Moderné vzdelávanie pre vedomostnú spoločnosť / Projekt je spolufinancovaný zo zdrojov EÚ

Vladimír Bobot
Miroslava Jakubeková

Informačná bezpečnosť v škole

2013

Publikácia bola vydaná a financovaná z prostriedkov ESF v rámci národného projektu Profesijný a kariérový rast pedagogických zamestnancov.
ITMS kód projektu 26120130002
ITMS kód projektu 26140230002

METODICKO-PEDAGOGICKÉ CENTRUM

Informačná bezpečnosť v škole

Vladimír Bobot
Miroslava Jakubeková

Bratislava 2013

Názov:	**Informačná bezpečnosť v škole**
Autori:	Ing. Vladimír Bobot
	Ing. Miroslava Jakubeková
Recenzenti:	Ing. Vladimír Slahučka
	Ing. Eva Žernovičová
Vydavateľ:	Metodicko-pedagogické centrum v Bratislave
Odborná redaktorka:	Mgr. Sylvia Laczová
Grafická úprava:	Ing. Vladimír Bobot
Vydanie:	1.
Rok vydania:	2013
Počet strán:	64
ISBN:	978-80-8052-486-9

Obsah

1 Úvod do problematiky

„Učiteľ je jedným zo základných činiteľov vzdelávacieho procesu, ktorý je profesionálne kvalifikovaným pedagogickým pracovníkom spoluzodpovedným za prípravu, riadenie, organizáciu a výsledky tohto procesu.“ (Průcha, Walterová, Mareš, 1998).

Rozvoj spoločenských, ale najmä technických vied nabral na sklonku dvadsiateho storočia nevídané tempo. S tým bezprostredne súvisia nové nároky na obsah a kvalitu vzdelávania. Obrovské množstvo nahromadených vedomostí a informačno-komunikačné technológie, umožňujúce sprístupnenie informácií rôzneho druhu v reálnom čase, vytvárajú na vzdelávanie nové podmienky. Súčasné možnosti získavania, spracovania a využívania informácií vytvárajú predpoklady na intenzifikáciu vyučovacieho procesu.

Používanie mobilných telefónov a počítačov sa pre mnohých ľudí stalo každodennou potrebou. Informačné technológie sa stali bežnou súčasťou väčšiny profesií a úplne samozrejme ich využívajú žiaci aj učitelia vo vyučovacom procese. Zdalo by sa, že tento vývoj je uspokojivý a nie je potrebné problematike venovať osobitnú pozornosť. Žiaľ, s fenoménom moderných informačných technológií sa postupne objavujú aj negatívne javy a hrozby. Rovnako rýchlo, ako sa vyvíjajú technológie na spracovanie informácií, objavujú sa aj spôsoby ako technológie a informácie zneužívať. Preto stále nástojčivejšie vzrastá potreba riešiť problematiku **informačnej bezpečnosti**. Pociťujú ju nielen firmy, ale aj bežní občania. Ide o náročný a dlhodobý problém, ktorý si vyžaduje pozornosť a spoluprácu odborníkov rôznych odvetví.

V súvislosti s tým sa objavuje požiadavka šírenia osvety a vzdelávania v oblasti informačnej bezpečnosti, ako aj požiadavka zakomponovať problematiku informačnej bezpečnosti aj do vzdelávacieho procesu v školách. Učitelia prejavujú záujem vzdelávať sa najmä v oblasti moderných vyučovacích metód s podporou informačných technológií, ktorého cieľom je inovácia vyu-

čovania na predmetovej a medzipredmetovej úrovni, využívanie multimédií, dostupného softvéru a edukačných programov, možností internetu, e-learningu a elektronickej komunikácie. Priebežne sa realizuje aj vzdelávanie zamerané na ovládanie modernej didaktickej techniky. Vzdelávanie učiteľov sa orientuje na využívanie moderných technológií na aktivizáciu žiaka v procese vyučovania a jeho nasmerovanie na celoživotné vzdelávanie.

Vo všeobecnosti môžeme povedať, že strategický význam vzdelávania v oblasti IKT je neoddeliteľnou súčasťou premeny každej spoločnosti na učiacu sa spoločnosť. A práve takáto spoločnosť potrebuje budovať koncepty nadstavbových systémov edukácie na báze celoživotného vzdelávania.

Nová rola učiteľa vyžaduje, aby naučil žiaka pracovať s informáciami a pripravil ho na celoživotné učenie sa. Moderné technológie dokážu efektívne využívať len tí, ktorí sú ochotní sledovať vývojové trendy a rozvíjať príslušné kompetencie. K základným kompetenciám patrí aj digitálna gramotnosť, ktorá je založená na sebaistom a zodpovednom používaní techniky, kritickom postoji k dostupným informáciám a rešpektovaní zásad bezpečnosti práce s informáciami. V súčasnosti narastá záujem o vzdelávanie zamerané na predchádzanie rizikám, ktoré s využívaním informačných technológií súvisia. Moderní a inovatívni učitelia chápu potrebu vyvažovania rizík súvisiacich s informačnými a komunikačnými technológiami poznávaním a dodržiavaním zásad informačnej bezpečnosti v bežnom, každodennom živote. Aby v rámci výchovno-vzdelávacieho procesu mohli pedagogickí a odborní zamestnanci v školstve poukázať na nebezpečenstvá, naznačiť možnosti, ako ich riešiť, ako im predchádzať, na koho sa obrátiť alebo kde vyhľadať pomoc, ak je to potrebné, musia mať sami dostatok informácií o aktuálnej situácii, o počítačovej kriminalite v reálnom svete, o možnej prevencii a alternatívnych riešeniach. Kontinuálne vzdelávanie v tejto oblasti je jednou z ciest, ako rozvíjať kompetencie učiteľov a vytvoriť predpoklady na prirodzené zakomponovanie problematiky informačnej bezpečnosti do výchovno-vzdelávacieho procesu.

Cieľom vzdelávacieho programu kontinuálneho vzdelávania je, aby učitelia:

- Poznali stratégiu Európskej únie a Slovenskej republiky v oblasti informačnej bezpečnosti.
- Dokázali identifikovať riziká v oblasti informačnej bezpečnosti z technického a personálneho hľadiska.
- Ovládali základné zásady bezpečnosti pri práci s informáciami.
- Poznali nástroje a možnosti prevencie, riešenia a poradenstva pri ohrození informačnej bezpečnosti.
- Využívali aktivizujúce metódy v oblasti zvyšovania informačnej bezpečnosti v procese vyučovania.

Obsah programu kontinuálneho vzdelávania sa orientuje na technické aspekty informačnej bezpečnosti, ale i na ochranu osôb a inštitúcií, ktoré súvisia s bezpečnosťou pri práci s informáciami. Program kontinuálneho vzdelávania je orientovaný na možnosti zvyšovania informačnej bezpečnosti v procese výchovy a vzdelávania.

1.1 Význam informačnej bezpečnosti

Pre široké spektrum problémov, s ktorými informačná bezpečnosť súvisí, nie je jednoduché pojem jednoznačne zadefinovať. Z odborného hľadiska pod informačnou bezpečnosťou chápeme schopnosť informačno-komunikačných systémov odolávať nástrahám, ktoré ohrozujú dostupnosť, dôveryhodnosť, integritu a bezpečnosť prenášaných, zverejnených a uchovávaných údajov a kvalitu s nimi súvisiacich služieb. Zjednodušene môžeme informačnú bezpečnosť chápať ako ochranu informačných a komunikačných technológií, a informácií, ktoré prostredníctvom nich sprostredkujeme.

K ohrozeniam, ktoré sú v centre pozornosti informačných bezpečnostných opatrení, patria náhodné aj zámerne vyvolané udalosti, ktoré môžu byť moti-

vované zákerným úmyslom, alebo vyplynú z neodborných zásahov, prípadne sú len následkom nevhodnej zábavy technicky zdatných jedincov a skupín. Bezpečnostné opatrenia sa týkajú zlyhania techniky, softvérov, internetových služieb (webové stránky, internetbanking, chat, e-mail, rôzne portálové riešenia ako e-learning a pod.) alebo priamo informácií. Centrom pozornosti sú tiež osoby, ktoré s technikou a informáciami pracujú a môžu ohroziť bezpečnosť na základe nevedomosti, nezodpovednosti, premyslenou činnosťou zameranou na získanie výhody, spôsobenie škody alebo podporu iných subjektov (špionáž, sabotáž, krádež a pod.).

S dôsledkami takýchto nekalých praktík majú dnes skúsenosti mnohí jedinci alebo firmy, počínajúc únikom osobných údajov z rôznych databáz (adries, telefónnych čísel a pod.) až po poškodenie webových stránok, zasielanie nevyžiadanej pošty, neoprávnené nadobudnutie výsledkov duševnej činnosti, zneužívanie dôvery alebo zavírenie počítačov. Škála možností sa vývojom technológií neustále rozširuje. K najzávažnejším prehreškom v tejto oblasti patrí neoprávnená manipulácia s údajmi akéhokoľvek druhu a krádeže založené na zneužití informačných technológií.

Problematiku rieši každý štát príslušnou legislatívou. Ústava Slovenskej republiky globálne zakotvuje právo na ochranu osobných údajov, ktoré je detailne upravené v Zákone o ochrane osobných údajov. Dozor nad dodržiavaním zákona vykonáva Úrad na ochranu osobných údajov, ktorý napr. pri príležitosti dňa ochrany osobných údajov (28. január) odpovedal prostredníctvom webu na otázky občanov súvisiace s ochranou osobných údajov. Podobne ako zákon ochraňuje osobné údaje, chráni aj autorské práva na umelecké diela, vedecké diela a iné diela, ktoré sú výsledkom vlastnej tvorivej duševnej činnosti autora. Práve moderné technológie sú často na príčine porušovania tohto práva, v dôsledku čoho autori nedostávajú za svoje dielo adekvátnu kompenzáciu.

Napriek zvyšovaniu aktivít na riešenie digitálnych výziev v rôznych vyspelých štátoch sveta sú opatrenia stále nedostatočné. Keďže globálne proble-

my vyžadujú globálne riešenia, predpokladá sa, že problematike prispôsobenia sa ohromnému technologickému pokroku, meniacim sa spoločenským normám a svetu, ktorý je čoraz viac postavený na elektronickej komunikácii bude venovaná pozornosť na báze nielen európskej, ale celosvetovej spolupráce.

Informačná bezpečnosť je celosvetový problém. Ľahký prístup ku komunikačným technológiám a internetu spôsobuje, že sa aj deti dostávajú k informáciám, ktoré ich môžu negatívne ovplyvniť. Podľa nadácie *Mijn Kind Online* holandské deti míňajú vo virtuálnych svetoch stále viac a viac peňazí. Pozornosť otázkam súvisiacim s obchodovaním detí na internete venuje aj Spojené kráľovstvo v dokumente *Briefing on the internet, e-commerce, children and young people*. Stanovisko Európskeho hospodárskeho a sociálneho výboru na tému „Preventívne opatrenia na ochranu detí pred sexuálnym zneužívaním“ poukazuje na to, že internet a ostatné technológie poskytujú nové príležitosti pre páchateľov a výrobu a distribúciu detskej pornografie (Úradný vestník Európskej únie, 2012). Rozširuje sa narušovanie súkromia, zneužívanie identity, duševného vlastníctva a iné škodlivé javy súvisiace so svetom informačných technológií. Na negatívny vplyv médií upozorňujú nielen rodičia a učitelia, ktorí sú s deťmi v každodennom kontakte, ale i psychológovia a odborníci na informačné technológie.

Problematika informačnej bezpečnosti je veľmi široká. Zahŕňa nielen otázky technologickej bezpečnosti, ochrany osobných, firemných a štátnych informácií, ale možné negatívne dopady informácií a informačných technológií na populáciu. Ide o prirodzené riziká, ale i cielené útoky a nečestné zámery. Preto sú aj otázky informačnej bezpečnosti riešené z hľadiska technického, spoločenského, ale aj legislatívneho. Napr. Európske hospodárske spoločenstvo podporuje iniciatívy Európskej komisie *Bezpečný internet a siete INSAFE a INHOPE* na podporu bezpečného používania internetu deťmi a všetkými členmi spoločnosti. Sloboda cestovania umožňuje páchateľom, aby sa zamerali na najzraniteľnejšie deti. Reklamné a komerčné postupy, ktorých cieľom sú deti, by mali byť v súlade so smernicou Európskeho parlamentu a Rady

o nekalých obchodných praktikách, aby sa na celoeurópskej úrovni jasne definovali bezpečnostné normy v oblasti internetu. V súvislosti s výrokom „...podnietiť poskytovateľov internetových služieb, aby na dobrovoľnej báze vypracovali kódexy správania a usmernenia pre blokovanie prístupu na takéto internetové stránky...“ (Smernica o nekalých obchodných praktikách, 2006).

Priebežne vznikajú nové pravidlá smerujúce k zvyšovaniu informačnej bezpečnosti. V roku 2000 to bola napríklad *Smernica o určitých právnych aspektoch služieb informačnej spoločnosti na vnútornom trhu, najmä o elektronickom obchode* (2000/31/ES), ktorá je základom postupov oznamovania a odstraňovania informácií na internete. Komisia stanovila v roku 2007 európsky prístup k mediálnej gramotnosti v digitálnom prostredí v dokumente s názvom *Európsky prístup k mediálnej gramotnosti v digitálnom prostredí* a v roku 2009 v *Odporúčaní Komisie o mediálnej gramotnosti v digitálnom prostredí pre konkurencieschopnejší audiovizuálny priemysel a priemysel obsahu a inkluzívnu znalostnú spoločnosť*. V roku 2009 boli vypracované *Bezpečnejšie zásady využívania sociálnych sietí v EÚ* a následne v rámci programu pre bezpečnejší internet bol zostavený v roku 2010 súpis usmernení vzťahujúcich sa na výrobu a poskytovanie online obsahu pre deti a mladých ľudí. Lisabonská stratégia *e_Europe* bola v roku 2010 nahradená *i-Initiative 2010*. V roku 2011 vstúpila do platnosti smernica o boji proti sexuálnemu zneužívaniu a sexuálnemu vykorisťovaniu detí a proti detskej pornografii. Kriminalizuje zločiny, medzi ktoré patrí detská pornografia, *grooming* detí (nadviazanie priateľstva s deťmi za účelom ich sexuálneho zneužitia), sexuálne zneužívanie prostredníctvom webovej kamery alebo pozeranie detskej pornografie na internete. Na problematiku reagujú postupne opatreniami aj jednotlivé krajiny, napríklad vytvorením tiesňových liniek (*Internet Watch Foundation,* Veľká Británia), poskytovaním bezplatného softvéru na rodičovskú kontrolu (Francúzsko), vytváraním mechanizmov na oznamovanie škodlivého a nezákonného obsahu (Česká republika) a pod.

Menej pozornosti bolo informačnej bezpečnosti venované v dokumente *Kľúčové údaje o vzdelávaní a inováciách prostredníctvom IKT v európskych školách 2011*, kde je pozornosť prednostne venovaná úrovni zručností a zabezpečenie dostupnosti informačných technológií. Práve v takomto dokumente je priestor na mapovanie vývoja informačnej bezpečnosti v edukačnom prostredí v populácii školopovinných detí.

Európska komisia zaradila boj proti počítačovej kriminalite za prioritu v rámci stratégie vnútornej bezpečnosti. Za dôležitú sa považuje prevencia a v spoločnom záujme je, aby bola celková európska stratégia pre internetovú bezpečnosť akceptovaná všetkými štátmi, aby všetky štáty ratifikovali *Dohovor Rady Európy o počítačovej kriminalite*. Jednou z iniciatív Komisie je aj vyhlásenie *Európskeho dňa bezpečného internetu* (9. február).

Európska stratégia vytvárania lepšieho internetu pre deti vychádza z toho, že stále viac detí začína používať internet už pred začiatkom školskej dochádzky. Na základe prieskumov medzi rodičmi v Európe internet používajú tri štvrtiny detí vo veku šesť až sedemnásť rokov. Pokiaľ pätnásťročné a šestnásťročné deti sa k práci s internetom dostali vo veku jedenásť rokov, deväťročné až desaťročné deti uvádzajú, že ho začali využívať v priemere už vo veku sedem rokov. Len jedna tretina detí vo veku deväť až dvanásť rokov uvádza, že na internete nájdu dostatok informácií vhodných pre svoj vek.

Moderné technológie ako iPady, androidy, smartfóny čítačky, skenery, multifunkčné zariadenia, konzoly, elektronické hračky a stavebnice alebo digitálne fotoaparáty, kamery a vizualizačné zariadenia sú vynikajúcou základňou na kreatívne vzdelávanie pokiaľ bude na mladšie a školopovinné deti pripravený vhodný vzdelávací obsah. Nebývalé príležitosti poskytujú práve internetové a mobilné aplikácie, vzdelávacie softvéry alebo hry. Inovačné správanie detí prirodzene vedie k využívaniu týchto možností na vzdelávanie, zber a spracovanie informácií, vyjadrovanie názorov, spoločenskú angažovanosť a komunikáciu s okolitým svetom. **Deti sú v tomto virtuálnom svete obzvlášť zraniteľné, je potrebné ich chrániť**.

