proč by to takhle mělo bejt, ale už jsem si ty hesla některý neměnila, už jsem si je nechala, jak jsem je měla, s tím, že si myslím, že jsou relativně bezpečný*". Aprobovaní učitelé se o e-bezpečnostních pravidlech v rámci výzkumu zmiňovali mnohem více než neaprobovaní učitelé – byť mnohdy přiznávali, že je nedodržují.

Někteří učitelé hovoří o e-bezpečnostních pravidlech jako o doplňku pravidel z běžného života, která je přirozené respektovat: „*(...) je to nějakej svět a člověk i v normálním světě se chová nějak, má nějaký pravidla bezpečnosti, za který nejde, než přejde přes silnici, tak se taky rozhlídne doprava doleva*". Část z nich vidí blízkou spojitost mezi riziky hrozícími ve virtuálním prostředí a v běžném životě: „*To člověk nepotřebuje ani číst, to dá. Ty mladý v tom umí dělat a vytipuje si, jako dřív byli tipovači, který chodili a viděli, krásná vila, ten tam šel malovat a obhlídnul, jak to tam vypadá, co jak (...)*".

[21] Stejně tak se může lišit postoj jednoho učitele k pravidlům týkajícím se různých oblastí technické e-bezpečnosti – zatímco některá pravidla učitel může dodržovat, jiná nikoliv.

5.1.8 Znaky nebezpečí

Spouštěčem pro určitý způsob ochrany před akutním nebezpečím jsou ***Znaky nebezpečí***, které učitelé rozpoznávají. Jelikož jsou tyto znaky úzce spjaty s jednotlivými oblastmi technické e-bezpečnosti a jejich výčet by byl obsáhlý, budeme se v následujícím textu zabývat pouze znaky související s problematikou hoaxu, spamu a phishingu, na níž jsme se v rámci výzkumu znaků nebezpečí zaměřili.

Znaky sledované v e-mailových zprávách. Při obdržení e-mailu se učitelé zaměřují na předmět e-mailu a jméno odesilatele. Zprávy od neznámých osob bez smysluplného předmětu přitom podle svých slov hodnotí jako podezřelé: „*Kouknu, na ty e-maily, kde je mi ten odesilatel doopravdy neznámej, tak vidím tam v předmětu nebo prvních pár slov, jako že je to něco doopravdy mimo, tak to rovnou mažu*“. Jestliže učitel e-mail nezhodnotí jako podezřelý, je ochoten jej otevřít. Při čtení e-mailu může učitel začít chápat e-mail jako podezřelý na základě samotného obsahu: „*Jak to začíná rakovinotvorný, tak už bych to asi pravděpodobně nečetl*“, na základě jazyka e-mailu: „*Dneska přichází mraky mailů typu, že je to česky, ale je to napůl anglicky a pochází to támhle z Nigérie a podobně, tak to rovnou mažu*“ nebo na základě jazykového stylu použitého v e-mailu: „*Proč to rovnou nesmazat a neřešit…Fakt záleží na tom, jak to bude napsaný a podaný*“.

Pokud e-mailová zpráva obsahuje přílohu, zaměřují se někteří učitelé na typ souboru v této příloze: „*Všechny soubory, který se mi občas objeví v mailu, se spustitelnou příponou, tak mažu*“, jiní učitelé podle svých slov zohledňují, zda znají odesilatele e-mailu: „*Přílohy jako neotvírám. To fakt jen od těch lidí, který znám*“, a další vyhodnocují oba tyto znaky zároveň: „*Všechno, co je spustitelnej soubor od lidí, který neznám, tak mažu*“.

> **Exkurz 7.** Během rozhovorů jsme se setkali s učiteli, kteří se ke znakům, jež při e-mailové komunikaci považují za podezřelé, vyjadřovali zkratkovitě a podle obecně platných pouček. Jeden z učitelů například uvedl: „*Neotevírám maily, který nevím, od koho jsou. Ty rovnou vyhazuju*“. Protože daný učitel v době konání rozhovoru působil na více školách zároveň a vedl kurzy distančního vzdělávání, bylo pravděpodobné, že nezná všechny své studenty. Na náš dotaz, jak nakládá s e-maily, které jsou sice od neznámého odesilatele, ale jejichž předmět se váže k jeho zaměstnání, učitel odpověděl: „*No, tak ty maily v tom případě otvírám. Ale dívám se na předmět, a navíc to (e-mailový klient) ukazuje i část textu, takže tam*

vidím, co je první věta v textu. Tak podle toho se rozhodnu, jestli to otevřu nebo ne“.

5.1.9 Konkrétní způsoby ochrany a návyky

Kategorie ***Konkrétní způsoby ochrany a návyky*** se zabývá způsoby, jak se učitelé ICT brání před negativními jevy při používání digitálních technologií. Tvoří ji jak postupy preventivní, tak i postupy řešení následků. V následujícím textu uvedeme průřezové způsoby ochrany a poté se budeme zabývat jednotlivými oblastmi technické e-bezpečnosti (tj. ztrátou dat, malware, počítačovými hesly, nevyžádanou poštou a správou soukromí).

Reakce učitelů na konkrétní problém může být výrazně odlišná. Jedni se snaží situaci řešit vlastními silami a hledají primární pomoc na Internetu, případně se obrací se žádostí o radu na ICT odborníky ze svého okolí: „*(…) to bych se v tom chvíli zkoušel šťourat sám, protože samozřejmě já jsem takovej, že jakmile je problém, tak ho musím vyřešit. A kdyby mi to nepomohlo, tak bych se šel poradit s někým dalším, s nějakým kolegou ajťákem ze školy třeba*“. Část z nich se přitom snaží sbírat potřebné informace z různých zdrojů, které pak porovnají: „*Získám takhle informace z více míst, ne z jednoho. A pokud se budou shodovat, že to musím přeinstalovat, tak to musím přeinstalovat*“.

Ve stejné situaci by další učitelé požádali známé ICT odborníky o přímý zásah bez předchozí snahy o řešení problému vlastními silami: „*Protože já nejsem až tak dobrej ajťák, abych se v tomhle vyloženě vyznal sám. A zvlášť, když máte ty lidi kolem sebe (…), tak to sám neděláte*“. Jestliže neznají vhodné ICT odborníky ze svého okolí a vlastními silami nejsou schopni problém řešit, obrací se na specializované firmy.

> **Exkurz 8.** Během našeho zkoumání jsme se setkali s učitelem, který při řešení problému požádal o intervenci svou manželku. Ačkoliv podle učitelových slov jeho manželka není ICT odborníkem, v dané problematice se vyzná lépe: „*Protože to (soukromí na Facebooku) neumím ani pořádně nastavit, tak jsem řekl manželce, ať mi všechno zakáže, aby mne nemohl nikdo najít, nikdo vidět, nikdo napsat kromě těch, co si přidám do přátel. Tak zatím to docela funguje. Nevím, jak se to teda udělá…*“. Tento příklad podle našeho názoru ukazuje na neochotu některých učitelů učit se s určitou novou technologií zacházet a zaslouží si srovnání s učiteli, kteří se o trendy naopak aktivně zajímají (viz s. 69).

5.1.9.1 Zálohování

Svá data zálohují všichni námi oslovení učitelé, přičemž důraz kladou na data, která jsou podle nich důležitá. Mezi ně patří zejména soukromé fotografie, materiály potřebné pro pedagogickou činnost a další vzdělávání, případné jiné dokumenty či produkty tvůrčí činnosti učitele: „*(...) a taky veškerou muziku, kterou jsem napsal, mám prostě zálohovanou*“.

Umístění záloh. K zálohování dat učitelé využívají nejrůznější média – externí pevný disk, USB flash disk, CD, DVD a cloudové služby (například e-mailovou schránku a úložiště typu DropBox či SkyDrive). Řada z nich svá data zálohuje více způsoby; jako primární zálohovací médium nejčastěji volí externí pevný disk. Někteří učitelé chápou jako zálohu i zkopírování dat na několik vzájemně nezávislých PC: „*Zazálohuju něco na server, něco dám k sobě do počítače, a pak je má ještě každej učitel, co je vytvořil, u sebe. Takže (...) je třeba jedna sada výukových materiálů, těch DUMek, na třech počítačích*“. Za jistý způsob zálohy fotografií považují někteří učitelé jejich vytištění nebo začlenění do online fotogalerie: „*Vzhledem k tomu, že jsem je (určité fotografie) už poslal na to rajče (služba rajče.net), tak by se aspoň tam neztratily. (...) Už by sice nebyly v tom pětimegovým formátu, ale prostě bych fotky měl*“.

> **Exkurz 9.** Mezi učiteli lze ve využívání cloudových služeb (typu DropBox nebo OneDrive) najít značné rozdíly. Zatímco někteří z nich tyto služby nechtějí vůbec využívat: „*(...) stejně tak bych na Google nebo Microsoftu prostě celkově nedávala vůbec žádný data*“, jiní učitelé jsou ochotni zde zálohovat své dokumenty: „*úplně ty nejdůležitější data si dávám na takový ty služby jako je Google Drive nebo DropBox*“ a další zde podle svých slov kromě dokumentů uchovávají i fotografie. Učitelé, kteří cloudové služby nepoužívají, tak činí mimo jiné z důvodu nedůvěry k nim, jak diskutujeme na s. 67.

Pravidelnost záloh se mezi učiteli liší. Někteří tvrdí, že svá data zálohují v pravidelném intervalu (který se pohybuje od jednoho týdne po jeden rok): „*Snažím se (zálohovat) jednou za měsíc, ale zrovna vím, že teď jsem na to zapomněla*“. Jiní učitelé zálohují aktuálně vytvořená či upravená data: „*Zálohuju, kdykoliv něco vytvořím. Když něco vytvořím a mám to hotový, tak provedu zálohu. Když nic netvořím, tak co bych zálohoval*“. Část z nich využívá podle svých slov automatickou synchronizaci dat se vzdáleným serverem: „*Uložím si to do složky a ono to synchronizuje automaticky. Takže takhle já tady mám Skydrive, dokonce i pro školní věci*“. Kromě výše uvedených přístupů jsme se setkali s případem

učitele, který podle svých slov zálohuje data také před rizikovou operací se systémem: „*Zálohuju (…) nebo když třeba jdu s tím počítačem něco dělat, něco instalovat novýho, tak si to přetáhnu. Ale spíš jako když se něco děje*“.

Systematičnost záloh. Někteří učitelé se snaží data zálohovat systematicky, kdy část z nich vytváří kompletní zálohy (tj. každá záloha obsahuje všechna data), a další používají přírůstkové zálohování: „*Doplňuju nový data. Mám tam jenom tu jednu složku, tu si přetáhnu (na externí disk) a to, co mám nový, tak to se dokopíruje*“. Další učitelé zálohují aktuálně vytvořená či upravená data (jak je popsáno výše) – zatímco někteří z nich mají ve vytvořených zálohách určitý systém, jiní přiznávají nesystematické zálohování: „*Někdy (zálohuju data) dvakrát a někdy na to (médium), někdy na to. Není v tom tak úplný systém*“.

5.1.9.2 Malware a nefunkční OS

Ochrana před malware. Základem ochrany proti malware je u učitelů antivirový software s pravidelně aktualizovanou virovou databází. Část učitelů provádí aktivní antivirovou kontrolu, kterou realizují při kontaktu s potenciálně nebezpečným médiem či soubory: „*Oni (žáci) mi přinesli práci na flashce nebo CD, tak jsem si to projel a bylo to zavirovaný. Takže mne to přesvědčilo o tom, že to mám kontrolovat*“ nebo v pravidelném intervalu: „*Dělám si v počítači antivirovou kontrolu po restartu, tak zhruba jednou měsíčně*“. Někteří učitelé (v určitých situacích) spoléhají, že je antivir bude o přítomnosti hrozby sám informovat: „*Co se týče flashek a takhle, tak tam spoléhám na to, že mne ten antivirák ochrání. Když ji tam prostě dám a bude tam ten vir, tak že mi to prostě řekne*“. V případě, že je učitel antivirem upozorněn na rizikový soubor či webovou stránku, akceptuje jeho doporučení a soubor smaže či podezřelou webovou stránku opustí: „*(…) někdy se tam objeví černej vykřičník ve žlutém poli, tak to i kdyby to sebevíc mne lákalo, tak to neotevírám*“.

Učitelé se svým chováním při pohybu na Internetu liší. Zatímco jedni se podle svých slov snaží rizikovým stránkám vyhýbat, jiní je s vědomím případné hrozby navštíví: „*Vím, že mi třeba hrozí hrozba, ale i přesto se tam podívám, když potřebuju nebo mne to zajímá. Ono kolikrát mne to upozorní, že ta stránka obsahuje nějakej nebezpečnej materiál, tak to většinou zavírám*“. Mezi nimi je pak skupina učitelů, která se stránkám s rizikovým obsahem nevyhýbá, navštěvuje ale pouze osvědčené stránky, kde se doposud s malware nesetkala: „*(…) když si něco takovýho vyzkouším, tak už chodím na tu samou stránku, kde vím, že jsem nic nechytil*“. Příklad učitele, který by rizikové stránky navštěvoval z prostředí virtuálního počítače či využíval podobné techniky, jsme nenalezli.

Někteří učitelé chápou jako obranu proti malware také obezřetné používání e-mailové komunikace, kdy podle svých slov neotevírají podezřelé e-mailové zprávy a potenciálně nebezpečné přílohy e-mailových zpráv. Jak se zmiňujeme v kapitole 5.1.6, toto chování však někteří učitelé opouští v případě, že je jako odesilatel takové zprávy uveden člověk z jejich blízkého okolí.

Řešení následků[22]. Ve způsobu odstraňování malware ze svého PC se učitelé liší. Někteří by podle svých slov nechali řešení problému na antiviru a v případě neúspěchu by použili radikální opatření ve formě přeinstalování celého operačního systému nebo naformátování dotčených diskových oddílů: "*Důvěřuju tomu, že kdyby v tom byl nějaký virus, tak se ten antivirus prostě ozve. Když se neozve, tak naformátovat počítač, pokud to půjde*". Jiní učitelé by se pokusili tutéž situaci řešit přesněji cílenými postupy – soubor obsahující malware by se snažili nalézt (například přes nouzový režim systému) a následně jej ručně smazat: „*Byl to klasickej policejní vir. Nejdřív jsem zkoušel všelicos, ale nešlo to, ale samozřejmě pomohl nouzovej režim*".

V rámci rozhovorů jsme se setkali i s učitelem, který po instalaci operačního systému vytvářel obraz diskového oddílu s nainstalovaným operačním systémem, který by v případě napadení PC malwarem mohl použít k obnově systému: „*já ho vždycky zálohuju, když je novej. Protože chci si vytvořit tu čistou novou zálohu*". Poznamenejme, že někteří z učitelů, kteří by se podle svého vyjádření snažili si s problémem poradit sami, se k tomuto tématu vyjadřovali velice nepřesně a vyhýbavě: „*Nějak bych to dělal, nevím jak. Takovýhle zkoušení nevím (...) Prostě bych se do toho systému podíval a pak bych viděl (...)*".

5.1.9.3 Zabezpečení účtů

Množství hesel. Pro zabezpečení svých účtů používají učitelé zpravidla několik různých hesel. Pro přístup ke službám pro ně velmi citlivým (zejména internetovému bankovnictví) používají jedinečná hesla, která nevyužívají u žádné jiné služby. Někteří učitelé používají pro přístup k vzájemně příbuzným službám jedno společné heslo: „*(...) když ta služba je podobná, třeba na ten e-mail školní i ten můj, oboje mám na Seznamu, tak mám stejný heslo*", další využívají navzájem podobná hesla a jiní tvrdí, že volí heslo pro každou službu odlišné: „*Mám tři e-mailový schránky, na kterých mi záleží, tak tam mám (ty hesla) jiný*". Pro

[22] V tomto odstavci se budeme zabývat chováním učitelů, kteří by se snažili problém vyřešit svépomocí. Přenecháním řešení problému na odborníkovi se zabýváme v úvodu této kapitoly na s. 79.

zabezpečení služeb, které nejsou podle názoru jednotlivých učitelů důležité, používají zpravidla jedno heslo společné pro všechny tyto služby: „*Někde používám takový to opakující se heslo, kde mi tak na tom nějak nezáleží, třeba pro registraci do tohodle e-shopu*“ nebo vzájemně velmi podobná hesla.

Na straně druhé jsme se setkali také s příklady učitelů, kteří podle svých slov používají pro všechny služby jediné heslo: „*Ty (hesla), který tady já si vymejšlím sám, ve většině případů je stejný*“ nebo několik málo navzájem podobných hesel: „*Mám jich (hesel) několik, ale je to podobný. Hodně podobný, ale něčím se to liší. Číslama třeba nebo tak*“.

Složitost hesel. Složitost hesel a interval jejich obměny učitelé obvykle odvozují od důležitosti dané služby; v tomto a následujícím odstavci se budeme zabývat hesly, které se daní učitelé snaží chránit nejvíce. Učitelé pro zabezpečení důležitých služeb používají obvykle poměrně dlouhé heslo, například: „*Tam, kde mi na tom záleží, tam je třeba 12místný, 16místný*“. Někteří učitelé podle svých slov vytvářejí hesla, která splňují doporučované parametry bezpečného hesla: „*(Je to) změť písmen a číslic. Takže se v tom vyznám jenom já, že já vím, kde se vzaly ty písmena a číslice*“. Jiní učitelé tvoří hesla vzniklá spojením několika slov nebo slova a určitého čísla: „*Osobně mně se (všechna hesla) točí kolem jednoho slova a k tomu jsou přidaný nějaký čísla*“. Tato čísla přitom mohou být spojena s osobními údaji daného učitele: „*(...) je to kombinace osobních dat. (...) Nemusí to být rodné číslo, může to být letopočet, můžou to být různá jiná čísla*“.

Obměňování hesel. Z hlediska obměňování hesel v čase se učitelé liší, zatímco jedni svá hesla neobměňují nebo je obměňují jednou za několik let: „*U e-mailu jsem ho třeba měnila, ale už zase poslední dva roky ho mám stejný, ty jídelny, ty si vůbec neměním*“, jiní tvrdí, že u důležitých služeb je obměňují pravidelně několikrát ročně: „*U těch skutečně důležitých… zase to tak nějak nepřeháním, tak řekněme čtvrt roku, tři měsíce to vychází změny těch hesel*“.

Zatímco někteří učitelé při změně hesla vytváří zcela nové heslo, jiní upraví původní heslo: „*Víceméně já to nějakým zásadním způsobem neměním. Změním buď nějakou tu koncovku, nebo tam přidám někde nějaký číslo*“ a další použijí jiné heslo ze sady jimi používaných hesel: „*Používám těch pět, šest hesel, a když se po mně žádá změna, tak vezmu jiný z pěti, šesti hesel a dám ho jako nový heslo*“.

Uchovávání hesel. Protože někteří učitelé mají problém si pamatovat všechna svá hesla, vytváří tito učitelé seznamy vybraných hesel: „*Mám víc hesel a některý, který málo*

navštěvuju, ty mám vypsaný, ty který jsou důležitý, tak ty si pamatuju“. Část z nich podle svých slov zapisovaná hesla modifikuje tak, aby je nebylo možno přímo použít: „*Třeba ulice kde bydlím – Zahradní 27. Zahradní27, jsem měl (jako heslo). A vím, že když tam udělám 27 a ještě trojku k tomu, tak vím, že ta trojka tam není*“. Poznamenejme, že jsme se setkali i s příkladem učitele, který místo ručně vytvářeného seznamu hesel používá software pro správu hesel: „*Samozřejmě mám program, kam si můžu ty hesla zapisovat, kterej to šifruje, ty hesla (...)*“.

Ochrana hesel. Někteří učitelé se snaží chránit svá hesla proti odpozorování jinými osobami, například žáky: „*snažím se, aby se mi nikdo nedíval na ruce, když píšu heslo, třeba když se studenti přijdou podívat na nějaký výsledky z testu, tak se je snažím navést, aby se mi tam nekoukali*“ nebo „*Já většinou píšu tak rychle, že si toho nikdo nevšimne (...) Já většinou to projedu všema deseti tadyto (základní klávesová část), takže nemají šanci (...)*“. Pokud by heslo bylo prozrazeno, učitelé se jej snaží urychleně změnit: „*(...) omylem ho někomu řeknu nebo ho právě řeknu záměrně, protože potřebuje k mýmu e-mailu si tam něco stáhnout, něco mi vytisknout, okamžitě potom provedu změnu hesla*“.

5.1.9.4 Obrana před nevyžádanou poštou

Ochrana před spamem. Řada učitelů se před doručováním spamu do své e-mailové schránky aktivně brání, někteří učitelé však chápou spam jako nevyhnutelný jev a obranu proti němu nehledají. Ti, kteří se spamu brání, se snaží mimo nezbytných případů nezveřejňovat e-mailovou adresu na webových stránkách nebo alespoň upravit uvedenou adresu do takové podoby, aby bylo ztíženo její využití spamovacími roboty: „*My jsme ji (e-mailovou adresu) měli na stránkách napsanou normálně, tak teď jsme dali zavináč do závorky, jak to dělá většina firem (...)*“. Někteří učitelé při registracích k online službám využívají sekundární e-mailový účet, který jim slouží především k tomuto účelu a který nepoužívají k běžné komunikaci: „*Mám dva e-mailový účty (...) A na ten starej už mi chodí spousta spamu. Takže když někde zadávám nějakou adresu (...), tak zadávám svojí starou e-mailovou adresu, kam chodím jednou za měsíc. A tam ať mi prostě chodí spamu, kolik chce*“. Při obdržení nevyžádaného e-mailu učitelé tuto zprávu obvykle smažou nebo ji označí jako spam; někteří z nich se snaží takovouto zprávu neotevírat, aby neupozornili na aktivitu své e-mailové schránky: „*Většinou na to vůbec nereaguju, abych neukazoval, že je ta adresa nějakým způsobem živá nebo že tam prostě něco je*“. V případě nevyžádané obchodní nabídky se část učitelů snaží odhlásit od dalšího odebírání nabídek dané společnosti: „*(...)*

dělám to, jak je tam na konci v tom mailu, že chceme zrušit tu informaci, tak dám zrušit a přestane to chodit“.

V ochraně před spamem pomáhají učitelům antispamové filtry. Většina učitelů využívá základního nastavení těchto filtrů: „*(...) moje e-mailová schránka má nějakej spamovej filtr, samozřejmě jsem si ho nepsala já a doufám, že mi něco přefiltruje (...)*“ či je učí přesněji reagovat na spam – nevyžádanou poštu označují jako spam nebo ručně přidají odesilatele mezi zakázané adresy: „*Mám na Seznamu e-mail klasickej a tam jsou nastavený různý filtry, takže tam tímhletím způsobem se ty spamy automaticky mažou. Co označím jako spam nebo přidám do toho filtru, tak se to automaticky maže*“. Setkali jsme se však i s příkladem učitele, který si definoval vlastní pravidla pro rozpoznávání spamu: „*Pokoušel jsem se s tím bojovat tak, že jsem si nastavil filtr, že všechno, co končí na .com, tak mi bude odfiltrovaný do spamu (...)*“.

Ochrana před hoaxem. V případě obdržení poplašné zprávy se učitelé rozhodují na základě závažnosti zprávy. Jestliže se jich obsah zprávy přímo dotýká, snaží se podle svých slov obvykle ověřit pravdivost zprávy z nezávislých zdrojů (viz dále). Pokud je obsahem zprávy varování před obecnou hrozbou (např. údajná zdravotní rizika běžných potravin), odmítá řada učitelů pravdivost takové zprávy ověřovat: „*Já to ani nestuduju, jestli to může bejt pravda nebo ne, protože jako v tej situaci vždycky prohraju. Jestli to je pravda nebo ne, tak to nesmíte ani řešit. Protože si to nemůžete ověřit*“. Někteří učitelé jsou vůči takové zprávě skeptičtí vzhledem k tomu, že je nevyžádaná: „*Informace tohoto typu si zjišťuji někde úplně jinde. Než z takovejhle mailů*“. Důvodem, proč část z těchto učitelé odmítá pravdivost zprávy ověřovat, je přesycenost podobnými nevyžádanými zprávami. Jeden učitel například vypověděl: „*(...) takhle kdybych měl fungovat, tak nic nejím, nic nepiju, nic nepoužívám, maximálně se živím syrovým masem, který si ulovím*“.

Primárním zdrojem k ověření pravdivosti zprávy jsou pro většinu učitelů informační portály veřejné správy: „*Podíval bych se na stránky třeba příslušnýho ministerstva, jestli je tam nějaká vyhláška nebo co to obnáší*“ a zdroje vyhledané k danému problému přes internetový vyhledávač: „*(...) do hledáčku si napsat tadyto třeba to SLS nebo celý tohleto… Často používám Google, to asi nejčastějš*“. Někteří učitelé by se podle svých slov snažili ověřovat pravdivost informace mimo online prostředí: „*Zeptala bych se kolegyně chemikářky*“ nebo s pomocí komunitních zdrojů: „*Jsou různý fóra na Internetu, kde se dá zjistit, (...) jestli je to pravdivej e-mail nebo ne a pak samozřejmě poptání kamarádů, známých, jestli jim taky něco takovýho přišlo a co si o tom myslej*“. O využití služeb

monitorujících poplašné zprávy (např. Hoax.cz) se zmínila pouze malá část učitelů. Další šíření poplašných zpráv učitelé vesměs odmítají: „*Tak maximálně bych si řekl, to je zajímavý, ale rozhodně bych to neposlal někomu dalšímu*“, někteří připouštějí přeposlání závažné zprávy po důkladném ověření její pravdivosti.

Registrace k online službám. Při registracích k online službám učitelé obvykle zvažují důvěryhodnost dané služby a citlivost údajů, které daná služba při registraci požaduje. Jestliže daná služba požaduje zadání dat pro učitele příliš soukromých nebo pro ně daná služba není dostatečně důvěryhodná, někteří učitelé danou registraci zcela odmítnou: „*Když mi to prostě bez toho nechtějí nějakým způsobem zpřístupnit, tak se to pokusím sehnat jinak, nejdu do toho*“. Jiní by posuzovali, zda má daná služba účinný kontrolní mechanismus nebo zda je na zadaná data vázána další činnost[23]. Pokud nikoliv, pokusili by se zadat nepravdivé údaje: „*Já jsem e-mail zadal správnej, ale jméno, příjmení jsem zadal jiný. To jsem šidil, to jsem si vymyslel. Ten mail musí bejt (správnej), protože Vám přijde nějakej potvrzovací (e-mail), takže ten ošidit nemůžete (…)*“.

5.1.9.5 Soukromí v online prostředí a používání sociálních sítí

Rozsah a způsob používání sociálních sítí. Učitelé se v rozsahu používání sociálních sítí značně liší. Zatímco jedni podle svých slov sociální sítě nepoužívají, jiní používají sociální sítě příležitostně a další je používají často[24]. Rozdílný je také způsob používání sociálních sítí, kdy zatímco jedni je používají pouze pro komunikaci pomocí chatu a případně přijímají informace od ostatních, jiní aktivně vytváří obsah viditelný pro ostatní.

Ačkoliv většina námi oslovených učitelů využívá sociální sítě k osobním účelům, setkali jsme se s učitelem, který chápe svůj profil na sociální síti jako pracovně-zájmový a podle svých slov zde nezveřejňuje žádné soukromé informace: *„(…) nepotřebuju něco ze svého soukromí sdělovat, to ne. Spíš se zapojuju se do nějakých takových diskuzí, který mne baví, který mne zajímají*“. Kromě toho někteří učitelé používají alternativní sociální sítě, které jim pomáhají v realizaci jejich koníčků (například cestovatelská síť Couchsurfing.com).

[23] Za tuto činnost lze považovat například zaslání objednaného zboží na zadanou poštovní adresu

[24] Na profil jednoho ze zkoumaných učitelů bylo za poslední tři měsíce umístěno 55 statusů (případné komentáře pod statusem do tohoto počtu nezahrnujeme). Některé z nich inicioval zkoumaný učitel, jiné na jeho zeď umístili jeho přátelé.

Ochrana soukromí. Učitelé se obvykle snaží své soukromí na sociálních sítích chránit. Někteří se rozhodli o svém soukromí nepublikovat informace prostřednictvím statusů ani pro okruh svých přátel, jak dokládá následující citace: „*Lidem, který chci, aby věděli třeba můj momentální stav, to řeknu osobně nebo jim to zavolám. Nebo pošlu SMS. Anebo jim to napíšu do zprávy v chatu. Ale nemusím to věšet na zeď (...)*“. Někteří z těchto učitelů jsou na sociálních sítích ochotni zveřejňovat informace, které podle nich nejsou osobního charakteru: „*(...) na tom nevidím nic závadnýho, protože tohleto si myslím, že je to informace, kdyby se mne ten člověk zeptal, tak mu to klidně řeknu*“.

> **Exkurz 10.** Zajímavým přístupem, se kterým jsme se setkali, je uveřejňování zpráv na sociálních sítích ve formě alegorie. Jeden učitel vypověděl, že ačkoliv jsou tyto zprávy viditelné pro všechny přátele, jejich pravý smysl by měli být schopni určit jen blízcí přátelé. Osoby, se kterými neudržuje učitel bližší kontakt (v případě tohoto učitele například jeho žáci), chápou tuto zprávu jen v povrchní rovině a odhalování soukromí je tím omezeno.

Jiní učitelé se zveřejňování soukromých informací nebrání, avšak trvají na rozvážném výběru těchto informací a důsledném nastavení práv pouze pro vybrané osoby – příkladem budiž výpověď jednoho z učitelů: „*Můžeš jim ukázat, co je u vás novýho, ale současně bych trval na tom, aby to bylo všechno tak, jak má bejt, aby to nemohl vidět nikdo cizí, aby se prostě k tomu nikdo nemohl dostat*“. Poznamenejme, že jsme se setkali i s příkladem učitele, který na sociálních sítích v okruhu svých přátel bez větších obav zveřejňuje informace ze svého soukromí: „*Občas se pochlubím se svým momentálním stavem, když už mne to fakt naštve a chci to vykřičet do světa. Nebo se svým stavem po ránu, pokud to má vtipnej podklad*“.

Zveřejňování fotografií. Učitelé zveřejňování fotografií na sociálních sítích vnímají rozdílně. Někteří z nich publikování fotografií na svém profilu zcela odmítají, jiní se zveřejňování fotografií pro okruh přátel nebrání: „*Tak je člověk na dovolený, se mu zdá, že se mu povedly ty fotky, klidně bez lidí, tak je tam dá, ať si je lidi prohlídnou“*. Jako rizikové z hlediska soukromí chápou někteří učitelé možnost v rámci sítě Facebook označit ve fotografii určitou osobu, čímž dojde ke zpřístupnění takové fotografie i pro přátele označené osoby: „*Já sám teda razím zásadu, že nelíbí se mi to právo těch třetích osob označovat osoby na fotografii, to mi tam jako dost vadí*“, zatímco jiní toto označování za problematické nepovažují: „*Relativně mi to (označování na fotkách) nevadí. Pokud ta fotka opravdu není taková, že by mne třeba mohla poškodit v práci nebo něco, tak rozhodně ne*“.

> **Exkurz 11.** V rámci zkoumání jsme se setkali s učitelem, který na svém profilu uveřejňuje fotografie zachycující jej během večerních akcí s přáteli. Na náš dotaz, jak tyto fotografie vnímá, odpověděl: „*Fotka, že jsem někde byl, támhle, s někým, s drinkem v ruce, nevadí. Ale kdyby to byla fotka, která by mne mohla nějakým způsobem zkompromitovat, ať už v osobním životě nebo hlavně v práci, tak to by mi hrozně vadilo*“.

Někteří učitelé své fotografie místo zveřejňování na sociálních sítích umisťují do specializovaných webových fotogalerií. Část z nich zde své fotografie chrání proti přístupu nepovolaných osob pomocí hesla: „*Používám servery, který jsou určený čistě pro fotky a tam je to zaheslovaný, přístup je jenom těm, kterým dám to heslo*“. Další učitelé ve webových fotogaleriích některé své fotografie zveřejňují, aniž by je proti náhodnému přístupu explicitně chránili: „*(…) jinak spíš svým přátelům dám odkaz třeba na rajče.net (…)*“. Je třeba poznamenat, že za jistou formu ochrany lze považovat již nutnost zadat správný odkaz pro zobrazení fotogalerie. Nelze však vyloučit, že bude možné danou fotogalerii nalézt prostřednictvím webového vyhledávače i bez znalosti přesné URL adresy.

> **Exkurz 12.** Během zkoumání jsme se setkali s učitelem, který na sociální síti Google+ zveřejňuje svá dokumentační fotoalba z prázdninových cest a odkaz na ně má uvedený na svých webových stránkách. Na náš dotaz, zda to nevnímá jako odhalování soukromí, odpověděl, že nikoliv, neboť “*(…) jsou to vyloženě věci, který jsou public a takhle to dávám komukoliv, koho by to zajímalo. Čas od času se mi stane, že mne někdo osloví, kdo si mne vygooglil, respektive vygooglil si třeba něco o místě, který znám, a jsem mu schopen poradit (…)*“.

Přátelení se se žáky na sociálních sítích je pro řadu učitelů aktuálním až kontroverzním tématem, avšak chování jednotlivých učitelů je značně odlišné. Někteří učitelé přátelení se se žáky zásadně odmítají, jak dokládá následující citace: „*já bych se přikláněla k tomu (si žáky na Facebooku) nepřidávat a myslím si, že by to bylo i dobrý, kdyby to tak všichni vyučující dělali, že by si je nepřidávali*“. Jiní takové chování za problematické nepovažují nebo se se svými žáky za určitých podmínek přátelí. Nejčastějším požadavkem je neodhalovat před žáky své soukromí. K dosažení tohoto cíle se snaží například nezveřejňovat své soukromí (jak je diskutováno výše) nebo členit virtuální přátele na určité skupiny s omezenou viditelností jednotlivých příspěvků: „*(…) to zveřejňování myslím, že mám vrstevnatý, takže co nechci, aby si (žáci) prohlíželi, tak omezuju na patřičný skupiny*

(...)“. Během zkoumání jsme se setkali s učitelem, který na sociálních sítích své soukromí před žáky zveřejňuje, jak dokládá Exkurz 13.

