

**MATEMATICKO-FYZIKÁLNÍ
FAKULTA**
Univerzita Karlova

DIPLOMOVÁ PRÁCE

Bc. Adam Papula

Výukový modul o fungování internetu pro střední školy

Katedra softwaru a výuky informatiky

Vedoucí diplomové práce: doc. Mgr. Cyril Brom, Ph.D.

Studijní program: Učitelství matematiky pro střední
školy

Praha 2026

Prohlašuji, že jsem tuto diplomovou práci vypracoval(a) samostatně a výhradně s použitím citovaných pramenů, literatury a dalších odborných zdrojů. Beru na vědomí, že se na moji práci vztahují práva a povinnosti vyplývající ze zákona č. 121/2000 Sb., autorského zákona v platném znění, zejména skutečnost, že Univerzita Karlova má právo na uzavření licenční smlouvy o užití této práce jako školního díla podle §60 odst. 1 autorského zákona.

V dne

Podpis autora

Na tomto místě bych chtěl v první řadě velmi poděkovat svému vedoucímu práce, doc. Mgr. Cyrilovi Bromovi, Ph.D., za odborné vedení, podnětné připomínky a trpělivost, se kterou přistupoval k mým dotazům v průběhu celého výzkumu.

Mé poděkování dále patří Mgr. Lence Forstové za řadu cenných odborných podnětů a inspirativní diskuse, které mi pomohly při tvorbě a ladění výukového modulu.

Děkuji také všem vyučujícím informatiky na středních školách, kteří mi umožnili realizovat výzkumné šetření ve svých třídách a poskytli mi nezbytné zázemí pro testování. Bez jejich ochoty a vstřícného přístupu by nebylo možné praktickou část této práce realizovat.

Název práce: Výukový modul o fungování internetu pro střední školy

Autor: Bc. Adam Papula

Katedra: Katedra softwaru a výuky informatiky

Vedoucí diplomové práce: doc. Mgr. Cyril Brom, Ph.D., Katedra softwaru a výuky informatiky

Abstrakt: Diplomová práce reaguje na revizi Rámcového vzdělávacího programu a s ní související nedostatek materiálů pro výuku počítačových sítí. Cílem práce je navrhnout, otestovat a poskytnout kompletní sadu výukových materiálů pro čtyřhodinový konstruktivistický modul. Práce se zaměřuje na žáky 1. a 2. ročníku středních škol, ovšem v rámci testování byla ověřována kognitivní přístupnost i v nižších ročnících víceletých gymnázií. Modul pokrývá témata bezdrátových sítí, přenosu dat, bezpečnosti a internetu věcí s důrazem na aktivní zapojení žáků.

Teoreticky se práce opírá o konstruktivismus a model E-U-R, které doplňují dva v tomto kontextu méně známé přístupy: rámec konceptuální změny a model výukové rekonstrukce. Modul byl iterativně vylepšován a pilotován na sedmi školách. Aby byla ověřena spodní hranice kognitivní přístupnosti, byl modul testován v širším věkovém spektru, přičemž celková úspěšnost a chybovost žáků byla vyhodnocována za celý výzkumný vzorek jako celek.

Kvantitativní analýza dat potvrdila pozitivní vliv modulu na znalosti žáků. Porovnání pre-testů a post-testů prokázalo statisticky významný nárůst vědomostí se silným účinkem ($d = 1,85$, $p < 0,001$, $N = 154$). Retence znalostí byla potvrzena odloženými testy, kde si žáci i přes přirozený pokles udrželi výrazně lepší výsledky než před zahájením výuky ($d = 1,27$, $p < 0,001$, $n = 99$). Z pozorování během výuky vyplynulo, že pro žáky tercií víceletých gymnázií je látka již na hranici srozumitelnosti a vyžaduje od vyučujícího větší dopomoc a delší čas. Výstupem práce jsou prakticky ověřené materiály připravené k přímému nasazení ve výuce.

