Realizace školního projektu malé domácí počítačové sítě

Bc. Anna Křepelková

Diplomová práce
2024

Univerzita Tomáše Bati ve Zlíně
Fakulta aplikované informatiky

Univerzita Tomáše Bati ve Zlíně
Fakulta aplikované informatiky
Ústav informatiky a umělé inteligence

Akademický rok: 2023/2024

ZADÁNÍ DIPLOMOVÉ PRÁCE

(projektu, uměleckého díla, uměleckého výkonu)

Jméno a příjmení:	**Bc. Anna Křepelková**
Osobní číslo:	**A21627**
Studijní program:	**N3902 Inženýrská informatika**
Studijní obor:	**Učitelství informatiky pro střední školy**
Forma studia:	**Prezenční**
Téma práce:	**Realizace školního projektu malé domácí počítačové sítě**
Téma práce anglicky:	**Implementation of a School Project of a Small Home Computer Network**

Zásady pro vypracování

1. Proveďte literární rešerši tématu domácí počítačové sítě.
2. Navrhněte vhodný výukový projekt a jeho zařazení do výuky na základní nebo střední škole.
3. Stanovte didaktické cíle a připravte jednotlivé pracovní a metodické listy.
4. Ověřte vhodnou formou reálnou využitelnost pracovních listů ve výuce.
5. Vyhodnoťte úspěšnost a přínos projektu.

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

Seznam doporučené literatury:

1. ČAPEK, Robert, 2022. *Moderní didaktika – Lexikon výukových a hodnoticích metod*. Praha: Grada. ISBN 978-80-247--3450-7.
2. ČÍKA, Petr, 2017. *Internet věcí pro inteligentní domácnost: Internet of things for smart home : zkrácená verze habilitační práce*. Brno: Vysoké učení technické v Brně, nakladatelství VUTIUM. ISBN 978-80-214-5559-7.
3. DÖMISCHOVÁ, Ivona, 2011. *Projektová výuka: moderní strategie vzdělávání v České republice a německy mluvících zemích*. Olomouc: Univerzita Palackého v Olomouci. ISBN 978-80-244-2915-1.
4. *Didaktika informatiky*, 2022. Online. Wikipedia. Dostupné z: https://cs.wikipedia.org/wiki/Didaktika_informatiky. [cit. 2022-10-23].
5. NÁRODNÍ ÚŘAD PRO KYBERNETICKOU A INFORMAČNÍ BEZPEČNOST [NUKIB]. *Doporučení k ochraně počítačů a chytrých zařízení v domácnosti*. Online. Dostupné z: https://www.nukib.cz/cs/infoservis/doporuceni/1512-ochrante-svuj-domov-proti-hackerum/. [cit. 2023-11-14].

Vedoucí diplomové práce: **prof. Mgr. Roman Jašek, Ph.D., DBA**
Ústav informatiky a umělé inteligence

Datum zadání diplomové práce: **5. listopadu 2023**
Termín odevzdání diplomové práce: **13. května 2024**

UNIVERZITA TOMÁŠE BATI VE ZLÍNĚ
Fakulta aplikované informatiky
DĚKAN
L.S.

doc. Ing. Jiří Vojtěšek, Ph.D. v.r.
děkan

prof. Mgr. Roman Jašek, Ph.D., DBA v.r.
ředitel ústavu

Ve Zlíně dne 5. ledna 2024

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 práce bude uložen v příruční knihovně Fakulty aplikované informatiky Univerzity Tomáše Bati ve Zlíně;
- 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 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 Anna Křepelková, v.r.

ABSTRAKT

Cílem diplomové práce je vytvořit výukový projekt na téma domácích počítačových sítí na druhém stupni. V teoretické části byl provedena literární rešerše na téma domácí počítačové sítě. Další část diplomové práce se zabývá návrhem vhodného výukového projektu. Následně byly vytvořeny prezentace, pracovní listy, test a metodické listy. V další části byla zaznamenána příprava samotné výuky a realizace. Nakonec bylo zhodnoceno, jaký přínos práce má, jaké má silné a slabé stránky a jaký má možný budoucí vývoj.

Klíčová slova: didaktika, informatika, počítačové sítě, chytrá domácnost, sdílené úložiště, zálohování dat, kyberbezpečnost, zabezpečení sítí, chytrá zařízení,

ABSTRACT

The aim of the thesis is to create a teaching project on home computer networks at the second level. In the theoretical part, a literature search on the topic of home computer networks was conducted. The next part of the thesis deals with the design of a suitable teaching project. Subsequently, presentations, worksheets, test and method sheets were created. In the next part, the preparation of the actual teaching and implementation was recorded. Finally, the contribution of the work, its strengths and weaknesses and possible future developments were evaluated.

Keywords: didactics, informatics, computer networks, smart home, shared storage, data backup, cybersecurity, network security, smart devices,

OBSAH

ÚVOD **8**
I TEORETICKÁ ČÁST **9**
1 DOMÁCÍ POČÍTAČOVÉ SÍTĚ **10**
1.1 POČÍTAČOVÁ SÍŤ 10
1.1.1 Dělení podle fyzické topologie 10
1.1.2 Dělení sítí podle postavení 11
1.1.3 Dělení podle velikosti 11
1.2 KOMUNIKACE V POČÍTAČOVÉ SÍTI 12
1.2.1 Protokoly 12
1.2.2 Adresy 12
1.2.3 DNS 13
1.2.4 Pakety 13
1.3 PRVKY A ZAŘÍZENÍ DOMÁCÍ POČÍTAČOVÉ SÍTĚ 13
1.3.1 Aktivní prvky 13
1.3.2 Pasivní prvky 14
1.3.2.1 Drátové 14
1.3.2.2 Bezdrátové 14
1.3.3 Koncová zařízení 15
1.4 ZABEZPEČENÍ DOMÁCÍCH POČÍTAČOVÝCH SÍTÍ 15
1.4.1 Hrozby 15
1.4.1.1 Malware 16
1.4.2 Hacking 16
1.4.3 Zabezpečení koncových zařízení 17
1.4.3.1 Antivirus 18
1.4.3.2 Firewall 18
1.4.3.3 VPN 18
1.4.3.4 Hesla 19
1.4.4 Zabezpečení prvků 20
1.5 CHYTRÁ DOMÁCNOST 20
1.5.1 Definice 20
1.5.2 Chytrý dům 21
1.5.3 Prvky 21
1.5.4 Zabezpečení 22
1.6 SDÍLENÉ ÚLOŽIŠTĚ 22
1.6.1 Definice 23
1.6.1.1 Zálohování dat 23
1.6.2 Druhy úložišť 24
1.6.2.1 Online úložiště 24
1.6.2.2 Hardwarová úložiště 24
2 DIDAKTIKA **26**
2.1 VÝUKOVÉ METODY 27
2.1.1 Výklad 27
2.1.2 Pracovní listy 27
2.1.3 Skupinová práce 28

2.1.4 Didaktická hra Domino 28
2.1.5 Didaktický test 28
2.2 BLOOMOVA TAXONOMIE 28
3 NÁVRH VÝUKOVÉHO PROJEKTU 30
3.1 STANOVENÍ DIDAKTICKÉHO CÍLE 30
3.1.1 Obecné cíle 30
3.1.2 Dílčí cíle 30
3.2 SESTAVENÍ CÍLŮ DO VÝUKY 31
3.2.1 Základy počítačových sítí 31
3.2.2 Zabezpečení počítačových sítí 31
3.2.3 Chytré domácí sítě 31
3.2.4 Sdílené úložiště 32
3.2.5 Ověření znalostí 32
3.3 VÝBĚR VYUČOVACÍCH METOD 32
II PRAKTICKÁ ČÁST 33
4 VYTVÁŘENÍ MATERIÁLŮ 34
4.1 VYTVOŘENÍ PREZENTACÍ 34
4.1.1 Prezentace Základy počítačových sítí 34
4.1.2 Prezentace Zabezpečení počítačových sítí 35
4.1.3 Prezentace Chytrá domácnost 36
4.1.4 Prezentace Sdílené úložiště 37
4.2 PRACOVNÍ LISTY 38
4.2.1 Pracovní list Základy počítačový sítí 38
4.2.2 Pracovní list Zabezpečení počítačových sítí 39
4.2.3 Pracovní list Chytrá domácnost 40
4.2.4 Pracovní list Sdílené úložiště 41
4.3 TEST 42
5 PŘÍPRAVA HODINY 44
5.1 METODICKÉ LISTY 44
5.1.1 První hodina – Základy počítačových sítí 45
5.1.2 Druhá hodina – Základy počítačových sítí – cvičení 45
5.1.3 Třetí hodina – Zabezpečení počítačových sítí 46
5.1.4 Čtvrtá hodina – Zabezpečení počítačových sítí – cvičení 46
5.1.5 Pátá hodina – Chytrá domácnost 46
5.1.6 Šestá hodina – Sdílené úložiště 47
5.1.7 Sedmá hodina – Opakování, test 47
6 OVĚŘENÍ FUNKČNOSTI ŘEŠENÍ 49
6.1 HODNOCENÍ PEDAGOGA 49
6.2 HODNOCENÍ ŽÁKŮ 49
7 ZHODNOCENÍ VÝUKOVÉHO PROJEKTU 51
7.1 SILNÉ STRÁNKY 51
7.2 SLABÉ STRÁNKY 51
7.3 BUDOUCÍ ZMĚNY 51
ZÁVĚR 52
SEZNAM POUŽITÉ LITERATURY 53

SEZNAM POUŽITÝCH SYMBOLŮ A ZKRATEK 58
SEZNAM OBRÁZKŮ 60
SEZNAM TABULEK 61
SEZNAM PŘÍLOH 62

ÚVOD

Počítače a počítačové sítě jsou jedním ze základů moderní civilizace. Pokud by se stalo, že by počítačové sítě přestaly přes noc fungovat, zavládl by všude chaos. Všechny důležité systémy jako jsou například elektrárny, výroba a distribuce jídla, banky, a mnoho dalších jsou jimi již řízeny. Počítače usnadňují těžkou práci a umožňují lidstvu další rozvoj technologií. Počítačové sítě jsou s lidmi každý den a jejich vliv se stále rozšiřuje. Proto je důležité, aby lidé věděli, jak fungují, proč jsou důležité a jak je zabezpečit.

V domácnostech je velký nárůst technologií a do styku s nimi přichází stále mladší děti. Ve škole by se tedy měli dozvědět informace navíc, které jim mohou pomoci rozvíjet jejich tvůrčí schopnosti v rámci využívání technologií. Téma domácí počítačové sítě ale není dostatečně pokryté v již existujících učebních materiálech. Proto je téma této práce aktuální, protože se změnou v rámci nové informatiky na školách jsou počítačové sítě jedno z probíraných témat.

Teoretická část se bude zabývat základními pojmy z oblasti domácích počítačových sítí. Pojmy jako jsou koncová zařízení, topologie, aktivní a pasivní prvky, adresy v síti, komunikaci. V další kapitole je popsáno, co je kyberbezpečnost, jakým hrozbám čelí a jaká jsou řešení těchto problémů. Pojmy jako malware, hacking, antivirus, firewall, VPN a další. Toto téma je zvlášť důležité pro děti, které si ještě neuvědomují nástrahy digitálního světa. Kapitola chytré domácnosti se zabývá jejich vymezením, IoT a prvkům, výhodami a nevýhodami a opatřeními proti jejich bezpečnostním problémům. Poslední část teorie je věnovaná sdílenému úložišti, jeho druhům a výhodám a problémům, pojmům jako je zálohování, cloud, síťové úložiště a jejich výhodám a nevýhodám.

V praktické části se nejprve načrtne hrubý návrh výukových materiálů a metod a technologií na ně použitých. Následně se rozhodnou didaktické cíle a podle nich se ony návrhy musí vytvořit a otestovat. Budou vytvořeny prezentace, na nich navázané pracovní listy a poté metodické listy pro učitele. Na závěr je třeba materiály vyhodnotit, zjistit jejich silné a slabé stránky a promyslet případné budoucí změny.

I. TEORETICKÁ ČÁST

1 DOMÁCÍ POČÍTAČOVÉ SÍTĚ

Podle českého statistického úřadu se v Česku v roce 2020 nacházelo 81 % domácností s přístupem k internetu [6]. Tudíž je potřeba vysvětlit, jak počítačové sítě fungují, jak se o ně starat, jak se připojit k internetu, jak se na internetu chovat a jaké jsou možnosti a rizika.

Dříve než bude vysvětleno, co je domácí síť, je nejprve třeba podívat se na počítačovou síť.

1.1 Počítačová síť

Podle webu Khan Academy [7] je počítačová síť definovaná jako skupina vzájemně propojených zařízení, která odesílají a přijímají informace. Weby Umíme informatiku [8] a it-network.cz [9] mají podobné definice jako již zmíněná Khan Academy.

Jen je ještě potřeba dodat, že komunikace v počítačové síti má nějaká pravidla, které zajišťují určité protokoly. Tyto sítě se rozdělují se podle různých parametrů.

1.1.1 Dělení podle fyzické topologie

Topologie zobrazuje to, jak jsou mezi sebou jednotlivé zařízení a prvky propojeny. V tomto případě se jedná čistě o fyzickou topologii.

První topologie, která je často zmiňována, je topologie kruhová. **Kruhová topologie** se vyznačuje tím, že všechny prvky jsou propojeny za sebou do kruhu [9][10][11]. V případě výpadku jednoho zařízení je tedy možné stále ještě komunikovat se všemi v síti. Problém nastává při výpadku dvou stanic od sebe vzdálených. Při takovém výpadku se totiž může stát, že alespoň jedno zařízení nemá možnost komunikace. Záleží také na velikosti (počtu zařízení) sítě, protože čím větší počet zařízení, tím větší je možnost, že vypadnou nesousedící zařízení, a tedy i možnost ztráty komunikace pro větší počet zařízení, ale síť stále částečně funguje.

Další častou topologií je tzv. **hvězdicová topologie**. To znamená, že má nějaký centrální prvek, který propojuje všechna ostatní zařízení [7][9][10][11]. Pokud by se stalo, že vypadne centrální prvek, síť se stává nefunkční. Při vypadnutí jednoho zařízení síť ale stále funguje. Tento druh topologie je často v domácnostech, protože je jednoduchá na udržování a správu.

Následující topologie se nyní už příliš nepoužívá. Jedná se o takzvanou **sběrnicovou topologii**, anglicky bus. Komunikaci zajišťuje přenosové médium – sběrnice, ke které jsou ostatní zařízení připojena [9][10][11]. Problém nastává, především pokud chtějí komunikovat

zařízení najednou, pak nastává tzv. kolize, která ochromí celou síť. Byly ale vymyšleny protokoly, které tento problém vyřešily.

Další používanou topologií je **stromová**. Jde o postupné rozvětvování prvků a až na konci je zařízení. Používá se ve firmách, protože je vhodná pro přidání mnoho zařízení a sub sítí. [9][10]

Topologií existuje i více, ale tyto jsou nejvíce zmiňované. Zařízení můžou být propojená i více cestami. Například čtyři zařízení, která jsou spolu propojena všemi různými možnými cestami. V takových zapojeních nastává problém tzv. redundance (nadbytečnost) některých cest. V tu chvíli při vypadnutí zařízení nebo propojení se nic nestane a komunikace pokračuje dál. Na druhou stranu to není příliš finančně výhodné a přehledné.

1.1.2 Dělení sítí podle postavení

V počítačových sítí je také jakási hierarchie, a právě tato hierarchie také hraje roli v jejich dělení. Rozdělují se na dvě základní: klient-server a peer-to-peer.