Vzhľadom na to, že sa služby na internete neustále vyvíjajú, vplyv na bezpečnosť detí nie je možné vopred predvídať.

Základom stratégie sú štyri piliere, ktoré sa navzájom dopĺňajú:

1. Podpora kvality online obsahu pre mladých ľudí.
2. Zvyšovanie informovanosti a zlepšovanie možností.
3. Vytváranie bezpečného online prostredia pre deti.
4. Boj proti pohlavnému zneužívaniu a sexuálnemu vykorisťovaniu detí.

„Nestačí len chrániť deti, pokiaľ sú na internete. Je potrebné posilniť digitálnu gramotnosť mladých Európanov a ich rodičov, aby boli schopní vybudovať si vlastnú ochranu a zodpovednosť v online prostredí.“ (Európska stratégia vytvárania lepšieho internetu pre deti, 2012). Pre školy z toho vyplýva úloha zamerať sa na zvyšovanie gramotnosti detí v oblasti digitálneho prostredia a médií, na rozvoj sociálnych schopností a povedomia. Mali by zabezpečiť prístup detí ku kreatívnemu obsahu na internete, ktorý by stimuloval ich predstavivosť a podporoval ich učenie.

V končenom dôsledku to bude mať vplyv na ich lepšie šance zamestnať sa v budúcnosti. Očakáva sa aj prínos z lepších postupov identifikácie, oznamovania a odstraňovania škodlivých informácií na celospoločenskej úrovni (rodina, firmy, inštitúcie). (Európska stratégia vytvárania lepšieho internetu pre deti, 2012).

Dôležitým dokumentom je v tejto súvislosti Uznesenie Európskeho parlamentu z mája 2012 o stratégii vnútornej bezpečnosti Európskej únie. V súčasnosti sa Európsky parlament zaoberá dvoma právnymi normami súvisiacimi s ochranou osobných údajov – jednou je nariadenie ustanovujúce rámec EÚ na ochranu osobných údajov a druhou je smernica na ochranu údajov na účely súdneho vyšetrovania. Reforma Európskej komisie zavádza pravidlá, ktoré umožnia občanom lepšiu kontrolu nad používaním ich osobných údajov. Dôležitou novinkou je „právo byť zabudnutý“, ktoré umožňuje občanom žiadať o odstránenie svojich osobných údajov z rôznych databáz

v inštitúciách, ktoré nie sú na to oprávnené. Dôraz sa kladie na potrebu súhlasu na využívanie a prenos osobných údajov a na pokuty a sankcie za porušenie práv na ochranu súkromia.

1.2 Národná stratégia pre informačnú bezpečnosť a legislatívne normy

Informačná bezpečnosť v SR. Bezpečnostná stratégia SR týkajúca sa informatizácie spoločnosti bola prijatá v roku 2001. Na ňu nadväzuje mnoho dokumentov, ktoré riešia problematiku autorských práv, bezpečnosť informácií v bankách, elektronický obchod, počítačovú kriminalitu, elektronický podpis, ochranu osobných údajov, normy a štandardy a medzinárodnú spoluprácu v tejto oblasti. Jedným z dokumentov je napríklad výnos o *Štandardoch pre elektronické informačné systémy na správu registratúry* z roku 2011.

Aktualizovanie znenia stratégie v roku 2005 vychádzalo z faktu, že miera informatizácie spoločnosti dosiahla vysoký stupeň a stále sa zvyšuje, s čím súvisí aj nárast rýchlosti prenosu informácií a ich globálna dostupnosť. Preto je potrebné venovať pozornosť zraniteľnosti informačných a komunikačných systémov, neoprávnenému prístupu k informáciám, šíreniu počítačových vírusov a dezinformácií, ktoré sú rastúcou hrozbou pre každú krajinu.

V roku 2008 bol na Slovensku schválený dokument *Národná stratégia pre informačnú bezpečnosť v SR*, ktorého hlavným cieľom je vytvoriť rámec informačnej bezpečnosti. Na základe východiskového stavu stanovuje kompetencie, právomoci, priority a kroky na dosiahnutie cieľa. Opatrenia stratégie sú nasmerované na zvýšenie dôveryhodnosti elektronických služieb, elektronického obchodu a konkurencieschopnosti Slovenska. Predmetom záujmu sú napríklad opatrenia proti úniku informácií, ich neoprávnenému použitiu, porušenie ochrany osobných údajov, ochrana informačných a komunikačných systémov, poškodenie mena štátnych inštitúcií a tiež opatrenia na presadzovanie právnych noriem.

Strategické ciele sú:

- prevencia – ochrana digitálneho priestoru Slovenska, predchádzanie incidentom.
- pripravenosť – schopnosť reagovať na bezpečnostné incidenty a minimalizovať ich dosah.
- udržateľnosť – udržanie a rozširovanie kompetencií Slovenska i oblasti informačnej bezpečnosti.

Strategické priority:

- Ochrana ľudských práv a slobôd v súvislosti s využívaním internetu.
- Budovanie povedomia a kompetentnosti v informačnej bezpečnosti.
- Vytváranie bezpečného prostredia.
- Zefektívnenie riadenia informačnej bezpečnosti.
- Ochrana štátnej infraštruktúry.
- Národná a medzinárodná spolupráca.
- Rozširovanie kompetencie.

Vo vzťahu k vzdelávaniu sa na základe stratégie a akčného plánu, ktorý bol na jej uplatnenie vypracovaný, analyzuje stav potrieb používateľov IKT a mapujú sa kapacitné a obsahové možnosti školského a iného vzdelávania. Predpokladá sa vytvorenie štandardu základných znalostí v oblasti informačnej bezpečnosti pre jednotlivé kategórie používateľov informačných a komunikačných technológií. Vzdelávanie je potrebné zamerať na zvýšenie úrovne poznania o možnostiach ochrany pred hrozbami prostredníctvom internetu a realizovať ho pre jednotlivé cieľové skupiny vo všetkých vzdelávacích programoch formálneho aj neformálneho vzdelávania. Na základe potrieb budú navrhnuté programy na zvyšovanie bezpečnostného povedomia najmä pre používateľov s osobitými nárokmi na informačnú bezpečnosť. Problematika informačnej bezpečnosti sa stane súčasťou všetkých predmetov nielen študijných predmetov týkajúcich sa informatiky. V rámci stratégie bude podporo-

vané vydávanie odbornej literatúry a metodických dokumentov zameraných na riešenie problémov informačnej bezpečnosti.

Stratégia je rozpracovaná na základe strategických materiálov SR a EÚ na obdobie piatich rokov a jej uplatnenie v praxi sa očakáva od všetkých subjektov. Preto aj v oblasti vzdelávania v regionálnom školstve treba problematike venovať systematickú pozornosť. (Národná stratégia pre informačnú bezpečnosť v SR, 2008).

Slovensko sa zapája do medzinárodných aktivít, ako je napríklad deň bezpečnejšieho internetu (obrázok 1, prevzatý z www.saferinternet.org/web/guest/safer-internet-day.jpg), ktorý začiatkom februára od roku 2004 organizuje európska organizácia INSAFE vo viac ako 65 krajinách sveta. Zameraný je na podporu bezpečnejšieho a zodpovedného využívania online technológií a mobilných telefónov predovšetkým u detí a mladých ľudí na celom svete. V roku 2012 bola pri tejto príležitosti v Bratislave symbolicky pokrstená publikácia Deti v sieti, ktorá je bezplatne dostupná na stiahnutie na *www.zodpovedne.sk* alebo v niektorých elektronických kníhkupectvách.

Obrázok 1 Deň bezpečnejšieho internetu

1.3 Zákon o ochrane osobných údajov

Základným zákonom, v ktorom štát stanovuje predpisy na prácu s informáciami je Ústava Slovenskej republiky. Je pozoruhodné, s akým predstihom tvorcovia základného zákona štátu predpokladali rozmach možných rizík práce s informáciami. V čase prijatia Ústavy SR (1992) nebol ešte na svete webový prehliadač (prvý grafický browser *Mosaic* bol sprístupnený v roku 1993), počítačové siete boli doménou akademických pracovníkov vysokých škôl a ich

študentov a termín *internet* sa začal používať o štyri roky neskôr. Ústava stanovuje základné zásady práce s informáciami vzhľadom na ich bezpečnosť až v štyroch článkoch. V článku 19, odsek 3 je uvedené: „Každý má právo na ochranu pred neoprávneným zhromažďovaním, zverejňovaním alebo iným zneužívaním údajov o svojej osobe.“ (Ústava SR). Článok 22, odsek 2 uvádza: “Nikto nesmie porušiť listové tajomstvo ani tajomstvo iných písomností a záznamov, či už uchovávaných v súkromí, alebo zasielaných poštou, alebo **iným spôsobom**.“ (Ústava SR).

Zatiaľ existuje hranica medzi právom vyjadriť myšlienku a mierou pravdivosti tejto myšlienky. Budúcnosť smeruje na jednej strane k totálnemu liberalizmu, ktorý zaplaví médiá vrátane internetu treťotriednymi informáciami (bohužiaľ na objednávku väčšiny spoločnosti) a na druhej strane k totalitarizmu, ktorý rôznosť myšlienok úplne potlačí. Ústava je v tomto smere otvorená. Článok 26 odsek 2 Ústavy SR stanovuje základné právo človeka vyjadriť názor: „Každý má právo vyjadrovať svoje názory slovom, písmom, tlačou, obrazom alebo iným spôsobom, ako aj slobodne vyhľadávať, prijímať a rozširovať idey a informácie bez ohľadu na hranice štátu.“ Na druhej strane si štát v tom istom článku odsek 4 vyhradzuje právo reštrikcie: „Slobodu prejavu a právo vyhľadávať a šíriť informácie možno obmedziť zákonom, ak ide o opatrenia v demokratickej spoločnosti nevyhnutné na ochranu práv a slobôd iných, bezpečnosť štátu, verejného poriadku, ochranu verejného zdravia a mravnosti“. Súčasný krehký status quo je udržateľný – zákony reflektujú a trestajú potenciálne hrozby.

Ochranou osobných údajov sa v slovenskej legislatíve detailne zaoberá zákon č. 363/2005 Z. z. – zákon o ochrane osobných údajov. Vzhľadom na veľmi širokú problematiku, ktorú zákon rieši, venujme sa len vybraným bodom súvisiacim so školstvom:

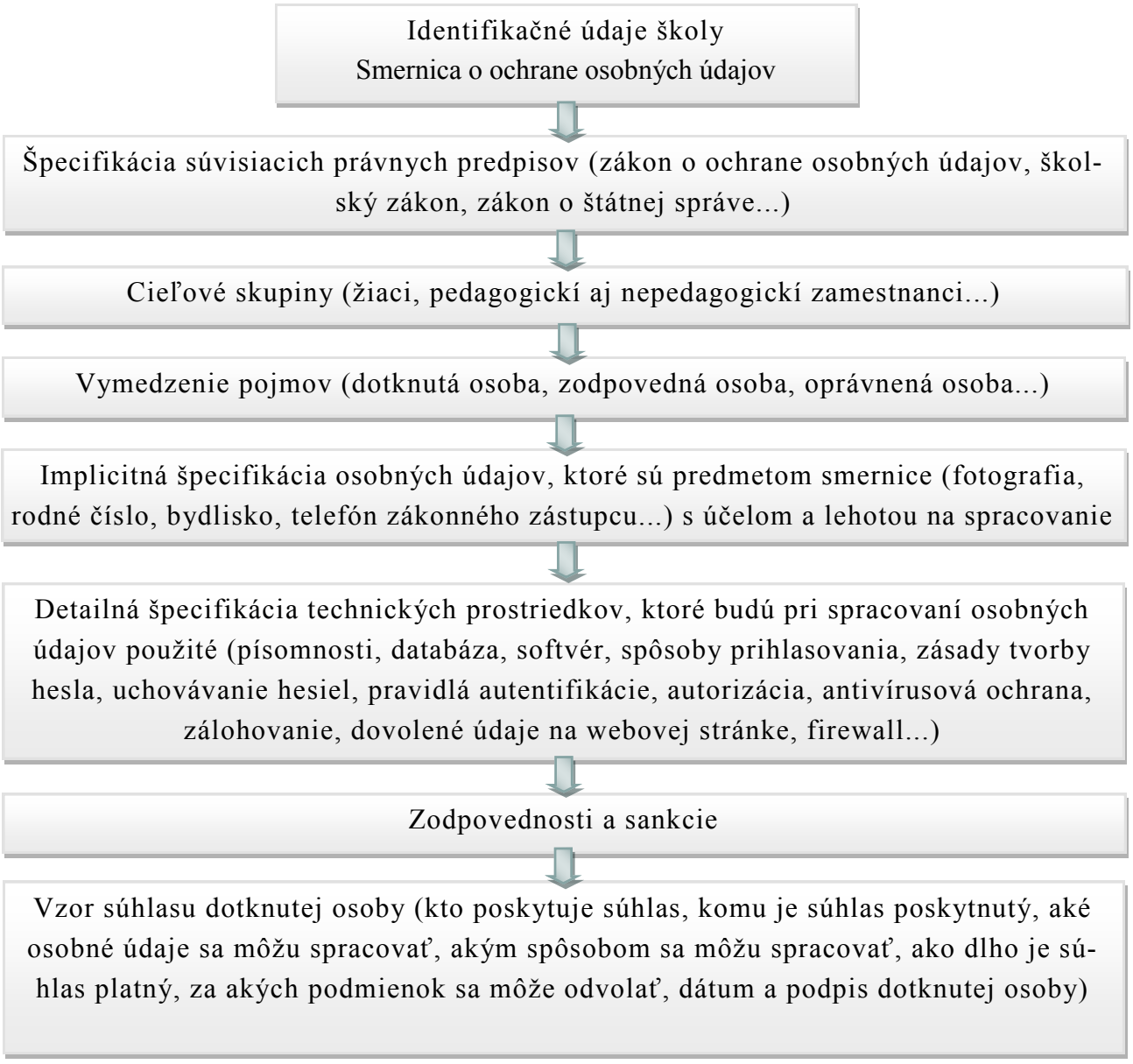
1. Čo je **osobný údaj?** Akýkoľvek znak, vlastnosť, charakteristika, ktoré môžu byť použité na zistenie identity človeka. Fotografia, rodné číslo, odtlačok prsta (sietnica oka) alebo DNA patria medzi tie, ktoré nemožno

spochybniť. V zmysle § 3 zákona sú však osobnými údajmi aj znaky „ktoré tvoria jej fyzickú, fyziologickú, psychickú, mentálnu, ekonomickú, kultúrnu alebo sociálnu identitu.“ Ide o hmotnosť, výšku, pohlavie, adresu, dátum narodenia, členstvo v krúžku, politickú príslušnosť, zamestnanie, vierovyznanie, farbu očí, a ad absurdum aj to, či žiak nosí okuliare alebo chodí do školy obutý.

2. Čo je **spracovanie** osobných údajov? Spracovanie údajov je v zmysle § 4, odsek 1 písmeno a) zákona o ochrane osobných údajov „akákoľvek operácia... s osobnými údajmi, napr. ich získavanie, zhromažďovanie... sprístupňovanie alebo zverejňovanie.“ Spracovanie údajov je aj ich zverejnenie na školskej webovej stránke.
3. § 7 odsek 1 zákona hovorí, že „Osobné údaje možno **spracúvať len so súhlasom dotknutej osoby**, ak tento zákon neustanovuje inak.“
4. Iné zákony (§ 29 ods. 7 zákona č. 596/2003 o štátnej správe v školstve a viacero paragrafov zákona o výchove a vzdelávaní – školský zákon č. 245/2008 Z. z.) taxatívne vymenúvajú tie osobné údaje, ktoré je možné **spracovávať aj bez súhlasu dotknutej osoby**: meno a priezvisko, dátum a miesto narodenia, bydlisko, rodné číslo, štátna príslušnosť, národnosť, osobné údaje o identifikácii zákonných zástupcov dieťaťa alebo žiaka, údaje o fyzickom a duševnom zdraví, mentálnu identitu vrátane výsledkov pedagogicko-psychologickej a špeciálnopedagogickej diagnostiky. Paragraf 11 odsek 7 školského zákona upresňuje údaje o zákonných zástupcoch na spracovanie ich mena a priezviska, adresy zamestnávateľa, trvalého bydliska a telefónneho kontaktu. Podľa § 24 odsek 4 k nim v prípade zápisu dieťaťa na základnú škola patrí aj údaj o mieste narodenia.

Z uvedeného vyplýva, že škola môže vo svojom informačnom systéme ukladať osobné údaje bez súhlasu žiaka ako dotknutej osoby. Uverejnenie fotografie žiaka na webovej stránke školy bez jeho súhlasu pokladáme za porušenie zákonov.

Povinnosťou školy podľa zákona o ochrane osobných údajov je vymedziť prostriedky, spôsoby a ďalšie podmienky na spracovanie osobných údajov. Povinnosť vyplýva z § 6 ods.1 písm. b) zákona. Odporúčanou formou je napr. smernica, ktorej štruktúra môže byť nasledovná (obrázok 2). Najdôležitejšou a technicky najnáročnejšou časťou smernice je bod, v ktorom sa definujú nástroje, metódy a postupy samotného zabezpečenia a ochrany osobných údajov pred zneužitím. Nie sú určené žiadnym predpisom a ich špecifikácia je daná odbornými znalosťami učiteľov v škole, resp. odporúčaniami zriaďovateľa.