Klíčová slova: internet, Wi-Fi, kyber-bezpečnost, střední školy, výuka, modelové hodiny, informatika

Title: Lessons about functioning of the internet for upper secondary schools

Author: Bc. Adam Papula

Department: Department of Software and Computer Science Education

Supervisor: doc. Mgr. Cyril Brom, Ph.D., Department of Software and Computer Science Education

Abstract: This thesis responds to the revision of the Framework Educational Programme and the subsequent shortage of teaching materials for computer networking education. The aim of the work is to design, test, and provide a comprehensive set of teaching materials for a four-hour constructivist module. Although the primary focus is on students in the 1st and 2nd years of upper secondary schools, the testing also verified cognitive accessibility in the lower grades of multi-year grammar schools. The module covers topics such as wireless networks, data transmission, security, and the Internet of Things (IoT), with an emphasis on active student engagement.

Theoretically, the work is grounded in constructivism and the E-U-R model (Evocation-Understanding-Reflection), supplemented by two approaches less common in this context: the Conceptual Change Framework and the Model of Educational Reconstruction. The module was iteratively improved and piloted at seven schools. To verify cognitive accessibility and the lower limit of difficulty, testing was conducted across a broader age spectrum, monitoring students' overall success and error rates across the entire research sample as a whole.

Quantitative data analysis confirmed the positive impact of the module on students' knowledge. A comparison of pre-tests and post-tests demonstrated a statistically significant increase in knowledge with a strong effect size ($d = 1,85$, $p < 0,001$, $N = 154$). Knowledge retention was confirmed by delayed tests, where students maintained significantly better results than before the instruction, despite a natural decline ($d = 1,27$, $p < 0,001$, $n = 99$). Observations during lessons revealed that for students in the third year of eight-year grammar schools (tercie), the subject matter is on the verge of comprehensibility and requires greater teacher support and more time. The output of this work consists of practically tested materials ready for direct implementation in teaching.

Keywords: internet, Wi-Fi, cyber-security, upper secondary schools, education, model lessons, computer science

Obsah

Úvod	9
I Teoretická část	11
1 Didaktická a pedagogická východiska	12
1.1 Konstruktivismus a konceptuální změna	12
1.2 Výuka prostřednictvím analogií a modelů	12
1.3 Model výukové rekonstrukce a E-U-R	13
2 Informatika v kurikulu a analýza dostupných zdrojů	16
2.1 Revize RVP pro střední školy a obsahové vymezení	16
2.1.1 Prerekvizity ze ZŠ a požadavky na středoškolské vzdělávání	16
2.1.2 Kurikulární návaznost a reálný stav	17
2.1.3 Časové vymezení a organizace výuky	18
2.2 Analýza a srovnání dostupných materiálů	18
2.2.1 Metodika analýzy a kritéria výběru zdrojů	18
2.2.2 Absence tématu v nových publikacích a na metodických portálech	19
2.2.3 Online materiály pro nové RVP	21
2.2.4 Inovativní materiály pro nižší stupně vzdělávání	23
2.2.5 Výhled a připravované publikace	26
2.3 Identifikace didaktického problému	26
2.4 Teoretická východiska výzkumu	27
2.4.1 Konstrukční výzkum	28
2.4.2 Akční výzkum a role učitele-výzkumníka	29
2.5 Formativní hodnocení jako nástroj ověřování	29
II Praktická část	31
3 Návrh a popis výukového modulu	32
3.1 Výběr a didaktická redukce učiva	32
3.1.1 Tematická struktura a posloupnost modulu	33
3.1.2 Aplikovaná didaktická redukce	33
3.2 Detailní rozbor výukových hodin	34

