Řešené úlohy z oblasti digitální technologie – údržba a ochrana dat

Bc. Tereza Plšková

Diplomová práce
2018

Univerzita Tomáše Bati ve Zlíně
Fakulta aplikované informatiky

Univerzita Tomáše Bati ve Zlíně
Fakulta aplikované informatiky
akademický rok: 2017/2018

ZADÁNÍ DIPLOMOVÉ PRÁCE
(PROJEKTU, UMĚLECKÉHO DÍLA, UMĚLECKÉHO VÝKONU)

Jméno a příjmení:	**Bc. Tereza Plšková**
Osobní číslo:	**A16212**
Studijní program:	**N3902 Inženýrská informatika**
Studijní obor:	**Učitelství informatiky pro střední školy**
Forma studia:	**prezenční**
Téma práce:	**Řešené úlohy z oblasti digitální technologie – údržba a ochrana dat**
Téma anglicky:	**A Set of Pre-solved Tasks from the Digital Technology Maintenance and Data Protection Fields**

Zásady pro vypracování:

1. **Seznamte se s rámcovým vzdělávacím programem pro gymnázia a odborné vzdělávání.**
2. **Proveďte průzkum používaných nástrojů a existujících podkladů pro výuku na středních školách zaměřených na údržbu a ochranu dat.**
3. **Vytvořte podklady pro výuku zaměřené na údržbu a ochranu dat.**
4. **Vypracujte pracovní listy pro ověření technických schopností posluchačů.**
5. **Prakticky ověřte sadu úloh pomocí dotazníku.**

Rozsah diplomové práce:

Rozsah příloh:

Forma zpracování diplomové práce: **tištěná/elektronická**

Seznam odborné literatury:

1. **KRÁL, Mojmír. Bezpečný internet: chraňte sebe i svůj počítač. První vydání. Praha: Grada Publishing, a.s., 2015, 183 s. Průvodce. ISBN 978-80-247-5453-6.**
2. **SZOR, Peter. Počítačové viry: analýza útoku a obrana. Brno: Zoner Press, 2006, 608 s. Encyklopedie Zoner Press. ISBN 80-86815-04-8. Dostupné také z: http://katalog.k.utb.cz/F/?func=service&doc_library=UTB01&doc_number=000028527&line_nun BRIEF&service_type=MEDIA**
3. **PECINOVSKÝ, Josef. Archivace a komprimace dat: jak zálohovat data, jak komprimovat soubory WinRAR, WinZip, WinAce, Windows a nástroje komprese dat, jak archivovat data ve Windows. Praha: Grada, 2003, 116 s. Snadno a rychle. ISBN 8024706598.**
4. **ANDRUŠKO, Alena. Internet, informační společnost a autorské právo. Praha: Wolters Kluwer, 2016, xxii, 254. Právní monografie. ISBN 978-80-7552-327-3.**
5. **BURDA, Karel. Úvod do kryptografie. Vydání první. Brno: Akademické nakladatelství CERM, 2015, 108 s. ISBN 978-80-7204-925-7.**
6. **BROOKSHEAR, J. Glenn, David T. SMITH a Dennis BRYLOW. Informatika. Brno: Computer Press, 2013. ISBN 978-802-5138-052.**
7. **NAVRÁTIL, Pavel a Michal JIŘÍČEK. S počítačem nejen k maturitě. 9. vydání. Prostějov: Computer Media, 2016. ISBN 978-807-4022-531.**

Vedoucí diplomové práce: **Ing. Karel Perůtka, Ph.D.**
Ústav řízení procesů

Datum zadání diplomové práce: **1. prosince 2017**

Termín odevzdání diplomové práce: **16. května 2018**

Ve Zlíně dne 11. prosince 2017

doc. Mgr. Milan Adámek, Ph.D.
děkan

prof. Mgr. Roman Jašek, Ph.D.
garant oboru

Prohlašuji, že

- beru na vědomí, že odevzdáním diplomové práce souhlasím se zveřejněním své práce podle zákona č. 111/1998 Sb. o vysokých školách a o změně a doplnění dalších zákonů (zákon o vysokých školách), ve znění pozdějších právních předpisů, bez ohledu na výsledek obhajoby;
- beru na vědomí, že diplomová práce bude uložena v elektronické podobě v univerzitním informačním systému dostupná k prezenčnímu nahlédnutí, že jeden výtisk diplomové/bakalářské práce bude uložen v příruční knihovně Fakulty aplikované informatiky Univerzity Tomáše Bati ve Zlíně a jeden výtisk bude uložen u vedoucího práce;
- byl/a jsem seznámen/a s tím, že na moji diplomovou práci se plně vztahuje zákon č. 121/2000 Sb. o právu autorském, o právech souvisejících s právem autorským a o změně některých zákonů (autorský zákon) ve znění pozdějších právních předpisů, zejm. § 35 odst. 3;
- beru na vědomí, že podle § 60 odst. 1 autorského zákona má UTB ve Zlíně právo na uzavření licenční smlouvy o užití školního díla v rozsahu § 12 odst. 4 autorského zákona;
- beru na vědomí, že podle § 60 odst. 2 a 3 autorského zákona mohu užít své dílo – diplomovou práci nebo poskytnout licenci k jejímu využití jen připouští-li tak licenční smlouva uzavřená mezi mnou a Univerzitou Tomáše Bati ve Zlíně s tím, že vyrovnání případného přiměřeného příspěvku na úhradu nákladů, které byly Univerzitou Tomáše Bati ve Zlíně na vytvoření díla vynaloženy (až do jejich skutečné výše) bude rovněž předmětem této licenční smlouvy;
- beru na vědomí, že pokud bylo k vypracování diplomové práce využito softwaru poskytnutého Univerzitou Tomáše Bati ve Zlíně nebo jinými subjekty pouze ke studijním a výzkumným účelům (tedy pouze k nekomerčnímu využití), nelze výsledky diplomové/bakalářské práce využít ke komerčním účelům;
- beru na vědomí, že pokud je výstupem diplomové práce jakýkoliv softwarový produkt, považují se za součást práce rovněž i zdrojové kódy, popř. soubory, ze kterých se projekt skládá. Neodevzdání této součásti může být důvodem k neobhájení práce.

Prohlašuji,

- že jsem na diplomové práci pracoval samostatně a použitou literaturu jsem citoval. V případě publikace výsledků budu uveden jako spoluautor.
- že odevzdaná verze diplomové práce a verze elektronická nahraná do IS/STAG jsou totožné.

Ve Zlíně, dne 4.5.2018

.....

podpis diplomanta

ABSTRAKT

Náplní diplomové práce je příprava řešených úloh z oblasti digitální technologie – ochrana a údržba dat. Materiály jsou určeny zejména pro začínající učitele a slouží pro prohloubení znalostí žáků středních škol v počítačové bezpečnosti.

Práce je rozdělena standardně na dvě části. V teoretické části je vysvětlen pojem rámcový vzdělávací program pro střední odborné vzdělávání a gymnázia. Vedle RVP je v teoretické práci uveden výčet a popis programů, které jsou nejčastěji využívány na středních školách pro práci se soubory a složkami. V neposlední řadě obsahuje část zaměřenou na cloudová uložiště, cloud computing a nejznámější služby poskytující cloudová uložiště.

Úvod praktické části je zaměřen zejména na analýzu dotazníkového šetření vytvořený s využitím formulářů dostupných na Google Disk. Hlavní náplní praktické části jsou vyučovací hodiny, které obsahují cíle hodiny, teoretické podklady a návody na práci v jednotlivých programech. Výstupem diplomové práce vedle textových podkladů pro výuku jsou také prezentace shrnující tuto problematiku a pracovní listy sloužící k ověření získaných informací a naplnění cílů. V závěru praktické části je vypracována další analýza, tentokrát zaměřená na ověření a zhodnocení vypracovaných materiálů.

Klíčová slova: rámcový vzdělávací program, Průzkumník souborů, Total Commander, cloudová uložiště, ochrana a údržba dat, správa souborů, složek a disků, zabezpečení počítače, autorská práva, GDPR

ABSTRACT

The main content of this Diploma thesis is creation of pre-solved tasks from the digital technology – data protection and maintenance. Created materials are intended primarily for beginning teachers and they can be used to deepen knowledge of high school students in computer security.

The work is divided into two parts. In the theoretical part there is clarified term framework educational program for secondary vocational education and for grammar schools. In addition to the RVP in the theoretical part there is a list of the programs that are most often used in the high schools for working with files and folders and description of these programs. Finally, this part includes section dedicated to cloud storage, cloud computing and the most famous cloud storage services.

The introduction of the practical part focuses on the analysis of the questionnaire survey which was created using the forms available on Google Drive. The main content of the practical part are lessons, which contains main aims of each lesson, the theoretical resource materials and the instructions for work in the individual programs. The outputs of this work are presentations summarizing this topic and the worksheets which serve to verify student's knowledge obtained during classes. Another purpose of this worksheets is to verify the fulfilment of the set goals. At the end of the practical part there is another analysis. This analysis focuses on the evaluation of developed materials.

Keywords: Framework educational program, File Explorer, Total Commander, cloud storage, maintenance and data protection, management of files, folders and disks, computer security, copyright, GDPR

Na tomto místě bych ráda poděkovala vedoucímu mé diplomové práce Ing. Karlu Perůtkovi, Ph.D. za odborné vedení a pomoc při zpracování této diplomové práce. Dále také své rodině a přátelům za podporu během celého studia.

Prohlašuji, že odevzdaná verze diplomové práce a verze elektronická nahraná do IS/STAG jsou totožné.

OBSAH

ÚVOD

V dnešní době využívají informační a komunikační technologie stále mladší děti. Často i nevědomky sdílí velmi osobní informace, které lze velmi snadno zneužít. Tvoří tak zranitelnou skupinu uživatelů, na kterou se mohou útočníci zaměřit. Proto je nutné klást velký důraz na jejich vzdělávání v oblasti počítačové bezpečnosti a zvyšovat jejich povědomí o kyberkriminalitě. Ochrana a údržba dat je na středních školách vyučována nejen v hodinách informačních a komunikačních technologií, ale také jako průřezové téma. Někteří vyučující proto nevěnují tomuto tématu dostatečnou pozornost.

Cílem diplomové práce bylo vytvořit univerzální výukové materiály, které by mohly být využívány při výuce informatiky na středních školách i gymnáziích. Materiály byly vypracovány na základě analýzy rámcových vzdělávacích programů a dotazníkového šetření, které se zaměřovalo na témata zařazená do výuky ochrany a údržby dat.

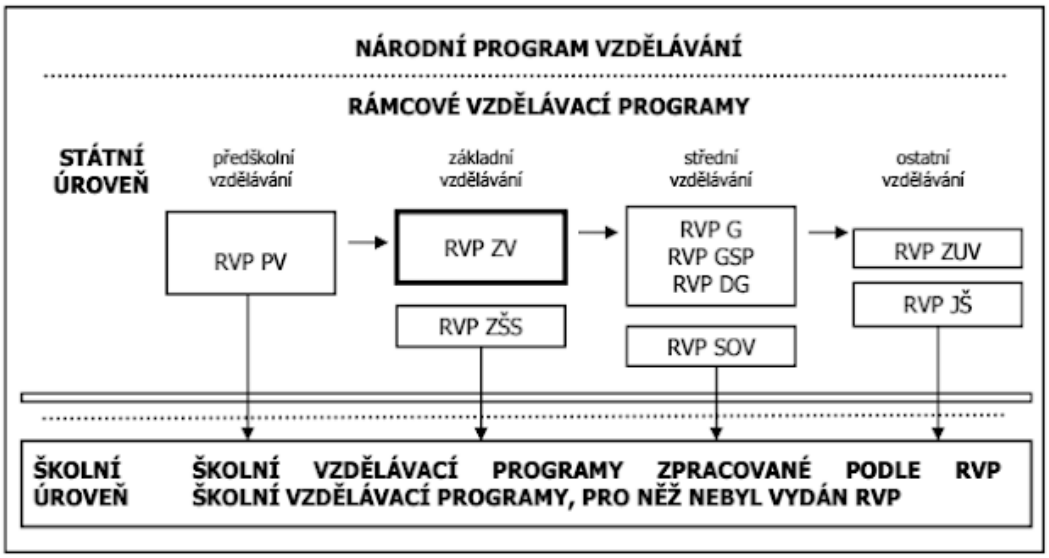
Výstupem práce jsou vyučovací hodiny, prezentace a pracovní listy. Vyučovací hodiny vedle teoretických podkladů obsahují také seznam nově osvojených pojmů a kognitivní, psychomotorické a afektivní cíle hodiny, jejichž splnění lze ověřit zejména pomocí pracovních listů. K pracovním listům jsou přiloženy i návrhy jejich řešení. Veškeré výukové materiály byly vytvořeny s využitím programů Microsoft Office, konkrétně Word a PowerPoint. Hlavním důvodem využití zmíněných programů je jejich velké rozšíření středních školách.

Diplomová práce v neposlední řadě obsahuje také analýzu vytvořených materiálů a průzkumu aktuálních znalostí žáků vybrané střední školy. Výsledek této analýzy poukazuje na některé nedostatky žáků, zejména v oblasti ochrany dat a počítačové bezpečnosti.

I. TEORETICKÁ ČÁST

1 RÁMCOVÝ VZDĚLÁVACÍ PROGRAM

Rámcové vzdělávací programy (RVP) představují závazný kurikulární dokument pro každý obor vzdělání v předškolním, základním a středním vzdělávání, na základě kterých jsou tvořeny školní vzdělávací programy (ŠVP). Zavedeny byly zákonem č. 561/2004 Sb., o předškolním, základním, středním, vyšším odborném a jiném vzdělávání (Školský zákon). RVP spadají společně s Bílou knihou (národním programem vzdělávání – NVP) do státní úrovně v systému kurikulárních dokumentů (Obr. 1). Vydává je ministerstvo školství a tělovýchovy (MŠMT) po projednání s příslušnými ministry. Výjimku tvoří RVP pro obory vzdělávání, které spadají pod ministerstvo obrany, vnitra a spravedlnosti. Taková RVP jsou vydávána příslušným ministerstvem po projednání s MŠMT. [1], [2]



Obrázek 1: Schéma systému kurikulárních dokumentů [3]

Rámcové vzdělávací programy se dělí na:

- RVP PV – rámcový vzdělávací program pro předškolní vzdělávání
- RVP ZV – rámcový vzdělávací program pro základní vzdělávání
- RVP ZŠS – rámcový vzdělávací program pro obor vzdělání základní škola speciální
- RVP G – rámcový vzdělávací program pro gymnázia
- RVP GSP – rámcový vzdělávací program pro gymnázia se sportovní přípravou
- RVP DG – rámcový vzdělávací program pro dvojjazyčná gymnázia
- RVP SOV – rámcový vzdělávací program prostřední odborné vzdělávání
- RVP ZUV– rámcový vzdělávací program pro základní umělecké vzdělávání
- RVP JŠ – rámcový vzdělávací program pro jazykové školy s právem státní zkoušky [3]

Rámcové vzdělávací programy obsahují zejména konkrétní cíle, formy, délku a povinný obsah vzdělávání. Dále jsou zde uvedeny zásady pro tvorbu ŠVP, organizační uspořádání, profesní profily a materiální a personální podmínky. Výraznou změnou oproti dřívějšímu vzdělávání je důraz na klíčové kompetence. Ty představují soubor vědomostí, dovedností, schopností a postojů, které mají být ve výuce rozvíjeny v průběhu vzdělávání. Dále jsou zde vymezena průřezová témata, která by se měla prolínat mezi předměty i ročníky vzdělávání. [1], [2]

1.1 Rámcový vzdělávací program pro gymnázia

RVP pro gymnázia je určen pro tvorbu ŠVP na čtyřletých gymnáziích a vyšším stupni víceletých gymnázií. K dispozici jsou také speciální RVP pro gymnázia se sportovní přípravou, dvojjazyčná gymnázia a gymnázia v angličtině.

Je zde definováno šest klíčových kompetencí – k učení, k řešení problémů, komunikativní, sociální a personální, občanská a k podnikavosti. [4]

RVP pro gymnázia dále stanovuje osm vzdělávacích oblastí, které obsahují charakteristiku a cílové zaměření vzdělávací oblasti a vzdělávací obsah. Jedná se o:

- jazyk a jazykovou komunikaci (český jazyk a literatura, cizí jazyk a další jazyky),
- matematiku a její aplikace,
- člověka a přírodu (fyzika, chemie, biologie, geografie, geologie),
- člověka a společnost (občanský a společenskovědní základ, dějepis, geografie),
- člověka a svět práce,
- umění a kulturu (hudební a výtvarný obor),
- člověka a zdraví (výchova ke zdraví, tělesná výchova),
- informatiku a informační a komunikační technologie. [4]

Dále jsou zde vymezena průřezová témata. Jako průřezová témata jsou vybrána ta, která jsou vnímána jako aktuální. Patří sem osobností a sociální výchova, výchova k myšlený v evropských a globálních souvislostech, multikulturní výchova, environmentální výchova a mediální výchova. [4]

Informatika a informační a komunikační technologie (ICT)

Oblast informatika a ICT navazuje na oblasti v základním vzdělávání zaměřené na zvládnutí základní úrovně informační gramotnosti. Je zaměřena zejména na prohlubování schopností

žáků využívat informační a komunikační technologie, a to zejména tvůrčím způsobem. Dále se zaměřuje na využívání informačních zdrojů a možnosti aplikačního programového vybavení s cílem zlepšení orientace v narůstajícím množstvím informací a při respektování právních a etických zásad. [4]

RVP rozděluje vzdělávací obsah na několik sekcí – digitální technologie; zdroje a vyhledávání informací, komunikace; zpracovávání a prezentace informací. Každá sekce dále vždy obsahuje popis očekávaných výstupů u žáka a obsah učiva. Časová dotace za čtyři roky studia na informační technologie je stanovena na čtyři hodiny, přičemž si škola sama stanový v ŠVP, ve který ročnících se budou vyučovat. [4]

1.2 Rámcový vzdělávací program pro střední odborné vzdělávání

RVP pro střední odborné vzdělávání jsou rozděleny podle kategorií soustavy oborů vzdělávání (Obory J, Obory E, Obory, H, Obory L a M, Konzervatoře a Nástavbová studia). Pro každý obor vzdělávání existuje jeden RVP. Obory zaměřené na informační technologie spadají do kategorie Obory L a M, ty poskytující střední vzdělávání s maturitní zkouškou.

Vzdělávání v oboru v souladu s cíli středního odborného vzdělávání směřuje k tomu, aby si žáci vytvořili klíčové kompetence odpovídající jejich schopnostem a studijním předpokladům. Vedle klíčových kompetencích jsou zde vždy definovány odborné kompetence v závislosti na oboru vzdělávání. RVP pro odborné vzdělávání definuje těchto osm klíčových kompetencí:

- kompetence k učení,
- kompetence k řešení problémů,
- komunikativní kompetence,
- personální a sociální kompetence,
- občanské kompetence a kulturní povědomí,
- kompetence k pracovnímu uplatnění a podnikatelským aktivitám,
- matematické kompetence,
- kompetence využívat prostředky informační a komunikačních technologií a pracovat s informacemi. [5], [6]

Dále jsou zde stejně jako v předchozím RVP definovány průřezová témata – občan v demokratické společnosti; člověk a životní prostředí; člověk a svět práce; informační a komunikační technologie. [5], [6]

Vzdělávání v informačních a komunikačních technologií

Všechny rámcové vzdělávací programy pro střední odborné vzdělávání definují stejné oblasti spadající do informačních a komunikačních technologií. Jedná se o oblasti zaměřené na:

- práci s počítačem, operační systém, soubory, adresářová struktura, souhrnné cíle,
- práci se standardním aplikačním programovým vybavením,
- práci v lokální síti, elektronická komunikace, komunikační a přenosové možnosti Internetu,
- informační zdroje, celosvětová počítačová síť Internet. [6]

Minimální počet vyučovacích hodin v oblasti vzdělávání v informačních a komunikačních technologií za celou dobu vzdělávání je stanoven na 6 hodin týdně (192 hodin celkově). [6]

1.2.1 Zaměření na informační technologie

Informatické obory jsou označovány kódem 18-20-M/01. Spadají sem obory zaměřené na výpočetní techniku, elektronické počítačové systémy, informační technologii – aplikaci osobních počítačů, správu informačních systémů, počítačové elektronické systémy a informatiku v ekonomice.