Klient-server je druh sítě, ve které server poskytuje služby jinému zařízení (klient). Klient posílá požadavky a server na ně posílá odpovědi. [8][9][11]

Naopak ve spojení **peer-to-peer** (rovný s rovným) mají obě zařízení stejnou roli. Často jsou využívána pro sdílení souborů (hudby, videí). [8][9][11]

Veškeré požadavky na webové stránky jsou pomocí architektury klient-server. V případě komunikace peer-to-peer je často zmiňovaná metoda sdílení souborů torrent.

1.1.3 Dělení podle velikosti

Podle rozlehlosti každé sítě můžeme určit čtyři základní typy:

- PAN (Personal Area Network) je nejmenší síť a jejím účelem je spojit osobní zařízení [8][9], např. mobilní telefon a laptop. Jsou spolehlivé na vzdálenost jen pár metrů. Nejčastěji využívá technologie Bluetooth, NFC nebo IrDA.
- LAN (Local Area Network) je síť používaná v domácnosti a jednotlivých budovách [7][8][9][11]. Propojuje například počítače, tiskárny, mobilní telefony, chytré televize a další koncová zařízení. Dosah má několik stovek metrů. Nejčastější technologie jsou Ethernet a Wi-Fi. Často používaná je také zkratka WLAN (Wireless LAN).

- MAN (Metropolitan Area Network) je síť, která propojuje města [9]. Jde o síť umožňující větší rychlost přenosu dat než u LAN, která zvládne propojit více zařízení. Dosah má v rámci desítek kilometrů.
- WAN (Wide Area Network) je síť umožňující komunikaci na velké vzdálenosti i tisíce kilometrů [7][8][9][11]. Spojuje sítě MAN a LAN ve velkých vzdálenostech a rychlostech. Příkladem je třeba internet.

1.2 Komunikace v počítačové síti

V rámci domácí síťové komunikace funguje předávání informací často pomocí paketů a protokolů. Pakety pak zvládnou dorazit do cíle díky tzv. adresaci. Adresace je používání jednoznačných identifikátorů zařízení. Autoři komunikaci v síti často přirovnávají k poště, kdy se pakety stávají dopisy a zařízení používají adresu tak, aby paket došel do cílové destinace [9][12].

1.2.1 Protokoly

Protokol je soubor pravidel, podle kterých se pakety přenáší a dále s nimi pracuje. Nejdůležitějším protokolem je IP (Internet Protocol). Ten zajišťuje tzv. směrování, tedy aby se pakety dostaly na správné zařízení. [8][12]

1.2.2 Adresy

IP adresy pomáhají rozlišit jednotlivá zařízení v počítačové síti, adresa proto musí být v dané síti jedinečná. Existují dva základní druhy adres, které se v počítačových sítích používají.

IPv4 je protokol, který určuje zápis pomocí 32bitového čísla rozděleného na čtyři části po osmi bitech oddělených tečkami. To znamená, že mohou být použitá čísla od 0-255. Například IP adresa 192.168.2.10. [8][12][13]

Rozhraní a rozsah sítě pak určuje tzv. síťová maska, která má stejný tvar zápisu jako IP adresa. Často ji je možné vidět ve tvaru 255.255.255.0. Případně se může zkracovat do tzv. prefixu, tedy zkráceného záznamu IP adresy, např. 192.168.2.10/28. [8][12][13]

Adresy se rozdělují na veřejné a privátní, například již dříve zmíněná adresa 192.168.2.10 je soukromá a například adresa 185.17.117.32 je veřejná. Ty veřejné se používají v prostředí internetu a ty soukromé v lokálních sítích (domácí síť). Takto rozdělené jsou, protože počet IP adres je omezen a začalo docházet místo, jak internet stále více a více rostl. [8][12][13]

Jako odpověď na nedostatek IPv4 adres bylo zavedení IPv6 adres. Adresy jsou zapisovány pomocí 128bitového čísla jako čtyři hexadecimální čísla po osmi skupinách oddělených dvojtečkami. To znamená, že může být použito hexadecimální číslo (0-f). Například 0123:4567:89ab:cdef:0000:0123:4567:89af. To číslo je dost dlouhé a proto, pokud jsou v zápisu v jedné části nuly, je možné zápis jednou zkrátit pomocí dvou dvojteček, například 0123:4567:89ab:cdef::0123:4567:89af. [8][12][13]

Existují ještě takzvané **MAC adresy**, které jsou dané už od výrobce onoho zařízení. Zapisují se hexadecimálně a oddělují se dvojtečkou.

1.2.3 DNS

DNS neboli Domain Name Systém pomáhá v prostředí internetu tím, že překládá těžko zapamatovatelnou IP adresu na tzv. doménové jméno. Pokud je potřeba zobrazit například stránku s doménou utb.cz, tak nikdo nemusí zadávat IP adresu, ale stačí napsat doménové jméno a stránka se objeví. [8][12]

1.2.4 Pakety

Paket je blok dat, který se přenáší v počítačové síti. Pakety jsou vlastně rozdělené informace zabalené do balíčků, které pak putují k adresátovi. Paket je rozdělen do bloků. Každý blok nese určité informace o tom, kdo jej vytvořil, kam putuje, jak dlouho má existovat apod. [8]

1.3 Prvky a zařízení domácí počítačové sítě

Díky počítačovým prvkům můžeme přenášet pakety mezi koncovými zařízeními. Často se také nazývají síťovými zařízeními. Tyto prvky se rozdělují na aktivní a pasivní.

1.3.1 Aktivní prvky

Aktivní prvky nějak upravují nebo zesilují signál, který přenášejí. Mezi nejčastější aktivní prvky patří:

- **Switch** také jinak přepínač, který pomáhá větvit a propojit jednotlivé prvky a koncová zařízení [8][14]. Switch je zařízení, které má více portů (zdířek), takže je možné rozšířit danou síť.
- **Repeater** nebo také opakovač pomáhá opravit, vyčistit a zesílit signál [14]. Často se po-užívá pro prodloužení dosahu dané sítě.

- **Router** neboli směrovač přeposílá pakety správným příjemcům a stará se o bezpečnost sítě [8][14]. Je tedy „chytřejší“ než switch a je třeba ho nastavit (nakonfigurovat). Má vlastní IP adresu a zabezpečení heslem.

1.3.2 Pasivní prvky

Jde především o kabeláž a konektory, které se používají při komunikaci v počítačové síti. Tyto prvky signál nijak neupravují, jen jej přeposílají.

1.3.2.1 Drátové

Kabely jsou rozděleny na metalické (kovové) a optické (skleněné). Protokoly pro drátový přenos se jmenují Ethernet.

Metalické kabely jsou kovové dráty, které pomocí elektrického signálu nesou informaci. Jsou používanější než optické, protože mají přiměřenější cenu a v domácnosti (na krátké vzdálenosti) jsou dostačující. Navíc se mohou ohnout více než kabely optické, tudíž je jejich použití v domácích sítích praktičtější. Pokud se metalický kabel přesekne, je jednodušší a ekonomičtější jej nahradit, popřípadě opravit. [8][15]

Optické kabely obsahují skleněné vlákno, které pomocí světla (laseru) přenášejí informaci. Používají se na delší vzdálenost, protože možnost ztráty signálu je mnohem menší než u metalických kabelů. Pokud se optický kabel příliš ohne, může se zlomit a pak je potřeba speciální vybavení na sletování. Pro jejich spolehlivost jsou často používané pro hlavní rozvody mezi kontinenty, městy, internetovými poskytovateli i budovami. [8][15]

1.3.2.2 Bezdrátové

Bezdrátový přenos je v domácnostech nejpoužívanější, protože umožňuje mobilitu, kterou drátové spojení neumožňuje. Navíc většina zařízení v domácnosti je bezdrátových. Problém s bezdrátovými přenosy oproti drátovým může být časté rušení signálu.

Nejpoužívanější bezdrátovou technologií je Wi-Fi (Wireless Fidelity). Je to soubor protokolů, které se používají především pro přístup k internetu. Přenos probíhá pomocí rádiových vln. Wi-Fi je často používána v kombinaci s Ethernetem pomocí Wi-Fi routerů nebo tzv. přístupových bodů. Přístupové body (Access Point) a Wi-Fi routery umožnují vysílat bezdrátový signál přes antény pomocí rádiových vln. Je potřeba si svou Wi-Fi síť dobře zabezpečit, protože připojit se na ni může kdokoliv v dosahu signálu, pokud tomu není zabráněno. [15]

Bluetooth je další standard pro bezdrátovou komunikaci. Používá se především v rámci malých osobních sítích [8] [16] (PAN), například pro připojení myši, klávesnice, sluchátek, mobilního telefonu atd. ke koncovému zařízení (počítač). Umí připojit i více zařízení najednou. Pro zabezpečení se používá mimo jiné i tzv. párování, tedy způsob identifikace a zapamatování daného zařízení. Oproti Wi-Fi má menší dosah.

Dnes často využívaná technologie **NFC** (Near Field Comunication) je spojovaná především s bezkontaktními platbami. Jde opět o komunikaci pomocí radiových vln, která je navíc zabezpečená pomocí šifrování, ale vzdálenost, na kterou ji lze použít, je do pár centimetrů. Tato technologie se také používá při ověřování identity pomocí čipů. [17]

1.3.3 Koncová zařízení

Koncové zařízení nebo také síťové zařízení je definováno jako technologie v počítačové síti, která může odesílat a přijímat informace v počítačové síti. Například v domácích sítích to může být počítač, laptop, mobilní telefon, tablet, tiskárna a chytré hodinky, prsten, televize apod. [18]

1.4 Zabezpečení domácích počítačových sítí

Zabezpečení domácích počítačových sítí je důležité a stále aktuální téma. Často si lidé neuvědomují, že správné zabezpečení je stejně potřebné jako počítačová síť samotná.

Zabezpečení sítě neboli kyberbezpečnost se stará o to, aby do sítě nikdo nevstoupil neoprávněně, tedy někdo cizí. [19][20][21]

Jde o zajištění dostupnosti (funkčnosti), soukromí (bez úniků dat), správnosti (data nebyla pozměněná) a sítě. [19][20][21]

Zabývá se prevencí (opatření před tím, než se něco stane), odhalením chyb a poté jejich opravou nebo odstraněním. [19][20][21]

1.4.1 Hrozby

Hrozby, které mohou narušit domácí počítačovou síť:

Únik dat nebo také krádež, zveřejnění nebo jiné narušení, například pomocí malwaru nebo hackingu. [19][20]

Nedovolenými změnami se myslí například změna přístupu uživatele nebo pozměnění souborů. [19][20]

Zničení části nebo celé sítě (dat) například technickou závadou, nebo nehodou zaviněnou lidskou chybou. [19][20]

1.4.1.1 Malware

Malware (Malicious software) neboli škodlivý program nebo aplikace. Jejich účelem je získat přístup do počítače a poté data získat nebo je pozměnit či zničit.

Existuje mnoho druhů malwaru.

Trojský kůň je druh malwaru, který se dostane do počítače skrytý v nějakém neškodném programu nebo příloze e-mailu. Používá se pro přístup do systému, převzetí kontroly nebo získání dat. Pokud se chcete chránit před tímto malwarem, je třeba si pořídit antivirus a aktualizovat systém a programy.[22]

Dalším příkladem je tzv. **Spyware** (Spying software), který získá citlivé informace (přihlašovací údaje, osobní dokumenty) a posílá je útočníkovi. Skrývá se za normální procesy, takže je těžké jej vystopovat. Pokud bychom jej chtěli odhalit, museli bychom se podívat, jestli se nezpomalilo připojení k internetu nebo pomocí správce úloh zjistit podezřelou aktivitu. Pro prevenci je třeba aktualizovat, používat antivirus, chovat se zodpovědně a používat firewall.[22]

Ransomware (Ransom software) je malware, který se dostane do počítače, zamkne přístup k datům a pro odemčení požaduje určitou částku. Zde nastupuje dilema, jestli výkupné zaplatit, nebo zločin nahlásit na policii. Pokud je výkupné zaplaceno, podporuje se tím využívání a další vývoj těchto programů, ale data se odemknou. Navíc je tu i možnost, že útočník bude požadovat další peníze. Pokud s tímto problémem půjdete na policii, pomůžete tím dalším obětem, ale je šance, že svá data již nedostanete zpět nebo to potrvá dlouho. Opatření před ransomwarem jsou zálohovat data, aktualizovat a chovat se zodpovědně. [22][23]

Počítačový virus je druh malwaru, který když se dostane do počítače, upravuje soubory a programy a dokáže se kopírovat a šířit. Ochrana před tímto malwarem je používat antivirus, zálohovat a chovat se zodpovědně. [22][23]

1.4.2 Hacking

Hacking je zneužití zařízení pro neoprávněný přístup [24][25]. Hacker je člověk, který provádí hacking. Hacking může být nelegální i legální. Nelegální hacking provádí útočník často pro získání peněz, informací nebo slávy mezi ostatními hackery. Legální hackeři často

pracují pro firmy, ve kterých provádí kontrolu zabezpečení. Existují i další druhy hackerů, ti se nazývají podle barev například white, black, grey, red a anglický název pro klobouk hat (white hat hacker).

White hat hacker neboli etický hacker je ten, který se pomocí útoků snaží opravit díry v zabezpečení a tím pomoci organizaci, která si ho najala. Díry v bezpečnosti využije jen se souhlasem a neprozradí je, dokud nejsou opraveny. [24][25]

Grey hat hacker sice obchází zákony a etiku, ale dělá to většinou pro dobrou věc. Díry v systému nezneužije, ale ani neoznámí dané organizaci. [24][25]

Blue hat hacker je také etickým hackerem, který testuje odolnost systému organizace, která si ho najme jako white hat, ale většinou to dělá ještě před tím, než je onen systém zveřejněn. [24]

Red hat hacker používá malware a další útoky jako black hat, ale snaží se jimi bojovat proti nim. Nevadí mu porušovat zákony. [24]

Green hat hacker je tzv. zelenáč, tedy nováček v oboru hackingu, který se učí sám. Nemá špatné úmysly, ale někdy může svým jednáním způsobit škodu. [24]

Black hat hacker díry v bezpečnosti zneužívá pro poškození nebo vydělání si. Využívá malware a další útoky pro získání peněz nebo ublížení. Díry v bezpečnosti sdílí s ostatními black hat hackery. [24][25]

Nejčastějšími cíli útoku mohou být chytrá zařízení jako telefony (především se systémem Android, protože je používanější), webkamery, routery a e-maily [25]

1.4.3 Zabezpečení koncových zařízení

Pro zabezpečení zařízení je třeba používat antivirus, firewall, VPN, zálohovat (ukládat data i jinam), aktualizovat systém i aplikace a nastavit přístupová práva (co smí a nesmí uživatelé dělat). [2]

Zabezpečit zařízení heslem (PINem) nebo biometricky, tedy pomocí fyzických atributů (otisk prstu, otisk dlaně, snímání oka, snímání obličeje apod.) [5].

Heslo: často měnit a mít, pokud možno, pro každý účet jiné, používat silné heslo (znaky, čísla a malá/velká písmena, dostatečně dlouhé a nepoužívat slova). Důvod, proč nepoužívat slova, je slovníkový útok. Je to druh napadení využitím všech slov ve slovníku (databázi). [5]

Password Manager (manažer hesel) je učen pro správu hesel a snadnější ukládání a zadávání hesel.