3.2.1	Hodina 1: Bezdrátové počítačové sítě	34
3.2.2	Hodina 2: Přenos dat v sítích	37
3.2.3	Hodina 3: Bezpečnost v sítích a ochrana dat	39
3.2.4	Hodina 4: Internet věcí a chytrá domácnost	41
4	Metodika výzkumu a testování	44
4.1	Cíle a design výzkumu	44
4.2	Výzkumný vzorek a prostředí	44
4.3	Nástroje sběru dat	45
4.4	Průběh testování a etické zásady	47
5	Výsledky testování	49
5.1	Iterativní vývoj modulu	49
5.1.1	Úpravy 1. vyučovací hodiny	49
5.1.2	Úpravy 2. vyučovací hodiny	50
5.1.3	Úpravy 3. vyučovací hodiny	52
5.1.4	Úpravy 4. vyučovací hodiny	52
5.1.5	Reflexe a změny během plného nasazení	54
5.2	Zhodnocení efektu výuky	54
5.2.1	Celkový znalostní posun a retence znalostí	55
5.2.2	Odbourávání žákovských prekonceptů	57
6	Diskuze a limity	59
6.1	Limity výzkumu a navrženého modulu	60
6.1.1	Efekt výzkumníka a absence kontrolní skupiny	60
6.1.2	Limity plynoucí z organizace výuky a časových rozestupů	61
6.1.3	Podněty pro budoucí výzkum	61
6.2	Doporučení pro pedagogickou praxi	62
6.2.1	Zapojení fyzických simulací (unplugged aktivity)	62
6.2.2	Kritický přístup k Internetu věcí a soukromí	62
6.2.3	Práce s prekoncepty a formativní hodnocení	63
6.3	Shrnutí diskuze a naplnění cílů výzkumu	63
	Závěr	64
	Literatura	65
	Seznam obrázků	69
	Seznam tabulek	69
A	Přílohy	70
A.1	Didaktický test	70
A.2	Prezentace	72
A.2.1	Prezentace pro 1. hodinu	72

A.2.2	Prezentace pro 2. hodinu	75
A.2.3	Prezentace pro 3. hodinu	79
A.2.4	Prezentace pro 4. hodinu	82
A.3	Metodické listy	86
A.3.1	Metodické listy pro 1. hodinu	86
A.3.2	Metodické listy pro 2. hodinu	89
A.3.3	Metodické listy pro 3. hodinu	101
A.3.4	Metodické listy pro 4. hodinu	105
A.4	Pracovní listy	108
A.4.1	Pracovní list pro 1. hodinu	108
A.4.2	Pracovní list pro 2. hodinu	109
A.4.3	Pracovní list pro 3. hodinu	110
A.4.4	Pracovní list pro 4. hodinu	111
A.5	Protokoly	112
A.5.1	Protokol ke třídě	112
A.5.2	Protokol pro pozorovatele	113
A.6	Informovaný souhlas	114

Úvod

Nedávná revize Rámcového vzdělávacího programu pro základní vzdělávání (RVP ZV) [1] a Rámcového vzdělávacího programu pro gymnázia (RVP G) [2] přinesla do výuky informatiky zásadní změnu. Předmět se transformoval z pouhého nácviku uživatelských dovedností k hlubšímu pochopení principů fungování digitálních technologií a rozvoji informatického myšlení. Do středoškolského kurikula se tak dostala témata spojená s architekturou počítačových sítí, jako je paketový přenos dat, zabezpečený přenos, typy a vlastnosti bezdrátových sítí či nově se rozvíjející Internet věcí (IoT). Tato kurikulární změna však v praxi narazila na zásadní překážku. Vyučujícím chybí kvalitní, metodicky propracované a okamžitě použitelné materiály k výuce těchto specifických témat.

V posledních letech vznikla řada kvalitních prací a iniciativ, které na tuto změnu reagovaly. Většina z nich se však primárně zaměřila na úroveň základních škol. Yaghobová [3] zmapovala žákovské prekoncepce o internetu na 2. stupni ZŠ, na což navázali například Šmíd [4] nebo Mazná [5] výukovými materiály. Odborná literatura a systematické přehledy [6, 7] rovněž poskytují detailní vhled do toho, jak sítě chápou děti a mladší žáci.

Výuka na středních školách však v tomto ohledu zůstává do značné míry opomíjena. Středoškolští studenti sice disponují vyšší mírou abstrakce, což umožňuje zařazení technicky náročnějšího učiva, současná nabídka materiálů to však nereflktuje. Studenti jsou přitom v reálném životě vystaveni digitálním hrozbám a složitějším konceptům, jako je virtuální privátní síť či masivní rozvoj Internetu věcí (IoT). Současná nabídka pro střední školy (např. učebnice Roubala [8]) má často podobu spíše tradičních výkladových textů, kterým chybí aktivizační přesah.