RVP pro odborné vzdělávání definuje vedle klíčových kompetencích také odborné kompetence. Pro obory zaměřené na informační technologie jsou vymezeny tyto odborné kompetence:

- navrhovat, sestavovat a udržovat HW,
- pracovat se základním programovým vybavením,
- pracovat s aplikačním programovým vybavením,
- navrhovat, realizovat a administrovat počítačové sítě,
- programovat a vyvíjet uživatelská, databázová a webová řešení,
- dbát na bezpečnost práce a ochranu zdraví při práci,
- usilovat o nevyšší kvalitu své práce, výrobků nebo služeb,
- jednat ekonomicky a v souladu se strategií udržitelného rozvoje. [5]

Oproti gymnáziím je v RVP pro informační obory definováno devět vzdělávacích oblastí. Pro různé obory odborného vzdělávání jsou definovány stejné oblasti vzdělávání. Jediný rozdíl tvoří oblast odborného vzdělávání u některých oborů. Tyto oblasti si každá škola dále

rozpracovává ve školním vzdělávacím programu do jednotlivých vyučovacích hodin. Jedná se o:

- jazykové vzdělávání a komunikaci,
- společenskovědní vzdělávání,
- přírodovědné vzdělávání,
- matematické vzdělávání,
- estetické vzdělávání,
- vzdělávání pro zdraví,
- vzdělávání v informačních a komunikačních technologiích,
- ekonomické vzdělávání. [5]

Vzdělávání v informačních a komunikačních technologií

Cílem vzdělávání v oblasti informačních a komunikačních technologií je zejména naučit žáky pracovat s prostředky ICT a s informacemi. Vzdělávání je dále vhodné rozšířit dle aktuálních vzdělávacích potřeb, které mohou být ovlivněny trhem práce, vývojem počítačových technologií a specifika daných oborů. Oblasti učiva informačních a komunikačních technologií se neliší od oblastí definovaných v RVP pro jiné obory vzdělávání. Jedná se o:

- práci s počítačem, operační systém, soubory, adresářová struktura, souhrnné cíle,
- práci se standardním aplikačním programovým vybavením,
- práci v lokální síti, elektronická komunikace, komunikační a přenosové možnosti Internetu,
- informační zdroje, celosvětová počítačová síť Internet. [5]

V každé oblasti je dále detailněji rozepsán obsah tematického celku a očekávané výsledky vzdělávání žáka.

RVP pro informační obory dále obsahuje vymezení několika konkrétních okruhů z oblasti ICT. Lze zde najít okruh hardware, základní programové vybavení, aplikační programové vybavení, počítačové sítě a programování a vývoj aplikací.

Rámcové rozvržení obsahu vzdělávání související s ICT je znázorněno v následující tabulce.

Vzdělávací oblasti a obsahové okruhy	Minimální počet vyučovacích hodin za celou dobu vzdělávání	
	týdenních	celkový
Vzdělávání v informačních a komunikačních technologiích	4	128
Hardware	5	160
Operační systémy	6	192
Aplikační software	8	256
Počítačové sítě	4	128
Programování a vývoj aplikací	8	256

Tabulka 1: Rámcové rozvržení obsahu vzdělávání v oblasti ICT [5]

2 NÁSTROJE PRO PRÁCI SE SOUBORY A SLOŽKAMI

Pro práci se soubory a složkami lze využít nespočet různých programů. Každý počítač má své vlastní vestavěné programy v závislosti na operačním systému, který využívá. Samozřejmostí je také možnost využití programů dostupných na internetu ať už v placené verzi nebo jako freeware.

2.1 Nástroje OS Windows

Mezi nástroje vestavěné v operačním systému Windows patří File Explorer a Tento počítač.

2.1.1 File Explorer

File Explorer (Průzkumník souborů), je program, který slouží pro práci se soubory a jejich správou v operačním systému Microsoft Windows. Poprvé byl zavede ve verzi Windows 95 jako náhrada správce souborů ve starších verzích. Program byl postupně vyvíjen a z původně jednoduchého navigačního nástroje vznikl nástroj na správu souborů. Vedle správy disků, souborů a složek má také důležitou funkci při zobrazování grafického uživatelského rozhraní a umožňuje také uživateli počítač ovládat, ať už přes hlavní panel, nabídku start či přes plochu. [7]

Součástí Průzkumníku jsou nejčastěji používané složky, nejnovější soubory a panel nástrojů rychlý přístup. Ve verzi Windows 10 rychlý přístup vedle složek uživatele a disků obsahuje také složku pro cloudové uložiště OneDrive. To umožňuje velmi rychlé a snadné přesouvání a ukládání do cloudového uložiště přímo z Průzkumníku.

2.1.2 Tento počítač

Nástroj Tento počítač slouží na rozdíl od Průzkumníku zejména pro práci s disky, které jsou připojeny do počítače. Pomocí tohoto nástroje lze také velmi snadno přistupovat na sdílené disky mezi více počítači. V neposlední řadě zde lze vybrané disky spravovat – optimalizovat, vyčistit nebo formátovat.

2.2 Finder

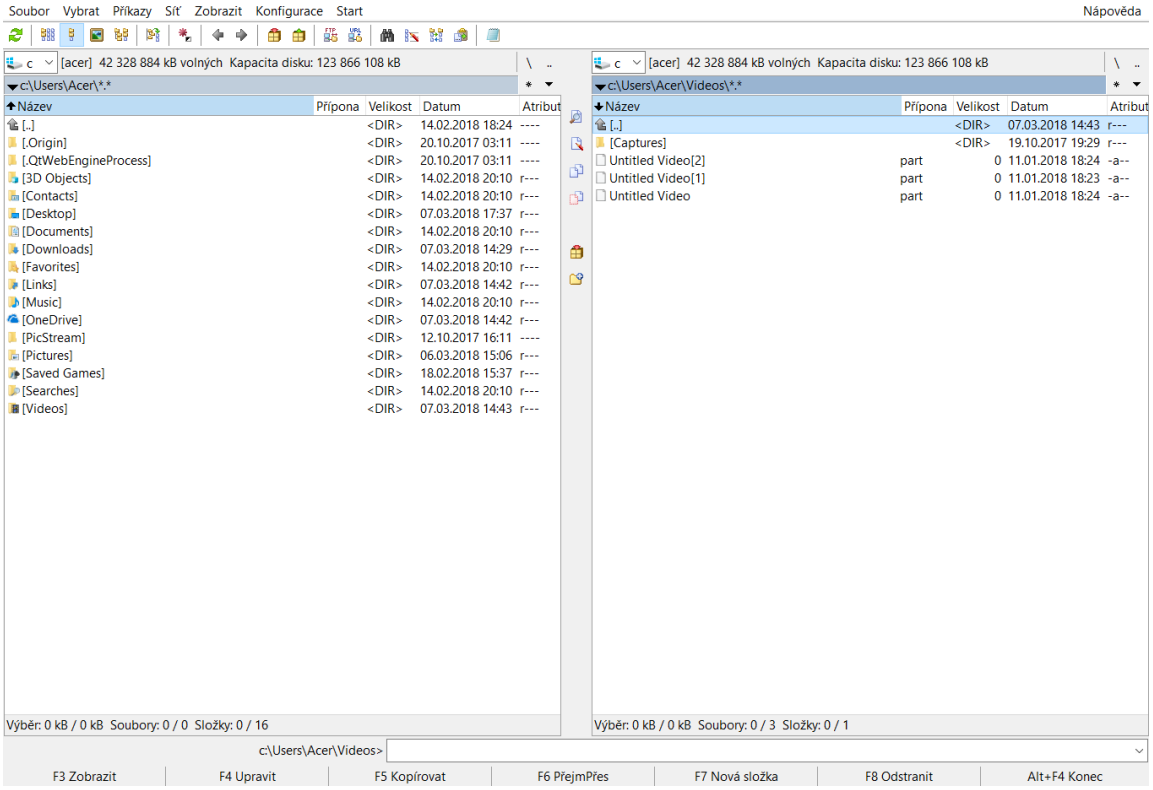
Finder je program umožňující pracovat s dokumenty, složkami či soubory v zařízení od firmy Apple. Tento program má téměř totožné využití jako File Explorer ve Windows zařízeních. Finder se spouští automaticky po zapnutí zařízení a zůstává neustále otevřený. Jeho

součástí je horná řádek nabídek a plocha pod ním. Mezi jeho hlavní funkce patří snadné zobrazování souborů, vytváření a mazání složek a vyhledávání pomocí Spotlightu. [8]

2.3 Total Commander

Total Commander je velmi populární správce souborů pro operační systémy Microsoft Windows. Mezi hlavní vlastnosti programu patří rozdělení uživatelského rozhraní na dva panely s adresáři, které se zobrazují vedle sebe a usnadňují tak práci se soubory a složkami. Vedle správy souborů a složek umožňuje také připojení ke vzdáleným diskům a implementaci a psaní vlastních pluginů. Vytvořené pluginy umožňují uživateli například prohlížet obrázky či přehrávat hudbu. Program dále umožňuje také archivaci souborů a podporuje nejrůznější formáty včetně ZIP i RAR. [9]

Program Total Commander je nabízen v 64bitové, 32bitové a dříve i v 16 bitové verzi jako sharewere včetně verzí pro kapesní počítače a mobilní telefony s operačním systémem Windows a Android. Tyto verze jsou nabízeny jako freeware, standardní verze pro počítač je nabízena pouze jako shareware. [9]



Obrázek 2: Uživatelské rozhraní programu Total Commander verze 9.12

2.3.1 Historie programu

Program Total Commander je vyvíjen Christianem Ghislerem od roku 1992 ve Švýcarsku. První verze programu byla vytvořena v roce 1993 pro Windows 3.1x v němčině a jednalo se pouze o 16bitovou verzi. Byla pojmenována Windows Commander 1.00d. Ještě v tomtéž roce byla vytvořena anglická verze Windows Commander 1.10e. Mezi lety 1994 a 1995 byl program rozšířen do mezinárodní verze a doplněn o francouzštinu, dánštinu a holandštinu. Další velký krok přišel v roce 1996, kdy byla vydána první 32bitová verze Windows Commander 3.0. Tato verze byla naprogramována v Delphi. [10]

V roce 2002 byl program přejmenován na dnes známý Total Commander. Důvodem byl spor o ochrannou známku „Windows“. Poslední velké změny přišly v roce 2012, kdy byly uvolněny verze pro Android a první 64bitová verze tohoto programu. Zatím nejnovější verze Total Commander 9.12 vyšla 24.11.2017. [10]

3 CLOUDOVÁ ULOŽIŠTĚ

Jako cloudová uložiště jsou označovány služby, které nepracují lokálně na počítači a umožňují zálohovat, archivovat a sdílet data prostřednictvím internetu s využitím cloud computingu. K takto uloženým datům lze pak přistupovat z libovolného zařízení (notebook, tablet, mobilní telefon). Cloudová uložiště a obecně cloudové služby a aplikace jsou uloženy v tzv. Cloudu, tedy v síti serverů a počítačů umístěných někde v kyberprostoru. [10], [13]

Pojmem Cloud Computing není označován konkrétní hardware nebo software ale model dodávání výpočetních služeb (serverů, uložišť, databází, analytických nástrojů apod.) přes internet. Uživatel, který si zakoupí službu založenou na cloud computingu k ní přistupuje vzdáleně například pomocí prohlížeče, mobilní aplikace či klienta elektronické pošty. [10], [11], [13]

Výhody:

- automatická synchronizace a zálohování dat,
- přístupnost k souborům z libovolného zařízení a místa,
- možnost obnovy smazaných souborů po určitý čas,
- snadné a rychlé sdílení souborů s jinými uživateli,
- možnost využití verzování souborů. [13]

Nevýhody:

- nutné připojení k internetu,
- větší riziko neoprávněného přístupu k uloženým souborům,
- možnost narušení soukromí. [13]

3.1.1 Typy cloudových služeb

Cloudové služby lze rozdělit do tří základních modelů: Software as a Service (SAAS), Platform as a Service (PAAS) a Infrastructure as Service (IAAS)

SAAS

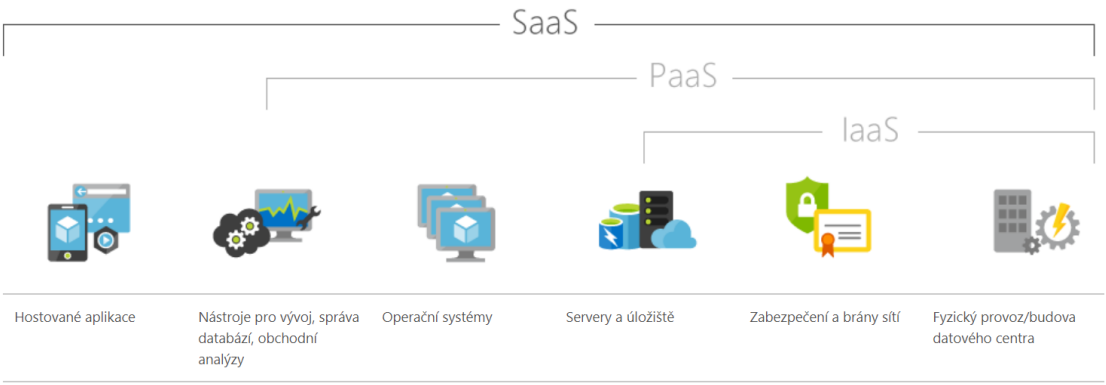
Model SAAS (software jako služba) je nejběžnější produkt využívaný koncovým uživatelem. Dává mu k dispozici softwarové aplikace, přičemž jejichž údržba, správa a uchovávání dat zabezpečuje poskytovatel. Obvykle není u toho modelu vyžadována instalace žádného programu, uživatel přistupuje ke službě pouze pomocí rozhraní dostupného přes internet. Příklad služby založené na tomto modelu je například Google Drive. [12]

PAAS

Model PAAS (platforma jako služba) je využíván nejčastěji vývojáři a provozovateli softwaru. Je založen na zprostředkovávání pracovního prostředí a nástrojů, které slouží pro vývoj, tvorbu a testování webových aplikací. Tento model využívá služba Apprenda. [12]

IAAS

Model IAAS (infrastruktura jako služba) je základní kategorie cloudových služeb a označuje ty služby, které poskytují uživateli prostředky pro výpočetní aktivitu. Využívá ho například Amazon Web Service či Google Compute Engine. [12]



Obrázek 3: Základní modely cloudových služeb [12]

3.1.2 Příklady cloudových uložišť

S rozmachem výpočetní technologie roste i nabídka služeb poskytujících cloudová uložiště. Nabídka na trhu je tak bohatá, že téměř každá služba nabízí základní balíček s prostorem zdarma. Mezi nejznámější patří zejména cloudové uložiště Box, Drop Box, OneDrive a Google Drive.

Box

Uložiště Box je zaměřeno zejména na firmy. Umožňuje nastavení oprávnění přístupu k souborům pro jednotlivé uživatele, přiřazovat úkoly či zanechávat poznámky. Bezpečnost sdílených dat zaručuje možnost nastavení hesla či doby, po kterou budou data sdílena. Nabízí zdarma až 10 GB, kdy velikost nahrávaného souboru je omezena na 250 MB. Nevýhodou je, že verzování souborů je umožněno pouze platícím uživatelům. Data lze synchronizovat pomocí aplikace dostupné pro zařízení Windows, ale i pro mobilní telefony s Androidem a iOS. [13]

DropBox

Firma Dropbox, Inc. byla založena v roce 2007, přičemž spuštění uložiště proběhlo o rok později.

Po registraci získá uživatel zdarma 2 GB paměti. Tu lze navýšit až na 20 GB pomocí používání mobilní aplikace či doporučení uložiště novým uživatelům. Na rozdíl od předchozího uložiště je velikost nahrávaných souborů bez limitu a umožňuje také verzování dokumentů i v bezplatné verzi. Dropbox uchovává verze všech souborů po dobu 30 dnů. Synchronizační aplikace jsou k dispozici pro počítače s operačními systémy Windows, Mac i Linux a mobilní telefony s Androidem i iOS. [14]

OneDrive

OneDrive (dříve SkyDrive) je uložiště společnosti Microsoft. Služba podporuje 93 jazyků včetně češtiny. Nabízí zdarma 5 GB paměti a verzování je povoleno pouze u dokumentů Microsoft Office. OneDrive se také vyznačuje následujícími prvky:

- Office Online – aplikace umožňující nahrávání, vytváření, úpravu a sdílení dokumentů Microsoft Office přímo z prohlížeče.
- Integrace do sociálních sítí – propojení OneDrive se sociálními sítěmi (Facebook, LinkedIn, Twitter) umožňuje rychlé a snadné sdílení dokumentů mezi přáteli používající tyto sociální sítě.
- Prezentace fotografií v prohlížeči bez nutnosti jejich stahování.
- Podpora formátu ZIP.
- Obnova smazaných dat pomocí „koše“. [15]

V novějších verzích operačního systému Windows 8 a víše je OneDrive již integrován jako aplikace a je plně synchronní s ostatními aplikacemi.

Google Drive

Google Drive od společnosti Google byl uveden do provozu v roce 2012. Podporuje téměř jakýkoliv formát. Ukládat tak lze téměř cokoliv od fotek přes články a nákresy až po zvukové nahrávky a videa. Výhodou je také propojení s balíčkem Microsoft Office. Google Drive obsahuje výkonné vyhledávání, které dokáže rozpoznat objekt na obrázcích či text v naskenovaných dokumentech. Součástí je také aplikace Google Forms, která slouží pro vytváření dotazníků a průzkumů. [16]

Google Drive nabízí prostor až 15 GB, který je sdílený mezi Disk, Gmail a Fotky Google. Dále nabízí uchovávání posledních 100 verzí souborů po dobu 30 dnů. Výhodou Google Drive je provázanost s dalšími produkty společnosti Google jako je online kancelářský balík a e-mailový klient. [16]

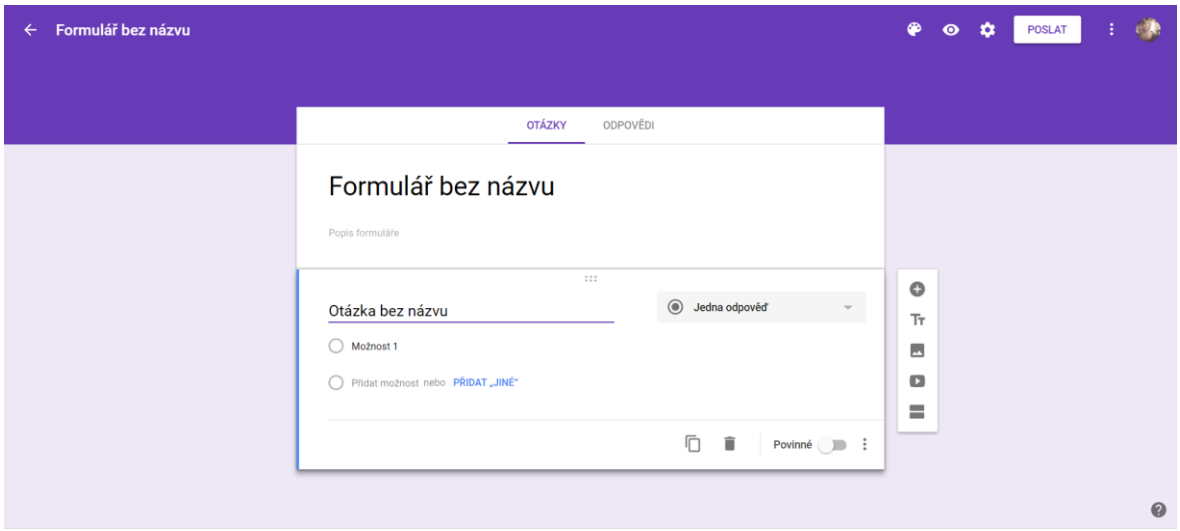
II. PRAKTICKÁ ČÁST

4 ANALÝZA POUŽÍVANÝCH NÁSTROJŮ A OBSAH HODIN NA ŠKOLÁCH

Pro vytvoření výukových materiálů bylo nejprve nutné provést analýzu dat. Za tímto účelem byl vytvořen elektronický dotazník. Hlavním cílem dotazníku bylo zjištění, jaká podtémata jsou zařazena do tematického celku údržba a ochrana dat, kolik hodin je tomuto tématu celkově věnováno a zda vyučující využívají nějaké podpůrné nástroje a softwary. Všechny zjištěné informace sloužily pro tvorbu prezentací a následně i pracovních listů.

