Univerzita Hradec Králové

Přírodovědecká fakulta

Katedra informatiky

Informační bezpečnost jako velmi důležitá oblast výuky informatiky na základní a střední škole

Diplomová práce

Autor: Bc. Miroslav Beránek

Studijní program: N1101 – Matematika

Studijní obor: PřF P-NMATSSK

P-NSSKIN

Vedoucí práce: PhDr. Michal Musílek, Ph.D.

Hradec Králové

2014

Univerzita Hradec Králové
Přírodovědecká fakulta

Zadání diplomové práce

Autor:	**Bc. Miroslav Beránek**
Studijní program:	N1101 Matematika
Studijní obor:	Učitelství matematiky pro střední školy Učitelství pro střední školy - informatika
Název závěrečné práce:	**Informační bezpečnost jako velmi důležitá oblast výuky informatiky na základní a střední škole**
Název závěrečné práce AJ:	Information security as a very important area of computer science teaching at secondary school

Cíl, metody, literatura, předpoklady:

Cílem práce je zmapovat důležitou oblast informační bezpečnosti, provést její didaktickou analýzu a navrhnout témata a rozsah přístupný žákům základních a středních škol. Teoretická část práce by měla představovat přehled různých nástrah a nebezpečí, které mohou pro uživatele informačních a komunikačních technologií znamenat riziko či dokonce ohrožení. Budou zde popsány základní techniky, které jsou zneužívány v elektronické kriminalitě, stejně jako doporučení pro uživatele, jak se mají ochránit před těmito nástrahami, jak zabezpečit svoji identitu a soukromí a jak spolehlivě archivovat svá cenná data. Praktickou částí práce budou pracovní listy pro výuku témat z oblasti počítačové bezpečnosti na základních i středních školách. Výuka s pomocí těchto pracovních listů bude prakticky odzkoušena a zároveň bude vhodným způsobem zmapováno subjektivní vnímání důležitosti takto získaných vědomostí a dovedností žáky, jichž se výuka dotkne.

Garantující pracoviště:	Katedra informatiky, Přírodovědecká fakulta
Vedoucí práce:	PhDr. Michal Musílek, Ph.D.
Konzultant:	
Oponent:	doc. RNDr. Štěpán Hubálovský, Ph.D.

Datum zadání závěrečné práce: 17. 4. 2013

Datum odevzdání závěrečné práce: 30. 11. 2014

Prohlášení

Prohlašuji, že jsem tuto diplomovou práci vypracoval pod vedením vedoucího diplomové práce samostatně a uvedl jsem všechny použité prameny a literaturu.

V Hradci Králové dne 30. 11. 2014

Bc. Miroslav Beránek

Anotace

BERÁNEK, MIROSLAV. Informační bezpečnost jako velmi důležitá oblast výuky informatiky na základní a střední škole, Hradec Králové: Přírodovědecká fakulta Univerzity Hradec Králové, 2014, 82 stran, Diplomová práce

Diplomová práce „Informační bezpečnost jako velmi důležitá oblast výuky informatiky na základní a střední škole“ se zaměřuje na čtyři základní oblasti nebezpečí, která hrozí žákům, při práci s informačními a komunikačními technologiemi. První kapitola se zabývá zdravotními riziky a předcházení onemocněním, způsobeným dlouhodobým sezení u počítače. Druhá seznámí čtenáře s riziky ztráty a odcizení dat, softwarovou obranou před zcizením informací. Třetí část práce je zaměřena na ukládání, zálohování a archivaci dat a poslední kapitola se zabývá nástrahami internetu, kyberšikanou apod. Součástí práce je také výzkum, mapující chování žáků a práci s ICT a pracovní listy.

Klíčová slova: ochrana zdraví, softwarové nebezpečí, zálohování, kyberšikana, internetové nástrahy

Anotace

BERÁNEK, MIROSLAV. Information security as a very important area of information technology education at primary and secondary schools', Hradec Králové: Přírodovědecká fakulta Univerzity Hradec Králové, 2014, 82 pages, Diplomová práce

This diploma thesis called 'Information security as a very important area of information technology education at primary and secondary schools' is focused on four basic danger areas which endanger learners when working with information and communication technologies. The first chapter deals with health risks and prevention of diseases caused by long-term sitting at computers. The second one makes readers familiar with risks of data loss or theft and software protection against data theft. The third part of the thesis is focused on the issue connected with how to save, backup and archive data. Finally, the last chapter deals with internet dangers, cyberbullying etc. The thesis also includes a research mapping learners' behaviour and working with ICT and worksheets.

Key words: health protection, software danger, data backup, cyberbullying, internet dangers

Obsah

Úvod

Moje diplomová práce se zaměří na rizika a nebezpečí při práci s informačními a komunikačními technologiemi. Cílem práce je zmapování možných hrozeb, se kterými se žáci mohou setkat při užívání informačních a komunikačních technologií. V práci budou jednotlivá nebezpečí popsána, uveden přehled a popis jejich příčin, následků a možností jak se jim bránit a předcházet jim. Každou kapitolu doplní pracovní list. Výuka jednotlivých témat bude zařazena během školního roku do výuky a na jeho konci zjištěno dotazníkem, jak si žáci osvojili jednotlivé poznatky.

První kapitola se bude zabývat zdravotními riziky. Nesprávné sezení, dlouhodobé sledování obrazovky, špatné držení těla či uspořádání prostoru, to jsou jen některé faktory ovlivňující zdravotní stav uživatelů. Je proto důležité vědět, jak správně uspořádat okolí počítače, nastavit židli a kdy a jak často provádět zdravotní přestávky.

Druhá kapitola se zaměří na různá rizika jak může dojít ke zcizení dat a jak se pomocí antivirových programů, šifrování a dalším podobným možnostem bránit útokům na naše soukromí.

Třetí část se zaměří na uchování dat, především zálohování a archivaci. Bude obsahovat přehled základních hardwarových a softwarových prostředků, které by žáci měli znát a případně využívat pro ukládání svých dat.

Poslední kapitola se bude věnovat hrozbám číhajícím na internetu. Kyberšikana, sexting, internetová závislost a další nástrahy číhající v on-line světě dnes a denně ovlivňují uživatele a je třeba o nich vědět a nejlépe jim i předcházet.

Po každé kapitole bude připraven pracovní list pro žáky, týkající se dané oblasti a také jeho řešení s případným komentářem. Celou práci uzavřu výzkumem o tom, jak žáci základní školy a gymnázia vnímají jednotlivé nástrahy, jak se sami chovají a jaké pravidla při práci s ICT dodržují.

1 Zdravotní rizika při práci s počítačem

S přibývajícími technologiemi přibývá také zdravotních rizik, která v souvislosti s nimi vznikají. Řada žáků, ale i dospělých, tráví většinu dne sezením u počítače či sledováním televize a zapomínají na pohyb a další aktivity. Při současném rozmachu notebooků, tabletu a chytrých technologií už ani uživatele nic nedrží u stolu, většinou se různě „povalují“ v křeslech a na gaučích. Dochází tak k zatěžování našeho těla a celkově organizmu, což může vést k různým zdravotním komplikacím.

1.1 Technické prostředky ovlivňující zdraví

1.1.1 RSI - Repetitive Strain Injury

Repetitive straun injury (RSI) je česky často označováno jako syndrom z opakovaného přetížení (SOP). Jedná se bolestivost často několika částí těla, která je způsobena častým opakováním stejných pohybů při monotónní práci. V souvislosti s vývojem počítačů a jejich proniknutím snad do všech odvětví lidské činnosti, se často stává, že u zařízení sedíme dlouhé hodiny a vykonáváme stále stejné pohyby s myší a klávesnicí. Tím dochází k dlouhodobému namáhání určitých partií těla, které se poté projeví bolestí „bez zjevné příčiny“. RSI postihuje především krční páteř, šlachy a nervy ruky, ramena, záda, ale i dolní končetiny. K nejznámějším problémům patří zajisté tzv. „karpální tunel“. Kromě opakování pohybů také dochází ke zpevnění některých částí těla, jako jsou záda a paže. Toto dlouhodobé držení stále stejné pozice je pro organizmus horší než aktivní činnost. Pro předejití těmto postižením je proto nutné dělat kratší přestávky, či měnit polohu těla, aby se nenamáhali vždy stejné části dlouhodobě. Mezi činitele ovlivňující naši práci nepatří pouze klávesnice, myš a židle, na které sedíme, ale celá řada dalších činitelů jako je pracovní prostředí, osvětlení a další …

1.1.2 Sezení u počítače

Počítačová židle, křeslo k počítači apod. bývá především vybíráno jako „doplněk“ k počítači s ohledem na design a jak se hodí do pokoje. Často je ovšem zapomínáno na to, že v něm budeme trávit prací řadu hodin a mělo by tedy splňovat určité předpoklady pro zdravé sezení. Kancelářská židle musí být výškově stavitelná. Ať už ve škole nebo doma, u počítače se střídá

řada osob a ty by měli mít možnost upravit si výšku sedadla dle svých potřeb. Sedadlo by mělo být tak vysoko, aby stehna byla mírně skloněna dolů, případně směřovala rovně. Lýtková část nohy má směřovat kolmo k podlaze. Pokud nám to naše velikost neumožnuje, je dobré si pořídit podpěrku nohou. Výška sedáku také souvisí s výškou stolu. Sedák je zapotřebí mít tak vysoko, aby ruce mohli volně ležet na pracovní desce a svíraly s ní přibližně pravý úhel. Vhodné je také doplnění opěrek rukou, na kterých mohou být lokty volně položeny.

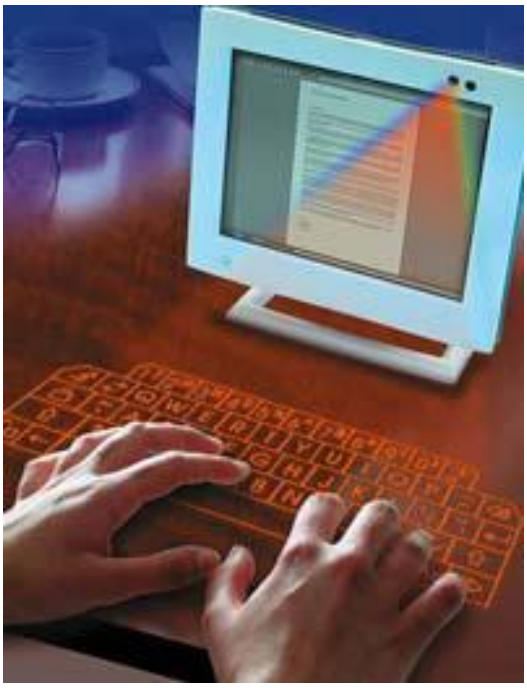
Alternativou kancelářské židle může být v domácnosti (ve škole je značně nevhodný) použití gymnastického míče. Ten nás totiž nutí sedět aktivně a dynamicky, kdy nedržíme strnule jednu pozici, ale balancujeme. Je na něm také nutné sedět vzpřímeně, což šetří páteř. Nutí nás neustále používat nohy jako oporu, nedochází tak k přetěžování některých částí a jejich stlačení, jako například na židli, kdy si hodíme nohu přes nohu. Jelikož nemáme o co opřít záda, naše svaly se neustále drobně pohybují a tím nezůstávají v jedné strnulé poloze, uvolňují se a napínají.

1.1.3 Klávesnice

Klávesnice u počítače či notebooku je po špatném sezení hlavní příčinou onemocnění prstů, zápěstí, loktů a jiných částí paže. Oproti psacím strojům, stačí totiž moderní klávesnici velmi lehký stisk, kdežto dříve bylo nutné vyvinout značnou sílu pro úhoz a tím docházelo k posilování svalstva. U moderních zařízení jsou klávesy citlivé, nelze na nich nechat volně spočinout prsty a tak dochází k neustálému napětí v oblasti zápěstí. Klávesnice by měla být spíše ve vodorovné poloze a při rozsáhlejším psaní textu, ve škole například při výuce psaní na počítači, je vhodné použít podpěrky pod ruce. Denně by práce s klávesnicí neměla přesáhnout 4 hodiny při pěti normostranách za hodinu.

Chceme-li předejít zdravotním rizikům, můžeme si pořídit některou klávesnici s alternativním rozložením kláves, což je vhodné pro ty, kteří tráví značnou část dne zadáváním textu do počítače. Klávesy u alternativních typů bývají nejčastěji uspořádány tak, aby uživatel nemusel tolik vytáčet zápěstí a držel jej v přirozené poloze.

Dalším velkým problémem zejména školního prostředí je hygiena. U počítače se často střídá několik žáků, kteří mají více či méně špinavé ruce a část „své špíny“ tak zanechávají na klávesnici, případně také myši. Je proto nutné věnovat těmto zařízením zvýšenou pozornost při úklidu a použít vhodné úklidové prostředky. V současné době je na trhu řada možností pro čištění, často ale stačí použít vlhký hadr se saponátem a otřít klávesy. Případně jsou k dispozici čistící hmoty, spreje apod. Alespoň jednou ročně by měl být také vyčištěn prostor pod klávesami, což je již technicky náročnější a nelze to požadovat po uklízečce. Často je v současnosti jednodušším řešením zakoupení nových zařízení.



OBR. 1 PROJEKČNÍ KLÁVESNICE

Vyřešením hygienických problémů, které ovšem nemusí být každému pohodlné a neřeší problémy fyziologické, je použití virtuální klávesnice společnosti VKB Inc. Toto zařízení promítá obraz na jakýkoliv rovný povrch a infračervený paprsek snímá pohyb prstů a signál poté předává do připojeného zařízení (tablet, počítač apod.). Tento systém se jistě v budoucnu uplatní tam, kde bude třeba hygienické prostředí, jako jsou právě školy, nemocnice a další.

Abychom předešli onemocnění rukou z dlouhodobé práce s klávesnicí, je vhodné dodržovat několik zásad:

- Než začne psát, provedeme několik cviků k protažení a uvolnění dlaní a zápěstí.
- Po každé hodině práce si dopřejeme 10 – 15 min přestávku.
- Při přestávkách opět procvičíme zápěstí.
- Při koupi klávesnice nevybírat pouze podle designu, ale také podle toho, jak se nám budou stiskávat jednotlivá tlačítka a zda je velikost kláves pohodlná a vhodně rozložená dle našich potřeb.

1.1.4 Myš

Počítačová myš je nejčastější příčinou zánětu tzv. karpálního tunelu. Žáci ve škole i doma drží dlouhou dobu myš při práci či hraní her. V práci u počítače myší často klikají zaměstnanci jen na kolonky a mají ruku v neustále sevřené poloze. Během toho dochází k tlaku na karpální tunel a ten se uzavírá a stahuje tak nervy. Následkem toho je pak brnění konečků prstů, bolesti během spánku a v krajním případě postižení nedovoluje zcela rozevřít dlaň. Řešením je poté operace.

Chceme-li předejít těmto potížím, je vhodné často zařazovat přestávky a procvičovat zápěstí. Pro dlouhodobou práci je vhodné zakoupit myš s možností nastavení velikostí podle potřeb uživatele. Pokud nechceme investovat do drahé myši, je vhodné při koupi vyzkoušet velikost a pohodlnost držení. Rozhodně není vhodná myš za pár desítek korun ve tvaru „půlvajíčka“, za pár stokorun již můžeme pořídit myš vhodného tvaru do ruky.

Ve škole opět vyvstává otázka hygieny. Stejně jako vznikají virtuální klávesnice, promítající pouze obraz na libovolnou, rovnou pracovní desku, tak i počítačová myš může fungovat na základě infračerveného snímání pohybu ruky. Jak u virtuálních klávesnicí, tak u myši, rozšíření nových technologií brání především jejich cena. Dalším problémem je fyzická nepřítomnost zařízení, která může být pro některé uživatele velkým problémem.

1.1.5 Monitor

Zastoupení CRT monitorů na trhu již výrazně pokleslo a vyskytují se spíše ojediněle, proto se v následující části budu zabývat především monitory LCD a novějšími.

Problémem při práci s monitorem je především zrak a krční páteř. Monitor neumisťujeme proti oknu, aby nedocházelo k odleskům a odrazu světla od pracovní plochy. Měl by být umístěn tak, aby na monitor, ani nám do obličeje, nedopadalo přímé sluneční světlo. Umístění monitoru závisí především na jeho úhlopříčce, obecně platí, čím větší úhlopříčka, tím je třeba i větší vzdálenost od očí. Průměrná vzdálenost se pohybuje okolo 40 – 50 cm. Horní hrana monitoruje zároveň s očima. Pokud musíme naklánět hlavu, namáháme tak svaly krční páteře. Není ani dobré otáčení hlavou či umístění nad úrovní očí. Potřebujeme-li opisovat text, umístíme jej do úrovně monitoru.

Při nastavování jasu monitoru, nepoužíváme maximální hodnoty, monitor neslouží jako lampička, proto při práci v noci používáme stolní lampu, případně můžeme použít přisvětlení pomocí různých USB lampiček, kterých je na trhu celá řada a mohou nám tak osvítit klávesnici. USB lampičky nám ale nenahradí stolní lampu, kterou je nutné použít při práci s textem na papíře, opisování textu apod.

Po delší práci s monitorem můžeme pociťovat pálení, či únavu očí. Při dlouhodobější práci dochází k omezenému mrkání. Oči se tak vysušují a můžeme dojít k zarudnutí a pálení. Při problémech s očima můžeme použít některé výrobky pro zvlhčení oční bulvy. Sledujeme-li neustále monitor, namáháme stále okohybné svaly. Soustředěním na jedno místo může dojít ke zhoršení zraku. Alespoň každou hodinu je potřeba oči „protáhnout“, únavě očí předejdeme jednoduchým cvičením. Zaostřete na blízký předmět, nejlépe například na špičku nosu, poté přeostřete na vzdálenější předmět, třeba zeď a nakonec se zahleďte z okna do dáli. Během celého cvičení, je třeba mrkat více, než jsme zvyklí, doporučuje se také zadívat se do zelené louky či lesa. Zelená barva je pro oči nejpříjemnější a nejméně náročná.