Dvoufaktorové ověřování je možnost zadání hesla spolu s ještě další metodou ověřování.

Chovat se zodpovědně!

Neklikat na podezřelé linky (například http://mojebanka.cz). [5]

Nechodit na nezabezpečené nebo podezřelé stránky. [5]

Nestahovat podezřelé programy a přílohy a programy, stahování jen z oficiálních stránek (Microsoft Store, Google Play, App Store, Steam atd.). [5]

Domácí počítačová síť musí být správně zabezpečená, aby byla funkční. Ztráta dat je hrozba, která je všudypřítomná. Mnohdy je těžké si uvědomit, co by se stalo, pokud by osobní data jako jsou osobní dokumenty, fotky a další soubory zmizely a uživatel by k nim již neměl přístup. To je důvod, proč je důležité si svá data zálohovat, ať už na cloudové úložiště, nebo na jiné médium. Vždy je dobré mít více kopií.

1.4.3.1 Antivirus

Zajišťuje bezpečnost počítače. Antivirus je štít proti škodlivým programům, které si mou najít cestu do zařízení. Je vždy vhodné hledět na instalaci antiviru na každé možné zařízení jako na první věc, kterou je třeba udělat. [26]

Chrání především proti malwaru. Antivirus může být jak placený, tak i bezplatný. Bezplatná verze na základní ochranu postačí, ale obsahuje jen omezené funkce (inspekce sítě a firewall). Placené verze mohou obsahovat funkce navíc: rodičovská kontrola, ochrana e-mailu, zálohování apod. Zástupci nejznámějších antivirů jsou ESET, Avast, Kaspersky, McAfee, Bitdefender a další. [27]

1.4.3.2 Firewall

Firewall zajišťuje bezpečnost počítače tím, že kontroluje komunikaci v síti. Chrání zařízení před neoprávněným převzetím kontroly [29]. Může obsahovat i VPN. V dnešní době součástí antivirů. Není bezpečné vypínat firewall.

1.4.3.3 VPN

VPN (Virtual Private Network) neboli virtuální soukromá síť je zabezpečení, které šifruje komunikaci. Šifrování je zabezpečení dat proti odposlouchávání. Používá se především při

komunikaci na internetu. Zařízení se připojí na server, který poskytne jinou IP adresu. Poskytnutím jiné adresy je možné skrýt skutečnou polohu zařízení i jeho identitu. [28]

Výhodou VPN je vytvoření šifrovaného, a tedy i bezpečnějšího spojení. Další výhodou je skrytí IP adresy, jde tedy o další ochranu před hackery. Bezpečné připojení i na veřejných sítích je další pozitivum, které VPN nabízí. [28]

Nevýhodou může být to, že většina VPN služeb je placených a to měsíčně. Dalším negativem je snížení rychlosti připojení. Navíc některé VPN služby nemusí být tak zabezpečené, jak bychom si přáli. [28]

1.4.3.4 Hesla

Každé zařízení v počítačové síti by mělo mít zabezpečení pomocí hesla, PINu nebo jiných přihlašovacích metod, protože přes nezabezpečená místa se může kdokoliv dostat do sítě a ohrozit ostatní v síti.

Hesla musí být silná, odlišná a občas se i měnit. Silná hesla bývají více než osm znaků dlouhá, používají velká a malá písmena, symboly a číslice. Odlišnými hesly je míněno to, že každý účet by správně měl mít vlastní heslo, aby se nemohlo stát, že útočník zjistí jedno heslo a dostane se kamkoliv. [5]

V níže uvedené tabulce č. 2 je vidět 10 nejpoužívanějších hesel v České republice za rok 2023. Sloupec Pořadí ukazuje posloupnost jednotlivých hesel podle počtu výskytů. Sloupec čas prolomení označuje, jak dlouho může trvat přijít na heslo.

Tabulka 1: Ukázka nejčastějších hesel v ČR v roce 2023 [45]

Pořadí	**Heslo**	**Čas prolomení**	**Počet**
1	admin	<1 s	10 796
2	123456	<1 s	9 941
3	123456789	<1 s	6 528
4	Heslo1234	17 min.	6 237
5	user	1 s	3 164
6	bara1234	2 min.	3 150
7	maminka123	1 den	2 540

8	*AB12CD34	1 den	2 244
9	12345	<1 s	2 220
10	heslo	10 s	2 072

Pravidelná aktualizace všech programů a operačního systému je důležitá, protože řeší případné problémy v zabezpečení. Proto je třeba vždy aktualizovat, kdykoliv to jde.

Klasické „neklikat na přílohy a odkazy e-mailů a textových zpráv, které nejsou známé“ tu také nesmí chybět. Díky kliknutí na podezřelý odkaz nebo přílohu se může stáhnout škodlivý program (malware), který může ohrozit bezpečnost celé sítě. [5][23][35]

1.4.4 Zabezpečení prvků

Zabezpečení prvků v počítačové síti je dalším důležitým bodem. Vždy je třeba změnit výchozí heslo na routeru [5][19][20], protože pokud hacker výchozí heslo zjistí, má přístup do nastavení a může vyměnit uložené webové stránky za falešné (phishing). Tímto způsobem může získat přihlašovací údaje a další citlivá data.

Důležité je také zabezpečit svou Wi-Fi pomocí silného hesla a správného šifrování. Dříve se používalo šifrování WEP, které je dnes už neefektivní, a proto se začalo používat WPA2. [19][20]

Wi-Fi síť je možné zabezpečit i takzvaným white listem, tedy seznamem povolených MAC adres. Je to bezpečnější než heslo, ale pokud by se chtěli k síti připojit dočasní uživatelé, je třeba je postupně přidat a po jejich odchodu vymazat. Existuje i black list, ve kterém se zakáže dané MAC adrese se připojit. Ve většině domácnostech se proto používá heslo, protože je jednodušší jej změnit.

1.5 Chytrá domácnost

Chytrá domácnost je nejnovějším trendem moderního bydlení. Důraz se klade především na její zabezpečení.

1.5.1 Definice

Chytrá domácnost je budoucností technologického vývoje. Jde o přidání multifunkčnosti koncovému zařízení, kterým lze ovládat všechny technologie v domácnosti, také nazývané IoT.

IoT (internet věcí) je chytré zařízení, které umí komunikovat s dalšími zařízeními [2], často v rámci internetu. Může se jednat o osvětlení, spotřebiče, přístroje, termostat, zabezpečení (kamery, zámky) a další užitečná elektronické zařízení [30][31]. Všechny tyto technologie většinou fungují bezdrátově a na dálku. Je možné povolit i vzdálený přístup, takže stačí se připojit kdekoliv na internet a je možné ovládat všechny připojené objekty doma. U spotřebičů a přístrojů je možné nastavit automatické funkce, jako je například kupování náplní, když dojde. Lze nastavit časovač, kdy se mají spustit jednotlivé přístroje nebo přidat podmínky.

Chytrá domácnost je souborem technologií a zařízení v domácnosti, která jsou připojená přes domácí síť a internet. Chytrá domácnost má své výhody i nevýhody, ale získává stále větší popularitu.

Výhodou pro chytrou domácnost je možnost v průběhu času ušetřit peníze na úspoře elektřiny, tepla a vody. Další výhodou je také pohodlnost a přístupnost, kdy je ovládání všech zařízení možné pomocí aplikace v telefonu, tedy odkudkoliv a kdykoliv. Díky chytré domácnosti je také možné si domov zabezpečit pomocí kamer, chytrých zámků, alarmu atd. Další výhodou je také rozšíření možností ovládání jednotlivých zařízení.[30][31]

Nevýhodou může být vysoká pořizovací cena (záleží na počtu chytrých zařízení), která se může pohybovat až do šestimístné cifry [30]. Další nevýhodou může být, že množství informací je třeba dostatečně zabezpečit. Každá informace, kterou zařízení získá, se někam ukládá. Proto je třeba si dávat pozor na výrobce a prodejce těchto zařízení.

1.5.2 Chytrý dům

Inteligentní nebo také chytrý dům se liší od chytré domácnosti tím, že už od samotného projektu a stavby domu se počítá s chytrou domácností. Chytrý dům má tedy chytrou domácnost, ale chytrá domácnost nemusí mít chytrý dům. [33]

Výhodou chytrého domu je lepší spolupráce, ovládání a komunikace mezi zařízeními a lepší zabudování do samotného domu. Nevýhodou je vyšší cena a také to, že projekt chytrého domu je většinou od jedné firmy, která dodá vlastní zařízení. Projekt od jedné firmy je ale také výhodou, protože se nemusí řešit sloučení různých technologií a aplikací.

1.5.3 Prvky

Router je nezbytným prvkem každé chytré domácnosti. Především ten výkonný a spolehlivý. Většina zařízení je totiž připojená přes router do domácí sítě, případně přes internet. Je

vhodné, pokud máte více zařízení v domácnosti, použít další prvky, přes které se připojí na router, aby se zabránilo přetížení sítě. [33]

Centrální jednotka je prvek, který sloučí různé ovládání zařízení přes různé aplikace do jedné přehledné aplikace, kterou je možné snadno ovládat třeba pomocí mobilního telefonu. [33]

Hlasový asistent je už jen takový doplněk k jednoduššímu ovládání. Díky němu je možné zařízení ovládat pomocí hlasových příkazů. Bohužel v České republice ještě není možné pořídit asistenta s podporou českého jazyka. Pokud vám nevadí nastavování a programování, můžete si svého českého asistenta vytvořit sami, ale pokud umíte dobře anglicky, je možné si vybrat ze Siri od Applu, Alexy od Amazonu nebo Google asistenta.

Nutno podotknout, že se často můžete setkat s centrálními jednotkami, které už mají zabudované hlasové asistenty.

1.5.4 Zabezpečení

Stejně jako každá počítačová síť je u chytrých domácností potřeba zabezpečit jednotlivá zařízení i celou síť. Kvůli připojení chytré domácnosti na internet vzniká řada bezpečnostních problémů. Při pořizování centrální jednotky je třeba si dát pozor na výrobce. Mnoho výrobců levnějších variant může mít problém se zabezpečením a šifrováním, tedy že zařízení mohou být napadnuta a odposlouchávána. Někteří odborníci upozorňují i na problém výrobců a připojení k internetu, které je přístupový bod pro případný útok [35]. Všechna zařízení v chytré domácnosti shromažďují data a ty pak dostanou do centrální jednotky – hrozí i odposlouchávání ze strany výrobců. Jednotlivým zařízením pak také hrozí napadení, protože nejsou dostatečně zabezpečena a nemusí tak odchytit škodlivý software. Uživatelé chytrých domácností ale musí provádět pravidelné údržby systému, jako jsou aktualizace na zařízení. Problém je i nepřehlednost uživatelského prostředí některých zařízení – takže je složité provádět aktualizace. [32][33][34]

Uživatelé si musí dát pozor a instalovat aplikace přes oficiální obchody (Google play, AppStore, …). [32][34]

1.6 Sdílené úložiště

Sdílená úložiště umožňují zálohování dat a sdílení souborů. Existuje mnoho možností, jak si zařídit domácí úložiště. [36]

1.6.1 Definice

Sdílené úložiště je technologie, která umožňuje sdílet a ukládat data v počítačové síti nebo na internetu. Umožňuje zálohování, upravování a archivaci dat. Některé, především online úložiště, nabízí i pokročilou formu sdílení, jako je přístup nebo úprava dokumentů skupinou uživatelů najednou. V případě hardwarových řešení se může úložiště propojit s počítačovou sítí a sdílet soubory jen v rámci sítě. [36]

1.6.1.1 Zálohování dat

Zálohování je možnost ochrany před ztrátou, poškozením, krádeží a zničení dat. V rámci domácích sítí je možné zálohovat pomocí zabudované funkce v operačním systému Microsoft Windows. Zálohování může být tzv. **manuální** neboli ruční, kdy je třeba, abyste mysleli na to, kdy zálohovat a spustit zálohovací proces. Díky tomuto druhu budete mít přehled a kontrolu. [36][39]

Automatické zálohování má výhodu v tom, že se nemusíte starat o proces. Také je v počítačové síti s velkým počtem zařízení možné zálohovat více zařízení najednou. Tento druh zajišťuje i **pravidelné** zálohování, které je stejně tak důležité. Nepravidelné zálohování totiž může způsobit, že nastane velká časová mezera, při které je riziko ztráty dat o to citelnější. [36][39][40]

Nejvhodnější je zálohovat data ve třech kopiích, z nichž jedna by měla být mimo vaši domácnost.

Záloha na flash disk je rychlá, ale určená spíše pro menší soubory (malá kapacita) a není vhodná dlouhodobě. CD/DVD se dnes již příliš nepoužívají, protože mají malou kapacitu a v dnešní době mají CD/DVD mechaniku již málokterá zařízení. Zálohování na externí disk jednoduché, ale může být pomalé a existuje hrozba ztráty nebo poškození disku. Síťový disk se používá spíše ve firmách a školách, kdy má každý uživatel přístup na serveru k části disku. Zálohování na NAS (Network Attached Storage) je podobné jako u síťového disku, ale může mít více funkcí, např. galerie fotek nebo server pro média. [36][39]

Zálohování dat na cloud neboli online úložiště je jednoduché. Další výhodou je přístupnost k datům z kteréhokoliv zařízení odkudkoliv na světě. Nevýhodou je omezená kapacita bezplatných verzí (v rámci GB). Navíc je přístup na cloud závislý na internetovém připojení. V rámci bezpečnosti jsou také obavy o data, která jsou online, protože hrozí útok a případně jejich krádež.

Pro zálohování souborů se hodí soubory dostatečně zmenšit, aby nezabíraly tolik místa. Komprimace souborů je další možnost pro manuální zálohování. Výsledný soubor má příponu ZIP nebo RAR. [39]

1.6.2 Druhy úložišť

Úložiště můžeme rozdělit na dvě kategorie: online a hardwarová. V případě velkého přesunu dat se musí připravit speciální hardware, který to umožní.

1.6.2.1 Online úložiště

Vzdálená nebo také cloudová úložiště jsou používané zejména kvůli nenáročnosti na uživatele. Stačí si jen založit účet a nahrát všechny soubory.

Výhodou online úložišť je možnost otevřít a upravovat soubory přímo v úložišti. Dalším pozitivem může být to, že se data neztratí v případě, že zasáhnou přírodní živly nebo lidský faktor. Stávají se čím dál populárnějšími i proto, že jejich základní verze je často zdarma a je třeba si připlatit jen v případě dalších funkcí zálohování a většího objemu dat. [39][40]

Nevýhodou je nutnost internetového připojení a ztráta kontroly nad obsahem na úložišti a snadnější přístup pro případného útočníka. [40]

Příklady online úložišť: Google Disk, Microsoft OneDrive, DropBox, Apple iCloud, Mega, Uložto, atd.

1.6.2.2 Hardwarová úložiště

Pojem hardwarové úložiště znamená, že je třeba pořídit si fyzické médium, na které je potom možné ukládat data. Při pořizování hardwarového úložiště je cena vyšší než u cloudových služeb a je potřeba onen hardware připojit a případně nakonfigurovat.