4.1 Tvorba dotazníku

Dotazník byl vytvořen pomocí online aplikace Google Forms dostupné na Google Drive. Práce s touto aplikací je velmi snadná a intuitivní bez nutnosti instalování programu do počítače. Dotazník lze následně jednoduše přeposlat pomocí přímého zadání e-mailové adresy nebo pomocí odkazu. Výhodou je i možnost zkrácení URL adresy přímo v aplikaci.



Obrázek 4: Rozhraní online aplikace Google Forms

4.2 Výběr a oslovení středních škol

Pro výběr středních škol a gymnázií byl využit seznam dostupný na webových stránkách www.stredniskoly.cz/seznam-skol/. Tato stránka rozděluje školy dle krajů a následně i dle okresů. Vybrány byly zejména střední školy s obory zaměřenými na informační technologie a gymnázia. Dále byl seznam škol rozšířen o školy, kde je na výuku informačních technologií také kladen velký důraz, jako jsou například střední průmyslové školy.

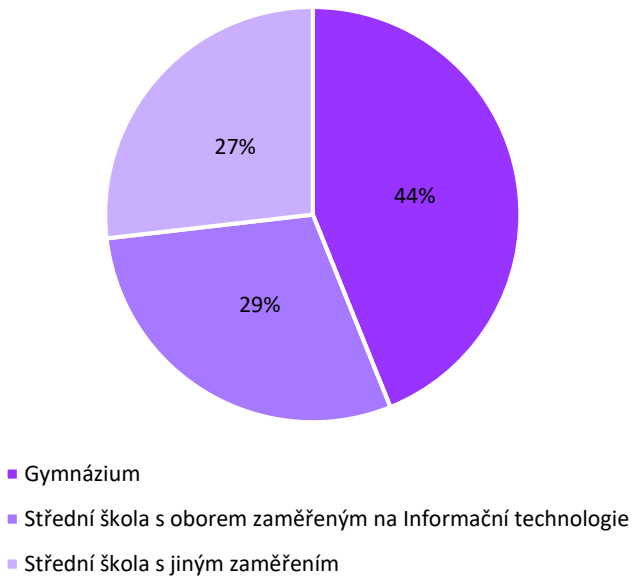
Pro komunikaci s řediteli vybraných škol byly využity e-maily volně dostupné na webových stránkách škol. Za účelem dotazníkového šetření bylo osloveno celkem 104 škol ze Zlínského, Jihomoravského, Olomouckého a Moravskoslezského kraje, z toho pět e-mailu nebylo z různých důvodů doručeno.

4.3 Získané informace

Z celkově 99 doručených e-mailů bylo přijato 41 odpovědí. Dotazník obsahoval šest otázek, které byly všechny povinné. Vedle otázek směrovaných na již zavedený obsah hodin informačních technologií byla přidána jedna otázka, která byla zaměřena na zahrnutí nového nařízení o ochraně osobních údajů GDPR (General Data Protection Regulation) do výuky.

4.3.1 Na jaké střední škole vyučujete Informační technologie?

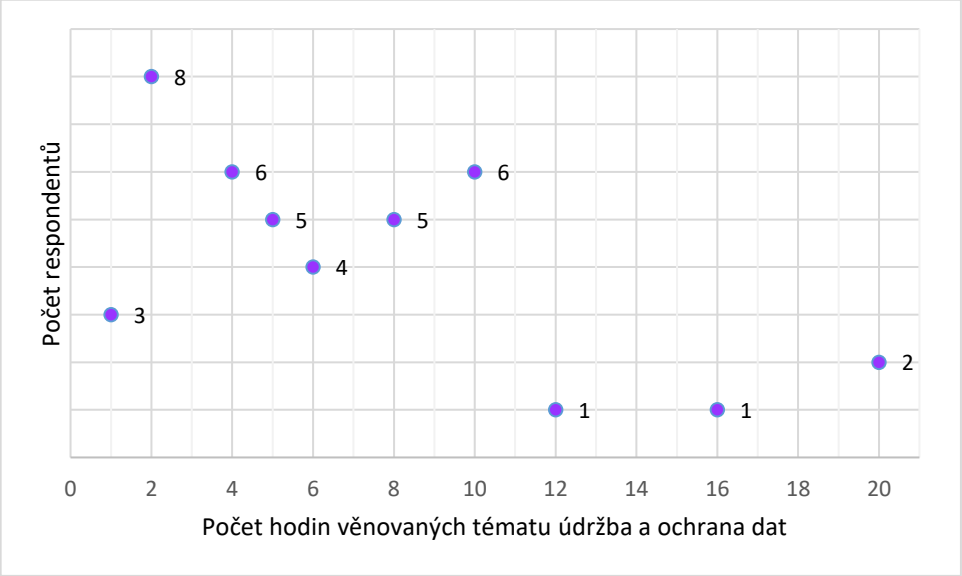
První otázka sloužila zejména pro roztřídění respondentů do kategorií dle typu školy. Dále slouží jako výchozí informace pro rozhodování, na jaký typ školy se spíše zaměřit při tvorbě výukových materiálů. Na výběr byly tři možnosti: gymnázium, střední škola s oborem zaměřeným na informační technologie a střední škola s jiným zaměřením. Z celkových 41 respondentů vyučuje 18 učitelů na gymnáziu (44 %), 12 na středních škola s oborem zaměřeným na informační technologie (29 %) a 11 na jiných středních školách (27 %).



Graf 1: Druhy škol respondentů

4.3.2 Kolik hodin přibližně věnujete výuce tematického celku ochrana a údržba dat v průběhu celého roku?

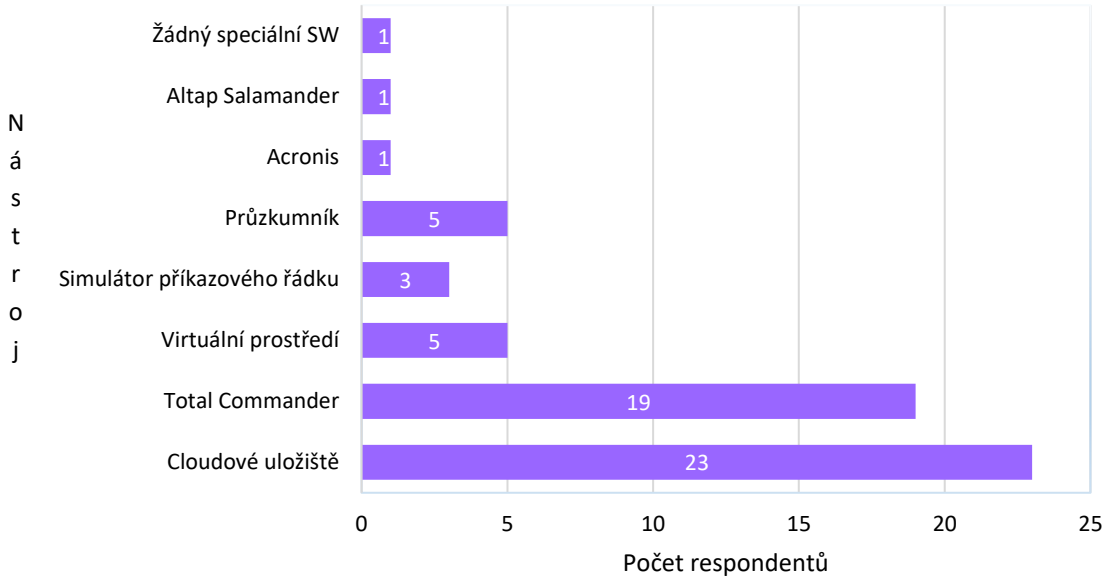
Cílem této otázky bylo zjistit celkový počet hodin věnovaných tematickému celku ochrana a údržba dat. Pro tuto otázku bylo umožněno zadávání libovolných odpovědi a zřejmě i proto se odpovědi respondentů značně lišily. Někteří vyučující téma považují za průřezové, proto bylo těžší odhadnout počet hodin, který tématu věnují. Odpovědi se pohybovali v rozmezí od 1 do 20 hodin. Pro určení počtu hodin byla využita průměrná hodnota zaokrouhlena na jednotky nahoru.



Graf 2: Počet hodin věnovaných výuce ochrany a údržby dat

4.3.3 Jaký software či služby využíváte při výuce tematického celku ochrana a údržba dat?

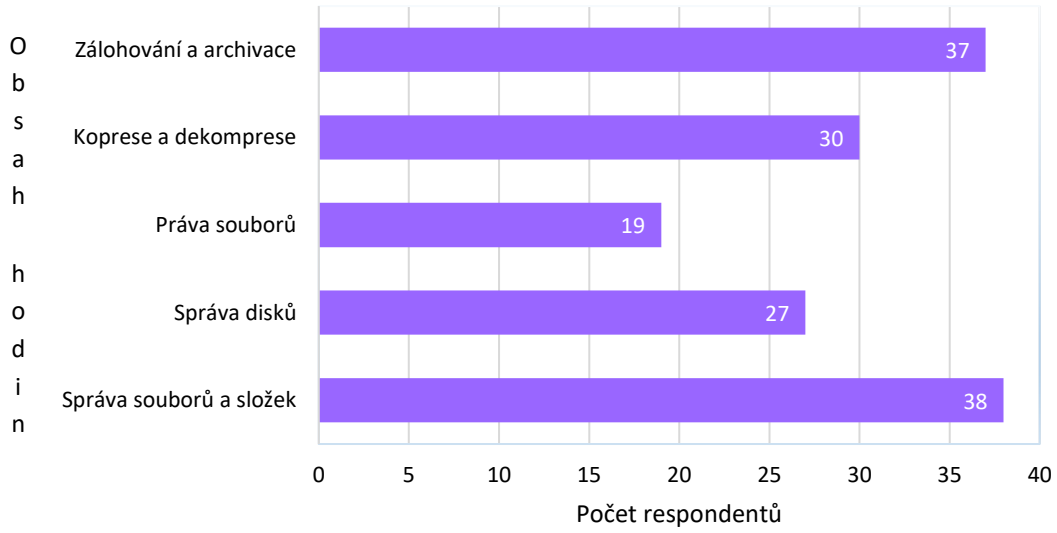
U otázky tři bylo na výběr z nabídky s možností doplnění vlastního nástroje. Respondenti často volili právě možnost otevřené odpovědi. Dle odpovědí jsou využívány při vyučování údržby dat zejména cloudová uložiště (23 respondentů) a Total Commander (19 respondentů). Mezi méně časté odpovědi patří virtuální prostředí, průzkumník Windows a obecně systémové nastavení Windows. Ostatní nástroje byly zmíněny pouze jednou, proto nejsou při tvorbě výukových materiálu využity.



Graf 3: Nástroje využívané při výuce ochrany a údržby dat

4.3.4 Jaká témata zařazujete do tematického celku údržba dat?

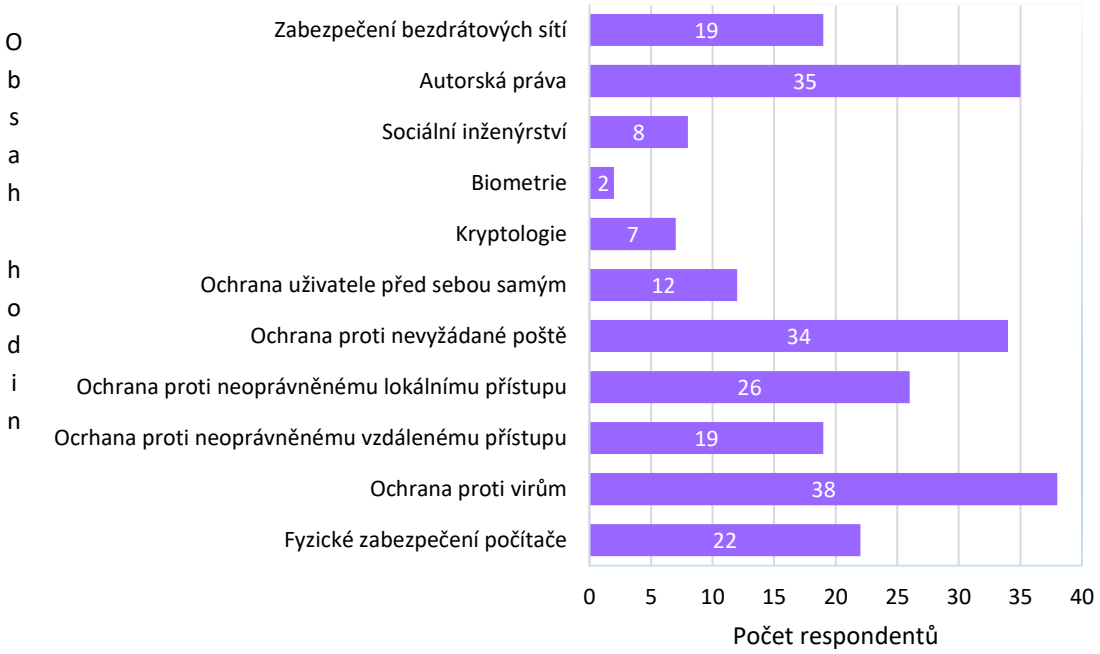
Pro získání informací o obsahu vyučovacích hodin bylo téma rozděleno na dvě části. V případě údržby dat téměř vždy alespoň polovina vyučujících zařazuje nabízená podtémata do výuky. Nejčastěji jsou hodiny zaměřeny na správu souborů a složek (38 respondentů) a jejich následné zálohování a archivaci (37 respondentů). Více jak 70 % respondentů odpovědělo, že do výuky pravidelně zařazují také komprimaci a dekomprimaci dat. Nejméně jsou do výuky zařazována práva souborů (19 respondentů).



Graf 4: Obsah hodin při výuce údržba dat

4.3.5 Jaká témata zařazujete do tematického celku ochrana dat?

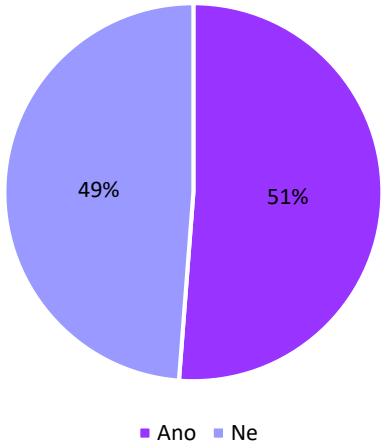
Druhou část výuky tvoří ochrana dat. V tomto případě se odpovědi více lišily. Dle získaných informací je do výuky nejčastěji zahrnována ochrana dat proti virům (38 respondentů), ochrana proti nevyžádané poště (34 respondentů) a autorská práva (35 respondentů). Nejméně často pak biometrie (2 respondenti) a kryptologie (7 respondentů). V závislosti na odpovědích byl následně určen rozsah jednotlivých podtémat.



Graf 5: Obsah hodin při výuce ochrana dat

Plánujete do tematického celku zahrnout nové nařízení GDPR?

S novým nařízením o ochraně osobních údajů se nabízela otázka o zahrnutí GDPR do výuky informačních technologií. Větší polovina respondentů (51 %) odpověděla, že neplánují téma zahrnout do hodin informatiky. Rozdíl dvě procenta (jedné odpovědi) ale není tak markantní, proto se práce bude zabývat i nařízením GDPR.

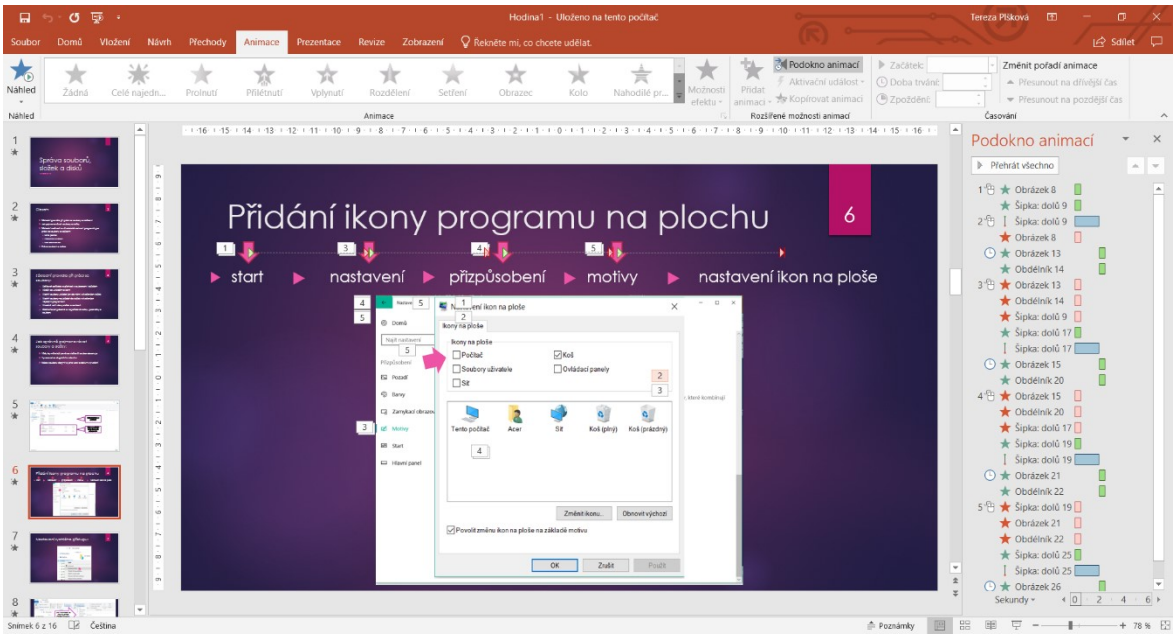


Graf 6: Zařazení GDPR do výuky

5 VYTVÁŘENÍ PREZENTACÍ A PRACOVNÍCH LISTŮ

Hlavní součástí práce jsou prezentace, které shrnují veškeré informace týkající se ochrany a údržby dat sloužící pro výuku tohoto tématu. Pro tvorbu prezentací byl využit program Microsoft Office PowerPoint 2016 z balíčku Office 365. Prezentace obsahují stručný přehled veškerých teoretických informací včetně praktických ukázek práce v nástrojích pro správu souborů a složek.

Pro interaktivní znázornění praktických ukázek bylo využito zejména animací v kombinaci vložených tvarů. Výsledkem práce je sedm prezentací pro každou hodinu vytvořenou v následující kapitole. Názvy jednotlivých prezentací vždy odpovídají číslu aktuální hodiny (*Hodina1.pptx, Hodina2.pptx*, atd.).