> **Exkurz 13.** V rámci zkoumání jsme se setkali s učitelem, který se na Facebooku přátelí se svými žáky a zároveň zde uveřejňuje příspěvky osobní povahy (viz Exkurz 11). Podle svých slov kvůli žákům své chování na Facebooku nezměnil. Na náš dotaz, jak žáci na tyto příspěvky reagovali, odpověděl: „*Ty statusy byly (pro ně) atraktivní a brali to naprosto v pohodě, s humorem a se zdravým humorem, takže nikde nic dál nešířili, co se týče v rámci školy a tak dále, jelo to prostě jenom mezi náma. Nebo respektive mezi těma, kdo to všechno viděli. (...)*“.

Řada učitelů se na sociálních sítích přátelí se svými bývalými žáky, přičemž tento postup praktikují i učitelé, kteří se se svými současnými žáky přátelit odmítají: „*Já mám zásadu tu, že dokud je ten dotyčný mým studentem, tak si ho nepřidávám, jakmile mým studentem být přestane, a on mne třeba požádá o přátelství, tak si ho přidám*“.

Správa nepoužívaných účtů. Nepoužívané účty na sociálních sítích a komunitních serverech se někteří učitelé snaží rušit, jako důvod uvádějí snahu o kontrolu online informací o své osobě a odstraňování stop své dřívější aktivity. Jeden z učitelů vypověděl: „*Vím, že z minulosti tam ještě něco může bejt, i když jsem se snažil zrušit stránky jako Spolužáci a podobně. (...) A nechci, aby ty informace o mně byly přístupný*“.

> **Exkurz 14.** Během zkoumání jsme ve veřejné části profilu jednoho z učitelů na Facebooku nalezli odkaz na jeho přezdívku, kterou používá v online prostředí. Na základě této přezdívky jsme prostřednictvím vyhledávače Google.com nalezli profil daného učitele na jistém seznamovacím portálu, kde o sobě uvádí řadu informací a fotografií. Na tomto příkladu se ukazuje, že je vhodné občas provést audit informací, které je možné o sobě na Internetu na základě obecně známých informací dohledat, a provést vhodnou korekci těchto údajů online.

5.1.10 Výstupy ochrany

Kategorie ***Výstupy ochrany*** se zabývá výsledkem ***Konkrétních způsobů ochrany a návyků***. Tato kategorie do značné míry překrývá s kategorií ***Konkrétní způsoby ochrany a návyky***, neboť finální stav ochrany implicitně reflektuje použité způsoby ochrany. Jestliže například učitel pravidelně zálohuje svá data na externí disk (což je způsob ochrany), má svá data zálohovaná na externím disku (což lze označit za výstup ochrany). Z důvodu implicitní

podobnosti s kategorií ***Konkrétní způsoby ochrany a návyky*** se popisem těchto výstupů ochrany nebudeme hlouběji zabývat.

5.1.11 Negativa ochrany

Kategorie ***Negativa ochrany*** je stejně jako kategorie ***Výstupy ochrany*** zaměřena na výsledky ***Konkrétních způsobů ochrany a návyků***. Tato kategorie se (na rozdíl od kategorie ***Výstupy ochrany***) zabývá negativními jevy, které mohou vznikat z překážek ochrany, jestliže se učitel rozhodne chovat co nejbezpečněji, a které učitele určitým způsobem omezují.

Mezi negativa ochrany patří:

- časová náročnost: „*(…) zase taky člověk nějakým způsobem rozlišuje prostě větší nebezpečí, menší nebezpečí a třeba u těch menších je míň důslednej a taky prostě to vyžaduje nějaký čas*“
- náročnost na pamatování: „*Já jsem to dělal (obměňoval svá hesla), ale (…) pak jsem si to vždycky pletl. Nový – starý – nový – starý*“
- nepříjemnost opakující se činnosti: „*To, co je školy, co jsme dělali ty šablony, tak to jsem zálohovala asi třikrát na dvě flashky a ještě v počítači a ještě jsem si něco tady do školy takhle uložila, ale zase potom, když se udělala nějaká změna v tom jednom, tak se musel ten soubor čtyřikrát otevírat, přehrávat*“
- ochuzení o určité informace: „*Registrace nedělám. Jakmile něco chtějí registrovat, tak tam se nepřihlašuju, teď jsem třeba, možná že člověk přijde i o nějakou informaci třeba důležitou (…)*“ nebo „*To mi napsal šéf, já jsem to nepoznal (...) Takhle, on mi to napsal, ono to spadlo do spamu no a já jsem se do spamu nekoukal 14 dní*“

5.1.12 Subjektivní hodnocení kompetencí

Kategorie ***Subjektivní hodnocení kompetencí*** se zabývá tím, jak jednotliví učitelé vnímají své kompetence v oblasti technické e-bezpečnosti. Zatímco většina učitelů sama sebe označuje za poučeného laika: „*Samozřejmě za ty léta letoucí, co se v tom pohybuju, tak v podstatě jsem samouk, který o tom něco ví. Ale za odborníka typu ajťáka se nepovažuju*“, někteří se spíše považují za odborníka než laika a cítí se být v problematice znalí: „*Laik rozhodně nejsem, ale že bych byl nějakej extra odborník, to ne. Já si myslím, že jsem takovej vyšší průměr*“.

Značné odlišnosti lze nalézt v hodnocení samotných kompetencí. Učitelé se obvykle domnívají, že jejich orientace v problematice je přiměřená a dostatečná vzhledem k jejich potřebám a úkolům na ně kladeným: „*Já se v tom vyznám tak, jak potřebuju v tu chvíli. Kdybych si to potřeboval rozšířit, tak bych musel do toho vhlédnout víc a věnoval se tomu*“, tedy že jsou schopni problematiku vyučovat: „*pro potřeby, co mám ty děti naučit, mi to stačí*“ a adekvátně se starat o svěřené digitální technologie: „*(...) běžný věci, který (...) potřebuju tady, abych se aspoň trochu staral o ty počítače ve škole, že zvládám*“.

Zaznamenali jsme i názory opačné, které vyjadřovaly obavu z neschopnosti vypořádat se s případným e-bezpečnostním incidentem: „*Zavirovanej počítač jsem nikdy neměla a mám v tom obrovský štěstí, že se mi to nikdy nestalo. Protože by s tím bylo hrozně obstrukcí a potíží a kdoví, jestli bych si s tím dokázala poradit (...)*“ či nedostatku znalostí a zkušeností, což se může promítnout také do výuky daného učitele: „*V podstatě se tak nějak držím toho, co bych jim měl říkat a říkám jim to, ale s většinou těch věcí nemám za prvý osobní zkušenost, jak se v tom tak úplně nepohybuju, a za druhý nemám ten nadhled*“.

Se svými e-bezpečnostními návyky a zvolenými řešeními jsou učitelé spokojeni: „*Spíš prostě z těch možností, co jsou, mi vyšel nejlíp*“ nebo „*Nepoužívám ho a jsem šťastnej, že ho nepoužívám*“. Opačný případ, kdy by učitel se svými návyky či používanými řešeními spokojen nebyl, jsme nezaznamenali.

5.1.13 Hodnocení druhých

Kategorie ***Hodnocení druhých*** se zabývá názorem učitelů na kompetence dalších osob v oblasti technické e-bezpečnosti. Učitelé toto hodnocení uváděli spontánně, aby blíže vyjasnili svůj postoj k určité záležitosti. Jelikož se obvykle vymezují vůči chování druhých, je většina hodnocení druhých osob kritických.

Kritika nesprávného chování. Někteří učitelé se negativně staví k chování:

- relativně neznámých osob: „*(...) zdaleka ne všichni (na jistém fóru) dodržovali to stejný na druhej straně. Mnozí se tam jako opravdu jenom bavěj a mystifikujou a není to pak, jak psali*“,
- svých žáků: „*Protože děti, těm v podstatě to bylo jedno, kam jdou, protože když jsou navíc někde v jiný síti, tak to zobrazím, je mi to fuk*“,

- svých kolegů: „*Do toho notebooku se děti dostaly, většinou protože paní učitelka s prominutím byla takový trdlo, že jim to heslo řekla a jakmile ho řekla v jedné třídě, tak to věděla celá škola*“ a
- svých přátel: „*Mám kamarádku, která bezhlavě, když jede na dovolenou, všech 200 fotek, který udělá na tý dovolený u moře, a ona je fakt hezká, tak okamžitě druhej den, jak se vrátí z dovolený, dá na Facebook. Já bych řekl, že je dost blbá (...)*“.

Kritika správce vs. uživatele. Učitelé, kteří spravují počítačovou síť školy (nebo její část), hodnotí negativně žáky i své kolegy za nezodpovědné chování k digitálním technologiím: „*Učitelé tedy bohužel mají flashky povolený a pak to podle toho vypadá, že mi tam občas něco přijde (hlášení o útoku malware), a někteří to moc neřeší*“. Jeden z oslovených učitelů naopak kritizoval správce školní počítačové sítě za příliš restriktivní nastavení: „*Vzhledem k tomu, že si nemůžete ani naformátovat ani vlastní flashku, tak to zrovna není příjemná záležitost a na některých počítačích nejde změnit nějaký nastavení, aniž bych byl správce nebo síťař. (...) Tak to člověka naštve (...)*“. Další z učitelů, který spravuje školní počítačovou síť, tento názorový střet potvrdil slovy: „*Každej učitel Vám řekne, že je pro bezpečnost, že bezpečnost je strašně důležitá, ale myslí na žáky. Nemyslí na sebe. (...) Čili platí taková ta zásada: »Ano, bezpečnost je výborná, ale ne u mne. Neboli mne nesmí omezovat«*“.

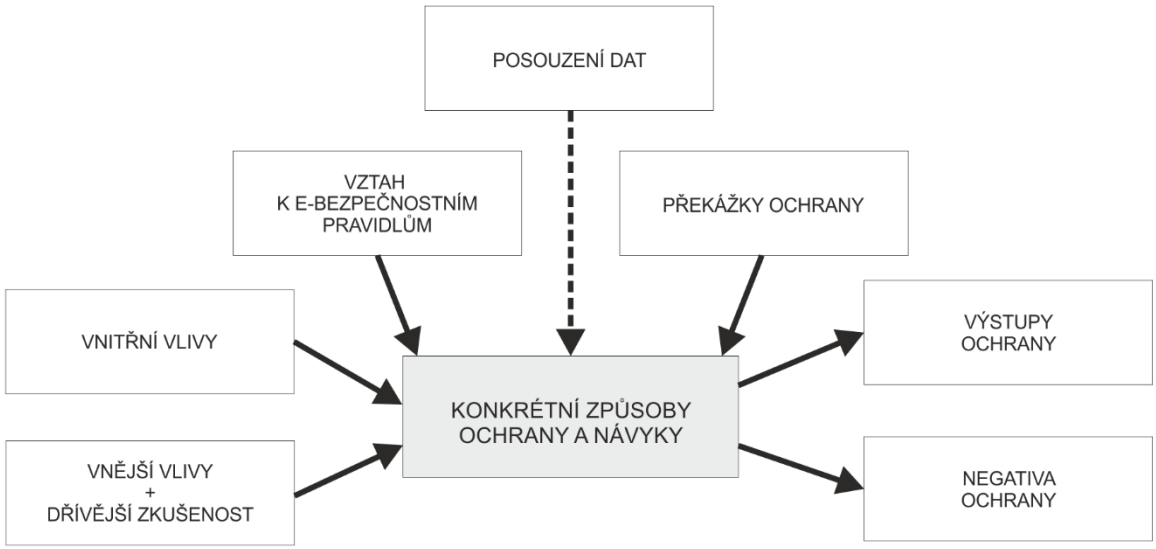
Souhlas s chováním druhých se ve výpovědích učitelů objevuje velice zřídka. Zaznamenali jsme jen příklady, kdy učitel pochválil člena své rodiny za chování na sociálních sítích (tehdy učitel jako příklad člověka obezřetně nakládajícího se soukromými informacemi uvedl svou manželku) a kdy jiný učitel podpořil pravidla svého kolegy při přátelení se se žáky na sociálních sítích: „*Jeden kolega, který je ze základky, tam má, a to se mi hrozně líbí, ten tam má napsáno: »Nepřijímám žádosti osob mladších 15 let až na čestné výjimky« (...)*“.

5.2 Proces utváření kompetencí učitelů ICT

5.2.1 Hlavní model utváření kompetencí učitelů ICT

Na základě výzkumu byl vytvořen model utváření kompetencí učitelů ICT z pohledu získávání způsobů ochrany. Z tohoto hlediska jsou centrální kategorií modelu ***Konkrétní způsoby ochrany a návyky***, tedy metody a rutiny, jimiž se učitelé ICT brání před negativními jevy při používání digitálních technologií. Vztahy mezi touto a ostatními kategoriemi můžeme rozdělit na vlivy na tyto rutiny a na důsledky těchto rutin.

Mezi vlivy patří ***Vnější vlivy***, ***Vnitřní vlivy***, ***Vztah k e-bezpečnostním pravidlům***, ***Překážky ochrany*** a ***Posouzení dat***. Podle zvoleného typu ochrany vznikají ***Výstupy ochrany*** a mohou vznikat také ***Negativa ochrany***. Podrobný popis jednotlivých kategorií jsme uvedli v kapitole 5.1; schéma vztahů mezi kategoriemi modelu je zachyceno v diagramu v Obrázku 12. Vztahy mezi kategoriemi jsou v diagramu znázorněny šipkami, které ukazují směr ovlivňování.



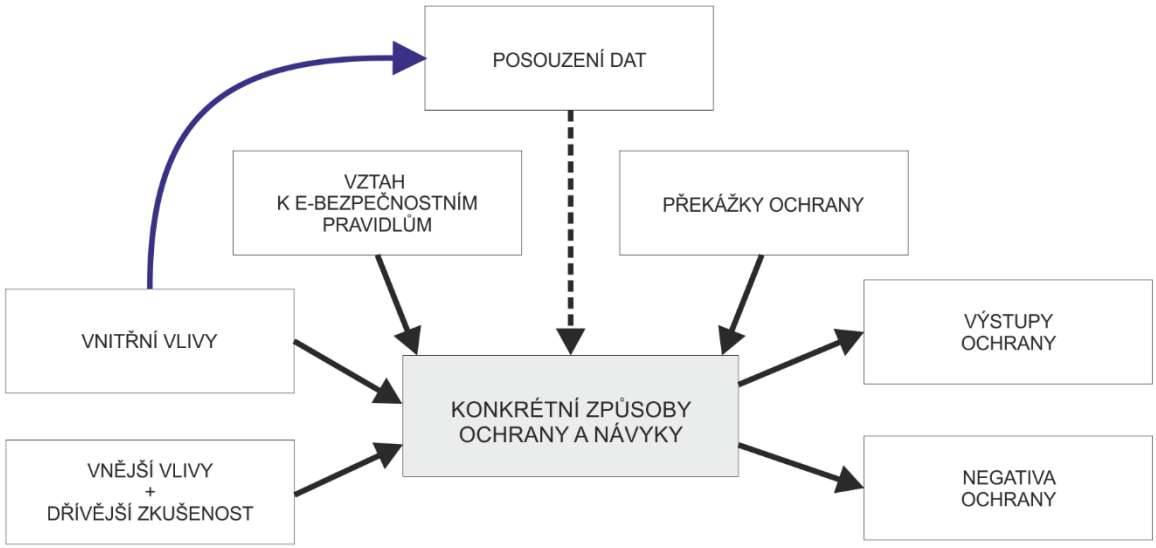
Obrázek 12: Vztahy mezi kategoriemi v základním modelu utváření kompetencí učitelů ICT. Vztah ***Posouzení dat*** k hlavní kategorii je zobrazen přerušovanou čárou, neboť jde o intervenující podmínku popisovaného procesu (na rozdíl od ostatních šipek představujících příčinné vlivy)

Na ***Konkrétní způsoby ochrany a návyky*** v modelu příčinně působí kategorie ***Vnější vlivy*** (kam zahrnujeme i dřívější negativní zkušenost), ***Vnitřní vlivy***, ***Vztah k e-bezpečnostním pravidlům*** a ***Překážky ochrany***. Kategorie ***Posouzení dat*** je v modelu intervenující podmínkou. Důsledkem ***Konkrétních způsobů ochrany a návyků*** jsou kategorie ***Výstupy ochrany*** a ***Negativa ochrany***. Zatímco některé vztahy mezi kategoriemi

jsou z hlediska fungování modelu triviální povahy a stručně jsme je popsali během deskripce jednotlivých kategorií v kapitole 5.1, v následujícím textu se budeme zabývat popisem vztahů, ve kterých je potřeba k odlišení případů použít dimenzionální škály vlastností v rámci kategorií.

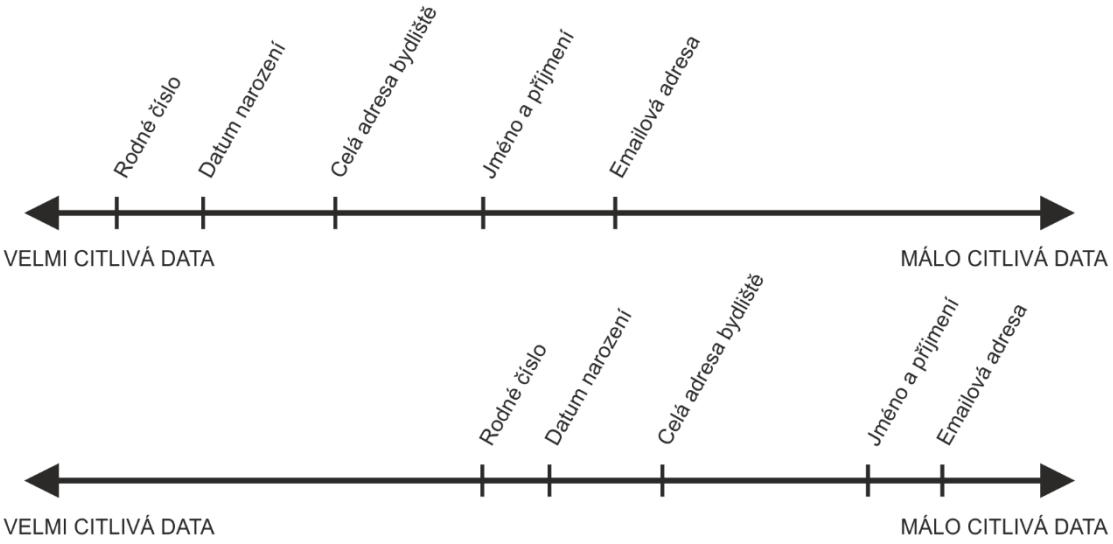
5.2.1.1 Role Vnitřních vlivů

Kategorie ***Vnitřní vlivy*** působí na několik kategorií modelu; zřejmý je vliv na kategorie ***Posouzení dat*** a ***Konkrétní způsoby ochrany a návyky***, pravděpodobný je vliv na ***Překážky ochrany*** a ***Vztah k e-bezpečnostním pravidlům***. Obrázek 13 ukazuje upravený model utváření kompetencí učitelů ICT, který zohledňuje uvedený zřejmý vliv na další kategorie modelu. V následujícím textu se budeme postupně zabývat jednotlivými vztahy.



Obrázek 13: Působení ***Vnitřních vlivů*** na další kategorie modelu utváření kompetencí učitelů ICT

Působení na *Posouzení dat*. *Posouzení dat* je ovlivňováno důvěřivostí či nedůvěřivostí učitele a mírou jeho opatrnosti. Čím je učitel v oblasti technické e-bezpečnosti nedůvěřivější a opatrnější, tím více považuje svá data za citlivá a cenná: „*Adresu bydliště bych jim asi neposkytl. To mi připadá, že to přece nikdo normální nepotřebuje, kdo poskytuje články*“. Obrázek 14 ukazuje příklad hodnocení citlivosti svých dat dvěma učiteli – jedním méně opatrným a druhým více opatrným.



Obrázek 14: Příklad hodnocení citlivosti osobních dat dvěma učiteli. Horní škála zachycuje hodnocení opatrnějšího učitele, dolní škála hodnocení méně opatrného učitele

Podobně lze říci, že čím je učitel v oblasti technické e-bezpečnosti nedůvěřivější a opatrnější, tím méně považuje zdroje, se kterými interaguje, za důvěryhodné.

Působení na *Konkrétní způsoby ochrany a návyky*. *Konkrétní způsoby ochrany a návyky* mohou být ovlivňovány přímo ***Vnitřními vlivy***, tedy bez mezičlánku v podobě další kategorie. Na učitelovy konkrétní způsoby ochrany a návyky může působit projekce role učitele, jeho přemýšlivost a pragmatičnost či zásadovost. Příkladem působení pragmatičnosti budiž situace, kdy se učitel potřebuje registrovat k neznámé online službě: „*Tak asi kdybych ho (nějaký dokument) potřeboval, tak bych se registroval nějakým vymyšleným jménem (...)*“.

5.2.1.2 Role Posouzení dat

Role cennosti a citlivosti dat spočívá ve vlivu cennosti a citlivosti dat na centrální kategorii modelu. Jelikož je pro učitele prakticky nemožné chránit veškerá svá data maximálním možným způsobem, podle tohoto faktoru se učitel rozhoduje, jakým způsobem (a tedy jak silně) bude konkrétní data chránit. Čím více učitel vnímá konkrétní data jako cennější či citlivější, tím silnější způsob ochrany volí. Následující výrok ilustruje uvažování nad zvolenou intenzitou zálohování dat: „*Fotky jsou (...) asi to nejdůležitější, co zálohuju. Možná je zálohuju víc, než ty dokumenty, což by asi mělo bejt naopak*“.

Role důvěryhodnosti zdroje spočívá ve vlivu důvěryhodnosti zdroje na centrální kategorii modelu. Jelikož je pro učitele prakticky nemožné být maximálně obezřetný při interakci s jakýmkoliv zdrojem, podle faktoru ***Posouzení dat*** se rozhoduje, jak moc bude

opatrný při interakci s určitým zdrojem. Čím méně učitel považuje určitý zdroj za důvěryhodný, tím opatrnější při interakci s ním je. Následující citace ilustruje rozhodování nad zadáním e-mailové adresy do webového formuláře: "*Když budu mít pocit, že to je důvěryhodný, (...), tak pak asi jsem schopen asi zadat ten svůj novej nebo školní mail. Pokud trošku mám pocit, že to tam k tomu není, tak zadávám prostě ten svůj spamovej mail*".

5.2.1.3 Znalost e-bezpečnostních pravidel vs. jejich dodržování

Učitele lze podle vztahu k e-bezpečnostním pravidlům (a bezpečným postupům) rozdělit podle dvou kritérií:

- Znalost e-bezpečnostních pravidel (a bezpečných postupů práce)
- Chování podle těchto pravidel (a používání bezpečných postupů práce)

Jelikož jsou tato dvě kritéria klasifikace na sobě nezávislá, existují ve vztahu k e-bezpečnostním pravidlům celkem čtyři skupiny učitelů:

- Učitelé, kteří e-bezpečnostní pravidla znají a dodržují je
- Učitelé, kteří e-bezpečnostní pravidla znají, ale nedodržují je
- Učitelé, kteří e-bezpečnostní pravidla neznají a nedodržují je
- Učitelé, kteří e-bezpečnostní pravidla neznají, ale chovají se v duchu těchto pravidel

Učitelé, kteří se chovají v duchu e-bezpečnostních pravidel, aniž by znali jejich znění, tak činí obvykle na základě vlastní intuice a přemýšlení o problematice. Jeden učitel například na náš dotaz, proč si data uchovává na více místech zároveň, odpověděl: „*Jednak protože bych mohl fyzicky přijít o tu flashku a jednak nevím, jak ona je odolná jako taková vůči nějakýmu poškození virama nebo stárnutím nebo takhle (...)*".

Opačný rozpor mezi znalostmi učitelů a jejich chováním lze nalézt u učitelů, kteří sice e-bezpečnostní pravidla znají, ale zároveň přiznávají jejich nedodržování. Jeden učitel například vypověděl: „*Samozřejmě, učím o tom, že by se ty hesla měly střídat, měly by bejt nějak dlouhý, ale mám pocit, že to nějak nedodržuju. I když to teoreticky vím*". Důvodem, proč se tito učitelé podle e-bezpečnostních pravidel nechovají, ač je znají, jsou ***Překážky ochrany***.

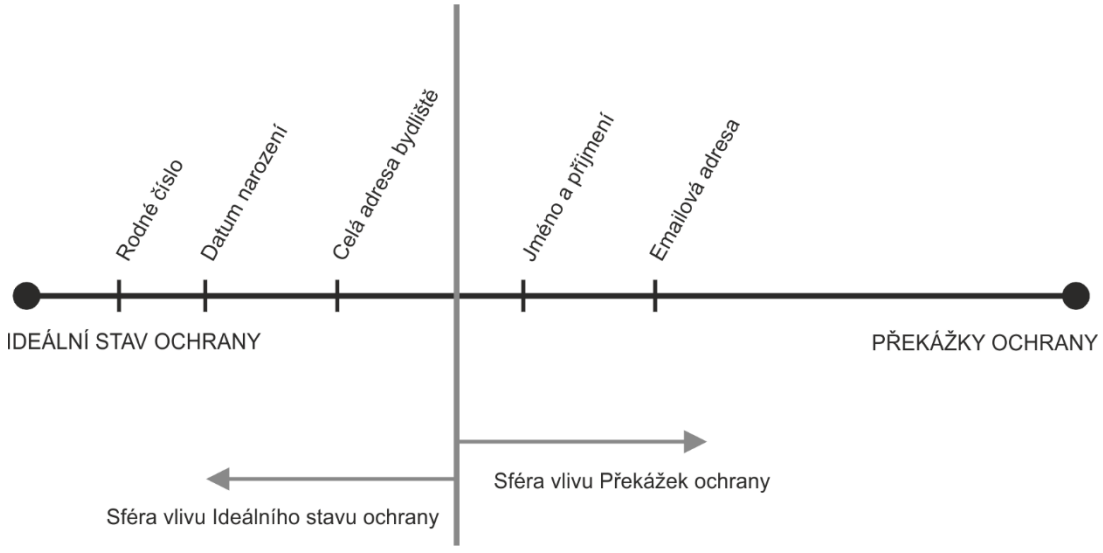
> **Exkurz 15.** Jednoho z učitelů, který se v rámci rozhovoru několikrát zmínil, že nedodržuje určitá e-bezpečnostní pravidla, ač je zná, jsme se zeptali, proč na tento rozpor upozorňuje. Odpověděl, že to nečiní záměrně a patrně tím chce podvědomě ukázat, že problematice teoreticky rozumí a je kompetentní ji učit.

5.2.1.4 Ideální stav ochrany vs. Překážky ochrany

Učitel činí vědomý či nevědomý kompromis mezi ***Ideálním stavem ochrany*** (zakotveným v e-bezpečnostních pravidlech) a omezeními, která jsou dána ***Překážkami ochrany***. Jedna učitelka například vypověděla: „*Snažím se (pravidelně měnit hesla), ale tím, jak je to fakt náročný na paměť, (...) to asi nedělám tak často, jak bych měla (...)*“.

Proces utváření konkrétního chování učitele lze dobře demonstrovat na příkladu překážek, které spočívají v nárocích zvoleného způsobu ochrany na osobu učitele (například časová náročnost ochrany či nároky na zapamatování). Tuto problematiku si lze představit jako dva soupeřící antagonismy – ***Ideální stav ochrany*** a ***Překážky ochrany***. Velikost sféry vlivu ***Překážek ochrany*** se přitom může v čase měnit v závislosti na individuálním posouzení závažnosti překážek učitelem.

V tomto bodě vstupuje do procesu rozhodování o konkrétním způsobu ochrany faktor ***Posouzení dat***. Učitel se tehdy rozhoduje, pro jaká data použije silný způsob ochrany a pro která slabší. Čím jsou konkrétní data pro učitele důležitější, tím více je posouvá do sféry vlivu ***Ideálního stavu ochrany*** (a tím se jejich ochrana více podobá tomuto ***Ideálnímu stavu ochrany***). Čím jsou naopak data pro učitele méně důležitá, tím více se dostávají do sféry vlivu ***Překážek ochrany*** (a tím méně je bude učitel chránit). Následující citace vystihuje rozhodování učitele o poskytnutí osobních dat při registraci k online službě: „*Jméno, příjmení (bych dal) taky, ale už bych neudával třeba datum narození, telefonní číslo nebo adresu, rodný číslo vůbec ne (...) Ale e-mail a jméno, příjmení, to bych jim asi poskytl*“. Na Obrázku 15 je pak tento konkrétní příklad zachycen schematicky.



Obrázek 15: Příklad stanovení osobních údajů, které bude učitel zadávat při registraci k online službě (umístěné ve sféře vlivu ***Překážek ochrany***) a které nikoliv (ve sféře vlivu ***Ideálního stavu ochrany***). Umístění

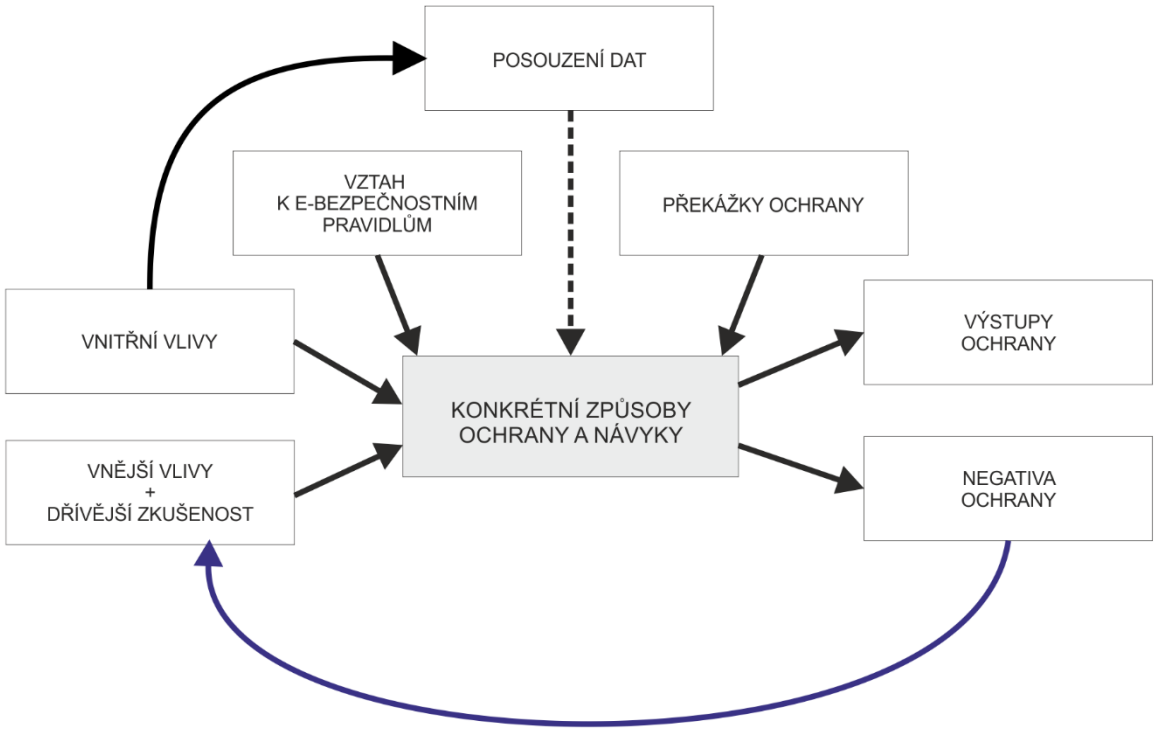
rozhraní mezi oběma sférami se může měnit v závislosti na individuálním posouzení závažnosti překážek ochrany učitelem.

Podobný princip lze nalézt u vnímání různých zdrojů – čím je daný zdroj pro učitele méně věrohodný, tím více jej posouvá do sféry vlivu ***Ideálního stavu ochrany*** (a tím se učitelova ochrana více podobá tomuto ideálnímu stavu). Čím jsou naopak zdroj pro učitele více věrohodný, tím více se dostává do sféry vlivu ***Překážek ochrany*** (a tím méně se učitel při interakci s ním bude chránit).

5.2.1.5 Reakce na negativum ochrany

V případě výskytu negativa ochrany se učitel musí rozhodnout, zda se s tímto omezením smířit a zůstat nadále silně chráněn, nebo danou ochranu opustit. K opuštění dosavadní ochrany dojde v důsledku převážení negativa ochrany, kdy učitel přehodnotí své způsoby ochrany a začne se chránit slaběji.

Výše uvedené možnosti reakce na negativum ochrany demonstrují následující dvě výpovědi učitelů o obměňování hesel. Smíření se s negativem ochrany najdeme ve výpovědi „*Jak jich mám víc, těžko si to pamatovat. Často se hodně obtížně dostávám do mailu (...) A k těm starším službám už prostě nevím, jaký tam bylo heslo*“. Opuštění ochrany je patrné v „*Já jsem to dělal, ale pak jsem si to vždycky pletl. Nový heslo – starý – nový – starý (...), tak jsem nechal pořád jedno a to stejný*“.