Ukládání dat na **pevný disk** je možné na **SSD** (Solid State Drive), který je rychlý, tichý, odolný a spolehlivý. Nevýhodou může být vyšší cena oproti HDD a při častém použití se rychle opotřebovává. **HDD** (Hard Disk Drive) má oproti SSD větší kapacitu a nižší cena, ale je pomalejší, těžší a méně odolné. V případě externích disků je odolnost lepší. Navíc externí disky mohou mít další funkce jako je např. automatické zálohování nebo připojení přes USB-C. [37][39]

NAS (Network Attached Storage) je síťově připojené datové úložiště, které umožňuje sdílení dat z více zařízení najednou. Vhodný je pro automatické zálohování. Díky dalším funkcím,

rozšiřitelnosti a spolehlivosti je tak užitečným pomocníkem. Nevýhodou je ale vysoká cena. Pro základní použití v domácnosti je spíše vhodnější **desktop** verze. Jsou určeny pro zálohování, sdílení souborů a je jednoduché je používat. Oproti tomu je pro velké organizace spíše vhodnější **rack** verze. Ta nabízí možnost zapojení velkého počtu disků, a tudíž má velkou kapacitu a výkon.[38][39]

2 DIDAKTIKA

Protože téma domácí sítě bude probíráno se žáky, je potřeba si vysvětlit základní didaktické pojmy, principy a metody, které během výuky použijeme.

Didaktika znamená způsob výuky, který má nějaké zásady, cíle a nástroje, díky kterým pak můžeme dosáhnout didaktického cíle [41].

Didaktické zásady jsou požadavky na výuku pedagoga, díky kterým si žák učivo zapamatuje, výuka ho bude bavit a motivovat k vlastnímu vzdělávání.

Nejčastěji uváděnými didaktickými zásadami jsou:

- názornosti (používání názorných příkladů)
- spojení teorie s praxí (využití v reálném životě)
- vědeckosti (tedy odbornosti učitele a látky)
- přiměřenosti (zjistit rozsah, obtížnost učiva, přizpůsobit úroveň učiva žákům)
- aktuálnosti (počítat s úrovní vědomostí, dovedností a návyků žáka)
- zpětné vazby (v průběhu celé výuky se ujišťovat, že žáci chápou a vědí, co dělat)
- uvědomělosti a aktivity (nalezení a využití motivace žáka pro jeho rozvoj)
- individuálního přístupu (žákův zdravotní, psychický stav a jeho zkušenosti a postoje)
- soustavnosti (uspořádání učiva do logických celků)
- trvalosti (žák by si měl vědomosti a dovednosti zapamatovat)
- kulturního kontextu (respekt k jednotlivým kulturám)

Didaktické cíle jsou očekávaný výsledek, kterého chceme u žáka dosáhnout. Cíle se mohou dělit na několik druhů (např. krátkodobé a dlouhodobé nebo nižší a vyšší) a mají své podmínky. Cíle by měly být:

- přiměřené (nestanovit je příliš velké)
- jednoznačné (jasně definované)
- kontrolovatelné
- konzistentní (nesmí být v rozporu s hlavním cílem)
- komplexní (působení na celek žáka)

2.1 Výukové metody

Při tvorbě přípravy je třeba vždy hledět na trvání jednotlivých metod, které se ve výuce použijí, na učebnu, ve které se bude výuka konat, a především na didaktický cíl, který byl již dříve vytvořen.

Formy výuky je možné členit na individuální, skupinovou či hromadnou [3].

Individuální výuka znamená, že obsah výuky je přizpůsoben každému žákovi podle jeho potřeb. Její výhodou je velmi dobrá efektivita učení a dobrá zpětná vazba pro učitele, ale nevýhodou je časová náročnost a nemožnost spolupráce žáků. [3][41]

Pojmem skupinová výuka se myslí taková výuka, ve které žáci pracují ve skupinách o různých velikostech, které si buď vytvoří sami, nebo je učitel určí. Výhodou skupinové výuky je spolupráce mezi žáky ve skupině, ale nevýhodou pak je menší aktivita jednotlivců, nízká individualita a nízká zpětná vazba. [41]

Hromadná výuka spočívá v tom, že všichni žáci dělají to samé. Je to nejčastější forma výuky ve škole a mezi její metody patří například přednáška. Výhodou je časová nenáročnost na přípravu, nevýhodou je nízká efektivnost učení a nízká aktivita žáků. [41]

Nejvhodnější je kombinovat ve výuce alespoň 3 metody, které nám zajistí zájem žáků o téma a jejich motivaci dozvědět se co nejvíce [1].

Formy výuky se samozřejmě ve vyučování často mění a je vhodné střídat aktivnost a neaktivnost žáků v případě, že je potřeba probrat náročnější téma.

2.1.1 Výklad

Tato metoda se používá na vysvětlení pojmů a jejich vzájemných vztahů [42]. Učitel by měl začít základními informacemi, které pak zdůvodní, a uvede příklad z praxe. Následně může přidat podrobnosti a zajímavosti, které zpestří jeho výklad. Je dobré mít k výkladu připravené i nějaké kontrolní otázky pro žáky nebo doplnit výklad nějakými obrázky a ukázkami. Tato metoda se nazývá interaktivní přednáška.

2.1.2 Pracovní listy

Pracovní listy jsou vytvářeny proto, aby si žáci lépe zapamatovali důležité informace tím, že si je napíšou. Zároveň si žák může z pracovních listů vytvořit vlastní učebnici. Navíc má něco hmatatelného a jde vlastně o důkaz jeho práce.

2.1.3 Skupinová práce

Díky rozdělení do skupin je možné ukázat žákům význam spolupráce a komunikace. Při skupinové práci nejde o rivalitu ve skupině, ale o dosáhnutí řešení vzájemnou pomocí. Skupinová práce poskytuje lepší porozumění látky a rozvíjí týmovou práci a tvořivost. Žáky můžeme rozdělit do skupin různých velikostí podle druhu úkolu, počtu žáků, zájmu žáků, jejich úrovně znalostí atd. [3][42]

2.1.4 Didaktická hra Domino

Jde o aktivizační metodu, která se může použít jako aktivita pro zopakování učiva. Hra je určená na 10-15 minut. [47]

Učitel vytiskne a rozstříhá sady kartiček domina, které rozdá do dvojic. Žáci kartičky otočí názvem hry nahoru a střídají se v otáčení kartiček a jejich přiřazováním. Přiřazuje se pojem ke správnému výroku. Pokud se stane, že kartička do řady nepasuje, žák si ji nechá, pokračuje další žák, a až půjde kartička přiložit ke správnému výrazu, hráč, který ji vlastní, ji přiloží. Hra končí po dokončení celé řady (kruhu).

2.1.5 Didaktický test

Test je jedním z didaktických nástrojů pro zjišťování úrovně znalostí žáků za určité období. Je to nástroj pro objektivní měření výsledků. Test by měl splňovat čtyři podmínky: objektivita, validita, spolehlivost a citlivost. Objektivitou se myslí to, že jsou předem určená pravidla, která platí pro všechny, a výsledky by měly být co nejméně ovlivněny. Validitou se myslí to, aby test splnil účel, pro který byl určen. Spolehlivostí se myslí, že výsledky jsou stabilní a opakovatelné.[42]

Test by tedy měl mít různé druhy otázek (otevřené, uzavřené, s jednou odpovědí nebo s více), neměl by napovídat odpověď na jinou otázkou a neměl by obsahovat tytéž odpovědi.

2.2 Bloomova taxonomie

Bloomova taxonomie je vyjádření výukových cílů v kognitivní oblasti. Postupuje se od nejnižších cílů po nejvyšší. Nejnižší stupeň je zapamatování, poté následuje pochopení, dále aplikace, analýza, syntéza a evaluace. [41][43][46]

Tabulka 2: Ukázka tabulky Bloomova taxonomie [46]

Cílová kategorie	**Typická slovesa vyjadřující cíle**
Zapamatování (Znalost)	Definovat, napsat, opakovat, pojmenovat, popsat, reprodukovat, seřadit, vybrat, vysvětlit, určit
Pochopení (Porozumění)	Dokázat, interpretovat, ilustrovat, objasnit, odhadnout, opravit, přeložit, uskutečnit, vyjádřit vlastními slovy, vypočítat, zkontrolovat, změřit, jinak formulovat
Aplikace	Aplikovat, demonstrovat, diskutovat, interpretovat, načrtnout, navrhnout, uvést vztah, plánovat, použít, registrovat, řešit, uspořádat, vyčíslit, vyzkoušet, prokázat
Analýza	Analyzovat, provézt rozbor, rozhodnout, rozlišit, rozčlenit, specifikovat, najít principy uspořádání
Syntéza	Kategorizovat, klasifikovat, zkombinovat, modifikovat, navrhnout, zorganizovat, reorganizovat, shrnout, napsat zprávu, vyvodit všeobecné závěry
Hodnocení	Argumentovat, obhájit, ocenit, oponovat, porovnat, posoudit, prověřit, vybrat, vyvrátit, zdůvodnit, zhodnotit, podpořit názor, srovnat, provést kritiku, uvést klady a zápory

V rámci výukového procesu by se mělo postupovat od nejnižšího stupně, ale ne vždy musí dosáhnout toho nejvyššího.

3 NÁVRH VÝUKOVÉHO PROJEKTU

Návrh výukového projektu je začátek v plánování pro vytvoření materiálů, které pak budou moci být vyzkoušené.

3.1 Stanovení didaktického cíle

Stanovením didaktického cíle je jednodušší vybrat výukové metody a nástroje. Díky nim je snazší motivovat žáky, protože motivovaní žáci mají větší důvod si zapamatovat znalosti a dovednosti.

Pro zpřehlednění je vhodné si určit podmínky, které budou určovat směr. První podmínkou je, že úkoly v materiálech by měly propojit teoretické znalosti a příklady z reálného života. To pomůže k motivaci žáků, k čemu jim tyto vědomosti vlastně budou. Další podmínkou je, aby byly přehledné a žáci se v nich vyznali. Poslední podmínkou je, aby materiály byly reálně použitelné ve výuce na druhém stupni základní školy nebo prvním ročníku střední školy.

3.1.1 Obecné cíle

Obecné cíle jsou dlouhodobé, které jsou ukotveny v kurikulárních dokumentech [46], jako je například Rámcový vzdělávací program (dále jen RVP) [43].

V tomto opatření ministra školství a tělovýchovy se téma počítačových sítí sice probírá na prvním i druhém stupni, ale vzhledem k detailnosti na druhém stupni, bylo potřeba vymyslet a vytvořit nové a detailnější materiály. Tematický celek Digitální technologie je výstup *I-9-4-03*, který očekává, že žák umí vybrat nejvhodnější způsob připojení zařízení do počítačové sítě, umí říct příklady počítačových sítí a popsat jejich charakteristické znaky.

3.1.2 Dílčí cíle

Dílčí cíle určuje učitel v rámci každé vyučovací hodiny. Cíle musí mít specifikované – co se mají žáci naučit, zopakovat, prohloubit a v jakém časovém úseku. [46]

Cíle existují kognitivní, afektivní a psychomotorické. Kognitivní neboli poznávací jsou často spojeny s Bloomovou taxonomií, používají slova: pojmenovat, vyjádřit vlastními slovy, řešit, analyzovat, navrhnout, zdůvodnit. [42][46].

Afektivní neboli postojové cíle často používají slova: vnímat, akceptovat, vytvářet hodnoty, naslouchat. Je těžké je specifikovat, protože často souvisí kognitivními nebo psychomotorickými cíli. [42][46]

Psychomotorické neboli výcvikové cíle používají slova jako psát, kreslit, stavět, prezentovat, demonstrovat. [42][46]

3.2 Sestavení cílů do výuky

Nejprve je třeba určit konkrétní cíle v jednotlivých vyučovacích hodinách, které pak určí, jaké výukové metody použít.

3.2.1 Základy počítačových sítí

Žáci 9. ročníku po první hodině:

- umí vysvětlit, co je počítačová síť.
- znají pojmy zařízení, topologie, LAN a IP adresa.
- ví, jaký je rozdíl mezi aktivními a pasivními prvky.
- zvládnou popsat svou domácí síť.

Důvodem pro vybrání tohoto téma na začátek je ten, že bude navazovat na výuku softwaru a hardwaru. Navíc může být potom představeno zabezpečení domácích počítačových sítí, které používá právě základní pojmy k prohloubení znalostí.

3.2.2 Zabezpečení počítačových sítí

Žáci 9. ročníku po druhé hodině:

- ví, co je kyberbezpečnost.
- znají hrozby pro bezpečnost počítačových sítí.
- dokážou vyjmenovat bezpečnostní opatření.
- zvládnou doporučit zabezpečení pro svou domácí síť.

Navázání na předchozí hodinu zabezpečením počítačových sítí.

3.2.3 Chytré domácí sítě

Žáci 9. ročníku po třetí hodině:

- umí říct, co je to chytrá domácnost.
- dokážou vyjmenovat zařízení a prvky v chytré domácí síti.

- znají hrozby, které se pojí s chytrou domácností.
- zvládnou uvažovat o budoucím vývoji chytrých domácností.

3.2.4 Sdílené úložiště

Žáci 9. ročníku po čtvrté hodině:

- dokážou říct, co je to sdílené úložiště.
- umí popsat rozdíly mezi hardwarovým a online úložištěm.
- znají výhody a nevýhody jednotlivých řešení.
- zvládnou vybrat, doporučit a obhájit řešení sdílení souborů.

3.2.5 Ověření znalostí

V páté hodině pak bude ověřeno splnění jednotlivých cílů. Nejspíš se ještě jednou zopakují základní pojmy, aby si žáci osvěžili paměť.

3.3 Výběr vyučovacích metod

Na základě určených dílčích cílů v jednotlivých hodinách se vybere forma a metody výuky.

První část frontální výuky bude výklad prokládaný otázkami případně úkoly pro žáky na zaktivizování. Zde má hlavní roli učitel, který předává znalosti žákům, kteří se je snaží pochopit.

Druhá část hodiny bude kombinovaná a věnovaná aplikaci toho, co se již dozvěděli pomocí samostatné práce. Samostatná práce bude formou pracovních listů, které si žáci vyplní a mohou si je následně nechat místo zápisků.

V poslední hodině si budou moci žáci i učitel ověřit, zda si něco zapamatovali. Nejprve může použít didaktickou hru Domino pro zopakování základních pojmů z počítačových sítí. Důvodem pro zopakování před testem je časová mezera mezi hodinami a pro setřídění znalostí u žáků, kteří třeba chyběli jednu hodinu. Test bude mít maximálně deset otázek, protože toto téma je v RVP jen okrajově.

II. PRAKTICKÁ ČÁST

4 VYTVÁŘENÍ MATERIÁLŮ

Při vytváření materiálů je nejdříve potřeba se rozhodnout, které nástroje použít.

Canva [48] je webový nástroj pro vytváření dokumentů, plakátů, videí, prezentací. Má velkou výhodu v grafických možnostech, jako je například využití šablon a stylů. Možnost přidání a volného pozicování velkého množství prvků: tvary, tabulky, text, fotografie, grafiky apod. je dalším pozitivem. Nevýhodou může být to, že část obsahu je jen pro uživatele verze Canva Pro, která je placená. V Canvě byly vytvořeny pracovní listy.