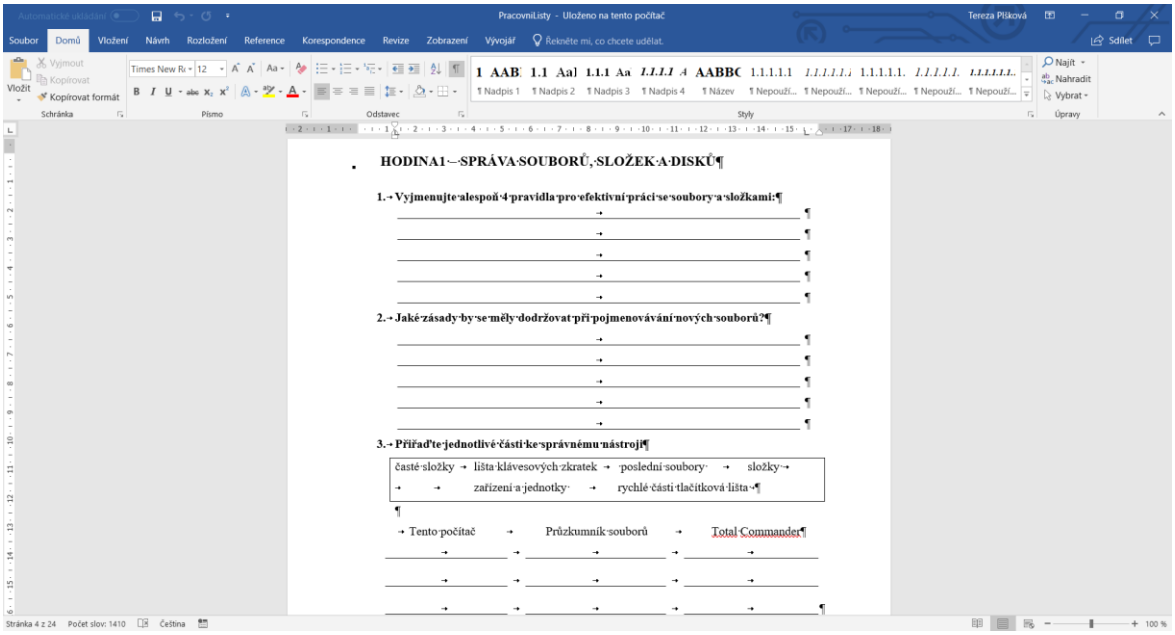


Obrázek 5: Ukázka využití animací pro tvorbu prezentací

Pro ověření informací nově získaných z vytvořených hodin byly navrhnuty pracovní listy. Tyto listy obsahují jak teoretické, tak praktické úkoly. Všechny pracovní listy jsou uloženy v jednom komplexním dokumentu ve formátu PDF (*PracovniListy.pdf*). Jednotlivé části jsou pro snadnější orientaci pojmenovány stejně jako prezentace podle čísla hodin. Vedle pracovních listů soubor obsahuje také návrhy řešení.

Pro tvorbu pracovních listů nebyl využit žádný speciální software, jelikož se budou rozdávat pravděpodobně v tištěné podobě. Nejjednodušší proto bylo je vytvořit v programu MS Word 2016. Otázky a úkoly v pracovních listech jsou voleny tak, aby na základě vyplněných listů

bylo možné ověřit, zda byly splněny cíle (převážně kognitivní a psychomotorické) definované na začátku vyučovací hodiny.



HODINA1—SPRÁVA SOUBORŮ, SLOŽEK A DISKŮ

1. Vyjmenujte alespoň 4 pravidla pro efektivní práci se soubory a složkami:

2. Jaké zásady by se měly dodržovat při pojmenovávání nových souborů?

3. Přiřaďte jednotlivé části ke správnému nástroji

Tento počítač	Průzkumník souborů	Total Commander

Obrázek 6: Ukázka využití tabulátorů pro tvorbu pracovních listů

6 MATERIÁLY PRO VÝUKU OCHRANY A ÚDRŽBY DAT

Dle informací získaných z dotazníkového šetření byl obsah rozdělen do sedmi vyučovacích hodin. Pro výuku údržby dat byly na základě získaných informaci zvoleny tyto nástroje a služby: Total Commander, Cloudové uložiště a Windows Explorer.

Téma údržba a ochrana dat bylo pak rozděleno následovně:

1. hodina – správa souborů, složek a disků
   - správa souborů a složek
   - správa disků
   - práva souborů

2. hodina – základy údržby a ochrany dat
   - zálohování dat
   - archivace dat
   - komprimace a dekomprimace dat

3. hodina – bezpečné zacházení s počítačem a na počítači
   - fyzické zabezpečení počítače
   - ochrana uživatele před sebou samým
   - sociální inženýrství

4. hodina – ochrana proti nevyžádanému přístupu
   - ochrana proti nevyžádanému vzdálenému přístupu
   - ochrana proti nevyžádanému lokálnímu přístupu

5. hodina – bezpečná komunikace
   - ochrana proti virům
   - ochrana proti nevyžádané poště
   - digitální podpis

6. hodina – zabezpečení bezdrátových sítí
   - zabezpečení bezdrátové sítě
   - kryptologie

7. hodina – autorská práva a ochrana osobních údajů
   - autorská práva
   - GDPR

Na základě této osnovy byly následně vytvořeny nové učební materiály. Tyto materiály vedle teorie a popisu práce v nástrojích pro správu souborů a složek obsahují také seznam nově osvojených pojmů a cíle hodiny. Prezentace byly přizpůsobeny stanovenému počtu sedmi hodin stejně jako pracovní listy.

6.1 1. hodina

Téma hodiny: Správa souborů, složek a disků

Nově osvojené pojmy: File Explorer, Finder, Total Commander

Cíle hodiny:

Kognitivní:	Žák bude znát základní nastavitelná oprávnění v účtech operačního systému Windows.
Psychomotorický:	Žák zvládne efektivně pracovat se soubory a složkami s využitím nástrojů Průzkumník souborů, Tento počítač a Total Commander.
Afektivní:	Žák pochopí význam správného pojmenování souborů a složek pro efektivní práci na počítači.

Přílohy: prezentace a pracovní list *Hodina1*

6.1.1 Správa souborů, složek a disků

Základním pravidlem při ochraně dat je udržovat si pořádek a přehled v souborech a složkách. Je důležité vědět co ukládám a kam. Tím pádem i vím, kde co hledat, a v horším případě i co se ztratilo.

Základní pravidla pro správu souborů a složek

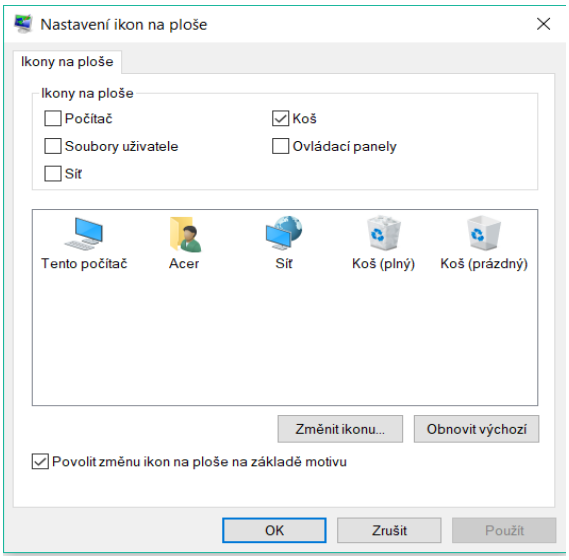
Prvním krokem je vytvoření nového adresáře (složky) pro ukládání vlastních datových souborů. Nikdy pro ukládání takových souborů není vhodné používat složky, které si vytvořil nějaký program. To by mohlo vést k problémů při spuštění daného programu. Velmi důležitý je při tvorbě složek zejména volba názvu. Vždy by mělo být jasné, jaká data přesně obsahuje. V neposlední době je dobré také odstranit nepotřebné či prázdné složky a podsložky.

Druhým krokem je vhodné pojmenování jednotlivých souborů ve složkách, zejména se pak vyvarovat duplicitním názvům. Stejně jako u adresářů je nutné občas projít veškeré soubory a smazat nebo archivovat ty nepotřebné.

Nástroje pro práci se soubory, složkami a disky

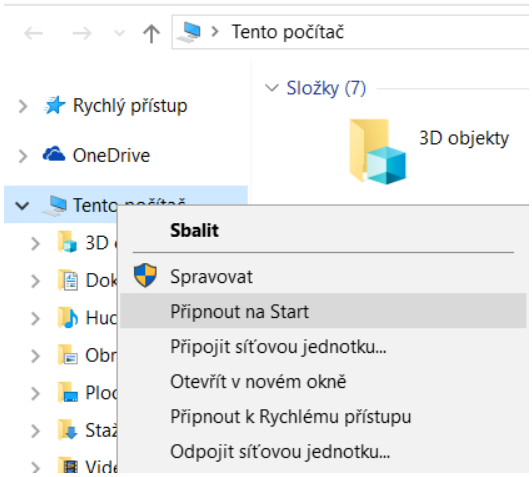
Pro práci se soubory, složkami a disky lze využít několik nástrojů, které jsou součástí počítače – `Tento počítač` nebo `Průzkumník Windows`.

`Tento počítač` přehledně zobrazuje veškeré disky, které jsou v počítači zapojeny a základní složky, které obsahuje každý počítač (Dokumenty, Hudba, Obrázky, Plocha apod.) Lze zde například velmi snadno zjistit celková velikost a volné místo na jednotlivých discích. Nástroj `Tento počítač` lze velmi jednoduše spustit poklepáním na ikonu na ploše nebo přes nabídku `start`. Ikonu lze jednoduše na plochu přidat přes `start -> nastavení -> přizpůsobení -> motivy -> nastavení ikon na ploše.`



Obrázek 7: Nastavení ikon na ploše v operačním systému Windows

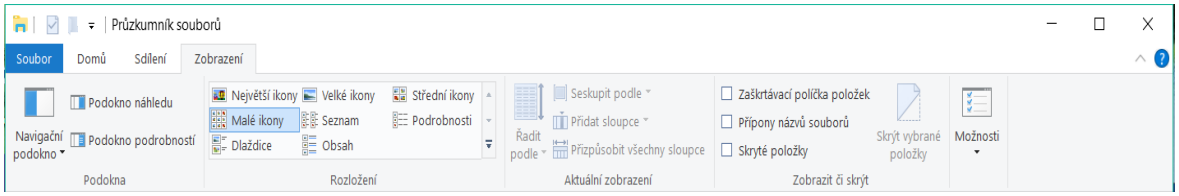
Pro rychlý přístup k tomuto nástroji je možné jej připnout na panel nástrojů jednoduchým kliknutím pravého tlačítka myši na název programu v levé části spuštěného okna a vybrat možnost `Připnout na start`.



Obrázek 8: Upravení panelu nástrojů přidáním nástroje Tento počítač

V horní části nástroje je pás karet. Ten obsahuje kartu `Soubor, Počítač a Zobrazení`. Po kliknutí na libovolný disk se pás karet doplní o kartu `Správa`. Tato karta umožňuje optimalizovat, vyčistit a formátovat vybraný disk. Optimalizace disku se většinou provádí automaticky a lze nastavit, zda má proběhnout denně, týdně nebo měsíčně.

Druhým nástrojem pro správu souborů v operačních systémech Windows je `Průzkumník`. Jeho alternativou pro počítače od firmy Apple je program `Finder`. Tento nástroj při spuštění zobrazí složku `Rychlý přístup`, která zobrazuje nejčastěji otvírané složky a soubory, s kterými uživatel pracoval v poslední době. Spustit lze kliknutím na ikonu v panelu nástrojů, vybráním v nabídce `start` nebo stisknutím zkratky `WIN+E`. Průzkumník se nejčastěji používá pro otevírání dokumentů a programů, vyhledávání souborů a složek a základní práci s nimi jako je jejich přejmenovávání, kopírování či mazání. Pás karet `Průzkumníku` obsahuje kartu `Soubor, Domů, Sdílení a Zobrazení`. Karta `Zobrazení` stejně jako u předchozího nástroje slouží zejména pro změnu vzhledu zobrazených složek. Rozložení s využití různě velikých `ikon` nezobrazuje žádné dodatečné informace. `Dlaždice` jsou naproti tomu doplněny o cesty jednotlivých souborů, `Obsah` o datum poslední změny, autora a velikost souborů a `Podrobnosti` lze nastavit libovolně pomocí tlačítka `Přidat sloupce`.



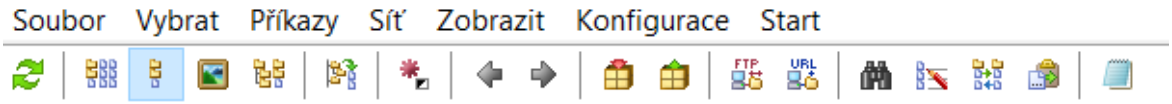
Obrázek 9: Karta Zobrazení nástroje Průzkumník souborů

Vedle již vestavěných nástrojů pro správu souborů lze využít i jiné nástroje jako je například Total Commander, Altap Salamander či Double Commander.

Program Total Commander se vyznačuje zejména rozdělením uživatelského rozhraní do dvou panelů. Uživatel tak může snadno a rychle pracovat se soubory a složkami na dvou různých discích. Práce v programu je založena na klávesových zkratkách. Nejdůležitější zkratky pro správu souborů a složek jsou vypsány ve spodní části programu – `F3` Zobrazit,

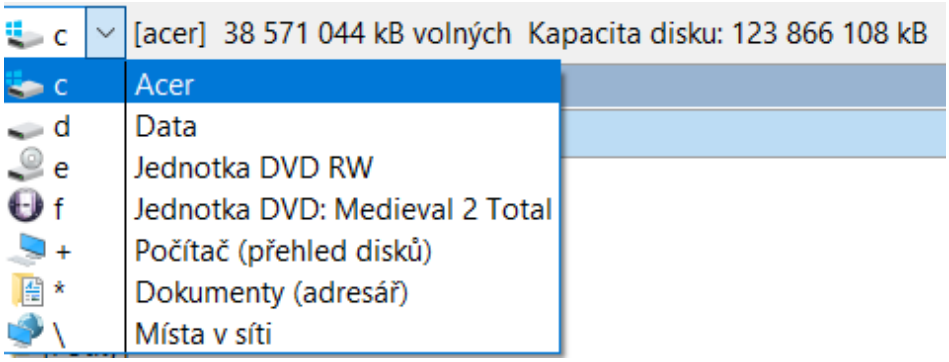
`F4` Upravit, `F5` Kopírovat, `F6` PřejmPřes (přejmenovat nebo přesunout), `F7` Nová složka, `F8` Odstranit a `Alt+F4` Konec.

V horní částí programu jsou karty, pomocí kterých také s programem pracovat. Při otevření libovolné karty je téměř u každé nabídky zobrazena také klávesová zkratka. Vedle klávesových zkratek a karet lze program ovládat také pomocí ikon, které se nacházejí pod pásem karet a v rámu rozdělující panely zobrazující obsah disků.



Obrázek 10: Hlavní nabídka karet a ikon programu Total Commander

Poslední částí programu jsou rozbalovací seznamy se všemi disky počítače. Při zvolení libovolného disku se zobrazí také jeho celková kapacita včetně volné paměti.



Obrázek 11: Nabídka výběru jednotlivých disků v programu Total Commander

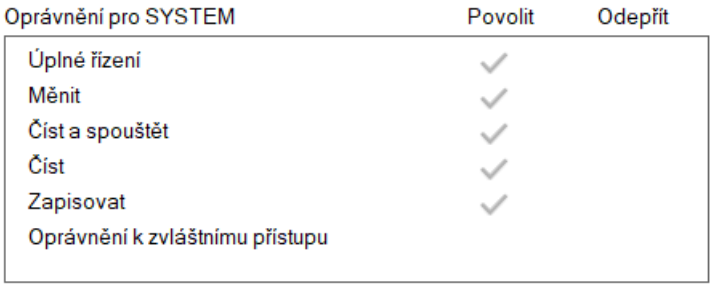
6.1.2 Práva souborů

Nastavování práv souborů je doporučeno měnit v programech pro tvorbu virtuálního prostředí.

Uživatel má u jednotlivých souborů nastavená práva v závislosti na typu účtu, přes který je přihlášen. V operačním systému Windows jsou možné upravovat tato oprávnění:

- úplné řízení – umožňuje uživateli nebo skupině úplné řízení vybraného souboru nebo složky (povolením tohoto oprávnění jsou automaticky povolena všechna následující oprávnění),
- měnit – umožňuje uživateli nebo skupinám číst, vytvářet, měnit a odstraňovat soubory, nikoliv ale měnit práva či vlastnictví souborů,

- číst a spouštět – umožňuje uživateli nebo skupinám zobrazovat soubory a spouštět programy,
- zobrazovat obsah složky – poskytuje stejné oprávnění jako předchozí možnost, ale pouze u složek,
- číst – umožňuje uživateli nebo skupinám zobrazit obsah složky, atributy souborů, číst oprávnění a synchronizovat soubory,
- zapisovat – umožňuje uživateli nebo skupinám vytvářet soubory, zapisovat data, číst oprávnění a atributy a synchronizovat soubory. [18]
- speciální oprávnění – nastavená oprávnění neodpovídají žádný výše uvedené možnosti.



Obrázek 12: Ukázka nastavený oprávnění pro vybraného uživatele

6.2 2. hodina

Téma hodiny: Základy ochrany a údržby dat

Nově osvojené pojmy: zálohování dat, archivace dat, komprese dat, dekomprese dat, warehouse

Cíle hodiny:

Kognitivní: Žák bude znát rozdíl mezi zálohování a archivací. Žák dokáže vysvětlit pojem komprimace a dekomprimace dat.

Psychomotorický: Žák se dokáže orientovat v uživatelském rozhraní uložiště Google Drive. Žák bude umět komprimovat data pomocí programu Total Commander.

Afektivní: Žák pochopí význam zálohování a archivace při ochraně dat.

Přílohy: prezentace a pracovní list *Hodina2*

6.2.1 Zálohování a archivace dat

Data a informace tvoří nejcennější obsah počítače. Proto zálohování dat a jejich archivace je prvním krokem nejen údržby ale i samotné ochrany dat. Zálohování a archivace jsou dva různé pojmy. Zálohováním rozumíme vytvoření kopie dat, která slouží pro jejich obnovu v případě ztráty. Archivace je naproti tomu uchovávání unikátních a důležitých dat pro pozdější využití nebo ze zákonné povinnosti po delší dobu. Archivace je právě proto z důvodu dlouhodobého uchovávání dat náročnější na záznamová média než zálohování.

Zálohování

Jak už bylo řečeno, zálohy jsou kopie dat, které jsou ukládána na jiném datovém nosiči či místě. Taková data lze pak využít v případě ztráty dat či jejich poškození způsobené chybou samotného uživatele či fyzickým selháním systému.

Důležitým pojmem souvisejícím se zálohováním je verzování. Jedná se o uchovávání historie veškerých změn, které byly provedeny v informacích nebo datech. Verzování ale může způsobit problém v přehlednosti vytvořených záloh. Je proto nutné si vytvořit svůj vlastní systém ve vytváření záloh a verzí svých souborů. Pomoci může správné pojmenování souborů, kdy je v názvu uveden také datum vytvoření a verze souboru. [19]

Prvním krokem zabezpečení vytvořených dat je uložení kopie těchto dat na pevný disk počítače do jiné složky. Takové zálohování ochrání data před jejich nechtěným smazáním, ale už ne před poruchou pevného disku.

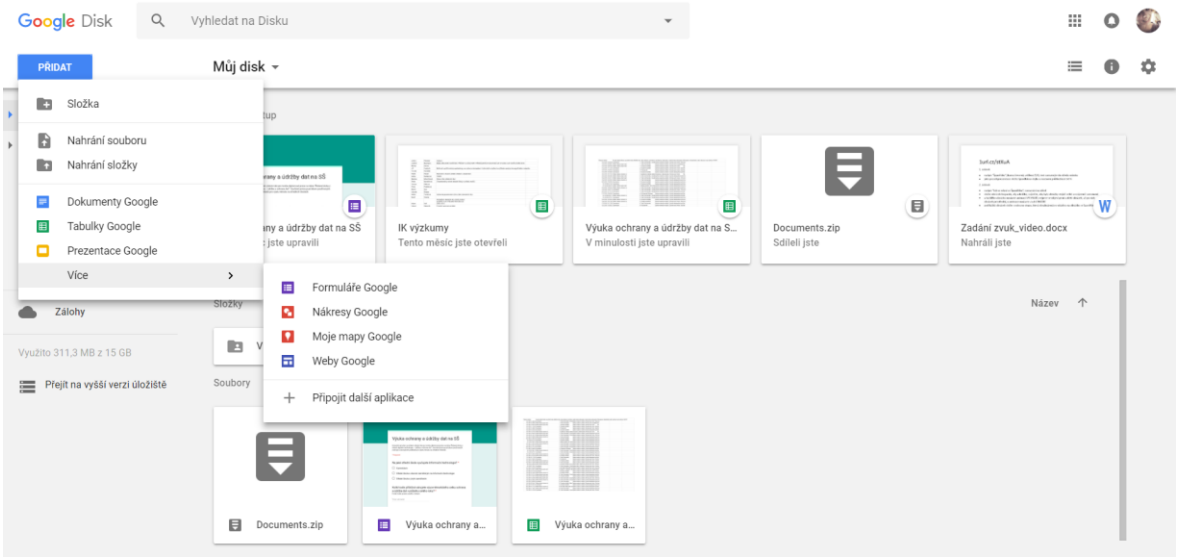
Není proto bezpečné spoléhat pouze na zálohy na pevném disku. Je vhodné využít externí paměťové média jako jsou externí pevné disky, USB flash disky, optická média (CD, DVD), paměťové karty a jiné. Zálohy na externích paměťových médií ochrání data v případě havárie počítači či krádeží. Pro firmy je vhodné využívat pro zálohování tzv. WareHouse. Jedná se o externí datové uložiště. Data jsou zde uložena v několika kopiích, což zabezpečuje vysokou bezpečnost.