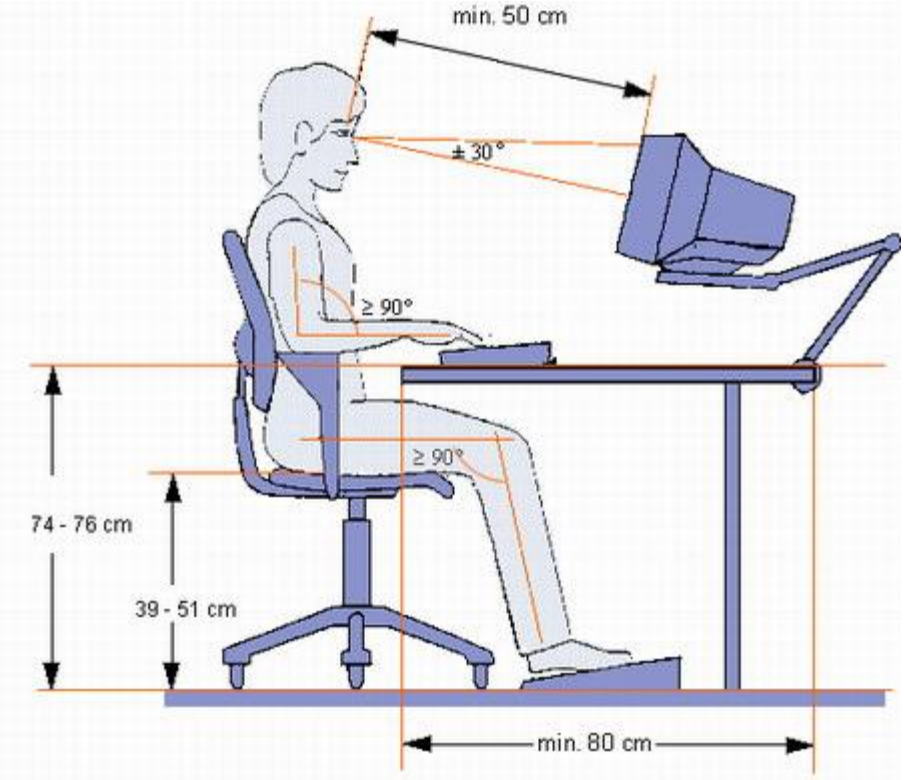
Používáme-li k běžnému čtení textu brýle, je vhodné požádat svého lékaře o speciální brýle na počítač. Klasické brýle nám mohou při práci s monitorem přivodit boleti hlavy či únavu očí.

Pomoci předejít potížím s očima nám můžou i různé softwarové prostředky, které připomenou pravidelné přestávky. U těchto programů můžeme nastavit různé úrovně omezení, od vyskakovacího okna, jenž připomene zdravotní přestávku, až po zamčení pracovní plochy monitoru na určitou dobu. Program nám tak přináší ochranu zraku při dlouhodobé práci, a upozornění na dodržování přestávek, přičemž jeho obsluha je jednoduchá a běží na pozadí systému.

1.1.6 Poloha těla při práci na počítači

Naše zdraví při práci s počítačem ovlivňuje celá řada faktorů a o některých z nich jsme se již zmínili, ale na náš organizmus vždy působí tyto vlivy současně. Základem je určitě správné sezení, poloha těla u počítače je ovlivněna pracovním stolem, kancelářskou židlí a celkovým uspořádáním prostoru.

Při sezení je dobré dodržovat několik základních pravidel, kterým se někdy také říká pravidla pravých úhlů. Chodidla při práci musejí být na podlaze nebo na podložce, nesmí volně viset ze židle dolů, aby nedocházelo k tlaku na stehna. Lýtková část a stehenní část by spolu měla svírat pravý úhel, přičemž lýtko směřuje kolmo k zemi. Záda se stehny svírají také přibližně pravý úhel. Paže jsou volně podél těla, v ideálním případě spočívají na loketních opěrkách u židle. V lokti ruce opět svírají pravý úhel. Pracovní deska stolu je mírně pod úrovní dlaní, aby na ní mohli volně spočinout. Zápěstí se nesmí nepříjemně vytáčet či být ohnuté (ať již vzhůru či dolů). Pokud používáme podpěrky rukou při psaní, nesmíme o ně opírat zápěstí, ale spodní část dlaně, jinak dochází k tlaku na nervy karpálního tunelu. Monitor stolního počítače má být umístěn tak, aby vrchní část byla v úrovni očí. Vhodná vzdálenost je v rozmezí 40 – 60 centimetrů od očí. Samozřejmě závisí na velikosti monitoru, čím větší je jeho úhlopříčka, tím dále jej umístíme. Monitor také nesmí být umístěn tak, aby docházelo k odleskům. V učebnách je vhodné na okna umístit stínící rolety i pro případ, že učebna je severním směrem. Nejde pouze o monitor, ale i o další zobrazovací zařízení, například projektor, pro které je vhodné zatemnit okna. Myš používáme ergonomickou tak, aby ruka nebyla křečovitě sevřená. Při dlouhodobé práci s myší či pro sportovní hráče her jsou na trhu i myši s možností manuálního nastavení, aby padla uživateli „na míru“.



OBR. 2: SPRÁVNÉ SEZENÍ U POČÍTAČE

1.2 Nejčastější zdravotní potíže

1.2.1 Karpální tunel

Karpálním tunelem označujeme malý prostor mezi zápěstními kůstkami, kterým vedo u šlachy a nervy do dlaně a prstů. Při dlouhodobějším tlaku na zápěstí, například při opírání zápěstí o podložku či hranu klávesnice, stolu, nebo také držením myši, je vyvíjen tlak na kůstky a vazy v zápěstí a dochází k zužování tohoto prostoru a postupnému zánětu. Projevy tohoto syndromu jsou dobře prozkoumané. Onemocnění začíná brněním konečků prstů, které zesiluje v noci. To zejména proto, že procházející nervy ovládají jemnou motoriku. Mravenčení přechází poté ke slabosti, bolesti celých prstů a dlaně. Prsty začnou otékat, sníží se také

OBR. 3: MÍSTO VZNIUK ZÁNĚTU KARPÁLNÍHO TUNELU

hybnost. V konečných stádiích člověk postižený syndromem karpálního tunelu již neotevře plně dlaň. Oproti tenisovému loktu, který v klidu nebolí, bolesti spojené se zánětem karpálního tunelu se dostavují i v klidovém stavu a operativní řešení je tak nevyhnutelné.

Ukázka z článku pro žáky o princovi, jenž nebral varování v úvahu:

„ … Mladý pane, notebook ideální není, myš si kupte, i dockstation existují. Ruce jako pavouk skroucené máte, co ta záda polámaná? A pane, co na stole ten větráček váš pohledává? Přes ruce foukajíc, v budoucnu trpět budete. Mladý muž tyto výtky za hlavu hodil, vždyť chladný vzduch mu dobře dělal a notebook vše v jednom skýtal. Deformované tělo jeho poté večer ku Xboxu usedlo, aby ruce jeho od gamepadu další dávku dostaly. Ani pravidelná basketbalová hra zabránit tomu nemohla, cesta do pekla jasně vytyčená byla.

A jednoho pochmurného dne v ruce pálení, škubání a bolest ozvaly se. Mladý muž zkazky hrůzostrašné slýchával, nikdy však na bubáky nevěřil, a proto i tentokrát velkou váhu tomu nepřikládal. Bolest však o sobě stále více dávat věděla a mnohem pravidelněji a silněji svého nositele zachvacovala. Nebylo zbytí, i náš mladík si to přiznat musel – syndrom karpálního tunelu usídlil se v něm. …“ (Sedlák, 2009)

1.2.2 Tenisový loket

Dříve onemocnění, související především s vrcholovými sportovci se nyní přenáší do celé řady oblastí, kde dochází k monotónní a dlouhotrvající činnosti. Při psaní textu máme lokty položené na loketní opěrce kancelářského křesla a dlouhodobě zatěžujeme určité úpony šlach ke kostře, čím dochází ke vzniku zánětů. Zpočátku se onemocnění projevuje pouze při pohmatu či tlaku na vnější část loktu, později může dojít k otoku, silné bolesti a omezení možnosti pohybu. Typickým znakem je, že v případě, kdy je ruka v klidu a nevykonává žádnou námahu, bolesti sami ustupují.

1.2.3 Onemocnění páteře

Páteř je jednou z nejnamáhavějších částí těla při práci s počítačem. Žáci tráví sezením velkou část svého dne. Ve škole sedí v lavicích, doma u počítače. Doma navíc málokdy opravdu „sedí“ na židli a hrají různé hry online, spíše se povalují s notebookem či chytrým telefonem v křesle nebo v posteli a přispívají tak ke vniku různých onemocnění páteře.

Nejvíce zatížená bývá krční páteř. Ta nese celou váhu hlavy a umožňuje její pohyb do všech stran. Při práci s počítačem je přitom často hlava skloněná směrem dolů a tak dochází k zatížení krčních obratlů a jejich zablokování. Proto má být monitor umístěn tak, aby horní okraj byl v úrovni očí, a hlavu jsme tak drželi vzpřímeně. Hrudní část páteře většinou ohýbám do oblouku, nebo jednostranně zatěžujeme nošením notebooku v brašně přes rameno, místo batohu na záda. Bederní páteř nejvíce ovlivňuje to, jak sedíme. Nohy mají být u sebe, stehna svírat se zády přibližně pravý úhel a stejně tak s lýtky. Pokud si při sezení dáváme nohu přes nohu, nebo dokonce „zkroutíme nohu pod sebe“ dochází k vychýlení bederní části páteře. Svaly se pak přepínají jedním směrem a jsou nejčastější příčinou bolestí zad.

1.2.4 Zrakové potíže

Velký vliv má monitor na naše oči. Při delší práci může dojít k slzení očí, které jsou unavené, zarudlé a může dojít až k rozmazanému či rozdvojenému vidění, jež může skončit trvalým poškozením zraku.

Člověk běžně, bez povšimnutí, mrkne přibližně 15krát za minutu. Během sledování obrazovky se dlouhou dobu oko zaostřuje na stále stejnou vzdálenost, a aniž bychom si to uvědomovali, velmi se sníží intenzita mrkání. To je důležité zejména proto, že zvlhčuje povrch oční bulvy, čistí oko od nečistot a při jeho nedostatku je oko vysušené a lehce dojde k jeho podráždění či dokonce poškození. Pro tyto případy je dobré mít po ruce oční kapky a dělat pravidelné přestávky. Pro okohybné svaly je lepší, je-li horní hrana monitoru umístěna ve výši očí, které pak při práci směřují mírně dolů. Nesmí ovšem dojít k naklánění a namáhání krční páteře.

1.3 Jak předcházet potížím

Nejdůležitějším prostředkem pro předcházení různým zdravotním problémům je správné nastavení pracovního prostoru. I když přicházíme na jednu hodinu na výuku či zaskakujeme za kolegu, je nezbytné si vše nastavit tak, aby se nám co nejlépe pracovalo. Především výšku monitoru a židle, pokud je to možné. Pracujeme-li s počítačem dlouhodobě (bloková výuka informatiky, projekt tvořený na počítači apod.) je nutné provádět zdravotní přestávky a během nich alespoň některá kompenzační cvičení, která nám uvolní zatuhlé svaly po monotónní činnosti.

1.3.1 Cviky na oči

Procvičení očí patří mezi základní kompenzační cvičení, pro zdravý zrak sestavil například MUDr. Dušan Šponar Desatero správného vidění (Šponar, 2009):

1) Dioptrické brýle a čočky. Noste dioptrické brýle co nejméně. Považujte je za pomůcku při činnostech, při kterých musíte vidět jasně, a navykněte si je sundávat, jakmile takovou činnost ukončíte. Pokud se bez brýlí dostaví bolesti hlavy, namáháte příliš svůj zrak, místo toho, abyste se uvolnili a akceptovali svůj zrak.
2) Čtení zblízka. Nezaostřujte dlouhodobě na krátkou vzdálenost. Při práci na počítači se každých pár minut zadívejte do dálky.
3) Sluneční brýle. Během dne noste venku kvalitní sluneční brýle nepropouštějící UV záření. Toto záření je hlavní příčinou šedého zákalu.
4) Cvičení. Starejte se o pečlivě svůj zrak! Chcete-li pravdu zlepšit svůj zrak, začněte provádět pravidelné oční cviky.
5) Strava a tekutiny. Zlepšete svou stravu a vyhněte se zejména pokrmům, které obsahují velké množství cukru. Ten může způsobit otok oční čočky a zhoršovat krátkozrakost. Konzumujte méně tuků, pijte hodně tekutin, jezte celozrnné výrobky, hodně ovoce a zeleniny, nesolte.
6) Dieta. Trpíte-li šeroslepostí, doporučuje se dieta šetřící játra s omezením živočišných tuků spolu s pravidelným užíváním dýňových semínek.

7) Vitamíny a minerály. Trpíte-li šedým zákalem, doplňte následující živiny: denně multivitaminový přípravek plus navíc 50 mg zinku 400 jednotek vitamínu E 10.000 jednotek beta-karotenu a B-komplex.
8) Vývoj dítěte. Pro správný vývoj zraku je důležité, aby dítě mělo již od narození dobrý zrakový kontakt s vnějším svitem plným jasných barev a různých tvarů. Oční vada zvaná tupozrakost může být zhoršována umístěním kolébky u zdi.
9) Správné držení těla. Dbejte na správné držení těla! Astigmatismus může být způsoben špatným držením těla, kdy je hlava nakláněna ze zvyku k jedné straně.
10) Pozitivní přístup. Uvědomte si, že zlepšení vašeho zraku je možné.

1.3.2 Cviky na protažení rukou

Cvičení na protažení rukou po delší práci je celá řada a mnoho jich jistě známe. Připomeňme si alespoň nějaké, například můžeme předpažit ruce, uchopit navzájem dlaně a otočit je směrem vně. Tak procvičíme nejen prsty, ale protáhneme i vnitřní stranu paží. Zápěstí protáhneme nejlépe tak, že zatlačíme dlaní na hřbet druhé ruky

1.3.3 Cviky na protažení zad

Správné protažení zad jsme se jistě učili v hodinách tělocviku, připomeňme tedy alespoň pár jednoduchých cviků.

Posadíme se do tureckého sedu, narovnáme záda a obě paže položíme dlaněmi na temeno hlavy. Poté s výdechem přitlačíme bradu k hrudníku. Cvik můžeme provádět i na židli. V tureckém sedu může také z rovných zad sklápět hlavu do klína a vytvářet tzv. „kočičí hřbet.“ Obdobou je klasický kočičí hřbet, kdy si klekneme na kolena a dlaněmi se opřeme o podlahu, při nádechu poté prohneme hruď směrem k zemi, při výdechu prohneme záda nahoru. K protažení krční páteře použijeme jednoduché cviky na židli. Posadíme se vzpřímeně a hlavou kroužíme kolem tak, že zakloníme co nejvíce dozadu, poté položíme ucho na rameno, následně opřeme hlavu o hruď a druhé ucho na rameno. Přitom je důležité správně dýchat a držet rovná záda.

Cviků na protažení je celá řada a je dobré ve volné chvíli u počítače provádět aspoň některé z nich. Nejlépe v pravidelných zdravotních přestávkách.

Pracovní list – Jak správně sedět u počítače

Jméno a příjmení: **Třída:**

Škola:

1) **Který z obrázků zobrazuje správné sezení u počítače?**



2) **Tzv. karpální tunel je způsoben:**
   a) Dlouhodobým držení počítačové myši
   b) Špatnou opěrkou hlavy
   c) Dlouhodobým předkláněním hlavy
   d) „Blikáním“ CRT monitorů
3) **Vhodná vzdálenost pro umístění monitoru od očí je:**
   a) 15 – 30 cm
   b) 30 – 45 cm
   c) 45 – 55 cm
   d) 55 cm a více
4) **Pálení či svědění očí při delší práci je způsobeno hlavně:**
   a) Nedostatečným mrkáním
   b) Nastavenými barvami
   c) Okolním prostředím
   d) Špatně umístěným monitorem
5) **Pravidelné přestávky je třeba uskutečnit každých:**
   a) 10 minut
   b) 20 minut
   c) 30 minut
   d) 60 minut
6) **Mezi základní pravidla pro správné sezení je dodržování úhlů u nohou, trupu a paží o velikosti:**
   a) 40°
   b) 60°
   c) 90°
   d) 120°

Řešení k pracovnímu listu - Jak správně sedět u počítače

Otázka č. 1

Správná odpověď je poslední obrázek. První obrázek je tzv. chabé držení sedu, kdy není zpevněné svalstvo, je vyvíjen vysoký tlak na páteř a oči jsou blízko monitoru. Druhý obrázek zobrazuje sed „zborcený“, jenž opět neposkytuje žádné zpevnění a oporu pro páteř. V této poloze můžeme často vidět žáky při práci na notebooku či tabletu. Třetí obrázek znázorňuje správné držení těla.

Otázka č. 2

správná odpověď je a) Dlouhodobým držení počítačové myši, při němž je vyvíjen tlak na zápěstí, ve kterém dochází ke zúžení karpálního tunelu, kde procházejí nervy do dlaně.

Otázka č. 3

správná odpověď je c) 45 – 55 cm

Otázka č. 4

Pálení očí je způsobeno nedostatečným mrkáním, které si při soustředěné práci ani neuvědomujeme.

Otázka č. 5

Doporučený interval přestávek je každých 20 minut, během přestávky je vhodné provést protažení a některá kompenzační cvičení.

Otázka č. 6

Základní pravidlo doporučuje udržovat úhel 90° mezi lýtkem a stehnem, stehnem a trupem a také mezi paží a předloktím.

2 Rizika ztráty a zcizení dat

Ochrana našeho vlastního zdraví je patrně nejdůležitější, je jistě zapotřebí mít správně nastaveny veškeré hardwarové komponenty, aby se nám příjemně pracovala. Zdravotní přestávky nejsou důležité jen pro naše tělo, ale také pro duševní pohodu. Z dlouhodobého sledování monitoru kromě svalového napětí můžou také nastat bolesti hlavy, či psychické problémy. Ovšem naši duševní pohodu dokáže narušit nejen psychická námaha, ale také ztráta pracně vytvořených dat, ať už jejich napadením počítače pirátským software, jejich odcizením či smazáním kvůli fyzickému poškození. Tomu všemu je třeba také předcházet. V současnosti, kdy si každý nosíme malý počítač v kapse v podobě chytrého telefonu a naši žáci místo nového kola dostávají nové tablety, je především softwarová ochrana našich osobních údajů, které díky novým technologiím máme neustále po ruce a tak roste nebezpečí jejich zcizení.

2.1 Softwarové napadení počítače

Již s prvními počítači a programy, které mohli vytvářet vývojáři doma, se začaly objevovat také první počítačové viry. Prvním vir osobních počítačů byl v roce 1981 Elk Cloner a napadal počítače Apple II. Připojoval se k boot sektoru diskety a po infikování způsoboval uživateli obracení obrazovky, případně vyskakování blikajícího textu. Na prvních osobních počítačích firmy IBM se roku 1986 objevil vir Brain původem z Pákistánu.

V současné době existuje celá řada škodlivého software, který ohrožuje naše bezpečí, ruší naši práci a poškozuje počítač. Tím se dostáváme k tomu, co to vlastně vir je. Jedná se o prostý počítačový program, který někdo naprogramoval a vypustil do sítě. Souhrnně je tento software označován jako malware (z anglického Malicious software = zlomyslný program). Mezi základní znaky patří schopnost replikovat sebe sama a dále se šířit pomocí dostupných prostředků. K šíření poslední dobou přispěl obrovský boom internetu, organizace i jednotlivci jsou nuceni vynakládat nemalé prostředky na ochranu před různými útoky na jejich data.

Pro vytvoření malware je nutná dávka inteligence. Autoři jsou často dobrými programátory a k vytvoření viru je vedou různé důvody. Většina tvůrců pouze zkouší své schopnosti, zda dokáží proniknout do systému a napadnout počítač, řada z nich poté i pošle své viry

antivirovým společnostem. Dalším důvodem může být opravdové napadnutí počítače a získání tak citlivých údajů, například k internetovému bankovnictví, emailové adrese a další. Mohou také chtít pouze poškodit určitou organizaci nebo společnost, napadnou tak její síť a z ní se může již šířit vir do internetu jen jako vedlejší důsledek. Cílem také bývá ovládnutí počítače a vytvoření tzv. zombie, skrz něj jsou pak odeslány spamy a napadány další uživatelé.