Obrázek 16: Vliv ***Negativ ochrany*** na ***Vnější vlivy*** ochrany: Opuštění ochrany na základě ***Negativ ochrany***

5.2.1.6 Negativní zkušenost a reakce na ni

Učitel může v oblasti technické e-bezpečnosti prožít určitou negativní zkušenost. V následujícím textu se omezíme na chápání negativní zkušenosti jako výstupu ochrany (ačkoliv negativní zkušenost může vzniknout nezávisle na ***Konkrétních způsobech ochrany a návycích*** učitele, jak diskutujeme v kapitole 5.1.1) [25].

> **Exkurz 16**. V rámci rozhovorů jsme kromě negativní zkušenosti zaznamenali příklady pozitivní zkušenosti, kdy učitel díky vhodně zvolenému způsobu ochrany předešel rizikové situaci nebo ji díky vhodnému návyku elegantně vyřešil. Výsledkem této pozitivní zkušenosti je spokojenost s daným návykem a případně jeho upevnění, kdy by učitel řešil obdobnou situaci stejným způsobem i v budoucnu. Jeden učitel na náš dotaz, jak by řešil situaci, kdy dochází opakovaně k „zamrzání počítače", odpověděl: „*Zkusil bych ten počítač restartovat, jestli by to pomohlo, jestli by naběhnul znova, někdy v notebooku třeba i vyndám baterii (...) S tímhletím mám dobrou zkušenost, že baterku úplně vyndám*".

Možné důsledky negativní zkušenosti jsou následující:

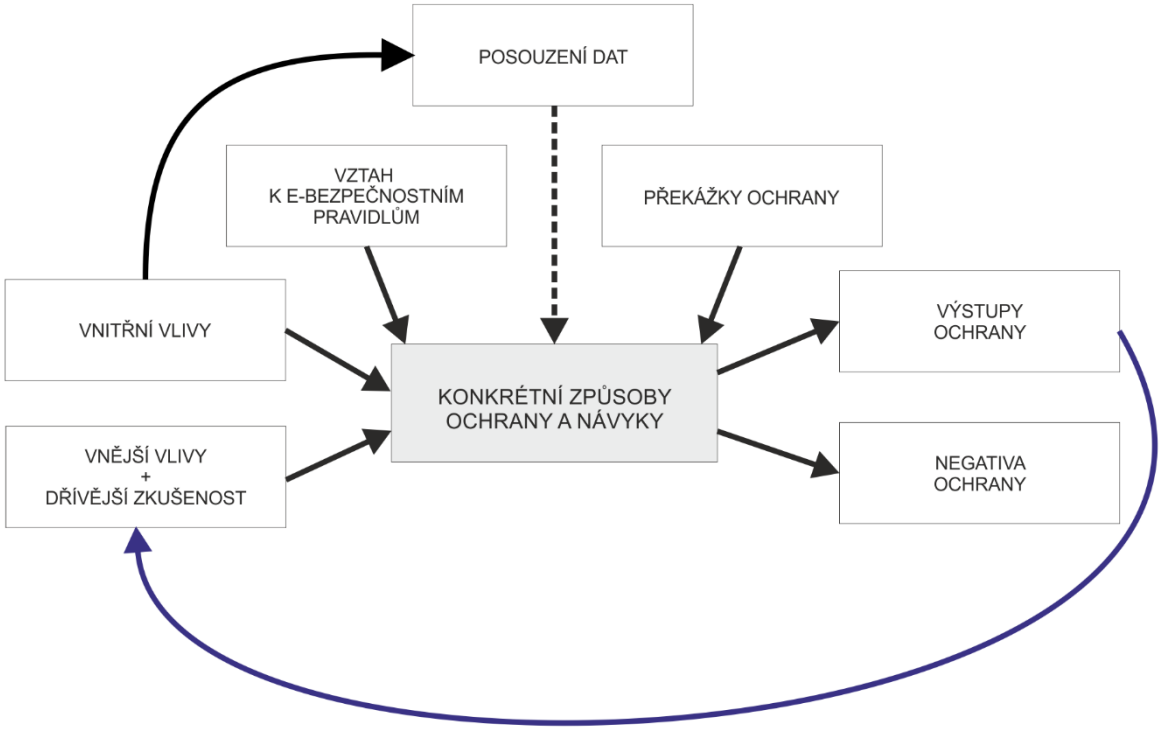
- bezpečnější chování
- zlepšení znalostí a dovedností
- ovlivnění psychických vlastností a emocí spojených s technickou e-bezpečností

Bezpečnější chování. Učitel se může začít chránit silněji, jestliže převáží přínos ochrany nad překážkami ochrany a učitel má pocit, že je výhodné se začít lépe chránit. V modelu z Obrázku 15 se tato situace projeví tak, že učitel začne posuzovat svá data jako cennější či citlivější, v důsledku čehož se konkrétní data dostanou ze sféry vlivu ***Překážek ochrany*** do sféry vlivu ***Ideálního stavu ochrany***.

Tato situace často nastává na základě negativní zkušenosti, z níž se učitel poučí a zlepší své e-bezpečnostní návyky. Toto ilustruje následující citace, která ukazuje, proč jeden z učitelů začal zálohovat svá data: „*Strašně mne vytrestalo to, že jsem přišel o jedinečný dílo, který už nikdy zpátky dohromady nedám a do dneška neexistuje, a tak jsem se začal tímto způsobem bránit (tj. pravidelně zálohovat). Asi kdyby se mi to nestalo, tak bych tak důslednej*

[25] Negativní zkušenost nelze zpravidla zaměňovat za negativum ochrany, ačkoliv oba typy jevů mají na učitele negativní dopad. Zatímco negativum ochrany je jev vzniklý v důsledku velmi bezpečného způsobu ochrany, negativní zkušenost obvykle naopak vzniká při nedodržení e-bezpečnostních pravidel.

nebyl“. Jestliže učitel před negativní zkušeností dané e-bezpečnostní návyky měl, mohou se tím tyto návyky upevnit: „*Což to já jsem věděl předtím (že mám zálohovat data). Mne to jenom potvrdilo, že je to třeba*“.



Obrázek 17: Poučení se z negativní zkušenosti, která plyne z nevhodně zvolených způsobů ochrany

Zdá se, že při procesu poučení se z negativní zkušenosti nezáleží, zda učitel před touto negativní zkušeností znal dané e-bezpečností pravidlo (a adekvátní bezpečnostní postup) či nikoliv. Pokud toto pravidlo znal, učitel může přejít ze skupiny osob, které sice dané e-bezpečnostní pravidlo znají, ale nechovají se podle něj, do skupiny osob, které dané e-bezpečnostní pravidlo znají a chovají se podle něj. Jeden učitel o zálohování pracovního počítače například vypověděl: „*Tady na tom počítači mi zkolaboval pevný disk (...) Já jsem si doslova zoufal, protože já jsem to v té době neměl zálohovaný (...) měl jsem něco vypálený na DVDčku, ale už zase rok starý nebo jak dlouho, to byla moje blbost teda, jo, že jsem to neměl zálohovaný. (...) Od té doby velice důsledně jednou týdně to zálohuju. (...) Přestože všechny děti učím zálohovat, zálohovat, zálohovat, tak sám jsem to nedodržel*“.

Negativní zkušenost však ve smyslu bezpečnějšího chování nemusí učitele vůbec ovlivnit. Zda jej negativní zkušenost ovlivní či nikoliv, závisí mimo jiné na osobnosti daného učitele či pocitu viny za daný problém – jestliže učitel svou vinu na problému odmítá, jeho chování se mnohdy nemění.

> **Exkurz 17.** V rámci výzkumu jsme zaznamenali případ učitele, který zaviroval pracovní počítač. Vzhledem k nepoužitelnosti počítače k běžné práci muselo být informováno oddělení informačních systémů, které zjistilo příčinu v přítomnosti viru a postaralo se o odstranění tohoto viru. Z výpovědi učitele vyplynulo, že si nebyl vědom nějaké konkrétní chyby, která by incident způsobila. Jako příčinu uvedl blíže neurčenou nepozornost při práci na Internetu, která se dle jeho vyjádření může stát. Podle svých slov nebyl učitel tímto incidentem ve svém chování ovlivněn.

Většina z oslovených učitelů, kteří sice e-bezpečnostní pravidla znají, ale podle svých slov je nedodržují, se při rozhovorech nezmínila, že by v dané problematice prožila nějakou negativní zkušenost. V kombinaci s poučením se z negativní zkušenosti u řady učitelů lze usuzovat, že učitelé, kteří prožili v určité problematice nějakou negativní zkušenost, dodržují příslušná e-bezpečnostní pravidla více než učitelé, kteří ji neprožili.

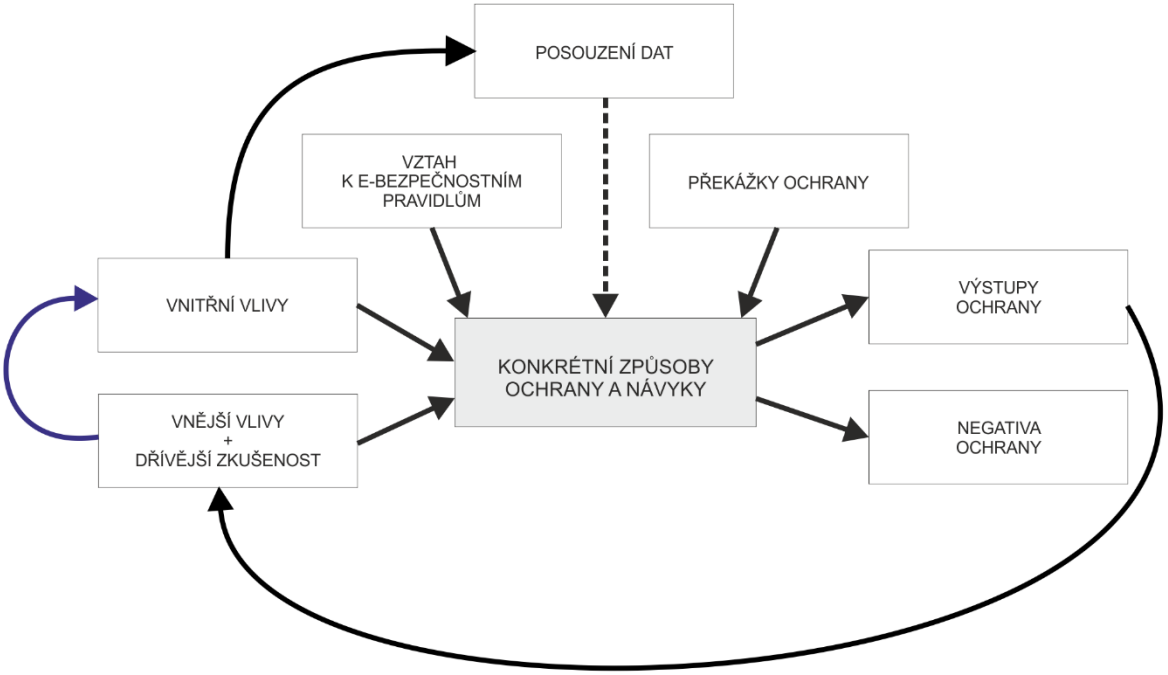
Negativní zkušenost a poučení z ní může mít i opačný než očekávaný a zmiňovaný pozitivní dopad na kvalitu ochrany dat. Příkladem tohoto opačného dopadu je opuštění ochrany na základě výskytu ***Negativ ochrany***. Tehdy jsou negativní zkušeností ***Negativa ochrany*** (např. učitel zapomněl své heslo) a úpravou chování je opuštění dané ochrany (např. učitel přestal hesla obměňovat).

Zlepšení znalostí a dovedností. Prodělaná negativní zkušenost může ovlivnit nejen chování učitele ve smyslu bezpečnějšího chování, ale také může zlepšit jeho znalosti či dovednosti v situaci, kdy se problémem začne zabývat. Nezáleží přitom, zda hledá příčiny problému nebo zda se snaží vyřešit jeho následky. Jeden z učitelů na náš dotaz, odkud čerpá své znalosti a dovednosti, například uvedl: „*Prostě párkrát se mi stalo, že se někdo někam naboural (...), nějaký viry jsem taky zachytil a věděl jsem, co s nima (...) Takže nějaký zkušenosti s tím jsou trošku vyšší, než má normální uživatel*“.

> **Exkurz 18.** Specifickým typem zlepšení dovedností na základě negativní zkušenosti je rozpoznávání nových znaků nebezpečí. Učitel tehdy začlení příznaky doprovázející situaci, která vyústila v negativní zkušenost, mezi rozpoznávané ***Znaky nebezpečí,*** aby v případě jejich příštího výskytu byl schopen dané riziko rozpoznat jistěji.

Projekce do psychických vlastností a emocí. Negativní zkušenost se také může promítnout do změn psychických vlastností a do emocí učitele spojených s technickou

e-bezpečností, které v modelu začleňujeme pod ***Vnitřní vlivy***. Učitel může začít být opatrnější, nedůvěřivější nebo mít obavu z opakování incidentu. Tyto změny posléze ovlivňují chování učitelů v problematice technické e-bezpečnosti. Následující citace ukazuje, proč učitel odmítá otevírat neznámé spustitelné soubory: „*Když se Vám zaviruje jeden počítač, tak to je malér, když se Vám zaviruje celá síť, tak je to na zbláznění. To už jsem tady zažil taky několik bezesných nocí, kdy jsem odcházel ze školy v pět ráno a myslel jsem si, že už mám všechny počítače vyčištěný, ráno to všichni zapnuli a bylo to znova. To není žádná sranda. Takže se bojím*“.



Obrázek 18: Projekce negativní zkušenosti, která plyne z nevhodného způsobu ochrany, do psychických vlastností a emocí

K výše uvedeným změnám nicméně nemusí dojít vždy. Jeden z učitelů například na náš dotaz, zda se někdy začal opakování incidentu obávat, odpověděl: „*Ne. Prostě byla to zkušenost, že se to stalo. Vím, jak to vyřešit pro příště nebo aspoň kdyby se stala podobná situace, tak jakým směrem se ubírat …*“.

Pokud jsou původci negativní zkušenosti osoby, o kterých měl učitel dobré mínění, může se u daného učitele projevit zklamání. Toto zklamání můžou způsobit například jeho žáci při vzájemné interakci na sociální síti: „*Z některejch těch informací (co publikovali na zdi sociální sítě Facebook) jsem byla úplně otřesená docela (…) Jakože v některejch dřímá to zlo úplně, hodně velký. A že to prostě pouštějí do světa*“.

5.2.2 Další zjištěné vztahy mezi kategoriemi

5.2.2.1 Reakce na Znaky nebezpečí

Jak jsme konstatovali v kapitole 5.1.8, spouštěčem pro konkrétní způsob ochrany před akutním nebezpečím jsou ***Znaky nebezpečí***, které učitelé rozpoznávají: „*(...) fotografie by neměly mít příponu exe. Exe jsou spustitelný soubory, takže asi bych neotvíral. (...) Všechny soubory, který se mi občas objeví v mailu, se spustitelnou příponou, tak mažu*“. ***Znaky nebezpečí*** však nemusejí adekvátní reakci vedoucí k eliminaci rizika spustit vždy – někteří učitelé přiznávají, že i přes rozpoznaný znak nebezpečí by možná v rizikovém chování pokračovali: „*Tady je velká pravděpodobnost, že bych to spustila, i když cítím, že by to nebylo správný, že bych se Tě nejdříve měla dotázat (...). Když to má tu příponu exe*“ nebo by přinejmenším zvažovali, jak se v dané situaci zachovat: „*Já bych ho třeba nesmazal, ale když tam byla přípona exe, tak mi to připadá, že když to je spouštěcí přípona, tak (...) kdyby to měly bejt jenom fotky, tak by tam mělo bejt jpeg*“.

Typickou překážkou ochrany, která brání učitelům reagovat na znak nebezpečí nejbezpečnějším možným způsobem, je nekritická důvěra ve známé či blízké osoby. Tehdy někteří učitelé předpokládají, že data zaslaná touto osobou (nebo jménem této osoby) pro ně nebudou představovat riziko, a na znak nebezpečí by nereagovali: „*Přiznám se, že od Tebe bych se asi podíval. Známejm, kamarádům v tomhle věřím, když mi něco pošlou*“. Jiní učitelé by se vzhledem k rozpoznanému znaku nebezpečí ve stejné situaci snažili původnost zprávy ověřit: „*Kdyby mi přišlo od nějakýho známýho exe soubor a já ho nečekal, tak napřed mu třeba zavolám, co to je*“ nebo by se snažili nezávadnost dat prověřit technickými prostředky: „*Když ho znám, tohodle člověka, tak řeknu ano, je to ze školy, tak v první řadě tam mám antivirovej program a ten nastavenej tak, aby mi to kontroloval*“. Další učitelé by vzhledem k rozpoznanému znaku nebezpečí i v této situaci zvolili stejný způsob ochrany, jako kdyby data pocházela od nedůvěryhodné osoby (viz citace na začátku předchozího odstavce).

5.2.2.2 Vztah učitele k druhým osobám

Jak jsme konstatovali v kapitole 5.1.13, jestliže učitelé hodnotí chování druhých osob, vyjadřují se obvykle kriticky. Tato kritika obvykle souvisí se zásadami daného učitele, jak se bezpečně (případně správně) chovat při používání digitálních technologií. Učitelé pak negativně hodnotí to, že druzí tyto zásady nedodržují: „*Vím, že takoví studenti u nás jsou, že si některé učitelé přidávají, a ti učitelé, že to potvrzují. Nebo možná i naopak to je. Mně to přijde trošku děsivý (...) Já mám zásadu tu, že dokud je ten dotyčný mým studentem, tak si*

ho nepřidávám, jakmile mým studentem být přestane, a on si mne třeba požádá o přátelství, tak si ho přidám“. Učitelova kritika může pramenit z jeho osobnosti: „*Mám tam (na Facebooku) pár dětí ze střední, z gymplu v přátelích a už jenom třeba z toho důvodu tam nezveřejňuju takhle ty stavy, protože nechci, aby to věděl úplně každej. Ale ty děti jsou sdílný úplně nehorázně*“ nebo může vzniknout na základě ***Vnějších vlivů***, typicky jestliže učitel prožije nějakou negativní zkušenost: „*On (virus) se mi nedostal do počítače, ale oni (žáci) mi přinesli práci na flashce nebo CD, tak jsem si to projel a bylo to zavirovaný (...) Ty děti nemusejí mít doma antivirový programy, (protože) to stojí peníze a myslí si, že není třeba to chránit, což je chyba. A když brouzdá po Internetu, tak neví, kdy si co stáhne*“.

Negativní zkušenost nemusí mít ve vztahu k druhým za následek pouze kritiku rizikového chování druhých osob, ale také aktivní snahu učitele přesvědčit další osoby, aby se chovaly bezpečněji: „*U těch předních (USB zdířek) se mi kolikrát stalo, že byly nefunkční, že mi odpálily flash disk, takže ze začátku jsem skutečně upozorňoval učitele na to, že flash disk je zařízení přenosné, nikoliv zařízení zálohovací*“.

Profese učitele a jeho osobní život spolu v oblasti technické e-bezpečnosti úzce souvisí. Zkušenostmi z výuky nebo z problémů řešených se žáky či kolegy mohou učitelé obohacovat své vlastní odborné znalosti, dovednosti či na jejich základě upravovat své chování: „*Člověk to (počet hesel) musí zredukovat, protože vím, že když jsme tady měli přihlašování do systému, tak ty děti zapomenou za měsíc heslo jenom proto, že je Windows vyzve, že si ho musí změnit*“. A opačně, své nově získané znalosti (zejména aktuálních informací) někteří učitelé operativně vkládají do své výuky: „*Když mne (známý ICT odborník) na něco upozorní, tak já to samozřejmě přenáším těm žákům. Obzvlášť pokud se to týká antivirové ochrany, nových virů, nebezpečí a podobně*“.

5.2.2.3 Konzultace s odborníky

Část učitelů spolupracuje s ICT odborníkem, se kterým konzultuje odborné záležitosti týkající se technické e-bezpečnosti (viz začátek kapitoly 5.1.9). Těmito odborníky mohou být členové širší rodiny, jejich přátelé a známí: „*Hodně čerpám od toho M., který pracuje pro tu firmu v Táboře, a známe se z dob, kdy u mne maturoval, takže jako nemám problém se zeptat, vysvětlí, pomůže*“. Kromě konzultací někteří učitelé své známé, kteří jsou ICT odborníky, žádají o přímou intervenci v případě problému: „*Zavolal bych kamarádům, kteří tomu rozumí, aby se mi na to přišli podívat. Tak to řeším standardně já. Vždycky, když se něco stane, na nic nesahám, a zavolám toho, kdo tomu rozumí*“.

Někteří učitelé, ačkoliv mají zájem o problematiku technické e-bezpečnosti, nemají možnost své otázky s nikým konzultovat. Jestliže dostanou příležitost mluvit s odborníkem na danou problematiku, snaží se načerpat nové informace. Příkladem budiž naše výzkumné rozhovory, během nichž se část učitelů aktivně ptala na témata, která je zaujala: „*(k tomuto tématu už doplnit nechci) asi nic, spíš mi řekněte, co tohleto znamená, když se to otevře? Abychom věděli …*“. Na konci rozhovorů, kdy jsme se učitelů ptali na dojem z rozhovoru, někteří z nich spontánně zhodnotili, že se během rozhovoru dozvěděli nové informace: „*Tak jsme si popovídali na zajímavý téma. Jsme si popovídali a zjistil jsem, že je možno rozesílat e-maily (z mé adresy), aniž by někdo znal mé heslo a tam se naboural, že jsou tam chybičky v tomhletom*“.

Spolupráci učitelů ICT s ICT odborníky je podle našeho názoru možno iniciovat při vysokoškolské přípravě učitelů ICT. Tehdy lze (na fakultách, kde se kromě učitelů ICT připravují i budoucí ICT odborníci) zajistit setkávání obou skupin studentů v některých kurzech tak, aby mezi nimi docházelo ke vzniku sociálních vazeb. Tyto vazby mohou přetrvat i po vstupu studentů do praxe.

5.2.3 Diskuze výsledků

V této kapitole budeme diskutovat některá významná zjištění obsažená v námi vytvořeném modelu s ohledem na dříve publikované teorie týkající se lidského chování. Chování respondentů odpovídá teorii operantního podmiňování podle Skinnera (2014) v tom, že se mění chování jedince (nebo uvažování o budoucím chování ve výpovědích) na základě důsledků jeho předchozího chování. Jde konkrétně o negativní zpevnění jako důsledek potřeby vyhnout se nepříjemným podnětům, tedy např. na základě negativní zkušenosti se ztrátou dat se mění chování jedince směrem k větší odpovědnosti při zálohování apod.

Chování respondentů odpovídá modelu triadického recipročního determinismu podle Bandury (Janoušek, 1992) v tom smyslu, že chování respondentů opravdu průběžně působí na jeho osobní charakteristiky a také na okolní prostředí (nejen je jimi ovlivňováno). Vliv na osobní charakteristiky je patrný v reakci na negativní zkušenost plynoucí z nevhodně zvoleného chování, kdy se učitel může stát opatrnějším či nedůvěřivějším. Působení na okolní prostředí je možno nalézt v situacích, kdy učitel aktivně mění e-bezpečnostní politiku školy, například realizuje restriktivní nastavení vedoucí ke snížení pravděpodobnosti e-bezpečnostního incidentu. Tuto situaci vystihuje následující citace: „*(...) Dřív tam na těch*

počítačích byly nějaký erotický snímky a tak dále. To bylo z toho důvodu, že tam měli ty práva a mohli všechno. Takže tohle všechno jsem nějakým způsobem musel začít řešit. Abych to nemusel jenom opravovat. Teď mají studenti nějaký nastavení na serveru, který se načte, a v podstatě nemají k dispozici Ovládací panely nebo tam se jim vnutí Plocha, taková tmavě modrá (...)".

Přijmeme-li model chování respondentů podle uvedené Skinnerovy teorie, nabízí se uvažovat o tom, jakým způsobem řídit, vést učení jedince ke zvládnutí jeho e-bezpečnosti. Negativní zpevnění může být realizováno tak, že vyučující zařídí negativní zážitek, který bude intenzívnější, pokud se bude více týkat osoby učícího se. Např. lze předpokládat, že přednáška o rizicích elektronického zabezpečení bude účinnější, pokud proběhne s pozvaným odborníkem, který bude dokumentovat na konkrétních případech příběhy lidí, s nimiž se učící se může ztotožnit. Ještě daleko účinnější bude osobní negativní zážitek s prolomením ochrany vlastních citlivých dat. Využitím obou uvedených přístupů ve výuce a jejich vlivem na kompetence učících se osob se zabýváme v kapitolách 4.2 a 5.3.

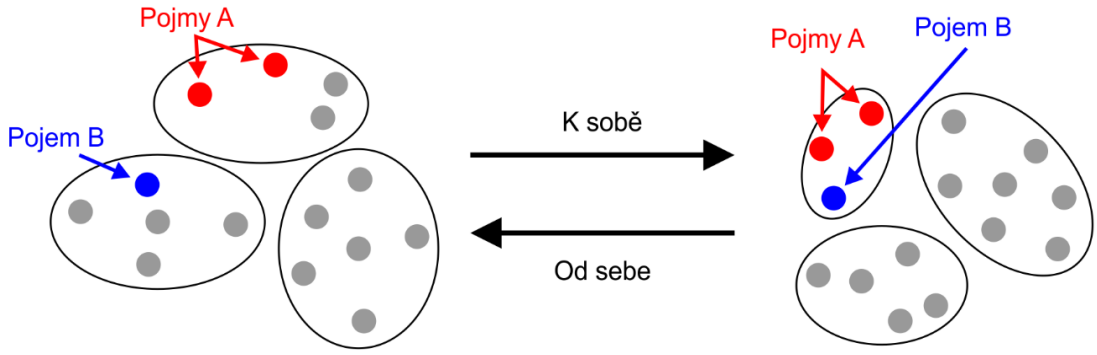
Další otázkou, vyplývající z teorie operantního podmiňování, je otázka vyhasínání a obnovování operantního chování. Vyhasínání a obnovování operantního podmiňování jsme během výzkumu zaznamenali – následující citace vyjadřuje přístup jednoho učitelů k zálohování svých dat: „*Už zase jsem (v zálohování) polevoval, od tý doby, co jsem ztratil ten koncert, už jsem trošku polevoval a pak mne to vytrestalo… Ztratil jsem pět stránek diplomky… A tím se mi to obnovilo, že musím dávat bacha a už zase zálohuju, zálohuju, zálohuju…*" Je však otázkou, zdali by ke zpevnění docházelo spíše u pravidelného nebo nahodilého posilování (např. pravidelné výzvy ke změně hesla u některých internetových služeb mohou být brány jako obtěžující a jedinec může vzít za negativní zážitek právě toto obtěžování jako snahu o omezení jeho svobody). K zodpovězení těchto otázek by byl potřeba longitudinální výzkum, zkoumající vývoj chování a povědomí o e-bezpečnosti v průběhu delší doby, ten však není součástí této práce.

5.3 Evaluace optimalizačního nástroje

5.3.1 Výsledky evaluace

V této kapitole popíšeme výsledky evaluace optimalizačního nástroje, jehož účelem je zvyšovat kompetence učících se osob v oblasti technické e-bezpečnosti, podle jednotlivých typů výuky. Výsledky budeme prezentovat z pohledu, jak daný typ výuky ovlivnil vnímání vybraných pojmů technické e-bezpečnosti respondenty. Pro každý typ výuky zde uvádíme následující informace:

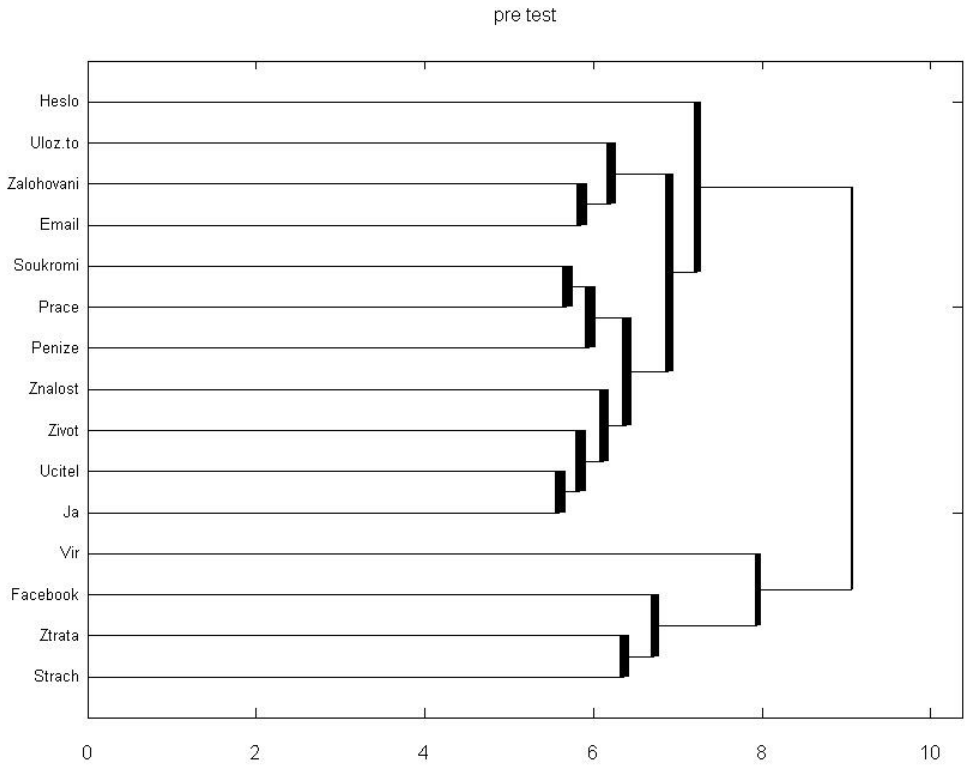
- Dendrogramy, zobrazující vzájemnou podobnost vybraných pojmů ve vnímání dané skupiny respondentů před výukou (tj. v pretestu) a po výuce (tj. v posttestu)
- Tabulku se seznamem přesunů pojmů mezi shluky při porovnání dendrogramů pretestu a posttestu. Do tabulky jsou zařazeny pouze přesuny pojmů, které obstály při porovnání s kontrolní skupinou. V řádcích tabulky:
    - Směr *K sobě* znamená, že v dendrogramu pretestu tvořily množiny *Pojmy A* a *Pojmy B* dva různé shluky, zatímco v dendrogramu posttestu vytvořily jeden shluk[26].
    - Směr *Od sebe* znamená, že v dendrogramu pretestu vytvořily množiny *Pojmy A* a *Pojmy B* jeden shluk, zatímco v dendrogramu posttestu tvořily dva různé shluky[26].
- Diskuzi zjištěných přesunů pojmů mezi shluky.



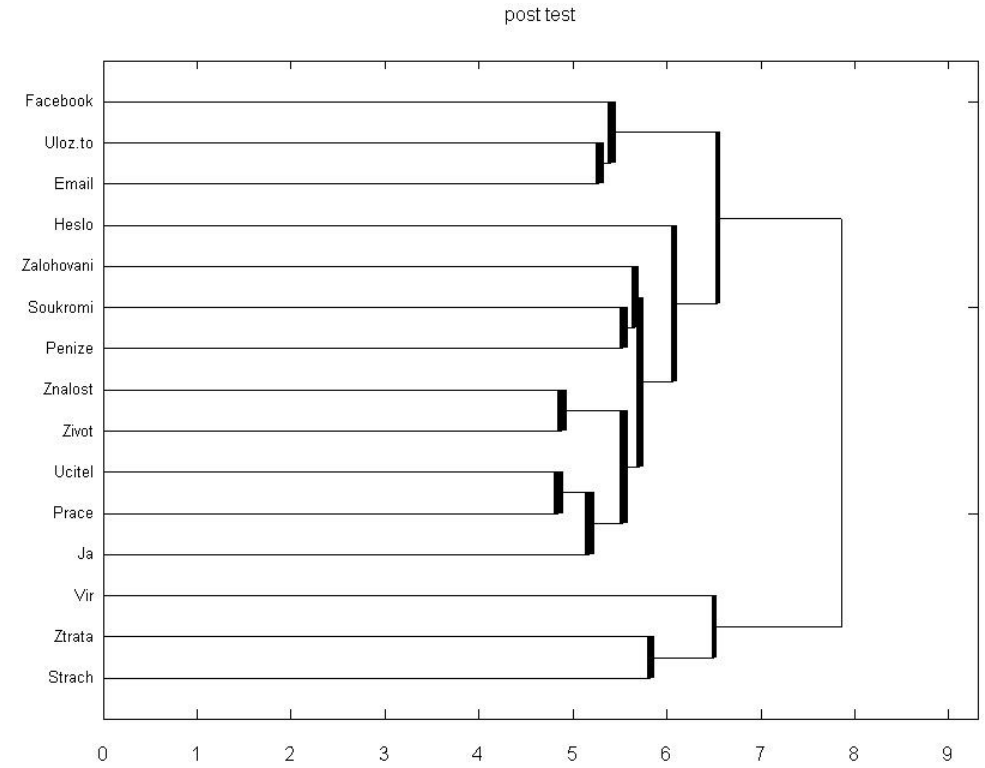
Obrázek 19: Ukázka přesunu pojmů mezi shluky při třech shlucích. Zatímco v diagramu vlevo tvoří *Pojmy A* a *Pojem B* dva různé shluky, v diagramu vpravo tvoří jeden shluk

[26] Toto srovnání bylo provedeno při rozkladu množiny všech pojmů na určitý počet shluků, který byl jednotný pro dendrogram pretestu i dendrogram posttestu. Tento počet shluků je uveden ve sloupci *Při počtu shluků*.