Vedle paměťových médií jsou v dnešní době hojně využívány také vzdálené zálohovací služby – cloudová uložiště. Ty umožňují ukládat data pomocí internetu do cloudu. K takto uloženým datům lze pak přistupovat vzdáleně pomocí libovolného zařízení s využitím prohlížeče či speciální aplikace.

Archivace

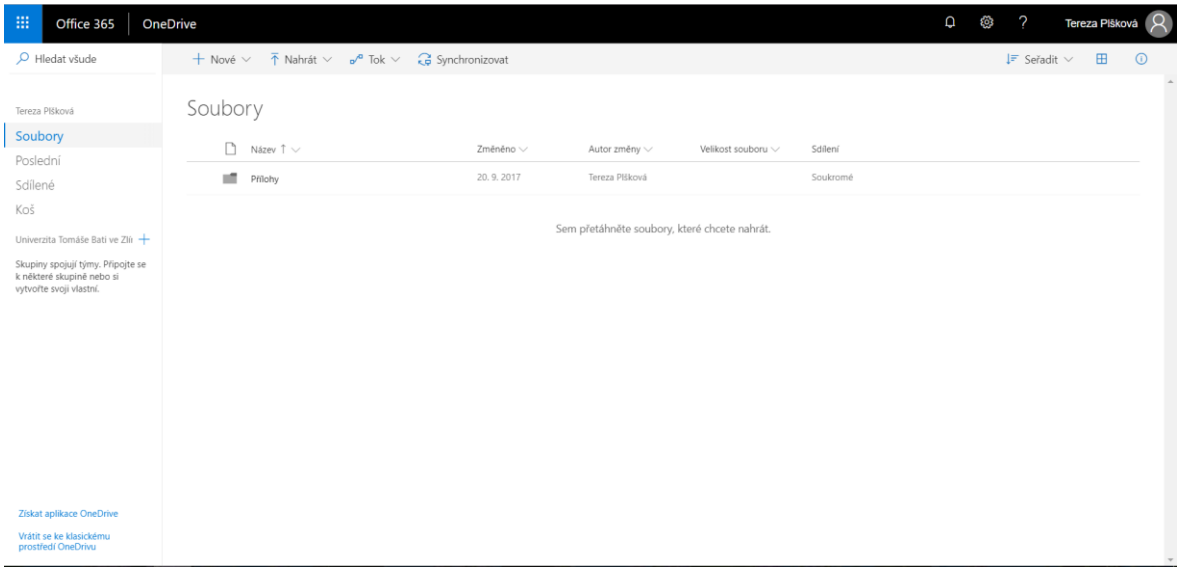
Archivace je proces, který slouží ke dlouhodobému uchovávání dat. Pro archivaci dat lze využít stejná datová média jako pro ukládání zálohy. Pro větší přehlednost je vhodné využívat zvlášť média pro zálohy a zvlášť pro zálohy. Pokud to není možné, je vhodné soubory ukládat alespoň do různých složek. [19]

Vytvořit archiv lze také pomocí datových uložišť. Výhodou je zejména možnost rychlé nahrání souborů pomocí prohlížeče s libovolného zařízení. Pokud má uživatel účet na Google propojený s více zařízeními, lze k takto nahraným souborům přistupovat z každého takového zařízení. Cloudová uložiště lze také se zařízením synchronizovat. Nově vytvořená data se pak automaticky nahrají i do Cloudu. Mezi nejpoužívanější cloudová uložiště patří Google Disk, One Drive a DropBox.



Obrázek 13: Uživatelské rozhraní cloudového uložiště Google Disk

Cloudová uložiště standardně umožňují vytváření složek a nahrané soubory tak třídit. Výhodou Google Disku a OneDrive je vytváření i vlastních souborů – dokumentů, tabulek, prezentací či formulářů. Samozřejmostí je možnost synchronizace uložiště s počítačem.



Obrázek 14: Uživatelské rozhraní cloudového uložiště OneDrive

6.2.2 Komprimace a dekomprimace dat

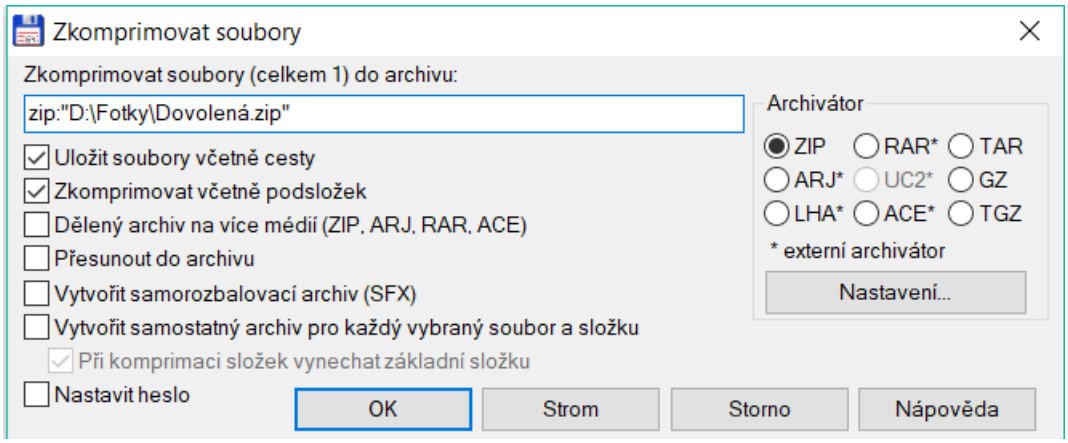
Uchovávání velkého množství dat často zabírá mnoho místa na disku. Za tímto účelem ukládané soubory velmi často procházejí tzv. komprimací (kompresi). Jako komprimaci dat označujeme zpracování počítačových dat za účelem zmenšení jejich objemu při současném zachování informací obsažených v datech. Nejčastěji se data komprimují za účelem jejich archivace nebo přenosu po síti. [19]

Komprimace může být ztrátová i bezeztrátová. Při ztrátové komprimaci dochází k nenávratné ztrátě části informací, které nelze již zpětně získat. Využívá se pouze tam, kde lze takovou ztrátu tolerovat, například při komprimaci zvuku či obrazu. Výhodou ztrátové komprese je velmi nízká velikost výsledného souboru. V případě bezeztrátové komprese nedochází ke ztrátě informací. Výhodou je zpětná rekonstrukce souboru do původní podoby, což je důležité například u textových souborů. Zpětná rekonstrukce souboru se nazývá dekomprimace [19], [21]

Komprimace v programu Total Commander

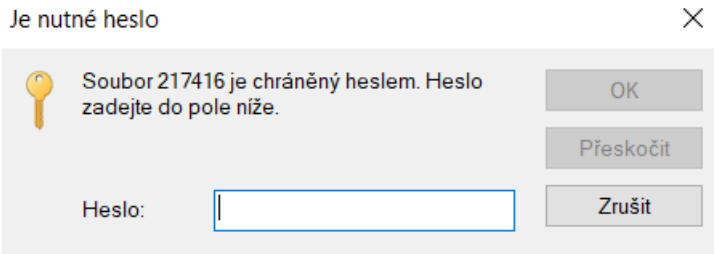
Zkomprimované soubory Za účelem komprimace dat lze využít nespočet programů, např.: 7-ZIP, WinRar či WinZip, ale také souborový manažer Total Commander. Komprimaci v Total Commanderu lze spustit kliknutím na složku, která má být zkomprimována a jednou z následujících možností. Vybráním karty `Soubor` a následně možnosti `Komprimovat`, stisknutím ikony  , nebo stisknutím zkratky `ALT+F5`. Nejprve je nutné zvolit cestu, kam má být zkomprimovaný soubor uložen a jeho název. Dále je nutné zvolit archivátor.

A nakonec je možné pomocí zaškrtávacích polí vybrat co vše se bude komprimovat a zda se mají soubory také přesunout do archivu, nebo nastavit heslo.



Obrázek 15: Komprimace souborů v programu Total Commander

V případě, že uživatel při komprimaci zaškrtne pole nastavit heslo, zobrazí se mu po stisknutí tlačítka OK okno, kde lze zadat vybrané heslo. Heslo je nutné zadat dvakrát. V případě, že by chtěl ať už stejný nebo jiný uživatel soubory ve složce dekomprimovat a zobrazit, musí zadat zvolené heslo. Pokud heslo nezná, složka se mu nerozbalí.



Obrázek 16: Dekomprimace s využitím hesla v programu Total Commander

6.3 3. hodina

Téma hodiny: Bezpečné zacházení s počítačem a na počítači

Nově osvojené pojmy: sandbox, sociální inženýrství, pretexting, phishing, pharming

Cíle hodiny:

Kognitivní: Žák dokáže vysvětlit pojem sociální inženýrství a vyjmenovat a popsat metody sociálního inženýrství.

Psychomotorický: Žák bude schopný vypnout a zapnout používání koše v operačním systému Windows. Žák bude umět rozeznat podvodný e-mail a webovou stránku.

Afektivní: Žák pochopí význam fyzického zabezpečení počítače při ochraně dat.

Přílohy: prezentace a pracovní list *Hodina3*

6.3.1 Fyzické zabezpečení počítače[1]

Fyzickým zabezpečením se uživatel zařízení snaží zabránit jakékoliv neoprávněné manipulaci nebo nechtěnému mechanickému porušení, které mohou vést ke ztrátě nebo porušení dat. Fyzické zabezpečení zejména stolního počítače může být první překážkou v případě potenciálního útoku. Jelikož prolomení nastaveného zabezpečení a hesel může méně zkušeným hackerům trvat delší dobu je pro ně nejjednodušší odpojit harddisk počítače a pokračovat na práci bez rušení jinde.

Součástí fyzického zabezpečení je fyzická bezpečnost budovy a místnosti včetně oken a vstupních dveří. Samozřejmostí by mělo také být elektronické zabezpečení a požární systém. Fyzické zabezpečení hraje velkou roli zejména ve firemním prostředí, kde únik informací obvykle znamená větší ztrátu než u osobních dat běžných uživatelů. Zde se využívají nejrůznější možnosti zamezení vstupu neoprávněných osob, například bezpečnostní kamery, vstupy na čipové karty či s využitím biometrických metod (otisky prstů, skenování sítnice či duhovky apod.).

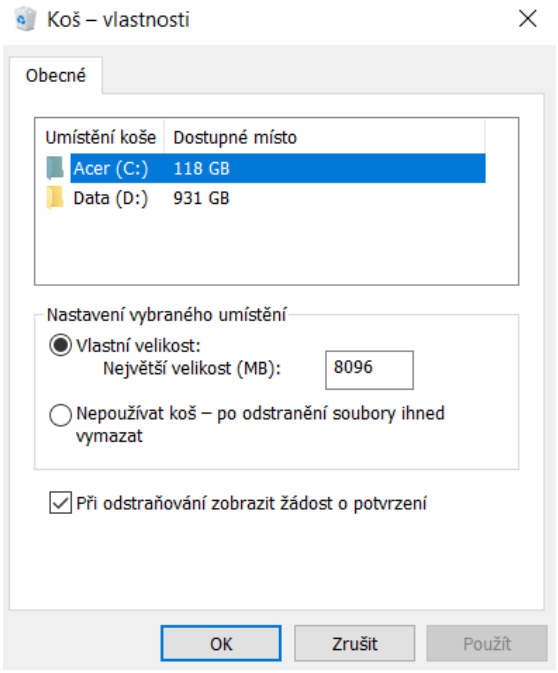
Pro běžného uživatele je důležité zejména nenechávat zařízení bez dozoru. Dále je vhodné zvolit takovou počítačovou skříň, která neumožňuje snadný přístup ke zbytku hardware počítače. Existují počítačové skříně vybavené zámky, nebo je možné skříň umístit do uzamykatelných části pracovního stolu. Samozřejmostí je nastavení přístupových hesel. (Více o heslech v následující hodině).

6.3.2 Ochrana uživatele před sebou samým

Při práci s počítačem je vedle nejrůznější zabezpečovacích programů důležité také samotné chování uživatele. Mezi nejčastější chyby uživatele je nechtěné smazání souboru. Záchranou pro uživatele je `Koš`. Obnovení smazaných souborů lze jednoduše přes tlačítka `Obnovit všechny položky` nebo `Obnovit vybrané položky`. Důležité ale je mít

[1] Kniha stručně a výstižně shrnující počítačovou bezpečnost: Bezpečnost v online prostředí, ISBN 978-80-260-9543-9

v nastavení zapnuté používání Koše. Zda je používání zapnuto lze zkontrolovat ve vlastnostech koše na záložce `Správa`. Pokud je vybrána možnost `Nepoužívat koš`, smazané soubory se z počítače ihned odstraní a uživatel je nemůže rychle a snadno obnovit. Pokud smazaný soubor přesahuje nastavenou velikost opět se automaticky smaže a nepůjde jej obnovit. Pro takové případy je proto vhodné zálohovat veškerá důležitá data na jiných zařízeních nebo pomocí cloudových uložišť.



Obrázek 17: Nastavení vypnutí a zapnutí používání koše

Ochránit uživatele před špatným rozhodnutím může také volba správné typu účtu, na kterém pracuje. Administrátorský účet a učet správce mají mnohem více oprávnění než standardní účty. Další možností může být změna práv uživatele.

V neposlední řadě existují také programy, které zajišťují bezpečnější práci na počítači. Jedná se o aplikace typu sandbox. Sandbox si lze doslova představit jako pískoviště, kdy se písek nedostane mimo něj. Sandbox vytvoří v počítači ohraničený prostor, kde lze bezpečně pracovat. Pokud uživatel pracuje v prostoru vytvořeném tímto programem, nedochází k zanášení operačního systému a má omezený přístup ke zdrojům počítače (využívá jen vybrané adresáře, servery, porty apod.) Pomocí sandboxu lze například spustit neotestovaný kód či program od neověřených dodavatelů či zdrojů, jelikož po uzavření programu se veškerá data vymažou. [20]

6.3.3 Sociální inženýrství

Jaký je nejjednodušší způsob získání cizího hesla? Zeptat se! O tom přesně je sociální inženýrství. Jedná se o přesvědčování a ovlivňování lidí s cílem oklamat je. Účelem sociální inženýrství je získání důležitých informací, aniž by uživatel tušil, že byl právě oklamán. Sociální inženýrství nemusí probíhat pouze v osobním kontaktu s obětí.

Jednou z technik sociálního inženýrství je pretexting. Jedná se o kombinaci lživých informací s pravdivými. Přidáním pravdivé informace oběť nabyde dojmu, že není nebezpečné sdílet další informace. Většina informací, které útočníci následně zneužívají, jsou většinou snadno dostupná. Jedná se například o rodná čísla či rodné jméno matky.

Další technikou sociálního inženýrství je phishing. Phishingem se označuje podvodná technika, jejímž účelem je získání citlivých údajů oběti. Nejčastěji přihlašovací údaje a hesla, čísla kreditních karet apod. Základem phishingu je podvodný e-mail, který nejčastěji obsahuje odkaz na falešné stránky vytvořené útočníkem. Tyto stránky mohou vypadat například jako webové stránky banky. Všechny údaje zadané do takových stránek jdou přímo k útočníkovi a ten je pak velmi snadno může zneužít. Útočníci také mohou využívat tzv. telefonní phishing pomocí hlasového automatu. Oběť je po zavolání na podvodné telefonní číslo vyzvána k přihlášení například pomocí hesla či PINu. [24]

Nástupce phishingu je tzv. pharming. Stejně jako phishing má za úkol získat citlivé údaje uživatelů. Pharming je ale pro uživatele mnohem těžší rozeznat, jelikož útočník dokáže napadnout doménu a přepsat IP adresu stránky. Uživatel je tak po zadání názvu stránek nebo kliknutím na odkaz přesměrován na stránky falešné. [24]

Proti sociálnímu inženýrství je nejlepší obranou zdravý rozum a osvěta.[2] Uživatel by nikdy neměl dávat žádné osobě, ani cizí a ani známé, žádné citlivé údaje jako jsou hesla a PIN kódy. Banky nikdy nepožadují po klientech změnu údajů přes e-mail. Pokud si uživatel neví rady, je možné vysledovat několik znaků, které mohou upozornit na podvodný e-mail. Phishingové e-maily často oslovují pouze obecně (dobrý den, ahoj) a nepoužívají jména příjemců. Dále obsahují podezřelé odkazy na falešné stránky nebo podezřelé přílohy. Takové

[2] Webová stránka shrnující problematiku bezpečnosti na internetu vytvořená ve spolupráci youtubera Jirky Krále a firmy Avast, kterou lze využít pro zpestření výuky: https://www.budsafeonline.cz/

útoky mohou často chodit ze zahraničí, proto je nutné také dbát na to, zda neobsahují gramatické chyby a překlepy.

Předmět: [redacted] Informace o Vaši zásilce
Datum: Thu, 27 Nov 2014 09:28:50 +0100
Od: Ceská pošta <tracktrace@cs-post24.com>
Společnost: cs-post24.com
Komu: [redacted] [redacted].zcu.cz>

logo

[redacted]

Vaše zásilka *DR631396851C* dorazila na 24. listopadu 2014. Courier nebyl schopen doru`eit zásilku pro vás. Vytisknout informace o Vaší zásilky a ukázat, že v nejbližší pošt`i, aby si zásilku.

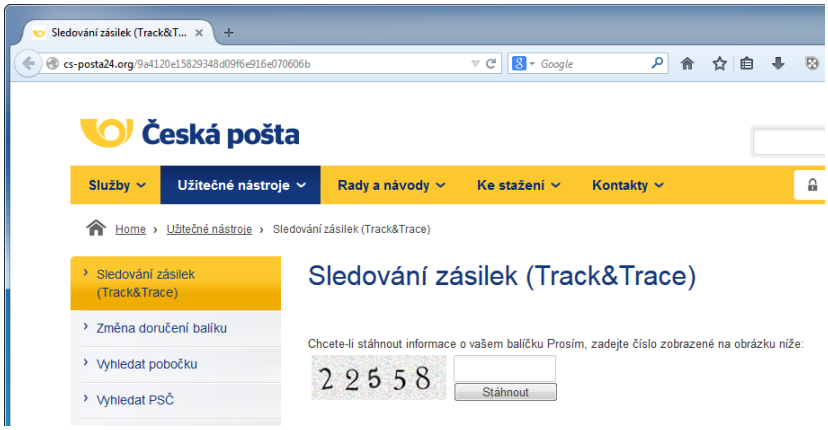
Stáhn`ite si informace o zásilka
<http://cs-post24.com/service.php?id=027364718>

Pokud je zásilka neobdrží do 15 pracovních dn`u `Eeská pošta bude mít právo nárokovat odškodn`iní od si pro své udržení ve výši 52,5 K`e za každý den vedení.
M`užete si najít informace o postupu a podmínkách poi pozemku chov v nejbližší kanceláoi.