Vytvořený malware poté dělíme do několika kategorií podle dopadu na uživatele:

- **Adware**
  - Jedná se o software, který znepříjemňuje uživateli práci s počítačem množstvím zobrazovaných reklam, vyskakovacích bannerů a podobně. Tento typ škodlivého software se většinou šíří jako součást jiného programu a uživatel jej často nainstaluje díky vlastní nepozornosti. Existuje řada programů vyhledávající a odstraňující adware, mezi nejznámější patří patrně Spybot Search & Destroy.
- **Spyware**
  - Funguje obdobně jako adware, uživatel je ale nevědomě nainstaluje s programem do počítače a poté dojde k zobrazování reklam, vyskakování bannerů a podobně. Ovšem spyware odesílá data o aktivitě uživatele (navštívených stránkách, spuštěných aplikacích, …), a pak zobrazuje cílené reklamy.
- **Červ**
  - Jako červ = worm se označuje program, který se dokáže samostatně dominovým efektem šířit, po své duplikaci a rozeslání na ostatní místa v síti. Kromě zahlcení komunikace v sítí, způsobuje také například nefunkčnost počítače či částí počítače a systému, prohledává data a odesílá je svému tvůrci. Základem červů se stal program, který ve společnosti XEROX měl za úkol hlídat vytížení procesoru a v případě uvolnění mu přidělit činnost. Druhá skupina červů, tzv. Nachi, měla za úkol najít chybu v systému a pokud se mu podařilo proniknout, stáhl z webu Microsoftu záplatu a poté restartoval počítač.

- V poslední době se internetem šíří červ blokující prohlížeč či uživatelský účet. Po infikaci se zobrazí varovné hlášení, upozorňují na zablokování prohlížeče a požaduje zaplacení poplatku za opětovné zprovoznění.

OBR. 4: TZV. POLICEJNÍ VIR (SCREEN OBRAZOVKY)

- **Hoax**
  - Hoax nás zaplavuje dnes a denně ze všech stran, nejen pouze z internetu. Dříve se tyto zprávy označovaly lidově jako „novinářská kachna.“ V současnosti k jejich masovému rozšíření přispěl především email. Hoax je jakákoliv zpráva, která se nás snaží přesvědčit o faktech a v závěru často ještě žádá o rozeslání dalším uživatelům, abyste je také varovali. Dříve se tak věřilo, že je nebezpečné šlápnout na jehlu, protože projede žilou do srdce. U banánu se nedoporučovala jíst špička, protože do ní koušou jedovatí pavouci a podobně. V současnosti se jedná spíše o řetězové zprávy vzbuzující soucit či naopak obavy z možné skutečnosti. Řada takovýchto zpráv se také snaží poškodit

podniky či velké společnosti například šíření zpráv o škodlivosti jejich potravin atd.

- Velkým fenoménem hoaxu je současně i facebook, kde sdílením přispějete 1 cent na operaci nemocného dítěte nebo zachráníte 10 štěňat. Protože těchto poplašných a matoucích zpráv přibývá, vznikla již v roce 2000 internetová stránka www.hoax.cz zabývající se ověřováním a zveřejňováním těchto sdělení.
- Ukázka hoaxu z února 2014 šířeného emailem: „Dnes jsem vezl docela dost vín na jednu akci přes pana z Charity Praha. Fakt docela velká objednávka, desítky kartonů a osobně vybrány vína kolem 600,- Kč za láhev. (…) Půlka z vín šla do auta nějakým papalášům z Charity, ale to jsem neřešil. Pak mi byly předány peníze, vše hotově a já jen tak mezi řečí se při nastupování do auta venku zeptal, co je to za akci. A jednalo se o počítání výnosu Tříkrálové sbírky za celou Prahu. Udělalo se mi dost šoufl a upřímně jsem měl slzy na krajíčku. Jen ukázka, jak je mimo jiné nakládáno s vybranými penězi na rádoby bohulibé účely… to Česko je …“

- **Trojský kůň**
  - Jak již název napovídá, jedná se o program, který se sice tváří jako neškodný a uživatel jej často nevědomě nainstaluje z přílohy v emailu. Oproti ostatnímu druhu malware je tento typ zákeřnější a může více narušit naše soukromí. Trojský kůň nejčastěji sbírá a odesílá data svému tvůrci. Může se jednat o keylogger, který sleduje stisknuté klávesy a tak získá přístup k našemu internetovému bankovnictví. Další typ otevře jakousi „cestu“ do počítače, tzv. backdoor, kterým může autor ovládat napadený počítač a využít ho tak k rozesílání spamu či sledování jiných zařízení v síti.
- **Spam, ham**
  - Spam = nevyžádaná emailová zpráva. Spam v současnosti nejvíce zahlcuje emailové schránky uživatelů. Tyto emaily jsou posílány na stovky emailových schránek současně, aniž by odesílatele zajímalo, zda se jedná o adresy dětí, dospělých, úředních schránek apod. Problémem je především množství času a energie potřebných k třídění, mazání a přenosu těchto zpráv. Podle agentury

ČTK[1] v roce 2013 tvořily spamy 70% emailů, z nichž většina pocházela z Číny a USA. Obdobou spamu je tzv. HAM, kdy již emaily nejsou odesílány náhodně, ale vytipovaným uživatelům, podle jejich aktivity na internetu.

- **Vir**
  - Tímto pojmem bývají často označovány všechny předešlé druhy malware. Počítačový vir má ale specifičnost v tom, že jako jediný se dokáže sám duplikovat, infikovat další soubory či dokumenty a rozeslat je dále do sítě. Viry jsou velmi nepříjemné, protože většinou způsobují velké škody. Mohou mazat či přesouvat soubory, blokovat otvírání aplikací či připojení počítače k síti. Jiné druhy mohou zatěžovat systém vysíláním množství požadavků.
- a další …

2.2 Jak se chránit proti napadení malware a ztrátě dat

Fyzické zabezpečení

- K USB flash diskům, paměťovým kartám a podobným zařízením by neměl mít přístup jiný uživatel. Ten může i neúmyslně infikovat tato úložiště a po připojení k našemu zařízení můžeme být napadeni i my. V případě, že již někomu (nebo i my od někoho) disk půjčíme, před jeho použitím necháme provést antivirovou kontrolu, což není nic obtížného. Většina rozšířených antivirů je zavedena do nabídky pod pravým tlačítkem myši. Klikneme ta na flash disk atd. pravým tlačítkem myši a zvolíme možnost zkontrolovat zařízení, najít viry na … Název činnosti pro kontrolu se již může měnit v závislosti na programu.
- Data, která máme na externím paměťovém médiu, je možné lehce zcizit. Důležité informace, přístupové flash disky s bezpečnostními certifikáty a podobně důležité věci je třeba uchovávat na bezpečném místě, ne na pracovním stole. Kromě zcizení hrozí také nebezpečí přírodních živlů, jako je voda, požár a jiné. Zálohy či archivy proto skladujeme na jiném místě, než je naše pracoviště. Při požáru kanceláře je velice pravděpodobné, že shoří či budou poškozena jak data v počítači tak i na záložních

[1] Podíl spamu loni mírně klesl. *Marketing a media* [online]. 2014, 24. 1. 2014 [cit. 2014-03-23]. Dostupné z: http://mam.ihned.cz/c1-61609590-podil-spamu-loni-mirne-klesl

discích v zásuvce stolu. Proto je uložíme do bezpečné schránky či trezoru, případně na jiném bezpečném místě na pracovišti nebo doma.

- Pro opravdu bezpečné uložení našich dat si můžeme pronajmout datový prostor ve středisku Fort Knox I, II ve Švýcarsku. Toto datové úložiště disponuje špičkovou technikou proti softwarovému napadení a je vybudováno v horách s velkou řadou bezpečnostních opatření před všemi možnými přírodními, ale i lidskými dopady. Servery jsou uloženy tak, že je neohrozí ani atomový výbuch a přístup do zařízení je umožněn pouze několika vyvoleným, kteří prošli vysokým stupněm zabezpečení.

Pracovat s bezpečným software

- V současné době již existuje oficiální a bezpečný software, který je alternativou k placené verzi. Můžeme používat operační systém Linux Mint, který má příjemné grafické rozhraní. Pro práci s daty (text, tabulky, prezentace), pokud nejsme nároční postačí on-line aplikace společnosti Microsoft, nebo lze stáhnout OpenOffice Org s totožnými funkcemi a mnoho dalších aplikací nahrazující placené produkty. Při instalaci a následném obcházení licencí software je velké riziko infikování počítače malware.

Bootování systému

- Při spouštění operačního systému dochází k tzv. bootování, neboli zavádění systému. Máme-li jej nastavené například na USB či CD-mechaniku, může při zavádění dojít k načtení viru. Při startu systému stačí kliknout na klávesu pro spuštění Dos (nejčastěji F11, Delete) a v nastavení bootování změnit priority a první zavést pevný disk.

Provádět pravidelné zálohy

- I přes dodržení veškerých pravidel, může dojít k nakažení systému některým druhem malware a my následně přijdeme o data. Je proto nutné provádět pravidelné zálohy na externí zařízení či server. O zálohách se budeme bavit dále.

Správná instalace software

- Při instalaci řady programů je vhodné nechat předem instalační soubory zkontrolovat antivirovým programem (viz Fyzické napadení - kontrola flash). Při samotné instalaci poté pozorně čteme všechny informace, které potvrzujeme. K řadě programů je připojen například program „Čištění disku“ nebo nástrojová lišta do okna prohlížeče. Při instalaci proto kontrolujeme zaškrtnuté kolonky a tyto instalace deaktivujeme.

Aktuální antivirové programy a systém

- Většině případů infekce předejde některý z antivirovýh programů. Do počítače neistalujeme současně dva programy kontrolující stejnou činnost (například AVG a Avast). Mohlo by dojít k jejich kolizi. U všech je ale nutné nechat provádět automatické aktualizace a neodkládat je na později, stejně tak i u operačního systému a dalších nainstalovaných aplikací.

Používat vlastní rozum

- Všeobecně známá věc - nestahovat neznáme přílohy, neotvírat podezřelé emaily, … Je často uživateli opomíjená. Je důležité při práci s počítačem přemýšlet a dávat si pozor na to, co sami dovolujeme instalovat a spouštět.

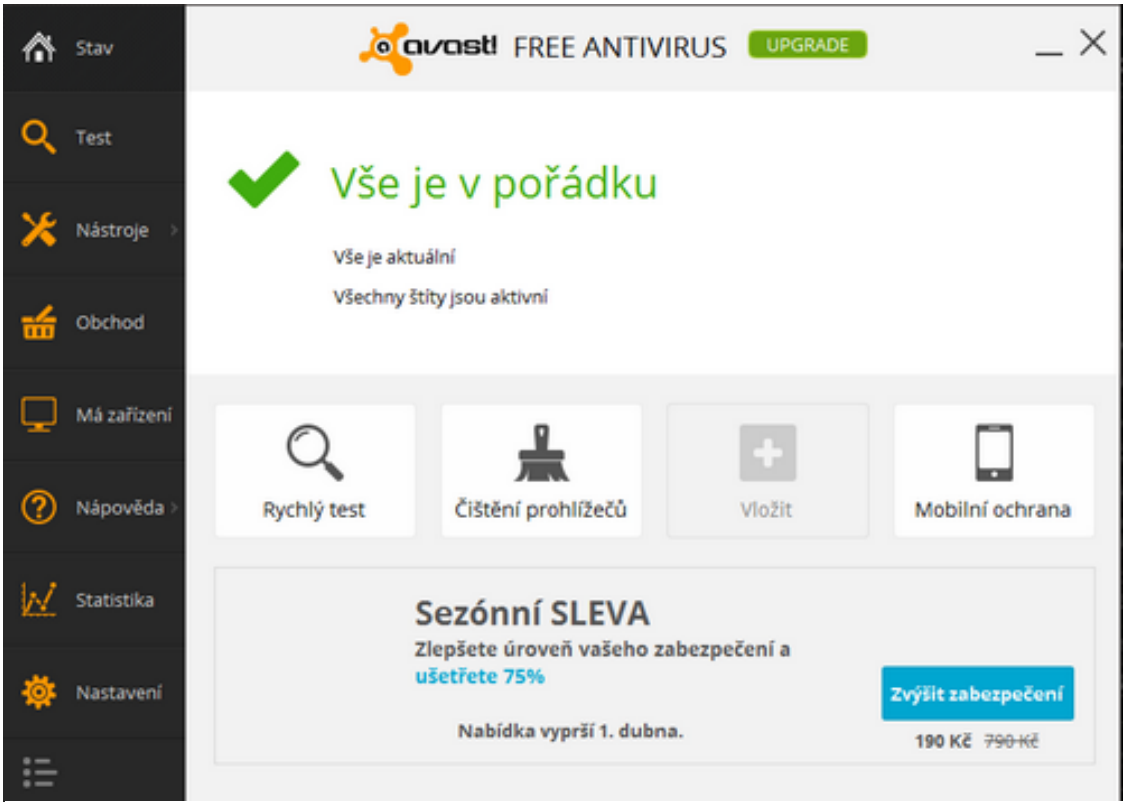
Informování

- Je důležité sledovat sdělovací prostředky a internetové stránky věnující se počítačové bezpečnosti (například www.viry.cz, www.hoax.cz, …). Mohou se zde objevit informace k hrozícím nebezpečím a jak jim předcházet. V případě napadení virem je důležité také tuto skutečnost oznámit všem, jejichž zařízení jste mohli ohrozit (firemní síť, usb klíčenky, apod.)

2.3 Antivirové programy

Hlavní obranou proti napadení našeho počítače škodlivým software je především vlastní zdravý rozum. Není dobré otvírat neznámé emaily, podezřelé zprávy ani instalovat aplikace z nedůvěryhodných zdrojů. Ovšem opatrnost nestačí a je třeba také mít nainstalovaný antivirový software a další software k odstranění různého malwaru.

- **Avast**
  - Avast! Free antivirus patří k nejlepším antivirovým programům, zdarma dostupným pro osobní či nekomerční použití. Kromě antiviru obsahuje také antispyware, kontrolu nežádoucích programů, kontrolu emailu a mnoho dalších aplikací, přitom je stále jednoduchý a po instalaci si jej nemusíme již všímat. Poslední verze avast! Free antivirus 2014 je také plně kompatibilní s novými Windows 8 a 8.1



OBR. 5: ANTIVIROVÝ PROGRAM AVAST! (SCREEN)

- **AVG**
  - AVG AntiVirus FREE 2014 je druhým rozšířeným antivirovým programem, který je nabízený zdarma pro domácí uživatele. Obsahuje všechny nástroje stejně jako avast!, dále pak například AVG Do Not Track, která kontroluje činnost webových stránek, zdali neukládají zbytečná data o uživateli či nestahují citlivé informace. U obou programů samozřejmě existují také jejich placené verze pro komerční využití či s nabídkou dalších služeb.

OBR. 6: LOGO AVG

- **ESSED NOD32**
  - ESSED SET NOD32 Antivirus 7 zajišťuje nejen standartní ochranu uživatele, ale nabízí také řadu dalších bezpečnostních prvků, které ochrání váš počítač a přenosná zařízení proti celé řadě útoků. Na základě známých kódů se také snaží vyhledávat a detekovat nově vznikající malware. Jako Antivirový program byl několikrát oceněn časopisem Virus Bulletin jako nejlepší antivir. Jeho základní instalace pro domácnost pro 3 stanice stojí 1249 Kč s DPH.

OBR. 7: LOGO ESSED NOD 32

- **Kaspersky**
  - Antivirový program Kaspersky Anti-Virus 2014 chrání počítač nejen před nebezpečími přímo z internetu, ale i z cloudu, aplikace čím dál rozšířenější mezi uživateli. Chrání proti virům, červům, trojský koním a dalšímu druhu malware, při čemž minimálně zatěžuje systém a také uživatele dotazy a informace mi o aktualizacích apod. Pro domácí použití je cena roční licence 449 Kč s DPH.

OBR. 8: LOGO KASPERSKY

2.4 Ochrana proti ostatnímu malware

- **Spyware Terminator**
  - Spyware Terminator 2012 je program, který v reálném čase hlídá počítač před napadením různým spyware, trojskými koňmi a adware. Automaticky spouštěné kontroly vyhledají software, který se mohl naistalovat bez vašeho vědomí a sbírat data o vás či zobrazovat reklamy na internetových stránkách. Od verze 2012 je součástí také aplikace Web Security Guard, která kontroluje činnost internetových stránek při jejich prohlížení. Program je opět pro domácí uživatele poskytován zdarma, s možnosti připlacení dalších služeb.
- **Ad-Adware**
  - Ad-Adware Free Antivirus + 11 ochrání zařízení především proti spyware, pop-up oknům a dalším sledovacím programům. Tento program je opět pro nekomerční použití v základní verzi zdarma, za příplatek si můžete zakoupit plnou verzi, která bude skenovaní provádět real-time a také navíc obsahuje utilitu pro kontrolu registru počítače a v případě jeho napadení dojde k okamžitému blokování.
- **Spybot**
  - Jako součást oblíbených prográmků, například pro zobrazování počasí na ploše či různých nástrojových lišt v prohlížeči, dochází často k instalaci spyware sledující vaši činnost na internetu a odesílající podrobnosti o vás na server, odkud jich již může jeho autor zneužívat. Spybot Search&Destroy dokáže takovéto aplikace vyhledat a blokovat. Program je pro nekomerční užití zdarma a ochrání nás před spyware, adware a dalšími útoky. Od poslední verze je též dostupná podpora pro Windows 8.

2.5 Ochrana dat pomocí šifrování

Pro případ, že i přes všechna naše opatření, používání antiviru a ochraně dat před ostatními uživateli, dojde k úniku osobních informací či jejich krádeži, můžeme je chránit pomocí šifrování. Šifrování je algoritmus, který převádí čitelná data na cízímu uživateli nečitelná. Celý proces probíhá na základě daného klíče. Šifrovací klíč je poté potřebný k otevření

zašifrovaného dokumentu neboli k dešifrování. Podle toho také rozlišujeme symetrické a asymetrické šifrování.

Při symetrickém šifrování je stejný klíč pro šifrování i pro dešifrování. Všichni uživatelé s tímto klíčem poté mohou otevřít libovolná data, která podle něj byla i zašifrována. Hodí se tedy hlavně pro komunikaci například jen mezi dvěma uživateli, případně pro šifrování našich osobních dat nebo při zálohování. Proces je také rychlejší a jednodušší.

Asymetrické šifrování využívá dvou klíčů, resp. jejich párů. Uživatel, který data šifruje, zadá klasický šifrovací klíč (standardně například heslo), který je stejný pro všechny. Pro otevření, dešifrování informací, je ale důležitá znalost druhého, dešifrovacího klíče. Podle něj se mohou každému uživateli zobrazit data určená pouze pro jeho osobu.