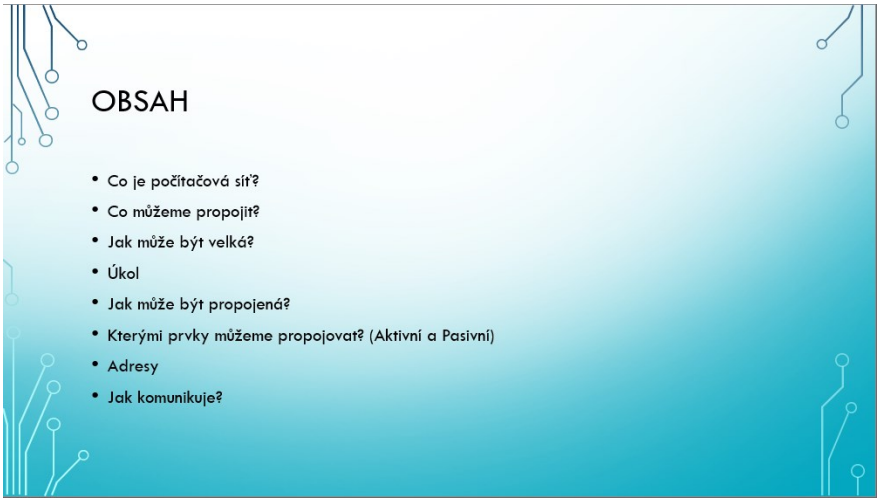
Aplikací, která byla použita pro vytvoření prezenatcí, je PowerPoint od Microsoftu. Je to klasický nástroj pro podporu výkladu ve výuce, který je přehledný, jednoduchý a praktický. Nevýhodou může opět být, že pro vytváření obsahu je placený, ale v dnešní době školy platí celý balíček Office 365, takže tento problém je snadno řešitelný.

4.1 Vytvoření prezentací

Prezentace byly vytvořeny nejdříve, protože měly pomoci s výkladem látky. Každá prezentace má úvodní a závěrečný snímek, obsah a kontrolní otázky. Slidy s výkladem jsou proloženy otázkami pro žáky, které žáky donutí přemýšlet nad tématem. V prezentacích je pomocí sekce poznámek napsaný celý výklad a přepis je vložen do metodických listů. Zdroje obrázků jsou uvedené přímo v prezentacích, kromě obrázků na úvodních slidech, které jsou přímo z fotobanky Microsoftu.

4.1.1 Prezentace Základy počítačových sítí

Nejprve bylo potřeba přijít s přibližným obsahem prezentace. Poté byly vypracovány jednotlivé slidy se základními pojmy z počítačové sítě. Mezi vysvětlováním topologií počítačových sítí byl vložen úkol pro žáky, který je zaktivizuje. Nakonec byly přidány kontrolní otázky, aby se zopakovalo, co se v prezentaci žáci dozvěděli.

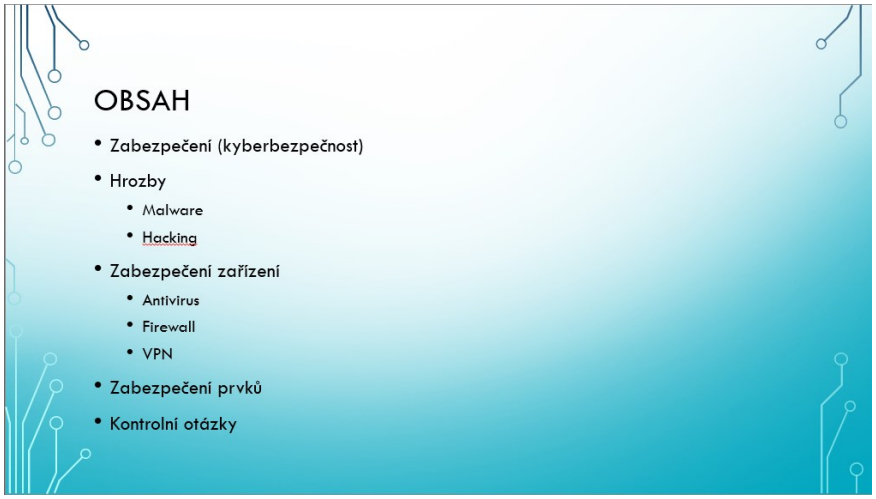


Obrázek 1: Ukázka obsahu prezentace Základy počítačových sítí

První slide obsahuje úvodní slide s názvem celého tématu. Jak už bylo zmíněno, na dalším slidu je obsah, který žákům přiblíží, co se bude probírat. Další je na řadě stručná definice toho, co je to počítačová síť a proč je důležitá. Slide „Co můžeme propojit?“ vysvětluje a uvádí příklady pojmu koncové zařízení. Na dalším slidu je rozdělení počítačových sítí podle velikosti a vysvětluje je. Následující slide je zadání úkolu, díky kterému mohou žáci pochopit, jak různě můžeme propojovat koncová zařízení, a další slide obsahuje sérii obrázků s koncovými zařízeními, které si žáci pomocí kreslení na interaktivní tabuli procvičí. Na dalším slidu je pak rozdělení těch nejzákladnějších fyzický topologií. Slide „Kterými prvky můžeme propojovat?“ obsahuje obrázky a názvy tří nejpoužívanějších aktivních prvků a následující slide ukazuje rozdělení pasivních prvků. Další slide je věnovaný adresaci v síti, takže se zde probírá IP adresa a zmíněná je i MAC adresa. Slide „Jak komunikuje?“ je věnovaný přiblížení komunikace v počítačové síti pomocí příkladu s poštou. Nakonec prezentace je slide s kontrolními otázkami, které ověřují žákovu pozornost a poslední slide obsahuje poděkování za pozornost.

4.1.2 Prezentace Zabezpečení počítačových sítí

Na začátku vytváření bylo opět základním problémem, jak bude vypadat obsah prezentace. Slide Obsah je tedy pro nastínění toho, co bude součástí výkladu. Základní pojmy z kyberbezpečnosti byly důležité pro další podtéma, takže byly zařazeny do prezentace spolu s úkoly pro žáky. Nakonec byly opět přidány kontrolní otázky, které zjistí pozornost žáků.

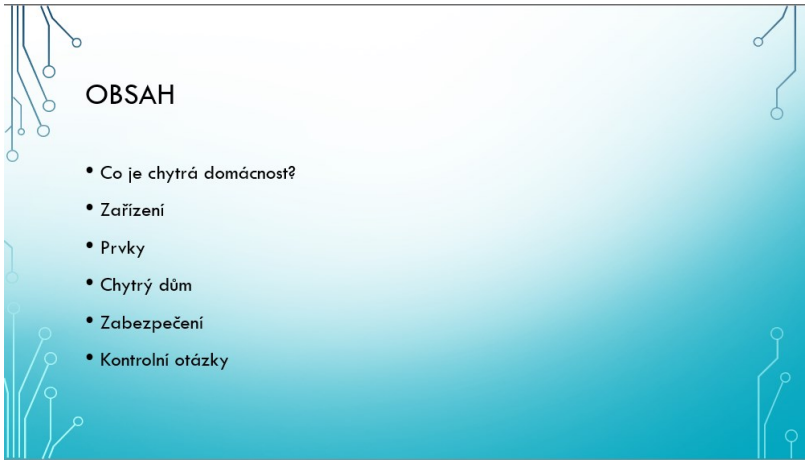


Obrázek 2: Ukázka obsahu z prezentace na téma Zabezpečení počítačových sítí

První slide je úvodní a má název tématu a aktuálního podtéma. Další slide má vypsaný obsah prezentace a následující slide je definice pojmu zabezpečení sítě, její cíle a nástroje. Hrozby jsou na navazujícím slidu, protože je důležité, aby si žáci uvědomili, jaké druhy nebezpečí může ohrožovat počítačovou síť. Na dalším snímku je již vysvětlení pojmu malware, který je jednou z hrozeb koncových zařízení, a nejznámější druhy malwaru. Další slide vysvětluje pojem hacking, kdo je to hacker a jaké druhy hackerů mohou být, aby si žáci uvědomili, že existuje i jiný typ hackera než ten „zlý“. Slide Zabezpečení zařízení dává bezpečnostní tipy, jak chránit koncové zařízení před hrozbami a další slide Antivirus na to navazuje vysvětlením, co to je, jaké má druhy a funkce, a nejznámější příklady. Následující slide se věnuje vysvětlením definice firewallu a jeho funkce. Další slide VPN vysvětluje tento pojem a jaké jsou jeho druhy, aby žáci věděli, o čem to mluví v reklamách na ně. Následující slide se věnuje tipům pro zabezpečení prvků v síti, tedy zabezpečení routeru a Wi-Fi. Předposlední slide opět obsahuje kontrolní otázky a poslední slide poděkování za pozornost.

4.1.3 Prezentace Chytrá domácnost

Vytvoření obsahu prezentace bylo opět tou první věcí, kterou byla potřeba vyřešit. Nejprve bylo nutné definovat, co to je chytrá domácnost, její výhody a nevýhody, poté mohla být vypsána některá zařízení chytré domácnosti. Dalším tématem byly prvky v chytré domácnosti a samotné tipy pro zabezpečení. Nesměly chybět ani kontrolní otázky.

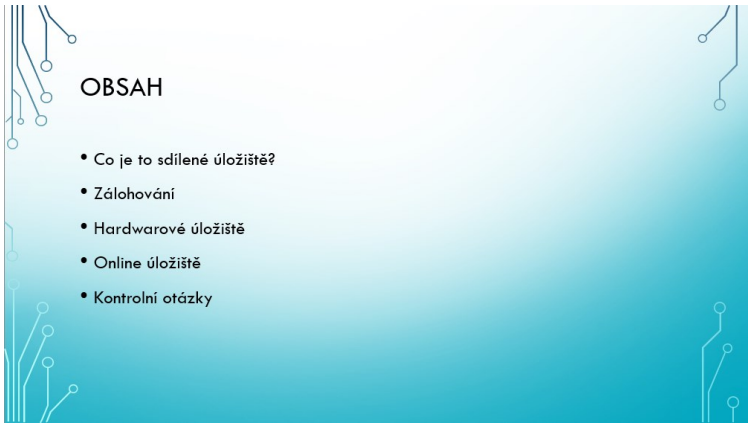


Obrázek 3: Ukázka obsahu prezentace Chytrá domácnost

První dva snímky jsou název a obsah prezentace, které nastíní probíranou látku. Další slide obsahuje video od organizace *Kraje pro bezpečný internet*, které žákům přiblíží animovanou formou, co to vlastně ta chytrá domácnost je. Následuje slide se shrnutím pozitiv a negativ chytré domácnosti. Další slide jen ukazuje některé příklady chytrých zařízení, které se v domácnosti mohou nacházet. Slide Prvky stručně vysvětluje, na co nezapomenout při pořizování chytré domácnosti. Následný slide jen vysvětluje rozdíl mezi pojmy chytrá domácnost a chytrý dům. Na dalším slidu jsou rozepsány tipy pro zabezpečení chytré domácnosti. Prezentaci uzavírají snímek kontrolní otázky a poděkování za pozornost.

4.1.4 Prezentace Sdílené úložiště

Jako první úkon se opět stalo zesumírování obsahu prezentace. Krátká definice, co je to sdílené úložiště byla v první části. Další část byla věnovaná zálohování a druhům a příkladům takovýchto úložišť. Nakonec byly opět přidány kontrolní otázky.



Obrázek 4: Ukázka obsahu prezentace Sdílené úložiště

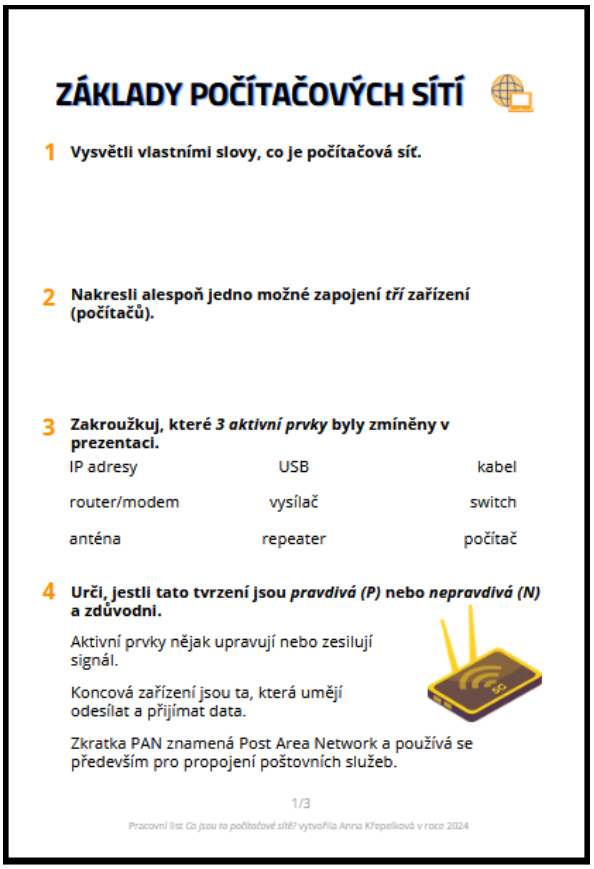
První slidy obsahují název prezentace a její obsah. Následný slide definuje, co to je a jaké jsou jeho funkce. Další slide se zabývá významem zálohování, vypisuje druhy a média, na která můžeme zálohovat. Následující slide ukazuje a popisuje druhy hardwarových úložišť a jejich výhody a určení. Slide Online úložiště nastiňuje jeho výhody a nevýhody a nejznámější zástupce cloudových služeb. Nakonec pomocí kontrolních otázek je shrnutý obsah prezentace a poděkování za pozornost.

4.2 Pracovní listy

Pracovní listy byly vytvořeny k prezentacím a měly tak navazovat na výklad. Každý pracovní list má název tématu, ke kterému se vztahuje, sadu otázek k ověření znalostí z výkladu a sadu úkolů pro lepší zafixování učiva.

4.2.1 Pracovní list Základy počítačový sítí

Pracovní list, který navazuje na stejnojmennou prezentaci, má čtyři otázky na pojmy a informace z výkladu a tři úkoly pro procvičení znalostí a spojení s praktickou stránkou.



ZÁKLADY POČÍTAČOVÝCH SÍTÍ

1 **Vysvětli vlastními slovy, co je počítačová síť.**

2 **Nakresli alespoň jedno možné zapojení *tří* zařízení (počítačů).**

3 **Zakroužkuj, které *3 aktivní prvky* byly zmíněny v prezentaci.**

IP adresy	USB	kabel
router/modem	vysílač	switch
anténa	repeater	počítač

4 **Urči, jestli tato tvrzení jsou *pravdivá (P)* nebo *nepravdivá (N)* a zdůvodni.**

Aktivní prvky nějak upravují nebo zesilují signál.

Koncová zařízení jsou ta, která umějí odesílat a přijímat data.

Zkratka PAN znamená Post Area Network a používá se především pro propojení poštovních služeb.