5.3.1.1 Zážitková výuka



Obrázek 20: Dendrogram pretestu pro **Zážitkovou výuku** – všichni respondenti, kteří absolvovali tento typ výuky



Obrázek 21: Dendrogram posttestu pro **Zážitkovou výuku** – všichni respondenti, kteří absolvovali tento typ výuky

Na základě analýzy dendrogramů z Obrázku 20 a Obrázku 21 byly u respondentů, kteří absolvovali **Zážitkovou výuku**, jako významné zjištěny přesuny pojmů uvedené v Tabulce 4.

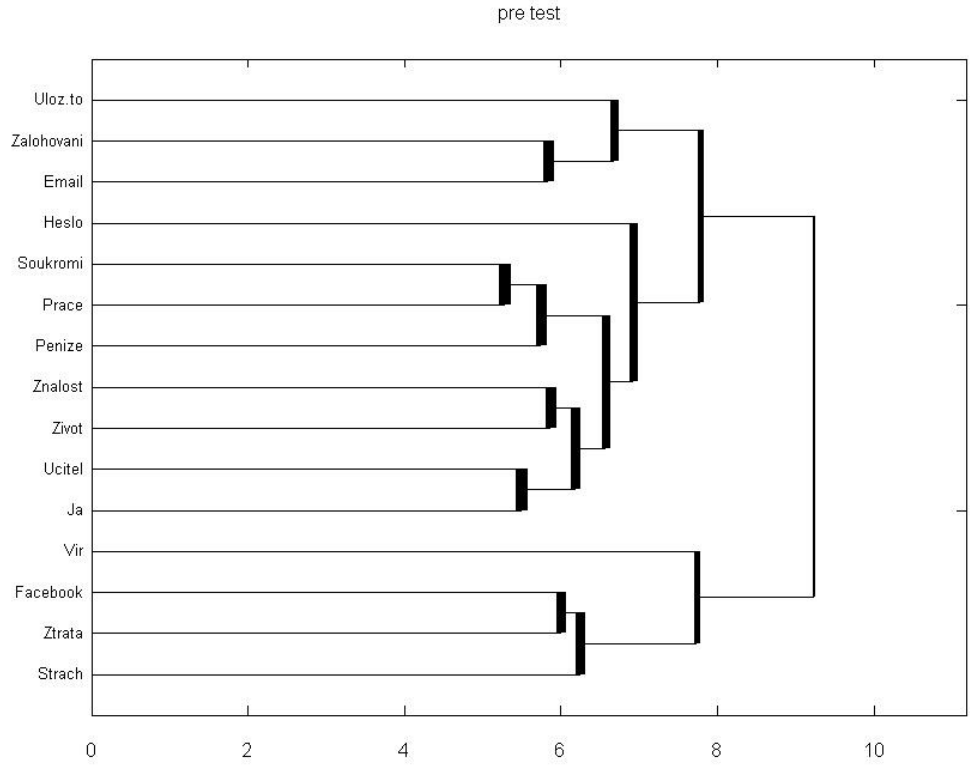
Tabulka 4: Přesuny pojmů mezi shluky pro **Zážitkovou výuku** – všichni respondenti, kteří absolvovali tento typ výuky

Pojmy A	Pojmy B	Směr	Při počtu shluků
Zálohování	Soukromí, Peníze	K sobě	7
Facebook	Ulož.to, E-mail	K sobě	10

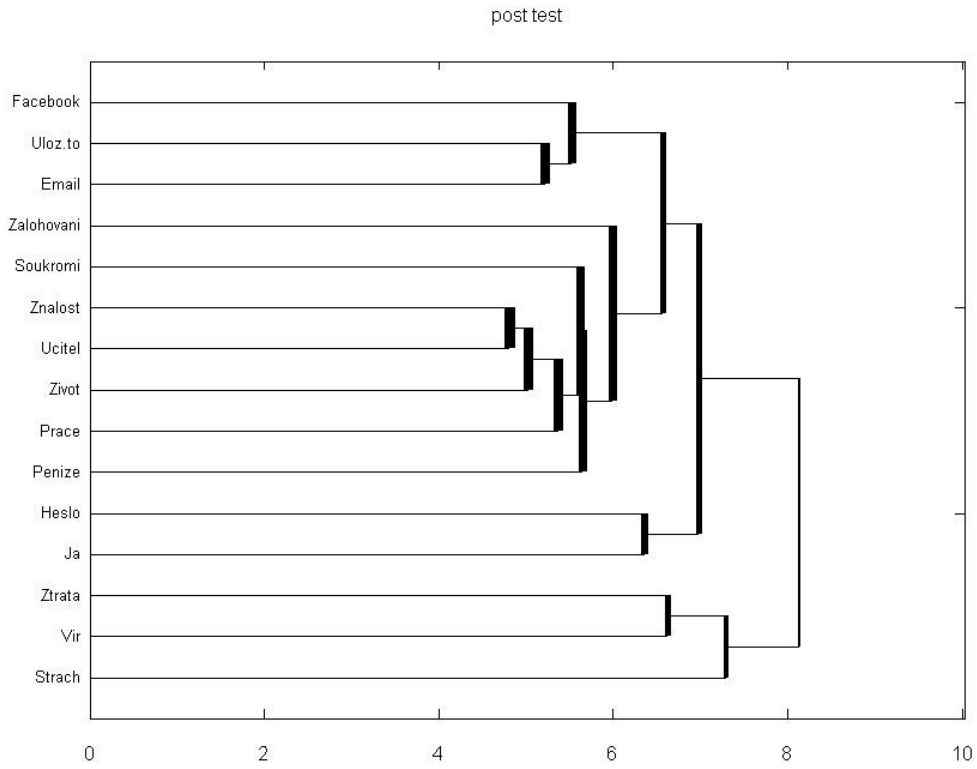
Přiblížení pojmu **Zálohování k** pojmům **Soukromí a Peníze** vysvětlujeme tak, že respondenti začali vnímat tyto pojmy jako navzájem si podobnější. To lze interpretovat tak, že **respondenti začali více vnímat, že zálohování dat může být klíčem k ušetření peněz** za zbytečné náklady spojené s obnovou a znovuvytvořením poškozených či ztracených dat. Dále se lze domnívat, že **začali zálohování dat vnímat jako metodu, jak si uchovat své soukromí**, zejména své soukromé vzpomínky a důležité dokumenty. Ačkoliv toto pravděpodobně nesouvisí s negativní zkušeností, kterou jsme v rámci **Zážitkové výuky** zprostředkovali, je možné, že to souvisí s částí výuky založené na výkladu učitele. Efektivnost výuky přitom mohla být zvýšena předchozími zážitkovými prvky implementovanými do výuky. Zjištěnou změnu ve vnímání dotčených pojmů **lze považovat za splnění cíle** použitého typu výuky, neboť dává naději, že respondenti po výuce považují zálohování za činnost chránící jejich data více než před výukou (a budou tedy dbát na zálohování svých dat pečlivěji než před výukou).

Přiblížení pojmu **Facebook** k pojmům **Ulož.to** a **E-mail** vysvětlujeme tak, že respondenti začali vnímat tyto pojmy jako podobnější. To lze interpretovat tak, že **respondenti si začali více uvědomovat spojitost jednotlivých služeb** spočívající v možnosti sdílet informace a data mezi různými uživateli. Ačkoliv toto pravděpodobně nesouvisí s negativní zkušeností, kterou jsme v rámci **Zážitkové výuky** zprostředkovali, je možné, že je zde souvislost s částí výuky založené na výkladu učitele. Jelikož však výuka nebyla primárně zaměřena na rozlišení různých typů cloudových služeb, ale na jejich vhodnost z hlediska uložení soukromých dat, **nepovažujeme** zjištěnou změnu ve vnímání dotčených pojmů **za splnění cíle** použitého typu výuky.

Zážitková výuka s rizikovou registrací



Obrázek 22: Dendrogram pretestu pro **Zážitkovou výuku** – pouze respondenti, kteří podlehli hrozbě rizikové registrace



Obrázek 23: Dendrogram posttestu pro **Zážitkovou výuku** – pouze respondenti, kteří podlehli hrozbě rizikové registrace

Na základě analýzy dendrogramů z Obrázku 22 a Obrázku 23 byly u respondentů, kteří absolvovali **Zážitkovou výuku** a zároveň kteří podlehli hrozbě rizikové registrace, jako významné zjištěny přesuny pojmů uvedené v Tabulce 5.

Tabulka 5: Přesuny pojmů mezi shluky pro **Zážitkovou výuku** – pouze respondenti, kteří podlehli hrozbě rizikové registrace

Pojmy A	Pojmy B	Směr	Při počtu shluků
Heslo	Já	K sobě	5
Heslo, Já	Soukromí, Práce, Život, Peníze, Znalost, Učitel	Od sebe	4
Vir	Ztráta	K sobě	4
Facebook	Ulož.to, E-mail	K sobě	10

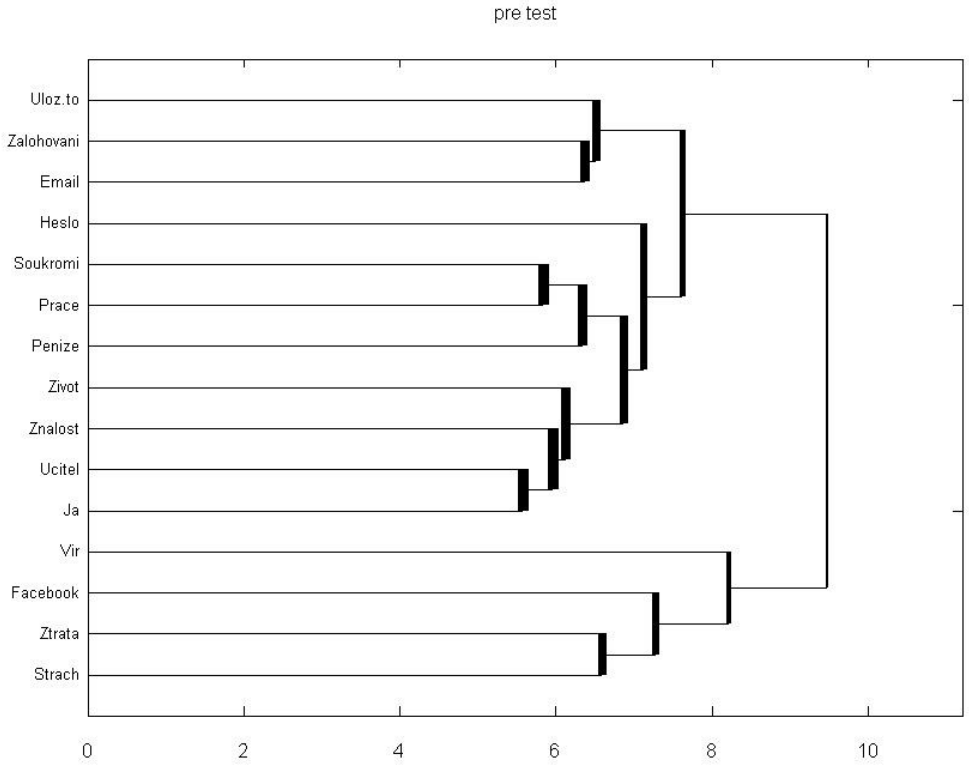
Přiblížení pojmu **Heslo** k pojmu **Já** vysvětlujeme tak, že respondenti začali vnímat tyto pojmy jako navzájem si podobnější. To lze interpretovat tak, že **respondenti si začali více uvědomovat, že heslo je klíčem k jejich osobnosti a datům** a že právě vhodná volba a ochrana hesla je způsobem, jak chránit sama sebe při používání digitálních technologií. Domníváme se, že toto úzce souvisí s negativní zkušeností, kterou jsme v rámci **Zážitkové výuky** zprostředkovali a kterou respondenti přímo zažili. Respondenti totiž byli během následné výuky poučeni, že odhalení hesla podobným způsobem může vést k ohrožení dalších služeb používaných uživatelem (např. e-mailové schránka, Facebook, školní informační systém). Uvedený posun ve vnímání pojmů Heslo a Já je dále umocněn oddálením těchto dvou pojmů od shluku pojmů Soukromí, Práce, Život, Peníze, Znalost a Učitel. Zjištěnou změnu ve vnímání dotčených pojmů **považujeme za splnění cíle** použitého typu výuky, neboť dává naději, že respondenti po výuce považují heslo za prvek chránící jejich osobu a data více než před výukou (a budou tedy při volbě hesla a práci s ním důslednější než před výukou).

Přiblížení pojmu **Vir** k pojmu **Ztráta** vysvětlujeme tak, že respondenti začali vnímat tyto pojmy jako navzájem si podobnější. To lze interpretovat tak, že **respondenti si začali více uvědomovat, že působení viru s sebou nese riziko určité ztráty** (například ztráty dat, ztráty soukromí či finanční ztráty). Domníváme se, že toto může souviset s negativní zkušeností, kterou jsme v rámci **Zážitkové výuky** zprostředkovali a kterou respondenti přímo zažili. Na základě prožité negativní zkušenosti spojené s demonstrací, jak snadno lze odhalit heslo uživatele a prolomit tak zabezpečení důležitých služeb vlivem působení hackera, si mohli respondenti uvědomit analogii, že podobně snadno může při neopatrném používání digitálních technologií dojít ke ztrátě dat z důvodu působení viru. Názor, jak je

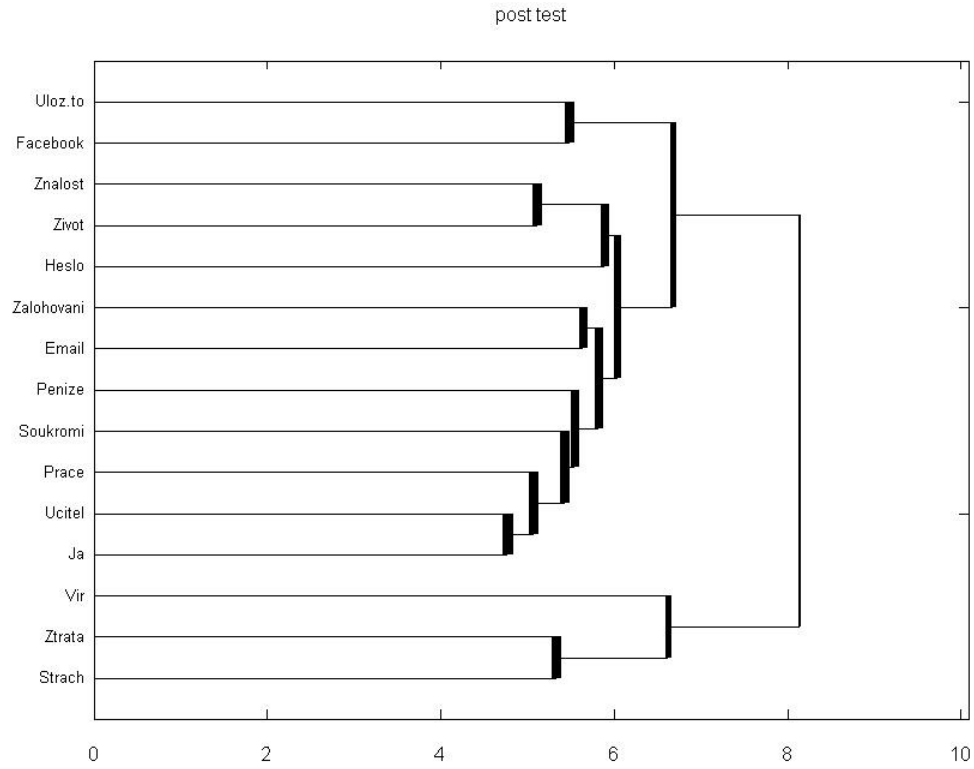
snadné se stát obětí e-bezpečnostní hrozby, přitom při výuce v rámci výkladu učitel uvedl. Zjištěnou změnu ve vnímání dotčených pojmů **lze považovat za splnění cíle** použitého typu výuky, neboť dává naději, že respondenti po výuce považují vir za negativní jev vedoucí k určité ztrátě více než před výukou (a budou se tedy před viry chránit důsledněji než před výukou).

Přiblížení pojmu **Facebook** k pojmům **Ulož.to** a **E-mail** vysvětlujeme tak, že respondenti začali vnímat tyto pojmy jako podobnější. To lze interpretovat tak, že **respondenti si začali více uvědomovat souvislost jednotlivých služeb** spočívající v možnosti sdílet informace a data mezi různými uživateli. Ačkoliv toto pravděpodobně nesouvisí s negativní zkušeností, kterou jsme v rámci **Zážitkové výuky** zprostředkovali, je možné, že to souvisí s částí výuky založené na výkladu učitele. Jelikož však výuka nebyla primárně zaměřena na rozlišení různých typů cloudových služeb, ale na jejich vhodnost z hlediska uložení soukromých dat, **nepovažujeme** zjištěnou změnu ve vnímání dotčených pojmů **za splnění cíle** použitého typu výuky.

Zážitková výuka s nebezpečným uváděním osobních údajů



Obrázek 24: Dendrogram pretestu pro **Zážitkovou výuku** – pouze respondenti, kteří podlehli hrozbě nebezpečného uvádění osobních údajů



Obrázek 25: Dendrogram posttestu pro **Zážitkovou výuku** – pouze respondenti, kteří podlehli hrozbě nebezpečného uvádění osobních údajů

Na základě analýzy dendrogramů z Obrázku 24 a Obrázku 25 byly u respondentů, kteří absolvovali **Zážitkovou výuku** a zároveň kteří podlehli hrozbě nebezpečného uvádění osobních údajů, jako významné zjištěny přesuny pojmů uvedené v Tabulce 6.

Tabulka 6: Přesuny pojmů mezi shluky pro **Zážitkovou výuku** – pouze respondenti, kteří podlehli hrozbě nebezpečného uvádění osobních údajů

Pojmy A	**Pojmy B**	**Směr**	**Při počtu shluků**
Ulož.to	E-mail	Od sebe	7
Ulož.to	Facebook	K sobě	8
Ztráta	Strach	K sobě	9

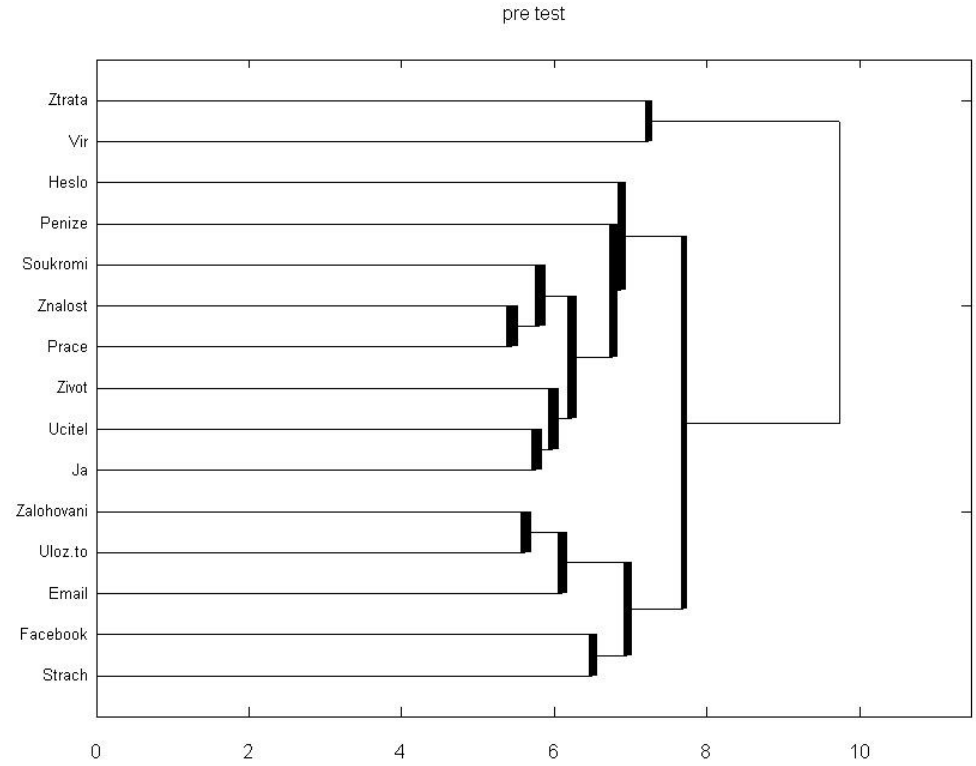
Oddálení pojmu **Ulož.to** od pojmu **E-mail** vysvětlujeme tak, že respondenti začali vnímat tyto pojmy jako navzájem méně podobné. To lze interpretovat tak, že **respondenti si začali více uvědomovat rozdíl mezi soukromými a veřejnými službami Internetu** – tedy že zatímco služba Ulož.to je do značné míry veřejným prostorem, který slouží ke sdílení dat mezi uživateli a je nevhodný k uchovávání osobních dat, e-mailová schránka je prostorem soukromým, do kterého by jiní uživatelé neměli mít přístup a ve kterém je možno osobní data uchovávat. Ačkoliv toto pravděpodobně nesouvisí s negativní zkušeností, kterou jsme v rámci **Zážitkové výuky** zprostředkovali, je možné, že to souvisí s částí výuky

založené na výkladu učitele. Zjištěnou změnu ve vnímání dotčených pojmů **lze považovat za splnění cíle** použitého typu výuky, neboť dává naději, že respondenti po výuce vnímají rozdíly mezi různými cloudovými službami více než před výukou (a budou tedy pečlivěji než před výukou zvažovat, jaká data konkrétní službě svěřit a jak se při práci s danou službou chovat).

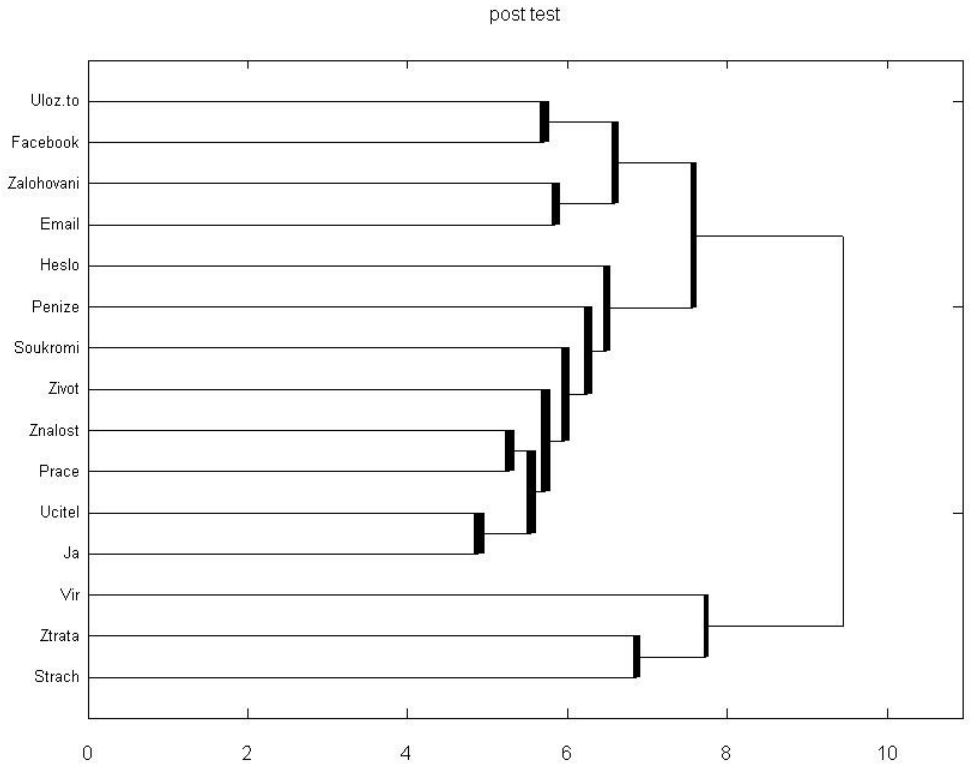
Přiblížení pojmu **Ulož.to** k pojmu **Facebook** vysvětlujeme tak, že respondenti začali vnímat tyto pojmy jako podobnější. To lze interpretovat tak, že **respondenti si začali více uvědomovat souvislost** obou služeb spočívající v publikování dat jedním uživatelem a jejich příležitostné konzumaci uživatelem jiným. Domníváme se, že toto může souviset s výše uvedeným oddálením pojmu Ulož.to od pojmu E-mail, v důsledku čehož se pojem Ulož.to přiblížil k jinému pojmu reprezentující online službu. Z tohoto důvodu **nepovažujeme** zjištěnou změnu ve vnímání dotčených pojmů **za splnění cíle** použitého typu výuky.

Přiblížení pojmu **Ztráta** k pojmu **Strach** vysvětlujeme tak, že respondenti začali vnímat tyto pojmy jako navzájem si podobnější. To lze interpretovat tak, že **respondenti začali více chápat ztrátu jako cosi nepříjemného**. Domníváme se, že toto může souviset s negativní zkušeností, kterou jsme v rámci **Zážitkové výuky** zprostředkovali a kterou respondenti přímo zažili. S respondenty bylo během následné výuky diskutováno, jaké důsledky může mít ztráta dat či ztráta kontroly nad jejich osobními daty, kdy učitel dával za příklad právě prožitou negativní zkušenost. Zjištěnou změnu ve vnímání dotčených pojmů **lze považovat za splnění cíle** použitého typu výuky, neboť dává naději, že ztráta bude respondenty po výuce vnímána jako cosi nepříjemného intenzivněji než před výukou (a budou se tedy před ztrátou dat či ztrátou kontroly nad osobními daty chránit důsledněji než před výukou).

5.3.1.2 Frontální výuka



Obrázek 26: Dendrogram pretestu pro **Frontální výuku**



Obrázek 27: Dendrogram posttestu pro **Frontální výuku**

Na základě analýzy dendrogramů z Obrázku 26 a Obrázku 27 byly u respondentů, kteří absolvovali **Frontální výuku**, jako významné zjištěny přesuny pojmů uvedené v Tabulce 7.

Tabulka 7: Přesuny pojmů mezi shluky pro **Frontální výuku**

Pojmy A	**Pojmy B**	**Směr**	**Při počtu shluků**
Vir	Ztráta	Od sebe	3
Ulož.to	Zálohování, E-mail	Od sebe	6
Ulož.to	Facebook	K sobě	8

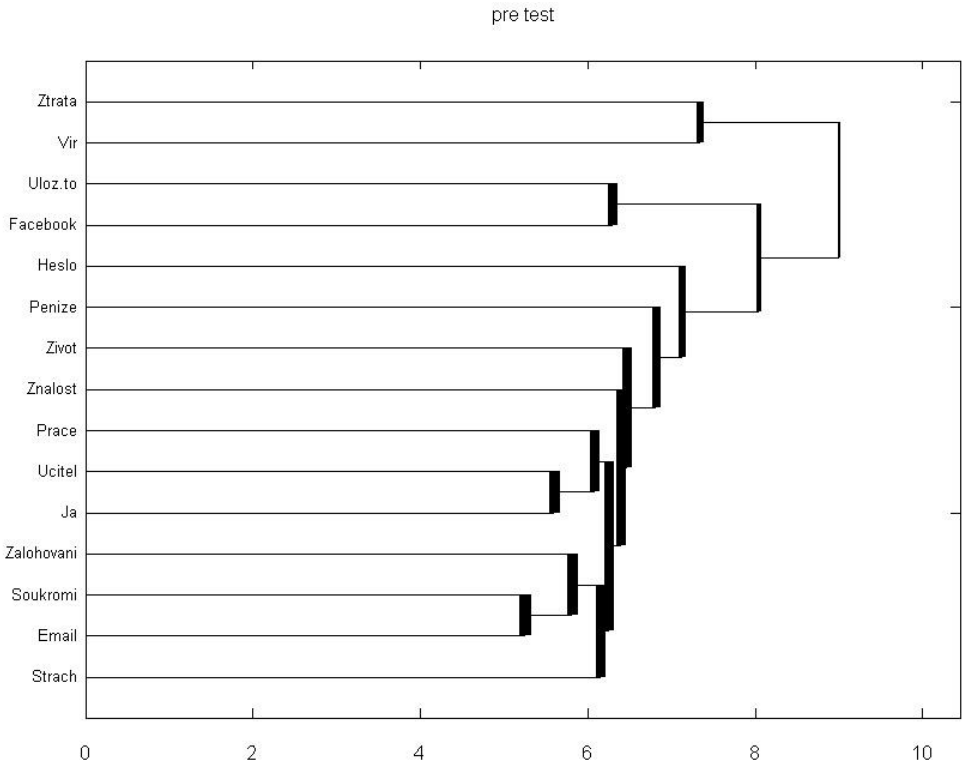
Oddálení pojmu **Vir** od pojmu **Ztráta** vysvětlujeme tak, že respondenti začali vnímat tyto pojmy jako navzájem méně podobné. To lze interpretovat tak, že **respondenti si začali méně uvědomovat, že působení viru s sebou nese riziko určité ztráty** (například ztráty dat, ztráty soukromí či finanční ztráty). Domníváme se, že toto může ukazovat na určitou kontraproduktivitu frontálního typu výuky, kdy respondentovy působní představy o počítačových virech byly výukou narušeny, avšak nedošlo k vybudování nového pojetí tohoto pojmu z hlediska následků. Z tohoto důvodu **nepovažujeme** zjištěnou změnu ve vnímání dotčených pojmů **za splnění cíle** použitého typu výuky.

Oddálení pojmu **Ulož.to** od pojmů **Zálohování a E-mail** vysvětlujeme tak, že respondenti začali vnímat tyto dvě skupiny pojmů jako navzájem méně podobné. To lze interpretovat tak, že **respondenti si začali více uvědomovat rozdíl mezi soukromými a veřejnými službami Internetu** – tedy že zatímco služba Ulož.to je do značné míry veřejným prostorem, který slouží ke sdílení dat mezi uživateli a je nevhodný k ukládání osobních dat a jejich zálohování, e-mailová schránka je prostorem soukromým, do kterého by jiní uživatelé neměli mít přístup a do kterého je možno osobní data ukládat a případně je zde ponechávat jako jistý typ zálohy. Domníváme se, že toto může souviset s absolvovaným typem výuky, neboť během výuky byli studenti informováni o různých typech cloudových služeb a jejich vhodnosti k zálohování dat. Zjištěnou změnu vnímání dotčených pojmů **lze považovat za splnění cíle** použitého typu výuky, neboť dává naději, že respondenti po výuce vnímají rozdíly mezi různými cloudovými službami více než před výukou (a budou tedy pečlivěji než před výukou zvažovat, jaká data konkrétní službě svěřit a jak se při práci s danou službou chovat).

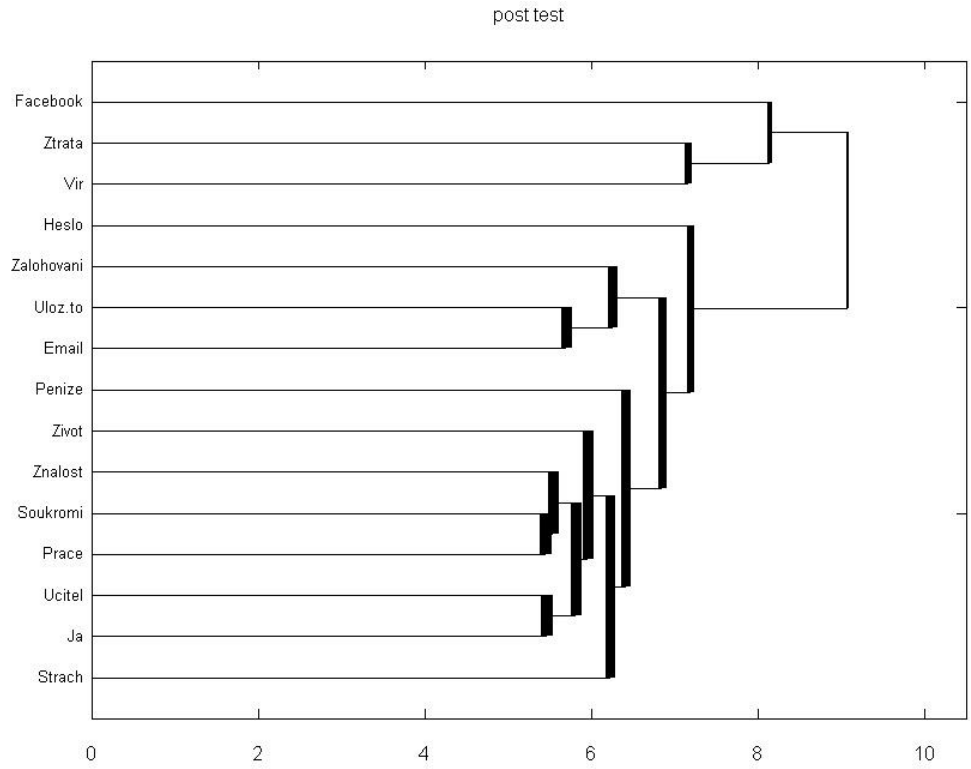
Přiblížení pojmu **Ulož.to** k pojmu **Facebook** vysvětlujeme tak, že respondenti začali vnímat tyto pojmy jako podobnější. To lze interpretovat tak, že **respondenti si začali více uvědomovat souvislost obou služeb** spočívající v publikování dat jedním uživatelem

a jejich příležitostné konzumaci uživatelem jiným. Domníváme se, že toto může souviset s výše uvedeným oddálením pojmu Ulož.to od pojmu E-mail, v důsledku čehož se pojem Ulož.to přiblížil k jinému pojmu reprezentující online službu. Z tohoto důvodu **nepovažujeme** zjištěnou změnu ve vnímání dotčených pojmů **za splnění cíle** použitého typu výuky.