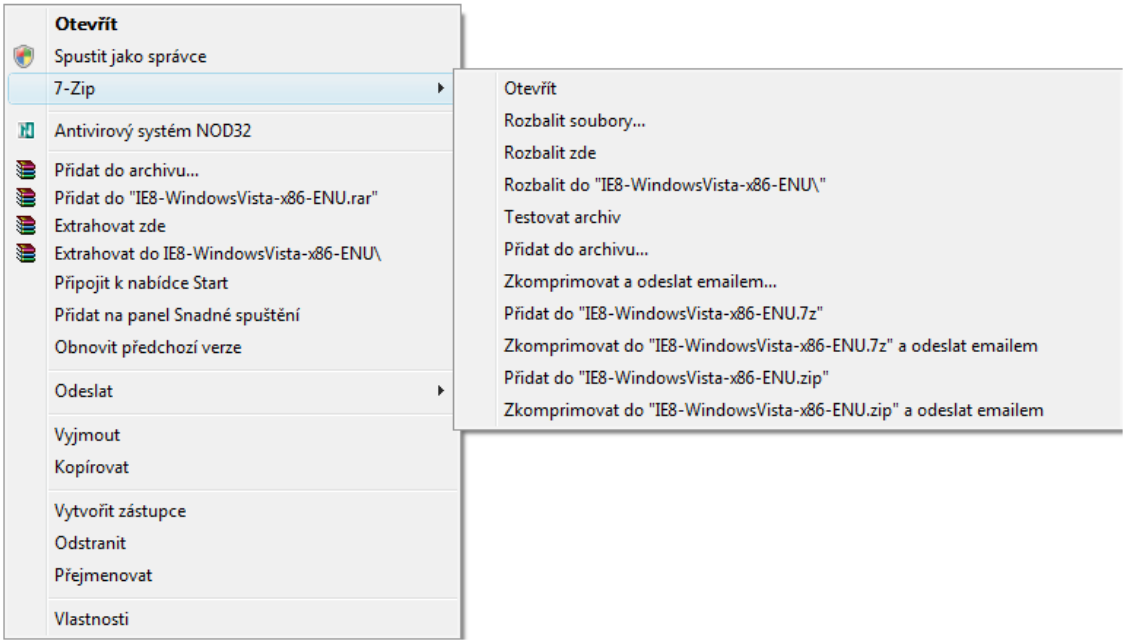
Společnost XEROX přišla také s novým způsobem šifrování dat, tzv. Intelligent Redaction (inteligentní redigování). Princip spočívá v tom, že je možné zakódovat pouze určitou část dokumentu, odstavec v textu, část v obrázkovém souboru. Současně i rozpozná tajnou informaci v ostatních souborech v počítači a provede jejich utajení. Uživatel tak vidí celistvý dokument, a nemusí si ani povšimnout zašifrovaných informací.

Většina uživatelů se šifrování obává, a vnímá jej jako něco, co je možné pouze ve velkých firmách či dokonce ve filmech. Pro šifrování existuje přitom celá řada programů, které jsou placené, ale i volně dostupné pro běžné uživatele. Je třeba pouze dbát na to a neplést si šifrování se zálohováním dat.

- **MyLock Box** – je velmi jednoduchý program zdarma dostupný. Při jeho instalaci uživatel zadá heslo a vybere složku, ve které chce mít utajené soubory. Po uzamčení této složky dojde k jejímu skrytí a pro ostatní uživatele je, stejně jako její obsah, neviditelná. Při spuštění programu je poté nutné zadat heslo, a skrytou složku odemknout. Nevýhodou tohoto programu je, že data jsou dostupná pouze uživateli na zařízení, kde je program naistalován. Soubory nelze zaslat jinému uživateli.
- **7-Zip** – Jedná se také o freewarový software, který ovšem určen především ke komprimaci či archivaci dat. Program 7-Zip pracuje se všemi běžnými formáty typu 7Z, ZIP, RAR, CAB, ARJ, LZH, RPM, DEB, GZIP, … Při instalaci se implementuje do nabídky pod pravým tlačítkem myši a při komprimaci složky tak postačí kliknutím

přímo na složku zvolit nabídku Komprimovat. Umí také vytvářet samorozbalovací EXE soubory, které je možné šifrovat pomocí hesla. Proti MyLock Boxu tak vytváří soubory, které jsou snadno přenositelné, případně je můžeme zasílat i jinému uživateli., který k jejich otevření bude potřebovat znát heslo.

- **Nabídka**



OBR. 9: ZAZIPOVÁNÍ SOUBORU (SCREEN)

2.6 SSO – systém bezpečného přihlášení

Technologie jednotného přihlašování (SSO z anglického single sing-on) přišla do České republiky před několika lety. Jedná se v základě o velmi jednoduchou myšlenku. Uživatel se zaregistruje na jediných stránkách a následně zde vyplní veškeré osobní údaje, které může vyžadovat přihlášení na jinou internetovou službu. Služby navíc získají přístup k aktuálním údajům, které má uživatel v SSO vyplněné a není proto třeba je ve všech účtech měnit adresu, telefon či email. Jednotlivé weby mohou aktuální údaje získat z hlavního účtu. Pro přístup k účtu SSO navíc uživatel používá certifikát, který zvyšuje zabezpečení jeho hesel pro další služby. Velkým rizikem u těchto služeb je, že pod jedním účtem máme všechny své přístupové údaje a hesla. Získá-li tak někdo náš certifikát pro přihlášení do služby, zpřístupní se mu tak veškerá hesla a přihlašovací údaje ke všem registrovaným účtům. Hlavním

provozovatelem v Česku je společnosti CZ.NIC, správce českých domén, který poskytuje zdarma pro uživatele službu MojeId.

2.7 Elektronický podpis

Elektronický podpis je obecný pojem, který označuje jakékoliv elektronický prostředek ověření identity. V podstatě rozlišuje 3 druhy elektronického podpisu. Digitální podpis, který je nejčastěji používaný. Sken ručního podpisu, který není moc bezpečný a lze jej jednoduše zfalšovat a biometrický podpis, který se provádí z biometrických vlastností jedince (otisk prstu, sítnice apod.).

V České republice upravuje užití digitálního podpisu zákon č. 227/2000 Sb. Jedná se o řetězec znaků o velikostí 0,5 – 3 kilobajty. Podpis je vázán na jednotlivý dokument a nelze jej tedy znovu použít. Každý uživatel dostane od vydavatele elektronického podpisu svůj klíč, který slouží k ověření identity.

Pracovní list – Ochrana dat

Jméno a příjmení: **Třída:**

Škola:

1) **Vyhledej v osmisměrce 7 základních druhů malware.**

A	T	R	O	J	A	N
X	D	P	H	L	J	Z
F	T	W	O	Č	K	M
M	E	U	A	E	C	R
A	W	B	X	R	I	J
P	A	R	H	V	E	D
S	P	Y	W	A	R	E

2) **Spoj správné dvojice**

Adware	Odesílá data z počítače tvůrci
Trojský kůň	Nevyžádaná pošta
HOAX	Zobrazuje reklamy
Spam	„Novinářská kachana“

3) **Mezi antivirové programy nepatří**
   a) AVG
   b) ASUS
   c) AVAST
   d) ESSED
4) **Co není uznáváno jako elektronický podpis:**
   a) Digitální podpis
   b) Sken ručního podpisu
   c) Biometrický podpis
   d) Sken občanského průkazu
5) **Jako šifrovací klíč je označován:**
   a) Klíč k otevření bezpečnostní chránky
   b) Heslo pro přístup k souboru
   c) Proces převodu dat do šifry
   d) Program kódující informace
6) **Zkratka SSO značí:**
   a) Mezinárodní kód pomoci při havárii počítače
   b) Systém jednotného přihlašení
   c) Systém sdílení dat organizace
   d) Správa souborů organizace

Řešení k pracovnímu listu – Ochrana dat

Otázka č. 1 - Osmisměrka:

Hledaná slova jsou – Trojan, Adware, Spyware, Hoax, Vir, Spam, Červ

A	T	R	O	J	A	N
X	D	P	H	L	J	Z
F	T	W	O	Č	K	M
M	E	U	A	E	C	R
A	W	B	X	R	I	J
P	A	R	H	V	E	D
S	P	Y	W	A	R	E

Otázka č. 2 – správné dvojice

a) Adware – Zobrazuje reklamy
b) Trojský kůň - Odesílá data z počítače tvůrci
c) HOAX – „Novinářská kachna“
d) Spam – Nevyžádaná pošta

Otázka č. 3

Asus (společnost vyrábějící počítače a další IT zařízení)

Otázka č. 4

Sken občanského průkazu – nikdy nikomu neposílejme oskenovaný OP

Otázka č. 5

Heslo k otevření souboru, přihlášení apod.

Otázka č. 6

SSO je systém jednotného přihlášení, z anglického single sing-on

3 Zálohování

Každý z nás vytváří při práci na počítači množství dat. Ať už jsou data užitečná a významná, nebo jde jen o jakési „hraní a zkoušení“, je důležité se také zabývat otázkou ochrany těchto dat, jejich ukládáním, vytvářením záloh a případnou archivací pro budoucí využití. Strávit několik hodin na nějakém úkolu a následně práci ztratit například tak, že omylem naformátujeme jiný flash disk, je velmi nepříjemné. Proto je záloha a archivace důležitá.

3.1 Zálohování a archivace

Při zálohování dat dochází k vytváření kopií původních dat. Takovéto zálohy jsou velmi vhodné v případě, že dojde k fyzické ztrátě, například z důvodu selhání hardware. Poškození pevného disku, flash disku či optického disku je nejčastější příčinou. I když existují specializované firmy, zabývající se obnovou, nebo pokusem alespoň o částečnou obnovu ztracených dat, celý proces je pro uživatele značně finančně náročný, a proto je lepší mu předcházet. Zálohujeme především taková data, která jsou důležitá, nebo jejich vytvoření zabralo nemálo času. Data ze zálohy je možné rychle obnovit, v případě potřeby by měla být uživateli záloha rychle dostupná a jejich obnova nenáročná. Zálohujeme nejčastěji kontakty, rozpracované dokumenty, data aktuální pro rozpracovaný projekt atd. Záložní kopii proto průběžně ukládáme také na jiné úložiště, odkud ji je možné rychle obnovit.

Archivace, na rozdíl od zálohování, které vytváří kopii existujících souborů, slouží k trvalému uložení dat, například fotografií. Tato data průběžně nepoužíváme a nevyžadujeme tak jejich rychlou obnovu. Při archivaci můžeme také soubory komprimovat do formátu .zip či .rar a ušetřit tak místo. Archivovaná data je nutné ukládat na externí úložiště a v ideálním případě také v jiných prostorách, aby případné přírodní živly nezničily jak náš počítač, tak i naše archivy. Při archivování nejčastěji také odstraňujeme původní data z počítače.

3.1.1 Druhy zálohování dat

Základním rozlišením záloh je způsob ukládání dat, podle toho, jak přidáváme nové zálohy. Existuje několik druhů:

- **Nestrukturovaná** – Tento typ zálohy probíhá nejčastěji na optické disky v domácnostech, či menších firmách. Na DVD jsou vypalovány nepotřebné soubory, fotografie, filmy, které by se někdy mohli hodit. Disky jsou popisovány často pouze jako Záloha 1 ... X, v lepším případě názvy složek. V takto vytvořené záloze se těžko vyhledávají soubory pro obnovení, disky se kupí až z nich je pěkný „komínek“.
- **Plná a následně inkrementální (přírůstková)** - Při prvním zálohování tohoto typu je vytvořena úplná záloha všech dat uživatele. Následné zálohy již neukládají znovu celá data, ale pouze ty soubory, které byly od poslední zálohy změněny nebo vytvořeny. Při využití inkrementální zálohy nejsou tak vysoké požadavky na úložný prostor, ovšem při obnovení je třeba, aby byl celý řetězec záloh kompletní, protože při poškození jedné části, dochází ke ztrátě i v ostatních zálohách.
- **Plná a následně diferenciální (rozdílové)** – Jak už název napovídá, opět začínáme zálohou všech souborů a dokumentů. Při dalším zálohování ovšem oproti inkrementální záloze, která zaznamenává následné změny a řetězí tyto změny, diferenciální záloha vytváří nové zálohy všech následně změněných a nově vytvořených dokumentů. Výhodou tohoto typu tak je, že při ztrátě některé části, neztratíme zálohy následující. Nevýhodou je větší náročnost na skladovací prostor. Často také dochází k automatickému mazání předešlých záloh a zanechání několika posledních. Na tomto principu funguje známá funkce operačního systému Windows Obnovení systému.
- **Průběžná záloha** – Každý z nás se již setkal například ve wordu, kdy po nechtěném vypnutí, pádu systému apod. je nám nabídnuta poslední verze rozpracovaného dokumentu. Postupné změny se ukládají to tzv. žurnálu změn (logu), ze kterého je lze opět obnovit po nechtěném pádu programu.
- **Záloha celého systému** – Tento typ zálohy užíval třeba operační systém Windows XP. Při nastavení automatických záloh docházelo pravidelně k zálohování celého disku počítače. Zálohovány byly nejen soubory a dokumenty, ale také systémová nastavení a uživatelské účty. Tato záloha je velmi náročná na prostor a kapacitu záložních médií.

3.1.2 Zálohovací schémata

Jedním ze základních prvků zálohování, je správné použití zálohovacích zařízení. Pokud bychom měli dva zálohovací disky, a celý rok ukládali na jeden a následující rok na druhý disk, je velká šance, že disk pro aktuální dobu bude spíše poškozen. Proto existují tři základní zálohovací schémata.

Grandfather – Father – Son – Toto zálohovací schéma je složité především na hardwarové prostředky. Základem jsou 3 sady zálohovacích zařízení. Na první sadu je prováděna denně inkrementální záloha. Jsou zapsány pouze změny a nové soubory. Na druhou sadu je prováděna úplná týdenní záloha a na třetí sadu zálohujeme všechna data jednou měsíčně. Denní záloha je označována jako Son, týdenní jako Father, a měsíční poté jako Grandfather.

Round – robin – Jedná se o nejjednodušší princip zálohování. Podle počtu zálohovacích zařízení rozdělíme týden na jednotlivé úseky a každá týden ve stejný den provádíme zálohu na určité zařízení. Pro 5 zařízení si na každý den vyhradíme jedno a denně provádíme zálohu. Následující týden postupně pak přepisujeme zálohy od nejstarší (pondělní) po nejmladší (páteční). K dispozici tak jsou vždy poslední 4 zálohy. Tento typ zálohování je vhodnější pro domácí užití či menších podniků.

Tower of Hanoi – Jak už název napovídá, zálohování probíhá na principu známé logické hry. Vyžaduje použití pěti zálohovacích sad, nazývaných media set. Na tyto sety probíhají střídavě zálohy podle určitých dní a media sety jsou užívány v šestnácti denních cyklech. Tento typ je velmi složitý a vyžaduje speciální zálohovací software.

3.2 Hardware prostředky pro ukládání a zálohování dat

3.2.1 Optické disky

Optická média nejsou nejvhodnější pro ukládání a archivaci většího množství dat, hodí se například pro video soubory, případně hudbu a fotografie. Vyhledávání určitých dat na optických discích není nejrychlejší ani nejpohodlnější. Při ukládání je potřeba také dodržovat několik zásad, především ideální teplota (kolem 22°C) a vlhkost (cca 55%). Životnost je kolem 100 let u lisovaných disků, jejich čitelnost ovšem klesá s každým použitím. U doma

vypalovaných disků a podle přístupu uživatelů se životnost zkracuje až na pouhých 7 let. Problémem je také fyzické poškození disku.

3.2.1.1 CD disky

První CD vyrobily firmy Sony a Philips v roce 1979 a původně vznikla jako náhražka gramofonových desek. Disky měly sloužit především pro záznam a ukládání hudby. Od toho se odvíjela i kapacita. První návrh kapacity byl 60 minut hudebního záznamu, ovšem dnes se již vyrábějí všechny CD disky s kapacitou 74 minut záznamu, což odpovídá 700 MB. Jedním z důvodů pro tuto kapacitu byl ten, aby se na disk vešla celá Devátá symfonie Ludwiga van Beethowena.

Disk se skládá ze tří vrstev. Spodní bývá polykarbonátová, do které je při výrobě vyznačena drážka pro vedení laserového paprsku. Tato vrstva slouží jako ochranná pro střední vrstvu. Ta je tvořena nejčastěji stříbrnou fólií (dříve zlatou) obsahující barvivo. Do vrstvy barviva probíhá samotný záznam dat. Záznam probíhá mechanicky, ozáření barviva laserem dochází ke změně struktury a vznikají díry, označované jako pity, které jsou jakýmisi prohlubněmi v zapisovací vrstvě. Při výrobě originálních disku se tyto pity lisují přímo do zapisovací vrstvy, jsou tak výraznější, hlubší a lisovaná CD tak mají vyšší životnost. Při vypalování mají pity nepravidelné okraje a jsou i méně hluboké, proto životnost optických disků vypalovaných doma není tak vysoká. Poslední vrstvu tvoří ochranná fólie na kterou je možný popis disku či jeho potisk.

Na CD se zapisuje obdobně jako na LP spirálovitě. Oproti gramofonové desce zápis a čtení neprobíhá od kraje ke středu, ale od středu. Standartní rozměry disku jsou 1,2 mm tloušťka, 120 mm průměr a 15 mm průměr vnitřního otvoru. Na disku je přibližně 15 tisíc závitů, což odpovídá pěti kilometrům dráhy.

Na disk můžeme zapisovat dvěma způsoby. Singlesession zapíše data v jedné stopě a poté je disk uzavřen a již na něj není možné nic dalšího zapsat a je možné čtení v jakékoliv mechanice. Druhá technika multisession neuzavře po zápisu disk. Je možné tak přidávat postupně další data až do zaplnění. Tento typ má nevýhodu v tom, že disky nelze přehrát v běžných přehrávačích.

CD disky se dělí do několika skupin, které jsou definovány vždy podle barvy knihy:

- **Audio CD – Červená kniha** – Tento standart je definován roku 1980 a je určen primárně pro záznam hudby. Minimální délka záznamové stopy je 4 sekundy a na disk je možné zaznamenat maximálně 99 záznamových stop.
- **CD-ROM – Žlutá kniha** – Disk na který lze uchovat data i hudbu. Záznam v typu Mode 1 dělí disk na dva sektory, první je určen pro hudbu a druhý sektor pro data. V typu Mode 2 není žádný vyhraněný prostor.
- **CD-R, CD-RW – Oranžová kniha** – CD-R je disk určený pro několikanásobný záznam dat, tedy záznam multisession. Typ CD-RW umožňuje vymazání zapsaných dat na disku a jeho znovu vypálení.
- **CD-i – Zelená kniha** – Jedná se o typ, který se nerozšířil, ovšem měl sloužit pro záznam dat z počítače. Pro jejich přehrání je třeba speciální přehrávač.
- **CD – Video – Bílá kniha** – Tato kniha definuje standart pro komprimaci videí tak, aby se vešla na disk o kapacitě 700 MB. Kvalita takovýchto videí dosahuje kvality záznamu na VHS.
- **CD – Extra – Modrá kniha** – Definuje záznam dat a hudby na disk tak, aby HIFI systémy či jiné přehrávače přehráli bez problému zvukový záznam.