Obrázok 2 Smernica školy o ochrane osobných údajov

1.4 Zákon o ochrane osobných údajov

S ochranou ľudských práv a slobôd ako strategickou prioritou informačnej bezpečnosti úzko súvisí pomerne zložitá problematika autorských práv. Základný legislatívny dokument ktorý práva autorov rieši je zákon č. 618/2003 (Autorský zákon). Všeobecné informácie k problematike sú uvedené napríklad v publikácii "*Autorské právo a práva súvisiace s autorským právom z hľadiska aktuálnych harmonizačných tendencií na úrovni EÚ*". Základné otázky uplatnenia autorského práva v školskej praxi sú podrobne rozobraté v publikácii "*Autorské právo v školách*". Obe publikácie autorov Z. Adamovej a A. Škreka sú dostupné na internete.

1.5 Základné pojmy

V publikácii sú uvádzané pojmy charakterizujúce spôsoby útoku na dôverné informácie, ktoré vyžadujú jednoduché alebo komplexnejšie vysvetlenie:

1. **Sociálne inžinierstvo**. Proces neoprávneného získavania informácií pomocou psychickej manipulácie osoby, ktorá môže prístup k informáciám umožniť. Sociálne inžinierstvo nahrádza technické prostriedky psychologickými, pričom sa zameriava na najslabšie ohnivko v zabezpečení informácií – samotného človeka, na jeho nevedomosť, naivitu až hlúposť. Najpoužívanejšou metódou je phishing a pharming.
2. **Phishing** (udička). Ide o vyžiadanie dôvernej informácie spoliehajúc sa na emóciu užívateľa. „Vážený klient, ako ste určite zachytili v dennej tlači, stala sa naša banka v dňoch... terčom útoku hackerskej skupiny... Z toho dôvodu Vás láskavo prosíme o zaslanie Vašich prístupových údajov do internetbankingu z dôvodu ich spárovania s našimi databázami. Administrátor banky“. Aj keď práve nemáme svoj deň, dáme sa nachytať? Podobnou metódou sú oznamy o veľkých výhrach, ktorých vyplateniu bráni len zaslanie 1 % z výhernej čiastky na náklady za prevod peňazí na účet oklamaného naivného užívateľa a pod.

3. **Pharming**. Ide o získanie dôvernej informácie nepozornosťou užívateľa. Predstavme si webovú stránku, ktorá je vizuálne identická so stránkou nášho internetbankingu. Vyrobiť ju a online sprístupniť na internete nie je zložité, šikovný programátor to zvládne za pár dní. Zadaním prihlasovacieho mena a hesla sa tieto dáta uložia na server crackera, ktorý ich vie okamžite zneužiť. Ako je to možné? Namiesto adresy nazovbanky.sk sme zadali napr. nayovbankz.sk. Sofistikovanejší pharming spočíva v napadnutí súboru, v ktorom má prehliadač, resp. operačný systém uložené informácie o navštívených webových stránkach. Ak sme otvorili napr. stránku nazovbanky.sk, údaje o IP adrese tejto stránky sa zaznamenali do *cache* pamäte prehliadača. Nasledujúce otvorenie tej istej stránky bude rýchlejšie, pretože prehliadač nezisťuje IP adresu nazovstranky.sk na DNS servery niekde na internete, ale v súbore na lokálnom počítači, kde je uložený zoznam navštívených stránok. Získame tým 1 sekundu, ale v prípade napadnutia a modifikácie tohto súboru môžeme byť presmerovaný práve na stránku nayovbankz.sk, kde na naše prihlasovacie údaje čaká cracker.
4. **Malware** (*malicious*, škodlivý). Ide o softvér, ktorý bol naprogramovaný na účely zneužitia dôverných informácií priamo z nášho lokálneho počítača. Malware je všeobecný pojem, ktorý zahŕňa špecifické druhy škodlivého softvéru – vírusy, červy, trójske kone, adware, spyware a pod. Ubrániť sa phishingu a pharmingu nie je ťažké – stačí byť obozretný. Ubrániť sa malware vyžaduje od užívateľa dodržiavanie zásad **aktívnej bezpečnosti.**
5. **Vírus**. Je druh malvéru, ktorý sa „rozmnožuje“ bez vedomia užívateľa. Vie sa sám nakopírovať do iných programov v rámci vášho počítača, a z neho pomocou prenositeľných pamäťových médií do iných počítačov. Najčastejšou cestou infekcie sú nedôveryhodné internetové zdroje, z ktorých sťahujeme a inštalujeme softvér. Hlavným atribútom vírusu je jeho replikácia, t.j. schopnosť kopírovať sa do iných súborov. Vždy je pripojený k nejakému programu, z čoho vyplýva, že sa môže aktivovať len spustením tohto programu. Z hľadiska informačnej bezpečnosti nie je až taký

nebezpečný, pretože jeho deštrukčná činnosť sa zameriava hlavne na destabilizáciu činnosti počítača (spomalenie, nefunkčnosť...).

6. **Červy** (warms). Na rozdiel od vírusu červ vystupuje samostatne, nie je súčasťou iných programov, čím sa zvyšuje možnosť jeho šírenia pri rôznych operáciách operačného systému (napr. štart systému). Nebezpečnosť červov je v ich kvantite a v súčasnosti sa vyskytujú najčastejšie. Podobne ako vírusy väčšinou len destabilizujú činnosť počítača.
7. **Trójske kone**. Pripomínajú legendu z Homérovej Iliady. Tvária sa ako užitočný softvér (napr. komprimačný), ktorý v sebe skrýva deštrukčnú činnosť. Ak máme na počítači trójskeho koňa, pravdepodobne si cracker pripravuje útok na náš počítač.
8. **Adware** (*advertisement*, reklamný softvér). S inštaláciou bezplatných proprietárnych (majúcich autora) softvérových produktov dostávame často na náš počítač aj reklamný softvér, ktorý nám ponúka reklamu rôznych produktov (a jeho stiahnutie obyčajne v licenčných podmienkach nevedomky odsúhlasujeme). Adware nie je nebezpečný ale, podobne ako spam, otravujúci.
9. **Spyware** (*spy*, špión). Z hľadiska informačnej bezpečnosti ho pokladáme za najnebezpečnejší druh škodlivého softvéru. Dôvodom je jeho špecializácia na odosielanie dát z nášho počítača na počítač crackera, samozrejme bez nášho vedomia. Dátami môžu byť napr. aktuálne zadávané heslá alebo čísla kreditných kariet. Inštalácia spyware je podobná adware – obyčajne s jeho inštaláciou, argumentujúcou nevinným odosielaním informácií o histórií navštívených stránok, súhlasíme. Vidina *free* strihacieho softvéru alebo sťahovača videí z *youtube* prevláda nad našou obozretnosťou.
10. **Hacker**. Programátor, ktorý tvorí počítačový program s cieľom preniknutia do cudzieho informačného systému za účelom skúmania dokonalosti tohto systému a svojho sebazdokonaľovania. Hacker diery v systéme nezneužíva, ale upozorňuje na ne. V súčasnosti je tento pojem medializo-

vaný skôr v negatívnom zmysle – ako človek, ktorý z nezabezpečených systémov kradne informácie vo svoj materiálny prospech.

11. **Cracker**. Človek, ktorý vyvinul škodlivý kód (program) s motiváciou zneužiť získané informácie vo svoj prospech.
12. **Crack** (kreknutý program). Ak do proprietárneho plateného softvéru vloží cracker kód, ktorý znefunkční bezpečnostné prvky takéhoto softvéru (napr. žiadnym alebo univerzálnym heslom, alebo odstránením časového limitu používania) a ponúkne ho na internete na stiahnutie, hovoríme o kreknutej verzii. Odhliadnuc od porušenia autorských práv vlastníka soft-véru je dôležitejšie upozorniť na nebezpečenstvo pre samotných používateľov takýchto programov—nie je žiadna záruka, že v kreknutej verzii sa nenachádza malware.
13. **Grooming detí.** Proces manipulácie detí prostredníctvom sociálnych sietí na ich sexuálne zneužívanie (virtuálneho aj reálneho). Grooming je vyhľadávanie stretnutí na základe dôverného vzťahu z internetu, pričom zvyčajne ide o zámerné ovplyvňovanie dieťaťa dospelou osobou pre následné sexuálne zneužitie. Prejavuje sa bežnými aktivitami, ale i neobvyklým záujmom o dieťa, o jeho zvyky a súkromie, orientáciou na sexuálne podfarbené témy, zasielaním fotografií a videí s nemravným obsahom. Prevenciou je informovanosť o kontaktoch a aktivitách detí v digitálnom svete a bezvýhradné obmedzenie styku so známosťami z internetu a neznámymi osobami.
14. **Spam.** Je to nevyžiadaná hromadne rozoslaná správa. Môže byť distribuovaná cez sociálne siete alebo prostredníctvom e-mailu. Obsah zvyčajne nie je škodlivý, má reklamný, komerčný alebo informačný charakter. Môže mať aj reťazový charakter, ak sa samotní adresáti podieľajú na jeho ďalšom rozosielaní. Ochranou je antispamový filter a aktualizácia zoznamu spamových adries (z ktorých je spam najčastejšie šírený).
15. **Hoax**. Je falošná, podvodná, poplašná a zavádzajúca nevyžiadaná správa alebo kanadský žart. Často je to reťazový e-mail, ktorý mnohí používate-

lia z rôznym zámerom posielajú ďalej (pre zábavu, zo súcitu, v snahe niekomu poradiť, z obavy, ktorú vyvolá časť správy a pod.). Zasielanie reťazových, nevyžiadaných správ nie je v súlade s etiketou. Adresátov obťažuje a sieť preťažuje. Najlepšou ochranou je zdravý úsudok a ignorovanie podobných správ. V prípade, že niekto podobné správy pravidelne na adresu zasiela, je vhodné ho na to upozorniť alebo zaradiť medzi spamové adresy. Skôr, ako podľahneme pokušeniu zaslať podobnú správu ďalej, skontrolujme, či sa nenachádza napríklad na hoax.sk alebo hoax.cz, kde sú podobné správy monitorované.

16. **Dialer.** Je program, ktorý s vedomím alebo bez vedomia používateľa mení parametre vytáčaného prístupu do internetu. Môže tak zneužívať pripojenie majiteľa takéhoto čísla (ohrození sú len tí, ktorí sú pripojení cez modem komutovanou linkou), pripojiť sa na zahraničné číslo alebo na audiotextové číslo. Dialer nainštaluje sám používateľ. Môže sa to stať pri bežnom surfovaní po webových stránkach a nevedomým odklikaním rôznych okien. Firmy touto cestou napríklad spoplatňujú obsah stránok.
17. **Backdoor**. Pôvodne si *zadné dvierka* nechávali programátori komerčných aj *free* desktopových a webových aplikácií za účelom vzdialeného (z iného počítača cez počítačovú sieť) prístupu na počítač. Ide teda o obídenie autentifikácie užívateľa v prihlasovacích formulároch (prihlásenie do počítača, e-mailu, aplikácie na internete...).
18. **Warez** (slangový výraz). Je to autorské dielo, s ktorým je nelegálne nakladané (ako príklad použime oskenované knihy sprístupnené v pdf na stiahnutie). Činnosť sa nazýva počítačové pirátstvo a týka sa napríklad počítačových hier, softvérov, filmov, hudby, elektronických kníh a pod. Používatelia, ktorí z takýchto *warez* zdrojov niečo získajú, sú často presvedčení, že ide o legálnu cestu. Vo väčšine krajín je táto činnosť nelegálna, niektoré krajiny ju prehliadajú alebo situáciu neriešia a v rozvojovom svete môže byť aj legálna. V každom prípade sú stránky, ponúkajúce *warez*, zdrojom malware.

19. **Cloud computing.** Princíp *počítačov v oblakoch* je jednoduchý: webová aplikácia nie je umiestnená na jednom serveri ale na *n* serveroch rozdelených naprieč svetadielmi. Výhodou je rýchlosť pripojenia – po zadaní google.com do adresného riadku sme presmerovaný na google.sk, t. j. aplikácia vyhľadávania je umiestnená na servery niekde blízko nás. Predpokladáme, že s masovým nástupom smartfónov (rýchlosť pripojenia na internet vzduchom je oproti metalickým alebo optickým káblom rádovo nižšia) sa *cloud computing* stane marketingovým hitom, avšak pre školské aplikácie typu učebných portálov význam neprinesie. Z hľadiska bezpečnosti dát na cloudových serverov je takéto decentralizované riešenie menej bezpečné – jeden server sa dá lepšie zabezpečiť ako *n* serverov.
20. **Geolokácia.** Umožňuje identifikovať geografickú polohu používateľa mobilného telefónu, počítača pripojeného k internetu a pod. Pokiaľ sa pri prihlásení na stránku objaví požiadavka na informácie o geolokácii (Google Location Services) je potrebné zvážiť, či súhlasiť alebo odmietnuť. Informácie o polohe, odoslané web stránky podliehajú zásadám súkromia tejto webovej stránky.
21. **Skenovanie elektronickej pošty.** Väčšina poskytovateľov webových hostingových služieb (na ich serveroch sú umiestnené webové stránky aj všetky e-maily) legálne skenuje poštu kvôli filtrovania spamu, detekcie vírusu, kontroly pravopisu, posielaniu automatickej pošty a pod. Podobné postupy niektorých portálov umožňujú na základe kľúčových slov vyhľadávať konkrétne obsahy, napríklad na marketingové účely. Podľa Európskej deklarácie ľudských práv je zachytávanie listov, ich otváranie, čítanie, resp. spôsobovanie ich oneskoreného príjmu príjemcom porušením ľudských práv. Preto sa skenovanie elektronickej pošty posudzuje z hľadiska jeho účelu.
22. **Využívanie informácií na sociálnych sieťach.** Umožňuje tretím stranám zneužívať informácie zverejnené na sociálnych sieťach. Ide o sociálne inžinierstvo bez osobného kontaktu so zneužívanou osobou.

23. **Cookies** (sušienky). Krátky text uložený do *cache* pamäte operačného systému, generovaný navštívenou webovou stránkou. Ak napr. nakupujeme v elektronickom obchode, sú do nich ukladané dáta o objednávaných položkách. Cookies nemôžu byť zneužité na šírenie malware. Keďže môžu byť čítané a modifikované (aj cookies, vytvorené inou aplikáciou), sociálni inžinieri môžu mať algoritmy na ich analýzu a zistiť z nich napr. aké stránky sú z počítača navštevované, aké výrobky sú preferované pri elektronických nákupoch a pod. Cookies sú užitočné a nie sú bezpečnostným rizikom. Možnosť zberu údajov v nich uložených sliedičom prekazíme ich občasným vymazaním v prehliadači cez Nástroje/Vymazať históriu prehliadania (so zaškrtnutými *cookies*).
24. **IP adresa.** Umožňuje identifikovať počítač po pripojení k internetu podľa jedinečného čísla. Práve preto zjednodušenie identifikácie používateľov cez IP adresy môže smerovať k narušovaniu súkromia. U poskytovateľov pripojenia, ktorí majú priamu možnosť zistiť identitu majiteľa pripojenia, by mali byť IP adresy osobným údajom.
25. **Podvodné lotérie.** Ide o rozposielanie e-mailov o výhre adresáta (vysoké finančné čiastky, dovolenky, automobily a pod.), pričom táto bude vyplatená za určitých podmienok. Zvyčajne je potrebná registrácia a určite sa žiada zaplatenie manipulačného poplatku, a to často opakovane. V žiadnom prípade netreba podľahnúť podobnému pokušeniu, ani keby za ním stál najznámejší filantrop. Hlavnou ochranou je antispamový filter a zdravý rozum.
26. **Nigerské listy (SCAM419).** Správy, oznamujúce nadobudnutie dedičstva, získanie majetku alebo finančnej čiastky. Cieľom sú podvodne vylákané poplatky súvisiace s administrovaním prevodu majetku. Ochrana spočíva v ignorovaní podobných e-mailov a aktuálnej antispamovej ochrane. V tomto prípade je treba mať na zreteli, že nič nie je zadarmo a najdrahšia je ľudská hlúposť.