Toto je generován automaticky zprávu, pokud nechcete poijímat zprávy od nás prosím odhlásit <http://cs-post24.com/unsubscribe.php?id=625568844>

Obrázek 18: Ukázka podvodného e-mailu využívající phishing

Pokud žádné takové znaky nezpozorujete, je možné se orientovat právě podle falešných stránek. Takové stránky nepoužívají zabezpečené připojení https a certifikáty. Často se také nejedná o aktuální vzhled stránek a log. Cílem takových stránek je získat přihlašovací údaje, proto mohou obsahovat pouze tlačítka a formuláře pro login, ale už ne pro novou registraci. V neposlední řadě je nutné zaměřit pozornost na samotnou URL adresu, ve které mohou být nepatrné rozdíly, chyby či překlepy.



Obrázek 19: Ukázka falešné stránky využívající phishing

6.4 4. hodina

Téma hodiny: Ochrana proti nevyžádanému přístupu

Nově osvojené pojmy: firewall, hash funkce

Cíle hodiny:

Kognitivní:	Žák bude umět vysvětlit pojem firewall a hash funkce.
Psychomotorický:	Žák bude schopný vytvořit bezpečné heslo. Žák bude umět změnit heslo svého učtu v operačním systému Windows.
Afektivní:	Žák pochopí důležitost silného hesla pro zabezpečení počítače proti nevyžádanému lokálnímu přístupu.

Přílohy: prezentace a pracovní list *Hodina4*

6.4.1 Ochrana proti nevyžádanému vzdálenému přístupu

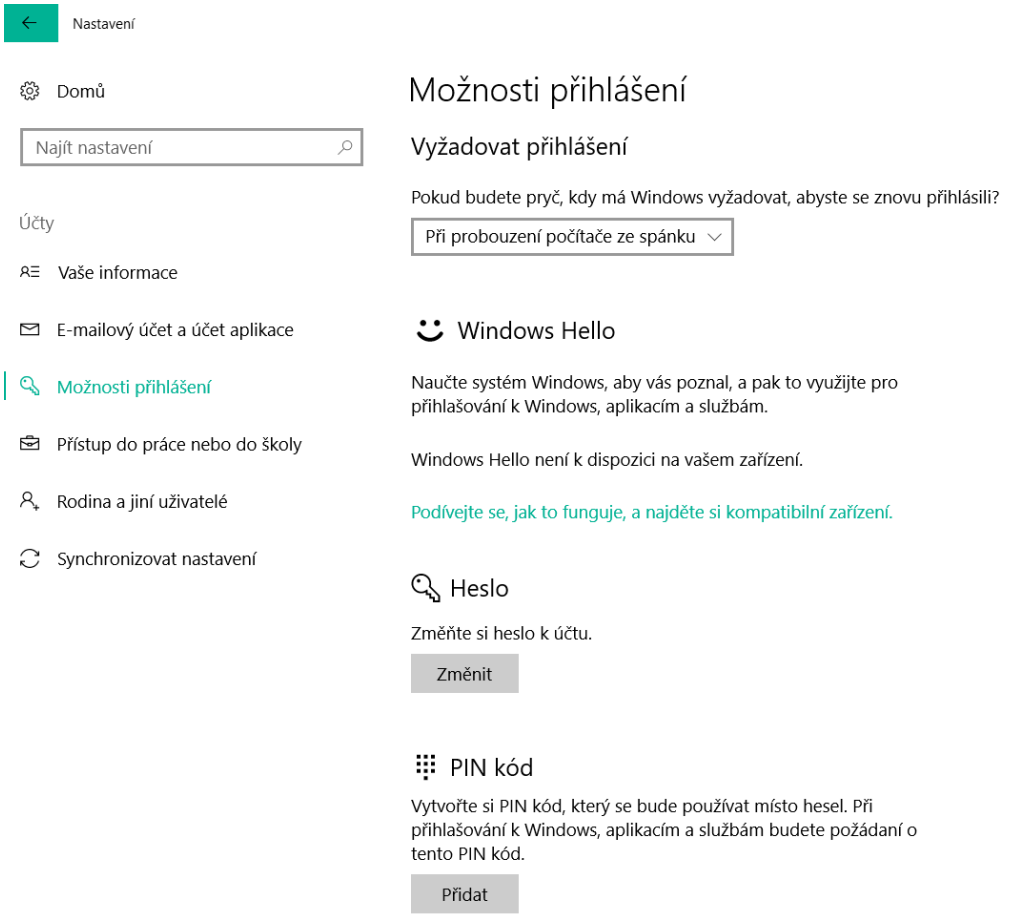
Další formou útoku je nevyžádaný vzdálený přístup. Jedná se o útok hackera na počítač s využitím jiného zařízení. Útočník proto nemusí být přímo v blízkosti oběti.

Chránit se proti takovému útoku lze zejména pomocí firewallu. Firewall tvoří „zeď“ mezi počítačem uživatele a Internetem. Kontroluje bezpečnost různých sítích na různých úrovních. Dokáže filtrovat a omezovat síťový provoz pomocí kontrolování cílových IP adres a portů. Lze tedy říct, že firewally zajišťují bezpečnost při vstupu nebo výstupu dat do a ze sítě. [22], [23]

6.4.2 Ochrana proti nevyžádanému lokálnímu přístupu

Vedle vzdáleného přístupu je nutné také počítač chránit před nevyžádaným lokálním přístupem. Útočníci nepotřebují vždy jiné zařízení, aby se mohli dostat do cizího počítače. Základní formou takové ochrany je zabezpečení počítače heslem. Prvním krokem je samozřejmě zabezpečení přístupu do počítače pomocí hesla do Windows. Takové heslo lze ale snadno obejít, pokud nejsou dodrženy základní pravidla pro vytváření bezpečného hesla.

Pokud nemáte nastavené heslo do Windows, nebo jej chcete změnit, lze to jednoduše přes `nastavení -> účty -> možnosti přihlášení -> Heslo (přidat nebo změnit heslo).`



Obrázek 20: Změna hesla v operačním systému Windows 10

Bezpečné heslo by mělo být minimálně 8 znaků dlouhé (ideálně delší než 14 znaků) a skládat se z kombinace velkých a malých písmen, číslic a povolených speciálních znaků. Dále by nemělo obsahovat žádné slova z dostupných slovníků, opakující se znaky nebo údaje souvisí s uživatelem (jeho jméno, datum narození, telefonní číslo apod.). Mezi dosud nejpoužívanější hesla stále patří 12345. Pro každý účet uživatele je vhodné využívat jiné heslo. Vytvořená hesla si, pokud možno, snažte zapamatovat. Nikam je neukládejte a ani nezapisujte. Pokud potřebuje uživatel pomoct s generováním bezpečného hesla, je v nabídce na internetu několik online generátoru.[3]

[3] Online generátor pro tvorbu bezpečného hesla, které je doplněno o nápovědu na jeho zapamatování: https://passwordsgenerator.net/

Využitím různých znaků v hesle znesnadňuje prolomení pomocí útoku hrubou silou. Takové útoky většinou provádí velmi výkonné počítače. Principem takového útoku je vyzkoušení veškerých možných kombinací znaků. Proto čím více znaků heslo má a čím je heslo delší, tím je i bezpečnější a odolnější proti takovým útokům. [22]

Dalším způsobem prolamování hesel je tzv. Slovníková metoda. Při využívání slovníkové metody útočník zkouší veškerá slova a kombinace zanesené ve slovníku daného jazyka. Útoku slovníkovou metodou lze zabránit heslem sestaveného z náhodných kombinací. [22]

Vedle běžného hesla lze počítač ochránit také BIOS heslem. Takové heslo lze ale velmi snadno resetovat pouhým odpojením baterie. Proto je velmi důležité také dbát na fyzické zabezpečení počítače.

U většiny sociálních sítí, e-mailů a některých dalších služeb a programů lze využít dvoufázové ověření. Pokud má uživatel dvoufázové ověřování zapnuto, je při přihlašování vyžadován vedle hesla i speciální kód. Ověřovací kód se vždy generuje nový, proto je složitější jej prolomit. Je ale nutné mít účty propojené s telefonem nebo e-mailem, aby bylo možné kód uživateli zaslat.

Hash funkce

Pro zvýšení bezpečnosti uložených hesel se využívají hash funkce. Hash funkce umožňují jednosměrné převedení libovolně dlouhého textu na tzv. hash neboli otisk. Výhodou hashování je, že z otisku nelze zpětně odvodit původní zprávu. Z toho důvodu se hash funkce využívají při ukládání hesel do systému. Při zadání hesla se spočítá jeho otisk a ten se následně uloží do systému. Při zpětném zadávání hesla se opět spočítá jeho otisk a ten se porovnává s původním otiskem. Při chybném zadání hesla otisky nebudou souhlasit a uživatel nebude přihlášen. Hash funkce se dále využívají například při digitálních podpisech (více v následující hodině. [22], [23]

6.5 5. hodina

Téma hodiny: Bezpečná komunikace – ochrana proti škodlivým programům a nevyžádané poště

Nově osvojené pojmy: malware, logické bomby, spyware, hoax, digitální podpis, elektronický podpis

Cíle hodiny:

Kognitivní:	Žák dokáže vyjmenovat a popsat škodlivé programy. Žák bude umět vysvětlit pojem spam, hoax a digitální podpis.
Psychomotorický:	Žák dokáže zkontrolovat stav svého počítače pomocí programu Windows Defender.
Afektivní:	Žák pochopí důležitost antivirových programů při ochraně proti škodlivým programům.

Přílohy: prezentace a pracovní list *Hodina5*

6.5.1 Bezpečná komunikace

S rozmachem sociálních sítí je nutné klást čím dál větší důraz na dodržování základních pravidel bezpečné komunikace. Prvním pravidlem nejen při komunikaci, ale při využívání internetu obecně, je práce, pokud možno na stránkách, které využívají zabezpečené verze protokolu http. Lze je poznat podle označení https. Takové stránky mají vyšší úroveň zabezpečení. Proto je vhodné takové stránky využívat vedle komunikace také k přihlašování do různých účtů. Pokud se přihlašujete na cizí počítače, nezapomeňte se vždy odhlásit!

6.5.2 Ochrana proti škodlivým programům

V první řadě je nutné vysvětlit před čím se vůbec máme chránit. Jako malware označujeme jakékoliv škodlivé programy, pomocí kterých hackeři infikují počítače či mobilní zařízení. [4]Z takto infikovaných zařízení lze následně získat například citlivé údaje, hesla, důležitá data či jednoduše zablokovat přístup do zařízení. Mezi malware patří:

- viry – škodlivý program, který se dokáže sám šířit bez vědomí uživatele připojením sebe sama na jiný program nebo soubor.
- počítačoví červi – škodlivý program, který se také dokáže sám šířit. Na rozdíl od viru ale nepotřebuje hostitele.
- logické bomby – jsou záměrně naprogramované chyby, které se spustí po splnění předem dané podmínky (např.: uplynutí daného času).

[4] Aktuální hrozby lze nalézt na adrese: http://www.virovyradar.cz/

- trojští koně – jedná se o skryté dodatečné funkce běžných programů. Příkladem trojského koně jsou tzv. zadní vrátka, které umožňují přístup útočníka do systému.
- spyware – počítačový program, který bez vědomí uživatele odesílá data z počítače pomocí internetu. Pomocí spyware lze získat informace pro cílovou reklamu, ale i přístupové údaje. [23], [25]

Malware se velmi často šíří přes sociální sítě, přílohy v e-mailu, napadených webových stránek, bezplatných služeb a nejrůznějších stažených dat.

Jak se bránit před malware?

1. Používejte antivirové a antimalwarové programy.
2. Antivirový program pravidelně aktualizujte.
3. Neotvírejte e-mailové přílohy od neznámých odesílatelů (zejména s přílohou *.exe)
4. Dávejte si pozor na dvojité a skryté formáty příloh (např.: foto.jpeg.exe).
5. Nechoďte na webové stránky, na které odkazuje neznámý email

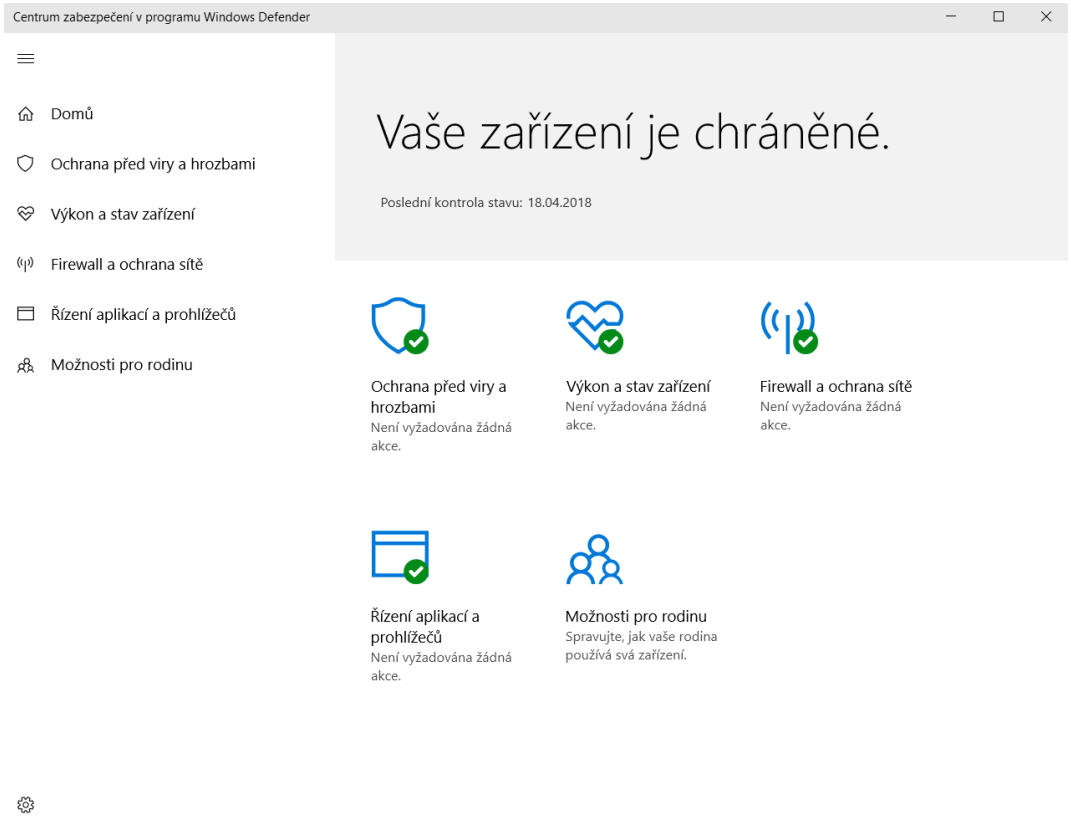
Důležitým krokem při ochraně před škodlivými programy je rozpoznat, zda počítač již není infikovaný. Napadený počítač může zobrazovat větší množství reklam, vykazovat chyby operačního systému, dlouho načítat internet nebo se dlouho zapínat, mohou přibývat a mizet soubory a ikony, nebo být zašifrované, může docházet k odesílání zpráv bez vědomí uživatele či dojít k celkovému zpomalení počítače. Pokud počítač vykazuje podobné znaky, je dobré provést kontrolu pomocí antivirového programu.

Antivirové programy

Antivirový program by měl být součástí každého počítače a slouží zejména jako prevence. Tyto programy fungují na principu porovnávání souborů na disku počítače se svou databází známých virů a škodlivých souborů. Proto je velmi důležité mít antivirový program vždy aktualizovaný.

Nabídka antivirů je v dnešní době velmi bohatá. Samotný Microsoft se snaží bránit uživatele svých operačních systémů (Windows 8 – Windows 10) pomocí integrovaného programu Windows Defender. K dispozici jsou jak placené verze, tak verze zdarma. Verze zdarma nabízí například Avast, AVG nebo Avira. Nevýhodou neplacených programů jsou omezené funkce. Takové verze většinou nemají vlastní firewall, ochranu před spamem a neblokují

phishing. V nabídce jsou také online scannery, které umožňují kontrolu počítače bez nutnosti instalace nebo registrace.[5] [25]



Obrázek 21: Náhled prostředí programu Windows Defender

6.5.3 Ochrana proti nevyžádané poště

Nevyžádanou poštu označujeme jako spam. Spamy jsou obvykle šířeny masově. Nejčastěji obsahují reklamní sdělení, ale mohou také s sebou nést škodlivé programy, phishingové či pharmingové e-maily či hoaxy.[6]

Jako hoax lze označit falešnou poplašnou zprávu, která velmi často vyzývá k dalšímu rozesílání. Mezi nejčastější hoaxy patří varování před nejrůznějšími počítačovými viry, falešné prosby o pomoc a řetězové dopisy. Hoaxy nemusí být vždy přímo škodlivé pro uživatele. Velmi často pouze obtěžují příjemce a zbytečně zatěžují servery. Nesou s sebou ale i jistá

[5] Firma ESET nabízí online scanner dostupný na adrese: https://www.eset.com/cz/online-scanner/
[6] Více o hoaxech a ukázky, jak mohou vypadat lze nalézt na adrese: http://www.hoax.cz/cze/

rizika vyzrazení důvěrných informací (zejména e-mailové adresy). Hoaxy také velmi často vyzývají k zadání dalších citlivých údajů jako je adresa, rodné číslo, číslo účtu a podobně. [25]

Jak se chránit?

Uživatel se může proti spamu chránit do určité míry také sám. Důležité je nezadávat e-mailovou adresu na podezřelé internetové stránky či formuláře. Takové formuláře mohou být vytvořeny právě za účelem sbírání e-mailových adres a rozesílání spamů. Vedle vhodného chování uživatele je také nutné používat firewall a antivir. Tyto programy mohou počítač ochránit před škodlivým programem, který by mohl rozesílat spamy do jiných zařízení. Zejména antivir je důležité používat od prvního spuštění počítače a pravidelně jej aktualizovat, popřípadě nastavit automatické aktualizace.

V neposlední řadě je třeba využívat antispamové filtry. Spamy lze filtrovat jak přímo ve schránce, tak při stahování e-mailů uživatelem do počítače. Existuje několik metod rozpoznávání, zda se jedná o spam nebo ne. Prvním způsobem je filtrace podle obsahu dopisu, kdy filtry vyhledávají určité rysy typické pro spamy. Další možností jsou DCC filtry. Ty využívají databáze spamů, které jsou sestavována na základě zkušeností jiných uživatelů.

6.5.4 Digitální podpis

Poslat podvodný e-mail může v dnešní době téměř každý kdo má počítač s přístupem k internetu. Proto je velmi nutné vědět, jak si lze ověřit, zda e-mail opravdu poslal vlastník e-mailové adresy. K tomu slouží digitální podpis.

Digitální podpis umožňuje jednoznačnou identifikaci odesílatele. Skládá se z elektronického podpisu a certifikátu. Elektronický podpis je dodatečná informace, která se připojuje k datům a pomocí níž lze odesílatele identifikovat. Takto lze podepsat téměř cokoliv. Certifikát pak zajišťuje identitu konkrétní osoby. Vedle osobních certifikátů zajišťující ověření totožnosti jednotlivých osob existují i certifikáty serverové. [22]

6.6 6. hodina

Téma hodiny: Zabezpečení bezdrátových sítí

Nově osvojené pojmy: kryptologie, kryptografie, šifrování, kryptoanalýza, steganografie, frekvenční analýza

Cíle hodiny:

Kognitivní:	Žák dokáže vyjmenovat možnosti zabezpečení bezdrátových sítí. Žák bude umět vysvětlit pojem kryptologie, kryptografie a kryptoanalýza.
Psychomotorický:	Žák bude umět zašifrovat data pomocí posouvání písmen v abecedě.
Afektivní:	Žák pochopí důležitost zabezpečení bezdrátových sítí.

Přílohy: prezentace a pracovní list *Hodina6*

6.6.1 Zabezpečení bezdrátové sítě

Používání Wi-Fi s sebou nese hned několik nevýhod. Wi-Fi sítě často pokrývají mnohem větší oblast, než je potřeba. Příkladem je spousta sítí, které nabízí nejrůznější restaurace a podniky, kdy se na jejich Wi-Fi lze připojit mnohdy i několik desítek metrů od budovy, ve které sídlí. Případní útočníci tak mohou sítě napadnout z mnohem větší vzdálenosti. Tím samozřejmě vyvstane riziko úniku citlivých informací, modifikace přenášených dat či odposlouchávání. Nevýhodou Wi-Fi sítě je také vysoká pravděpodobnost neoprávněného či nechtěného připojení cizí osoby.