3.2.1.2 DVD disk

DVD začala vznikat v roce 1994. Původně se jednalo o dvě korporace, Multimedial CD a Super Disc, které spolu soupeřily. Obě zařízení nebyla navzájem kompatibilní a velké počítačové firmy jako Microsoft a Apple se je rozhodly nepodporovat oba formáty. Společnosti se vzájemně dohodly na jednotném formátu a v roce 1995 vzniklo první DVD-ROM. Název DVD původně označoval Digital Versatile Disk (digitální víčeúčelový disk), firma Dollywood jej často označovala jako Digital Video Disk. Dnešní zkratka DVD již je oficiálním názvem produktu.

DVD má obdobné technické parametry jako CD, především rozměry. Oproti délce pitu 0,83 mikrometru a rozestupu drážek 1,6 pitu u CD, má DVD disk hustší záznam. Pit se zkrátil na 0,4 mikrometru a rozestupy jsou pouze 0,74 mikrometru. Zápis opět probíhá spirálově od středu ke kraji.

Kapacita disku se proti tomu navýšena několikanásobně a dělí disky do 4 kategorií:

- **DVD 5** má kapacitu 4,7 GB. Záznam probíhá na jedné straně v jedné vrstvě. Disky se označují jako DVD-RAM, DVD±R, DVD±RW.
- **DVD 9** dosahuje kapacit 8,5 GB. Záznam je opět na jedné straně, ovšem probíhá ve dvou vrstvách. Disky se označují DVD±R DL.
- **DVD 10** má kapacitu 9,4 GB. Jedná se o oboustranné DVD tvořené dvěma disky DVD 5.
- **DVD 18** je oboustranný disk tvořený dvěma disky DVD 9. Jeho kapacita je 17,04 GB.

Stejně jako standarty u CD, vznikla v roce 1998 organizace DVD Fórum, která stanovila základní vlastnosti disků.

- **DVD – RAM:** Nejstarší typ média. Je určen především pro počítače a nebývá kompatibilní s běžnými přehrávači. Životnost tohoto typu disku se uvádí až 30 let.
- **DVD – R:** Tento typ disků přečte většina zařízení. Oproti předchozímu typu je možné na něj zapisovat rychlozí 18x.
- **DVD + R:** Typ je téměř shodný s předchozím, ovšem je možné na něm přeskakovat různé části filmů. Oba dva disku jsou také tvořeny dvěma kotouči o tloušťce 0,6 mm. Záznamová vrstva je mezi těmito kotouči a data jsou tak více chráněná před poškrábání.
- **DVD ± RW:** je shodný s disky DVD±R, ovšem umožňují smazání a přepis disku až tisíckrát.
- **DVD ± R DL:** Od roku 2005 jsou na trhu disky, ve kterých probíhá záznam do dvou vrstev. Dvojnásobná kapacita je velmi vhodná pro ukládání dat a jejich archivování

3.2.1.3 BLU-RAY, HD-DVD

Historie těchto dvou typů disků se začala psát v roce 2000, kdy filmy v nových větších rozlišeních již nebylo možné nahrát na běžná média. V Japonsku došlo ke zdokonalení vlastností modrého laserového paprsku a díky jeho vlastnostem se stal novým typem pro optické disky. Modrý paprsek má kratší vlnovou délku, přibližně 405 nanometrů, což

umožnilo zmenšení velikosti pitů a drah mezi nimi z původních 1600 nm u CDčka na 320 nanometrů u Blu-ray. V současnosti ovšem je stále finančně náročné pořízení disků a mechanik.

HD DVD vzniklo přibližně ve stejnou dobu jako Blu-ray a zpočátku spolu tyto technologie soupeřily. Obě technologie ovšem nebyly vzájemně kompatibilní a velké filmové produkce spíše preferovali Blue-ray od firmy Sony. Společnost Toshiba vyvíjející HD DVD tuto technologie přestala dále rozvíjet v roce 2008, kdy v únoru oznámila její konec.

Technické parametry disku jsou stejné jako u CD a DVD, způsob zápisu je ovšem zcela rozdílný, a tak je Blue-ray nekompatibilní. Blu-ray paprsek je zapisován modrým laserem o vlnové délce 406 nanometrů. Délka pitu je pouze 0,15 mikrometrů a probíhá pouze 0,1 mm pod povrch. Základní kapacita je 25 GB.

Disky jsou označovány jako BD-ROM, sloužící pouze pro čtení, BD-R umožňující zápis a BD-RW na nichž je možný i přepis.

3.2.2 Pevné disky

V roce 1953 vyvinula firma IBM první pevný disk. Jeho kapacita byla pouhých 5 MB, což ovšem na tu dobu byl velký úspěch. Cena toho disku byla také velmi vysoká, kolem $200 000. V roce 1980 byl vyvinut disk o velikosti 5,25 palců ve firmě Shugart Associates, která existuje do dnešního dne pod názvem Seagate Technology. Velikost disku 3,5‘‘ vznikla roku 1983 a o pět let později došlo také ke snížení výšky a disky tak získaly dnešní podobu. Následně docházelo už k pouze k miniaturizaci disků a navyšování kapacit.

Pevné disky jsou velmi vhodným médiem pro ukládání dat. Není tu tak velké riziko fyzického poškození. Lze na nich velmi rychle vyhledávat uložená data a obnovit je. Jejich kapacita je mnohokrát vyšší než u optických médií. Zápis i čtení je mnohokrát rychlejší. Pevný disk lze skladovat v běžných pokojových podmínkách. Při používání se s disky nesmí pohybovat, předejdeme tak jejich mechanickému poškození. Data na disku vydrží relativně dlouhou dobu, záruční doba na většinu zařízení je 5 let, ovšem životnost při správném skladování může být až sto let.

3.2.2.1 HDD

HDD (Hard Disk Drive) označuje starší, ale rozšířenější typ pevného disku. Jeho princip a struktura je plně mechanická. Tělo disku, označováno jako šasi, je hermeticky uzavřeno, aby se dovnitř nedostaly žádné nečistoty. Uvnitř nalezneme sadu disků, na které zapisovací (a zároveň čtecí) hlavy ukládají data obdobně jako na optické disky. Zápis probíhá na tzv. plotny, což je sada disků. Ty se otáčení rychlostí až 15 tisíc otáček za minutu. Hlavy se nacházejí pouze jeden mikrometr nad samotným diskem. Jejich pohyb po disku zajišťuje vystavovací mechanizmus, jímž pohybuje lineární motorek. Dále zde nalezneme řadu konektorů pro připojení, vyrovnávací paměť pro rychlé načítání apod.

Mezi základní vlastnosti disku patří jeho rozměr. V současnosti nejrozšířenějším typem disku jsou 3,5“ a 2,5“ disky. Dalším parametrem je určitě kapacita disku, která se oproti počátečním pěti megabajtům několikanásobně zvýšila, a v současnosti je již možné pořídit disk běžně o velikosti dvou až tří terabajtů. Důležitý je počet otáček za minutu (RPM). Běžné disky se otáčí rychlostí 4 – 8 tis. otáček za minutu, oproti profesionálním zařízením s rychlostí až 15 tisíc ot./min. Pro připojení se nejčastěji využívají sběrnice ATA, eSATA, USB či FireWire u externích disků.

Data na disku jsou uložena v kruhových spirálách. Stopa je poté dělena na sektory o minimální délce 4096 B.

Celý disk je mechanickým zařízením, které je citlivé na otřesy a nárazy. Je-li v činnosti, nemělo by se s ním nijak pohybovat, aby nedošlo k dotyku hlavy s plotnami a jejich poškození, které je neopravitelné. Při vypnutém disku hlavy nejsou nad záznamovou plochou a nemůžou ji tak poškodit. Skladování je možné za běžných podmínek. Teplo nesmí přesáhnout 50°C a samozřejmě, jako každé jiné elektrické zařízení nesmí přijít disk do styku s vodou. Životnost může být až 100 let.

3.2.2.2 SSD

SSD disk (Solid-state drive) není oproti HDD tvořen pohyblivými mechanickými částmi, ale sadou energeticky nezávislých flash pamětí. Jednotlivé komponenty jsou osazeny na tištěném spoji. Rozměry disku SSD jsou shodné s rozměry klasických HDD, aby byla zajištěna

kompatibilita. Menší verze těchto disků jsou často umísťovány do přenosných zařízení (notebooky, tablety apod.) protože nejsou náchylné k otřesům. Neobsahují žádné pohyblivé části, jsou tedy i tiché a neruší. Další jejich výhodou je také nízká spotřeba energie.

Hlavním nedostatkem disků SSD je jejich cena. Oproti klasickým HDD diskům je jejich cena je nesrovnatelná a zdaleka nedosahují takových kapacit. Zatímco HDD o kapacitě 2 TB stojí kolem dvou tisíc korun, disk SSD o kapacitě 500 GB lze pořídíme za deset tisíc korun. Tím se dostáváme i k druhému problému, kterým je maximální kapacita, jenž je kolem 500 GB, kdežto disky HDD lze pořídit i s kapacitou 4 TB.

3.2.3 Flash disky, paměťové karty

3.2.3.1 Flash disky

První disky flash, či USB klíčenky, jak jsou někdy nazývány, se začaly objevovat v roce 2000 a jejich kapacita byla 8 MB. Vzhledem vysokému konkurenčnímu boji ovšem jejich cena rychle klesala a tak zcela vytlačily diskety. Jejich velkou výhodou je snadná manipulace, přenositelnost a v neposlední řadě také kapacita v porovnání s cenou. Největšího rozšíření se dočkaly disky s kapacitou 8GB, v současnosti jsou ovšem k dispozici disky až s 128 GB místa. Nejsou náročné na skladování a lze je nosit po kapsách.

USB disk se skládá pouze z tištěného spoje, který je osazen energeticky nezávislou flash pamětí. Celé zařízení je uloženo v ochranném pouzdře. Rozměry flash disku mohou být velmi malé, řádově v několika desítkách milimetrů. Dražší typy obsahují také mechanický přepínač, chránící disk proti přepsání.

Výhodou těchto zařízení pro zálohování informací je jejich nenáročnost, připojit je lze prakticky k jakémukoliv zařízení a mít tak potřebná data stále s sebou. Data na disku je třeba chránit především proti fyzickému přístupu a vnějším vlivům (teplota, vlhkost). Řada disků obsahuje vlastní šifrovací software.

3.2.3.2 Paměťové karty

Paměťové karty oproti flash disku jsou mnohem menší (mikro SD) a nelze je připojit klasickým USB konektorem, jinak fungují v principu obdobně. Používají se především

do zařízení, ve kterých rozšiřují vnitřní paměť (fotoaparáty, mobily, tablety, …). K počítači jsou poté nejčastěji připojovány skrze tato zařízení. Pokud bychom chtěli přesto kartu připojit přímo do počítače, je třeba mít čtečku paměťových karet a případně adaptéry pro jednotlivé druhy. Skladování není nijak náročně, stačí se vyvarovat extrémním teplotám a vlhkosti, obdobně jako u USB disků.

3.3 Online datová úložiště

Trendem poslední doby je neumisťovat všechna data na svých serverech, záložních discích či nosit s sebou disky flash, ale s rozšířením internetového připojení pomocí mobilních sítí, či wifi, připojení, která zdarma nabízí již většina velkých měst i na veřejných prostranstvích, mít všechna data uložená v jakémsi virtuálním disku na internetu, tzv. cloudu. Tento systém nám umožňuje svá data mít kdykoliv k dispozici a často s nimi i pracovat jen s pomocí internetového prohlížeče. Mezi prvními kdo tuto službu nabídl byla společnost Google se svým prostředím Google disk a za ním následovali rychle další (Sky Drive Microsoftu, iCloud od Apple).

Řada uživatelů propadla novému trendu a mají tak prakticky všechny své dokumentu uložené na některém virtuálním úložišti, ovšem málo kdo z nich si uvědomuje, že takto poskytuje informace třetím stranám. Mnoho lidí také využívá tyto služby pro ukládání záložních souborů, aniž by se zajímala o bezpečnostní prvky, které samotné servery nabízejí. Musíme také myslet na to, že často těchto služeb využíváme zdarma a bez záruk. Většina webových úložišť je k dispozici v bezplatné verzi pro domácí uživatele. Nabízejí také programy pro většinu současných zařízení (PC, tablety, mobily), pomocí kterých lze jednoduše nahrávat soubory a případně s nimi pracovat.

DropBox

Jedná se pouze o webové úložiště, které umožňuje především ukládání a sdílení souborů s ostatními uživateli. Pro ukládání souborů je možné využít buď klienta, kterého lze naistalovat do počítače, nebo webové prostředí. To ovšem omezuje velikost nahrávaného souboru na 300MB. Úložiště je provozováno dle pokynů DMCA, dodržuje tedy autorská práva, ovšem vyhrazuje si také právo jakýkoliv soubor smazat. Samozřejmostí je zákaz nahrávání pornografického a ostatního závadného materiálu.

Google Disk

Online úložiště společnosti Google nabídlo kromě možnosti ukládání souborů, jejich synchronizaci pomocí aplikace pro jednotlivá zařízení, on-line správu textových, tabulkových a prezentačních souborů. Dále je k dispozici kalendář s osobním plánovačem a samozřejmě vše provázáno s emailem. Dnes už tato služba nabízí celý balík aplikací včetně převodu pdf do textu a dalších.

One Drive

Toto uložiště vzniklo jako odpověď na Google disk a bylo také zdarma poskytnuto uživatelům. Jeho předchůdcem byl tzv. Office 365, který jako profesionální nástroj přetrvává dodnes. Samotný název One drive je platný až do letošního roku, služba byla dříve dostupná pod názvem Sky drive. Velkou výhodou tohoto prostředí je plná kompatibilita s Microsoft office, a také nástroje pro on-line úpravu dokumentů jsou graficky velmi podobné Office 2007, ovšem s některými omezeními.

3.4 Síťová úložiště

Ve větších organizacích, firmách a často i ve školách existuje jedno úložiště pro centrální ukládání dat a zálohování. Ostatní uživatelé mají tak přístup ke společným datům a není potřeba přenášet soubory na discích nebo je posílat emailem. Při centrálním zálohování není třeba každý počítač chránit například záložním zdrojem, ten pak stačí například pouze pro server nebo pro počítač určený k ukládání dat. Pro data se používá několik pevných disků osazených v jednom zařízení, které je buď přímo v serveru, nebo ve vlastní síti. Tato úložiště dělíme podle systému ukládání dat a druhu připojení v síti.

3.4.1 RAID diskový pole

RAID znamená "Redundant Array of Independent Disks", neboli záložní pole tvořené sadou nezávislých disků. Pro ukládání dat je užito několik disků, což umožňuje zvýšit ochranu dat před jejich ztrátou způsobenou smazáním či hardwarovou poruchou. Sada disků se pro počítač tváří jako jeden logický svazek a technické propojení je řešeno softwarově nebo hardwarově. Při softwarovém řešení se o spojení do logické jednotky postará operační systém. Toto řešení

je sice levnější, ale náročnější na výkon počítače. Hardwarově spojení řeší řadič. V tomto případě se jedná o dražší variantu, kdy je diskové pole umístěno v samostatné skříni, která obsahuje nejen řadič, ale i vyrovnávací paměť s velkou kapacitou.

Podle způsobu ukládání dat existuje několik druhů diskových polí. Ovšem nesmíme zapomínat na to, že aby diskové pole mohlo být užito k zálohování, je třeba ho chránit také před vnějšími vlivy jako je oheň a voda.

RAID 0

I přesto, že je tento typ nejběžnější, určitě není nejbezpečnější. Disky jsou zapojeny sériově. Data jsou na disk ukládána buď střídavě, nebo postupně tak, že se zaplní nejdříve jeden disk a pak se začne zaplňovat další. Jediným pozitivním v tomto případě je zvětšení prostoru pro ukládání dat.

RAID 1

Tento typ je česky označován jako zrcadlení. Je zapotřebí minimálně dvou disků, případně jiný sudý počet, protože data na jednom disku jsou stejně zapisována na disk druhý. V případě výpadku jednoho disku tak nejsou žádná data ztracená. Nevýhodou je ovšem finanční náročnost, protože skutečná kapacita je pouze poloviční oproti fyzickému prostoru. Jedná se o jednoduchý a často bezproblémový systém, který je využíván na malých sítích.

RAID 5

RAID 5 je nejoblíbenější systém pro větší firemní či školní sítě. K jeho fungování je zapotřebí min. tří disků, kdy na první dva jsou data ukládána střídavě, a na třetí probíhá zápis samo opravného kódu. Při výpadku jakéhokoliv disku pak neztrácíme žádná data. Pro větší bezpečnost a zálohy je využívána obdoba tzv. RAID 6, kdy samo obnovovací kód je ukládán na dva disky a data se ukládají střídavě na další dva disky. K zapotřebí je tak min. 4 disků, často se ovšem užívá pěti a více.

3.4.2 Připojení úložiště

Direct Attached Storage – DAS

Jedná se o nejčastěji používané připojení, kdy jsou disky pro ukládání připojené přímo v serveru či vedle v diskovém poli. I když se jedná o nejjednodušší a také nejlevnější řešení, skrývá řadu nevýhod. Především může dojít k přehlcení serveru při hromadném ukládání z více zařízení najednou. Při poruše jsou data nedostupná a dalším omezením může být také kabeláž.

Network Attached Storage - NAS

Je tvořen jedním zařízením připojeným přímo k síti a sloužící k ukládání či zálohování dat. Toto řešení je sice levné, lze připojit zařízení s různým operačním systémem, ale s množstvím připojených zařízení může být problém s propustností a některé požadavky tak mohou být odmítnuty.

Storage Area Network – SAN

Tato síť je jistě nejlepší pro bezpečné zálohování. Je oddělená síť pro zálohování a síť pro servery. Sítě jsou propojeny optickými kabely, což umožňuje spojení i na velké vzdálenosti. Výhodou je stabilita systému, nezávislá činnost zálohovací a serverové sítě, a také možnost rychlého rozšíření záložního prostoru. Nedochází také k zahlcení daty, protože každý sever připojený k úložišti má přidělený určitý prostor.

3.5 Zálohovací software

Se zálohováním a archivováním dat nám může pomoci speciální software, který vše automaticky zajistí za nás. Pro zálohování je na trhu řada programů, jenž jsou nabízeny zdarma či za poplatek a umožňují nám tak zautomatizovat tuto činnost. Po instalaci nás program vyzve k zadání úložiště, nastavení frekvence záloh a výběr složek, které se mají zálohovat.

Mezi nejrozšířenější software patří Cobain Backup. Program je bezplatný a podporuje i češtinu. Umožňuje nám automatické zálohování složek a souborů na pevný disk, síťové

úložiště nebo FTP server. Dále nám umožňují nastavit kompresi do formátu .zip nebo 7.z a vše chránit heslem.

Z placených programů je často doporučovaný program Acronis True Image. Kromě všech běžných funkcí pro zálohy program také umožňuje automatickou obnovu počítače, vytváření kompletních obrazů disků a on-line úložiště s kapacitou 5 GB.