27. **Pyramídové hry.** Vyzerajú celkom nevinne a majú mnoho podôb. Sú staré viac ako 70 rokov, teda ešte z dôb pred internetom. Sľubujú veľké zisky za získanie ďalších účastníkov hry, za vloženie základného vkladu alebo distribúciu tovarov a služieb zapojením ďalších osôb. Sľubujú napríklad získanie veľkej finančnej čiastky po zaplatení 100 eur a získaní ďalších troch účastníkov. Samozrejme nikto nič nezíska okrem organizátora. Internet dal hrám nové podoby. Sú to napríklad „klikačky“, ktoré pod zámienkou získania kreditov a následne finančného zisku nútia účastníkov klikať na niektoré reklamy a stránky a robia tak medvediu službu marketingu. Podobný účel plnia surfovacie banery, ktoré vás nútia celé minúty pozerať a klikať na reklamu, čím sa stávate obeťou lovcov milovníkov reklamy. Jediná ochrana je zdravý rozum a ignorovanie podobných aktivít.
28. **Kyberšikanovanie** (*cyberbullying*). Zámerné poškodzovanie iných osôb prostredníctvom informačných a komunikačných technológií. Ide o vypuklý problém virtuálneho sveta, lebo je neviditeľné, deje sa nekontrolovane, opakovane, verejne alebo v súkromí. Ten kto šikanuje, si môže na základe falošnej identity zachovať anonymitu a šikanovaný nemá šancu šikane uniknúť ani v domácom prostredí. Môže sa diať výsmechom, urážaním, zastrašovaním, vydieraním, ale aj iným nepríjemným spôsobom, napríklad zverejňovaním hanlivých alebo nepravdivých informácií v rôznych formátoch. Môže mať tiež podobu ukradnutej identity, kybernetického prenasledovania (*cyberstalking*) alebo videí o násilí a sexuálnych útokoch (*happy slapping*). Ochrana pred podobnými útokmi nie je jednoduchá, vyžaduje si okamžitú reakciu (je potrebné sa zdôveriť alebo šikanovanie nahlásiť), odložiť dôkazy a zamedziť pokračovaniu.
29. **Makrovírus.** V súčastiach kancelárskych balíkov môžu byť implementované programy (makrá), ktoré slúžia na automatizáciu činnosti týchto programov, čo je hlavne v rozsiahlejších excelovských tabuľkách veľmi vhodné. Makro sa dá zneužiť – odstrániť ním súbor na pevnom disku nie

je problém. Ochrana proti makrovírusu je jednoduchá – povoľte použitie makier len v súboroch, ktoré pochádzajú z dôveryhodného zdroja.

2 Bezpečný internet

„*Zkušenost je dobrá škola, ale školné je příliš drahé*“ (Karel Čapek).

Využívanie elektronickej pošty, diskusných fór a sociálnych sietí je súčasťou každodenného života mladých ľudí. Tieto komunikačné nástroje priťahujú aj populáciu, ktorá nevyrastala v ére boomu informačných technológií. Práve kategória mladých a neskúsených ľudí si často neuvedomuje riziká spojené so zverejňovaním rôzneho druhu osobných informácií. Nikto z nich nechce na verejnom mieste do mikrofónu rozprávať o svojich problémoch, premietať súkromné video alebo ukazovať svoj album, ale mnohí z nich to bez akejkoľvek zábrany urobia na internete.

Z prieskumu medzi deťmi vyplynulo, že väčšina z nich by vlastné fotografie zverejnené na internete neukázala svojim rodičom. A možno aj mnohí dospelí nechcú, aby fotografie, ktoré zverejnili na internete, videli ľudia z ich najbližšieho okolia. Rovnako ako deti aj dospelí na základe výzvy bez váhania uvedú svoju adresu, telefónne číslo a v horšom prípade aj informácie týkajúce sa bankového účtu. Necítia sa ohrození, keď verejne uvádzajú dátum a miesto svojej dovolenky, popisujú svoje zvyky, ponúkajú na obdiv moderné zariadenie bytu alebo nebodaj zaujímavé informácie zo života rodiny a priateľov. Ak si aj uvedomujú dôvernosť týchto informácií, často predpokladajú, že sú schopní zabrániť ich zneužitiu.

Deti by sa mali už v škole naučiť ako narábať s digitálnymi informáciami, aby sa nedali zneužiť. Je to jeden zo spôsobov, ako ich upozorniť na význam obozretnosti, vychovať ich k zodpovednosti voči sebe a iným a šíriť osvetu aj medzi dospelou populáciou.

2.1 Technické aspekty informačnej spoločnosti

Charakteristickým znakom informačnej spoločnosti je jej závislosť na informáciách. Informácie môžu byť uložené rôznymi spôsobmi, napr. v knihách, magnetických páskach alebo, a dnes v prevažujúcej forme, na diskoch počítačov v binárnej forme. Počítače sú poprepájané navzájom v počítačových sieťach – internete. Vzájomná fyzická prepojenosť rôznych informačných úložísk dáva priestor na ich potenciálne zneužitie. V komerčnej oblasti na získanie plánov nového pohonu automobilu, v emocionálnej oblasti na vydieranie, v intelektuálnej oblasti na vykrádanie myšlienok druhých. Informačná spoločnosť pokladá informácie za motor svojho rozvoja a preto ich treba zabezpečovať. Očakávaným ale dlhodobým prechodom k znalostnej spoločnosti sa do popredia záujmu opäť dostane človek – jeho znalosti, schopnosti vedomosti, jeho know-how. Uvidíme, ako na tento trend zareagujú súčasní crackeri.

„*Moc v dnešním světě se přesouvá od lidí, kteří dříve kontrolovali informace k lidem, kteří kontrolují poznání*“ (Jonas Ridderstrale).

Bezpečnosť informácií v školskom prostredí z **technického hľadiska** zabezpečíme:

- Pravidelne kontrolovať používané zariadenia.
- Priebežne archivovať staré súbory.
- Pravidelne robiť antivírusovú kontrolu, vždy aj v externých zariadeniach (kľúč, harddisk a pod.).
- Na neznámych a nebezpečných miestach mať počítač (mobil) vždy na očiach.
- Poznať riziká nabúrania sa do počítača, telefónu alebo webkamery.

Z hľadiska softvéru:

- Priebežne aktualizovať verzie antivírusového programu.
- Pre distribúciu softvéru využívať len oficiálne servery.

- Využívať len legálne zakúpený alebo dostupný softvér.
- Spúšťať len overený softvér, nie neznáme programy, ktoré sú pripojené v e-mailoch.
- Nerozosielať hromadne zasielané e-maily s prílohami.
- Nastaviť dostatočný stupeň ochrany na fórach, chatoch, blogoch a v pošte.
- Kvalitný *firewall*.
- Aktualizovať využívaný operačný systém.

Z hľadiska informácií:

- Pristupovať opatrne k sťahovaným informáciám.
- Overovať si hodnovernosť zdrojov.
- Rozvážne pristupovať k zverejňovaniu videí, fotografií a akýchkoľvek súkromných informácií.
- Využívať bezpečnejšie formáty pri zverejňovaní informácií.
- Voliť si vhodné miesta na zverejnenie citlivých informácií.
- Nezverejňovať o sebe viac údajov, ako je nevyhnutné.
- Rešpektovať Zákon o ochrane osobných údajov.
- Neveriť vyhrážkam o tom, že v prípade nerozoslania e-mailu ďalším osobám nastane niečo negatívne (je to len psychologické vydieranie).
- Dbať na správnu tvorbu a používanie hesiel.
- Rozlišovať využívanie verejného a domáceho počítača.
- Poznať následky plagiátorstva a porušenia *copywrite*.
- Využívať filter na nežiaduci obsah alebo poštu.
- Neotvárať a nerozosielať poštu s neznámym, neslušným, zbytočným alebo škodlivým obsahom.
- Nevstupovať do pošty, počítača či telefónu inej osoby bez jej vedomia.

Z personálneho a etického hľadiska:

- Rešpektovať netiketu.

- Zásadne dodržiavať spoločenské a legislatívne normy.
- Dbať na ochranu identity.
- Zvážiť, s kým a o čom komunikovať.
- Overovať si dôveryhodnosť kontaktovaných osôb.
- Nepovažovať za priateľov neznámych ľudí z virtuálneho sveta.
- Brať na vedomie to, že profily neznámych osôb nemusia byť pravdivé.
- Nestretávať sa individuálne (osobne) s neznámymi osobami z internetu.
- Predvídať možné nekorektné konanie osôb, ktoré majú prístup k informáciám.
- Prezieravo sa správať k návrhom na zapojenie sa do skupinových aktivít.
- O podozrivých informáciách a nebezpečných situáciách hovoriť s blízkymi alebo odborníkmi.

Zjednodušme uvedené informácie na tieto **najzákladnejšie pravidlá**. Ich dodržiavaním eliminujeme 98 % bezpečnostných rizík.

1. Aktualizujme pravidelne (1 x za týždeň) operačný systém.
2. Komunikujme bezpečne pomocou https (secure) protokolu.
3. Používajme silné heslá (pozri ďalej).
4. Aktualizujme automaticky vírusovú databázu antivírusového programu a nechajme ho pracovať rezidentne (na pozadí, keď automaticky kontroluje dáta vstupujúce na lokálny pevný disk).
5. Aktualizujme používané prehliadače.
6. Buďme rozumní a opatrní, nepodceňujme možnosti malware.
7. Nespúšťajme neznáme súbory ani nevyžiadané prílohy e-mailov.
8. Neplaťme a nenakupujme na verejných počítačoch alebo s verejným wifi pripojením na internet.
9. Nepripájajme sa na stránky s pochybným obsahom.
10. Používajme minimálne *firewall* operačného systému.

Všeobecné rady:

Po pripojení na internet sa mnoho ľudí cíti ako v paralelnom svete, kde sa deje to isté, čo v reálnom. Stretnú sa tam s ľuďmi, ktorých majú často zidealizovaných napriek tomu, že ich nepoznajú, diskutujú s nimi, hádajú sa s nimi, zabávajú. Spôsob komunikácie často presahuje rámec komunikácie v reálnom živote. Príležitosti na nadväzovanie kontaktov sú často jednoduchšie ako v reálnom živote a je ich oveľa viac. Viac ako dospelých takéto vnímanie virtuálneho sveta ovplyvňuje deti, u ktorých to môže mať vplyv aj na psychický vývin. Najlepšiu príležitosť pôsobiť na deti majú dospelí, ktorí môžu týmto spôsobom ovplyvniť mravný vývoj a bezpečnosť detí a výchovne na ne pôsobiť. Preto je potrebné, aby dospelí v okolí detí venovali tejto problematike maximálnu pozornosť.

Dospelí by sa mali riadiť odporúčaniami, ktoré vyplynuli z praxe a odporúčaní odborníkov. Patria k nim napríklad:

- Vhodným spôsobom poučme deti o pravidlách správania sa na internete o zodpovednej komunikácii vo virtuálnom svete. Naučme deti chrániť si súkromie, používať heslá, prezývky a chrániť svoju identitu. Vysvetlime im, čo je netiketa, autorské právo, ochrana údajov, ktorá sa týka nielen ich, ale aj ostatných osôb a pod.
- Pri prvej príležitosti ich upozornime na to, čo môže byť pre nich zaujímavé, aké sú možnosti zábavy, ale poukážme aj na negatívne stránky. Vysvetlime im, že okrem potešenia a zábavy ponúka internet aj mnoho zaujímavostí a príležitostí na vzdelávanie.
- Sledujme kedy, kde a koľko času trávia deti na internete a vo virtuálnom svete. Na každý vek je odporúčaná iná dĺžka času – čím je dieťa staršie, tým môže byť čas dlhší. Pre malé deti je vhodný čas okolo 30 minút. Viac ako 2 hodiny súvisle by nemali sedieť za počítačom ani staršie deti. Nedovoľme, aby virtuálny svet nahradil bežné činnosti v reálnom svete, aby sa dieťa stalo závislým od virtuality.

- Dohodnime si s deťmi pravidlá, ktorými určíme ako dlho, v akých intervaloch a kedy budú tráviť čas na internete. Rovnako stanovíme obsah, ktorý je pre deti vhodný a ktoré stránky nebudú navštevovať. Dohodnime sa, aké údaje môžu bez nášho súhlasu na internete používať, ktoré je potrebné odsúhlasiť a ktoré nie je možné prezerať v žiadnom prípade.
- Počítač umiestnime na mieste, ktoré je bežne dostupné, najlepšie s možnosťou výhľadu na monitor.
- Snažme sa mať prehľad o tom, čo robia deti na počítači, či sa okrem komunikácie s virtuálnymi priateľmi zaujímajú aj o niečo iné, či využívajú čas aj na vzdelávanie.
- Sporadicky kontrolujme obsah, s ktorým deti prichádzajú do styku (prehľad o navštívených webových stránkach, stiahnutých softvéroch, uložených súboroch (textoch, obrázkoch, videách, zvukoch). Kontrolujme diskusné skupiny, chaty, blogy a sociálne siete, na ktorých sa dieťa pohybuje – dôležitá je primeranosť veku, obsah a čas strávený touto činnosťou.
- Poučme deti o rôznych rizikách, ktoré sú vo virtuálnom svete. Patrí k nim násilie, drogy, pornografia, nebezpečné ideológie, finančné pasce a pod.
- Upozornime ich na rozdiel medzi využívaním domáceho a verejného počítača.
- Poraďme im, ako sa majú v možných rizikových situáciách správať.
- Otvorene a so záujmom komunikujme s deťmi o internete. Požiadajme ich, aby nám ukázali čím sa zaoberajú – prejavme o to záujem. Zdieľajme spolu prehliadače a profily. Získajme si ich dôveru, ktorá nám umožní prirodzene sledovať aktivitu detí na internete.
- Vysvetlime deťom aj pravidlá a riziká súvisiace s e-mailovou komunikáciou. Diskutujme s nimi o tom, kto je odosielateľom a adresátom správ, o spôsobe komunikácie, o prijímaní a rozosielaní príloh a o možnom nebezpečnom obsahu správ. Dohodnime sa s nimi, že budú s nami konzultovať podozrivé e-maily a nevyžiadané e-maily od cudzích odosielateľov. Nastavme im pravidlá filtrovania nevyžiadanej pošty.

- Sledujme informácie na špecializovaných webových stránkach, v médiách o škodlivých javoch súvisiacich s digitálnymi technológiami.
- Zaujímajme sa o osoby, priateľov detí z virtuálneho sveta – hovorme o tom, s kým sa rozprávajú, komu niečo posielajú, s kým sa kontaktujú na sociálnej sieti. Upozornime ich na to, že na internete môžu natrafiť aj na ľudí so zlými úmyslami. Nedovoľme deťom stretnúť sa so známosťou z internetu bez dozoru, resp. osamote, na neznámom mieste a pod.
- Ak náhodou objavíme nebezpečný obsah alebo kontakty svojich detí, venujme im pozornosť, snažme sa riešiť problém komunikáciou s deťmi, alebo inými účinnými spôsobmi. Zákaz počítača zvyčajne nie je riešením situácie. Nástrahy číhajú aj mimo nášho dosahu.
- Nainštalujme do počítača programy, ktoré dokážu obmedziť dostupnosť stránok s nevhodným obsahom, prípadne dokážu kontrolovať obsah elektronickej komunikácie.
- Buďme opatrní pri používaní obsahu, ktorý je síce vhodný, potrebný a zaujímavý pre Vás, ale škodlivý alebo nebezpečný pre deti.
- Kontrolujme aj obsah hier, ktoré majú deti v počítači alebo v telefóne, alebo sa ich hrajú online na internete. Na posúdenie vhodnosti využime ratingové systémy, ktoré zverejňujú recenzie hier a upozorňujú na nevhodný obsah (napr. www.pegi.info/cs/index/id/956).
- Nikdy deti netrestajme alebo nekarhajme za to, čo sa nám zdá podozrivé alebo nebezpečné. Strata dôvery by mohla znamenať, že v budúcnosti riziká neodhalíme.

Pri podozrení sa poraďme s odborníkom (psychológ, pedagóg, psychiater, skúsený špecialista na informačné systémy), prípadne na linke dôvery (napr.: portal.gov.sk, www.linkadeti.sk, www.unicef.sk a pod.). Napriek tomu, že sú tam odborníci, ktorí vedia poradiť, špeciálne linky dôvery zamerané na riziká súvisiace s informačnou bezpečnosťou zatiaľ (žiaľ) nie sú na Slovensku zriadené.

Zjednodušene by sa dali uvedené informácie zhrnúť do **desiatich základných pravidiel pre rodičov**:

- Hovorme s deťmi o tom, čo pozitívne, zábavné, ale aj negatívne internet ponúka.
- Upozornime deti na potrebu informačnej bezpečnosti, význam hesiel a ochranu osobných údajov.
- Diskutujme s deťmi o zásadách netikety a potrebe zodpovedného správania sa.
- Zoznámme deti s nebezpečenstvom, hrozbami a možnými kriminálnymi aktivitami a poučme ich o tom, ako sa majú v podobných prípadoch správať.
- Hovorme s deťmi o tom, čo, kde a kedy na internete robia, budujme si u nich dôveru.
- Dohodnime si s deťmi pravidlá, koľko času budú tráviť na internete, aby mali dosť času aj na iné aktivity. Kontrolujme dodržiavanie pravidiel.
- Komunikujme s deťmi o priateľoch a iných osobách, s ktorými sa na internete kontaktujú.
- Zamedzme tomu, aby deti bez nášho vedomia osobne kontaktovali priateľov z internetu.
- Používajme internet. Naučme sa robiť s počítačom a modernými technológiami, ktoré dieťa využíva.
- Problémy riešme uvážene, v spolupráci s dieťaťom. V prípade podozrenia kontaktujme odborníkov.