Tento spíše pasivní přístup je problematický, protože dnešní dospívající sice vyrůstají v neustálém kontaktu s digitálními technologiemi, ale o fungování internetu si do třídy přinášejí hluboce zakořeněné mylné představy. Jak ukazují výzkumy, často jej vnímají zkresleně, například jako signál sídlící „v satelitech“ [6]. Pokud výuka stojí pouze na frontálním předávání faktů z učebnice, k vyvrácení těchto představ nemusí dojít. K dosažení skutečné konceptuální změny [9] je nutné učivo didakticky transformovat – tedy provést tzv. výukovou rekonstrukci [10, 11] – a vtáhnout žáky do aktivního procesu objevování a budování vlastního poznání.

Hlavním cílem této diplomové práce je navrhnout, otestovat a poskytnout ucelený konstruktivistický výukový modul pro 1. a 2. ročník středních škol a odpovídající ročníky víceletých gymnázií. Tento modul se zaměřuje na výuku bezdrátových sítí, principů přenosu dat, bezpečnosti a ochrany dat, včetně přesahu do problematiky Internetu věcí.

Dílčí cíle práce spočívají ve vytvoření sady podrobných metodických listů pro čtyři vyučovací hodiny a v návrhu navazujících pracovních listů a prezentací. Všechny tyto materiály jsou koncipovány s ohledem na maximální aktivizaci žáků a uplatnění modelu E-U-R (evokace – uvědomění si významu – reflexe). Aby byl výukový modul v praxi kompletní, je jeho součástí také sada nástrojů pro průběžné formativní ověřování, která vyučujícímu umožňuje bezprostředně sledovat, do jaké míry studenti probíraným konceptům porozuměli.

Po metodologické stránce práce vychází z principů akčního a konstrukčního výzkumu, což v praxi znamenalo, že výuku přímo realizoval autor práce v roli

učitele-výzkumníka. Celý modul prošel iterativním vývojem. Proces byl zahájen úvodním pilotním testováním, na které navázalo jedno menší testování pro zjištění prvotní odezvy. Následně proběhlo dalších pět samostatných iterací, během kterých byly materiály přímo ve výuce laděny a optimalizovány. Tyto úpravy nevycházely pouze z reálné odezvy od žáků, ale také z přímé reflexe vyučujícího – tedy z pozorování toho, které aktivity fungují, kde žáci narážejí na problémy nebo kde dochází k neefektivním časovým prostojeům. Tímto systematickým postupem v prostředí reálné školní třídy získal modul svou výslednou podobu, která je hlavní přílohou této práce.

Práce je rozdělena do dvou hlavních částí. První, teoretická část (kapitoly 1 a 2), shrnuje didaktická a pedagogická východiska, analyzuje postavení sítí v kurikulu a kriticky hodnotí dostupné výukové materiály. Tato analýza plynule ústí v identifikaci didaktického problému a představení zvolené výzkumné metodologie.

Druhá, praktická část (kapitoly 3 až 6), představuje samotné jádro práce. Třetí kapitola detailně popisuje navržený výukový modul, aplikovanou didaktickou redukci a rozebírá průběh jednotlivých vyučovacích hodin. Čtvrtá kapitola představuje zvolenou metodiku výzkumu a popisuje realizaci testování na výzkumném vzorku 154 žáků. Pátá kapitola se následně věnuje samotným výsledkům, konkrétně iterativnímu vývoji modulu na základě průběžné reflexe a vyhodnocení reálného znalostního posunu žáků. Závěrečná šestá kapitola interpretuje dosažené výsledky v širší diskuzi, reflektuje metodologické limity a formuluje konkrétní doporučení pro pedagogickou praxi.

Část I

Teoretická část

1 Didaktická a pedagogická východiska

Tato kapitola představuje teoretický základ pro samotný návrh výukových materiálů. Definuje, jakým způsobem žáci přistupují k novým a abstraktním poznatkům v informatice a jaké didaktické nástroje může vyučující využít k efektivnímu budování jejich mentálních modelů. Text postupně přechází od obecného paradigmatu konstruktivismu a teorie konceptuální změny přes specifický model výuky pomocí analogií až k didaktické rekonstrukci učiva a jeho strukturalizaci prostřednictvím třífázového modelu E-U-R.