Pracovní list – Zálohování a archivace dat

Jméno a příjmení: **Třída:**

Škola:

1) **Zálohování dat slouží k:**
   a) Vytváření kopií dat, které současně používáme
   b) Uložení nepotřebných dat, které mohou být v budoucnu využitelná
   c) Skrytí soukromých či osobních dokumentů
   d) Vyčištění prostoru na pevném disku
2) **Archivace dat slouží k:**
   a) Vytváření kopií dat, které současně používáme
   b) Uložení nepotřebných dat, které mohou být v budoucnu využitelná
   c) Skrytí soukromých či osobních dokumentů
   d) Vyčištění prostoru na pevném disku
3) **Seřaďte následující média podle kapacity**
   … CD
   … Blu-ray
   … HDD
   … DVD
4) **Základní kapacita DVD je:**
   a) 700 MB
   b) 4,7 GB
   c) 25 GB
   d) 1 TB
5) **Pro průběžné zálohování je nejvhodnější:**
   a) Optický disk
   b) Pevný disk
   c) Flash disk
   d) Disketa
6) **On-line datová úložiště slouží k:**
   a) Poskytování dat třetím osobám
   b) Správě a údržbě dat přes internetové rozhraní
   c) Archivování souborů a firemním serveru
   d) Vytvoření virtuálního disku v počítači

Řešení k pracovnímu listu - Zálohování a archivace dat

Otázka č. 1

Vytváření kopií dat, které současně používáme. Záloha by měla být rychle obnovitelná a zálohujeme soubory, které průběžně používáme.

Otázka č. 2

Uložení nepotřebných dat, které mohou být v budoucnu využitelná. Archivace neklade nároky na rychlé obnovení dat a je důležité ji uchovávat tak, aby nebyla poškozena vlivem vnějších činitelů.

Otázka č. 3

Nejvyšších kapacit dosahují pevné disky HDD, u kterých lze dosáhnout až několika terabajtů. Na druhém místě jsou Blu-ray disky se základní kapacitou 25 GB, následují DVD disky o 4,7 GB místa a nakonec 700 MB dosahují CD disky.

Otázka č. 4

DVD má základní kapacitu 4,7 GB.

Otázka č. 5

Nejvhodnější je pevný disk umožňující průběžný přepis dat, nahrávání a obnovení dat a jejich rychlé načtení a aktualizace.

Otázka č. 6

On-line datová úložiště slouží ke správě a údržbě dat přes virtuální prostředí pomocí internetového prohlížeče.

4 Online nebezpečí

Facebook, Twiter, MySpace, Lide.cz a další sociální sítě spojují v současnosti různé skupiny lidí. Sociální sítě v současnosti nahradily „sezení na lavičce a povídání si“. Žáci celé odpoledne sedí u svých počítačů, mobilů a tabletů, jen aby byli on-line a mohli „lajkovat“ svoje statuty a komunikovat s kamarády. Ve virtuální komunikaci chybí ovšem jeden základní prvek a to je řeč těla. Nevidíme toho kdo si s námi píše, nedokážeme svoje věty podložit správným výrazem ve tváři a tak dát najevo, že to co říkáme, myslíme opravdu vážně. Nové technologie nám umožňují sice spojení na tisíce kilometrů a komunikovat se svými známými i v zámoří, ovšem hrozí i řada rizik, kdy si můžeme psát se zcela cizí osobou, o které si myslíme, že je ten pravý (á), ale ve skutečnosti se jedná pouze o falešný profil a za ním stojí násilník. Existuje celá řada nebezpečí, která nám na internetu hrozí.

4.1 Kyberšikana

4.1.1 Šikana vs. kyberšikana

Šikana obecně nastává, když: *„Jeden nebo více žáků úmyslně, většinou opakovaně, týrá a zotročuje spolužáka či spolužáky a používá k tomu agresi.“* (Kolář, 2001) Šikana ovšem nemusí probíhat pouze ve školním prostředí, jsou známé i případy z pracoviště, armády a řady dalších, různých větších kolektivů.

Šikana je jakékoliv fyzické i psychické týrání, vydírání, či jiné omezování šikanované osoby šikanujícím. Strůjce útoků je poté označován jako agresor a ten, proti komu jsou útoky vedeny, se označuje jako oběť. Agresor ani oběť nemusí být pouze jedna osoba, může se jednat také o skupiny či skupinu, která šikanuje jedince. Agresoři bývají silnější, starší a často se s nějakou formou šikany osobně setkali, ať již doma nebo ve školním prostředí, když byli mladší. Obětí se nejčastěji stávají osoby nějak odlišné od ostatních. Sociálně slabší, zdravotně postižení, či lidé jiného náboženského vyznání či rasového původu. Pokud si agresor vybere svoji oběť, vždy si najde také důvod jí napadnout.

V praxi rozlišujeme dva druhy šikany. Při fyzické šikaně dochází k útokům, napadání a přímým fyzickým útokům. Oproti tomu při psychické šikaně se jedná především o ponižování, vydírání, posměch a podobně. Psychická šikana mívá často tragičtější konce,

v podobě sebevražd obětí, protože oproti fyzické není tolik vidět a oběť často tají. Že jí je ubližováno.

„Průběh šikany má několik fází:

- *První stupeň (zrod ostrakismu)*
  - *Šikana se může objevit kdekoliv, podmínky jejího vzniku nejsou totiž nijak neobvyklé. V každé skupině se najdou jedinci, kteří jsou méně oblíbení a vlivní.*
  - *Jde o mírné, převážně psychické formy násilí, kdy se okrajový člen necítí dobře. Ostatní ho více či méně odmítají, nebaví se s ním, pomlouvají ho, spřádají proti němu intriky a dělají na jeho účet drobné legrácky.*
- *Druhý stupeň (fyzická agrese a přitvrzování manipulace)*
  - *Existuje více důvodů pro postoupení do druhého stádia. Jedna z možností je odreagování žáků prostřednictvím nejslabšího jedince, který funguje jako ventil. Druhá možnost může nastat na školních zájezdech, kdy nejslabší slouží jako oživení programu. Třetí možnost nastane, když se ve třídě sejde více agresivních jedinců, kteří prostřednictvím násilí uspokojují své potřeby. Při bití a týrání zažívají jedinci pocit moci, který prolomí poslední zábrany.*
  - *Ovšem ani v tomto stupni nemusí šikana vypuknout. V případě, že ve třídě existuje soudržnost, kamarádské vztahy a převažují pozitivní mravní hodnoty, kdy žáci mají zásadně negativní postoje k násilí a ubližování slabším, pokusy o šikanování neuspějí.*
- *Třetí stupeň (klíčový moment – vytvoření jádra)*
  - *V tomto stupni se vytvoří skupinka agresorů, tzv. úderné jádro, které nyní již spolupracuje systematicky. Skupina je nyní rozdělena na řadu podskupin bojujících o vliv. Jestliže se do této doby nezformuje silná pozitivní podskupina, která bude alespoň rovnocenným partnerem podskupině tyranů, tažení tyranů za mocí může nerušeně pokračovat.*
- *Čtvrtý stupeň (většina přijímá normy agresorů)*
  - *Nyní jsou normy agresorů přijaty, většina je považuje za nepsané zákony. Kolář (1997) varuje, že v této fázi se i mírní a ukáznění žáci začnou chovat krutě, týrat spolužáka a dokonce u toho pociťovat uspokojení.*

- *Pátý stupeň (totalita neboli dokonalá šikana)*
    - *V poslední fázi dochází nastolení totalitní ideologie šikanování. Žáci jsou rozděleni na dvě skupiny lidí – na agresory a na oběti. Agresoři využívají vše, co lze zužitkovat, od materiálních věcí až po školní znalosti. Agresoři ztrácí veškeré zábrany, chtějí pouze provádět násilí, které považují za normální, dokonce za legraci. Tento nejvyšší stupeň je příznačný spíše pro šikany ve věznicích, vojenském prostředí a výchovných ústavech pro mládež. V mírnější podobě se však někdy vyskytuje i na školách."* (Kolář, 1997)

S fenoménem internetu přicházejí také nové formy šikany. Kyberšikana (cyberbullying) využívá kromě běžných prostředků přímého napadání, především nové technologie jako jsou chytré telefony, tablety a internet. Oběť je nejčastěji natočena či vyfocena v trapné či jinak nevhodné situaci a toto médium je poté umístěno na internet. Hlavní nebezpečí kyberšikany je v tom, že v několika okamžicích vidí fotografii či video ohromné množství lidí. Sdílením a přeposíláním zpráv a vzkazů se materiály rozšíří mezi spoustu uživatelů a agresor má tak vetší publikum, což jej často těší. Agresorovi tak on-line útoky nabízejí celou řadu nových možností. Především již nemusí být fyzicky zdatnější, stačí intelektuálně. Má možnost vystupovat v anonymitě a takoví pachatelé jsou i těžko dohledatelní. Na oběť může utočit 24 hodin denně, protože v případě klasické šikany, je zapotřebí, aby se oběť i agresor setkali ve stejný čas na jednom místě. Oběť tak před kyberšikanou nemá kam utéct.

Možností anonymního šikanování na internetu je celá řada. Tou nejjednodušší je rozesílání různých zpráv, které nějak pomlouvají či poškozují oběť. Dále se často jedná o fotografie, videonahrávky či fotomontáže. Při cílenější a promyšlenější šikaně jsou již vytvářeny často falešné internetové stránky, poškozující dotyčného, je zneužíván jeho účet apod. V každém případě je vypátrání agresora vždy složité. Pokud se to již podaří, může být zablokován a či v případě závažnější formy šikany i trestně stíhán.

4.1.2 Sociální sítě

Sociální sítě v současnosti velice nahrávají různým internetovým útokům. Je velice snadné přidat si do svého účtu nové přátele a zpočátku si s nimi dopisovat, ovšem často se může stát, že napíšeme něco, co bychom ve skutečném rozhovoru nikdy neřekli, pošleme intimní

fotografii nebo se ukážeme na webové kameře. Velice jednoduše může osoba na druhé straně materiály uchovat a použít je proti nám.

Ukázkou tohoto fenoménu byl nedávny projekt s Benem Cristovao, který se měl svléknout před webkamerou při chatu s neznámou slečnou. Ta vše zaznamenala a video umístila na internet. Velice rychle se „lajkováním“ rozšířilo mezi uživateli a dokonce jej převzali i bulvární časopisy. Aniž by si někdo ověřil jeho pravost či okolnosti vzniku, uveřejňoval ho. Zanedlouho poté vyšla zpráva projektu Seznam se bezpečně!, kde se ukázalo, že video vzniklo cíleně a mělo demonstrovat sílu internetových medií a rychlost šíření takovýchto zpráv.

Mezi největší sociální síť v současnosti patří zajisté Facebook. Vznikl v roce 2004 v Cambridge. Mark Zuckerberg vytvořil původně síť pouze pro uživatele univerzity Harward, ovšem velmi rychle si jej oblíbili i studenti jiných univerzit. V Česku se jako první připojila Masarykova univerzita. Od roku 2006 se již může zaregistrovat kdokoliv. I když podle pravidel se může registrovat pouze osoba starší 13 let, realita je někde jinde, asi podobně jako u pornografických stránek souhlasíte s tím, že vám bylo 18. Síť umožňuje sdílet prakticky cokoliv a s kýmkoliv. Je možné na virtuální zeď vystavit fotografie, videa, myšlenky a umožnit k nim přístup každému, kdo je v seznamu přátel.

Ask.fm je aplikace, kde uživatelé mohou posílat anonymně své dotazy konkrétní osobně. Právě anonymita je tu velmi nebezpečná a na profilech se pak často objevují narážky, posměchy a podobné zprávy.

Mezi další sociální sítě patří například Twiter Inc., sloužící především jako mikroblog a rozšířený v USA. Typicky českou sítí jsou Lidé.cz, které provozuje společnost Seznam.cz.

4.2 Prevence a řešení kyberšikany

S prevencí kyberšikany je třeba začít již na prvním stupni základní školy, kdy se děti poprvé většinou dostávají do kontaktu se sociálními sítěmi, chytrými telefony a on-line hrami. Základním prvkem ochrany je prevence a kontrola. Rodiče by neměli nechat své děti volně brouzdat po internetu a občas se podívat, co dělají, s kým si píšou a hlavně si všímat změn v chování. Ve škole je potřeba osvěta v oblasti kyberšikany, především učitelé informatiky

musí dbát na informování žáků a nebezpečí a reagovat včas na případné náznaky, že je někomu ubližováno. Žáci by měli vědět, že mají za kým přijít a komu se svěřit se svým problémem a v případě útoku přes digitální technologie je třeba spolupráce školního psychologa či výchovného poradce a kvalifikovaného učitele výpočetní techniky. Ten má větší přehled o možnostech blokování či odhalení útočníka. V závažných případech je nutné již spolupráce s policií.

4.2.1 Národní centrum bezpečnějšího internetu

Hlavní organizací zabývající se problémem kyberšikany u nás je Národní centrum bezpečnějšího internetu. Na stránkách saferinternet.cz řadů článků s aktuálními informacemi, týkajících se hrozeb. Každoročně v únoru pořádá SAFER INTERNET DAY (Den bezpečnějšího internetu) při jehož příležitosti vyhlašuje řadu soutěží pro žáky škol. Pro žáky také realizují přednášky a semináře.

4.2.2 Bezpečně online

Bezpečně online je dalším velkým a hlavně rozsáhlým projektem Národního centra bezpečnějšího internetu. Je zaměřen na rodiče, učitele a mládež, přičemž každá skupina má vlastní kategorii. Pro školy nabízí zdarma řadu výukových materiálů, jako jsou pracovní listy, brožury, ale třeba i videa s řadou témat kyberšikany.

4.2.3 Seznam se bezpečně

Společnost Seznam.cz provozuje portál www.seznamsebezpecne.cz, který se zaměřuje především na zneužívání identity, nástrahy internetové komunikace apod. Pro žáky nabízí řadu zajímavě natočených klipů o nástrahách rande na slepo, komunikace před webkamery a řadu dalších, kde jsou hlavními aktéry křečci. Humorně natočené scénky nenásilně ukazují žákům, co jim hrozí. Projekt seznamsebezpecne.cz také stojí za vznikem divadelní hry #jsi_user. Ta je tvořena autentickými zprávami a hláškami z blogů a chatů, navíc pro školy jsou představení zdarma. V neposlední řadě stojí projekt Nahá celebrita s Benem Cristovao, který je zmíněn výše.

4.2.4 E-bezpečí.cz

Projektů zaměřujících se na internetovou bezpečnost je celá řada. Neposledním v řadě, ale jistě velmi zajímavým, je E-bezpečí.cz. Tento projekt provozuje Centrum prevence rizikové virtuální komunikace Pedagogické fakulty Univerzity Palackého a zaměřuje se na všechny oblasti interneté komunikace, sextingu, kybergromingu, komunikace na sociálních sítí, … Kromě osvěty a poskytování poradenství se ale také věnuje výzkumu.

4.3 Kybergrooming

Termín kybergrooming (child grooming, cyber grooming) je druhem psychické manipulace realizované prostřednictvím internetu, mobilních telefonů a dalších souvisejících technologií (Kopecký, Krejčí 2010, Berson).

Kybergrooming je velice rozšířenou hrozbou internetové komunikace. Všude tam, kde lze vytvořit falešnou identitu (facebook.cz, ask.me, chatovací místnosti, …), dochází ve většině případů k tomu, že se uživatel vydává za někoho jiného. Nejčastější případy jsou starší muži, vydávající se mladší, za účelem vylákání dívek na schůzku. Tzv. groomer je často velice trpělivý a snaží se získat co největší důvěru své oběti. Dochází také k nákupu různých dárků, například kreditu do mobilu, do počítačové hry apod. I když je každý případ individuální, průběh postupuje nejčastěji podle následujícího schématu:

- Vzbuzení důvěry a izolace od okolí
- Budování přátelství, resp. „kupování si“ oběti různými dárky, kredity
- Získání osobních a důvěrných materiálů či informací, využitelných k vydírání
- Vytvoření závislosti na kontaktu s útočníkem
- Vyžádání osobní schůzky, v případě odmítnutí – využití důvěrných informací k nucené schůzce
- Napadení, zneužití či jiný způsob ublížení

Při komunikaci s neznámým uživatelem bychom nikdy v žádném případě neměli poskytovat své osobní informace. Pokud již chceme poznat druhou osobu důvěrněji, je třeba znát nejprve její identitu. Fotografie či live přenos přes videochat lze falšovat, je proto dobré požádat o fotografii s výtiskem určitých novin, či jinak specifikovanou. V případě osobní schůzky je

nutné někoho informovat, nejlépe dospělou osobu, která by mohla jít případně na setkání s námi. Jestliže se nám zdá chování osoby podezřelé, nechce se ukázat a podobně, je dobré komunikaci ihned ukončit. V případě že již požaduje erotické fotografie či důvěrné informace, měli bychom tuto skutečnost nahlásit policii či dospělé osobě.

4.4 Sexting

Z výzkumu Univerzity Palackého v Olomouci, provedeného v roce 2012, se setkalo 8% z 21.000 dotázaných žáků základních a středních škol se sextingem. Většinou sami poslali nebo přijali erotickou fotografii.

Sexting zahrnuje jakékoliv psaní zpráv, rozesílání fotek či videí se sexuální tématikou. Z pohledu odesílatele tak dochází k obtěžování druhé osoby, případně vydírání, které se může obrátit také proti osobě, která erotický materiál zaslala. Kromě osobních problémů je toto jednání také protizákonné u osob do 18ti let a nezáleží přitom na tom, zdali s focením souhlasili či jej sami vyžadovali. Jedná se poté o porušení zákona o mravní výchově mladistvých, především paragrafů:

§ 192 Výroba a jiné nakládání s dětskou pornografií

(1) Přechovávání (odnětí svobody až na 2 roky)

(2) Výroba, dovoz, vývoz, nabídka, zpřístupňování (odnětí svobody až na 3 roky)

Pokud toto spáchá jako člen organizované skupiny, dále rozšiřuje dětskou pornografii obzvláště účinným způsobem (film, rozhlas, televize, internet), či s cílem získat značný finanční prospěch, může být potrestán odnětím svobody až na 6 let, v případě mezinárodní organizované skupiny až na 8 let.

§ 193 Zneužití dítěte k výrobě pornografie

(1) Kdo přiměje, zjedná, najme, zláká, svede nebo zneužije dítě k výrobě pornografického díla nebo kořistí z účasti dítěte na takovém pornografickém díle, bude potrestán odnětím svobody na jeden rok až 5 let.

Organizovaně či s cílem získat značný finanční prospěch, může být potrestán odnětím svobody až na 6 let, v případě mezinárodní organizované skupiny až na 8 let.

4.5 Phishing

Podvodná metoda někdy též překládána jako rybaření. Jedná se o získávání osobních údajů uživatele pomocí falešných e-mailů či podvodných zpráv instant messengeru. Uživateli přijde zpráva, která se tváří důvěryhodně, protože odesílatel se vydává za manažera firmy, obchodního zástupce banky či administrátora stránek a po uživateli požaduje soukromé údaje jako například heslo, číslo karty či ověření PIN kódů kreditní karty. Ke zprávě je často také připojena příloha s „oficiálním“ dopisem, nebo adresa stránek, kde je třeba požadované údaje vyplnit. Autor tohoto sdělení poté získá prostředky k přístupu do uživatelského účtu či internetového bankovnictví. Jedním z posledních útoků byla zpráva od „České spořitelny“ s výzvou k zadání údajů k platební kartě (viz obrázek).