Niekoľko pravidiel pre voľbu hesiel:

- **Nepoužívajte na rôzne účely to isté heslo.** Pokiaľ máte pracovnú aj súkromnú e-mailovú adresu, profil na sociálnej sieti, elektronické bankovníctvo, prístup na rôzne portály, obchodujete na internete a využívate ďalšie kontakty prostredníctvom internetu, kde sa vyžaduje heslo, zvoľte si rôzne heslá. Mať desiatky adries s desiatkami hesiel vyžaduje dobrú

pamäť a tiež ochranu pred zneužitím. Mali by sme odlíšiť tie heslá, ktorých ochrana podlieha osobitnej ochrane (napríklad elektronické bankovníctvo). Takéto heslo sa používa výhradne na tento účel. Preto jedno heslo nepoužívame viackrát. Pri menšom počte hesiel môžeme pre ľahšie zapamätanie použiť jednoduché obmeny – napr. *1NoYe_25x%* a *2NoYe_25y%* – zmenila sa *1* na *2* a *x* na *y* alebo *MpXr_36c%* – písmená a čísla sa na klávesnici posunuli o jednu pozíciu doprava.

- **Nepoužívajte ako heslo jednoduché slová.** Ak nechcete, aby heslo, ktoré používate, nikomu len tak ľahko nenapadlo, nepoužívajte najmä tie slová, ktoré akokoľvek súvisia s vašou osobou**.** Nie je správne ako heslo použiť meno svojho miláčika – napr. *Murko*, alebo miesta, ktoré vám je blízke – napr. *Borčice*, mená obľúbených celebrít – napr. *Messi*, slová označujúce príbuzných – napr. *mamina*, *Zuzulka*, dátumy narodenia – *11121989* alebo *11dec89*, obľúbené jedlá – napr. *palacinky*. Kto o vás niečo vie, ľahko takéto heslo vydedukuje. Dnes už ani bežné slová zo slovníka nie sú považované za bezpečné – napr. *student*, *lyzovacka*. Na prelomenie hesla potom crackerovi stačí slovník.
- **Nepoužívajte krátke heslá.** Dávnou minulosťou je doba, keď sa ako heslo požívali štvormiestne heslá. Mnoho portálov takéto heslá už dnes neakceptuje. Často pri zadávaní hesla môžeme sledovať ukazovateľ jeho bezpečnosti, a tak si podľa vlastného uváženia bezpečnosť zvýšiť. Heslo by malo mať **šesť a viac znakov**. Ani takéto heslo crackerom dlho neodolá. Pokiaľ heslo chráni dôležité údaje, malo by mať **viac ako 10 znakov**. Odborníci hovoria, že crackeri na prelomenie hesla so 14 pozíciami potrebujú viac ako 24 hodín. Našťastie naše údaje nie sú stredobodom ich záujmu a pozornosti.
- **Použite v hesle okrem písmen a číslic aj nealfanumerické znaky.** V žiadnom prípade nepoužívajte písmená v abecednom poradí, vzostupne alebo zostupne zoradené čísla alebo iné jednoduché zoskupenia čísel a písmen – napr. *ABC123*, *asdfgh*, *qwerty*, *13579*. Bezpečnosť hesla sa

zvyšuje kombináciou čísel a písmen, pričom použijeme aspoň jedno veľké písmeno. Ešte vyššiu bezpečnosť si zabezpečíme, ak použijeme iné znaky okrem písmen a čísel (#, $, !, &) – napr. H78x9_f4%. Náhodne naťukané šesťmiestne heslo kombinované z písmen, čísel a znakov je spravidla veľmi bezpečné, horšie to je s jeho zapamätateľnosťou. Je vysoko pravdepodobné, že cracker odhalí heslo vytvorené z 8 čísel asi za 10 sekúnd, heslo z písmen a čísel za 253 dní a v prípade, že sa použije aj špeciálny znak, trvalo by mu to až 23 rokov.

- **Pravidelne meňte svoje heslá.** Heslo slúži na ochranu informácií, preto by ste mali predchádzať riziku jeho odhalenia aj tým, že ho pravidelne meníte. Niektorí správcovia systému vyžadujú pravidelnú zmenu hesla napríklad raz mesačne, raz za pol roka a pod. – zvyčajne to závisí od dôležitosti údajov, ktoré heslo chráni. Na to, aby ste si svoje údaje chránili, nepotrebujete správcu, heslo si podľa uváženia môžete meniť sami – určite ho nenechávajte bezo zmeny celé roky.
- **Používajte vlastný systém vytvárania hesiel.** Profesionáli pri ochrane dôležitých informácií od nepamäti používali rôzne kódovanie a šifrovanie. Pre takéto účely vytvárali odborníci zložité systémy, aby ochrana bola čo najdokonalejšia. Každý si môže vymyslieť vlastný systém, ktorý mu pomôže heslá vytvárať, meniť a navyše si ich aj zapamätať. Heslo môže byť usporiadané podľa určitého systému, ktorý predpokladá aj jeho pravidelnú aktualizáciu, napr. obľúbený slogan, z ktorého vyberiete určité písmená, spojíte ich s obľúbeným číslom alebo príslušným rokom a zvoleným znakom – napríklad v roku 2013 môžete z príslovia „Aká matka, taká Katka“ urobiť nasledovné dve heslá pre 1. a 2. polrok – zložitejšie: *1_Am13-tK* a *2_Am-tK13* alebo jednoduchšie: *1_AmtK13* a *AmtK13_2*. Také heslo si určite zapamätáte a jeho bezpečnosť je pomerne vysoká. Pre milovníkov matematiky, chémie a iných vied môžu byť základom systému vzorce, rovnice, rôzne názvy alebo osobnosti. Práve takáto pomôcka môže byť dostatočne rafinovaná, aby ste vytvorili bezpečné, ľahko zapamätateľné

heslo s možnosťou pravidelnej zmeny. Pre tých, ktorí nemajú chuť vymýšľať vlastné systémy na tvorbu hesiel slúžia manažéri hesiel – softvér, ktorý generuje jednorazové heslá pre rôzne systémy. Napriek tomu, že bývajú na rôznych bezpečnostných konferenciách spochybňované, v praxi sa bežne využívajú – napríklad LassPass, AgileBits alebo SplashData.

- **Heslá patria na bezpečné miesto.** Najbezpečnejšie miesto na uloženie hesiel je vlastná hlava. Pri dnešnom počte adries, ktoré majú na prístup rôzne heslá, to vždy nie je možné. Heslá ale určite nepatria do e-mailovej schránky alebo voľne dostupného priečinka v počítači a na jeho plochu. Ak máte heslá uložené v samostatnom súbore, mal by byť uložený mimo počítača, na niektorom záložnom disku alebo kľúči, ktorý bežne nie je dostupný tretím osobám. Heslá môžu byť v zápisníku, na papieri, na vyhradenom mieste, v telefóne – dôležité je, aby neboli nikomu dostupné. Najmä tie, ktoré si pozornosť z hľadiska bezpečnosti mimoriadne zaslúžia. Pokiaľ si dokážete uložiť jednoduchú pomôcku na tvorbu hesla, nie sú konkrétne heslá vystavené takému riziku odhalenia. Heslo k elektronickému bankovníctvu nepatrí k bankovej karte, ani k číslu bankového účtu, rovnako, ako nepatria heslá k príslušným e-mailovým adresám.
- **Viacstupňové overovanie prístupov.** V prípade, že máte záujem, alebo je nastavená vyššia ochrana, ponúkajú vám niektoré systémy na ochranu dát okrem hesla aj ďalšie overenie – napríklad zaslanie SMS správy o použití schránky, overenie niektorých informácií priamo na webe, alebo zadanie zaslaného overovacieho kódu. Takzvané bezpečnostné otázky, ktoré na tento účel slúžili v minulosti, sa už dnes nepovažujú za bezpečné a nie je potrebné na ne odpovedať – zvyčajne išlo o meno matky za slobodna, názov školy, obľúbeného herca, film, jedlo a pod. (tieto údaje sa dajú jednoducho zistiť, alebo ich po čase zabudne sám zadávajúci).
- **Heslo vieme jednoducho zapísať.** Pri písaní hesla je dôležité, aby sme nepotrebovali pomôcky v podobe ťahákov, aby sme ho vedeli napísať plynule, rýchle, podľa možnosti v rôznych častiach klávesnice, najlepšie

oboma rukami. Tak sa vytvoria predpoklady, aby sa heslo nedostalo do cudzích rúk, nedalo sa prečítať ani odpozorovať pri písaní nepovolanou osobou. Nikdy si heslo nehovoríme nahlas.

Menej známe ale dôležité aspekty sieťovej komunikácie:

- **Voľba** prehliadača **ovplyvňuje bezpečnosť.** Pre bežného človeka nie je obvyklé využívať v prístupe na internet rôzne prehliadače. Práve preto zavedenie takéhoto zvyku zvyšuje bezpečnosť na ochranu citlivých údajov. Ak používame na pripojenie sociálnej siete alebo čítanie jeden prehliadač, tak na pripojenie internetu, dôležitej poštovej schránky alebo na internetového obchodu použime iný. Je tiež dobre sledovať na internete informácie o bezpečnosti prehliadačov. Za rok 2011 uvádza štúdia Accuvant Labs spomedzi prehliadačov ako najmenej náchylný na útoky prehliadač Google Chrome.
- **Vplyv zdieľania na bezpečnosť.** Rôzne marketingové taktiky firiem získavajú pod rôznymi zámienkami od používateľov e-mailové adresy a heslá. Práve na takéto účely je dobré mať zriadenú anonymnú alebo dočasnú e-mailovú adresu. Pri zverejnení bežnej e-mailovej adresy vám do nej začnú okrem reklamných ponúk a dotazníkov danej firmy chodiť aj spamy, ďalšie ponuky a návrhy. Stáva sa to práve pre nedostatočnú ochranu poskytnutej adresy. Od takýchto nekalých ťahov nie je ďaleko k preniknutiu informácií o vás na verejnosť alebo k odhaleniu vášho hesla. Na jednorazové používanie e-mailovej adresy, napríklad na registráciu do fóra, pri sťahovaní informácií a podobne je užitočnejšie ochrániť svoju identitu práve dočasnými e-mailovými schránkami, ktoré sa dajú založiť bez registrácie a ich životnosť je niekoľko minút alebo hodín. Na príslušnom portáli, ktorý túto službu poskytuje, sa zdarma vygeneruje dočasná adresa, na ktorú je možné dostať očakávanú informáciu. Príkladom je www.emailnachvilku.cz, www.guerrillamail.com, www.tempinbox.com alebo www.10minutemail.net. Podobnú službu plní tzv. metamail

(www.metamail.com), ktorý umožní počas stanoveného času zasielať určité informácie priamo na váš e-mail bez jeho zverejnenia – napríklad zaujímavé články, ponuky a pod. Po uplynutí doby takto vytvorený metamail (lubovolny@metamail.co) zanikne a správy prestanú prichádzať. Napriek všetkým uvedeným opatreniam je vždy treba mať na zreteli to, že všetko, čo je uverejnené na internete, vrátane e-mailových správ a príloh, sa za určitých náhodných alebo zámerných postupov môže dostať na verejnosť.

- **Pri poskytovaní osobných údajov buďte obozretní.** V osobnom styku nezverejňujeme svoju adresu komukoľvek na počkanie. Ak ju aj niekomu povieme, určite mu nedáme kľúč, aby mohol kedykoľvek vstupovať do nášho súkromia. Rovnako sa treba správať k vlastnej e-mailovej adrese a heslu, ktoré sú kľúčom k našej pošte. Overte si dôveryhodnosť stránok, na ktorých pri registrácii poskytujete svoje údaje. Poskytujte len tie údaje, ktoré sú na registráciu nevyhnutné (označené hviezdičkou). Pred zaškrtnutím políčka, ktorým vyjadrujete súhlas s podmienkami (OK, Áno, Súhlasím...), si informácie pozorne prečítajte. Ešte vyššiu opatrnosť si vyžaduje zverejnenie domácej adresy, fotografie, osobných údajov, čísla bankomatovej karty alebo iných citlivých údajov, ktoré môžu byť zneužité.

3 Bezpečnosť pri práci s informáciami

3.1 Zdroje informácií

Internet ako vzájomné prepojenie lokálnych počítačových sietí je v súčasnosti najvyužívanejším informačným zdrojom. Dôvodom je vysoká rýchlosť prístupu k informáciám za takmer nulovú cenu. Internetom poskytované informácie môžeme hodnotiť z hľadiska viacerých kritérií:

1. **Presnosť.** Kvalita informácie je daná jej presnosťou. Relatívne ju vieme overiť komparáciou s inými zdrojmi alebo vlastným skúmaním. Verifiko-

vať informáciu z internetu iným komparačným zdrojom na internete je rýchle a pohodlné, ale presnosť získanej informácie tým nezvýšime. Prijateľnejšou možnosťou získania informácie sú podpísané internetové zdroje, kde je meno autora aspoň malou zárukou *chcenej* presnej informácie. Informácie, ktoré majú rozhodovať o našom správaní, postojoch alebo majú byť východiskom pre naše závažné rozhodnutia dôrazne neodporúčame získavať z internetu.

2. **Aktuálnosť.** Len v danom čase aktuálna informácia je použiteľná. Najpoužívanejší vyhľadávač má vo svojich *Search tools* (Vyhľadávacie nástroje) možnosť filtrovať webové stránky podľa dátumu poslednej aktualizácie. Zobrazené stránky nie vždy reflektujú nastavené hodnoty. Ak by internet existoval v dobe Mikuláša Kopernika, geocentrizmus by stále bol alternatívou heliocentrizmu. Internet je plný odpadu, ktorý nikto nevynáša.

Internet je vynikajúcim nástrojom na zorientovanie sa v problematike, ale na získanie hlbších vedomostí odporúčame využívať knihy, vlastný výskum a poznávanie.

3.2 Hodnovernosť poskytovateľa

Kredibilita (hodnovernosť) poskytovateľa informácií na internete je dôležitá hlavne v edukačnom procese. Moderné vyučovanie, založené na interaktivite a názornosti, musí internet používať ako svoju multimediálnu platformu na ktorej sú umiestnené presné a aktuálne oficiálne učebné materiály pre všetky typy škôl. Dôsledky by boli ťažko napraviteľné. V prípade edukačných materiálov pre základné a stredné školy by mala byť ich presnosť a aktuálnosť overená autoritami z radov vysokých škôl a zamestnávateľských zväzov a relevantnosť štátnymi inštitúciami v kompetencii ministerstva školstva.
Dôveryhodné informačné zdroje poznáme podľa nasledovných znakov:

- **Identifikácia autora.** Zdroj uvádza plné meno autora, jeho adresu, telefón, fotografiu. Autor sám seba jasne identifikuje čo zvyšuje záruku, že poskytuje hodnoverné informácie.
- **Citácie a použitá literatúra.** Zdroj, ktorý obsahuje citácie a správne štruktúrovaný zoznam použitej literatúry (známych autorov) je hodnovernejší ako zdroj postavený len na autorových myšlienkach.
- **Doména.** Ak je informačný zdroj uložený na doméne *free hostingového providera*, pravdepodobne sa autor schováva za anonymitu takéhoto pripojenia.
- **Text.** Dodržiavanie pravidiel pravopisu, štylistika a formálna úprava textu, uvedenie abstraktu a kľúčových slov zvyšuje v čitateľovi dojem hodnovernosti zdroja.
- **Webová stránka.** Informačný zdroj, uložený na graficky príjemnej stránke bez reklamy (alebo s neagresívnou reklamou), s hierarchickým a jednoduchým ovládaním, bez potenciálneho malware, zameraný len na určitú špecifickú problematiku sú atribúty dôveryhodného zdroja informácií.
- **Diskusia k informáciám.** Myslíme si, že diskutovať o zverejnených informáciách nie je pre hodnoverné zdroje vhodné. Každá diskusia vnáša do uceleného zdroja snahu o jeho negáciu, čo je v štádiu tvorby zdroja potrebné, ale po jeho zverejnení kontraproduktívne.
- **Netiketa.** Autor, ktorý prezentuje myšlienky iných ako svoje vlastné porušuje zákon a odsudzuje samého seba do zabudnutia.

3.3 Spracovanie informácií

Proces práce s informáciami pokračuje ich spracovaním. Pri výbere softvéru na prácu s informáciami sa musíme riadiť predovšetkým kritériom bezpečnosti. Aké programové vybavenie môžeme považovať za bezpečné?

1. Operačný systém môžeme považovať za bezpečný vtedy, ak je legálny a aktualizovaný. Legálnosť systému na neznámom lokálnom počítači si

vieme overiť jeho aktualizáciou. Ak je schopný prijímať aktualizácie z lokality Windows Update (Štart/Všetky programy/Windows Update), je legálny. Nelegálny (kreknutý) operačný systém je potenciálnou vstupnou bránou malware a keďže nie je možná jeho aktualizácia, nebezpečenstvo napadnutia sa zvyšuje.