1/3

Pracovní list *Co jsou to počítačové sítě?* vytvořila Anna Křepelková v roce 2024

Obrázek 5: Ukázka z pracovního listu Základy počítačových sítí

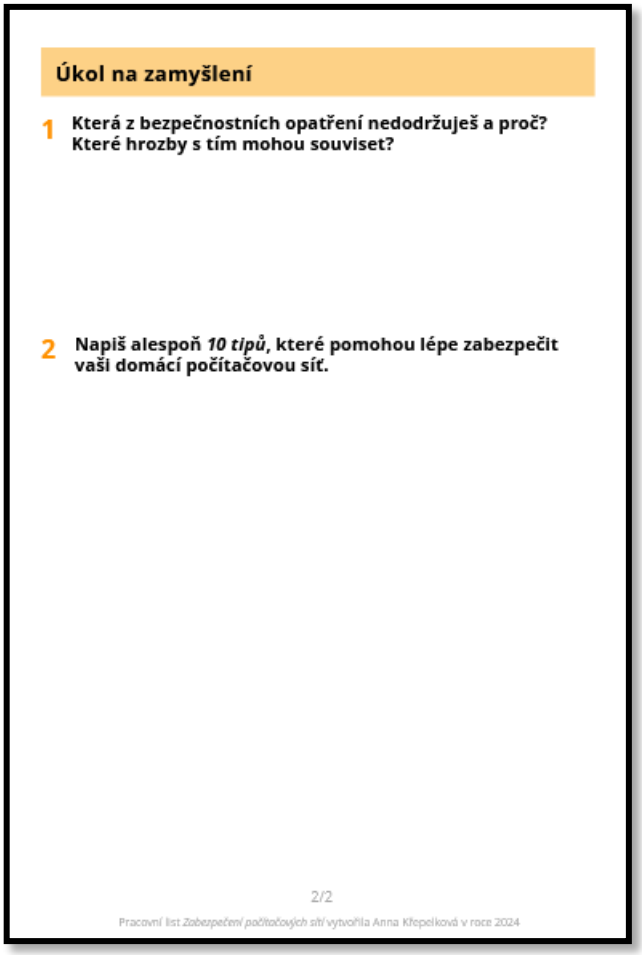
První cvičení se snaží, aby žáci vyjádřili, jak porozuměli definici počítačových sítí z výkladu. V dalším cvičení se zabývá propojením zařízení. Třetí cvičení je pro ověření toho, že si žáci pamatují rozdíl mezi aktivními a pasivními prvky. Další cvičení je koncipováno tak, aby si žáci osvěžili základní pojmy v počítačových sítích.

Následuje druhá část, a to úkoly pro aplikování znalostí. První úkol je pro zapsání, jaká zařízení používají doma. Dalším úkolem je zapsání aktivních a pasivních prvků v jejich domácí počítačové síti. Následuje úkol, který předchozí dva spojí a vyžaduje, aby žáci nakreslili jednoduchý diagram jejich domácí počítačové sítě.

4.2.2 Pracovní list Zabezpečení počítačových sítí

Pracovní list má dvě části. První část pracovního listu má tři cvičení na zopakování znalostí z prezentace a druhou část na uvědomění si důležitosti zabezpečení sítě.

V první části pracovního listu jsou cvičení určená k zopakování látky z výkladu. První cvičení se snaží, aby žáci formulovali vlastními slovy definici zabezpečení počítačové sítě. V dalším cvičení je úkolem vypsat hrozby, které mohou způsobit problémy v počítačové síti. Třetí cvičení se zabývá tím, aby si žáci zopakovali základní pojmy z bezpečnosti.

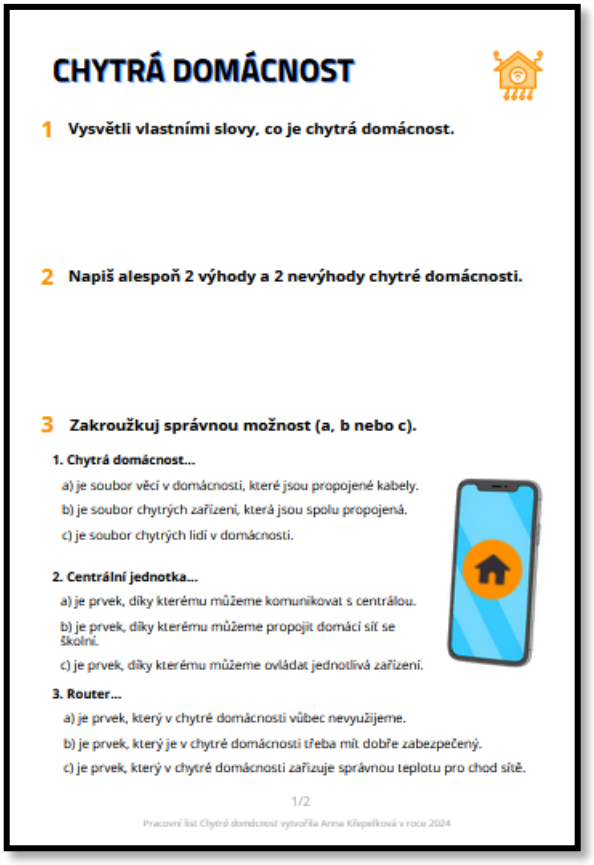


Obrázek 6: Ukázka z pracovního listu Zabezpečení počítačových sítí

V druhé části se nachází cvičení na zdůraznění důležitosti dodržování bezpečnostních opatření. Další úkol je na sepsání deseti tipů, které vychází z prvního úkolu, a tím si žák upevní znalost těchto opatření.

4.2.3 Pracovní list Chytrá domácnost

Pracovní list Chytrá domácnost má opět dvě části. První část obsahuje tři cvičení věnující se opakováním informací z výkladu a v druhé části úkoly, které se snaží zapojit žáky do úvah nad budoucností.



CHYTRÁ DOMÁCNOST

1 Vysvětli vlastními slovy, co je chytrá domácnost.

2 Napiš alespoň 2 výhody a 2 nevýhody chytré domácnosti.

3 Zakroužkuj správnou možnost (a, b nebo c).

1. Chytrá domácnost...
a) je soubor věcí v domácnosti, které jsou propojené kabely.
b) je soubor chytrých zařízení, která jsou spolu propojená.
c) je soubor chytrých lidí v domácnosti.

2. Centrální jednotka...
a) je prvek, díky kterému můžeme komunikovat s centrálou.
b) je prvek, díky kterému můžeme propojit domácí síť se školní.
c) je prvek, díky kterému můžeme ovládat jednotlivá zařízení.

3. Router...
a) je prvek, který v chytré domácnosti vůbec nevyužijeme.
b) je prvek, který je v chytré domácnosti třeba mít dobře zabezpečený.
c) je prvek, který v chytré domácnosti zařizuje správnou teplotu pro chod sítě.

1/2

Pracovní list Chytrá domácnost vytvořila Anna Křepelková v roce 2024

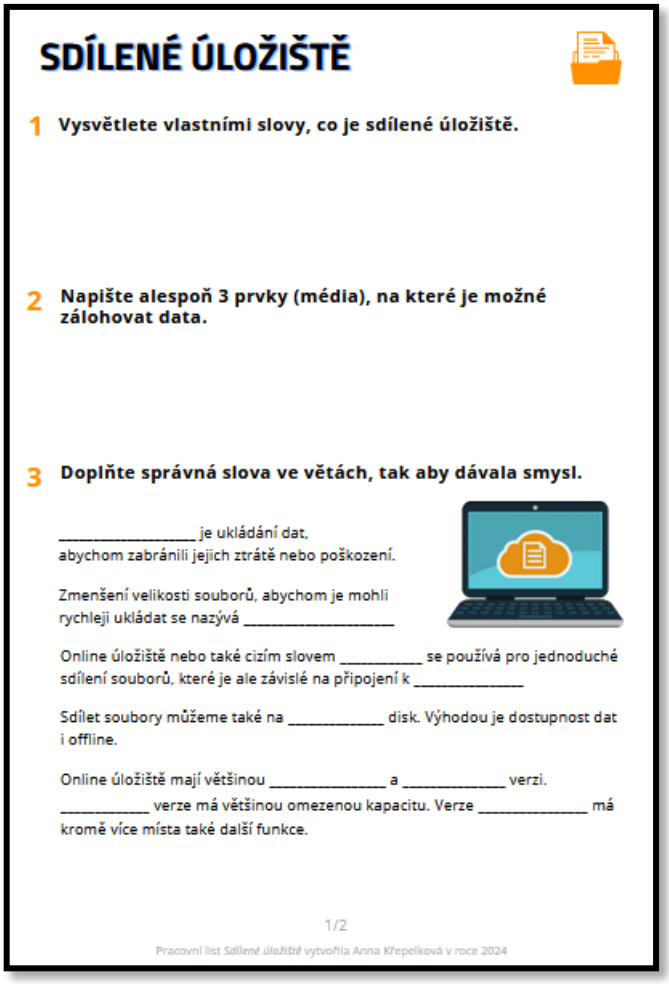
Obrázek 7: Ukázka z pracovního listu Chytrá domácnost

První cvičení v první části pracovního listu se zabývá tím, aby žáci vlastními slovy vyjádřili, co to je chytrá domácnost. V druhém cvičení žáci napíšou výhody a nevýhody chytré domácnosti. Třetí cvičení obsahuje zopakování pojmů z oblasti chytré domácnosti.

Druhá část má v prvním úkolu zadání, aby žáci napsali, zda mají doma chytrou domácnost, a které prvky a zařízení používají. Poslední úkol je na zamyšlení nad budoucností chytré domácnosti, který jim dovolí přemýšlet o různých funkcích a zařízeních a mohou se kreativně „vyřádit“.

4.2.4 Pracovní list Sdílené úložiště

Pracovní list na téma sdílené úložiště je určené pro dvojice žáků a má dvě části. První část se věnuje osvěžení paměti z výkladu a druhá část se věnuje rozboru a výběru nejvhodnějšího řešení sdílení úložiště pro domácí použití.



SDÍLENÉ ÚLOŽIŠTĚ

1 Vysvětlete vlastními slovy, co je sdílené úložiště.

2 Napište alespoň 3 prvky (média), na které je možné zálohovat data.

3 Doplňte správná slova ve větách, tak aby dávala smysl.

_____ je ukládání dat, abychom zabránili jejich ztrátě nebo poškození.

Zmenšení velikosti souborů, abychom je mohli rychleji ukládat se nazývá _____

Online úložiště nebo také cizím slovem _____ se používá pro jednoduché sdílení souborů, které je ale závislé na připojení k _____

Sdílet soubory můžeme také na _____ disk. Výhodou je dostupnost dat i offline.

Online úložiště mají většinou _____ a _____ verzi. _____ verze má většinou omezenou kapacitu. Verze _____ má kromě více místa také další funkce.

1/2

Pracovní list Sdílené úložiště vytvořila Anna Křepelková v roce 2024

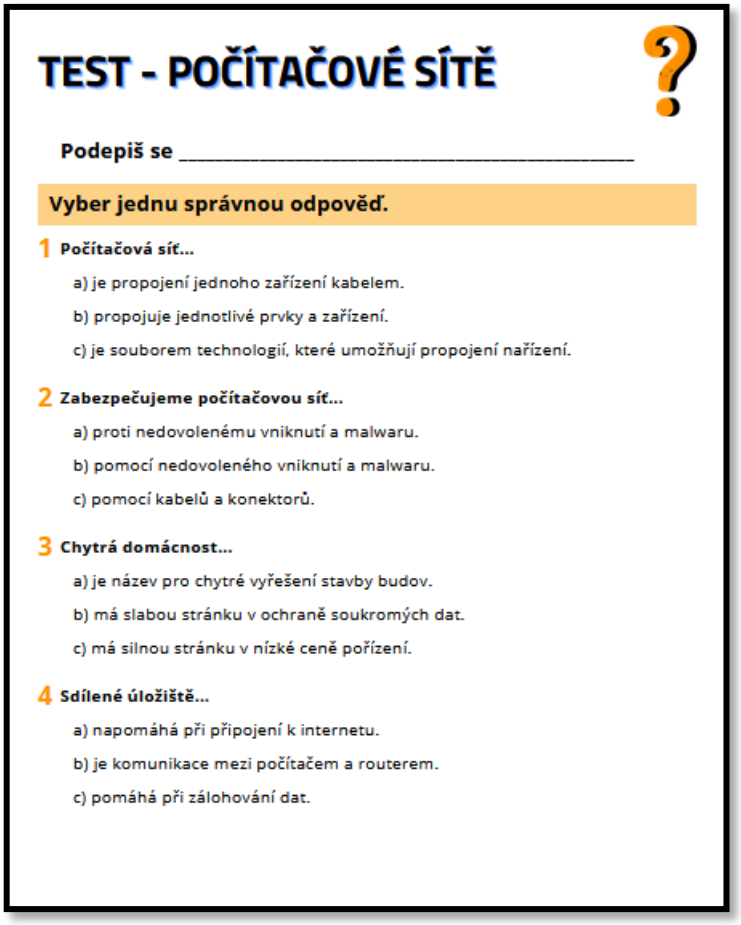
Obrázek 8: Ukázka z pracovního listu Sdílené úložiště

V prvním cvičení první části se žáci pokusí vyjádřit svou definici sdíleného úložiště. Další cvičení se zabývá zopakováním, na které prvky mohou zálohovat data. Třetí cvičení obsahuje osvěžení základních pojmů z výkladu.

Druhá část má dva úkoly. Prvním úkolem je, aby si žáci uvědomili, jestli používají sdílení souborů a zda sdílené úložiště využívají i doma. Ve druhém úkolu využijí žáci informace z internetu a zapíšou do tabulky jednotlivá řešení a jejich porovnání výhod, poté vyhodnotí řešení vhodné pro jejich domácnost.

4.3 Test

Test má celkem deset otázek, z toho devět je na pojmy z celého téma Počítačové sítě, tedy ze všech předchozích hodin. Desátá otázka je k tomu, aby žáci začali uvažovat i nad možnými následky, které mohou přijít s rychlým rozvojem technologie v domácnostech.



TEST - POČÍTAČOVÉ SÍTĚ

Podepiš se _____

Vyber jednu správnou odpověď.

1 Počítačová síť...

a) je propojení jednoho zařízení kabelem.

b) propojuje jednotlivé prvky a zařízení.

c) je souborem technologií, které umožňují propojení nařízení.

2 Zabezpečujeme počítačovou síť...

a) proti nedovolenému vniknutí a malwaru.

b) pomocí nedovoleného vniknutí a malwaru.

c) pomocí kabelů a konektorů.

3 Chytrá domácnost...

a) je název pro chytré vyřešení stavby budov.

b) má slabou stránku v ochraně soukromých dat.

c) má silnou stránku v nízké ceně pořízení.

4 Sdílené úložiště...

a) napomáhá při připojení k internetu.

b) je komunikace mezi počítačem a routerem.

c) pomáhá při zálohování dat.

Obrázek 9: Ukázka z testu na téma počítačové sítě

Otázky jedna až čtyři mají jen jednu odpověď a žáci musí zakroužkovat tu správnou. První otázka je o tom, jestli žáci ví, co je účelem počítačové sítě. Druhá otázka se týká definice zabezpečení počítačové sítě. Třetí otázka se zabývá chytrou domácností a jejím zabezpečením. Čtvrtá otázka se týká sdíleného úložiště a jeho funkcí.

Otázky pět až devět jsou otevřenými otázkami, u kterých mají žáci napsat správnou odpověď. Jedná se o otázky, které již v pracovních listech zodpovídali, takže by žáci neměli mít problém je zopakovat. Pátá otázka se zabývá třemi aktivními prvky, které byly zmíněny ve výkladu i pracovním listu. Účelem šesté otázky je zjistit, jestli si žáci pamatují pojem z bezpečnosti sítě. Sedmá otázka se týká téma chytrá domácnost a její prvky. V osmé otázce žáci vypisují prvky, na které se dá zálohovat, a devátá otázka se týká pojmu ze základů počítačových sítí.

Poslední otázka je koncipovaná jako zamyšlení se nad následky. Učitel ji může zařadit jako volitelnou otázku.

5 PŘÍPRAVA HODINY

Tematický celek počítačové sítě je určený na sedm vyučovacích hodin, přičemž jedna vyučovací hodina má 45 minut. Časový harmonogram se může měnit v závislosti na učiteli a šikovnosti samotných žáků. Navíc nejsou všechna témata stejně náročná na čas, takže se může stát, že v jedné vyučovací hodině se stihnou i dvě najednou. Pro podrobné informace o přípravě výuky byly vytvořeny metodické listy.