ČESKÁ SPOŘITELNA

Vážený kliente / klientko

při využívání služeb u naší banky Česká spořitelna a.s. / osobní účet
jsme zaevidovali na Vašem účtu podezřelé platební transakce.
Žádáme Vás tedy o aktualizaci dat na Vaší platební kartě.
V opačném případě bude Váš účet zablokován!
Věříme, že je i ve Vašem zájmu chránit bezpečnost Vašeho účtu.

Prosíme o vyplnění následujících údajů pro ověření disponibilního práva.

Zde prosím vyplňte:

Jméno a Příjmení: _____
Rodné číslo: _____
Místo bydliště: _____
Telefonní číslo: _____
Číslo platební karty: _____
Platnost karty: _____
CVC kód (poslední 3 čísla na zadní straně platební karty) _____

Bezpečnost při platebním styku s Vaší kartou VISA/MASTER CARD/MAESTRO
Kontrola klienta a jeho platebních karet Česká spořitelna a.s.

OBR. 10: FALEŠNÝ DOPIS OD BANKY

Základní zásadou proto je, pamatovat si, že žádná organizace nevyžaduje zasílání osobních údajů, hesel, čísel účtů apod. přes email. Pokud již otevřeme internetové stránky, které vyžadují jistý stupeň zabezpečení, v řádku s adresou musí být na začátku https://adresa.pripona, u podvodných stránek bývá často pouze http://něco.cz

4.6 Pharming

Pharming je obdobou phishingu, je ovšem více nebezpečný. Pomocí trojského koně či červa infikuje útočník počítač. Při zadání internetové adresy, například banky, dojde k útoku na DNS (Domain Name Systém). Protože každá internetová stránka je identifikovatelná podle IP

adresy (číslo složené ze 4 částí – např. 125.0.0.134) a pro jednoduchost a zapamatování je této IP adrese přiřazeno DNS – tedy název stránky. Při napadení DNS je přepsána IP adresa přiřazené stránky a uživatel je pak přesměrován na podvodné stránky, které jsou k nerozeznání od skutečných. Při přihlášení jsou poté například chybovou hláškou: „*Chyba při ověřování, zadejte PIN Vaší karty pro ověření pravosti Vašeho účtu,*“ získány osobní údaje klienta. V aktualizovaných internetových prohlížečích je již ochrana proti pharmingu zabudována, ovšem platí stejný problém jako u nákazy jiným malware. Nelze vytvořit dostatečnou ochranu proti něčemu, co ještě není. Proto se neustále někdo snaží tato zabezpečení obejít a osobní údaje získat.

4.7 Internetová závislost (netolismus)

Internetová závislost (netolismus, netholoismus) je závislost stejně jako třeba kouření, braní drog a podobně. Jedná se především o závislost psychickou. Závislý jedinec ztrácí přehled o okolí, zanedbává rodinu, přátelé, školu či práci. Dlouhodobé sezení u počítače má vliv na jeho zdraví. Neplnění běžných povinností poté vede k celkovému úpadku osobnosti a podobně jako například u výherních automatů, i do řady on-line her je možné dokupovat schopnosti, případně zakoupit postup do vyššího kola. Závislý člověk se tak může dostat až do konfliktu se zákonem, v případě že se mu finance nedostávají.

U žáků se závislost projevuje nervozitou v případě, že jsou odtrženy od internetu či jakéhokoliv zařízení, pomocí kterého by se mohli připojit. Kvůli neustálému sledování zpráv, hry a podobně dochází k omezení pití či příjmu potravy. Přichází nedostatek spánku. Postupně se vytrácejí jakékoliv jiné koníčky, volnočasové aktivity i styk s kamarády.

Při předejití těmto potížím je důležitý především včasný zásah rodičů či partnera, protože tato závislost není pouze doménou teenagerů. V případě, že se počítač a internet stává prioritou v životě jedince, je potřeba ihned stanovit jasná pravidla používání internetu. U žáků doma tuto skutečnost musejí zajistit rodiče. Nejlépe vyhranit čas hraní her a učení a striktně tato pravidla dodržovat. Dbát na rozvoj dítěte po všech stránkách a kontrolovat jeho aktivity na internetu. Pokud již dojde k tomu, že hraní on-line či jiných počítačových her, chatování, komunikace na sociálních sítích nebo jiná činnost s počítačem zabírá několik hodin denně, je třeba začít hledat řešení, v některých případech i odbornou pomoc. Především je nutné nalézt

jinou aktivitu, které se bude závislá osoba věnovat, což bývá obtížné, jelikož tyto aktivity se vytratily během závislosti. U žáků je poté třeba dohled rodičů, omezení času tráveného s počítačem či mobilem s připojením na internet.

Pracovní list – Internetové nebezpečí

Jméno a příjmení: **Třída:**

Škola:

1) **Hlavním nástrojem kyberšikany jsou:**
   a) Dopisy
   b) Fyzické útoky
   c) Virtuální komunikační prostředky
   d) Masmédia
2) **Sociální sítí není:**
   a) Facebook
   b) Seznam
   c) Lidé.cz
   d) Twiter
3) **Vytvořte dvojice**

a) Sexting	Fotografie, či zprávy se sexuální tématikou
b) Phishing	Kontakt pomocí falešné identity
c) Netolismus	Internetová závislost
d) Kybergrooming	Získávání osobních údajů pomocí emailu

4) **Jaký je rozdíl mezi šikanou a kyberšikanou?**

5) **Vyhledej internetové projekty věnované prevenci kyberšikany.**

6) **Která adresa je „tou pravou“ při vstupu do zabezpečeného internetového bankovnictví?**

   a) http://www.airbank.cz
   b) airbank.cz/secret
   c) www.airbank.cz/cs
   d) https://www.airbank.cz

Řešení k pracovnímu listu - Internetové nebezpečí

Otázka č. 1

Kyberšikana je prováděna nejčastěji prostřednictvím virtuálních komunikačních prostředků jako jsou mobily, sociální sítě, emaily apod.

Otázka č. 2

Seznam.cz, jedná se o vyhledávač

Otázka č. 3

Sexting = Fotografie, či zprávy se sexuální tématikou

Phishing = Získávání osobních údajů pomocí emailu

Netolismus = Internetová závislost

Kybergrooming = Kontakt pomocí falešné identiy

Otázka č. 4

Šikana je závislá především na osobním kontaktu a pachatel zná útočníka. Kyberšikana je často anonymní, zahrne mnohem více lidí a není třeba přímý fyzický kontakt.

Otázka č. 5

„Seznam se bezpečně!“ (www.seznamsebezpecne.cz)
„Bezpečně on-line.cz“ (www.bezpecneon-line.cz)
„Bezpečný internet.cz“ (www.bezpecnyinternet.cz)
„Protišikaně.cz“ (proti-sikane.saferinternet.cz)

Otázka č. 6

Správně je D, protože zabezpečený server má na začátku adresy HTTPS.

5 Dotazníkové šetření

Cílem šetření bylo zmapovat práci s počítačem u žáků základní školy a gymnázia. Především jak se chovají u počítače, co využívají na ochranu svých dat, informací a osobních údajů.

Celkem se zapojilo 75 žáků z toho 42 dívek. 28 žáků ze Základní školy Komenského ve Skutči a 47 žáků z vyššího stupně Gymnázia K. V. Raise v Hlinsku. Průměrný věk respondentů byl 15 let. Sběr proběhl přes internetový dotazník vytvoření v aplikaci Google disc, který výsledky ukládá do tabulky.

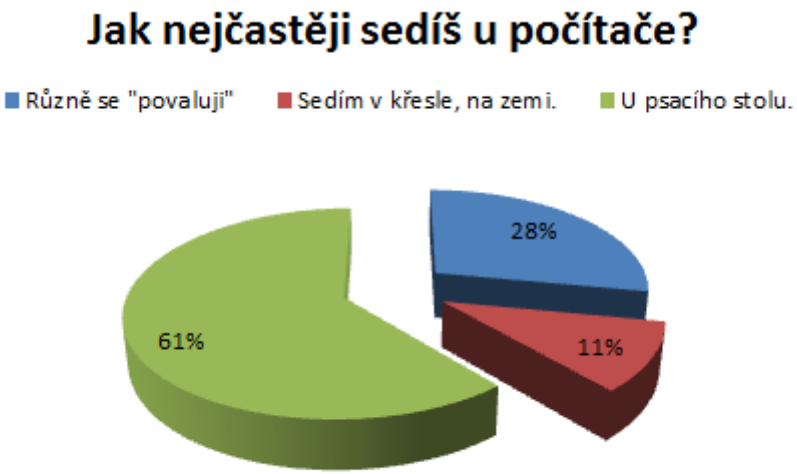
Na Základní škole Komenského Skuteč probíhá výuka informatiky v pátém, šestém, sedmém a devátém ročníku vždy po jedné vyučovací hodině týdně. V devátém ročníku poté jako dvouhodinovka jednou za čtrnáct dní. Jedná se o menší základní školu po jedné třídě v každém ročníku s průměrným počtem osmnácti dětí ve třídě. Přístup k internetu mají ve škole všichni žáci pomocí zabezpečené sítě wifi. Skuteč je město s přibližně 5 000 obyvateli

Na Gymnáziu K. V. Raise v Hlinsku byli dotazováni žáci na vyšším stupni v prvním a druhém ročníku. Informatika je vyučována v každém ročníku, po dvou hodinách týdně v prvním a druhém a po jedné hodině ve třetím a čtvrtém. Na vyšším stupni gymnázia jsou paralelní třídy průměrně po 25 žácích. Hlinsko má přibližně 10 000 obyvatel.

5.1 Výsledky šetření

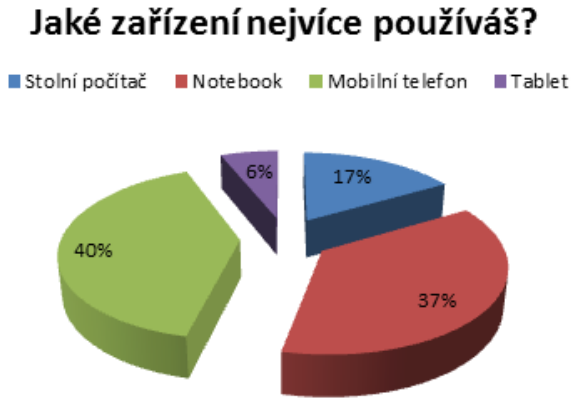
Otázka č. 1: Jak nejčastěji sedíš u počítače?

Nejvíce žáků odpovědělo, že sedí u psacího stolu (celkem 46), ale velká část se také jen různě „povaluje“, či sedí v křesle. Žáci si zatím neuvědomují následky špatného sezení u počítače a nedodržují základní pravidla.



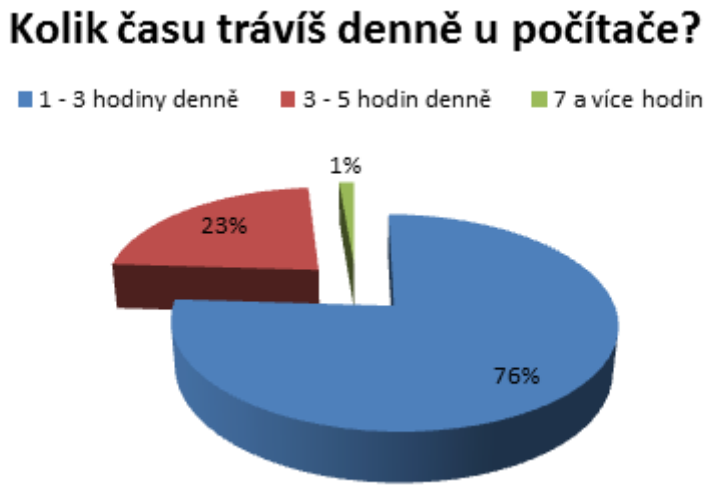
Otázka č. 2: Jaké zařízení nejvíce používáš?

Více než polovina žáků používá nejčastěji mobilní telefon a stejně tak i notebook. Již méně rozšířené jsou mezi žáky stolní počítače. Oproti očekávání, že v současné době, kdy tablety zažívají svůj boom, jejich užívání uvedlo pouze 7 žáků.



Otázka č. 3: Kolik času trávíš denně u počítače (notebooku, tabletu apod.)?

57 žáků uvedlo, že u počítače tráví maximálně 3 hodiny denně. Pouze jeden žák tráví převážnou většinu dne u počítače a odpověděl, že přes sedm hodin.

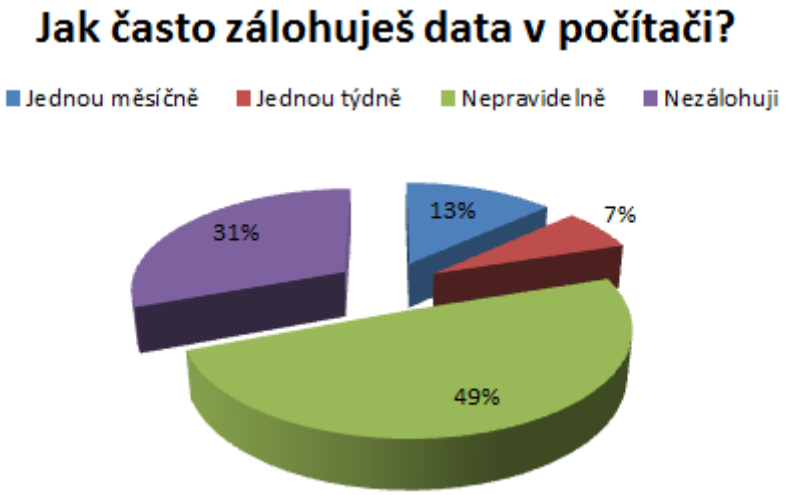


Otázka č. 4: Která z následujících aktivit je pro tebe nejdůležitější?

Oproti všeobecnému názoru, jak žáci tráví většinu času u počítače, odpovědělo 47 dotazovaných, že je pro ně důležité posezení s přáteli a 35 z nich také preferuje sport. Jen 15 žáků zaškrtlo možnost, že je pro ně důležitá komunikace na internetu. Žáci mohli zaškrtnout více možností.

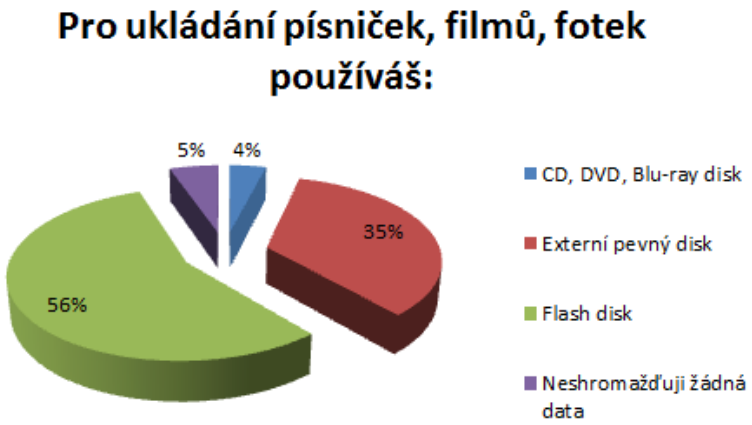
Otázka č. 5: Jak často zálohuješ data v počítači?

Obecně žáci zálohám nepřikládají velkou důležitost, což může být také tím, že data, která mají v počítači, nejsou tak důležitá, převážně hudba, filmy a nějaké ty úkoly do školy. Vůbec nezálohuje 23 dotazovaných a nepravidelně provádí zálohy polovina. Pravidelné týdenní či měsíční zálohy dohromady provádí pouze 15 respondentů.



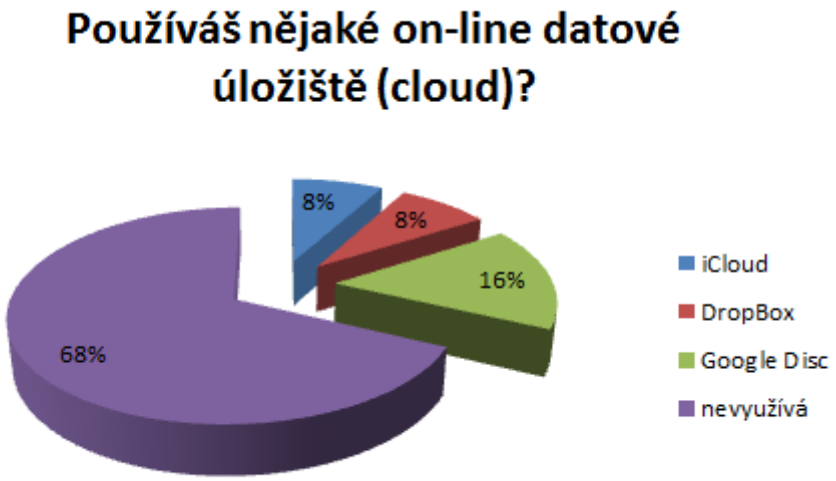
Otázka č. 6: Pro ukládání písniček, filmů, fotek používáš

Mezi žáky je nejrozšířenější ukládání na externí pevné disky případně flash disky. Pouze 3 žáci odpověděli, že používají nějaký druh optických medií a 4, že žádná data neshromažďují.



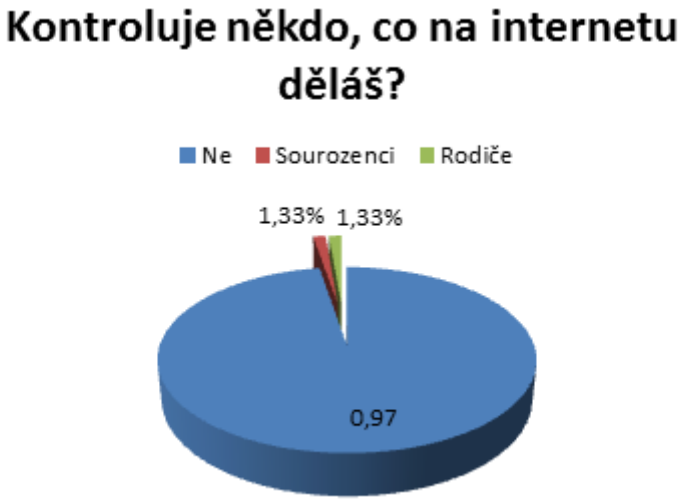
Otázka č. 7: Používáš nějaké on-line datové úložiště (cloud)?

I přes výhody on-line datový úložišť, které nabízejí dostupnost odkudkoliv bez ohledu na připojené zařízení, 51 dotazovaných tyto služby nevyužívá, ostatní využívají nejčastěji Google Disky, One Drive od Microsoftu a 6 žáků používá iCloud společnosti Apple.



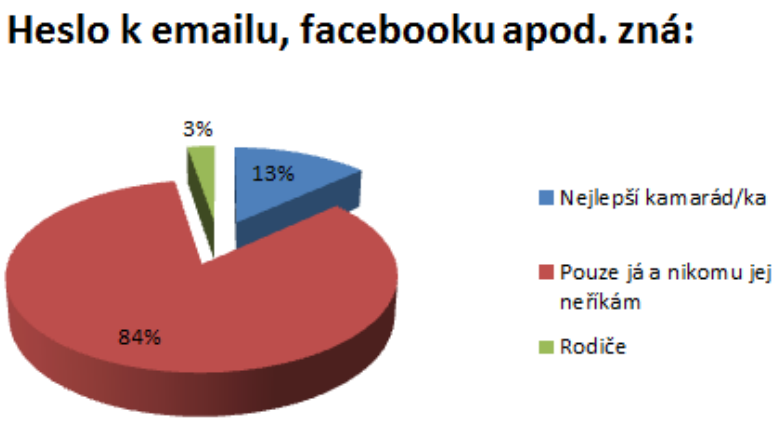
Otázka č. 8: Kontroluje někdo, co děláš na internetu?