2. Pre aplikačné programy platí to isté čo pre operačný systém. Ich legálnosť na neznámom počítači si síce overiť nevieme, ale podľa jeho správania (nestabilný chod, upozornenia o nutnosti zadania kódu a pod.) vieme je pravosť predpokladať.
3. Pomocné programy (komprimačné programy, multimediálne prehrávače, free editory, archivačné programy...) bývajú najčastejšou bránou pre malware, pretože ponúkajú nadštandardné možnosti na spracovanie informácií. Keď sa rozhodneme využiť ich, stiahnime ich z dôveryhodného zdroja (t.j. z pôvodnej stránky výrobcu tohto softvéru).

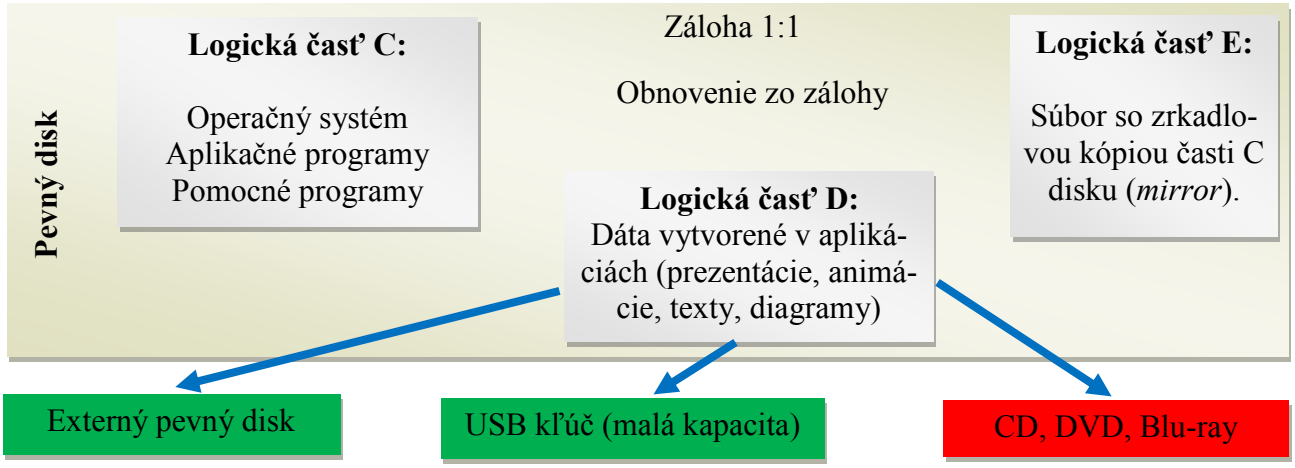
3.4 Ochrana, ukladanie, prenos a archivácia údajov

Aplikačným softvérom spracované (alebo vytvorené) informácie sú dáta, ktoré treba chrániť, pretože tie sú našimi autorskými výtvormi (aplikačný softvér máme na inštalačných médiách). Na ich ochranu platí jediné pravidlo: zálohovať! Ak dáta zálohujeme, žiadna hrozba zvonku nie je nebezpečná (vzhľadom na ohrozenie spracovaných informácií, iné nebezpečenstvá teraz nerozoberáme). Pri zálohovaní postupujme vždy nasledovne:

1. Dáta vytvárajme vždy na časti D pevného disku (nikdy nie v adresári Dokumenty, ktorý je súčasťou časti C pevného disku, na ktorom sa nachádza aj operačný systém.
2. Po každej významnejšej zmene dátového súboru ho ukladajme na externé pamäťové médium. Použime na to externý pevný disk alebo USB kľúč. Dátové úložiská na internete sú len prechodným riešením, keď nemáme

externý disk k dispozícii – potenciálne hrozí nebezpečenstvo ich zneužitia. CD, DVD alebo Blu-ray disky sú tiež použiteľné len ako časová náhrada externého pevného disku, pretože čas uchovania informácii na nich nepresahuje pri bežnom používaní niekoľko rokov.

3. Systém ukladania údajov by mal byť na všetkých žiackych aj učiteľských počítačoch rovnaký a zaisťujúci maximálnu bezpečnosť dát. Odporúčame ukladanie, uvedené na obrázku 3.



Obrázok 3 Správne rozdelenie softvéru na pevnom disku

Postup: Administrátor, ktorý inštaluje operačný systém, rozdelí pevný disk na logické časti C, D a E. Po jeho inštalácii a spustení nainštaluje všetky potrebné aplikačné programy – kancelársky balík, CAD systémy, grafické programy... a pomocné programy – antivírusový program, internetové prehliadače, komprimačné programy... Po vyskúšaní funkčnosti nainštalovaného softvéru cez lokalitu Windows Update aktualizuje operačný systém, aktualizuje všetky prehliadače a vírusovú databázu antivírusového programu. V konfigurácii antivírusového programu potvrdí možnosť automatickej aktualizácie vírusovej databázy a rezidentný spôsob ochrany (býva prednastavené).

Následne cez Ovládacie panely/Záloha a obnova vytvoríme kópiu celej logickej časti C disku (aj s nainštalovaným softvérom). Umiestniť ju môžeme na inú logickú časť – napr. E, ktorú sme na tento účel pripravili. Negatívum takéhoto riešenia je nemožnosť spätnej obnovy systému v prípade poruchy

pevného disku. Výhoda, hlavne v školách je, že administrátor má *image* na obnovu okamžite k dispozícii a obnova je relatívne rýchla.

Obraz môžeme umiestniť aj na USB kľúč (pravdepodobne nebude mať dostatočnú kapacitu), na externý pevný disk alebo dokonca na dátové úložisko na internete (významný dôvod na využitie takejto služby neexistuje). Umiestnenie *image* na médium mimo počítač je vhodné aj vtedy, keď máme problém s rozdelením disku na tri logické časti – časť E nám nahradí priestor na externom médiu.

Výhoda riešenia: Ak nám malware napadne počítač, bude jeho cieľom časť disku s programami (nie s dátami). Antivírusový program nám škodlivý softvér pravdepodobne lokalizuje a odstráni. Ak sa tak nestane, našou jedinou možnosťou ako malware z disku odstrániť, je *formátovanie* disku a následná inštalácia operačného systému a všetkých programov. Naše riešenie je oveľa efektívnejšie – spustíme systém z inštalačného média (pozor na správne zoradenie bootovacích zariadení v ROM pamäti počítača) a obnovíme systém jeho skopírovaním z časti, kde máme *mirror* uložený. Proces môže trvať podľa veľkosti inštalovaného softvéru aj viac hodín. Po jeho ukončení musíme opäť skontrolovať prítomnosť patchov (záplat, aktualizácii) pre operačný systém a internetové prehliadače. Samozrejmosť je nahratie aktuálnej vírusovej databázy. Podľa množstva nových aktualizácií si môžeme vytvoriť nový *image*.

3.5 Poskytovanie informácií – netiketa

Etiketa určuje v súlade s morálkou spoločnosti naše správanie v konkrétnych situáciách, vedie k ohľaduplnosti a empatii, citlivému prístupu k ostatným, úcte k človeku a má výrazný vplyv na vzťahy medzi ľuďmi. Podobné poslanie má netiketa (net = sieť + etiketa), ktorá predstavuje súbor pravidiel správania sa vo virtuálnom svete (na *nete*, na sieti). Súbor pravidiel správania sa a komunikácie na internete sa orientuje na dodržiavanie základných spoločenských zvyklostí, noriem na ochranu osobnosti, rešpektovanie

intelektuálneho vlastníctva a zásad na prácu s informáciami a informačno-komunikačnými prostriedkami.

Netiketa a etiketa nie sú legislatívne stanovené normy, nemajú striktne vymedzený rozsah a vyvíjajú sa súčasne s prostredím, pre ktoré platia. Ich význam je však rovnaký ako význam zákonov a legislatívnych noriem, pretože vnikli na základe potrieb spoločnosti, boli vytvorené ľuďmi dobrovoľne a sú historicky všeobecne akceptované a vyvíjajú sa podľa potrieb spoločnosti. Dodržiavanie týchto zásad ovplyvňuje vzťahy vo virtuálnom svete, súvisí s informačnou bezpečnosťou a v konečnom dôsledku môže mať vplyv aj na morálku spoločnosti. Porušovanie etikety alebo netikety je prejavom egoizmu, nevychovanosti, nezodpovednosti alebo arogancie. A hoci nemusí ísť o protizákonné konanie, je spoločensky neprijateľné, a spoločnosť ani jednotlivci by ho nemali tolerovať.

Pravidlá netikety si jednotliví účastníci virtuálneho sveta formujú postupne sami. Napriek tomu je potrebné definovať tie, ktoré platia všeobecne. Ich zverejnenie je základným predpokladom na ich akceptovanie a dôslednejšie uplatňovanie.

Základné zásady správania sa na internete:

- **V elektronickom styku sa správajte rovnako slušne ako v bežnom živote**. Nezabúdajte, že na druhej strane sú ľudia a počítač je len prostriedok komunikácie. Uvedomte si, že komunikácia je ochudobnená o reč tela, často aj o hlasový prejav a mimiku.
- **V elektronickej pošte postupujte ako v bežnej písomnej komunikácii,** neskrývajte svoju identitu, rešpektujte súkromie adresáta, neobťažujte ho zbytočnosťami.
- **Zabezpečte si ochranu osobných údajov**. Akceptujeme právo na ochranu osobných údajov aj u iných. Komunikácia prebieha na verejnej sieti a informácie môžu uniknúť a byť zneužité.

- **Komunikujete s dôveryhodnými osobami, zapájajte sa do komunikácie na overených portáloch.** Používanie prezývky v komunikácii je bežný zvyk. Držte sa zásady: „Najskôr počúvaj, potom odpovedaj.“ Niektoré témy, ako náboženstvo, politika a pod. sú citlivé a vyžadujú ohľaduplnosť a takt.
- **Dodržiavajte zásady bezpečnosti.** Správajte sa zodpovedne a opatrne. Na vlastnú ochranu a z ohľaduplnosti voči ostatným používajte antivírusovú ochranu a nešírte zbytočné a škodlivé informácie.
- **Pri práci s informáciami neporušujte etické a právne normy.** Neprezerajte si poštu a informácie, patriace výhradne iným osobám. Nevytvárajte kópie a neprivlastňujte si cudzie diela. Rešpektujte autorské práva a copyright.
- **Nezahlcujte priestor na ukladanie dát zbytočnosťami, kontrolujte obsah a rozsah uložených údajov.** Nezverejňujte na internete nepravdivé, zavádzajúce a neaktuálne informácie. Nezapájajte sa do pyramídových hier, posielania nevyžiadanej pošty a reťazenia elektronických správ. Netolerujte to iným.
- **Odpúšťajte iným chyby, nikoho nekritizujte a nezosmiešňujte.** Podobne ako v bežnej komunikácii aj digitálna má svoje úskalia. Berte na vedomie, že každý je omylný a digitálne prostredie odkrýva nevedomosť alebo nepozornosť viac ako osobná komunikácia.
- **Buďte užitoční**, pomôžte iným, nabudúce pomôžu oni vám. Zapájajte sa do diskusií, poraďte iným, podeľte sa so svojimi skúsenosťami.
- Vo svete internetu sa držte zásady: „**Nerobte druhým to, čo nechcete, aby robili oni vám**.“

3.6 Šifrovaná komunikácia

Internet si môžeme predstaviť ako dopravné tepny, v ktorých sa pohybujú informácie. Dôverný e-mail, heslo na prístup do bankového účtu, hudobné

dielo – čokoľvek z toho sa dá „odstaviť na vedľajšiu koľaj, rozobrať a zneužiť“. Vieme tomu zabrániť? Problém bol vyriešený už dávno v minulosti – informácie sa šifrovali. Najznámejšiu šifru minulosti reprezentuje elektromechanický kryptografický stroj *Enigma.*

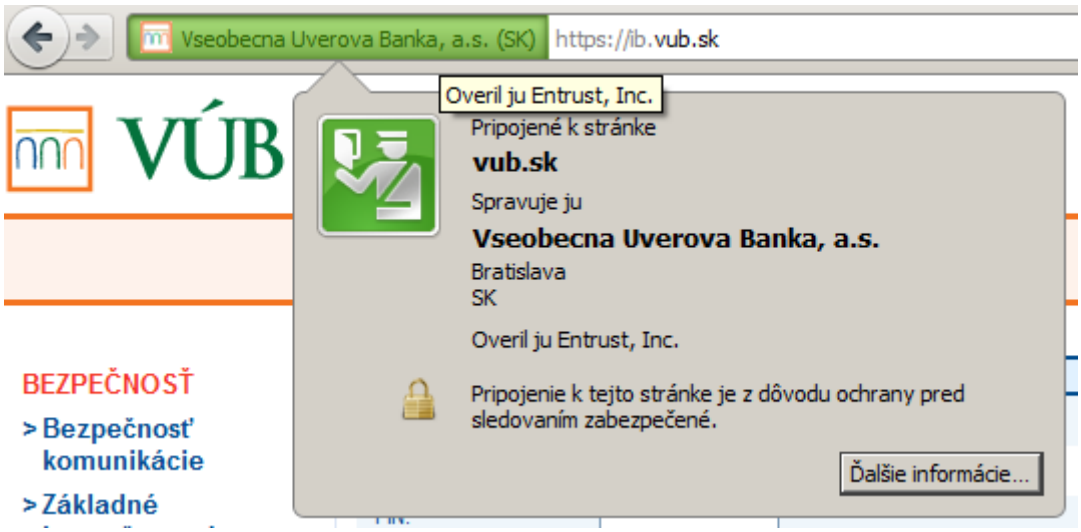
Šifrovanie je prevod bežného čitateľného textu do nečitateľnej formy pomocou algoritmu (kľúča). Ak je jeden kľúč rovnaký pre šifrovanie aj dešifrovanie, hovoríme o symetrickej šifre (Enigma). Jej nevýhodou je nutnosť okrem správy zasielať aj samotný kľúč (obrázok 4). Ak sú algoritmy rôzne, ide

Obrázok 4 Symetrické šifrovanie

o asymetrické šifrovanie, ktoré je v súčasnosti považované za najspoľahlivejšie. Šifrovanie nemôžeme zamieňať s kódovaním, pri ktorom síce dôjde k zmene čitateľného textu na nečitateľný, ale za účelom efektívnejšieho prenosu dát od vysielača k prijímaču alebo ukladania informácií, nie pre ich šifrovanie. Príkladom kódovania je prevod znakov do binárneho kódu (ASCII tabuľka), digitálneho signálu na analógový prenos dát prostredníctvom telefónnych liniek (modem) alebo modulácia analógového signálu na prenos zvukových dát vzduchom.

Asymetrické šifrovanie je základom elektronického podpisu (pozri časť 3.7). Symetrická šifra sa využíva pri zasielaní dát z prehliadača na server pomocou protokolu *https*. Pri nadviazaní spojenia medzi prehliadačom a serverom najskôr server vygeneruje kľúč, ktorý pošle asymetricky prehliadaču. Následná komunikácia prebieha šifrovaním dát týmto kľúčom symetricky.

Platí zásada: každá dôverná informácia musí byť zasielaná šifrovane, to znamená pomocou protokolu *https*. Presvedčíme sa o tom vizuálne v adresnom riadku (obrázok 5).



Obrázok 5 Overenie zabezpečenej komunikácie

Úloha: Do kufra vložíte balík s utajenými informáciami, kufor uzamknete zámkom, ktorý dokáže otvoriť len váš kľúč. Kufor pošlete inej osobe, ale kľúč od zámku si necháte. Ako sa adresát môže dostať nenásilne k balíku?

Riešenie: Adresát zamkne kufor iným zámkom, kufor vám pošle naspäť, kľúč si nechá. Vy odomknete svoj zámok (kľúč máte) a kufor pošlete naspäť. Adresát z neho odstráni svoj zámok svojím kľúčom.

Dnešné šifrovacie algoritmy nie sú založené na dôvtipe, ale na nemožnosti vyskúšať všetky možné kombinácie kľúča v reálnom čase. Pri súčasnej dĺžke kľúča 1024 bitov (4 bity predstavujú 16 možností riešenia, 1024 bitov predstavuje 2^{1024} možností) by procesor s taktovacou frekvenciou 1 GHz preskúmal všetky možnosti za 10^{293} rokov.