1.1 Konstruktivismus a konceptuální změna

Konstruktivistické pojetí výuky představuje jedno ze základních paradigmat moderní didaktiky [12]. Na rozdíl od tradiční transmisivní výuky, která staví na pasivním přijímání informací, vnímá konstruktivismus učení jako aktivní proces budování znalostí. Žák do třídy nikdy nepřichází jako „nepopsaný list“ [13]. Z předchozího vzdělávání i každodenního života si přináší vlastní, často intuitivní představy o fungování světa – takzvané prekoncepce.

Pokud jsou tyto představy neúplné nebo přímo chybné, představují při osvojování nového učiva překážku. Cílem výuky pak není pouze vršit další a další pojmy, ale vyvolat u žáků konceptuální změnu [14]. Vycházíme-li z klasické teorie kognitivního vývoje Jeana Piageta, nestačí nové informace pouze včlenit do stávajících struktur (asimilovat). Je nutné zásadně změnit a přeměnit samotná schémata žákova myšlení (akomodovat) [13]. Toho se v didaktice často dosahuje vyvoláním kognitivního konfliktu – tedy situace, kdy žák narazí na problém, který svými dosavadními představami nedokáže vyřešit.

Samotný kognitivní konflikt však není jedinou cestou a nezaručuje automatický úspěch. Žák totiž k přebudování svého mentálního modelu není nijak přirozeně nucen; jeho stávající naivní představy mu pro běžné fungování v digitálním světě obvykle plně dostačují. Pokud má tedy konceptuální změna reálně nastat, nestačí žákovi pouze ukázat, že se mýlí. Nový, vědecky korektní koncept pro něj musí být natolik srozumitelný a užitečný, aby sám aktivně přistoupil k opuštění svého dosavadního, bezpečně fungujícího modelu [14].

1.2 Výuka prostřednictvím analogií a modelů

Počítačové sítě jsou obor s vysokou mírou abstrakce. Mechanismy přenosu dat či protokoly jsou pro lidské oko neviditelné a žákům to komplikuje budování správných mentálních modelů. Osvědčeným didaktickým nástrojem pro překonání této bariéry je výuka prostřednictvím analogií. Analogie staví pomyslný most mezi tím, co žák již důvěrně zná z běžného života (zdrojový koncept), a novým, skrytým technologickým mechanismem (cílový koncept) [15].

Jako osvědčený nástroj pro systematickou práci s analogiemi slouží model TWA (Teaching with Analogies) od Shawna M. Glynnna [16]. Autor v něm varuje

před intuitivním a povrchním použitím analogií, které může v mysli žáků generovat další chybné představy.

Proces podle Glynnna nespočívá v nahodilém přirovnávání, ale definuje šest na sebe navazujících kroků pro didakticky bezpečné nasazení analogií ve výuce [16]:

1. **Představení cílového konceptu**

Vyučující nejprve představí samotný nový, dosud neznámý technologický mechanismus.

2. **Představení analogického konceptu**

Bezprostředně následuje uvedení situace z běžného života, kterou žák důvěrně zná.

3. **Identifikace relevantních podobností**

Dochází k obecnému vymezení toho, v čem si jsou oba koncepty podobné.

4. **Mapování společných znaků**

Následuje detailní propojení konkrétních prvků a vztahů mezi zdrojovým a cílovým konceptem.

5. **Upozornění na limity analogie**

Vyučující v tomto kroku explicitně vymezí odlišnosti (v čem se přirovnání od reálného fungování sítě liší), aby nedošlo k nežádoucímu zjednodušení či vzniku miskoncepcí.

6. **Vyvození závěrů**

Cyklus je zakončen shrnutím a ukotvením poznatků o původním cílovém konceptu.

Tento šestikrokový model dává vyučujícímu návod pro tvorbu jakýchkoliv výukových analogií bez rizika, že si z nich žáci odnesou chybné představy.