5.3.1.3 Přednáška odborníka



Obrázek 28: Dendrogram pretestu pro **Přednášku odborníka**



Obrázek 29: Dendrogram posttestu pro **Přednášku odborníka**

Na základě analýzy dendrogramů z Obrázku 28 a Obrázku 29 byly u respondentů, kteří absolvovali **Přednášku odborníka**, jako významné zjištěny přesuny pojmů uvedené v Tabulce 8.

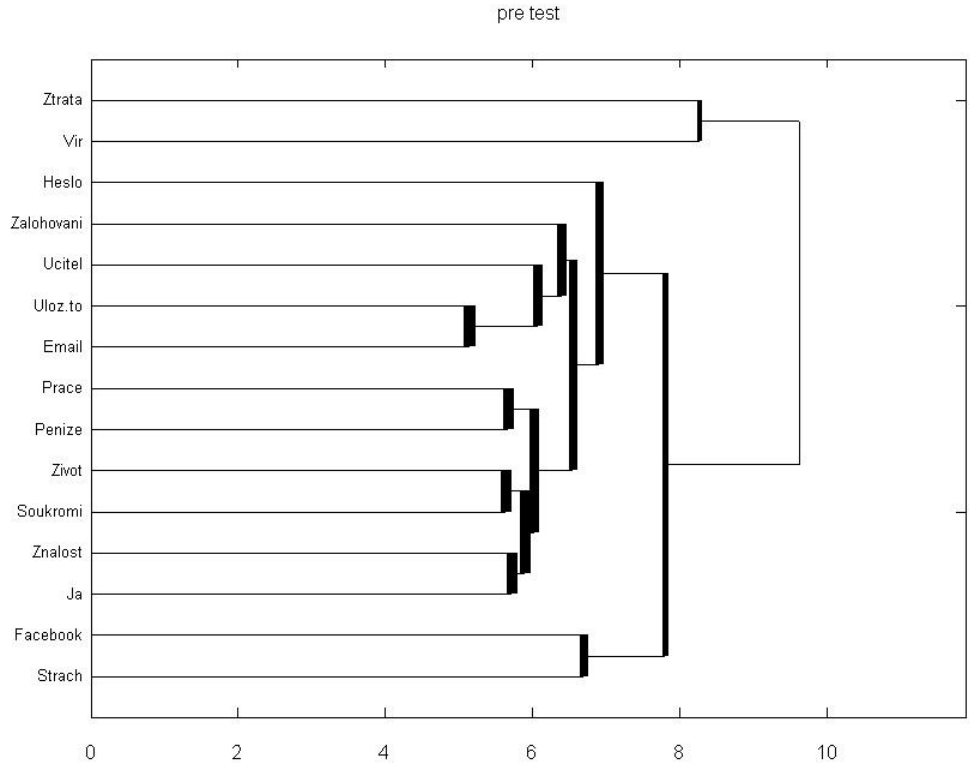
Tabulka 8: Přesuny pojmů mezi shluky pro **Přednášku odborníka**

Pojmy A	Pojmy B	Směr	Při počtu shluků
Vir	Ztráta	K sobě	4
Facebook	Ztráta, Vir	K sobě	2

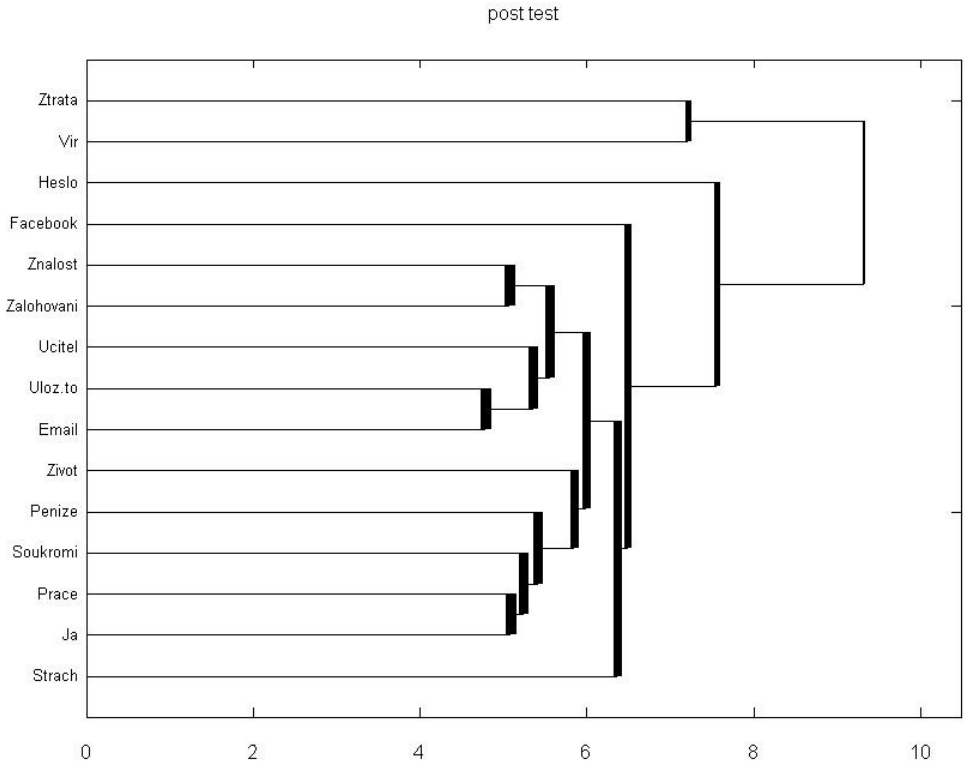
Přiblížení pojmu **Vir** k pojmu **Ztráta** vysvětlujeme tak, že respondenti začali vnímat tyto pojmy jako navzájem si podobnější. To lze interpretovat tak, že **respondenti si začali více uvědomovat, že působení viru s sebou nese riziko určité ztráty** (například ztráty dat, ztráty soukromí či finanční ztráty). Domníváme se, že toto souvisí s absolvovaným typem výuky, neboť při výkladu o malware se učitel zaměřoval právě na riziko ztráty dat způsobené malwarem. Zjištěnou změnu vnímání dotčených pojmů **lze považovat za splnění cíle** použitého typu výuky, neboť dává naději, že respondenti po výuce považují vir za negativní jev vedoucí k určité ztrátě více než před výukou (a budou se tedy před viry chránit důsledněji než před výukou).

Přiblížení pojmu **Facebook k** pojmům **Ztráta a Vir** vysvětlujeme tak, že respondenti začali vnímat tyto pojmy jako navzájem si podobnější. To lze interpretovat tak, že **respondenti si začali více uvědomovat, že používání služby Facebook s sebou nese riziko určité ztráty** (například ztráty soukromí, ztráty kontroly nad svými daty). Tento stav by pak bylo možno **přirovnat k působení počítačového viru**, který s sebou nese riziko obdobné ztráty. Domníváme se, že toto může souviset s absolvovaným typem výuky, neboť během výkladu o sociálních sítích byli studenti informováni o rizicích ohrožujících soukromí jedince, kam patří právě riziko ztráty soukromí či ztráty kontroly nad svými daty. Zjištěnou změnu vnímání dotčených pojmů **lze považovat za splnění cíle** použitého typu výuky, neboť dává naději, že si respondenti po výuce uvědomí riziko ztráty soukromí či ztráty kontroly nad svými daty při používání Facebooku více než před výukou (a budou se tedy při používání Facebooku chovat opatrněji než před výukou).

5.3.1.4 Skupinová výuka



Obrázek 30: Dendrogram pretestu pro **Skupinovou výuku**



Obrázek 31: Dendrogram posttestu pro **Skupinovou výuku**

Na základě analýzy dendrogramů z Obrázku 30 a Obrázku 31 byly u respondentů, kteří absolvovali **Skupinovou výuku**, jako významné zjištěny přesuny pojmů uvedené v Tabulce 9.

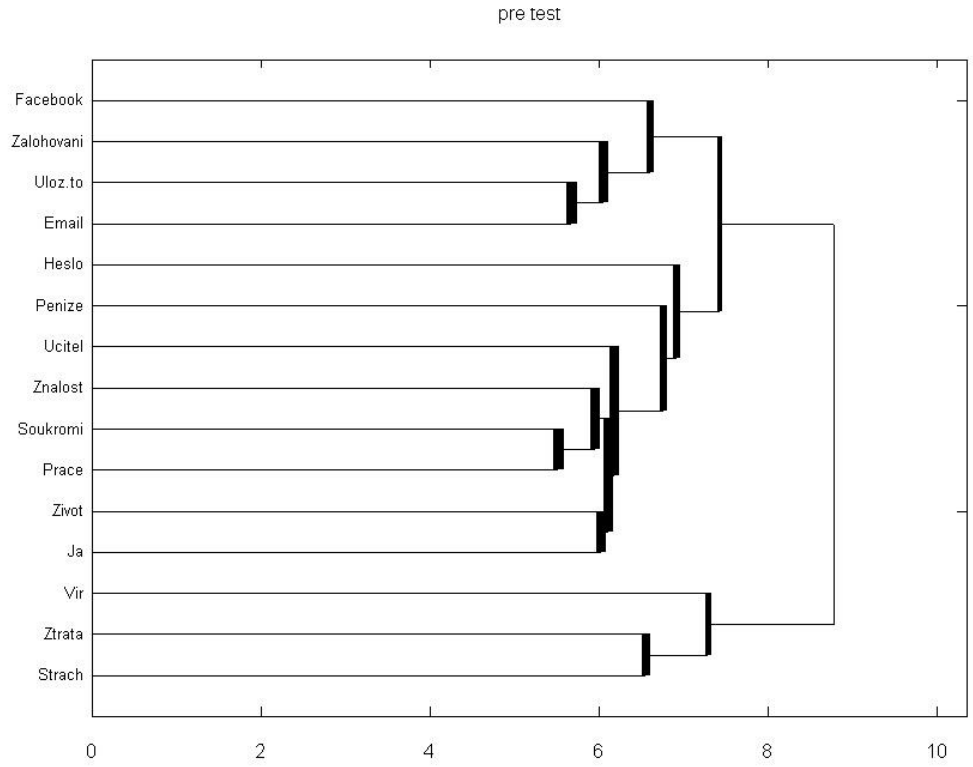
Tabulka 9: Přesuny pojmů mezi shluky pro **Skupinovou výuku**

Pojmy A	**Pojmy B**	**Směr**	**Při počtu shluků**
Zálohování	Znalost	K sobě	9
Znalost	Já, Soukromí, Práce, Život, Peníze	Od sebe	9

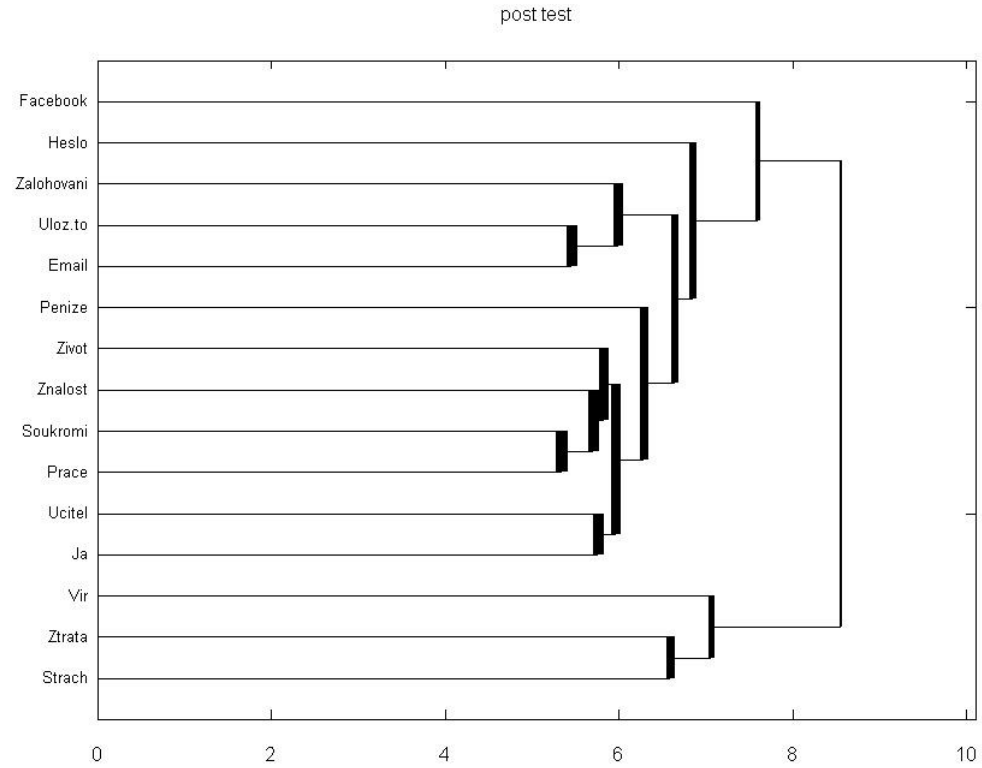
Přiblížení pojmu **Zálohování k** pojmu **Znalost** vysvětlujeme tak, že respondenti začali vnímat tyto pojmy jako navzájem si podobnější. To lze interpretovat tak, že **respondenti si začali více uvědomovat zálohování jako vědomou a cílenou činnost**, k jejímuž vykonávání jsou potřeba určité znalosti (například na jaká média a jakým způsobem provádět zálohy). Domníváme se, že toto může souviset s absolvovaným typem výuky, neboť jedno z témat pro skupinovou práci se týkalo zálohování dat (včetně výhod zálohování, možných způsobů zálohování a četnosti zálohování). Uvedený posun ve vnímání pojmů Zálohování a Znalost je dále umocněn oddálením pojmu Znalost od shluku pojmů Já, Soukromí, Práce, Život, Peníze. Zjištěnou změnu vnímání dotčených pojmů **lze**

považovat za splnění cíle použitého typu výuky, neboť dává naději, že si respondenti po výuce uvědomí zálohování jako vědomou a cílenou činnost více než před výukou (a budou tedy zálohování svých dat plánovat pečlivěji než před výukou).

5.3.1.5 Kontrolní skupina



Obrázek 32: Dendrogram pretestu pro kontrolní skupinu



Obrázek 33: Dendrogram posttestu pro kontrolní skupinu

5.3.2 Diskuze výsledků

5.3.2.1 Diskuze jednotlivých typů výuky

Zážitková výuka se zdá být z celkového hlediska (tj. v případě zaměření se na všechny studenty absolvující tento typ výuky) poměrně efektivní, avšak její efektivita zřejmě pramení spíše z části výuky založené na výkladu učitele než z té části, ve které byla studentům zprostředkována určitá negativní zkušenost. Během zkoumání jsme totiž nezaznamenali změny ve vnímání těch oblastí, ve kterých byli studenti vystaveni námi připraveným e-bezpečnostním hrozbám. Připravené e-bezpečnostní hrozby je z tohoto důvodu potřeba zejména z pohledu studentů, kteří na ně nereagovali a nestali se jejich oběťmi, chápat jen jako aktivizační prvky výuky.

K podobným závěrům jsme došli i při zkoumání změn ve vnímání problematiky u těch studentů, kteří se v rámci **Zážitkové výuky** podlehli hrozbě nebezpečného uvádění osobních údajů. Možným důvodem může být, že studenti se z tohoto negativního zážitku nepoučili. Studenti mohli odmítnout podíl viny za podlehnutí hrozbě, že důvěřovali službám poskytovaným školou a že oni nemohli situaci ovlivnit. Z těchto důvodů nelze tuto hrozbu považovat z hlediska efektivity výuky za příliš přínosnou a vzhledem ke komplikovanosti jejího nasazení bychom její používání jako aktivizačního prvku výuky spíše nedoporučovali.

U studentů, kteří v rámci **Zážitkové výuky** podlehli hrozbě rizikové registrace, došlo k posunu ve vnímání těch oblastí technické e-bezpečnosti, které s uvedenou e-bezpečnostní hrozbou souvisejí. Proto lze tuto hrozbu považovat z hlediska vlivu na e-bezpečnostní kompetence studentů, kteří jí podlehli, za přínosnou a hrozbu samotnou za svébytnou část výuky přesahující roli aktivizačního prvku.

Realizovaná **Frontální výuka** se zdá být v určitých ohledech efektivní, na straně druhé je zde riziko určité kontraproduktivity. Studentům totiž mohou být během výuky narušeny jejich původní představy o problematice (které mohou, ale nemusejí být zcela nesprávné), avšak nedojde (například z důvodu zahlcení fakty) v dostatečné míře k jejich nahrazení novým komplexním pojetím dané oblasti. Efektivita **Frontální výuky** mohla být zkreslena tím, že studenti i učitel jsou zvyklí tuto metodu rutinně používat, tudíž studenti sice nejsou zaujati novostí způsobu výuky, ale oni i učitel v jejím rámci dokáží pracovat velmi efektivně.

Výuka založená na **Přednášce odborníka** se zdá být poměrně efektivní, neboť u studentů, kteří ji absolvovali, došlo k posunům ve vnímání těch oblastí problematiky technické e-bezpečnosti, na něž byla výuka zaměřena. Efektivita výuky však mohla být zkreslena novostí použitého způsobu výuky, předpokládanou prestiží přednášejícího a očekáváním studentů, že jim probíranou tématiku odborník vysvětlí lépe než obvyklý učitel. Zároveň zde mohla určitou roli sehrát osoba vyučujícího, která byla odlišná od osoby učitele při ostatních typech výuky. K posunu však nedošlo ve všech sledovaných oblastech problematiky technické e-bezpečnosti, na něž byla výuka zaměřena.

Skupinová výuka podle vytvořeného scénáře se zdá být v určitých ohledech efektivní, avšak její dopad je slabší než u ostatních typů výuky. Efektivitu této metody však mohlo negativně ovlivnit to, že studenti pomocí této metody nejsou zvyklí pracovat, kvůli čemuž si nejsou schopni navzájem předat své poznatky.

5.3.2.2 Shrnutí diskuze

Z hlediska přínosu pro e-bezpečnostní kompetence studentů považujeme za úspěšnou výuku založenou na **Přednášce odborníka.** Tento přínos se zdá být výraznější než přínos běžné výuky pomocí frontální metody, avšak určitou roli mohla sehrát osoba vyučujícího, která byla u **Přednášky odborníka** a **Frontální výuky** odlišná.

Zážitkovou výuku považujeme za přínosnou u těch studentů, kteří podlehli hrozbě rizikové registrace. Naopak přínos **Zážitkové výuky** u studentů, kteří podlehli hrozbě nebezpečného uvádění osobních údajů, není zřejmý. Z toho lze usuzovat, že negativní

zkušenost může mít pozitivní vliv na postoje učících se osob, které připravené e-bezpečnostní hrozbě podlehli. Tento vliv se však nemusí objevit vždy, pravděpodobně záleží například na přijetí podílu viny za své oklamání učící se osobou.

6 PŘÍNOS VÝZKUMU

Přínos výzkumu odborných kompetencí učitelů ICT v oblasti technické e-bezpečnosti a vlivů na ně působících spočívá ve zmapování těchto kompetencí. Zjištění vlivů, působících na tyto kompetence, umožňuje lépe pochopit, proč se učitelé chovají konkrétním způsobem. Tato zjištění dávají možnost cíleně posilovat vlivy, které zajišťují zlepšování kompetencí učitelů ICT (například budovat sociální vazby mezi učiteli ICT a ICT odborníky) a upozorňují na ty vlivy, které bezpečnějšímu chování brání. Na základě identifikace těchto vlivů je možné působení některých z nich vhodně eliminovat pomocí edukace. Přínosem tohoto výzkumu je tedy možnost lépe stanovit obsah výuky současných a budoucích učitelů ICT v oblasti technické e-bezpečnosti.

Přínos výzkumu zaměřeného na proces utváření kompetencí učitelů ICT v oblasti technické e-bezpečnosti spočívá v identifikaci tohoto procesu. Na jeho základě je možné lépe cílit kurzy dalšího vzdělávání učitelů v této oblasti, kdy se ukazuje jako potřebné přesvědčit učitele o potřebnosti dodržovat patřičné e-bezpečnostní pravidla namísto zvyšování jejich znalostí. Toho lze dle výsledků výzkumu dosáhnout zprostředkováním určité negativní zkušenosti.

Část práce zaměřená na tvorbu optimalizačního nástroje ukazuje způsob, jak do výuky problematiky technické e-bezpečnosti přinést prvky autentického zážitku učícího se jedince. Zároveň je zde diskutován přínos tohoto způsobu výuky ve smyslu změn postojů učících se osob k problematice technické e-bezpečnosti ve srovnání s jinými typy výuky.

7 ZÁVĚR

E-bezpečnost je v současné době často diskutované téma, pro utváření potřebných kompetencí u dětí a mládeže je důležitá role školy. Doposud však nebyly více zkoumány příslušné odborné kompetence učitelů, a to ani učitelů ICT. Učitele v oblasti technické e-bezpečnosti nelze vnímat pouze jako didaktiky, ale také jako osobnosti, které svým příkladem a postoji mohou žáky značně ovlivnit.

V rámci výzkumu technické e-bezpečnosti jsme oslovili učitele ICT základních a středních škol. Realizovali jsme s nimi polostrukturované hloubkové rozhovory, doplněné didaktickým testem a hledáním informací o učitelově „virtuálním životě" na sociálních sítích. Zmapovali jsme současné kompetence učitelů ICT v oblasti technické e-bezpečnosti, vlivy na ně působící a vytvořili jsme teorii chování učitelů ICT a model takového chování.

Z utvořeného modelu vyplývá, že, že samotná znalost e-bezpečnostních pravidel pro bezpečné chování učitelů v oblasti technické e-bezpečnosti nestačí. Na chování učitelů totiž působí překážky, které brání učiteli chovat se bezpečně. Aby učitel tyto překážky překonal a choval se bezpečně, je nutné, aby uznal způsob chování popisovaný v pravidlech jako potřebný. K tomu může pomoci negativní zkušenost, kterou učitel prožije. Schéma tohoto chování odpovídá teorii operantního podmiňování podle Skinnera, neboť chování jedince se mění na základě důsledků jeho předchozího chování.

Důležitou otázkou spojenou s realizovaným výzkumem je přenositelnost představeného modelu na jiné skupiny osob a případně jeho zobecnitelnost. Jelikož byl výzkum realizován na učitelích ICT, nelze a priori předpokládat aplikovatelnost vytvořeného modelu na jiné skupiny osob. Učitel ICT nese jinou zodpovědnost než běžný učitel (pověst učitele jako ICT odborníka, zodpovědnost za správcovství svěřených digitálních technologií) či než běžný dospělý člověk (učitel jako vzor pro mladou generaci). V dalších výzkumech by bylo potřeba kvantitativně ověřit, zda je představený model aplikovatelný na všechny učitele základních a středních škol nebo dokonce na celou dospělou populaci.

Na základě výsledků z předchozí části výzkumu jsme realizovali pedagogický experiment, pomocí něhož jsme zjišťovali přínos různých výukových přístupů ke zvyšování kompetencí učitelů ICT v oblasti technické e-bezpečnosti. V jeho rámci jsme použili pedagogický přístup založený na simulaci e-bezpečnostní hrozby, na základě které učící se osoby přímo zažily určitou negativní zkušenost. Druhým realizovaným pedagogickým

přístupem vyplývajícím z výzkumu bylo zprostředkování negativní zkušenosti pomocí přednášky externího odborníka, který jednotlivá rizika dokumentoval na konkrétních případech příběhů lidí, s nimiž se učící se jedinec mohl ztotožnit.

Z výsledků experimentu vyplývá, že negativní zkušenost může mít pozitivní vliv na postoje těch učících se osob, které připravené e-bezpečnostní hrozbě podlehli. Výuka založená na přednášce externího odborníka měla příznivý vliv na postoje učících se osob v technické e-bezpečnosti a tento vliv se zdá být výraznější než vliv běžné výuky pomocí frontální metody. Zjištěné výsledky tak odpovídají příslušné části námi vytvořené teorie chování učitelů ICT.

Realizovaný výzkum nabízí teoretické východisko pro tvorbu kurikula výuky technické e-bezpečnosti, která by byla založena na zprostředkování negativní zkušenosti učícím se osobám, a pro vytváření nástrojů podporující tuto výuku. Přitom by však bylo nutno kromě technických hledisek realizace nutno zvažovat i etická a psychologická hlediska, což činí tento typ intervence poměrně náročným.

PUBLIKAČNÍ AKTIVITY

Vlastní publikační aktivity doktoranda rozděleny na tematické části.

Kapitola v odborné monografii:

- PECH, P., L. ČINČUROVÁ, M. GÜNZEL, R. HÁJKOVÁ, R. HAŠEK, A. HRANÍČEK, M. KAZDA, J. KOPECKÝ, M. KOTLASOVÁ, V. PETRÁŠKOVÁ, L. SAMKOVÁ, T. SUCHOPÁROVÁ, V. ŠIMANDL a J. VANÍČEK, 2015. *Badatelsky orientovaná výuka matematiky a informatiky s podporou technologií*. České Budějovice: Jihočeská univerzita v Českých Budějovicích, Pedagogická fakulta. 194 s. ISBN 978-80-7394-531-2.
- KOPECKÝ, K., M. HŘIVNOVÁ, A. MALÚŠKOVÁ, V. ŠIMANDL, V. DOBIÁŠ, J. ŠMAHAJ, P. CAKIRPALOGLU, S. DOBEŠOVÁ CAKIRPALOGLU, V. OČENÁŠKOVÁ, P. TOMÁNEK, L. TOMCZYK, A. WASINSKI a Z. VÁCLAVÍKOVÁ, 2013. *Rizika internetové komunikace v teorii a praxi*. Olomouc: Univerzita Palackého v Olomouci, Pedagogická fakulta. 188 s. ISBN 978-80-244-3571-8.
- GÜNZEL, M., R. HAŠEK, J. JAREŠ, J. LOMBART, P. PECH, V. ŠIMANDL, R. ŠTĚPÁNKOVÁ a J. VANÍČEK, 2012. *Integrace elektronických prostředí pro počítačem podporovanou výuku matematiky*. České Budějovice: Jihočeská univerzita v Českých Budějovicích, Pedagogická fakulta. 187 s. ISBN 978-80-7394-386-8.

Časopisy:

- ŠIMANDL, V., 2015. ICT Teachers, Social Network Sites and Online Privacy. *International Journal of Information and Communication Technologies in Education*. roč. 4, č. 4, s. 69–81. ISSN 1805-3726. Dostupné z https://periodicals.osu.eu/ictejournal/dokumenty/2015-04/ictejournal-2015-4.pdf
- ŠIMANDL, V., 2015. The use of GeoGebra software for typesetting mathematical text. *The Electronic Journal of Mathematics and Technology*. roč. 9, č. 3, s. 239–247. ISSN 1933-2823. Dostupné z: https://php.radford.edu/~ejmt/deliveryBoy.php?paper=eJMT_v9n3a4
- ŠIMANDL, V., 2015. ICT Teachers and Technical E-safety: Knowledge and Routines. *International Journal of Information and Communication Technologies in Education*.

roč. 4, č. 2, s. 50–65. ISSN 1805-3726. Dostupné z https://periodicals.osu.eu/ictejournal/dokumenty/2015-02/ictejournal-2015-2.pdf

- ŠIMANDL, V. a J. VANÍČEK, 2015. The Use of Inquiry Based Education in a Simulation Software Environment in Pre-Service ICT Teacher Training. *International Journal of Information and Communication Technologies in Education*. roč. 4, č. 1, s. 5–15. ISSN 1805-3726. Dostupné z https://periodicals.osu.eu/ictejournal/dokumenty/2015-01/ictejournal-2015-1.pdf
- ŠIMANDL, V., 2014. Odhalování podvádění v online soutěžích. *Journal of Technology and Information Education*. roč. 6, č. 2, s. 114–121. ISSN 1803-537X. Dostupné z http://jtie.upol.cz/pdfs/jti/2014/02/14.pdf

Příspěvky ve sbornících:

- ŠIMANDL, V., 2015. ICT Teachers and Social Network Sites. In: *Information and Communication Technology in Education. Proceedings* [CD-ROM]. Ostrava: Ostravská univerzita, Pedagogická fakulta, s. 196–203. ISBN 978-80-7464-763-5.
- ŠIMANDL, V., J. ZELENKA a J. SADIL, 2013. Výuka digitální bezpečnosti v českých školách. In: *DidInfo 2013*. Banská Bystrica: Univerzita Mateja Bela, Fakulta prírodných vied v Banskej Bystrici, s. 229–236. ISBN 978-80-557-0527-9.
- ŠIMANDL, V., 2013. Kompetence učitelů ICT v oblasti technické e-bezpečnosti. In: *Information and Communication Technology in Education – Ph.D. students section* [CD-ROM]. Ostrava: Ostravská univerzita, Pedagogická fakulta, s. 114–131. ISBN 978-80-7464-325-5.
- ŠIMANDL, V., 2012. Kompetence žáků v oblasti informační bezpečnosti. In: *Mezinárodní konference ICT ve vzdělávání – Sborník příspěvků*. Olomouc: Univerzita Palackého v Olomouci, s. 186–200. ISBN 978-80-244-3362-2.
- ŠIMANDL, V. a J. LHOTÁK, 2012. Kompetence žáků v oblasti digitální bezpečnosti v České republice. In: *DidInfo 2012* [CD-ROM]. Banská Bystrica: Univerzita Mateja Bela, Fakulta prírodných vied v Banskej Bystrici, s. 243–250. ISBN 978-80-557-0342-8.
- LEIPERT, J. a V. ŠIMANDL, 2012. Cloud learning – Learning through social networks and online services. In: *Information and Communication Technology in*

Education. Proceedings. Ostrava: Ostravská univerzita, Pedagogická fakulta, s. 147–150. ISBN 978-80-7464-135-0.

- ŠIMANDL, V., 2011. Online research activities for the teaching with the help of spreadsheets. In: *Information and Communication Technology in Education. Proceedings*. Ostrava: Ostravská univerzita, Pedagogická fakulta, s. 333–338. ISBN 978-80-7368-979-7.

Přednášky na konferencích:

- ŠIMANDL, V., 2014. ICT teachers and technical e-safety: knowledge and routines. *Conference Cyberspace 2014*. Brno: Masarykova univerzita v Brně, 28.–29. 11. 2014.
- ŠIMANDL, V., 2014. Using GeoGebra software to typeset mathematical text. *Conference CADGME 2014*. Halle: Martin-Luther-University of Halle-Wittenberg, 26.–29. 9. 2014.
- ŠIMANDL, V., 2014. Odhalování podvádění v soutěži Bobřík informatiky. *Konference DidactIG 2014*. Liberec: Technická univerzita v Liberci, 3.–5. 2. 2014.

Postery na konferencích:

- ŠIMANDL, V., V. DOBIÁŠ, V. a M. ŠERÝ, 2015. The influence of teaching methods during technical e-safety instruction. *ISSEP 2015*. Ljubljana: University of Ljubljana, Faculty of Computer and Information Science, 28. 9.–1. 10. 2015.

Mimo výše popsaných konferenčních příspěvků jsem uveden jako vedoucí těchto ***diplomových a bakalářských závěrečných prací***:

- CANDRA, M., 2015. *Online aplikace pro odhalování podvádění v soutěži Bobřík informatiky*. České Budějovice. Bakalářská práce. Jihočeská univerzita v Českých Budějovicích, Pedagogická fakulta, Katedra informatiky.
- KOVÁŘ, D., 2014. *Digitální bezpečnost ve školních vzdělávacích programech základních a středních škol*. České Budějovice. Bakalářská práce. Jihočeská univerzita v Českých Budějovicích, Pedagogická fakulta, Katedra informatiky.
- SADIL, J., 2013. *Kompetence studentů učitelství v oblasti digitální bezpečnosti*. České Budějovice. Bakalářská práce. Jihočeská univerzita v Českých Budějovicích, Pedagogická fakulta, Katedra informatiky.

- ZELENKA, J., 2013. *Výuka digitální bezpečnosti na ZŠ a SŠ*. České Budějovice. Bakalářská práce. Jihočeská univerzita v Českých Budějovicích, Pedagogická fakulta, Katedra informatiky.

LITERATURA

BALADA, J. et al., 2007. *Rámcový vzdělávací program pro gymnázia*. Praha: Výzkumný ústav pedagogický. ISBN 978-80-8700-11-3.