5.1 Metodické listy

Metodické listy pomáhají pedagogům zorientovat se v průběhu hodiny, které metody, kdy a jak použít. První dva metodické listy (Základy počítačových sítí, Zabezpečení počítačových sítí) jsou rozepsány na dvě vyučovací hodiny, ostatní listy jsou připraveny na jednu.

Každý metodický list má na začátku tabulku se základními informacemi, jako je jméno autora, datum vytvoření, téma vzdělávací oblasti apod.

Tabulka 3: Ukázka tabulky z prvního metodického listu

Autor výukového materiálu:	Bc. Anna Křepelková
Datum vytvoření:	1.4.2024
Cílová skupina (ročník):	9.ročník
Vzdělávací oblast:	Informatika
Téma:	Počítačové sítě – Základy počítačových sítí
Cíl:	Žáci umí definovat a vysvětlit, co je počítačová síť, analyzovat a posoudit počítačovou síť doma.
Časové vymezení:	2 vyučovací hodiny
Klíčové kompetence:	Kompetence k učení Kompetence k řešení problémů Kompetence komunikativní Kompetence pracovní
Podklady	1.Zaklady_pocitacovych_siti.pptx ukazka_domaci_sit.png 1.Pracovni_list-zaklady_pocitacovych_siti.pdf

Všechny metodické listy navíc začínají stručným představením tématu a účelu a nastíněním toho, co se za celou vyučovací hodinu bude dít. Následuje tabulka s přibližným časovým rozpisem a metodami. Další důležitou informací uvedenou v metodických listech jsou pomůcky, které k výuce budou učitelé potřebovat. Následuje konkrétní postup metod, které v hodině mají být použity, kde je uvedená metoda rozepsána do detailu. Další kapitolou je zhodnocení, ve kterém je shrnutí celé výuky a informace o navazujícím téma. Nakonec je v metodických listech uveden seznam zdrojů pro informace zmíněné ve výuce.

Metodické listy také obsahují správné odpovědi k otázkám v prezentacích, pracovních listech a testu.

5.1.1 První hodina – Základy počítačových sítí

K výuce je potřeba jen místnost s projektorem. Výuka začne úvodními formalitami, a poté krátkým úvodem do tématu. Následuje výklad pomocí powerpointové prezentace. V průběhu prezentace je možné odpovídat na otázky nebo debatovat na toto téma. Nakonec je prostor na zopakování a dotazy. Prezentace sestává z celkem čtrnácti slidů. Následuje shrnutí a ukončení hodiny.

V první hodině se žáci dozvěděli, co je počítačová síť, jaká zařízení v ní mohou komunikovat, jak takové zapojení může vypadat, dozvěděli se něco o prvcích v počítačové síti a vědí, jak se v síti komunikuje všeobecně. Další hodina je věnovaná procvičováním toho, co si žáci zapamatovali, a mohli zanalyzovat svou domácí síť pomocí pracovního listu.

5.1.2 Druhá hodina – Základy počítačových sítí – cvičení

K výuce je potřeba jen vytisknout pracovní listy (každý žák jeden pracovní list) a popř. místnost s projektorem na ukázání příkladu domácí sítě.

Výuka nejprve začne úvodními formalitami, a poté krátkým zopakováním tématu. Následuje představení pracovního listu a zadání úkolů. První část pracovního listu je rychlé zopakování úvodu prezentace. Druhá část už souvisí s procvičením a aplikací poznatků na svou domácí počítačovou síť. Výsledky pak žáci prezentují celé třídě.

V této hodině si žáci připomněli informace z minulé hodiny a navázali na to vyplňováním pracovních listů, které jim umožní spojit si vědomosti s něčím, co doma denně používají.

Na začátku příští hodiny je zajímavé se žáků zeptat, zda nějak změnili pohled na svou domácí počítačovou síť.

Další hodina je věnovaná zabezpečením těchto domácích počítačových sítí.

5.1.3 Třetí hodina – Zabezpečení počítačových sítí

K výuce je potřeba jen místnost s projektorem.

Výuka nejprve začne úvodními formalitami, a poté krátkým úvodem do tématu. Následuje výklad s pomocí powerpointové prezentace. V průběhu prezentace je možné odpovídat na otázky nebo debatovat na toto téma. Nakonec je prostor na zopakování a dotazy. Prezentace je složená ze čtrnácti slidů.

V první hodině se žáci dozvěděli o tom, co je zabezpečení počítačové sítě, jaké hrozby mohou očekávat a napadnout, jak se hrozbám bránit. Dozvěděli se něco o základních pojmech v rámci zabezpečení sítě.

Další hodina je věnovaná procvičováním toho, co si žáci zapamatovali a mohli lépe zabezpečit svou domácí síť.

5.1.4 Čtvrtá hodina – Zabezpečení počítačových sítí – cvičení

K výuce je potřeba jen vytisknout pracovní listy (každý žák jeden pracovní list).

Výuka nejprve začne úvodními formalitami, a poté krátkým zopakováním tématu. Následuje představení pracovního listu a zadání úkolů. První část pracovního listu je rychlé zopakování úvodu prezentace. Pro ušetření času je možné rozdělit žáky do dvojic a zadat, ať si navzájem opraví odpovědi. Správné odpovědi pak odhalí společně celá třída. Druhá část už souvisí s procvičením a aplikací poznatků na svou domácí počítačovou síť. Výsledky pak prezentují třídě.

V této hodině si žáci připomněli informace z minulé hodiny a navázali na to vyplňováním pracovních listů, které jim umožní spojit si vědomosti s něčím, co doma denně používají.

Na začátku další hodiny je zajímavé se zeptat, zda se začali řídit radami, které zazněly v minulé hodině.

Další hodina je věnovaná chytré domácnosti jako nejnovějšímu trendu moderní doby.

5.1.5 Pátá hodina – Chytrá domácnost

K výuce je potřeba jen místnost s projektorem.

Výuka nejprve začne úvodními formalitami, a poté krátkým úvodem do tématu. Následuje výklad pomocí powerpointové prezentace. Prezentace sestává z deseti slidů. Poté žáci budou pracovat s pracovními listy. V průběhu hodiny je možné odpovídat na otázky nebo debatovat na toto téma. Nakonec je prostor na zopakování a dotazy.

V první hodině se žáci dozvěděli o tom, co je chytrá domácnost, které prvky a zařízení může obsahovat, jaké hrozby ji mohou napadnout a jak se hrozbám bránit. Poté se žáci věnovali procvičováním toho, co si zapamatovali, aby lépe porozuměli výhodám i nástrahám, které chytré domácnosti ovlivňují.

Na začátku další hodiny je zajímavé se zeptat, zda se něco změnilo v jejich vnímání své (chytré) domácnosti.

Další hodina je věnovaná sdílenému úložišti.

5.1.6 Šestá hodina – Sdílené úložiště

K výuce je potřeba místnost s projektorem, vytisknuté pracovní listy (do každé dvojice žáků jeden pracovní list) a přístup k internetu.

Výuka nejprve začne úvodními formalitami, a poté krátkým úvodem do tématu. Následuje výklad pomocí powerpointové prezentace. V průběhu prezentace je možné odpovídat na otázky nebo debatovat na toto téma. Nakonec je prostor na zopakování a dotazy. V druhé části výuky žáci začnou ve dvojicích vyplňovat pracovní listy. V první části pracovního listu si zopakují pojmy z tématu sdílené úložiště a poté zanalyzují možnosti a vyberou jedno nejvhodnější sdílené úložiště pro jejich domácnost.

V první části hodiny se žáci pomocí prezentace dozvěděli, co je sdílené úložiště, co je zálohování, jaké druhy existují a jejich výhody a nevýhody. Druhá část hodiny byla věnovaná upevnění znalostí pomocí pracovního listu ve dvojicích. Žáci zde měli možnost zanalyzovat pozitiva a negativa jednotlivých řešení, vybrat si jedno a obhájit si svůj výběr.

Další hodina je věnovaná zopakováním si celého téma a ověřením znalostí pomocí testu.

5.1.7 Sedmá hodina – Opakování, test

K výuce je potřeba (interaktivní) tabule a vytištěné testy.

Na začátku hodiny doporučuji krátké zopakování látky pomocí didaktické hry Domino na téma Počítačové sítě. Učitel zadá žákům téma Domácí počítačové sítě a žáci postupně chodí k tabuli a zapisují jednotlivé názvy, které souvisí s tématem. Nakonec učitel zhodnotí a

doplní informace. Ve druhé části hodiny žáci vyplňují testy, které naznačily, kolik si toho žáci zapamatovali.

Systém hodnocení testu záleží na samotném učiteli.

Závěrečným testem je uzavřené celé téma počítačových sítí.

6 OVĚŘENÍ FUNKČNOSTI ŘEŠENÍ

Funkčnost řešení byla ověřena pomocí vyzkoušením přímo ve výuce a hodnocením učitele informatiky, který byl ve výuce přítomen. Z důvodu nedostatku času byla vyzkoušena jedna vyučovací hodina. Okomentování dalších materiálů bylo tedy jen pomocí pedagogových zkušeností. Testování proběhlo na Základní škole Čáslav, Masarykova v devátém ročníku.

6.1 Hodnocení pedagoga

“Prezentace jsou pěkně zpracované: mají obrázky, úkoly a kontrolní otázky, takže do výkladu jsou zapojeni i žáci. Oceňuji hodně obrázků a málo textu. Také se mi líbilo využití interaktivní tabule a kreslení přímo v prezentaci. Příště by to chtělo prezentaci trochu zkrátit, aby nebyla na celou vyučovací hodinu a přidat nějakou další aktivitu. Ostatní prezentace jsou kratší, takže délka je vhodnější a je z čeho vybírat.

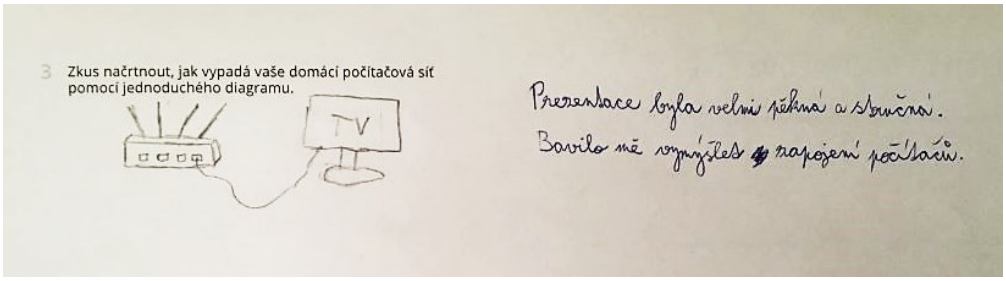
Na pracovních listech se mi líbí, že mají jednu část na zopakování toho, co žáci mohli slyšet ve výkladu a druhou část na rozvíjení tématu. Cvičení v pracovních listech jsou různorodá a doplněná o ilustrační obrázky. Jen při zadávání cvičení bylo potřeba zdůraznit celé zadání, protože žáci si je často nepřečetli.

Test má různé druhy otázek a jsou podobné těm v pracovních listech, takže žáci mají větší šanci odpovědět správně. Otázka na zamyšlení v testu je zajímavý nápad, ale bude se velmi těžko hodnotit odpověď.

Výukové materiály celkově dobře zpracované a žákům zpestří výuku.”

6.2 Hodnocení žáků

Žákům se hodina převážně líbila a bavilo je to. Prezentace pro ně byla přehledná a stručná. Úkol s propojováním je zaujal a díky interaktivní tabuli se stali součástí prezentace. Některým žákům se líbilo to, že měli možnost vidět vzorky optického kabelu a některým žákům se zase nelíbilo, že v prezentaci bylo hodně názvů, které se budou muset naučit. Navazující pracovní list byl také změnou oproti klasické výuce informatiky. Žáky zaujal úkol nakreslit svou počítačovou síť.



Obrázek 10: Ukázka z vyplněného pracovního listu Základy počítačových sítí s hodnocením

7 ZHODNOCENÍ VÝUKOVÉHO PROJEKTU

Výukový projekt se zaměřuje na téma počítačových sítí, které žáci na druhém stupni musí probrat. Vyhodnocení silných a slabých stránek je důležité pro tuto práci.

7.1 Silné stránky

Tematický celek Počítačové sítě má dobře promyšlená a aktuální témata. Prezentace a pracovní listy jsou dobře propojené a úkoly, kterými žáci procvičují znalosti, mají dobrou myšlenku. Žákům se líbily úkoly v prezentaci i pracovním listu. Prezentace mají správný tvar – obrázky, video a texty přiměřené, jednotnou úpravu a byly použity přechody a animace. Pracovní listy obsahují variabilní druhy cvičení a přidané obrázky je zpřehledňují. Zapojení didaktické hry pro zopakování učiva je nápad, který pomůže hravou formou zopakovat probranou látku. Test má přiměřený počet otázek na takovéto téma.

Bylo vytvořeno celkem asi deset výukových materiálů, ze kterých je možné si vybírat. K těmto materiálům bylo vytvořeno i pět metodických listů, které osvětlují přípravu hodiny, časový rozvrh a rozepisují jednotlivé metody. V metodických materiálech je rozepsán výklad a správné odpovědi v pracovních listech a testu.

7.2 Slabé stránky

Prezentace a pracovní listy na téma Chytrá domácnost a Sdílené úložiště jsou příliš náročné na čas, takže by bylo potřeba je zredukovat. Materiály na další hodiny je potřeba otestovat ve výuce, aby se k nim žáci mohli vyjádřit. Úkol v pracovním listu Základy počítačových sítí nepochopili žáci jako provázanost s předchozím úkolem na vyjmenování aktivních a pasivních prvků, takže je třeba některá zadání přeformulovat.

7.3 Budoucí změny

Pro příště bude lepší přidat více druhů výukových metod a zkrátit prezentace, aby byly přiměřenější. Dále je třeba přehodnotit formulace jednotlivých úkolů a cvičení.

ZÁVĚR

Počítačové sítě se používají dnes a denně a jsou nedílnou součástí moderního života. Domácí počítačové sítě začaly s příchodem prvních dostupných osobních počítačů. Od té doby se počet zařízení v domácnosti jen zvyšuje.

Zabezpečení domácích sítí a zařízení není vhodné brát na lehkou váhu. Mnoho uživatelů si neuvědomuje, že zařízení o svých uživatelích sbírají informace o nákupech, návycích, osobních dokumentech, účtech a mnoho dalšího. Následky nezabezpečené domácí sítě si tak nemusí uvědomit, dokud není pozdě a data jsou nenávratně poškozená, zničená nebo unikla na internet.

Mladá generace se učí už od raného dětství ovládat taková zařízení. Děti na počítačových sítí často závisí, ale neví, jak fungují, proto je potřeba jim přiblížit, co to je, jejich účel, funkce a jaké nástrahy na ně mohou číhat.

Účelem vytvořených materiálů je v rámci výuky informatiky vysvětlit základní informace o počítačových sítích a naučit žáky důležitost bezpečného chování a zásad při pohybování se na sítích.

Škola má však omezený počet hodin, které může přidělit na určité téma, takže je důležité naučit žáky to nejdůležitější a motivovat je, aby se o počítačové sítě zajímali a našli si další informace sami. To není jednoduché bez pomoci příprav a výukových materiálů, které jsou k dispozici i ostatním učitelům. V předmětu informatika však takové materiály, především se zaměřením na počítačové sítě, chybí nebo jsou nedostatečné. To mají tyto materiály částečně vyřešit.