3.7 Elektronický podpis

Elektronický podpis je legislatívne upravený zákonom č. 215/2005 Z. z. Zákon zavádza pojem tzv. *zaručeného elektronického podpisu.* Elektronicky podpísaný dokument v zmysle tohto zákona nahrádza notársky overený podpis na dokumente. Využíva sa dosť obmedzene (neporovnateľne vyššie náklady ako poštovné) v komunikácii firiem so štátnou správou. V budúcnosti však

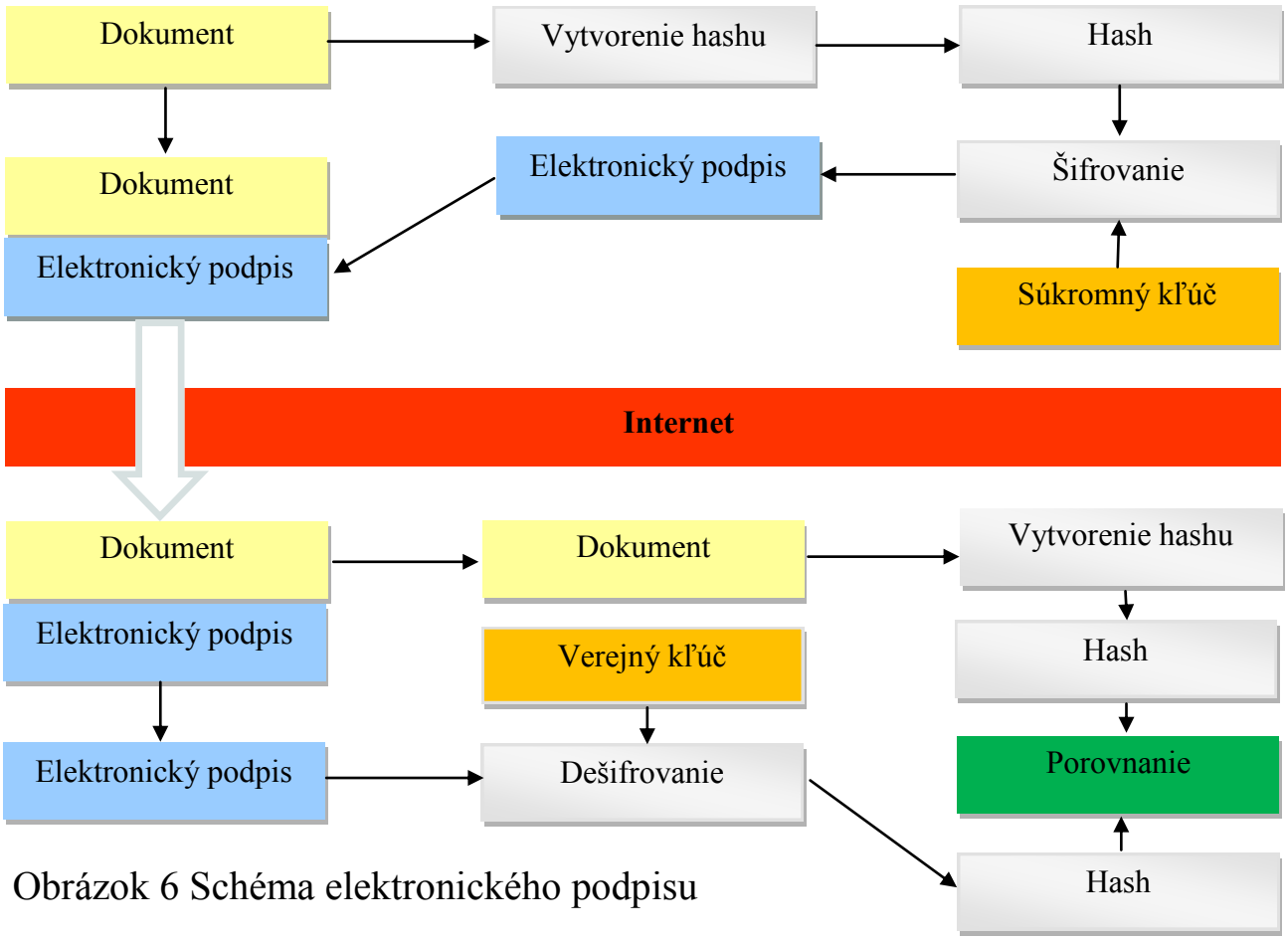
predpokladáme jeho masový rozvoj, napr. vzhľadom na možnosť zavedenia volieb prostredníctvom internetu.

Elektronický podpis zabezpečuje:

- Osoba, ktorá dokument podpisuje, je jednoznačne identifikovateľná (akoby u notára predložila občiansky preukaz).
- Dokument, ktorý dostane adresát, je totožný s odoslaným podpísaným dokumentom.

Princíp elektronického podpisu je nasledovný (obrázok 6):

1. Z podpisovaného dokumentu vytvoríme hash. Hash (odtlačok, môžeme ho porovnať s odtlačkom prsta) je vygenerovaný akronym dokumentu s veľkosťou cca 1 kB. Z hashu nie je možné pôvodný dokument získať.
2. Vytvorený hash je zašifrovaný pomocou súkromného kľúča. Výsledkom je súbor, reprezentujúci elektronický podpis.
3. Dokument a elektronický podpis sa pošlú cez internet adresátovi.



Obrázok 6 Schéma elektronického podpisu

4. Adresát na dokument aplikuje hashovací algoritmus. Výsledkom je hash prijatého dokumentu.
5. Adresát na dešifruje elektronický podpis verejne známym kľúčom. Jeho výsledkom je súbor, ktorý sa porovná s hashom z dokumentu.
6. Ak sú súbory rovnaké, dokument ani identita odosielateľa neboli zmenené.

Do procesu elektronického podpisovania vstupuje tzv. certifikačná autorita, ktorá predáva odosielateľovi dokumentu súkromný kľúč (program na USB kľúči, ktorý sa aplikuje na podpisovaný dokument) a potenciálnym adresátom verejný kľúč. Súčasne udržuje zoznam vydaných súkromných kľúčov na overenie autenticity odosielateľa.

4 Možnosti zvyšovania informačnej bezpečnosti v procese výchovy a vzdelávania

Mnoho podnetných a užitočných informácií je možné nájsť na portáloch, ktoré sú vytvorené na tento účel, alebo v rôznych médiách, ktoré sa problematike sporadicky na rôznej odbornej úrovni venujú.

Príklady portálov s problematikou informačnej bezpečnosti:

- http://www.bezpecnenainternete.sk/
- http://bezpecnesvedkom.webnode.sk/rady-pre-rodicov/
- http://www.bezpecnyinternet.sk/
- http://www.bezpecnynakup.sk/
- http://www.itpravo.sk/
- http://www.pomoc.sk
- http://www.zodpovedne.sk
- http://www.stopline.sk
- http://www.ovce.sk

- http://www.kry-sa.sk/
- http://internet.rodinka.sk/oprojekte.html
- http://pomoconline.cz/
- http://www.bezpecne-online.cz/
- http://www.bezpecnyinternet.cz/
- http://www.hoax.cz
- http://www.e-bezpeci.cz
- http://linkabezpeci.cz/data/articles/down_738.pdf
- http://www.pegi.info/cs/
- http://sk.wikipedia.org/wiki/Netiketa

Na overenie poznatkov o zásadách informačnej bezpečnosti a schopnosti ich uplatnenia je vhodné zostaviť jednoduché dotazníky, testy, ankety (jednoduchý príklad je na obrázku 7).

V oblasti posilňovania informačnej bezpečnosti medzi mladými ľuďmi je potrebné vo vyučovaní vyvážene kombinovať aktivity na získavanie poznatkov o tejto oblasti, na porozumenie problematike a na uplatňovanie poznatkov v praxi.

Pri práci s informáciami je vhodné nasmerovať pozornosť na dostupné informačné zdroje a špecializované stránky, kde je mnoho informácií a rád z tejto oblasti. Podobne ako pri iných informáciách je potrebné využiť pritom kritické myslenie, schopnosť triedenia a spracovania informácií. Dôležitá je prezentácia poznatkov a schopnosť ich využitia v praxi.

Okrem toho je vhodné využívať behaviorálne metódy vyučovania, keď sa žiaci ocitnú v situáciách, pri ktorých si môžu predstaviť pocity a situácie, ktoré sa im môžu stať, alebo ktoré môžu oni spôsobiť iným. Dôležitá je nielen realizácia aktivít a zážitkové učenie, ale veľký význam má spoločná analýza situácií a vyvodenie záverov pre bežný život.

Č.	Otázka	A/N	Správna odpoveď
1.	Môže ktokoľvek kopírovať moje osobné doklady?	☐	Nie (len oprávnené subjekty – banka, súd a pod.)
2.	Je správne odhadzovať dokumenty s osobnými údajmi, heslami, účtami do odpadkov bežným spôsobom?	☐	Nie (len fyzicky znehodnotené)
3.	Je správne používať osobné doklady ako zálohu?	☐	Nie (môže dôjsť k strate alebo zneužitiu)
4.	Je možné *nabúrať sa* do počítača cez mikrofón?	☐	Nie (prenáša analógový signál)
5.	Je vo fórach alebo blogoch potrebné nastaviť vysokú úroveň ochrany?	☐	Áno (ide o pripojenie k verejnej sieti)
6.	Je bezpečné prihlasovať sa do internetbankingu na verejnom mieste – z verejnej siete?	☐	Nie (najbezpečnejšie je prihlásiť sa z domácej siete)
7.	Je etické vymazať e-mail od neznámeho odosielateľa s podozrivým obsahom?	☐	Áno (je to správne, otvorenie nevyžiadanej pošty musíme zvážiť)
8.	Otvárame všetky prílohy, ktoré dostaneme elektronickou poštou?	☐	Nie (prílohy s neznámym obsahom neotvárame. V prípade potreby si overíme odosielateľa)
9.	Pri voľbe prezývky na rôznych portáloch vychádzame z vlastného mena?	☐	Nie (prezývka – nickname, by mala chrániť našu identitu)
10.	Zverejňujeme na webe fotografie priateľov s menami a priezviskami?	☐	Nie (chránime identitu seba i priateľov)
11.	Poskytujeme pri registrácii na portáloch všetky údaje, ktoré sú vo formulároch?	☐	Nie (vyplníme len povinné údaje)
12.	Čítame e-mailovú alebo inú elektronickú komunikáciu v pošte priateľov a rodinných príslušníkov?	☐	Nie (je to neetické, ide o osobnú korešpondenciu)

Obrázok 7 Jednoduchý test z informačnej bezpečnosti

4.1 Príklady aktivít pre žiakov

Aktivita č. 1 Pomáhajú nám skratky a internetový slang?

Cieľ aktivity: Objasniť význam účelného a efektívneho využívania internetového slangu.

Opis: Používanie internetového slangu (symbolov, skratiek, skomolenín) na internete je čím ďalej samozrejmejšie. Je potrebné zvážiť, komu a v akej situácii ich pošleme. Ide o nástroje neformálnej komunikácie, nepoužívajú sa v oficiálnej komunikácii, ale ani v prípade, že nemáme istotu, že nám druhá strana správne porozumie. Len v takom prípade plnia svoju funkciu – zjednodušiť komunikáciu (stručné vyjadrovanie), ušetriť čas (krátke texty) a vyjadriť to, čo zvyčajne nepopisujeme (mimiku a neverbálne prejavy). Vzhľadom na to, že jednotlivé výrazy môžu byť chápané aj vo viacerých významoch, v príklade je uvedený prehľad niekoľkých druhov slangových výrazov.

Úloha č. 1:

Pokúste sa dešifrovať nasledujúce dva zápisy, v ktorých je neprimerané množstvo slangu.

A) Som NOOB, pls pomôž mi urobiť DÚ. :-[|:) zajtra zbiera referáty. Budú :-C. :X

B) AFK, ozvem sa ASAP. BTW cg <3, :-* : T BRB :-)

Úloha č. 2:

Navrhnite vhodné použitie internetového slangu vo vlastnom texte – napíšte texty, v ktorom primerane použijete 3 slangové výrazy.

Pomôcky na vyriešenie úloh sú uvedené na obrázkoch č. 8, 9 a 10.

Aktivita č. 2 Môj blog

Cieľ aktivity: Vedieť zvoliť formu, obsah a prostriedky na zverejnenie informácií

Opis: Blog je pre mladých ľudí príležitosť písať a čítať o tom, čo ich zaujíma. Mnoho škôl pomocou virtuálneho vzdelávacieho prostredia ponúka možnosť vytvárať vlastný blog, zapájať sa do diskusie k určitej téme. Učitelia majú príležitosť pracovať so žiakmi na stratégiách súvisiacich s publikovaním vlastných textov. Povzbudzujú ich na tvorbu textov, učia ich štylizovať a štruktúrovať text, rešpektovať podmienky publikovania a ovládať príslušný

Skratka	Slovné spojenie	Význam	Skratka	Slovné spojenie	Význam
AFK	Away from key-board	Som vzdialený od klávesnice	FYI	For your infor-mation	Pre tvoju informáciu
ASAP	As soon as possible	Hneď ako to bude možné	G2G	Gonna to go	Musím ísť
B4	Before	Predtým	NOOB	Newbie	Začiatočník
BRB	Be right back	Hneď som späť	pls	Please	Prosím
BTW	By the way	Mimochodom	THX, TY	Thanks.	Ďakujem
cg	Congratulations	Gratulujem	Y?	Yes?	Áno?
DND	Do not disturb	Nerušiť	w8	Wait	Čakaj

Obrázok 8 Príklady internetového slangu

Všeobecné		Nálady		Neverbálne prejavy	
:)	Vtipné	=o)	Dobrá nálada	;) :-)	Úsmev
d:) : DD	Všetko v poriad-ku	=/	Zlá nálada	:D	Smiech, rehot
:-C	Problémy	:-!	Urazenosť	8-(	Smutný pohľad
:-x	Mlčanie	:X	Nadávanie	: T	Nastavuje tvár
=)	„Sranda“ musí byť	:@ :(0) :V	Ziape, jačí	:Q :~i :-€	Fajčí
:-[	Hanbí sa	:(ˇ-ˇ :-/	Smútok	:~(	Má nádchu
:o)	Myslí to dobre	:p :v	Hovorí a ho-vorí	:P :p :-)~	Vyplazuje jazyk
/:-)	Premýšľa	>:o :-§	Hnev	;)	Žmurká
O_o	Čože?	:'(	Plače	=* :-* ; o *	Posiela pusu
:|	Zhnusenie aj ne-výrazný úsmev	|-O	Zíva, je znude-ný	:( ) :):):) %(|)	Hlasný smiech

Obrázok 9 Príklady smajlíkov

Vyjadrenie štýlu		Zaujímaví ľudia		Iné	
8:) B:)	Okuliare na čele	+-:)	Pápež	<3	Srdiečko
(|:)	Prilba	*<:)>	Santa Claus	3:)	Certík
[:)	Walmen	:(O)	Nick Jagger	O:)	Anjelik
: |K:	Večerný úbor	?8o	Elton John	|:)	Učiteľ
:)o:	Kravata	:.)	Madona	@=o@	Počítačový maniak
--:-)	Pankáč	B)	Batman	<: I :(§	Hlupák
: {}	Rúž	8(:)	Mickey Mouse	<:)	Lyžiar, čarodejník, hrdina

Obrázok 10 Príklady smajlíkov zo sociálnych sietí

softvér. Spolu s poukázaním na riziká publikovania na verejnej sieti je potrebné povzbudiť všetkých, ktorí majú záujem vyjadriť svoje myšlienky a konfrontovať ich s rovesníkmi a pritom rozvíjať dôveru, tvorivosť a komunikačné zručnosti.

Úloha:

- Zvoľte si aktuálnu tému v oblasti ochrany životného prostredia.
- Napíšte na túto tému príspevok v rozsahu aspoň 20 riadkov – prečítajte si príspevky spolužiakov.
- Pri písaní sa inšpirujte blogmi, zverejnenými na webe.
- Diskutujte na danú tému.

Ktoré zásady je potrebné dodržať pri zverejnení príspevku na verejnom blogu? Na inšpiráciu odporúčame:

- ornst.blog.sme.sk/c/261831/Ekologia-v-mojich-ociach.html
- curma.blog.sme.sk/c/320481/Ako-ekologia-zabija-slony.html
- greenandsafetyworld.blog.pravda.sk/category/ekologia-hospodarstvo-a-zivotne-prostredie

Aktivita č. 3: Chatujme v škole

Cieľ aktivity: Vedieť uplatňovať zásady netikety v online diskusii

Opis: Sú témy, pri ktorých je dôležitá diskusia. Online diskusia je príležitosť, ako sa naučiť efektívne chatovať, budovať kultúru komunikácie a súčasne zaujímavo stráviť čas na vyučovaní. Prihlásenie sa na chat prináša príležitosť poukázať na zásady informačnej bezpečnosti.

Úloha:

- Prihláste na portál, ktorý zadá vyučujúci.
- Registrujte sa na portáli pod vedením učiteľa, zvoľte si vhodnú prezývku.
- Prečítajte si podmienky registrácie a potvrďte registráciu.
- Nastavte pravidlá diskusie.
- Vyskúšajte si diskusiu v skupine.
- Po ukončení diskusie sa odhláste.
- Porovnajte výhody a nevýhody osobnej a digitálnej účasti v diskusii.
- Definujte zásady chatovania (online diskusie).