BARROW, Ch. a G. HEYWOOD-EVERETT, 2006. *E-safety: the experience in English educational establishments* [online]. Coventry: Becta [cit. 2012-07-15]. Dostupné z: http://dera.ioe.ac.uk/1619/1/becta_2005_esafetyaudit_report.pdf

BECTA, 2005. *E-safety: Developing whole-school policies to support effective practice* [online]. Coventry: Becta [cit. 2013-02-02]. Dostupné z: http://www.wisekids.org.uk/BECTA%20Publications/esafety.pdf

BECTA, 2006. *Safeguarding children in a digital world: Developing a strategic approach to e-safety* [online]. Coventry: Becta [cit. 2012-09-14]. Dostupné z: http://webarchive.nationalarchives.gov.uk/20101102103654/ http://publications.becta.org.uk/download.cfm?resID=25933

BECTA, 2007. *Signposts to safety: Teaching e-safety at Key Stages 3 and 4* [online]. Coventry: Becta [cit. 2011-11-30]. Dostupné z: https://www.education.gov.uk/publications/eOrderingDownload/signposts_safety_ks3and4.pdf

BERÁNEK, L., 2009. Information systems security education for future teacher at secondary and primary schools. *Journal of Technology and Information Education* [online]. roč. 1, č. 2, s. 89–93 [cit. 2012-08-15]. ISSN 1803-537X. Dostupné z: http://jtie.upol.cz/pdfs/jti/2009/02/16.pdf

BUETTNER, Y. et al., 2002. *Information and Communication Technology in Education: A Curriculum for Schools and Programme of Teacher Development* [online]. Paris: UNESCO [cit. 2012-04-15]. Dostupné z: http://unesdoc.unesco.org/images/0012/001295/129538e.pdf

BYRON, T., 2008. *Safer Children in a Digital World: The Report of the Byron Review* [online]. Department for Children, Schools and Families [cit. 2012-03-22]. ISBN 978-1-84775-134-8. Dostupné z: http://webarchive.nationalarchives.gov.uk/20130401151715/http://www.education.gov.uk/publications/eOrderingDownload/DCSF-00334-2008.pdf

CERMAT, 2010. *Katalog požadavků zkoušek společné části maturitní zkoušky: Informatika, základní úroveň obtížnosti* [online]. [cit. 2012-04-07]. Dostupné z: http://digifolio.rvp.cz/artefact/file/download.php?file=15057&view=3049

CRANMER, S., J. POTTER a N. SELWYN, 2008. *Learners and technology: 7–11* [online]. Coventry: Becta [cit. 2012-04-16]. Dostupné z: http://dera.ioe.ac.uk/1630/7/becta_2008_learners7to11_report_Redacted.pdf

CRANMER, S., N. SELWYN a J. POTTER, 2009. Exploring primary pupils‘ experiences and understandings of ‚e-safety‘. *Education and Information Technologies* [online]. roč. 14, č. 2, s. 127–142 [cit. 2012-04-16]. ISSN 1360-2357. DOI 10.1007/s10639-008-9083-7. Dostupné z: http://www.springerlink.com/index/10.1007/s10639-008-9083-7

CROSS-TAB, 2010. *Online Reputation in a Connected World* [online]. [cit. 2013-02-02]. Dostupné z: http://www.job-hunt.org/guides/DPD_Online-Reputation-Research_overview.pdf

DOOLEY, J. J. et al., 2009. *Review of existing Australian and international cyber-safety research* [online]. Perth: Edith Cowan University, Child Health Promotion Research Centre [cit. 2012-09-12]. Dostupné z: http://unpan1.un.org/intradoc/groups/public/documents/apcity/unpan046312.pdf

DŽUBÁK, J., 2005. Zkontrolujte si svůj šampon. *Hoax.cz* [online]. [cit. 2013-02-28]. Dostupné z: http://www.hoax.cz/hoax/zkontrolujte-si-svuj-sampon/

ECDL FOUNDATION Ltd., 2007a. *European Computer Driving Licence / International Computer Driving Licence – Concepts ICT Sylabus 5.0 (M1)* [online]. [cit. 2012-10-04]. Dostupné z: http://www.ecdl.cz/data/Sylabus-ECDL-CZ-M1-5.0.pdf

ECDL FOUNDATION Ltd., 2007b. *European Computer Driving Licence / International Computer Driving Licence – Concepts ICT Sylabus 5.0 (M7)* [online]. [cit. 2012-10-04]. Dostupné z: http://www.ecdl.cz/data/Sylabus-ECDL-CZ-M7-5.0.pdf

EVROPSKÁ KOMISE, 2012. *Digitální agenda: Nová strategie pro zajištění větší bezpečnosti a lepšího obsahu pro děti a mládež na internetu* [online]. [cit. 2016-03-15]. Dostupné z: http://europa.eu/rapid/press-release_IP-12-445_cs.pdf

EYNON, R., 2009. *Harnessing Technology: The Learner and their Context: Mapping young people’s uses of technology in their own contexts – a nationally representative survey* [online]. Coventry: Becta [cit. 2012-10-12]. Dostupné z: http://archive.teachfind.com/becta/research.becta.org.uk/upload-dir/downloads/page_documents/research/reports/ht_learner_context_survey.doc

FEDERAL COMMUNICATION COMISSION, 2012. *Protecting Children in the 21st Century Act Amendment* [online]. Washington, D.C. [cit. 2015-04-10]. Dostupné z: http://www.fcc.gov/document/protecting-children-21st-century-act-amendment

FERJENČÍK, J., 2000. *Úvod do metodologie psychologického výzkumu: Jak zkoumat lidskou duši*. Praha: Portál. 255 s. ISBN 80-7178-367-6.

GARRISON, C. P. a O. G. POSEY, 2006. Computer Security Awareness of Accounting Students. In: *2006 Southwest Decision Sciences Institute Proceedings* [online]. [cit. 2012-02-02]. Dostupné z: http://www.swdsi.org/swdsi06/Proceedings06/Papers/A04.pdf

GET SAFE ONLINE, 2009. *UK Internet Security: State of the Nation: The Get Safe Online Report* [online]. [cit. 2012-06-04]. Dostupné z: https://www.getsafeonline.org/media/Reports/Get_Safe_Online_Report_2009.pdf

GET SAFE ONLINE, 2010. *UK Internet Security: State of the Nation: The Get Safe Online Report* [online]. [cit. 2012-06-04]. Dostupné z: https://www.getsafeonline.org/media/Reports/Get_Safe_Online_Report_2010.pdf

HAMPTON, K. N. et al., 2012. *Why most Facebook users get more than they give: The effect of Facebook 'power users' on everybody else* [online]. Washington D.C.: Pew Research Center [cit. 2013-02-03]. Dostupné z: http://pewinternet.org/Reports/2012/Facebook-users.aspx

HANUŠ, R. a L. CHYTILOVÁ, 2009. *Zážitkově pedagogické učení*. Vyd. 1. Praha: Grada. 192 s. ISBN 978-80-247-2816-2.

HENDL, J., 2005. *Kvalitativní výzkum: základní metody a aplikace*. Vyd. 1. Praha: Portál. 407 s. ISBN 80-736-7040-2.

HUCLOVÁ, M. a V. VRBÍK, 2011. Bezpečně s internetem na základní škole. *Arnica Acta Rerum Naturalium didactICA*. roč. 1, č. 2, s. 33–37. ISSN 1804-8366.

CHOU, Ch. a H. PENG, 2011. Promoting awareness of Internet safety in Taiwan in-service teacher education: A ten-year experience. *The Internet and Higher Education* [online]. roč. 14, č. 1, s. 44–53 [cit. 2013-01-14]. ISSN 1096-7516. DOI 10.1016/j.iheduc.2010.03.006. Dostupné z: http://www.sciencedirect.com/science/article/pii/S109675161000031X

CHRÁSKA, M., 1995. Změny v sémantickém prostoru studentů pedagogické fakulty. *Pedagogika* [online]. roč. 45, č. 1, s. 71–76 [cit. 2016-02-01]. Dostupné z: http://pages.pedf.cuni.cz/pedagogika/?attachment_id=3118&edmc=3118

CHRÁSKA, M., 2007. *Metody pedagogického výzkumu: Základy kvantitativního výzkumu*. Vyd. 1. Praha: Grada. 265 s. ISBN 978-80-247-1369-4.

INTERNATIONAL SOCIETY FOR TECHNOLOGY IN EDUCATION, 2008. *NETS-T Standards* [online]. [cit. 2012-10-04]. Dostupné z: http://www.iste.org/standards/ISTE-standards/standards-for-teachers

JANOUŠEK, J., 1992. Sociálně kognitivní teorie Alberta Bandury. *Československá psychologie* [online]. roč. 36, č. 5, s. 385–398 [cit. 2016-01-20]. ISSN 0009-062X. Dostupné z: http://web.ff.cuni.cz/~hosksaff/Janousek.pdf

KAPOUN, P., J. KAPOUNOVÁ a T. JAVORČÍK, 2011. Safety Electronic Communication. In: *Information and Communication Technology in Education. Proceedings*. Ostrava: Ostravská univerzita, Pedagogická fakulta, s. 143–151. ISBN 978-80-7368-979-7.

KASPERSKY LAB, 2015. *Consumer Security Risks Survey 2015* [online]. Kaspersky Lab [cit. 2016-04-03]. Dostupné z: https://press.kaspersky.com/files/2015/08/Kaspersky_Lab_Consumer_Security_Risks_Survey_2015_ENG.pdf

KERLINGER, F. N., 1972. *Základy výzkumu chování: Pedagogický a psychologický výzkum*. 1. vyd. Praha: Academia. 708 s.

KOLÁŘ, Z. et al., 2012. *Výkladový slovník z pedagogiky*. Vyd. 1. Praha: Grada. ISBN 978-80-247-3710-2.

LANG, M. et al., 2009. Social Networking and Personal Data Security: A Study of Attitudes and Public Awareness in Ireland. In: *Proceedings of International Conference on Management of e-Commerce and e-Government (ICMeCG), Nanchang, China, September 16-19*. IEEE Computer Society, s. 486–489.

LAURI, M. A., J. BORG a L. FARRUGIA, 2015. *Children's Internet Use and Parents' Perceptions of Their Children's Online Experience* [online]. Msida: University of Malta [cit. 2016-04-03]. Dostupné z: http://www.mca.org.mt/sites/default/files/attachments/notices/2015/childrens%20internet%20use%20and%20parents%20perceptions%20of%20their%20childrens%20online%20experience.pdf

LHOTÁK, J., 2010. *Jak škola chrání před počítačovým pirátstvím* [online]. České Budějovice [cit. 2012-02-01]. Bakalářská práce. Jihočeská univerzita v Českých Budějovicích, Pedagogická fakulta, Katedra informatiky. Dostupné z: http://theses.cz/id/2xs9d6/downloadPraceContent_adipIdno_15583

LIM, J. a J. C. RICHARDSON, 2016. Exploring the effects of students' social networking experience on social presence and perceptions of using SNSs for educational purposes. *The Internet and Higher Education* [online]. č. 29, s. 31–39 [cit. 2016-03-15]. ISSN 1096-7516. Dostupné z: http://www.sciencedirect.com/science/article/pii/S1096751615300075

LIVINGSTONE, S. a M. BULGER, 2013. *A Global Agenda for Children's Rights in the Digital Age* [online]. Florence: UNICEF Office of Research [cit. 2016-03-15]. Dostupné z: http://www.unicef-irc.org/publications/pdf/lse%20olol%20final3.pdf

LIVINGSTONE, S. a L. HADDON, 2008. Risky experiences for children online: Charting European research on children and the Internet. *Children & society* [online]. roč. 22, č. 4, s. 314–323 [cit. 2012-04-13]. ISSN 0951-0605. Dostupné z: http://eprints.lse.ac.uk/27076/

LIVINGSTONE, S. a L. HADDON, 2009. *EU Kids Online: Final Report* [online]. London: EU Kids Online [cit. 2011-10-24]. Dostupné z: http://www.lse.ac.uk/media@lse/research/EUKidsOnline/EU%20Kids%20I%20%282006-9%29/EU%20Kids%20Online%20I%20Reports/EUKidsOnlineFinalReport.pdf

MARANTO, G. a M. BARTON, 2010. Paradox and Promise: MySpace, Facebook, and the Sociopolitics of Social Networking in the Writing Classroom. *Computers and Composition* [online]. roč. 27, č. 1, s. 36–47 [cit. 2012-04-16]. ISSN 87554615. DOI 10.1016/j.compcom.2009.11.003. Dostupné z: http://www.mendeley.com/research/paradox-promise-myspace-facebook-sociopolitics-social-networking-writing-classroom/

MELOUN, M. a J. MILITKÝ, 2006. *Kompendium statistického zpracování dat: Metody a řešené úlohy*. Vyd. 2., přeprac. a rozš. Praha: Academia. 982 s. ISBN 80-200-1396-2.

MORENO M. A., M. PARKS a L. P. RICHARDSON, 2007. What are adolescents showing the world about their health risk behaviors on MySpace? *MedGenMed* [online]. roč. 9, č. 4 [cit. 2013-01-29]. Dostupné z: http://www.ncbi.nlm.nih.gov/pmc/articles/PMC2234280/

NASKE, P., 2011. Výuka informatiky a ICT na SŠ v ČR – rok 2011. *Metodický portál: Články* [online]. [cit. 2016-04-02]. ISSN 1802-4785. Dostupné z: http://clanky.rvp.cz/clanek/c/o/14359/vyuka-informatiky-a-ict-na-ss-v-cr---rok-2011.html

O'CONNOR, K. W. a G. B. SCHMIDT, 2015. "Facebook Fired": Legal Standards for Social Media–Based Terminations of K-12 Public School Teachers. *Journal of Workplace*

Rights (Sage Open) [online]. roč. 5, č. 1, s. 1–11 [cit. 2016-03-15]. Dostupné z: http://opus.ipfw.edu/ols_facpubs/82

OECD, 2011. The Protection of Children Online: Risks Faced by Children Online and Policies to Protect Them. In: *OECD Digital Economy Papers, No. 179* [online]. Paris: OECD Publishing [cit. 2012-08-15]. Dostupné z: http://dx.doi.org/10.1787/5kgcjf71pl28-en

OFCOM, 2011. *Children and parents: Media use and attitudes report* [online]. [cit. 2012-04-15]. Dostupné z: http://stakeholders.ofcom.org.uk/binaries/research/media-literacy/oct2011/Children_and_parents.pdf

OFCOM, 2015. *Ofcom report on internet safety measures: Strategies of parental protection for children online* [online]. [cit. 2016-03-15]. Dostupné z: http://stakeholders.ofcom.org.uk/binaries/internet/fourth_internet_safety_report.pdf

OFSTED, 2010. *The safe use of new technologies* [online]. Manchester: Ofsted [cit. 2013-02-02]. Dostupné z: http://webarchive.nationalarchives.gov.uk/20120408131156/http://www.ofsted.gov.uk/sites/default/files/documents/surveys-and-good-practice/t/The%20safe%20use%20of%20new%20technologies.pdf

PAPAVASILIOU, S., 2009. *Survey: Promotion of internet safety into the school curriculum* [online]. SaferInternet.gr [cit. 2012-05-30]. Dostupné z: http://www.saferinternet.org/c/document_library/get_file?p_l_id=10526&folderId=19099&name=DLFE-416.doc

PELIKÁN, J., 2004. *Základy empirického výzkumu pedagogických jevů*. Dotisk 1. vyd. Praha: Karolinum. 270 s. ISBN 80-7184-569-8.

PHIPPEN, A., 2011. *The Online Abuse of Professionals: Research Report from the UK Safer Internet Centre* [online]. Exeter: South West Grid for Learning [cit. 2013-02-02]. Dostupné z: http://files.lgfl.net/eSafety/Publications/11%2008%20swgfl%20-%20online%20abuse%20of%20professionals%20-%20Prof-Abuse-Full-Report.pdf

PÖSCHL, R., 2005. *Vnímání významu matematiky a fyziky středoškolskými studenty* [online]. Praha [cit. 2016-02-01]. Diplomová práce. Univerzita Karlova v Praze, Matematicko-fyzikální fakulta, Katedra didaktiky fyziky. Dostupné z: https://kdf.mff.cuni.cz/vyzkum/materialy/vnimani_vyznamu_M_a_F.pdf

PRŮCHA, J., E. WALTEROVÁ a J. MAREŠ, 2009. *Pedagogický slovník*. 6., aktualiz. a rozš. vyd. Praha: Portál. ISBN 978-80-7367-647-6.

PURCELL, K. et al., 2013. *How Teachers Are Using Technology at Home and in Their Classrooms* [online]. Washington D.C.: Pew Research Center [cit. 2016-03-15]. Dostupné z: http://www.pewinternet.org/files/old-media/Files/Reports/2013/PIP_TeachersandTechnologywithmethodology_PDF.pdf

RAMBOUSEK, V. et al., 2007. *Výzkum informační výchovy na základních školách*. Plzeň: Koniáš. 359 s. ISBN 978-80-86948-10-2.

SEAMAN, J. a H. TINTI-KANE, 2013. *Social Media for Teaching and Learning* [online]. Boston: Pearson [cit. 2016-03-14]. Dostupné z: http://www.pearsonlearningsolutions.com/assets/downloads/reports/social-media-for-teaching-and-learning-2013-report.pdf

SHARPLES, M. et al., 2009. E-safety and Web 2.0 for children aged 11–16. *Journal of Computer Assisted Learning* [online]. roč. 25, č. 1, s. 70–84 [cit. 2013-01-11]. DOI 10.1111/j.1365-2729.2008.00304.x. Dostupné z: http://onlinelibrary.wiley.com/doi/10.1111/j.1365-2729.2008.00304.x/full

SIMPSON, M. D., 2008. The Whole World (Wide Web) is Watching. *National Education Association* [online]. [cit. 2012-05-22]. Dostupné z: http://www.nea.org/home/12784.htm

SKINNER, B. F., 2014. *Science and human behavior* [online]. The B. F. Skinner Foundation [cit. 2016-01-15]. Dostupné z: http://www.bfskinner.org/newtestsite/wp-content/uploads/2014/02/ScienceHumanBehavior.pdf

SOUTH WEST GRID FOR LEARNING, 2009. *School Online Safety Template Policy* [online]. Exeter: South West Grid For Learning [cit. 2013-03-13]. Dostupné z: http://swgfl.org.uk/products-services/esafety/resources/creating-an-esafety-policy/Content/ESP_template-School-Template-Policy.aspx

SPIELHOFER, T., 2010. *Children's online risks and safety: A review of the available evidence* [online]. Slough: Nfer [cit. 2012-10-04]. Dostupné z: http://www.nfer.ac.uk/nfer/publications/COJ01/COJ01.pdf

STEEVES, V., 2012. *Young Canadians In A Wired World – Phase III: Teachers' Perspectives* [online]. Ottawa: MediaSmarts [cit. 2013-02-01]. Dostupné z: http://mediasmarts.ca/sites/mediasmarts/files/pdfs/publication-report/full/YCWWIII-Teachers-Perspectives.pdf

STEGANOS GmbH, 2008. *The state of computer privacy: Steganos 2008 survey into PC security* [online]. [cit. 2012-02-02]. Dostupné z: http://www.steganos.com/uploads/media/Steganos_Press_Release_2008-10-24_SurveyPCusersGraphicsWhitePaper.pdf

STRAUSS, A. a J. CORBINOVÁ, 1999. *Základy kvalitativního výzkumu: Postupy a techniky metody zakotvené teorie* (S. Ježek, Překl.). Boskovice: Albert. 228 s. ISBN 80-85834-60-X.

SYMANTEC CORPORATION, 2009. *Norton Online Living Report 09* [online]. Mountain View: Symantec Corporation [cit. 2012-10-04]. Dostupné z: http://us.norton.com/content/en/us/home_homeoffice/media/pdf/nofr/NOLR_Report_09.pdf

SYMANTEC CORPORATION, 2010. *Norton Online Family Report: Global insights into family life online* [online]. Mountain View: Symantec Corporation [cit. 2012-10-04]. Dostupné z: http://us.norton.com/content/en/us/home_homeoffice/media/pdf/nofr/Norton_Family-Report-USA_June9.pdf

SYMANTEC CORPORATION, 2011a. *Norton Cybercrime Report* [online]. Mountain View: Symantec Corporation [cit. 2012-08-22]. Dostupné z: http://us.norton.com/content/en/us/home_homeoffice/html/cybercrimereport/assets/downloads/en-us/NCR-DataSheet.pdf

SYMANTEC CORPORATION, 2011b. *Norton Cybercrime Report 2011* [online]. Mountain View: Symantec Corporation [cit. 2012-08-22]. Dostupné z: http://www.symantec.com/content/en/us/home_homeoffice/html/ncr/

SYMANTEC CORPORATION, 2013. *2013 Norton Report* [online]. Mountain View: Symantec Corporation [cit. 2016-03-15]. Dostupné z: https://www.symantec.com/content/en/us/about/presskits/b-norton-report-2013.en_ca.pdf

SYMANTEC CORPORATION, 2015. *Norton Cybersecurity Insights Report: Global Comparisons* [online]. Mountain View: Symantec Corporation [cit. 2016-03-15]. Dostupné z: https://us.norton.com/norton-cybersecurity-insights-report-us?inid=hho_norton.com_cybersecurityinsights_p3_seectryrpts

ŠEĎOVÁ, K., 2007a. Analýza kvalitativních dat. In: ŠVAŘÍČEK, R., K. ŠEĎOVÁ et al. *Kvalitativní výzkum v pedagogických vědách*. Praha: Portál, s. 207–247. ISBN 978-80-7367-313-0.

ŠEĎOVÁ, K., 2007b. Proces kvalitativního výzkumu a jeho plánování. In: ŠVAŘÍČEK, R., K. ŠEĎOVÁ et al. *Kvalitativní výzkum v pedagogických vědách*. Praha: Portál, s. 51–82. ISBN 978-80-7367-313-0.

ŠEĎOVÁ, K., 2007c. Zakotvená teorie. In: ŠVAŘÍČEK, R., K. ŠEĎOVÁ et al. *Kvalitativní výzkum v pedagogických vědách*. Praha: Portál, s. 84–96. ISBN 978-80-7367-313-0.

ŠERÝ, M., 2013. *Použití sémantického diferenciálu při hodnocení výuky na ZŠ* [online]. České Budějovice [cit. 2016-02-01]. Disertační práce. Jihočeská univerzita v Českých Budějovicích, Pedagogická fakulta, Katedra informatiky. Dostupné z: http://theses.cz/id/m7rifg/Disertacni_prace_2013_v_28.pdf

ŠVAŘÍČEK, R., 2007a. Hloubkový rozhovor. In: ŠVAŘÍČEK, R., K. ŠEĎOVÁ et al. *Kvalitativní výzkum v pedagogických vědách*. Praha: Portál, s. 159–184. ISBN 978-80-7367-313-0.

ŠVAŘÍČEK, R., 2007b. Kritéria kvality kvalitativního výzkumu. In: ŠVAŘÍČEK, R., K. ŠEĎOVÁ et al. *Kvalitativní výzkum v pedagogických vědách*. Praha: Portál, s. 28–50. ISBN 978-80-7367-313-0.

ŠVAŘÍČEK, R., 2007c. Triangulace. In: ŠVAŘÍČEK, R., K. ŠEĎOVÁ et al. *Kvalitativní výzkum v pedagogických vědách*. Praha: Portál, s. 202–206. ISBN 978-80-7367-313-0.

TEER, F. P., S. E. KRUCK a G. P. KRUCK, 2007. Empirical study of students computer security practices and perceptions. *Journal of Computer Information Systems*. roč. 47, č. 3, s. 105–110.

THE GALLUP ORGANISATION, 2008. *Towards a safer use of the Internet for children in the EU: A parents' perspective* [online]. [cit. 2012-07-11]. Dostupné z: http://ec.europa.eu/public_opinion/flash/fl_248_en.pdf

TNS OPINION & SOCIAL, 2015. *Special Eurobarometer 423 "Cyber Security"* [online]. [cit. 2016-04-02]. Dostupné z: http://ec.europa.eu/public_opinion/archives/ebs/ebs_423_en.pdf

VALCKE, M. et al., 2007. Primary school children's safe and unsafe use of the Internet at home and at school: An exploratory study. *Computers in Human Behavior* [online]. roč. 23, č. 6, s. 2838–2850 [cit. 2012-04-02]. ISSN 07475632. DOI 10.1016/j.chb.2006.05.008. Dostupné z: http://users.ugent.be/~mvalcke/CV/vecits.pdf

VETEŠKA, J., 2010. *Kompetence ve vzdělávání dospělých: pedagogické, andragogické a sociální aspekty*. Vyd. 1. Praha: Univerzita Jana Amose Komenského. ISBN 978-80-86723-98-3.

VETEŠKA, J. a M. TURECKIOVÁ, 2008a. *Kompetence ve vzdělávání*. Vyd. 1. Praha: Grada. ISBN 978-80-247-1770-8.

VETEŠKA, J. a M. TURECKIOVÁ, 2008b. *Vzdělávání a rozvoj podle kompetencí: kompetence v andragogice, pedagogice a řízení*. Vyd. 1. Praha: Univerzita Jana Amose Komenského. ISBN 978-80-86723-54-9.

ZATLOUKAL, T. et al., 2014. *Výroční zpráva České školní inspekce za školní rok 2013/2014* [online]. Praha: Česká školní inspekce [cit. 2016-03-19]. ISBN 978-80-905632-7-8. Dostupné z: http://www.csicr.cz/getattachment/dd56770f-2211-42bf-92d3-8265b8cb3530

ZOUZALOVÁ, S. a L. MALYON, 2011. Digitální dospělost? Průměrný jedenáctiletý má v oblasti technologií „znalosti dospělého člověka“. In: *AVG* [online]. Amsterdam: AVG Technologies [cit. 2013-02-02]. Dostupné z: http://www.avg.com/cz-cs/tiskove-zpravy.ndi-2753

ZOUZALOVÁ, S. a M. MADROVÁ, 2012. Váš budoucí zaměstnavatel se dívá. In: *AVG* [online]. Praha: AVG Technologies [cit. 2013-02-02]. Dostupné z: http://www.cnews.cz/vas-budouci-zamestnavatel-se-diva

PŘÍLOHY

Příloha A: Didaktický test předkládaný učitelům během rozhovorů

1. Co si myslíte, že je hlavním důvodem, proč lidé posílají spamy?[27]
   a) Protože se nudí
   b) Aby vydělali peníze
   c) Schválně otravují jiné lidi
   d) Chtějí získat nové přátele

2. Kolega Vás přijde požádat o radu – antivirový program na jeho počítači hlásí, že virová databáze je zastaralá. Co tato situace znamená?
   a) Antivir je mimo provoz, soubory nejsou kontrolovány
   b) Antivir není schopen odhalit nové hrozby
   c) Antivir pouze hlásí, že za posledních 24 hodin se ve světě neobjevila žádná nová virová nákaza
   d) Antivir oznamuje, že v počítači již 168 hodin nebyl nalezen nakažený soubor

3. Je bezpečné mít na USB flash disku důležitá data, která nejsou uložena nikde jinde, pokud nehrozí riziko fyzické ztráty zařízení?
   a) Ano
   b) Ne, data na USB flash disku se samovolně mohou stát nečitelnými
   c) Ne, na USB flash discích se po roce od poslední změny data sama smažou
   d) Ne, data na USB flash disk jsou náchylná ke smazání působením magnetu
   e) Ne, USB flash disk při zaplnění kapacity začne přepisovat nejstarší data

4. Během přestávky Vás přijde jeden z Vašich žáků požádat o radu. Obdržel e-mail, ve kterém je vyzván, aby zaslal zpět uživatelské jména a heslo k sociální síti Facebook. Autor e-mailu hrozí, že jestli požadovaná data nezašle, bude mu účet deaktivován. Jak by se měl zachovat?[28]
   a) Měl by vyplnit požadované informace a odpověď odeslat
   b) Měl by se zeptat odesilatele, proč je nutné data zasílat
   c) Měl by tento e-mail smazat
   d) Měl by se pokusit ověřit jméno odesilatele e-mailu na Internetu a podle toho se rozhodnout.

[27] Otázka byla převzata ze soutěže Bobřík informatiky. Původním autorem otázky je J. Helgers, otázka byla v rámci Bebras Contest publikována pod kódem 2010-NL-05.
[28] Otázka byla převzata ze soutěže Bobřík informatiky, v rámci Bebras Contest byla publikována pod kódem 2010-AT-03.

5. Za jakých podmínek je možné na sociální síti sdílet fotografie kamarádů ze společných akcí?[29]
   a) Pokud není obsah fotografie v rozporu se zákony České republiky
   b) Pokud je fotografie nijak neuráží či nezesměšňují
   c) Pokud jsou mezi přáteli na dané sociální síti
   d) Pokud k tomu dali svůj souhlas

6. Při prohlížení videí na webové stránce se objeví okno se zprávou, že počítač je nakažen počítačovým virem. Zároveň je zde ke stažení nabízen zdarma antivirový program. Jak by se měl člověk zachovat?
   a) Zprávu ignorovat a antivir nestahovat
   b) Antivir stáhnout a nainstalovat

7. Obdržíte anglicky psaný e-mail o výhře $ 10 000, kde jste jako odesilatel uveden Vy. Žádný takový e-mail jste si samozřejmě neposílal. Jak se zachováte?
   a) E-mailovou schránku bych měl(a) přestat používat, protože nad ní útočník převzal kontrolu a má přístup k veškerému obsahu
   b) Změním přístupové heslo k e-mailové schránce, aby ji útočník nemohl dále zneužívat
   c) Neudělám nic, danou e-mailovou zprávu budu ignorovat
   d) Rozešlu všem známým e-mail, že jsem tuto zprávu neposílal já

8. Vašemu partnerovi přijde do e-mailové schránky zpráva, že mu (jí) kdosi zasílá fotografie z letní dovolené a v příloze je soubor fotogalerie.exe. Váš partner si na jméno odesilatele nevzpomíná a ani Vám jméno nic neříká. Jaký postup doporučíte?[30]
   a) Ať si stáhne soubor do počítače a fotografie si prohlédne – nic se nemůže stát
   b) Ať e-mail smaže, soubor s příponou exe asi nebude fotogalerie
   c) Ať e-mail smaže, protože odesilatele nezná
   d) Ať stáhne soubor do počítače, zkontroluje jej antivirem a pak si prohlédne fotogalerii

[29] Otázka byla převzata ze soutěže Bobřík informatiky. Původními autory otázky jsou M. Slobodová a P. Tomcsányi, otázka byla v rámci Bebras Contest publikována pod kódem 2010-SK-10.
[30] Otázka byla převzata z bakalářské práce J. Lhotáka (2010).

Příloha B: Seznam hlavních otázek pro rozhovory s učiteli

Okruh hlavních otázek k problematice malware:

- V této otázce (otázka 10 v testu) jste odpověděl, že byste e-mail smazal. Proč byste tak učinil?
  - *Pozn.: Zeptat se tehdy, pokud takto skutečně odpověděl*
- Jak se snažíte chránit před útoky virů a spyware?
  - Podotázka: Na základě čeho jste si tuto strategii vypracoval? (Ve smyslu Co Vás inspirovalo k vypracování této strategie?)
- Jak byste reagoval, pokud by Váš počítač byl napaden virem a antivir by nefungoval?
- Stalo se Vám někdy, že byste kvůli své neopatrnosti stáhl do počítače virus?
  - Podotázka: Jak Vás tato situace ovlivnila?
    - *Pozn.: Zeptat se, pokud se to někdy stalo*

Okruh hlavních otázek k problematice spamu a hoaxu:

- V této otázce (otázka 9 v testu) jste odpověděl, že… Máte představu, jak by se mohlo stát, že byste byl uveden jako odesilatel e-mailu, i když jste ho neposílal?
- Jak se bráníte proti doručování spamu?
  - Podotázka: Na základě čeho jste si tuto strategii vypracoval?
- Jak budete reagovat, pokud dostanete do e-mailové schránky takovýto e-mail?
  - *Pozn.: Předložit vytištěnou e-mailovou zprávu z Přílohy C*
  - Podotázka: Co Vás vedlo k tomu, že jste si vypracoval právě takovouto strategii?

Okruh hlavních otázek k problematice sdílení osobních dat:

- Jaký je Váš názor na používání sociálních sítí?
  - *Pozn.: Jádro otázky, zda používá soc. sítě a co zde prezentuje*
- Co si myslíte o tom, že si učitel přidává žáky na sociálních sítích mezi své přátele?
- Jaký je Váš názor na sebeprezentaci člověka na Internetu?
- Co Vás ovlivnilo při rozhodování, zda se připojit na sociální síť / vytvořit si blog, kanál na Youtube, galerii na Picase?
- Jaké materiály či zdroje mohou učiteli pomoci při rozhodování, zda používat sociální sítě a přátelit se se žáky?
- Podle čeho se rozhodujete, zda v nějakém formuláři webové stránky uvedete své osobní údaje (telefon, e-mail, adresu)?

Okruh hlavních otázek k problematice počítačových hesel a krádeží identity:

- Co si myslíte o používání několika různých bezpečnostních hesel současně?
  - *Pozn.: Jádro otázky, zda jich sám používá více*
  - Podotázka: Používáte ke každé službě jedinečné heslo?
    - *Pozn.: Zeptat se, pokud používá více hesel*
    - Podotázka: Podle čeho volíte služby, k nimž používáte stejné heslo?
      - *Pozn.: Zeptat se, pokud nepoužívá u každé služby jedinečné heslo*
- Co Vás vedlo k tomu, že jste (ne)začal používat více bezpečnostních hesel?
  - *Pozn.: Ve smyslu, zda k tomu přispěly externí zdroje*
- Co si myslíte o obměňování bezpečnostních hesel?
  - *Pozn.: Jádro otázky, zda je sám obměňuje*
  - Podotázka: Jaký je důvod, že se rozhodnete nějaké heslo obměnit?
    - *Pozn.: Zeptat se, pokud je skutečně obměňuje*
  - Podotázka: Co Vás vedlo k tomu, že jste začal pravidelně obměňovat bezpečnostní hesla?
    - *Pozn.: Ve smyslu, zda k tomu přispěly externí zdroje*
    - *Pozn.: Zeptat se, pokud je skutečně pravidelně obměňuje*
- Jaké typy hesel jsou podle Vás bezpečné / nebezpečné?
  - Podotázka: Jak jste dospěl k názoru, že zrovna tato hesla jsou bezpečná / nebezpečná?

Okruh hlavních otázek k problematice havárií počítačů:

- Jaká data je podle Vás vhodné zálohovat?
- Jakým způsobem je podle Vás vhodné zálohovat počítačová data?
- Jaký systém zálohování jste si vytvořil?
- Co Vás vedlo k tomu, že jste (ne)začal zálohovat svá data?
  - Podotázka: Přihodila se Vám někdy ztráta dat?
- Na základě čeho jste si vypracoval právě takovouto strategii?