Téměř všichni z dotazovaných mají při činnosti s počítačem absolutní svobodu a nikdo je nekontroluje. Pouze dva žáci uvedli, že je kontrolují rodiče či starší sourozenec.



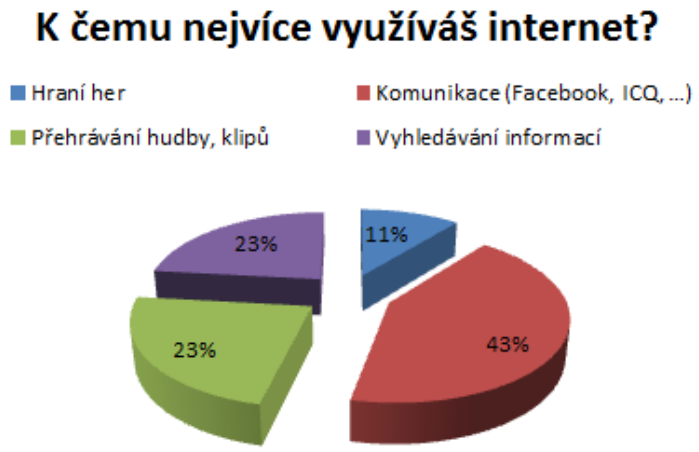
Otázka č. 9: Heslo k emailu, facebooku apod. zná:

Žáci vědí, že heslo je velmi důležité a znají i zásady pro jeho užívání a vytváření. Většinou jej i chrání a nikomu nesdělují. Pouze 10 z dotázaných odpovědělo, že heslo ví jeho nejlepší kamarád(ka) a dva své heslo sdělili rodičům.



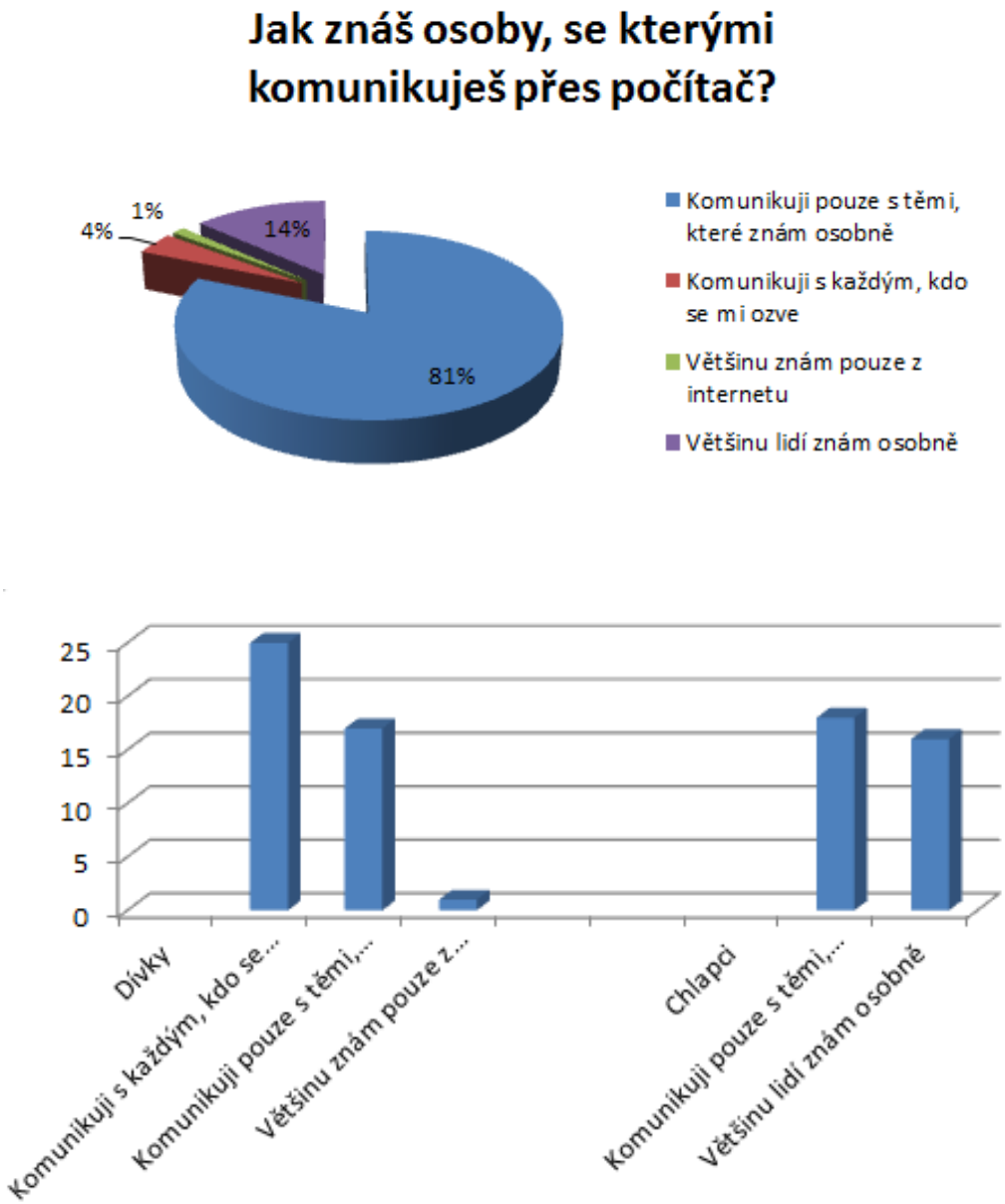
Otázka č. 10: K čemu nejvíce využíváš internet?

Zde mohli žáci vybrat z několika možností, nejčastěji internet užívají ke komunikaci s přáteli, tato možnost se objevila celkem 55krát, shodně po třiceti výběrech obdrželo přehrávání hudby a médií a také vyhledávání informací. Pouze čtrnáctkrát se objevilo hraní her. Výsledky nijak nepřekvapily, komunikace na internetu převládá všeobecně nad ostatními aktivitami.



Otázka č. 11: Jak znáš osoby, se kterými komunikuješ přes počítač?

Výsledky této otázky byly překvapující, protože většina žáků si píše pouze s těmi, které znají osobně, celkem tuto možnost vybralo 61 žáků. Respondenti, kteří komunikují s cizími lidmi, jenž se jim ozvali, a neznají je, byli pouze čtyři.



Otázka č. 12: Osobě, kterou neznáš, ale již dlouho se spolu bavíte, bys sdělil(a).

Žáci by neznámé osobě sdělili ve 48 případech informace o škole, kterou navštěvují. Ovšem patrně si neuvědomují, že pokud neznámá osoba ví, jak vypadají, a sdělí ji, kam chodí do školy, může je kontaktovat při příchodu (odchodu) ze školy. Hned na druhém místě je číslo mobilního telefonu. Možnost, že nesdělí žádné údaje, nebyla v dotazníku uvedena záměrně, abych zjistil, co jsou ochotni na sebe prozradit.

Otázka č. 13: Znáš některé z těchto projektů týkajících se bezpečnosti na internetu?

Velká část žáků nevěnuje pozornost stránkám, zabývajících se bezpečnosti a prevencí kyberšikany na internetu. 62 žáků odpovědělo, že žádné z uvedených stránek nezná.

5.2 Shrnutí dotazníkového šetření

Žáci obecně nevěnují pozornost bezpečnosti při práci s moderními technologiemi. Zálohují nepravidelně nebo vůbec, na počítači mají neomezený prostor pro komunikaci a nikdo nekontroluje jejich činnost. Z dotazníků vyplynulo, že by žáci poskytli osobní informaci neznámé osobě, nejčastěji údaje o škole nebo mobilní telefon.

I přesto, že probíhá výuka těchto pravidel a zásad, která ovlivňují zdraví, ochranu informací dat a soukromí, probíhá v dostatečném rozsahu jak na základní škole, tak na gymnáziu, žáci tyto hodiny berou patrně pouze jako „nutné zlo“. Riziko si uvědomí až tehdy, když nějaké problémy nastanou.

Závěr

Tato diplomová práce je zaměřena na základní rizika a hrozby, se kterými se může uživatel setkat při práci s počítačem. V každé kapitole je přehled možných nebezpečí, týkajících se dané oblasti, popsání jejich příčin a ochraně proti nim.

Nesprávné sezení u počítače, či ležení s notebookem apod., čím dál více ovlivňují zdravotní stav a fyzický vývoj našich žáků. Nedostatek pohybu a dlouhodobé namáhání určitých částí těla přispívá ke vzniku onemocnění zad, páteře, zánětu karpálního tunelu a mnoha dalším poškozením, který se dá předcházet vhodným cvičením, přestávkami a správným upravením pracovního prostředí.

Ze ztráty dat a s tím související třetí kapitola „Zálohování“ žáci nemají moc obavy a nesnaží se jim předcházet. Je to způsobeno především tím, že nevytvářejí zatím žádné důležité dokumenty a převážnou část jejich dat tvoří hudba a filmy. Otázkou zálohování se začnou tedy zabývat nejčastěji až v tom případě, že k jejich ztrátě dojde. Pro uchování a přenášení informací používají flash nebo externí disky.

O kyberšikaně a jejích různých formách slýcháme v současné době téměř denně. Podle výzkumu, který provedl server Seznam se bezpečně! a zúčastnilo se jej přes 21 tisíc dětí, se s nějakým projevem šikany setkala více jak polovina. Přesto o ní žáci mluvit nechtějí, do diskuzí se nezapojují a řada z nich „šikanuje“ na internetu své spolužáky či známé aniž by si to uvědomovali, berou to jako zábavu či legraci. Tímto tématem se zabývá v současnosti řada převážně neziskových organizací, ale i státní organizace a vláda vloni přijala řadu zákonů týkajících se kyberšikany.

Ke každému tématu je připojen pracovní list, který slouží k oživení hodiny a upevnění znalostí žáků o daném tématu. Může být také rozdán na úvod a následně diskuzí nad otázkami být problematika probrána. Ke každému listu je také řešení, u některých otázek doplněné o podrobnější informace.

Poslední částí diplomové práce jsou výsledky dotazníkového šetření, které se zaměřilo na chování žáků u počítače. Každá otázka je doplněna komentářem výsledku a grafem.

Cíle práce byly naplněny. Každá kapitola seznámí čtenáře s možnými riziky a nástrahami, které mohou uživatele potkat při užívání informačních a komunikačních technologií. Žáci byli průběžně během roku několikrát o těchto hrozbách informování nejen při výuce informatiky, ale i například během osvětových besed a vyplnili pracovní listy. Jak ovšem vyplývá z výsledků dotazníků a následné diskuze s žáky vyplývá, že si jednotlivé hrozby příliš neuvědomují a případné nebezpečí začnou řešit, až když k němu dojde. Například zálohování, nebo ochranu počítače antivirovými programy. Výuka bezpečnosti práce je často pro žáky „nutným zlem," a z hodin si nejvíce odnášejí vlastní poznatky, které někdo zažil, či vyzkoušel.

Zdroje

1. BERSON, I. H. *Grooming Cybervictims: The Psychosocial Effects of Online Exploitation for Youth*. University of South Florida. USA. On-line: http://www.cs.auckland.ac.nz/~john/N...e/I.Berson.pdf [cit. 2014-05-19].
2. BURSOVÁ, Marta. *Kompenzační cvičení: uvolňovací, protahovací, posilovací*. 1. vyd. Praha: Grada, 2005, 195 s. Fitness, síla, kondice. ISBN 80-247-0948-1. [cit. 2014-04-20].
3. DOSEDĚL, Tomáš. *Počítačová bezpečnost a ochrana dat*. Vyd. 1. Brno: Computer Press, 2004, 190 s. ISBN 80-251-0106-1 [cit. 2014-03-18].
4. HÁK, Igor a Josef ZELENKA. *Ochrana dat: škodlivý software*. Vyd. 1. Hradec Králové: Gaudeamus, 2005, 211 s. ISBN 80-704-1594-0. [cit. 2014-05-25]
5. KOPECKÝ, K., KREJČÍ, V. *Rizika internetové komunikace*. Olomouc: Net University, 2010 [cit. 2014-03-18].
6. KOLÁŘ, Michal. *Bolest šikanování*. Vyd. 1. Praha: Portál, 2001, 255 s. ISBN 80-717-8513-X. s. 27 [cit. 2014-03-18].
7. KOLÁŘ, Michal. *Skrytý svět šikanování ve školách: příčiny, diagnostika a praktická pomoc*. Vyd. 1. Praha: Portál, 1997, s. 127, ISBN 80-717-8123-1. [cit. 2014-03-18]
8. LAPÁČEK, Jiří. *Počítač v domácnosti: podrobný průvodce pro práci, zábavu i vzdělávání*. vyd. 1. Brno: Computer Press, 2006, 366 s. ISBN 80-251-1047-8 [cit. 2014-03-18].
9. MARTINKOVÁ, Jana a Josef ZELENKA. *Poškození pohybového aparátu při práci v kanceláři: škodlivý software*. 1. vyd. Praha: Mladá fronta, 2009, 31 s. ISBN 978-80-204-2050-3 [cit. 2014-06-12].
10. NEŠPOR, Karel a Josef ZELENKA. *Jak přežít počítač: škodlivý software*. Vyd. 1. Kralice na Hané: Computer Media, 2011, 128 s. ISBN 978-80-7402-069-8. [cit. 2014-04-14].
11. SEDLÁK, Jan. Kterak muž syndromem karpálního tunelu ochořel. In: *Živě.cz* [online]. Mladá fronta, 2009, 24. 7. 2009 [cit. 2014-03-18]. Dostupné z: http://www.zive.cz/clanky/kterak-muz-syndromem-karpalniho-tunelu-ochorel/sc-3-a-147997/default.aspx [cit. 2014-02-20].

12. ŠPONAR, Dušan. *Cvičíme.cz. Oční cviky [online]*. 2009 [cit. 2014-03-19]. Dostupné z: http://www.cvicime.cz/cviky/ocni-cviky/vsechny-strany.

Seznam obrazového materiálu

Zdroje obrazového materiálu

Virtuální klávesnice

ČERMÍK, Ivo. Mobil.idnes.cz. *Virtuální klávesnice nejen pro mobilní telefony* [online]. mafra, 202 [cit. 2014-03-06]. Dostupné z: http://mobil.idnes.cz/virtualni-klavesnice-nejen-pro-mobilni-telefony-f63-/mob_tech.aspx?c=A020603_5070665_mob_aktuality

Správné sezení u počítače

BROŽ, Josef. Svět harware: ... vše ze světa počítačů. In: *Počítače a zdravotní problémy* [online]. 2006, 2.3.2006 [cit. 2014-03-18]. Dostupné z: http://www.svethardware.cz/pocitace-a-zdravotni-problemy/13626/img/body-0.5FF2.jpg

Obrázek karpální tunel:

Syndrom karpálního tunelu (Carpal Tunnel). *Jednadvacitka.cz* [online]. 2012 [cit. 2014-03-18]. Dostupné z: http://www.jednadvacitka.cz/user/upload/oski/syndrom_karpalniho_tulenelu.jpg

Policejní virus

Viry.cz - Policejní virus: Likvidace fotografií, dokumentů aneb nový „policejní virus“ na scéně. [online]. 2013 [cit. 2014-08-04]. Dostupné z: http://www.viry.cz/wp-content/uploads/2013/09/viruszeman.jpg

Falešný dopis banky

Novinky.cz: Podvodníci se snaží mailem vylákat citlivá data, varuje Česká spořitelna [online]. 2013 [cit. 2014-08-04]. Dostupné z:http://media.novinky.cz/397/403977-original1-9t267.jpg

PŘÍLOHA 1 – DOTAZNÍK

Dotazník

Bezpečnost práce s počítačem

Dobrý den,

jmenuji se Miroslav Beránek a zpracovávám diplomovou práci na téma „Informační bezpečnost jako velmi důležitá oblast výuky informatiky na základní a střední škole“, jejíž součástí je i tento dotazník. Rád bych tě poprosil a vyplnění následujících otázek, zakroužkováním odpovědí. Předem děkuji za spolupráci.

On-line verze dotazníku je na adrese www.zskomenskeho-skutec.cz/dotaznik.html

1) **Pohlaví**
   a) Chlapec
   b) Dívka

2) **Věk: …….** **Škola:…….**

3) **Jak nejčastěji sedíš u počítače?**
   a) 
   b) 
   c) 

4) **Jaké zařízení nejvíce používáš:**
   a) Stolní počítač
   b) Notebook
   c) Tablet
   d) Mobilní telefon

5) **Kolik času trávíš denně u počítače (notebooku, tabletu apod.)?**
   a) 1 – 3 hodiny
   b) 3 – 5 hodin
   c) 5 – 7 hodin
   d) 7 a více

6) **Která z následujících aktivit je pro tebe nejdůležitější:**
   a) Sport
   b) Posezení s přáteli
   c) Komunikace s přáteli na internetu
   d) Jakákoliv činnost na počítači

7) **Jak často zálohuješ data v počítači?**
   a) Každý týden
   b) Každý měsíc
   c) Nepravidelně
   d) Vůbec

8) **Pro ukládání písniček, filmů, fotek používáš:**
   a) Flash disk
   b) Externí pevný disk
   c) CD, DVD, Blu-ray disk
   d) Neshromažďuji žádná data

9) **Používáš nějaké on-line datové úložiště (cloud)?**
   a) GoogleDisc, OneDrive Microsoft, iCloud
   b) DropBox apod.
   c) nevyužívám

10) **Kontroluje někdo, co na internetu děláš?**
   a) Ano – starší sourozenec
   b) Ano – rodiče
   c) Ne

11) **Heslo k emailu, facebooku apod. zná:**
   a) Pouze já a nikomu jej neříkám
   b) Nejlepší kamarád/ka
   c) Rodiče
   d) Několik lidí

12) K čemu nejvíce využíváš internet?

a) Komunikace (Facebook, ICQ, …)
b) Hraní her
c) Přehrávání hudby, klipů
d) Vyhledávání informací

13) Jak znáš osoby, se kterými komunikuješ přes počítač?

a) Komunikuji pouze s těmi, které znám osobně
b) Většinu lidí znám osobně
c) Většinu znám pouze z internetu
d) Komunikuji s každým, kdo se mi ozve

14) Osobě, kterou neznáš, ale již dlouho se spolu bavíte, bys sdělil:

a) Telefonní číslo
b) Adresu
c) Kam chodím do školy

15) Znáš některé z těchto projektů týkajících se bezpečnosti na internetu?

a) „Seznam se bezpečně!“ (www.seznamsebezpecne.cz)
b) „Bezpečně on-line.cz“ (www.bezpecneon-line.cz)
c) „Bezpečný internet.cz“ (www.bezpecnyinternet.cz)
d) „Protišikaně.cz“ (http://proti-sikane.saferinternet.cz)
e) žádný z těchto projektů neznám

DĚKUJI ZA VYPLNĚNÍ