Byly vytvořené materiály na téma pokrývající základy počítačových sítích a aktuální témata jako je bezpečnost těchto sítí, chytrá domácnost a sdílené úložiště. Žáci se dozvědí základní pojmy počítačových sítí, se kterými se pak pracují v navazujících praktických úkolech. V těchto úkolech se zamyslí, jak vypadá jejich domácí počítačová síť a jak s tím pracovat i nadále. Tipy pro zabezpečení sítí se dozví ve stejnojmenné prezentaci a pracovní listy nabízejí upevnění těchto bezpečnostních opatření. Chytrá domácnost a sdílené úložiště jsou zajímavá témata, která však materiály probírají jen okrajově. Nakonec se výuka uzavře závěrečným zopakováním pojmů pomocí didaktické hry a napsáním didaktického testu.

Výukové materiály pokrývají téma pomocí prezentací, pracovních listů a testu pro ověření znalostí a uzavření tematického okruhu.

SEZNAM POUŽITÉ LITERATURY

[1] ČAPEK, Robert. Moderní didaktika: Lexikon výukových a hodnoticích metod. Praha: Grada, 2015. ISBN 978-80-247-3450-7.

[2] ČÍKA, Petr, 2017. Internet věcí pro inteligentní domácnost: Internet of things for smart home: zkrácená verze habilitační práce. Brno: Vysoké učení technické v Brně, nakladatelství VUTIUM. ISBN 978-80-214-5559-7.

[3] DÖMISCHOVÁ, Ivona. Projektová výuka: Moderní strategie vzdělávání v České republice a německy mluvících zemích. Olomouc: Univerzita Palackého v Olomouci, 2011. ISBN 9788024429151.

[4] *Didaktika informatiky*, 2022. Online. Wikipedia. Dostupné z: https://cs.wikipedia.org/wiki/Didaktika_informatiky. [cit. 2022-10-23].

[5] NÁRODNÍ ÚŘAD PRO KYBERNETICKOU A INFORMAČNÍ BEZPEČNOST [NÚKIB]. Doporučení k ochraně počítačů a chytrých zařízení v domácnosti. Online. Dostupné z: https://nukib.gov.cz/cs/infoservis/doporuceni/1512-ochrante-svuj-domov-proti-hackerum/. [cit.2023-11-14].

[6] Informační společnost v číslech. Online. 2020, č. 061004-20. Praha: ČSÚ, 2020. Dostupné z: https://www.czso.cz/csu/czso/informacni-spolecnost-v-cislech-2020. [cit. 2024-03-01].

[7] *Počítačové sítě*. Online. Khan Academy. 2024. Dostupné z: https://cs.khanacademy.org/computing/informatika-pocitace-a-internet/x8887af37e7f1189a:internet/x8887af37e7f1189a:site-a-jejich-propojovani/a/computer-networks-overview. [cit. 2024-05-06].

[8] *Počítačové sítě*. Online. Umíme informatiku. 2024. Dostupné z: https://www.umimeinformatiku.cz/book/cviceni-pocitacove-site. [cit. 2024-05-06].

[9] NOVÁČEK, Šimon. *Lekce 1 - Sítě - Typy používaných sítí Zdroj: https://www.itnetwork.cz/site/zaklady/site-typy-pouzivanych-siti*. Online. Itnetwork.cz. 20n. l. Dostupné z: https://www.itnetwork.cz/site/zaklady/site-typy-pouzivanych-siti. [cit. 2024-05-06].

[10] *Co je topologie sítě v počítačových sítích*. Online. Etechblog.cz. 2024. Dostupné z: https://etechblog.cz/co-je-topologie-site-v-pocitacovych-sitich/. [cit. 2024-05-06].

[11] *Počítačové sítě*. Online. Učse online.cz. 2024. Dostupné z: https://www.ucseonline.cz/skola/zakladni-skola/skolni-zapisky/informatika/pocitacove-site/. [cit. 2024-05-05].

[12] *IP adresy a DNS*. Online. Khan Academy. Dostupné z: https://cs.khanacademy.org/computing/informatika-pocitace-a-internet/x8887af37e7f1189a:internet/x8887af37e7f1189a:ip-adresy/a/ip-v4-v6-addresses [cit. 2024-05-06].

[13] *IP adresa: Co to je IP adresa a jak zjistím svoji IP adresu*. Online. SEO akademie Collabim. 2023. Dostupné z: https://www.collabim.cz/akademie/knihovna/ip-adresa-co-to-je-ip-adresa-a-jak-zjistim-svoji-ip-adresu/. [cit. 2024-05-05].

[14] NOVÁČEK, Šimon. *Lekce 2 - Sítě - Typy síťových zařízení Zdroj: https://www.itnetwork.cz/site/zaklady/site-typy-pouzivanych-siti*. Online. Itnetwork.cz. 20n. l. Dostupné z: https://www.itnetwork.cz/site/zaklady/site-typy-sitovych-zarizeni [cit. 2024-05-06].

[15] *Pasivní síťové prvky (Passive Networking Components)*. Online. ManagementMania.com. 2018. Dostupné z: https://managementmania.com/cs/pasivni-sitove-prvky. [cit. 2024-05-08].

[16] *Co je to Bluetooth?* Online. IT slovník.cz. Dostupné z: https://it-slovnik.cz/pojem/bluetooth. [cit. 2024-05-08].

[17] Co je NFC? Online. *Alza.cz*. 2024. Dostupné z: https://www.alza.cz/co-je-nfc. [cit. 2024-05-08].

[18] *Síťové zařízení*. Online. Wikipedie. 2023. Dostupné z: https://cs.wikipedia.org/wiki/S%C3%AD%C5%A5ov%C3%A9_za%C5%99%C3%ADzen%C3%AD. [cit. 2024-05-08].

[19] *Co je zabezpečení sítě? Jak to funguje a proč je to důležité*. Online. Etechblog.cz. 2023. Dostupné z: https://etechblog.cz/co-je-zabezpeceni-site-jak-to-funguje-a-proc-je-to-dulezite/. [cit. 2024-05-05].

[20] *What is network security?* Online. IBM. Dostupné z: https://www.ibm.com/topics/network-security. [cit. 2024-05-05].

[21] *Kybernetická bezpečnost (kyberbezpečnost). Definice, význam, řízení, povinnosti a legislativa*. Online. Legislativa. 2022. Dostupné z: https://legislativa.cz/zdroje/kyberneticka-bezpecnost/kyberbezpecnost#cap4. [cit. 2024-05-08].

[22] *Co je malware?* Online. Eset. Dostupné z: https://www.eset.com/cz/malware/. [cit. 2024-05-05].

[23] Kybernetická bezpečnost: Hlavní a nově se objevující hrozby. Online. *Témata – Evropský parlament*. 2022. Dostupné z: https://www.europarl.europa.eu/topics/cs/article/20220120STO21428/kyberneticka-bezpecnost-hlavni-a-nove-se-objevujici-hrozby. [cit. 2024-05-08].

[24] *Kdo je hacker?* Online. Eset. Dostupné z: https://www.eset.com/cz/hacker/. [cit. 2024-05-05].

[25] *What is Hacking?* Online. Fortinet. 2024. Dostupné z: https://www.fortinet.com/resources/cyberglossary/what-is-hacking. [cit. 2024-05-05].

[26] *Co je antivirus?* Online. Eset. Dostupné z: https://www.eset.com/cz/antivirus-software/. [cit. 2024-05-05].

[27] ČERNÁ, Jana. Nejlepší antivir pro rok 2024. Online. In: *Všeuměl*. Dostupné z: https://www.vseumel.cz/antiviry-recenze/. [cit. 2024-05-05].

[28] *Co to je VPN?* Online. Eset. Dostupné z: https://www.eset.com/cz/vpn/#co-je-vpn. [cit. 2024-05-05].

[29] *Co je brána firewall?* Online. Eset. Dostupné z: https://www.eset.com/cz/firewall/. [cit. 2024-05-05].

[30] ROMANOVA, Michaela. *Chytrá domácnost: Co všechno umí a jaké jsou její výhody*. Online. TIPIO. 2022. Dostupné z: https://www.tipio.cz/chytra-domacnost/#Vyhody_chytre_domacnosti. [cit. 2024-05-05].

[31] MARTIN, Ricky. *IoT-Powered Smart Homes – A Whole New Level of Comfort and Control*. Online. MyTechMag. Dostupné z: https://www.mytechmag.com/iot-powered-smart-homes-a-whole-new-level-of-comfort-and-control/. [cit. 2024-05-05].

[32] *Smart domácnost – co to je a jak na ni?* Online. Deliving.cz. 2021. Dostupné z: https://www.deliving.cz/smart-domacnost-co-to-je-a-jak-na-ni/#Ovladani_smart_domacnosti. [cit. 2024-05-05].

[33] HERWIG, Bohumil. Co to je a jak funguje chytrý dům, chytrý byt a chytrá domácnost? Online. In: . Lupa.cz. Dostupné z: https://www.lupa.cz/clanky/co-to-je-a-jak-funguje-chytry-dum-chytry-byt-a-chytra-domacnost/. [cit. 2024-05-05].

[34] *Co je IoT?* Online. Eset. Dostupné z: https://www.eset.com/cz/iot/. [cit. 2024-05-05].

[35] Chytrá, ale bezpečná domácnost. Online. *CHIP*. 2017. Dostupné z: https://www.chip.cz/chytra-ale-bezpecna-domacnost. [cit. 2024-05-08].

[36] VINCE, Jan. Zálohování dat: věnujte mu pár desítek minut a budete mít klid na X let dopředu. Online. Digitální pevnost. 2019. Dostupné z: https://www.digitalnipevnost.cz/zpravodaj/detail/zalohovani-dat. [cit. 2024-05-05].

[37] RAYAPROLU, Aditya. What Is External Storage? [The Only Guide You'll Ever Need]. Online. *Techjury*. Roč. 2023. Dostupné z: https://techjury.net/blog/what-is-external-storage/. [cit. 2024-05-05].

[38] NAS úložiště. Online. In: Akademie IT, 2024. Dostupné z: https://akademieit.cz/nas-uloziste/. [cit. 2024-05-05].

[39] Zálohování dat (NÁVOD). Online. *Alza.cz*. Dostupné z: https://www.alza.cz/zalohovani-dat. [cit. 2024-05-08].

[40] Co je to cloud? Definice, výhody a využití v praxi. Online. In: . IPodnikatel.cz, 2023. Dostupné z: https://www.ipodnikatel.cz/co-je-to-cloud-definice-vyhody-a-vyuziti-v-praxi/. [cit. 2024-05-05].

[41] VALIŠOVÁ, Alena KOVAŘÍKOVÁ, Miroslava. Obecná didaktika. 2021. ISBN 978-80-271-3249-2.

[42] SCHINDLER, Radek. *Rukověť autora testových úloh*. Centrum pro zjišťování výsledků vzdělávání, 2006. ISBN 80-239-7111-5.

[43] *Bloom's Taxonomy*. Online. Vanderbilt University. 2001. Dostupné z: https://cft.vanderbilt.edu/guides-sub-pages/blooms-taxonomy/. [cit. 2024-05-08].

[44] ČESKÁ REPUBLIKA. Opatření ministra školství, mládeže a tělovýchovy, kterým se mění Rámcový vzdělávací program pro základní vzdělávání. In: . 2021, s. 174. Dostupné také z: https://www.msmt.cz/file/56005/

[45] NORD SECURITY. *Top 200 Most Common Passwords*. Online. NORD SECURITY. NordPass. 2023. Dostupné z: https://nordpass.com/most-common-passwords-list/. [cit. 2024-05-04].

[46] FIŠAROVÁ, Gabriela. Didaktické cíle (klasifikace, formulace, práce s cíli ve výuce). Online. In: . Brno: MUNI, 2008, s. 8. Dostupné z: https://is.muni.cz/el/1421/jaro2008/DPS003/um/4429574/didakticke_cile.pdf. [cit. 2024-05-06].

[47] NOVOTNÝ, Miloš a KRÁTKÁ, Markéta. Didaktická hra domino: řada vyjmenovaných slov po p. Online. In: *Metodický portál RVP.cz*. Npi, 2008, s. 5. ISSN 1802–4785. Dostupné z: https://dum.rvp.cz/materialy/didakticka-hra-domino-rada-vyjmenovanych-slov-po-p.html. [cit. 2024-05-07].

[48] Online. 2024. Dostupné z: https://www.canva.com/. [cit. 2024-05-06].

SEZNAM POUŽITÝCH SYMBOLŮ A ZKRATEK

CD/DVD	Compact Disc / Digital Versatile Disc.
DNS	Domain Name System.
GB	Gigabyte
HDD	Hard Disc Drive
IoT	Internet of Things
IP	Internet Protocol
IPv4	Internet Protocol version 4
IPv6	Internet Protocol version 6
IrDA	Infrared Data Association
LAN	Local Area Network
MAC	Media Access Control
MAN	Metropolitan Area Network
NAS	Network Attached Storage
NFC	Near Field Communication
PAN	Personal Area Network
PIN	Personal Identification Number
RAR	Roshal Archive
RVP	Rámcový vzdělávací program
SSD	Solid-State Drive
USB-C	Universal Seriál Bus – Type C
VPN	Virtual Private Network
WAN	Wide Area Network
WEP	Wired Equivalent Privacy
Wi-Fi	Wireless Fidelity

WLAN Wireless LAN

WPA2 Wireless Protected Access 2

ZIP

SEZNAM OBRÁZKŮ

Obrázek 1: Ukázka obsahu prezentace Základy počítačových sítí.....35
Obrázek 2: Ukázka obsahu z prezentace na téma Zabezpečení počítačových sítí 36
Obrázek 3: Ukázka obsahu prezentace Chytrá domácnost.....37
Obrázek 4: Ukázka obsahu prezentace Sdílené úložiště.....37
Obrázek 5: Ukázka z pracovního listu Základy počítačových sítí.....38
Obrázek 6: Ukázka z pracovního listu Zabezpečení počítačových sítí 40
Obrázek 7: Ukázka z pracovního listu Chytrá domácnost.....41
Obrázek 8: Ukázka z pracovního listu Sdílené úložiště 42
Obrázek 9: Ukázka z testu na téma počítačové sítě.....43
Obrázek 10: Ukázka z vyplněného pracovního listu Základy počítačových sítí s hodnocením.....50

SEZNAM TABULEK

Tabulka 1: Ukázka nejčastějších hesel v ČR v roce 2023 [16] 19
Tabulka 2: Ukázka tabulky z prvního metodického listu 44

SEZNAM PŘÍLOH

Příloha P I: Obsah CD

PŘÍLOHA P I: OBSAH CD

fulltext.pdf

Prezentace

- 1.Zaklady_pocitacovych_siti.pptx
- 2.Zabezpeceni_pocitacovych_siti.pptx
- 3.Chytra_domacnost.pptx
- 4.Sdilene_uloziste.pptx

Pracovni_listy

- 1.Pracovni_list-pocitacove_site.pdf
- 2.Pracovni_list-zabezpeceni_siti.pdf
- 3.Pracovni_list-chytra_domacnost.pdf
- 4.Pracovni_list-sdilene_uloziste.pdf
- Domino-zakladni_pojmy_pocitacove_site.pdf
- Test-pocitacove_site.pdf
- ukazka_domaci_sit.png

Metodicke_listy

- 1.Metodicky_list-pocitacove_site.docx
- 2.Metodicky_list-zabezpeceni_pocitacovych_siti.docx
- 3.Metodicky_list-chytra_domacnost.docx
- 4.Metodicky_list-sdilene_uloziste.docx
- 5.Metodicky_list-test.docx