Okruh hlavních všeobecných otázek:

- Co si myslíte, že by mohlo patřit do problematiky e-bezpečnosti?
- Jak se orientujete v problematice, o které jste nyní hovořil?
  - *Poznámka: Tuto otázku položit na začátku rozhovoru i na konci*
- Povězte mi o Vašem vztahu k informatice, jak jste se stal učitelem informatiky?
- Do jaké míry mají učitelé, kteří nevystudovali informatiku, ztíženou pozici při výuce témat, o kterých jsme mluvili?

Příloha C: Vzorová hoaxová zpráva[31]

[redacted]@seznam.cz)

Zkontrolujte si svůj šampon

26. 3. 2013, 15:11:53

Komu: v.simandl@seznam.cz

Rakovinotvorný SLS ve většině šamponů a v zubních pastách Colgate

Prosím čtěte pozorně. Zkontrolujte si doma svůj šampon.

Přečtěte si názvy látek v něm obsažené a prověřte, zda je mezi nimi Sodium Laureth Sulfate (nebo zkratka SLS). Tato látka je ve většině šamponů. Výrobci ji používají, neboť produkuje velké množství pěny a je levná. ALE - skutečností je, že SLS je tak silná chemikálie, že se používá na drhnutí garážových podlah! A je dokázáno, že po čase způsobuje rakovinu! To není vtip.

Mimochodem, SLS k vytváření "bublinek" obsahuje také zubní pasta Colgate!

Průzkum ukázal, že pravděpodobnost onemocnění rakovinou byla v osmdesátých letech 1:8000, zatímco v devadesátých už 1:3, což je nesmírně vážné.

Doufám, že to vezmete vážně i vy. Předejte tuto informaci ostatním, snad se tak přestaneme „prodávat“ rakovině. Jedná se o naše zdraví.

[31] Zpráva byla převzata z (Džubák, 2005).

Příloha D: Přehled kódů vztažených k jednotlivým kategoriím

Důvody (ne)používání SNS

Výuka: nevyužitelnost SNS pro výuku, sociální sítě – pracovní nástroj pro jiná povolání, výhody SNS pro výuku – komunikace, SNS – využitelnost pro výuku

Komunikace: pomoc při naplňování koníčku, SNS – příjem informací, SNS – zvědavost, sociální sítě – možnost komunikace, SNS – možnost spolupráce, SNS – zdroj pracovních informací dle zaměření, SNS – zábava, SNS – rychlé šíření informací, SNS – možnost kontaktu s exžáky, SNS – zdroj zájmových informací

Překážky: SNS – časová náročnost, SNS – nízká priorita, sociální sítě – koncentrace nepodložených informací, věková vymezenost vůči SNS, SNS – nedostatek spolupráce, SNS – bezpečnostní rizika, SNS – neosobnost, SNS – cílená reklama, SNS – možnost krádeže identity

Celkově: kritický pohled na SNS

Hodnocení druhých

kritika chování druhých, požadavek kompetentnosti uživatelů, překvapení z kompetencí druhých, kritika restriktivních nastavení

Konkrétní způsoby ochrany a návyky – hesla

***Množství hesel* (řazení):** jedinečnost důležitých hesel, více hesel, jedno heslo pro více služeb, jedno heslo pro podobné služby, jednorázové zapomenutelné heslo, jednorázové sdružené heslo, podobnost hesel, oblíbené heslo, jednotné heslo

***Obměna hesel* (řazení):** neobměňování hesel, nepravidelné obměňování hesel, příležitostné měnění hesel, obměňování hesel, pravidelné měnění hesel

***Obsah hesel* (řazení):** dlouhé heslo, heslo neobsahuje slovo, heslo jako sousloví, komplexní heslo, kombinace osobních dat, používání vygenerovaného hesla, osobní údaj jako heslo

***Typ obměny*:** zcela nová sada, částečná změna hesla, prohození hesel

***Uchování hesel* (řazení):** pamatování hesel, papírový seznam šifrovaných hesel, hesla v telefonu jako tel. čísla, papírový seznam nedůležitých hesel, papírový seznam generovaných hesel, sdělení hesel v rodině

fyzická ochrana hesla, rychlé psaní hesel, dvoufázová autentifikace, cloudový účet s omezenými právy, nezapamatovat heslo v prohlížeči, jednorázové sdělení hesla, provedení obměny hesla,

Konkrétní způsoby ochrany a návyky – obecné

ad-hoc hledání návodů, řešení problému svépomocí, hledání externí pomoci, konzultace praktického problému, nehledání strategie obrany, pomoc rodiny, průběžné sbírání informací, sbírání informací z více míst, uvědomění si dřívějších chyb, žádost o pomoc

známých odborníků, studium nezbytných informací, opuštění ochrany, přiměřené nároky na uživatele, restriktivní nastavení

Konkrétní způsoby ochrany a návyky – soukromí

Přátelení se žáky **(řazení):** odmítání přátelení se žáky, odmítání odhalování soukromí před žáky, akceptování přátelení se s žáky – dřívějšími přáteli, provádění přátelení s ex-žáky, odpřátelení se se žáky, neodmítání přátelení se žáky, přátelení se s prověřenými žáky, SNS – odmítání prvního kroku se žáky, přátelení se se žáky, odhalování soukromí před žáky

Používání SNS **(řazení):** nepoužívání SNS, nízké používání SNS, používání specializované SNS, časté používání SNS, školní SNS účet

Soukromí **(řazení):** aktivní chránění si soukromí, SNS – důsledné zabezpečení soukromí, SNS – neodhalování soukromí, nepoužívání fotoalb, uzavřenost vůči SNS, SNS – pracovně-zájmový profil, omezené sdílení fotek, rušení nepoužívaných účtů, uveřejnění hudebního vkusu, ochrana soukromí na SNS – alegorie, uveřejnění informací sdělovaných ne-virtuálně, SNS – odmítání viditelnosti pro třetí osoby, odmítání přátelení s nadřízenými, SNS – řízení informací o sobě, zaheslovaná fotoalba, prezentace fotek v cloudu, SNS – zveřejňování nezávadných fotografií, SNS – aktivní posty, SNS – zveřejňování fotografií, odhalování soukromí, SNS – otevřený profil

Konkrétní způsoby ochrany a návyky – viry a nefunkční OS

(Ne)Prevence **(řazení):** pravidelná aktualizace SW, pravidelná antivirová prevence, aktivní antivirová kontrola, restriktivní nastavení, vlastní nastavení antiviru, důraz na okamžité aktualizace, účty ve Windows, nenavštěvování rizikových stránek, prověřený zdroj, nespouštění rizikového obsahu, spolehnutí se na antivir, navštěvování rizikových stránek

Řešení následků **(řazení):** restart počítače, vir – podívat se do systému, spolehnutí se na antivir, vir odstraňovaný antivirem, ruční odstranění viru, nouzový režim, obnova systému-čistý obraz, reinstalace systému, formát pevného disku

Konkrétní způsoby ochrany a návyky – web a e-mail

Registrace **(řazení):** odmítání registrací, odmítání registrací – hledání alternativních řešení, smyšlené jméno, podstoupení registrace, pravdivé jméno,

Registrace e-shop (řazení): podstoupení registrace e-shop, e-shop – platba při převzetí, odmítání registrací, nepoužívání e-shopů

Ochrana před spamem **(řazení):** nešířit e-mailovou adresu, e-mail – nahrazení zavináče, kontrola původnosti, sekundární adresa, cílené nereagování na spam, neodhalování aktivity účtu, použití skryté kopie, smazání e-mailu, označení spamu, neotevírání e-mailu, odmítnutí reklamních sdělení, mail – unsubscribe, vlastní filtrování spamu, nebránění se spamu, primární adresa, otevření e-mailu

***Ochrana před hoaxem* (řazení):** ověření hoax.cz, nezávislé ověření informací, komunitní ověření pravdivosti hoaxu, odmítání pasivního přijetí informací, nezávazné ověření pravdivosti hoaxu, ověřování hoaxu offline, odmítání hromadných mailů od známých, smazání e-mailu, rezignace na ověření marginálních informací, rezignace na ověření marginálních informací

(Ne)šíření hoaxu: nepřeposílat nedůvěryhodné e-maily, nepřeposílání e-mailů, přeposílání důvěryhodných mailů, šíření ověřených informací

Hledání na internetu: vybírání relevantního zdroje, hledání ve více zdrojích, aktivní hledání zdrojů,

průběžná kontrola originálnosti webu, aktivní hledání zdrojů a služeb

Konkrétní způsoby ochrany a návyky – zálohování

***Typ zálohy* (řazení):** kompletní záloha, systematické zálohování, přírůstková záloha, záloha ad-hoc aktuálních dat, nesystematické zálohování

***Četnost záloh* (řazení):** automatické zálohování, pravidelnost záloh, zálohování při rizikové operaci, záloha ad-hoc aktuálních dat

Obsah záloh: zálohování důležitých dat, důraz na uchování fotek, uchovávání originálních souborů

Místo záloh: vícenásobná záloha, záloha do mailu, záloha na externí disk, zálohování do cloudu, fotogalerie jako záloha, zálohování na CD, zálohování na flashku, záloha na více PC, zálohování na papír

Důvody záloh: ochrana před ztrátou, zálohování pro uspořádání dat, zálohování pro uvolnění místa

provedení zálohy, použití zálohy, fyzická péče o zálohy,

Negativa ochrany

časová náročnost, odfiltrování i důležitých e-mailů, zapomenuté heslo, informační ochuzení, nutný update zálohy po změně dat

Okolnosti rozhodování

cennost dat, časová náročnost, nedokonalost tech. zábran, pomoc studentům, různá citlivost dat, různá důležitost služeb, trvanlivost dat, využití vlastní kreativity, návazné ověřující služby, pocit zodpovědnosti za školní sít

Projevy osobnostních vlastností

Osoba učitele: přátelský vztah se žáky, liberální přístup učitel-žák, demokratická výchova, obava o ztrátu autority, oddělení práce a osobního života, odstup učitel-žák, opatrnost kvůli žákům, zachování role učitele, propast učitel-žák, obava ze ztráty kroku s trendy,

snaha o vhled do života žáků, neobava z obsahu žákovských profilů na SNS, obava z obsahu žákovských profilů na SNS

(Ne)důvěra ve druhé: despekt vůči virtuálnímu životu, důvěra v profesionální řešení, důvěra ve vyzkoušené služby, důvěra ve služby zaměstnavatele, důvěra v reference známých, důvěra ve firmy zavazující se k ochraně dat, důvěra ve schopnosti druhých, důvěra v technické řešení, hoax – důvěra v oficiální zdroje, nedůvěra v cizí osoby a subjekty, nedůvěra v neznámé weby, nedůvěra v okrajové weby, nedůvěra v rizikové weby, nedůvěra v původ mailu, nedůvěra v technická řešení, nedůvěra ve schopnosti druhých, nedůvěra ve věci zdarma, nedůvěra v cizí infrastrukturu, omezenost důvěry v blízké, různá důvěra v ochranu hesel, obava o zabezpečení služeb, důvěra ve známé osoby – absence rizika, důvěra v šanci na nápravu

Obava o soukromí / majetek: hoax – obava z pravdivosti hrozby, obava o soukromí, obava z viru, obava z krádeže identity, obava ze ztráty dat, obava zneužití soukromých dat, ochrana osobnosti, ochrana soukromí, akutní obava o soukromí

Obava z něčeho: neobava z rizik, obava z prolomení hesla, obava z podvodu na internetu, obava z vlastní chyby, obava z promyšlenosti hrozby, obava z nepravdivosti informací na webu

Přemýšlení = snaha řešit rozumem: mít vlastní rozum, nespoléhání se na technickou ochranu, přemýšlení o pravdivosti, přemýšlení o problematice, rozhodování o podstoupení rizika, subjektivní rozlišení výše rizik

Profesionální / open řešení: důvěra v profesionální řešení, nedůvěra ve věci zdarma

bezpečnostní problém jako banální věc, inspirace názory druhých, preferování zdarma dostupného řešení, morální zásady, účel světí prostředky, ohled na druhé, zájem o zjištění pravdivosti, nelhaní o své osobě

Překážky ochrany

Vnější: nedokonalost tech. řešení, nedokonalost tech. zábran, nekomplexnost pravidel, offline důvody pro zveřejnění e-mailu, pracovní důvody – šíření mailu, vnější tlak na zveřejnění osobních informací, výukové důvody – přátelení se se žáky, operace v účtu druhou osobou, kusé a nevyvážené informace, požadavek registrace

Vnitřní: důvěra ve známé osoby – absence rizika, matná znalost, nedostatečné odborné znalosti, pocit nízké citlivosti dat, pocit nízké odbornosti, pohodlnost, přesycenost okrajovými informacemi, rezignace na plnou ochranu, únava, spěch, důvěra v šanci na nápravu, odmítnutí viny

Vnitřně-vnější: časová náročnost, náročnost na pamatování, zahlcenost daty, neaktuálnost záloh

Reakce na vnější vlivy

***Cílenost*:** nepoučení ze zkušenosti, poučení se ze zkušenosti, zkušenostní upevnění, neosvojený vnější požadavek, osvojený vnější požadavek, reakce na změnu podmínek, zklamání

Subjektivní hodnocení znalostí a chování

***Odbornost* (řazení):** dostatečné odborné znalosti, průměrný odborník, pocit schopnosti odstranění následků, pocit vhledu do IT, dostatečné znalosti pro výuku, pocit přiměřené orientace v problematice, poučený laik, ne-odborník v ICT, pocit nízké odbornosti, přiznání nedostatků v rozhledu, uvědomění si nedodržení doporučení, obava z nekompetentnosti při řešení problému, pocit neschopnosti rozeznat hrozbu, nedostatečné odborné znalosti pro výuku

spokojenost s návykem / řešením, pocit otevřenosti vůči SNS, pocit přiměřené obavy z malware

Technická ochrana

antispam, antispyware, antivirus, automatické aktualizace, bod obnovy systému, defaultní spamový filtr, firewall, SW na pamatování hesel, antivirová ochrana v cloudu

Vnější vlivy na chování

Samostudium: aktivní samostudium, ovlivnění internetem, doplňování znalostí z učebnic, ovlivnění časopisy o ICT, ovlivnění časopisy o uceleném tématu, ovlivnění manuály, ovlivnění učebnicemi, ovlivnění Facebookem, ovlivnění médii

Výuka: ovlivnění střední školou, ovlivnění školeními, ovlivnění vysokou školou, minimální ovlivnění vysokou školou, ovlivnění výukou obecně

Zkušenost: chybějící konkrétní osobni zkušenost, dříve nadměrná ochrana, dříve benevolentnější ochrana, negativní osobní zkušenost, negativní přenesená zkušenost, neprodělaná negativní osobní zkušenost, opakovaná negativní zkušenost, zkušenost s řešením problémů, řešení problému jako správce sítě, uživatelská osobní zkušenost, změna citlivosti dat

Aktivní interakce: ovlivnění kolegy, ovlivnění odborníky na ICT, ovlivnění znalejšími osobami, ovlivnění komunitou,

Zamýšlené mající jiný cíl: ovlivnění internetem, ovlivnění varováním systému, ovlivnění novou technologií, vnější bezpečnostní požadavek

ovlivnění obecné, metoda pokus-omyl

Vnitřní prameny

důvěřivost, intuitivní chování, nedůvěřivost, ochota se učit, ohleduplnost, opatrnost, pragmatičnost, pravdomluvnost, přemýšlivost, strach, zvědavost, zvídavost, zodpovědnost, zájem o technickou e-bezpečnost, neopatrnost, vyrovnanost

Vztah k bezpečnostním pravidlům

***Respektování* (řazení):** vlastní bezpečnostní pravidla, přirozené naplňování doporučení, přirozené doplnění offline návyků, respektování vlastních rad dávaných žákům, přijetí teoret. názorů, prosazování zásad u okolí, uvědomění si teorie a správných postupů, uvědomění si nedodržení doporučení, nerespektování pravidel dávaných žákům

Vztah k ICT

***Vztah k učitelství* (řazení):** tendence vystupovat jako příkladný učitel, pocit učitele o nutnosti zájmu o trendy ICT, aprobovaný učitel, nepedagog, neaprobovaný učitel, dlouhá praxe jako výhoda, učitel ICT dobrovolně, neaprobovanost není hendikep, víra ve vliv VŠ výuky, neaprobovanost jako hendikep, učitel ICT z nouze, učitel ICT z donucení

Vztah k PC: digitální imigrant, měnění potřeb v čase, nesprávce školní sítě, správce školní sítě, nesprávce svého PC, nízké používání internetu, omezená online komunikace, PC jako pracovní nástroj, používání mnoha internetových služeb, správce od píky, váznoucí komunikace přes ICT, aktivní zkoumání možností služby, zájem o trendy

Vztah k rozhovoru: apriori podceňování se, apriorní dojem stejný jako konečný, nepochopení zadání, nepřesná terminologie, rozhovor jako zajímavé popovídání, vyhýbavá odpověď

důraz na uživatelské použití IT, doplnění znalostí kvůli výuce, pocit tajemného světa IT

Znaky nebezpečí

až po pročtení e-mailu, jazyk e-mailu, nesprávně fungující PC, nevyžádanost e-mailu, neznámá osoba, příloha e-mailu, pop-up okna, SMART, styl e-mailu, technický znak, text e-mailu, varování systému, opakovaná žádost o přátelství, velký síťový provoz

Příloha E: Seznam analytických poznámek sloužících pro tvorbu kostry analytického příběhu

1. Učitel, který spravuje počítačovou učebnu, se poučí nejen ze svých chyb, ale i z chyb ostatních, jestliže musí řešit následky
   Potvrzeno
   Zakotveno: MO#58, KL#27, BK#25, BK#60, JT#58

~~2. Nepotvrzeno~~

3. U učitele se kvůli nedostatku znalostí projevuje obava, jestli je něco bezpečné. Jestliže tedy nemá dostatečné znalosti, chová se intuitivně a je raději opatrnější. Když chybí jedno -> projevuje se druhé
   Potvrzeno
   Zakotveno (škrt: nezřejmé nedostat. znal.): RI#75, RI#77, ~~BK#10~~, ~~HL#75~~
   Opak: Mail od známého: KZ#23, RZ#14, (ML#9), (RI)#27

4. Cirkularita: Silné heslo je zapomenuto, učitel prodělá negativní zkušenost a poučí se, že ochranu opustí
   Potvrzeno
   K. způsob ochrany -> Negativum ochrany -> Vnější vliv -> Reakce -> K. způsob ochrany
   Zakotveno: KZ#186, RI#129

5. Na základě negativní zkušenosti nebo názoru druhého začne učitel vnímat nějaký jev jako překážku ochrany
   Potvrzeno
   Vnější vliv -> Překážka
   Možná podobné jako 10
   Zakotveno: RI#153, HL#120, JM#38

6. U učitele se projevuje obava z nějaké hrozby na základě negativní zkušenosti. Může jít o obavu z, strach z, nedůvěru před, opatrnost před...
   Potvrzeno
   Zkušenost -> Poučení -> Obava -> K. způsob ochrany
   Zakotveno: ML#170, VF#156, HL#120, HL#102, HL#154, KL#27, JM#38, KZ#112
   Opak: PL#307, PL#310, PL#50, PL#209

7. Učitel zkouší novou službu, aby dokázal udržet tempo s dobou. Projevuje se pocit učitele, že by se měl zajímat o nové trendy
   Potvrzeno
   Zakotveno: JM#30, HL#96, JT#25

8. Učitel kritizuje chování druhých z pohledu správce sítě – má práci navíc
   Potvrzeno
   Střet správce (JT#15) vs. učitel (PL#328)
   Zakotveno: MC, MO, KL, JT#54

9. Negativní zkušenost se může projevit do Procesu zlepšování znalostí, ale nemusí. Záleží na dalších podmínkách (např. osobnost jedince, síla negativní zkušenosti, pocit viny za situaci)
   Potvrzeno
   Neprojevení se negativní zkuš. zakotveno: KZ#60, KL#32, PL#206, PL#204

10. Učitel sice mluví o pravidlech, ale zároveň přiznává, že se podle nich nechová
    Potvrzeno
    Zakotveno: KC#7, KC#97, KC#107, KC#125, ML#89, ML#158, VC#16, VF#36, VF#78, VF#128, VF#135, VF#156, VF#188, KL#117, HL#148, PL#177
    Spekulace: Učitel používá poznámku o pravidlech jako omluvu, že sám se podle nich nechová nebo si „sype popel na hlavu“. Zřejmě naznačuje, že je o problematice teoreticky dobře seznámen.
    U VF proto, že chce ukázat rozpor; nebo chce ukázat, že se v tom vyzná; možná chce ukázat výzkumníkovi, že je kompetentní to učit
    Vztah k 24

11. Bezpečnostní pravidla učitelům slouží jako reflexe, jak by se měli chovat a jak se chovají ve skutečnosti. Pravidla je neomezují, spíše inspirují.
    Poznámka

12. Vztah k ICT ovlivňuje nejen Konkrétní způsoby ochrany, ale také např. Vnější vlivy na chování. Myšlenka k ověření: Neaprobovaný učitel se mnohem více musí vzdělávat sám
    Spekulace

13. Některý učitel má zájem o problematiku, ale nemá příležitost své otázky s kým konzultovat. Diskuze s odborníkem může tento stav zlepšit
    Poznámka
    Podobné s 46
    Zakotven zájem o vysvětlení od výzkumníka: MC#103, MO#32, HL#73, RI#177
    Ukázka v praxi: KL#149

14. Některý učitel sdílí obavu US učitelských organizací, které se obávají o zneužití dat, která se týkají učitelů, na SNS žáky
    Potvrzeno
    Zakotveno: HL#102, RI#105 (částečně)
    Opak: PL#135

15. Učitel přenáší zkušenosti z výuky a z problémů řešených se žáky nebo kolegy i na své vlastní chování.
    Potvrzeno
    Podobné s 49
    Zakotveno: MC#16 (bez poučení), ML#170, RI#129, HL#152

16. Učitel zná doporučení, ale protože se nesetkal s negativním jevem, doporučení nedodržuje
    Potvrzeno
    Zakotveno: VF#78, VF#128, VF#136, KL#117, HL#148 (neg. zkušenost částečně), KC#8, KC#10, KC#107, KC#97 (částečná negativní přenesená zkušenost), ML#158 (částečná negativní přenesená zkušenost), ML#89, VC#16 (částečná negativní osobní zkušenost byla), VF#36 (částečná negativní zkušenost jako správce byla), VF#156 (negativní zkušenost byla, ale ne přímo u tohoto)
    Opak (tj. po negativní zkušenosti změna návyku): KL#101, VF#156 (na pomezí), MO#58, MO#72, RZ#192 (předtím není jistá znalost doporučení), RZ#196 (předtím není jistá znalost doporučení)
    Závěr: Podle KL#101, RZ#192 lze soudit, že funguje. Byl by však třeba experiment

17. Učitel, který má nějakou (relativně pevnou) zásadu, kritizuje druhé, že oni ji nedodržují
Potvrzeno
```
Zakotveno: KZ#168, KC#73, MC#94, RZ#172, VF#100, VF#102, MO#38, MO#58,
  KL#4, RI#155, BK#6, HL#39, ML#115, ML#87, ML#89, ML#174
```

18. Pokud učitelé hodnotí druhé, hodnotí je jako nekompetentní.
Potvrzeno
```
Zakotveno: kód Kritika chování druhých
Opak: VF#100, JT#27
```

19. Učitel kritizuje chování druhých na základě projekce svého já (P – obava o soukromí, opatrnost vůči žákům...) i na základě vnějších vlivů (V – sám už to negativum prožil)
Potvrzeno
```
Zakotveno-P: KC#73, ML#115, ML#89, ML#87, RZ#118, RZ#172, BK#6
Zakotveno-V: MC#94, MO#38, MO#58, RI#155, HL#39
Zakotveno-PV: KZ#168
Nerozhodnuto: ML#174, VF#100, VF#102, KL#4
```
Vypsány pouze některé kódy; podobné s 68

20. Učitel se snaží chovat bezpečně, má své ideální zásady. Existují však Překážky ochrany, které jeho chování mění. Učitel patrně řeší dilema, jak být v bezpečí a zároveň efektivně užívat ICT. Jestliže se chce nadále "silně" chránit, vznikne Negativum ochrany a na to musí reagovat – buď se s tím smířit, nebo návyk opustit.
Potvrzeno
```
Zakotveno-smíření: ML#150, BK#132, PL#179, ML#162, VF#57, HL#178, RI#79
Zakotveno-upuštění: KZ#186, KC#125, KL#99, HL#164, JT#60
```
Mimo důvěry ve známé – viz 22
Celkem dobře to vystihují registrace (ač je to hypotetická situace) – zde byl požadavek na opuštění ochrany (tj. zadat požadovaná data). Zjišťovali jsme přitom, jak budou učitelé reagovat.

21. Učitel na základě nějakého znaku nebezpečí zpozorní a reaguje určitým typem obrany (smazání e-mailu, ověření informace, formát HDD...)
Potvrzeno
```
Zakotveno: kódy Znaky nebezpečí (vyjma níže uvedených)
Rozhodování: KZ#12, MC#52 (AV kontrola), VF#61, VF#53, HL#15, RI#37
Opak: KC#8
```

22. Učitel důvěřuje známým osobám a věří v absenci rizika, ačkoliv si všiml rizikového znaku
Potvrzeno
```
Zakotveno: KZ#24(exe), KC#8(exe), ML#9(exe), RZ#14(exe), RI&27(exe)
Opak: VC#10(exe), KL#23(exe)
Testy: MC#46(exe), VF#06(exe), MO#19(exe), PL#22(exe), BK#19(exe)
```

23. Učitel může znát doporučení, ale aby jej začal dodržovat, musí mít pocit, že je to ziskové oproti souvisejícím omezením
Spekulace, kterou potvrzuje 42
```
KC a hesla #97: Přečetla, uznala důvody -> upravila jednání
VF: nedodržuje, protože to není tak závažné (cennost dat), aby se tak
  silně chránil -> dělá vědomý kompromis mezi ideálem a překážkami. VF
  říká, že zná, aby ukázal rozpor; nebo ukázal, že se v tom vyzná; nebo
  ukázal výzkumníkovi, že je kompetentní to učit.
```
Nutno nejen teoreticky učit, ale také přesvědčit, že má smysl se chránit. Podle toho uzpůsobit výuku – zážitková metoda, negativní příklady atd.

24. Aprobovaní učitelé se o pravidlech zmiňují, byť přiznávají, že je nerespektují. NEaprobovaní učitelé se o pravidlech zmiňují málo
    Potvrzeno
    Počet výskytů kategorie – aprobovaní: KC:9, ML:3, VF:19, PL:3
    Počet výskytů kategorie – neaprobovaní: KZ:0, MC:1, RZ:0, VC:2, MO:5, KL:2, RI:0, BK:0, HL:1, JM:1, JT:4

25. Zdá se, že existují 2 navzájem kolmé škály: znalost pravidel a reálné chování. Pak se každý učitel zařadí do jedné ze čtyř oblastí dle jednotlivých kvadrantů
    Potvrzeno
    Toto rozcestník:
    - Zná, ale nedodržuje viz 16
    - Nezná, ale chová se v jejich duchu viz 30
    - Zná a dodržuje např. MO#80, JT#40 a další
    - Nezdá a nedodržuje např. RZ#20, KZ#138

26. Učitel volí v případě napadení malware "černobílá" řešení.
    Potvrzeno
    Zakotveno: KC, KZ, ML#21, VC#24
    Opak: MO, MC (částečně), PL
    Podobné s 22

27. Některý učitel těžko rozeznává jemné rozdíly v zadání a trvá na svém výkladu problému
    Potvrzeno
    Zakotveno: KZ#67, KZ#16, KZ#212, VC#4, RI#57

28. Učitel dlouhodobě vystavený náhodnému přijímání informací je začíná odmítat
    Potvrzeno
    Zakotveno: KZ#100, ML#71, RZ#108
    Jiný důvod: RI#87 (čas)

29. Učitel má pocit, že jeho data (e-mail, Facebook, informační systém školy) nejsou citlivá, a tudíž bezpečnost hesel a zálohování "moc neřeší"
    Potvrzeno
    Zakotveno: KZ#188, KZ#202, VC#61, KL#125 (web ČŠI), RI#31, RI#59-63, RI#139, RI#145 (částečně), RI#157, BK#96, BK#104

30. Učitel, který neprošel žádným vzděláním, nezná teorii, poučky a nezažil negativní zkušenost, jedná intuitivně.
    Potvrzeno
    Zakotveno: KZ#230, MC#140, MC#222, VC#135, VC#145
    Poznámka: Nikde nejsou vnitřní ani vnější vlivy. Je jejich chování bezpečné?
    Poznámka: Toto jako jedna z dimenzí k pravidlům

31. Neaprobovaného učitele ICT a jeho znalosti značně ovlivňuje, nakolik má tuto problematiku učit.
    Potvrzeno částečně
    Zakotveno: KZ#6, KZ#232, RZ#210
    Opak: KC#2, KC#125
    Spekulace: (Neaprobovaného) Učitele na počátku kariéry učitele ICT ovlivňuje, nakolik má problematiku učit. Postupem času může získat hlubší znalosti – záleží na zájmu, správcování sítě atd.

32. Některý učitel se pro naplnění svých potřeb vystavuje nebezpečí. Bylo by možné eliminovat pomocí virtuálního počítače?
    Potvrzeno
    Zakotveno: VC#16, MO#52, RI#33, PL#26
    Prověřený zdroj jako kompromis: ML#21, VF#32, JM#8

33. Reakce učitelů po rozhovoru na nově získané znalosti
    Sonda
    Obohacení: MC (zajímavé povídání + nové info), RZ (nové info), VC (nové info), VF (nové info), PL (zajímavé povídání)
    Bez reakce (otázka na názor odbornosti po rozhovoru byla): KC, KL, RI
    Učitelova aktivita získat nové info viz 13

34. Některý učitel chápe řešení malware jako rutinní záležitost.
    Potvrzeno
    Zakotveno: VC#42 (napůl), MO#66, PL#50
    Obava z malware: KC#20, RZ#28, KL#27, VF#63 (napůl)

35. Učitel díky příchodu do praxe zlepšuje své návyky a znalosti, to průběžně pokračuje
    Potvrzeno
    Zakotveno: KZ#206, KC#101, HL#29 (částečně)
    Průběžně kvůli výuce: RI#159, HL#23, JT#60, VF#80, VF#192, JT#25 (trendy)
    Opak: RZ#210 (částečně), PL#324

36. U některých učitelů se objevuje kód Odmítání pasivního přijetí informací (v hoaxu).
    Potvrzeno
    Zakotveno: KZ#100, VC#94, KL#56
    Opak: KC#63, HL#81, JM#54, PL#69
    Aprobovaní více ověřují, neaprobovaní spíše odmítají

37. Někteří učitelé odmítají cloudu svěřovat svá data nebo zde zálohují dokumenty, které nepovažují za citlivé. Naopak fotografie odmítají cloudu svěřovat
    Potvrzeno
    Zakotveno: ML#198, PL#248, KC#115
    Důležité dokumenty: VF#156
    Opak: RZ#192 (mail, ale co?), MO#183, RI#149 (školní foto)

38. Některý učitel na SNS zveřejňuje jen věci, které se o něm ví i offline – uvědomuje si, že se to může donést žákům
    Potvrzeno
    Zakotveno: KZ#170 (částečně; není vliv žáků), ML#97, ML#101, HL#102, JM#36 (není vliv žáků), JT#21 (pracovní profil)
    Obdoba: RI#105 (nemá žáky, protože přátelé nefiltrují příspěvky)
    Opak: PL#89 (má žáky a publikuje)

39. Učitel má nějaký návyk, který se naučil a ten nemění. Uvědomuje si, že existuje i lepší postup, ale je konzervativní
    Potvrzeno
    Zakotveno: VF#78, VF#36
    Souvisí s bezpečnostními pravidly (viz 23) – zde je způsob ochrany, ne četnost hesel, absence ochrany, chybné rozhodnutí atd.
    Toto doplněk k 42, že je i v rovině způsobu ochrany

40. Učitel začne hledat lepší řešení, když původní postup zklame – prodělá nějakou negativní zkušenost. Tato změna návyků však nemusí proběhnout vždy
    Potvrzeno
    Zakotveno: KL#115 (hypoteticky), PL#256 (hypoteticky), MC#103 (netrápí -> neřeší), KZ#186 (opuštění ochrany), KZ#168, ML#51, RZ#32, RZ#192, RZ#196, VF#63, MO#72, KL#101, KL#121 (částečně), RI#33, RI#73, RI#155, HL#110 (nebyla negativní zkušenost, ale strach z ní), HL#180, JT#54 (vysvětlení), PL#121, PL#240
    Překážka ochrany -> Způsob ochrany -> Negativní zkušenost -> Poučení -> Nový způsob ochrany
    Neprojevení se negativní zkušenosti – viz 9

41. Učitel odmítá přátelení se žáky na SNS z důvodu obavy o ztrátu autority, odhalování sama sebe před žáky. Pokud žáci odejdou ze školy, učitel žádosti možná začne přijímat
    Potvrzeno
    Odmítání kvůli autoritě / odstupu: **KC#73**, MC#144, RZ#122, VC#116, **VF#108**, **RI#105**, HL#98 (vůbec nemít SNS)
    Přátelení s exžáky: KZ#150, **KC#73**, **VF#108**, **RI#99**

42. Učitel zná ideální stav, jak by mělo chování vypadat. Ovšem zda bude tato doporučení respektovat, záleží na tom, zda ho nebudou moc omezovat.
    Potvrzeno
    Zakotveno (přeškrtnuto = není zřejmá překážka): VF#128 (délka hesel), ~~KL#117 (četnost záloh)~~, ~~HL#148 (obměna hesel)~~, KC#8 (spuštění rizik. souboru), KC#107 (četnost záloh), ~~KC#97 (typ hesla)~~, ML#158 (obměna hesel), ML#89 (žáci na FB), VC#16 (navštěvování rizik. stránek), VF#36 (aplikace na zkoušku), VF#136 (obměna hesel), PL#177 (množství hesel)
    Souvisí s 23; omezení zejména Překážky ochrany (vnitřní)

43. Tento učitel se (stejně jako MO) aktivně stará o počítačovou síť školy a je pomocníkem externího správce sítě. Rozdíl oproti MC, VC, kteří – ač jsou hlavní učitelé IT na škole – takovýto přehled nemají
    Spekulace

44. Učitel má nějaké potřeby, požadavky a na jejich základě hledá vhodná řešení.
    Potvrzeno
    Zakotveno: KC#117, ML#182, ML#208, RZ#120, VC#183 (částečně), VF#84, VF#140, MO#72, KL#115, JM#26, PL#256
    Učitel je ochoten z ideálního řešení slevit – viz 23, 42

45. Příchod nové technologie může učitele ovlivnit, aby začal přemýšlet o svých potřebách. Řekne si "tohle je ono, to je řešení toho, co mne trápí" a začne to používat
    Potvrzeno částečně
    Zakotveno: VF#178
    Doplněk k 13, 46 – platí to nejen o postupech, ale i technologiích

46. Pro učitele ICT je výhodné mít známého odborníka na ICT, který ho může informovat o odborných záležitostech. Nejen mu poradit, pomoci v nouzi, ale i spolupracovat.
    Potvrzeno
    Funkční příklady: KL#145, KL#149, HL#17, HL#21
    Pomoc v nouzi: MC#92, ML#35, RZ#42
    Podobné s 13. Motivace pro spolupráci ITE a ITu.