Útoky na sít mohou být aktivní i pasivní. Mezi pasivní útoky patří zejména odposlouchávání dat ze sítě a monitorování provozu sítě. Odhalení takových útoků je většinou velmi obtížné, jelikož nedochází ke změně dat. Nejúčinnější ochranou proti pasivním útokům je šifrování.

Modifikace dat či vytváření falešných dat patří mezi aktivní útoky. V takovém případě se útočník může vydávat za někoho jiného nebo zabraňovat používání služby pomocí rušení zpráv a záměrnému snižování výkonnosti některé síťové služby. Aktivním útokům lze hůře zabránit než pasivním, ale lze je mnohem snadněji odhalit. [24]

Je proto velmi důležité dodržovat několik základních pravidel, které mohou zvýšit bezpečnost používané Wi-Fi sítě. Prvním krokem je využívání již zmíněného šifrování dat i komunikačního kanálu.

Vždy by měl uživatel využívat připojení, které má nějakou formu zabezpečení. Nejjednodušší varianta zabezpečení je WEP. Výhodou WEP (Wired Equivalent Privacy) zabezpečení je, že je zdarma. Nevýhodou je, že byl v roce 2000 prolomen. Nástupcem WEP zabezpečení je WPA (Wi-Fi Protected Access), později pak WPA2. [25]

Samozřejmostí je mít přístup do sítě zabezpečený heslem, jiným než implicitním. Tato hesla jsou pro každého hackera velmi snadno zjistitelná. Proto je velmi důležité změnit hesla nastavená od výrobců na vlastní a bezpečnější heslo. Taktéž je vhodné pozměnit název Wi-Fi sítě. Omezení dosahu Wi-Fi lze vhodným umístěním antény. Ideální je najít místo někde uprostřed bytu či domu. Nevhodné je ji naopak umístit ke stěnám či oknu.

V neposlední řadě je opět nutné mít nainstalované a aktualizované bezpečnostní software jako jsou antivirové programy a firewally.

6.6.2 Kryptologie

Kryptologie jako věda tvoří nepostradatelnou část ochrany dat. Kryptologie je věda o šifrách, která se skládá z kryptografie – šifrování a kryptoanalýzy – luštění šifer. V dnešní době, kdy se komunikace přesunula do sféry internetu je šifrování přenášených dat čím dál více důležitá. První dochované známky o utajování nebo šifrování komunikace jsou staré více než 3000 let. V průběhu historie existuje celá řada významných momentů, kdy kryptologie hrála velkou roli. Ať už se jedná o střet sparťanských a perských lodí v roce 480 př.n.l., odsouzení skotské královny Marie Stuartovny k smrti v roce 1586 či průběh První i Druhé světové války.[7] [26]

Jak už bylo řečeno, kryptologie se skládá z kryptografie a kryptoanalýzy. Cílem kryptografie je vymyslet systém, pomocí kterého lze rychle zašifrovat zprávy či data a zvýšit tak jejich bezpečnost. Pokud si dva lidé posílají mezi sebou zašifrované zprávy, třetí osoba o komunikaci obvykle ví, ale nemůže ji rozluštit. K rozluštění zašifrované zprávy je totiž třeba mít klíč nebo více klíčů. V tom se liší kryptografie od steganografie. Cílem steganografie je utajení zpráv tak, aby třetí strana ani nepoznala, že nějaká komunikace probíhá. Množství klíčů je dáno v závislosti na tom, zda se jedná o šifrování symetrické nebo asymetrické. Symetrické šifrování je rychlejší, méně náročné na výpočty, ale také méně bezpečné. Symetrické šifrování využívá pouze jeden klíč, který je nutný sdílet mezi účastníky komunikace. Tento problém je vyřešen v asymetrickém šifrování, kdy je pro šifrování využíván veřejný klíč a pro dešifrování klíč soukromý.[8] [27]

[7] Kryptologie byla motivem několika známých filmů, příkladem je film Kód Enigmy (2014) z Druhé světové války.
[8] Více o konkrétních šifrách a jejich principu lze vyčíst v knize Šifry a hry s nimi ISBN 978-80-7367-196-9.

Cílem kryptoanalýzy je rozluštění zpráv bez znalosti těchto klíčů. Velký význam v historii kryptoanalýzy hrála tzv. frekvenční analýza. Luštění zpráv na základě frekvenční analýzy je založeno na četnosti výskytu jednotlivých znaků v dané abecedě. Pokud byl text zašifrován jednoduššími šiframi založenými na principu posouvání znaků v abecedě, šlo ji pomocí frekvenční analýzy snadno rozluštit. [27]

Příklad šifrování pomocí posunu v abecedě o 3 místa doprava:

A -> D

B -> E

C -> F

INFORMATIKA -> LQIRUPDWLND

V dnešní době je vývoj kryptologie značně ovlivněn rozvojem počítačů. Díky moderní technologie lze velké operace nutné k šifrování i dešifrování provádět mnohem rychleji, snadněji a bez chyb. To samozřejmě nese vyšší riziko v prolomování šifer a snížení bezpečnosti jejich používání.

6.7 7. hodina

Téma hodiny: Ochrana osobních údajů a autorská práva

Nově osvojené pojmy: ISO 690, GDPR

Cíle hodiny:

Kognitivní:	Žák bude znát základní pojmy spojené s autorským zákonem. Žák bude umět vyjmenovat povinné prvky citací. Žák se bude orientovat v základech nařízení GDPR.
Psychomotorický:	Žák bude umět vytvořit citaci dle normy ISO 690.
Afektivní:	Žák pochopí význam autorského zákona a citování zdrojů při zpracovávání dat. Žák bude znát svá práva na ochranu osobních dat.

Přílohy: prezentace a pracovní list *Hodina7*

6.7.1 Autorská práva

Autorská práva jsou upravována zákonem č. 121/2000 Sb. o právu autorském, o právech souvisejících s právem autorským a o změně některých zákonů (autorským zákonem).

Autorská práva má každý autor ke svým dílům. Autorská díla na rozdíl od patentů nevyžadují žádnou registraci. [29]

Autorský zákon stanovuje, že nikdo nesmí užívat díla bez souhlasu držitele autorský práv, není-li zákonem stanovena výjimka. To znamená že nesmí dílo rozmnožovat, rozšiřovat, pronajímat, půjčovat, vystavovat nebo je sdělovat veřejnosti. Autorským dílem je dílo literární a jiné dílo umělecké a dílo vědecké. Za dílo se také považuje počítačový program a fotografie. Mezi autorská díle naopak nespadají například úřední díla jako jsou veřejné listiny a rejstříky, obecní kroniky, státní symbol či výtvor tradiční lidové kultury. [28], [29]

Autorská práva se dělí na osobnostní a majetková. Osobnostní práva zahrnují zejména právo osobovat si autorství, rozhodovat o zveřejnění díla a právo udělit souhlas ke změně nebo jinému zásahu do díla. Majetková práva pak zahrnují zejména právo dílo užívat a udělit souhlas k užití rozmnožovat, rozšiřovat, pronajímat, půjčovat a vystavovat. [28], [29]

Citace

Citováním použité literatury se vyhnete podezření z plagiátorství. [9] Pokud chce někdo převzít něčí text, část textu, obrázek, tabulku či graf je vždy nutné uvést autora. To samé platí, pokud je převzata samotná myšlenka, nápad nebo názor. Vedle chránění sama sebe lze pomocí citací snadněji vyhledat použitý zdroj a ověřit si tak pravdivost textu. Povinnost citovat použitou literaturu a odborné texty uvádí autorský zákon. Výjimku tvoří všeobecně známá fakta, ty se citovat nemusí. [29]

Mezi nejčastější způsoby citace patří citování dle normy ISO 690. Tato norma neuvádí přímo návod, jak citovat, ale spíše povinné prvky citace a jejich pořadí. Proto je-li zvolen nějaký styl citace nebo nástroj pro jejich tvorbu, je vhodné, aby se v průběhu již neměnil a všechny citace tak působili jednolitě. [30]

Veškeré použité zdroje mohou být vypsány v seznamu na konci práce. V takovém případě se na konec odstavce, pro který byla použita cizí práce, uvede do závorky odpovídající číslo ze seznamu. Pokud práce obsahuje pouze pár cizích zdrojů je možné citaci k nim uvést v poznámkách pod čarou. V neposlední řadě je možné citovat tzv. Harvardskou metodou. V tomto případě se do závorek za odstavec udává vždy autor a rok vydání. [30]

[9] Pro usnadnění vytváření citací dle normy ČSN ISO 690 existuje webová stránka: https://www.citace.com/

Mezi nejčastější prvky citace patří ISBN (v případě knihy), autor, název a podnázev, vydání, místo vydání, nakladatelství a rok vydání. V případě online zdrojů je v citaci také uveden název webu, URL adresa, typ nosiče a datum citování.

- Autor se uvádí v pořadí `Příjmení, Jméno.`
- Pokud je název příliš dlouhý, lze ho zkrátit vynecháním několika slov a přidáním tři teček (nelze vynechávat počáteční slova).
- Vydání se udává, pokud se jedná o jiné než první.
- Data vydání se uvádějí pouze v číslech, pouze v případě copyrightu se datum doplňuje o jeho zkratku `c2018`.
- Typ nosiče se udává u jiných než tištěných dokumentů, např. `[online], [DVD], [disk]…` [30]

Příklad citování knihy:

`Tvůrce. Název publikace: Podnázev. Vydání. Místo: nakladatel, rok. Počet stran. Edice. ISBN.`

Příklad citování webu:

`Tvůrce. Název webu: Podnázev [typ nosiče]. Místo: Nakladatelství, Rok vydání [Datum citování]. Dostupné z: URL adresa.`

6.7.2 GDPR

Obecné nařízení o ochraně osobních údajů (General Data Protection Regulation – GDPR) je nová legislativa Evropské Unie, která má zvýšit ochranu osobních dat občanů. Schválení nařízení proběhlo již v roce 2016, přičemž v platnost vstoupilo 25. května 2018. Cílem tohoto nařízení je zejména chránit a hájit práva občanů EU proti neoprávněnému zacházení s jejich daty a osobními údaji. V případě porušení nařízení hrozí vysoké pokuty. V České republice nařízení nahrazuje právní úpravu ochrany osobních údajů v podobě směrnice 95/46/ES a související zákon č. 101/2000 Sb. o ochraně osobních údajů. [31], [32]

GDPR se týká všech institucí, firem, online služeb a jednotlivců, kteří zpracovávají osobní údaje občanů EU. Ať už se jedná o údaje o zaměstnancích, zákaznících, klientů či dodavatelů. Oblast ochrany osobních údajů bude i nadále regulovat Úřad pro ochranu osobních údajů (ÚOOÚ), který bude částečně podřízen Evropskému sboru pro ochranu osobních

údajů (EDPB). Na Evropský sbor se mohou obrátit v případě pochybnosti o rozhodnutí Českého úřadu. [31], [32]

Nová nařízení o ochraně osobních údajů mají řešit nesrovnalosti předchozích legislativ. Původní legislativy vznikly v roce 1995, kdy nebyly tak rozšířeny technologie, neexistovaly sociální sítě a cloudová uložiště. [31], [32]

Mezi osobní údaje se řadí veškeré informace vztahující se k identifikaci fyzické osoby. Mezi obecné osobní údaje patří jméno, pohlaví, věk, datum narození, osobní stav, IP adresu, fotografické záznamy, organizační údaje, e-mailová adresa a telefonní číslo. Speciální kategorii tvoří osobní údaje o rasové či etnické příslušnosti, politické názory, náboženství, členství v oborech, zdravotní stav, sexuální orientace a záznamy o trestních deliktech. Mezi citlivé údaje pak nařízení zahrnuje genetické a biometrické údaje a osobní údaje dětí. Z působnosti GDPR jsou pak vyloučeny údaje o zemřelých osobách a údaje získané pouze pro osobní potřebu, které nemají obchodní charakter. [31], [32]

GDPR výrazně posiluje práva občanů. Občané mají zejména práva na přístup, opravu, výmaz, právo být zapomenut, právo na omezení zpracování, přenositelnost údajů a právo vznést námitku. Instituce a firmy mají naopak povinnost jmenovat pověřenou osobu zodpovědnou za ochranu osobních údajů, vést záznamy o činnostech zpracování a nově také vypracovávat posouzení vlivu na ochranu osobních údajů (DPIA) [31], [32]

Sankce v případě porušení nařízení mohou dosahovat až 20 000 000 EUR nebo 4 % celkového ročního obratu společnosti. Výše této sankce závisí například na závažnosti porušení, délce porušování, počtu poškozených občanů nebo míře škody. [31], [32]

7 DOTAZNÍKOVÉ ŠETŘENÍ PRO ANAÝZU SADY ÚLOH

Poslední část diplomové práce je zaměřena na analýzu vytvořených materiálů, která slouží zejména pro jejich ověření a v neposlední řadě také sebereflexi autora. Dotazníkové šetření probíhalo na soukromé střední škole ve Zlínském kraji, která nabízí jak obory s výučním listem, tak maturitní obory, a to včetně oboru zaměřeného na informační technologie. Dotazník byl rozdán pouze žákům maturitních oborů. Počet hodin vymezených pro předmět informační a komunikační technologie se liší v závislosti na konkrétním oboru studia. Obory s předmětem Informační a komunikační technologie mají na předmět vymezených 7 hodin (1-2-2-2) a obory s předmětem Informatika a výpočetní technika 12 hodin (2-4-4-2).

Pro tvorbu druhého dotazníku byl opět využit nástroj pro vytváření formulářů na Google Disk. Dotazník se skládal ze 12 otázek rozdělených do dvou sekcí. První sekce obsahovala otázky zaměřené na průzkum dosavadních znalostí respondentů v oblasti údržby a ochrany dat a počítačové bezpečnosti (otázka č. 1–6). Druhá část je pak věnována otázkám vztahujícím se k výukovým materiálům a jejich hodnocení (otázka č. 7–12). Většina otázek je uzavřená s omezeným výběrem odpovědí. Pouze dvě otázky jsou otevřené.

Dotazník byl žákům rozdán učiteli ICT. Aktuálně probírané učivo se bohužel neslučovalo se zpracovaným učivem v diplomové práci. Nebylo proto možné odučit všechny vytvořené hodiny přímo v praxi. Materiály byl žákům předány pomocí cloudového uložiště Google Disk společně s odkazem na dotazník. Všem třídám byl vždy poskytnut dostatečný čas na seznámení se s dostupnými materiály i na následné vyplnění dotazníku.

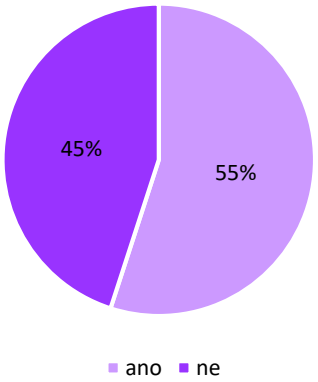
7.1 Získané informace

Dotazníky byly rozdány 40 žákům různých tříd maturitních oborů. Výhodou osobního kontaktu s konkrétními vyučujícími byla stoprocentní návratnost. Znalosti žáků mají v určitých oblastech pár mezer a dle zjištěných informací by žáci uvítali rozšíření svých znalostí v oblasti bezpečnosti.

7.1.1 Myslíte si, že vaše znalosti o počítačové bezpečnosti jsou dostatečné?

První otázka byla uzavřená. Jejím účelem bylo sebehodnocení znalostí respondentů v oblasti počítačové bezpečnosti. Více jak polovina respondentů považuje své znalosti za dostatečné, konkrétně 55 % žáků střední školy (22 respondentů). Z následujících otázek lze ale usoudit,

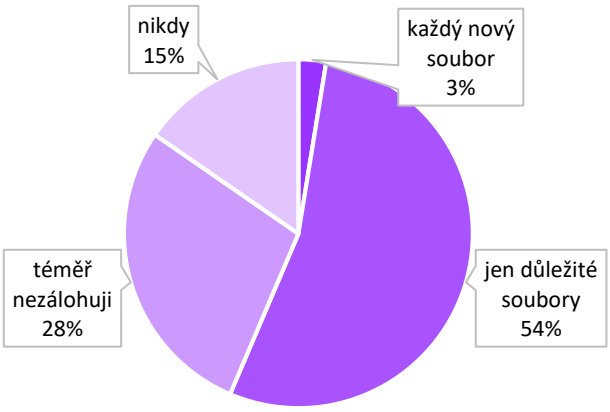
že žáci mají i nějaké mezery. Zbylých 45 % (18 respondentů) by uvítalo rozšíření svých znalostí.



Graf 7: Sebehodnocení znalostí žáků SŠ v oblasti počítačové bezpečnosti

7.1.2 Jak často zálohujete?

Druhá uzavřená otázka se zaměřuje na frekvenci zálohování dat. Z šetření vyplynulo, že více než polovina žáků střední školy (21 respondentů) zálohuje všechny důležité soubory. Bohužel pouze 3 % žáků (1 respondent) vybrané školy zálohuje každý nový vytvořený soubor. Alarmující fakt je taky ten, že 43 % žáků (17 respondentů) téměř nezálohuj nebo dokonce nikdy nezálohuje své data a riskují tak jejich úplnou ztrátu v případě poškození či odcizení počítače.

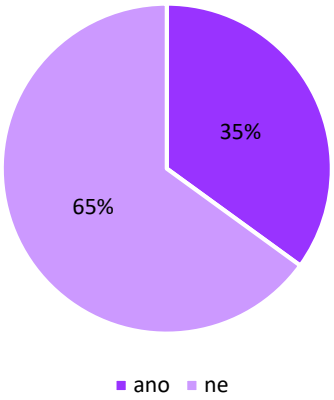


Graf 8: Frekvence zálohování osobních dat žáků SŠ

7.1.3 Říká vám něco pojem SOCIÁLNÍ INŽENÝRSTVÍ?

Třetí uzavřená otázka se týkala sociálního inženýrství. Více jak polovina žáků (26 respondentů) neznají výraz sociální inženýrství a představují tak pro útočníky snazší oběti. Sociální

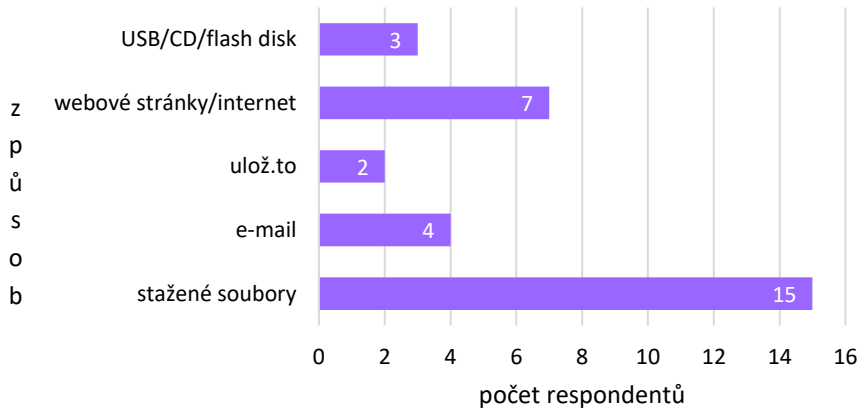
inženýrství představuje nejjednodušší a velmi efektivní způsob získávání citlivých údajů, proto je rozhodně nutné toto téma zařadit do výuky nejen na středních školách.