Aktivita č. 4: Hry vo vzdelávaní

Cieľ aktivity: Vedieť uplatňovať zásady bezpečnosti pri internetových hrách

Opis: Online hazardné hry zahŕňajú hry prostredníctvom akýchkoľvek digitálnych prostriedkov (PC, televízia, herné konzoly, mobilné zariadenia). Okrem toho, že predstavujú zábavu, sú o peniazoch, môžu spôsobiť závislosť, psychické problémy, nedostatok spánku, koncentrácie alebo sociálnu izoláciu. Vzhľadom na to, že hry sú bežnou súčasťou sveta žiakov, patria i do vyučovania. Mnoho učiteľov ich považuje za veľmi účinnú metódu vzdelávania. Pritom majú výbornú prirodzenú príležitosť poukázať na riziká spojené s hrami na internete, na možné závislosti a dopady gamblerstva na život človeka a rodiny

Úloha:

- Vyberte vhodné hry (vedomostné, logické, strategické, tvorivé, zábavné).
- Na zvolenú hru si vyberte spoluhráčov a oboznámte sa spoločne s pravidlami hry.
- V stanovenom čase hrajte zvolenú hru.
- Opíšte, čo sa počas hry naučili, v čom sa zdokonalili, aké mali pocity.
- Diskutujte o iných hrách, ktoré sú na internete dostupné a prečo ich ľudia hrajú.
- Diskutujte o rizikách spojených s častým hraním hier a s hazardnými hrami.
- Napíšte pravidlá na hranie hier na internete.

Aktivita č. 5: Internetové kontakty

Cieľ aktivity: Vedieť uplatňovať zásady na ochranu osobnosti v internetovom prostredí.

Opis: Bezpečné a zodpovedné používanie internetu je téma pre malých i veľkých. Mládež často nemá s kým prediskutovať problémy, s ktorými sa stretáva. Niekedy má učiteľ podozrenie, že predmetom záujmu žiakov sú drogy, alkohol alebo sexuálne témy. Preto aj pálčivé témy môžu byť predmetom diskusie na hodinách.

Úloha:

- Žiaci sa rozdelia na päť skupín.
- Každá zo skupín si prečíta svoj príbeh.
- Každá skupina navrhne riešenie situácie.
- Napokon žiaci oboznámia s príbehom a návrhom na riešenie ostaté dve skupiny.
- V závere sa uskutoční diskusia o javoch súvisiacich s informačnou bezpečnosťou.

- Žiaci diskutujú o situáciách, ktoré sa im stali, alebo o ktorých počuli od svojich priateľov.

Príbeh 1 – náhodná webová stránka.

Volám sa Daniel. Počas hodiny sme na webových stránkach hľadali informácie podľa zadania. Môj sused Andrej sa náhodou dostal na stránku o legalizácii marihuany, kde sa zapojil do diskusnej skupiny. Odvtedy na hodinách pravidelne navštevuje tieto stránky. Aj ja som tieto stránky navštívil, ale obsah ma nezaujal. Nie som si istý, čo mám urobiť – tváriť sa, že o tom nič neviem, presvedčiť spolužiaka, že koná nesprávne alebo nahlásiť učiteľovi nebezpečné počínanie spolužiaka?

Príbeh 2 – komunikácia na webe.

Volám sa Soňa. Navštevujem gymnázium, mám dobré študijné výsledky. Už niekoľko mesiacov mám priateľa, s ktorým som sa zoznámila prostredníctvom internetu a s ktorým často večer komunikujeme. Raz ma poprosil, či by som mu neukázala do kamery svoje prsia. Hoci som nemala veľmi chuť ani odvahu, nechcela som ho sklamať, a tak som mu vyhovela. Netrvalo dlho a zábery sa objavili nielen medzi jeho priateľmi, ale aj na internete. Hanbila som sa. Rodiča sa to dozvedeli a boli sklamaní. Nasledovali nočné mory a ani po odchode na vysokú školu sa asi tejto skúsenosti nezbavím.

Príbeh 3 – informácie na internete.

Volám sa Tomáš. Mám 16 rokov. Facebook sa stal súčasťou môjho každodenného života. Využívam ho dokonca na učenie a riešenie domácich úloh so spolužiakmi. Najradšej mám ale nezáväznú komunikáciu. Najmä pokiaľ mám takú zaujímavú tému ako dnes. Chystáme sa s rodičmi na dovolenku a teším sa, ako sa pochválim kamarátom. Ideme v jednom termíne do rovnakej destinácie ako spolužiačka. Dnes sa pokúsime zistiť, či v danom čase ide na to isté miesto ešte niekto z našich facebookových priateľov.

Príbeh 4 – prvé stretnutie.

Volám sa Naďa. Mám 14 rokov. Moji rodičia na mňa nemajú veľa času. Bývame v novom dome, kde ešte nemám priateľov. V škole mám dve dobré kamarátky Táňu a Ivonu. O to viac priateľov mám na internete. Najviac času trávim s Martinou a Milanom. Martina je mamička na materskej dovolenke, je odo mňa oveľa staršia, ale môžem sa jej zdôveriť, vždy ma vypočuje a rada mi poradí. Iba nedávno mi povedala, že je učiteľka a rada sa rozpráva s deťmi. Milana poznám menej, ale tiež sa o mňa zaujíma. Rozprávam sa s ním o mojich priateľstvách v škole, o svojich zvykoch, o tom čo ma baví. Vie, že popoludní nemám kam ísť, preto sme sa dohodli na stretnutí. Sľúbil mi, že príde pre mňa a urobíme si malý výlet. Nemala by som o tom nikomu hovoriť, je to naše tajomstvo. Chcela by som to povedať kamarátkam v škole – najradšej by som bola, keby sme na výlet mohli ísť všetky tri, ale tým by som prezradila tajomstvo. Určite sa to nemôže dozvedieť mama, lebo by ma nikam nepustila – ako vždy.

Príbeh 5 – prvé stretnutie.

Volám sa Félix. Mám 17 rokov a môj hlavný problém okrem školy je nedostatok peňazí. Nepodarí sa mi ušetriť na počítač. Vreckové mi stačí tak na pol mesiaca a zatiaľ sa mi nepodarilo zohnať brigádu. Včera sa na mňa usmialo šťastie. Spolužiaci z vyššieho ročníka hľadajú skupinu spoluhráčov do novej internetovej hry. Princíp je jednoduchý. Ak sa zaregistrujem a pošlem vstupný poplatok, dostanem sa do pyramídy, v rámci ktorej bude mojou úlohou získať ďalších hráčov, aby sa postupne vytvoril fond, z ktorého získam očakávané financie.

Aktivita č. 6: Zásady správania na internete.

Cieľ aktivity: Identifikovať základné zásady na bezpečnú prácu s internetom.

Opis: Žiaci budú pracovať v troch skupinách. Každá skupina navrhne práva, ktoré by sa mali dostať medzi 10 najdôležitejších zásad bezpečnej práce s internetom. Všetky pravidlá sa napíšu na tabuľu. Tie, ktoré sa opakujú alebo sú podobné sa zapíšu len raz. V prípade, že je potrebné niečo doplniť, žiaci to urobia spoločne na základe otázok učiteľa.

Nasleduje diskusia. Tretia skupina vyberie problémové pravidlo, ktorého zaradenie medzi najdôležitejšie je potrebné zvážiť. Prvá skupina obhajuje zaradenie tohto pravidla a druhá skupina argumentuje proti zaradeniu pravidla. Na základe takejto diskusie tretia skupiny rozhodne, ktoré argumenty boli silnejšie a presvedčivejšie.

Diskusia pokračuje. Druhá skupina vyberie jedno z pravidiel a dve skupiny argumentujú na jeho zaradenie alebo nezaradenie. Diskusia môže prebiehať ku každému z pravidiel, alebo len k vybraným. Na záver sa pravidlá zverejnia na dostupnom mieste.

Aktivita č. 7: Čo o sebe nevieme.

Cieľ aktivity: Rozpoznávať ohrozenia v oblasti internetovej bezpečnosti.

Opis: Triedu rozdelíme do troch skupín. Každá skupina bude mať za úlohu riešiť jednu aktuálnu oblasť informačnej bezpečnosti (napríklad elektronická pošta, internetbanking, kyberšikana alebo sociálne siete). Každá skupina zostaví pre danú problematiku anketu, z ktorej získa od ostatných dvoch skupín, prípadne od viacerých žiakov školy odpovede na svoje otázky. Na základe spracovania dotazníka interpretuje skupina výsledky a poukáže na problémy a skúsenosti v danej oblasti.

Na základe zistení sa uskutoční v triede riadená diskusia na jednotlivé témy, v rámci ktorej sa hľadajú návrhy na zlepšenie danej situácie a zúročenie skúseností v otázkach informačnej bezpečnosti.

Závery a odporúčania z diskusie spracuje každá skupina na poster, ktorý zverejní na dostupnom mieste v škole alebo v triede.

Aktivita č. 8: Súkromie na internete.

Cieľ aktivity: Analyzovať príčiny obmedzovania súkromia v internetovom prostredí.

Prvá časť aktivity. Žiaci sa rozdelia do dvojíc a rozhovorom zisťujú o spolužiakovi odpovede na nasledovné otázky:

- Kedy mám pocit, že je moje súkromie narušené?
- Kedy mám nárok na súkromie?
- Ako môžem ochrániť svoje súkromie?

Následne žiaci zakresľujú do spoločnej myšlienkovej mapy poznatky z rozhovorov so spolužiakmi. Ku každej z otázok vzniká samostatná myšlienková mapa.

Druhá časť aktivity. Následne žiaci odpovedajú na dichotomické otázky (odpoveď Áno/Nie), ktoré sú uvedené na tabuli, v elektronickom alebo papierovom dotazníku. Na tabuli sa zverejní počet kladných odpovedí za celú triedu. Príklady otázok v dotazníku:

- Zverejnil som na internete svoju fotku?
- Zverejnil som na internete vlastné video?
- Zverejnil som na internete svoje číslo telefónu?
- Zverejnil som na internete svoju adresu?
- Zverejnil som na internete svoj dátum narodenia?
- Pridal som si medzi priateľov osobu, ktorú som nepoznal?
- Otvoril som e-mail s neznámym obsahom od neznámej osoby?
- Zasielal som ďalej správy, ktoré som dostal ako nevyžiadané od niekoho iného?
- Poskytol som informácie o tom, čo rád nakupujem?
- Poskytol som informácie o tom kde a s kým trávim voľný čas?

Tretia časť aktivity. Objasnenie myšlienkových máp z prvej aktivity v kontexte zistení z druhej aktivity spolu s diskusiou k súvislostiam medzi prvou a druhou časťou aktivity.

Štvrtá časť aktivity. Domáca úloha. Každý žiak spracuje vlastnú myšlienkovú mapu, v ktorej znázorní možnosti zvýšenia ochrany svojej osobnosti a svojho súkromia.

Aktivita č. 9: Vieme si pomáhať?

Cieľ aktivity: Vedieť riešiť situácie súvisiace s ohrozením informačnej bezpečnosti.

Opis: Žiaci sa rozdelia do dvojíc, v ktorých budú riešiť možné prípady súvisiace s informačnou bezpečnosťou. Žiak si zvolí rolu A alebo B a následne si vytiahne kartičku, na ktorej je rola opísaná. Hranie rolí vyvoláva u žiakov emócie, kladie nároky na analýzu situácie, prijímanie rozhodnutí a argumentovanie svojich riešení. Po 7 – 10 minútach si žiaci vymenia roly. Na záver dvojice informujú o probléme a jeho možnom riešení celú triedu. Súčasne diskutujú o tom, ako sa cítili v jednotlivých rolách, ktoré kladné a negatívne pocity pritom mali. Podľa záujmu žiakov je možné k danej téme spracovať jednoduchý dialóg, resp. komiks.

Prípady na riešenie:

- Súrodenci (A – sestra, B – brat). Pri náhodnom prezeraní na webe ste zistili, že na internete sestra zverejnila vašu fotografiu aj s menom.
- Deti (A – malá sestra, B – starší súrodenec, brat alebo sestra). Práve ste zistili, že malá 10-ročná sestra má na internete profil na sociálnej sieti, vrátane fotografie a mobilného telefónu.
- Rodina (A – dieťa, B – rodič). Na základe toho, že ste na internete zverejnili svoje číslo telefónu, dostávate výhražné textové správy. Rozhodli ste sa o tom informovať nič netušiacich rodičov.

- Rodičia (A – dieťa, B – rodič). Rodičia objavili na vašej sociálnej sieti nevhodný obsah. Chcú to s vami riešiť.
- Spolužiaci (A – spolužiak, B – poškodený). Počas dňa bol počítač bez dozoru na lavici. Spolužiaci sa na ňom hrali svoju hru. Následne sa v ňom objavili vírusy, ktoré sa obvykle šíria s hrami.
- Učiteľ (A – učiteľ, B – žiak). Učiteľ má výhrady k vašej nespisovnej a pravopisne nesprávnej komunikácii v elektronickej pošte.
- Žiaci (A – žiačka, B – žiak). Žiačka sa pochválila svoju spolužiakovi, že zajtra po vyučovaní má ísť na stretnutie s priateľom, ktorého pozná len z internetu.
- Brat (A – sestra, B – brat). Sestra našla na stole počítač, v ktorom mal brat otvorenú elektronickú poštu. Len tak zo zábavy si prečítala niekoľko správ. Jednu poslala na svoju adresu a bratovej kamarátke vtipne odpovedala.
- Banka (A – matka, B – otec). Mama sa počas pobytu v kaviarni pripojila na internetbanking a kontrolovala si stav účtu. Otec nie je spokojný s počínaním matky, pretože ho považuje za nebezpečné.
- Starí rodičia (A – dedko, B – babka). Dedko práve dostal do mobilu správu, že vyhral zájazd do kúpeľov pre dve osoby. Na potvrdenie výhry je potrebné zaslať späť SMS v hodnote 20 €. Babka výhre neverí a nesúhlasí s jej prijatím.

Aktivita č. 10: Ohrození sú malí i veľkí.

Cieľ aktivity: Poukázať na možnosti zvýšenia internetovej bezpečnosti.

Opis: Učiteľ si pripraví niekoľko tvrdení týkajúcich sa informačnej bezpečnosti a dva plagáty so slovami Súhlasím/Nesúhlasím, ktoré umiestni na rôznych stranách miestnosti. Tvrdenia by mali vyjadrovať otázky informačnej bezpečnosti bez ohľadu na pohlavie a vek. Žiaci voľne stoja v priestore. Po prečítaní výroku sa žiaci zhromaždia pri plagáte, ktorý vyjadruje ich názor.

Možné tvrdenia:

- Internetbanking je pri dodržiavaní odporúčaných zásad celkom bezpečný.
- Na sociálnej sieti sa cítim bezpečne.
- Kyberšikana ohrozuje ľudí bez rozdielu veku.
- Hraním hier na internete si človek môže vybudovať závislosť a prípadne gamblerstvo.
- Antivírusová kontrola počítača, externých diskov a iných zariadení je nevyhnutná.
- Následne žiaci diskutujú o situáciách, ktoré pri jednotlivých výrokoch nastali a vyvodzujú závery vo vzťahu k informačnej bezpečnosti.
- Na domácu úlohu napíšu krátku esej na jednu z rozoberaných tém.

5 Záver

Internet je multimediálna komunikačná a prezentačná platforma. Jeho obsah nie je možné filtrovať alebo cenzúrovať. Pre deti školského veku až po adolescentov je na jednej strane najvyužívanejším nástrojom na získavanie informácií a na objavovanie sveta a na druhej strane otvoreným oknom pre zlodejov, pedofilov a pod. Veľkosť otvorenia tohto okna závisí v najvýznamnejšej miere od ich veku, mentálnej vyspelosti a počítačovej gramotnosti. Úlohou učiteľa v procese minimalizácie rizika plynúceho z negatívneho pôsobenia internetu je informovať a vysvetľovať.

Akcentovanie zdravého úsudku a uvedomenia si potenciálnych rizík pri akejkoľvek aktivite na internete je prvým predpokladom jeho bezpečného využívania. Druhým predpokladom sú znalosti – poznanie princípov útokov a spôsobov obrany proti nim. Učiteľovou zodpovednosťou je stáť vedľa žiaka a pomôcť mu nástrahy plynúce z využívania internetu a počítačových sietí eliminovať.

Zoznam bibliografických odkazov

Průcha, J., Walterová, E., Mareš, J. 1998. *Pedagogický slovník.* 2. vyd., Praha : Portál, 1998. ISBN 80-7178-252-1.

Stanovisko Európskeho hospodárskeho a sociálneho výboru na tému „Preventívne opatrenia na ochranu detí pred sexuálnym zneužívaním“. Úradný vestník Európskej únie. [online]. 2012. Dostupné na internete: <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:C:2012:024:0154:0158:SK:PDF>.

Smernica o nekalých obchodných praktikách. [online]. 2006. Dostupné na internete: <http://ec.europa.eu/consumers/cons_int/safe_shop/fair_bus_pract/ucp_sk.pdf>.

Európska stratégia vytvárania lepšieho internetu pre deti. [online]. [cit.2013-02-14]. Dostupné na internete: <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2012:0196:FIN:SK:PDF>.

Národná stratégia pre informačnú bezpečnosť v SR. [online]. 2008. Dostupné na internete: <http://www.informatizacia.sk/narodna-strategia-pre-ib/6783s>.

Zákon č. 460/1992 Z. z. Ústava SR. [online]. [cit.2013-02-16]. Dostupné na internete: <*www.zbierka.sk/sk/predpisy/460-1992-zb.p-2044.pdf* >.

Zákon č. 363/2005 Z. z. Zákon o ochrane osobných údajov. [online]. [cit.2013-02-11]. Dostupné na internete: <http://www.ekoway.sk/files/editor/uplne_znenie_363_2005_z.z..pdf>.