47. Vnitřní motivací pro studium problematiky (a tedy zlepšení znalostí) je zájem o obor, který může být osobní nebo profesní (jako učitel či jako správce)
Potvrzeno
Zájem jako učitel (nad rámec „osnov"): VF#18, VF#188, VF#192, RI#159 (obecně ICT), HL#96, JM#30, JT#25, KL#149, HL#23, JT#60
Zájem osobní: JM#6, HL#23, JT#60 (ICT obecně)
Zájem nerozlišený: HL#59, MO#32, MC#103, HL#73, VC#218, KC#32, BK#180 (obecně ICT), JT#62 (obecně ICT)
Opak: RZ#8
Není řešen zájem kvůli „základní" výuce – viz kód aktivní samostudium apod.

48. Jestliže přínos ochrany v očích učitele překoná překážky, učitel se začne lépe chránit. Viděný přínos se může zvýšit po negativní zkušenosti.
Neboli: Jestliže učitel prodělá negativní zkušenost, začne se lépe chránit. Vidí totiž, že ochrana má smysl.
Potvrzeno
Zakotveno s překážkou: KL#121
Zakotveno bez zřejmé překážky: KL#101, RZ#196
Podobné (stejné) s 23, 40

49. Učitel jako odborník a jako pedagog jsou dvě strany stejné mince. Svou znalost (zejména zajímavostí, novinek) učitel dává do výuky a naopak, zkušenostmi z výuky učitel obohacuje své odborné dovednosti.
Potvrzeno
Zakotveno Odbornost -> Výuka: KL#149, HL#59
Výuka, práce -> Odbornost: KC#100 (z učebnice), ML#170, RI#129, BK#60 (jako správce), HL#152, PL#83, MC#94, MO#72 (částečně; přenos domů)
Podobné s 15

50. Tento neaprobovaný učitel žádá o pomoc členy rodiny, kteří ač nejsou IT odborníci, jsou v problematice zběhlejší. Nechce se ale učit s nástrojem zacházet
Ojedinělý případ
Zakotveno: VC#106
Pouze ojedinělý případ, ale ukázka, že to také existuje

~~51. Poznámka~~

52. Učitel volí sílu ochrany podle citlivost dat, který chrání. Protipólem k citlivosti dat je pohodlnost pro zadávání a zapamatování.
Potvrzeno
Cennost / citlivost zakotvena (přeškrtnuto = není zřejmá překážka): KZ#202, VF#172 (částečně), ~~RI#33~~, ~~RI#151~~, ~~PL#272~~, KC#79, MC#172, MC#184, ~~MC#192~~, ML#140, ~~VC#127~~, VC#169, VF#132, ~~KL#125~~, ~~JT#40~~
Více viz 23, 29, 42

53. Některý Učitel se o problematice dozvídá ze zdrojů pro širokou veřejnost.
Potvrzeno
Zakotveno (přeškrtnuto = doporučení komunity): RI#35 (Facebook), ~~KZ#116 (komunita)~~, ~~VF#120 (komunita)~~, PL#77 (komunita), PL#163 (komunita), ~~PL#211 (komunita)~~, VC#200 (systém), RI#35 (systém), RI#137 (systém), MO#169 (média), KL#8 (média), RI#11 (média), RI#35 (média), RI#93 (média), RI#159 (média), HL#55 (média), HL#31 (média), JM#42 (média)
Spekulace: Aprobovaný učitel využívá oficiálních zdrojů

54. Některý učitel se snaží získat o praktických problémech co nejvíce informací, má snahu se doptávat na řešení. Velký rozdíl oproti ostatním, kteří PC svěří do servisu nebo předají fyzicky někomu jinému

Potvrzeno

Doptávači: MC#86, VC#48, MO#257 (částečně), MO#261, KL#19, JM#18, JM#22, PL#287, MC#72, KL#74, HL#51 (částečně), RI#35 (částečně), MC#90, PL#36, PL#283, PL#302, MC#92, PL#40

Předávači (tučně uživ. Problémy, které lze řešit / zkusit řešit): **VC#26**, MO#90 (Linux), MO#209 (server), **(KL#19)**, KL#101 (disk), **RI#37**, **RI#39**, **RI#41**, **RI#43**, **HL#35**, **HL#49**, **HL#51**, HL#176, PL#302, **ML#31**, **ML#35**, **RZ#40**, **RZ#42**, **BK#52** (částečně), **KZ#38**

55. Ačkoliv se ICT bezpečnost na vysoké škole (zřejmě) explicitně neučí, aprobovaní učitelé mají jakési IT myšlení, které jim dává možnost se chránit. Zároveň získají mnoho informací při studiu "náhodou"

Spekulace

Neboli: Pokud se aprobovaní liší, není to díky explicitnímu vzdělání (pak je možné, že je to díky zájmu o obor atd.)

56. Učitel na základě negativní zkušenosti se může začít chovat bezpečněji nebo vzroste jeho povědomí o dané oblasti, jeho znalosti, když hledá řešení. Nebo je zklamán, nebo nic... Navíc se může projevit ve vnitřní vlivy.

Potvrzeno

Toto rozcestník

Bezpečnější chování: viz 40; zakotveno (tučně osobní): **KZ#114**, **MC#94**, ML#39, ML#204, **ML#51**, ML#23, **RZ#28**, RZ#168, RZ#172, **RZ#192**, **RZ#32**, **RZ#196**, **VF#156**, **VF#63**, **MO#58**, **MO#72**, **KL#101**, **KL#121**, **RI#73**, **RI#155**, **BK#25**, HL#55, **HL#111**, HL#153, **HL#180**, **JM#24**, **JM#38**, **JT#58**, PL#83, **PL#121**, **PL#240**

Vyšší povědomí – viz 62

Projekce do vnitřních vlivů – viz 6, 69

Zklamání zakotveno: HL#108, PL#105

Nic zakotveno: KZ#60, KL#27 (zde obava), PL#204

Možno využít při výuce – learning by doing

57. Zatímco někteří učitelé reagují na znak nebezpečí nějakou akcí, jiní znak nebezpečí ignorují.

Potvrzeno

Akce zakotvena: KC#35, VF#65, VF#67, KL#44, RI#27, PL#75, ML#15, KZ#32, KC#6, KC#18, MC#41, MC#52 (částečně), ML#17, ML#61, RZ#12, VC#12, VF#4, VF#6, KL#60, KL#20, BK#17, PL#83, RI#33, RZ#24, VF#53, VF#180, JT#54, HL#43, ML#2, VC#2, VF#4, VF#51, MO#14, KL#23, RI#14, HL#15, JM#2, JT#15, PL#18, KZ#62, KZ#100, KC#18, ML#41, ML#65, RZ#61, KL#50, RI#87, RI#95, JM#44

Ignorování zakotveno (přeškrtnuto = zvažování): ~~VF#53~~, ~~RI#37~~, ~~VF#61~~, KZ#12, KC#8, ~~HL#15~~

V seznamu „zvažování / ignorování" chybí učitelé MO, **KL**, JT, **PL**, VC, BK, JM. Tučně označení v seznamu „akce" vícekrát

Toto jako výpis k 21

Poznámka: Asi nelze podle tohoto klasifikovat – hranice velice neostré

58. Některý učitel zadává při registraci pravdivé informace, pokud je to kontrolováno nebo je na to vázána další činnost (zaslání objednávky na adresu). Jestliže údaje nelze ověřit, zadává smyšlené.
Potvrzeno
Zakotveno: VC#75 (e-mail), VC#77, (e-mail), VC#81 (e-mail), MO#124 (e-mail), JM#48 (adresa)
Opak (nechce lhát): JM#50 (adresa), PL#171 (adresa), KC#47, RZ#77, RI#79, BK#202, MC#148, ML#127, VF#120

59. Některý učitel je ochoten se s náročným problémem malware zabývat sám
Potvrzeno
Zakotveno (tučně situace jiné než teoretické situace): **PL#36**, PL#40, **PL#283**, MC#88, **VC#34**, **VC#179**, KC#22, **MO#213**, **RI#37**, **MC#72**, **BK#24**, **MO#10**, **KL#27**, **JT#54**, KZ#48, **KL#19**
Opak (tj. předávači): ML#31, RZ#40, KZ#38, HL#49, RI#37, (VC#26), BK#52, (KL#19)
Shrnutí – Řešitelé malware: PL, MC, VC, (KC), MO, BK, KL, (RI), (KZ)
Shrnutí – Předávači: ML, RZ, HL, (KZ), (RI), (VC), (BK)
Částečně viz 62 a 54; toto vhodné pro klasifikaci učitelů

~~60. Poznámka~~

61. Některý učitel chce o obsahu SNS spojeném s jeho osobou rozhodovat sám a kriticky, nikoliv to nechat na druhých
Potvrzeno částečně
Zakotveno: JT#10, PL#91 (řídí informace, je-li nutné)
Opak: RI#105 (částečně), PL#93 (řídí informace, je-li nutné)

62. Tento učitel se učí díky řešení problémů, tj. na základě negativních zkušeností. Pokud je nějaký problém, snaží se ho vyřešit a tím se stává schopnějším nebo znalejším rizik
Potvrzeno
Zakotveno: PL#308, MC#72, RI#123, HL#14, HL#120, PL#281, JM#60 (částečně)

63. Učitel použije měkké opatření, a pokud by selhalo, sáhne k razantnějšímu
Potvrzeno
Zakotveno (hledání méně nákladných metod): KZ#48 (vir), MC#86 (vir), MO#66 (částečně; vir), PL#36 (vir), PL#17 (mail)
Přímo silné opatření: BK#76 (mail), JT#14 (mail), KC#22 (vir), VC#24 (vir)
Jen slabé opatření (nemají důležitá data -> neřeší): VC#61 (mail), RI#63 (mail)
Hledání v mailu od sebe sama a v problematice malware

64. Učitel začne rozpoznávat nebezpečí kromě jiného na základě dřívější negativní zkušenosti.
Potvrzeno
Zakotveno: PL#83, RI#33, JT#54
Ano, ale těch důvodů může být více (vrozená nedůvěra, poznatky z vnějšku)

65. U (tohoto) učitele se překážky ochrany vztahují také na vnější vlivy, kdy něco brání co nejefektivněji využívat vnější zdroje
Viz vnější překážky ochrany
Podobné s 23, 42

66. Tento učitel se nechá inspirovat názory druhých, nehledá oficiální zdroje, ale komunitní zdroje.
Potvrzeno
Zakotveno (tučně hoax): **PL#71**, **PL#73**, KZ#116, VF#120, **PL#77**, PL#163, PL#211
Opak (vše hoax): KZ#106 (částečně), MC#108, VC#98, KL#60

67. Tento uživatel požaduje ucelený balíček informací o určitém tématu – možný námět na školení učitelů
Připomínka

68. Učitel, který prožil negativní zkušenost, způsob ochrany začne prosazovat i u okolí
Potvrzeno
Zakotveno: MO#78, JM#56 (částečně – hoax), JT#8
Jiný důvod: VF#156, MO#187, JT#30
Podobné s 19, kde pasivně kritizuje. Zde aktivně radí / pomáhá

69. U učitele se negativní zkušenost projevuje ve vnitřní vlivy.
Potvrzeno
Zakotveno opatrnost: ML#168, RZ#168, VF#156 (částečně), HL#102, HL#154, JM#38 (částečně), JT#58
Zakotveno nedůvěřivost: KZ#112, HL#120
Zakotveno strach: KL#25
Podobné s 6

Příloha F: Formulář dotazníku sémantického diferenciálu

DOTAZNÍK
Sémantický diferenciál - SD

Pokyny k vyplnění:

Tento test je jistou formou hry se slovy a pocity, které ve Vás tato slova vzbuzují.
Na následujících stránkách najdete celkem 15 slov. U těchto slov je uvedeno 12 dvojic protikladných slov se sedmi prázdnými kolečky mezi nimi. U jednotlivých dvojic vybarvěte vždy jedno z těchto sedmi koleček podle toho, jak vám slovo připadá.

Chléb

tvrdý ● ○ ○ ○ ○ ○ ○ měkký

Nepřemýšlejte dlouho o jednotlivých slovech a párech, ale odpovídejte pokud možno spontánně. Je důležité, abyste nic nevynechali. Ani jeden pár slov. Nejsou žádné správné a nesprávné odpovědi. Pokud máte pocit, že škála nesouvisí se hodnoceným slovem, pak vyplňte škálu podle okamžitého dojmu nebo pocitu, který získáte a odhadněte, jak škálu vyplnit.

Pokud jste omylem označili nevhodnou odpověď a chcete se opravit, výrazně přeškrtněte chybnou odpověď a označte vybarvením odpověď správnou.

Chléb

tvrdý ⊗ ○ ○ ○ ● ○ ○ měkký

Vzhledem k tomu, že tento dotazník budete vyplňovat ještě na konci kurzu a je potřeba párovat tyto dotazníky je vyplněno číslo. Výsledky testu povedou posléze ke zkvalitnění výuky, nikoliv k Vašemu hodnocení. Po spárování budou dotazníky vyhodnocovány naprosto anonymně.

Př.:

UČO
68001

Pohlaví

M ○

Ž ○

Studijní skupina	UČO
S	

Dotazník SEMDIF ○ ○ ○ ● ○ verze: 2

Znalost

Užitečný	○	○	○	○	○	○	○	Neužitečný
Tlustý	○	○	○	○	○	○	○	Tenký
Rychlý	○	○	○	○	○	○	○	Pomalý
Jednoduchý	○	○	○	○	○	○	○	Složitý
Silný	○	○	○	○	○	○	○	Slabý
Aktivní	○	○	○	○	○	○	○	Pasivní
Nezbytný	○	○	○	○	○	○	○	Zbytečný
Těžký	○	○	○	○	○	○	○	Lehký
Statický	○	○	○	○	○	○	○	Dynamický
Dobrý	○	○	○	○	○	○	○	Špatný
Problémový	○	○	○	○	○	○	○	Bezproblémový
Horký	○	○	○	○	○	○	○	Studený

Zálohování

Užitečný	○	○	○	○	○	○	○	Neužitečný
Tlustý	○	○	○	○	○	○	○	Tenký
Rychlý	○	○	○	○	○	○	○	Pomalý
Jednoduchý	○	○	○	○	○	○	○	Složitý
Silný	○	○	○	○	○	○	○	Slabý
Aktivní	○	○	○	○	○	○	○	Pasivní
Nezbytný	○	○	○	○	○	○	○	Zbytečný
Těžký	○	○	○	○	○	○	○	Lehký
Statický	○	○	○	○	○	○	○	Dynamický
Dobrý	○	○	○	○	○	○	○	Špatný
Problémový	○	○	○	○	○	○	○	Bezproblémový
Horký	○	○	○	○	○	○	○	Studený

Učitel

Užitečný	○	○	○	○	○	○	○	Neužitečný
Tlustý	○	○	○	○	○	○	○	Tenký
Rychlý	○	○	○	○	○	○	○	Pomalý
Jednoduchý	○	○	○	○	○	○	○	Složitý
Silný	○	○	○	○	○	○	○	Slabý
Aktivní	○	○	○	○	○	○	○	Pasivní
Nezbytný	○	○	○	○	○	○	○	Zbytečný
Těžký	○	○	○	○	○	○	○	Lehký
Statický	○	○	○	○	○	○	○	Dynamický
Dobrý	○	○	○	○	○	○	○	Špatný
Problémový	○	○	○	○	○	○	○	Bezproblémový
Horký	○	○	○	○	○	○	○	Studený

Ulož.to

Užitečný	○	○	○	○	○	○	○	Neužitečný
Tlustý	○	○	○	○	○	○	○	Tenký
Rychlý	○	○	○	○	○	○	○	Pomalý
Jednoduchý	○	○	○	○	○	○	○	Složitý
Silný	○	○	○	○	○	○	○	Slabý
Aktivní	○	○	○	○	○	○	○	Pasivní
Nezbytný	○	○	○	○	○	○	○	Zbytečný
Těžký	○	○	○	○	○	○	○	Lehký
Statický	○	○	○	○	○	○	○	Dynamický
Dobrý	○	○	○	○	○	○	○	Špatný
Problémový	○	○	○	○	○	○	○	Bezproblémový
Horký	○	○	○	○	○	○	○	Studený

Život

Užitečný	○	○	○	○	○	○	○	Neužitečný
Tlustý	○	○	○	○	○	○	○	Tenký
Rychlý	○	○	○	○	○	○	○	Pomalý
Jednoduchý	○	○	○	○	○	○	○	Složitý
Silný	○	○	○	○	○	○	○	Slabý
Aktivní	○	○	○	○	○	○	○	Pasivní
Nezbytný	○	○	○	○	○	○	○	Zbytečný
Těžký	○	○	○	○	○	○	○	Lehký
Statický	○	○	○	○	○	○	○	Dynamický
Dobrý	○	○	○	○	○	○	○	Špatný
Problémový	○	○	○	○	○	○	○	Bezproblémový
Horký	○	○	○	○	○	○	○	Studený

UČO

Heslo

Užitečný	○	○	○	○	○	○	○	Neužitečný
Tlustý	○	○	○	○	○	○	○	Tenký
Rychlý	○	○	○	○	○	○	○	Pomalý
Jednoduchý	○	○	○	○	○	○	○	Složitý
Silný	○	○	○	○	○	○	○	Slabý
Aktivní	○	○	○	○	○	○	○	Pasivní
Nezbytný	○	○	○	○	○	○	○	Zbytečný
Těžký	○	○	○	○	○	○	○	Lehký
Statický	○	○	○	○	○	○	○	Dynamický
Dobrý	○	○	○	○	○	○	○	Špatný
Problémový	○	○	○	○	○	○	○	Bezproblémový
Horký	○	○	○	○	○	○	○	Studený

Facebook

Užitečný	○	○	○	○	○	○	○	Neužitečný
Tlustý	○	○	○	○	○	○	○	Tenký
Rychlý	○	○	○	○	○	○	○	Pomalý
Jednoduchý	○	○	○	○	○	○	○	Složitý
Silný	○	○	○	○	○	○	○	Slabý
Aktivní	○	○	○	○	○	○	○	Pasivní
Nezbytný	○	○	○	○	○	○	○	Zbytečný
Těžký	○	○	○	○	○	○	○	Lehký
Statický	○	○	○	○	○	○	○	Dynamický
Dobrý	○	○	○	○	○	○	○	Špatný
Problémový	○	○	○	○	○	○	○	Bezproblémový
Horký	○	○	○	○	○	○	○	Studený

Soukromí

Užitečný	○	○	○	○	○	○	○	Neužitečný
Tlustý	○	○	○	○	○	○	○	Tenký
Rychlý	○	○	○	○	○	○	○	Pomalý
Jednoduchý	○	○	○	○	○	○	○	Složitý
Silný	○	○	○	○	○	○	○	Slabý
Aktivní	○	○	○	○	○	○	○	Pasivní
Nezbytný	○	○	○	○	○	○	○	Zbytečný
Těžký	○	○	○	○	○	○	○	Lehký
Statický	○	○	○	○	○	○	○	Dynamický
Dobrý	○	○	○	○	○	○	○	Špatný
Problémový	○	○	○	○	○	○	○	Bezproblémový
Horký	○	○	○	○	○	○	○	Studený

Ztráta

Užitečný	○	○	○	○	○	○	○	Neužitečný
Tlustý	○	○	○	○	○	○	○	Tenký
Rychlý	○	○	○	○	○	○	○	Pomalý
Jednoduchý	○	○	○	○	○	○	○	Složitý
Silný	○	○	○	○	○	○	○	Slabý
Aktivní	○	○	○	○	○	○	○	Pasivní
Nezbytný	○	○	○	○	○	○	○	Zbytečný
Těžký	○	○	○	○	○	○	○	Lehký
Statický	○	○	○	○	○	○	○	Dynamický
Dobrý	○	○	○	○	○	○	○	Špatný
Problémový	○	○	○	○	○	○	○	Bezproblémový
Horký	○	○	○	○	○	○	○	Studený

Email

Užitečný	○	○	○	○	○	○	○	Neužitečný
Tlustý	○	○	○	○	○	○	○	Tenký
Rychlý	○	○	○	○	○	○	○	Pomalý
Jednoduchý	○	○	○	○	○	○	○	Složitý
Silný	○	○	○	○	○	○	○	Slabý
Aktivní	○	○	○	○	○	○	○	Pasivní
Nezbytný	○	○	○	○	○	○	○	Zbytečný
Těžký	○	○	○	○	○	○	○	Lehký
Statický	○	○	○	○	○	○	○	Dynamický
Dobrý	○	○	○	○	○	○	○	Špatný
Problémový	○	○	○	○	○	○	○	Bezproblémový
Horký	○	○	○	○	○	○	○	Studený

UČO

Vir

Užitečný	○	○	○	○	○	○	○	Neužitečný
Tlustý	○	○	○	○	○	○	○	Tenký
Rychlý	○	○	○	○	○	○	○	Pomalý
Jednoduchý	○	○	○	○	○	○	○	Složitý
Silný	○	○	○	○	○	○	○	Slabý
Aktivní	○	○	○	○	○	○	○	Pasivní
Nezbytný	○	○	○	○	○	○	○	Zbytečný
Těžký	○	○	○	○	○	○	○	Lehký
Statický	○	○	○	○	○	○	○	Dynamický
Dobrý	○	○	○	○	○	○	○	Špatný
Problémový	○	○	○	○	○	○	○	Bezproblémový
Horký	○	○	○	○	○	○	○	Studený

Práce

Užitečný	○	○	○	○	○	○	○	Neužitečný
Tlustý	○	○	○	○	○	○	○	Tenký
Rychlý	○	○	○	○	○	○	○	Pomalý
Jednoduchý	○	○	○	○	○	○	○	Složitý
Silný	○	○	○	○	○	○	○	Slabý
Aktivní	○	○	○	○	○	○	○	Pasivní
Nezbytný	○	○	○	○	○	○	○	Zbytečný
Těžký	○	○	○	○	○	○	○	Lehký
Statický	○	○	○	○	○	○	○	Dynamický
Dobrý	○	○	○	○	○	○	○	Špatný
Problémový	○	○	○	○	○	○	○	Bezproblémový
Horký	○	○	○	○	○	○	○	Studený

Peníze

Užitečný	○	○	○	○	○	○	○	Neužitečný
Tlustý	○	○	○	○	○	○	○	Tenký
Rychlý	○	○	○	○	○	○	○	Pomalý
Jednoduchý	○	○	○	○	○	○	○	Složitý
Silný	○	○	○	○	○	○	○	Slabý
Aktivní	○	○	○	○	○	○	○	Pasivní
Nezbytný	○	○	○	○	○	○	○	Zbytečný
Těžký	○	○	○	○	○	○	○	Lehký
Statický	○	○	○	○	○	○	○	Dynamický
Dobrý	○	○	○	○	○	○	○	Špatný
Problémový	○	○	○	○	○	○	○	Bezproblémový
Horký	○	○	○	○	○	○	○	Studený

Já

Užitečný	○	○	○	○	○	○	○	Neužitečný
Tlustý	○	○	○	○	○	○	○	Tenký
Rychlý	○	○	○	○	○	○	○	Pomalý
Jednoduchý	○	○	○	○	○	○	○	Složitý
Silný	○	○	○	○	○	○	○	Slabý
Aktivní	○	○	○	○	○	○	○	Pasivní
Nezbytný	○	○	○	○	○	○	○	Zbytečný
Těžký	○	○	○	○	○	○	○	Lehký
Statický	○	○	○	○	○	○	○	Dynamický
Dobrý	○	○	○	○	○	○	○	Špatný
Problémový	○	○	○	○	○	○	○	Bezproblémový
Horký	○	○	○	○	○	○	○	Studený

Strach

Užitečný	○	○	○	○	○	○	○	Neužitečný
Tlustý	○	○	○	○	○	○	○	Tenký
Rychlý	○	○	○	○	○	○	○	Pomalý
Jednoduchý	○	○	○	○	○	○	○	Složitý
Silný	○	○	○	○	○	○	○	Slabý
Aktivní	○	○	○	○	○	○	○	Pasivní
Nezbytný	○	○	○	○	○	○	○	Zbytečný
Těžký	○	○	○	○	○	○	○	Lehký
Statický	○	○	○	○	○	○	○	Dynamický
Dobrý	○	○	○	○	○	○	○	Špatný
Problémový	○	○	○	○	○	○	○	Bezproblémový
Horký	○	○	○	○	○	○	○	Studený

UČO

Příloha G: Hospitační zápis z pilotního nasazení výuky

Zážitková výuka

-	úvodní příběh o napadení	prezentace	30. min (spam)
facebook			
e-mail	1	2	1
zprávy	1	3	2
sport		3	3
baví se sousedem	1	1	4
mobil		6	4
video		2	1
učí se na něco jiného			1
slevomat			2
spí			1
nespecif (nevím)			2
is			
dopravní spojení			1
hry			
+			
ptají se		1	
baví se k tématu		1	
hledá k tématu			1
permanentně mimo	2-5 lidí, podle aktuálního tématu (táhnou peníze, porno,…)		
celkem lidí: cca 20			

Průběh hodiny:

studenti se mají přihlásit: "dnes to nefunguje", "to není nic těžkého to opravit", "měl jsem radost, že jsem dostal stipendium" – pedagogický konflikt
všichni okamžitě vtaženi do problému (zadali svoje RČ)
když učitel mluví o penězích ("útočníci vydělali 30mil"), jsou zaujati
spuštění prezentace a výklad k ní – pozornost upadá
tabulka e-mailů a hesel – funguje, nikdo se tam nechce najít
student sleduje videa, přeruší učitele nějakou triviální poznámkou – učitel se chytí (myslí si, že dává pozor)
interaktivní graf zaujal
rady jak zálohovat – zaujetí, možná proto, že byli nuceni zvednout ruku ti, kdo nezálohují (nepřihlásili se, že zálohují)
2. graf zaujal – životnost médií pro zálohu
1. dotaz na životnost CD (v prezentaci se tvrdí jen 3 roky)
30. min – unaveni, znuděni – vypli internet
hodina narušena autem rádia Kiss – někoho rozhodí

	promítané video – sledují všichni (kromě jedné na slevomatu – móda) "pánové, ještě chvilku, já už končím" – funguje na pány, pro ostatní signál odhlašovat se dotazy nejsou bezprostředně po hodině nikdo nediskutuje o probíraném tématu
učitel:	snaží se oživit výklad vlastními zkušenostmi a reálnými příběhy, aktualitami (má přehled) přístup s humorem frontální výuka – přednáška (98% času) přátelský přístup, nehraje si na boha ptá se občas, reagují ve směs ti samí
dojem:	studenti jsou okamžitě vtaženi do hodiny – konfrontováni se svým závěrem "dneska IS nefunguje" postupně se pozornost vytrácí přesunutí posledních řad dopředu přepnutí prezentace na interaktivní graf, video apod. je zaujme většina lidí je duchem přítomno, dává pozor

Přednáška odborníka

-	úvod	30 min	50 min
facebook	3	6	7
e-mail		1	
zprávy			1
sport			1
baví se sousedem		1	3
mobil		2	
video		1	1
učí se na něco jiného	1		
spí			
nespecif (nevím)		1	1
is		1	1
dopravní spojení			
hry			
+		2	1
ptají se		2	4
baví se k tématu			1
hledá k tématu			1
permanentně mimo	3 (dva vzadu + holka)		
celkem lidí			9

Průběh hodiny:
nový učitel – ještě k tomu s návštěvou, jsou zaujati
10 min – jsou zaujati odborníkem a situací s virem ve škole (všichni krom 1 – ten to přišel jenom odsedět, trading nebo něco podobného)
po chvíli zas vlna rozptýlení
když odpovídá jeden z nich, ostatní ho poslouchají
dotaz k tématu – můžu si udělat vlastní cloud?
jinak je to výzva k povídání – dva
dotaz – kdy se to stalo (libim se ti.cz)
50 min – v jednu chvíli v podstatě všichni mají na monitoru něco jiného (FB), plně se soustředí asi 3
když se mluví o mailu, dva do schránky koukají
ten jeden aktivní to trochu rozhodí
na konci dost dotazů (téma je zaujalo)

učitel (odborník):
snaží se směřovat dotazy na ty, kdo se baví (nedává pozor)
výklad plný historek z života
humor
občas se baví jen s jedním zájemcem, ostatní mimo
ptá se
jinak monologická přednáška

dojem:	odborník na bezpečnost je autorita a má na začátku pozornost všech jeden student je problematiky znalejší než ostatní, často strhává dotazy a připomínkami pozornost učitele jen k sobě studenti přemýšlí nad výkladem, diskutují s učitelem, mají několik dotazů (v průběhu asi 2, 4-5 na konci) fb spíš pasivně

Frontální výuka

-	úvod	prezentace (10 min)	30min	60 min
facebook	6	8	6	5
e-mail		3	3	1
baví se sousedem			2	
mobil				
učí se na něco jiného	1			1
slevomat			1	2
spí		1		
nespecif (nevím)				1
is		1	2	
dopravní spojení	1			
hry		2	1	
+				
ptají se			1	
baví se k tématu	1			
celkem lidí	13			
permanentně mimo	6	8	8	

Průběh hodiny: na začátku všichni na FB, ani se nechytli na napadení školní sítě...
s prezentací pozornost upadá
horší čitelnost projektoru
interaktivní graf (půlka nevnímá)
"případně existují 10min maily" – jak ukázal prakticky Vašek, není to pro každého samozřejmost (sledovali), tady se to úplně přešlo
promítané video – nefunguje
na aktivizační dotazy si učitel odpovídá sám
prezentace běží, učitel něco povídá – většina nevnímá
informace o fb ("co jste odškrtli") aspoň na chvilku zaujme
ke konci se pozornost trochu zlepšuje – někteří jsou svým nicněděláním tak znuděni, že vše vypnou a raději poslouchají (a ono je to i zaujme)

učitel: přesunutí posledních řad dopředu
ptá se na počet hesel (funguje přihlásit se, kdo má 5 hesel, 3 hesla...)
snaží se ptát i dál, odpovídá si sám
snaží se oživit výklad vlastními zkušenostmi a reálnými příběhy, aktualitami (má přehled) – nesledují, tak to většinou nefunguje

dojem: skupina celkově je mimo, nesleduje výklad – nereaguje
aktivně píšou na facebook a e-mail, hrají hry
ke konci zlepšení (mobil) – škoda, že neposlouchali od začátku

Skupinová výuka

-	úvod	brainstorming	papírky ve skupinkách	prezentace skupinkami
facebook	4	3	4	4
e-mail	1	1		1
zprávy				
baví se sousedem	1		4	5
mobil	2		3	3
video				
učí se na něco jiného				3
slevomat				
spí	1			
is	2	2	1	2
dopravní spojení				
hry				
+				
ptají se			3	2
baví se k tématu			8	
hledá k tématu			12	
celkem lidí	16			
permanentně mimo	0	0	0	2

Průběh hodiny: začátek brainstormingem (nepřekládat!:D)

papírky do skupinek – velmi rozmanitá spolupráce (většinou skupina řeší, jen výjimečně jsou flákači, kteří to nechávají na zástupci)

od ostatních aktivit (fb atd.) odrazuje procházení učitele mezi počítači, jednou upozorní na použití fb místo práce na zadání

v některých skupinkách přínosné diskuse o tématu (členové se aktivně ptají kolegů a zjišťují od nich informace, protože je to zajímá)

i tady je prostor pro fb a další aktivity – buď moc nepracují a spoléhají na ostatní členy týmu (větší skupiny) nebo už mají hotovo a čekají na ostatní

prezentace skupinové práce

nevýhoda nevýrazných osobností (nejdou slyšet, špatná artikulace – neni mu rozumět), někteří (4-5) lidí je neposlouchá

jedna skupinka (u okna to výrazně ruší bavením) – možná stačilo říct, "pane kolego už se otočte, už nemusíte spolupracovat", postupně se uklidní, jak se na ně blíží řada

jinak všichni celkem vnímají

nikdo nevyužil možnost projekce