Graf 9: Znalosti žáků SŠ o metodách získávání citlivých údajů

7.1.4 Víte, jakými způsoby se může do vašeho počítače dostat škodlivý program (vir, počítačový červ apod.)?

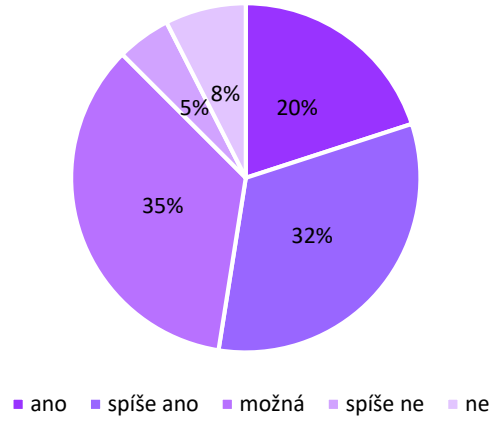
Jediná otevřená otázka se týkala rizika nakažení počítače škodlivým programem. Žáci mají relativně dobré znalosti o způsobu šíření malware. Jelikož se jednalo o otevřenou otázku, žáci odpovídali velmi různorodě. Jako nejčastější způsob žáci označili stahování nejrůznějších souborů a programů – 15 respondentů, přičemž 4 žáci uvedli konkrétně stránku ulož.to. Mezi další způsoby zařadili webové stránky a internet obecně (7 respondentů), přílohy e-mailu (4 respondenti) a extérní paměťová média jako je USB, CD nebo flash disk (3 respondenti). Někteří žáci odpovídali pouze obecně a neuváděli konkrétní způsoby.



Graf 10: Způsoby nakažení počítače škodlivým programem dle žáků SŠ

7.1.5 Dokázali byste rozeznat falešný e-mail nebo internetovou stránku?

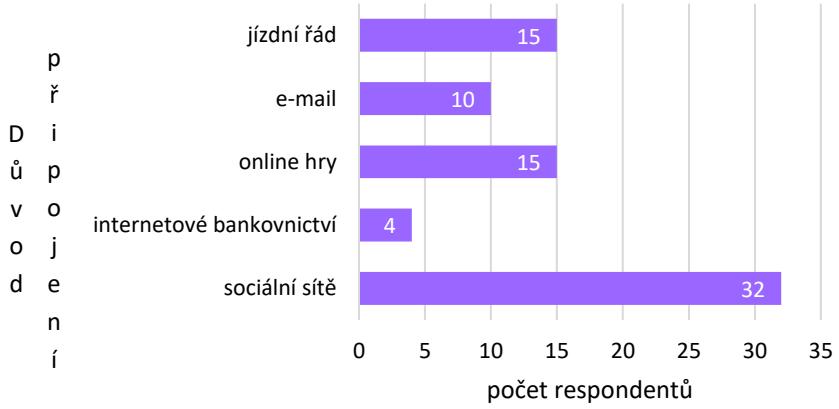
Pátá otázka se zaměřovala na znalosti žáků v oblasti phishingu, pharmingu a podvodných stránek obecně. Více jak polovina žáků (21 respondentů) si myslí, že by s největší pravděpodobností podvodné stránky a e-maily rozpoznala. 35 % žáků (14 respondentů) si nebylo příliš jistých a 13 % žáků (5 respondentů) by nejspíš podvod neodhalilo.



Graf 11: Schopnost žáků rozeznat falešný e-mail nebo internetovou stránku

7.1.6 Na veřejných Wi-Fi sítích se připojujete na:

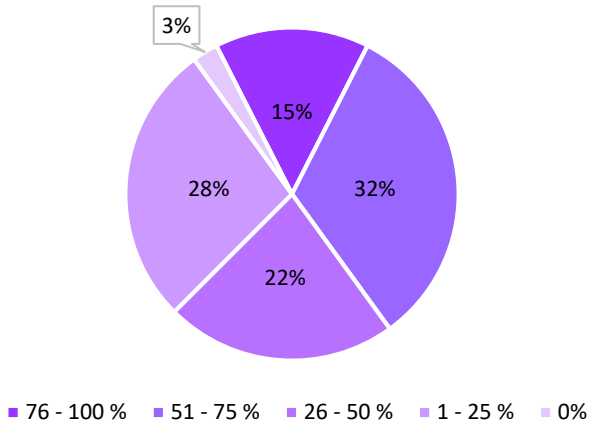
Poslední otázka první sekce byla zaměřena na důvody připojování žáků na veřejné Wi-Fi sítě. Nejvíce respondentů uvedlo jako důvod přístup na sociální sítě a tím riskují odposlouchávání konverzace nebo odcizení přístupových údajů. Stejnému riziku se vystavují také při přihlašování na e-mail. Mezi méně rizikové důvody pak patřilo hraní online her a vyhledávání na jízdním řádu. Alarmující je fakt, že 4 respondenti uvedli jako důvod připojení na veřejnou sít přístup do internetového bankovnictví.



Graf 12: Důvod připojování žáků na veřejné Wi-Fi sítě

7.1.7 Odhadem kolik procent informací v prezentacích bylo pro vás zcela nových?

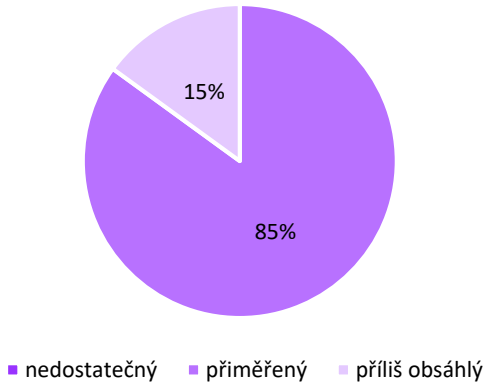
Sedmou otázkou se žáci při vyplňování přesunuli do druhé sekce určené pro samotné hodnocení materiálů. Z první otázky vyplynulo, že více jak polovina informací v materiálech byla většinu žáků (28 respondentů) zcela nových. Pro 28 % (11 respondentů) žáků bylo nových až 25 % informací a pouze 3 žáků (1 respondent) nenašlo v materiálech žádné nové informace.



Graf 13: Množství nových informací pro žáky ve vytvořených materiálech (v %)

7.1.8 Obsah materiálů vám přišel?

Jedním z kritérií hodnocení materiálu byl obsah. 85 % dotazovaných (34 respondentů) označilo obsah za přiměřený a pouze 15 % (6 respondentů) jej označilo za příliš dlouhý.



Graf 14: Hodnocení obsahu materiálů žáky SŠ

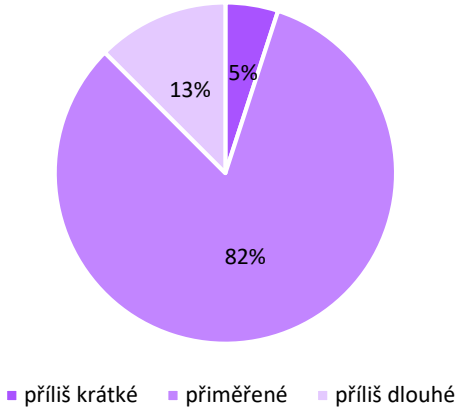
7.1.9 Chybělo vám v materiálech nějaké téma?

Jediná otevřená otázka druhého bloku byla nepovinná a sloužila pro konkrétní námitky k obsahu prezentací. Většina žáků využila možnosti neodpovídat a 13 respondentů uvedlo, že

žádné konkrétní téma v materiále nepostrádají. Jediné navrhnuté téma byly počítačové hry, které ale nespadají do okruhu ochrana a údržba dat.

7.1.10 Přiložené prezentace vám přišly:

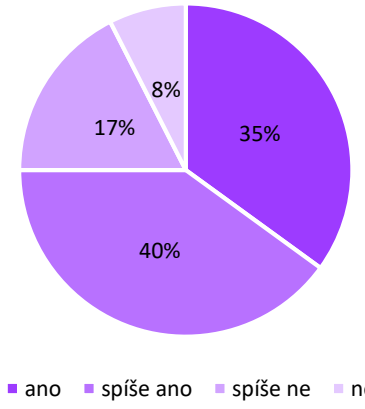
Další kritérium hodnocení byla délka prezentací. 82 % žáků (33 respondentů) označilo délku prezentací za přiměřené. Pouze pro 5 % (2 respondenti) žáků byly prezentace příliš krátké a pro 13 % (5 respondentů) dotazovaných naopak příliš dlouhé.



Graf 15: Hodnocení délky prezentací žáky SŠ

7.1.11 Připadaly vám přiložené materiály srozumitelné?

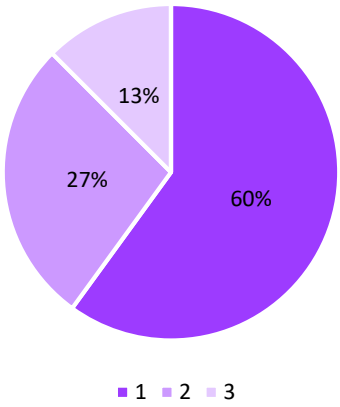
V neposlední řadě žáci mohli hodnotit srozumitelnost materiálů a obsahu. Celých 75 % (30 respondentů) dotazovaných označilo materiály za srozumitelné. Pouze 25 % (10 respondentů) uvedlo, že jsou pro ně informace nesrozumitelné. Hlavním důvodem může být fakt, že prezentace obsahovaly pro žáky nové informace.



Graf 16: Hodnocení obsahu materiálů žáky SŠ z hlediska srozumitelnosti

7.1.12 Vizuální stránka prezentací byla:

Cílem poslední otázky bylo zhodnotit celkovou vizuální stránku prezentací. Respondentům byla nabídnuta škála známek od 1 do 5. Převážná část dotazovaných hodnotila prezentace kladně a pouze 13 % žáků (5 respondentů) je označilo za průměrné.



Graf 17: Hodnocení vzhledu prezentací žáky SŠ na škále 1-5

ZÁVĚR

Cílem diplomové práce bylo vytvořit materiály pro výuku ochrany a údržby dat na středních školách. Vytvořené materiály jsou stavěny tak, aby prohloubily znalosti žáků středních škol zejména v oblasti počítačové bezpečnosti a upozornily na rizika, se kterými se mohou při práci na počítači setkat.

Diplomová práce je rozdělena na část teoretickou a praktickou. Teoretická část v úvodu popisuje rámcové vzdělávací programy pro střední odborné vzdělávání a gymnázia, zejména část zaměřenou na výuku informačních a komunikačních technologií. Dále obsahuje výčet a popis programů, které jsou využívány na středních školách pro správu souborů a disků. Konkrétně se jedná o nástroje vestavěné v operačních systémech Windows a Total Commander. Závěr teoretické části je věnován cloudovým službám a nejpoužívanějším cloudovým uložištím.

Praktická část se skládá z analýzy dotazníku, který sloužil pro získání povědomí o aktuálním obsahu vyučovacích hodin zaměřených na ochranu a údržbu dat a počtu hodin věnovaných této problematice. Na základě získaných informací z RVP a dotazníků bylo v další sekci praktické části vytvořeno sedm vyučovacích hodin, které se skládali z teoretických podkladů, cílů hodiny a seznamu nově osvojených pojmů. Součástí diplomové práce je také sedm prezentací shrnující danou problematiku (*Hodina1.pptx – Hodina7.pptx*) a pracovní listy (*PracovníListy.pdf*) vytvořené ke každé hodině, pomocí kterých lze ověřit nově získané znalosti žáků a zda byly naplněny cíle hodiny. Příloha s pracovními listy obsahuje také návrhy řešení těchto listů.

Závěr práce je věnován analýze materiálů a znalostí žáků středních škol. I když více jak polovina žáků považuje své znalosti za dostatečné, bylo pro většinu nejméně 50 % informací v materiálech zcela nových. Z toho lze soudit, že výuce ochrany a údržby dat na středních školách by měla být věnována mnohem větší pozornost. Nově vytvořené materiály žáci považují z velké části za přiměřeně dlouhý a srozumitelný a celkový vzhled prezentací hodnotí známkou 1 nebo 2.

SEZNAM POUŽITÉ LITERATURY

[1] Rámcové vzdělávací programy. Národní ústav pro vzdělávání [online]. Praha: NÚV, c2011-2018 [cit. 2018-03-07]. Dostupné z: http://www.nuv.cz/t/rvp

[2] Zákon č. 561/2004 Sb.: Zákon o předškolním, základním, středním, vyšším odborném a jiném vzdělávání (školský zákon). Zákony pro lidi [online]. Zlín: AION CS, c2010-2018 [cit. 2018-03-07]. Dostupné z: https://www.zakonyprolidi.cz/cs/2004-561

[3] Vymezení Rámcového vzdělávacího programu pro základní vzdělávání v systému kurikulárních dokumentů. Metodický portál: inspirace a zkušenosti učitelů [online]. 2015 [cit. 2018-03-07]. Dostupné z: https://digifolio.rvp.cz/view/view.php?id=10429

[4] BALADA, Jan. Rámcový vzdělávací program pro gymnázia: RVP G. Praha: Výzkumný ústav pedagogický v Praze, c2007. ISBN 978-80-87000-11-3.

[5] Rámcový vzdělávací program pro obor vzdělávání Informační technologie. Praha: Národní ústav odborného vzdělávání, 2008, 85 s.

[6] Národní ústav pro vzdělávání: RVP pro střední odborné vzdělávání. Národní ústav pro vzdělávání [online]. Praha, 2016 [cit. 2016-03-02]. Dostupné z: http://www.nuv.cz/t/rvp-os

[7] Microsoft: Nápověda pro Windows 10 [online]. Washington: Microsoft, c2018 [cit. 2018-04-19]. Dostupné z: https://support.microsoft.com/cs-cz/products/windows?os=windows-10

[8] Seznamte se s Finderem na Macu. Apple [online]. California: Apple, c2018 [cit. 2018-04-19]. Dostupné z: https://support.apple.com/cs-cz/HT201732

[9] Total Commander [online]. Switzerland: Ghisler Software, 2018 [cit. 2018-03-07]. Dostupné z: http://www.ghisler.com/

[10] Historie programu Total Commander. Total-commander [online]. c2009-2018 [cit. 2018-03-07]. Dostupné z: http://total-commander.eu/historie-programu-total-commander

[11] RYLICH, Jan. Cloudové služby: data i počítače v oblacích. Ikaros [online]. 2012, ročník 16, číslo 9 [cit. 2018-03-07]. urn:nbn:cz:ik-13965. ISSN 1212-5075. Dostupné z: http://ikaros.cz/node/13965

[12] Co je cloud computing?. Microsoft Azure [online]. Microsoft, c2018 [cit. 2018-03-07]. Dostupné z: https://azure.microsoft.com/cs-cz/overview/what-is-cloud-computing/

[13] Cloud. Management Mania [online]. Wilmington, 2017 [cit. 2018-03-07]. Dostupné z: https://managementmania.com/cs/cloud-computing

[14] Box [online]. California, c2018 [cit. 2018-03-20]. Dostupné z: https://www.box.com/

[15] Dropbox [online]. California, c2018 [cit. 2018-03-20]. Dostupné z: https://www.dropbox.com/

[16] Microsoft: OneDrive [online]. Washington: Microsoft, c2018 [cit. 2018-03-20]. Dostupné z: https://onedrive.live.com/about/cs-cz/

[17] Google Drive: cloudové uložiště [online]. California: Google, c2018 [cit. 2018-03-20]. Dostupné z: https://www.google.com/drive/

[18] Práva souborů ve Windows. FJFI: Katedra softwarového inženýrství [online]. Praha: FJFI ČVUT, c2017 [cit. 2018-04-19]. Dostupné z: https://ksi.fjfi.cvut.cz/prava-souboru-ve-windows

[19] PECINOVSKÝ, Josef. Archivace a komprimace dat: jak zálohovat data, jak komprimovat soubory WinRAR, WinZip, WinAce, Windows a nástroje komprese dat, jak archivovat data ve Windows. Praha: Grada, 2003, 116 s. Snadno a rychle. ISBN 8024706598.

[20] Sandboxie [online]. Spojené Království: Sandboxie Holdings, c2004-2018 [cit. 2018-04-19]. Dostupné z: https://www.sandboxie.com/

[21] BROOKSHEAR, J. Glenn, David T. SMITH a Dennis BRYLOW. Informatika. Brno: Computer Press, 2013. ISBN 978-802-5138-052.

[22] KLANDER, Lars. Hacker Proof: váš počítač, vaše síť a vaše připojení na internet. Je to opravdu bezpečné?. Brno: UNIS, 1998, 648 s., 1 CD-ROM. ISBN 8086097153.

[23] SZOR, Peter. Počítačové viry: analýza útoku a obrana. Brno: Zoner Press, 2006, 608 s. Encyklopedie Zoner Press. ISBN 80-86815-04-8. Dostupné také z: http://katalog.k.utb.cz/F/?func=service&doc_library=UTB01&doc_number=000028527&line_number=0002&func_code=WEB-BRIEF&service_type=MEDIA

[24] ŽID, Norbert. Orientace ve světě informatiky. Praha: Management Press, 1998, 391 s. ISBN 8085943581.

[25] KRÁL, Mojmír. Bezpečný internet: chraňte sebe i svůj počítač. Praha: Grada Publishing, 2015. Průvodce (Grada). ISBN 978-80-247-5453-6.

[26] HANŽL, Tomáš, Radek PELÁNEK a Ondřej VÝBORNÝ. Šifry a hry s nimi: kolektivní outdoorové hry se šiframi. Praha: Portál, 2007, 198 s. ISBN 978-80-7367-196-9. Dostupné také z: http://toc.nkp.cz/NKC/200706/contents/nkc20071715878_1.pdf

[27] BURDA, Karel. Úvod do kryptografie. Brno: Akademické nakladatelství CERM, 2015. ISBN 978-80-7204-925-7.

[28] ANDRUŠKO, Alena. Internet, informační společnost a autorské právo. Praha: Wolters Kluwer, 2016, xxii, 254. Právní monografie. ISBN 978-80-7552-327-3.

[29] Zákon č. 121/2000 Sb.: Zákon o právu autorském, o právech souvisejících s právem autorským a o změně některých zákonů (autorský zákon). Zákony pro lidi [online]. Zlín: AION, 2018 [cit. 2018-04-19]. Dostupné z: https://www.zakonyprolidi.cz/cs/2000-121

[30] Nová citační norma ČSN ISO 690:2011 - Bibliografické citace [online]. Plzeň: Firstová, 2011 [cit. 2018-04-19]. Dostupné z: https://sites.google.com/site/novaiso690/

[31] Regulation (EU) 2016/679 of the European Parliament and of the Council: GDPR. EUR - Lex: Access to European Union Law [online]. 2016 [cit. 2018-04-19]. Dostupné z: http://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1501688126470&uri=CELEX:32016R0679

[32] ŠKORNIČKOVÁ, Eva. Co je GDPR?. GDPR: Obecné nařízení o ochraně osobních údajů prakticky [online]. [cit. 2018-04-19]. Dostupné z: https://www.gdpr.cz/gdpr/

[33] KMOCH, Petr. Informatika a výpočetní technika pro střední školy. Vyd. 1. [i.e 3. vyd.]. Praha: Computer Press, c1997, 228 s. Učebnice pro střední školy. ISBN 8072267329.

[34] NAVRÁTIL, Pavel a Michal JIŘÍČEK. S počítačem nejen k maturitě. 9. vydání. Prostějov: Computer Media, 2016. ISBN 978-807-4022-531.

SEZNAM POUŽITÝCH SYMBOLŮ A ZKRATEK

RVP	Rámcový vzdělávací program.
ŠVP	Školní vzdělávací program.
NVP	Národní vzdělávací plán
MŠMT	Ministerstvo školství, mládeže a tělovýchovy
ICT	Information and Communication Technologies
SAAS	Software as a Service
PAAS	Platform as a Service
IAAS	Infrastructure as s Service
WEP	Wired Equivalent Privacy
WPA	Wi-Fi Protected Access
GDPR	General Data Protection Regulation
ÚOOÚ	Úřad pro ochranu osobních údajů
EDPB	Evropský sbor pro ochranu osobních údajů
DPIA	Data Protection Impact Assessment

SEZNAM OBRÁZKŮ

SEZNAM GRAFŮ

SEZNAM TABULEK

SEZNAM PŘÍLOH

Příloha P I: Prezentace *Hodina1.pptx*

Příloha P II: Prezentace *Hodina2.pptx*

Příloha P III: Prezentace *Hodina3.pptx*

Příloha P IV: Prezentace *Hodina4.pptx*

Příloha P V: Prezentace *Hodina5.pptx*

Příloha P VI: Prezentace *Hodina6.pptx*

Příloha P VII: Soubor pracovních listů *PracovniListy.pdf*