1.3 Model výukové rekonstrukce a E-U-R

Aby mohly být principy konstruktivismu a bezpečné práce s analogiemi reálně využity ve výuce, nelze žákům předkládat učivo v jeho surové vědecké podobě. Výhodiskem pro tento převod je Model výukové rekonstrukce [17]. Jeho hlavní myšlenka je přímočará: výukový obsah se nesmí tvořit pouze na základě izolovaného pohledu na samotný vědní obor. Oborové poznatky je naopak nutné neustále propojovat s tím, jak žáci myslí, s jejich každodenní zkušeností a s jejich prekoncepty.

V běžné školní praxi se tento proces často zužuje na nevhodné pojetí didaktické redukce – tedy na pouhé povrchní zjednodušování a škrtání učiva. Model výukové rekonstrukce k tomu ale přistupuje jinak. Obsah nemá být jen mechanicky osekán, ale musí projít cílenou *elementarizací*. Znamená to najít naprosté jádro a základní principy daného jevu. Odborné učivo se tak upraví na úroveň srozumitelnou žákům, aniž by ztratilo cokoli ze své faktické a technologické správnosti.

Aby se takto zrekonstruované a elementarizované učivo dalo bezpečně přenést do reálné vyučovací hodiny, vyžaduje jasnou strukturu. Jako osvědčený a funkční

rámec pro tyto účely slouží třífázový model E-U-R (Evokace, Uvědomění si významu, Reflexe), který reflektuje proces přirozeného lidského učení. Jeho důsledná aplikace vytváří předpoklady k tomu, že si žák učivo zapamatuje na delší dobu a z výuky bude odcházet více motivován [18].

Fáze evokace neslouží pouze k tomu, aby vyučující zmapoval výchozí stav třídy, ale především slouží k vnitřní aktivaci samotného žáka a k vyvolání jeho vnitřního zájmu o danou problematiku. Je nezbytné, aby žák pracoval samostatně a explicitně formuloval své dosavadní znalosti pomocí vlastního jazyka. Tím si rekonstruuje předchozí vědomosti, tvoří si základní strukturu pro přijímání nových faktů a jeho intuitivní prekoncepce či chybná porozumění se dostávají na povrch [18]. Aby k tomuto odhalení reálně došlo, musí mít učitel připravené vhodné otázky a podněty k přemýšlení, které žáky nasměrují, ale zároveň jim ponechají dostatečný prostor pro vlastní úsudek a volnou asociaci.

Velmi efektivní a často využívanou evokační technikou je brainstorming [18]. Cílem je shromáždit co největší množství nápadů, přičemž se metoda zaměřuje striktně na kvantitu, nikoliv na okamžitou kvalitu. Zásadním pravidlem brainstormingu je zákaz kritizování jakéhokoliv nápadu ze strany učitele i spolužáků [19]. Díky absenci hodnocení se snižují obavy žáků z chyby, žáci mají volnost a mohou se bez ostychu inspirovat již vyřčenými nápady [19, 18]. Tím vzniká nejen solidní informační báze pro kognitivní konflikt, ale metoda zároveň žáky silně aktivizuje a rozvíjí jejich tvořivé myšlení [18].

Alternativním, avšak komplexnějším nástrojem je tvorba myšlenkových map. Zde se vychází z jednoho ústředního pojmu zapsaného uprostřed, na který se pomocí spojnic nabalují a vizualizují další související termíny a vztahy mezi nimi. Oborová literatura tuto strategii často doporučuje již pro fázi evokace, neboť má stimulovat myšlení a nutit žáky hledat vazby ještě před důkladným prostudováním tématu [18].

Z hlediska kognitivní zátěže však může jít o metodu, která je pro samotný úvod hodiny příliš náročná. Nutnost soustředit se na vizuální tvorbu a architekturu mapy může odvádět pozornost od volné asociace a brzdít plynulý tok myšlenek, který je v evokaci žádoucí. Volba konkrétní evokační metody proto musí vždy striktně zohledňovat nejen didaktický cíl, ale i zkušenosti žáků.

Následuje fáze uvědomění si významu, v níž žáci přicházejí do kontaktu s novými informacemi. Jedním z hlavních cílů této etapy je bezprostředně udržet zájem žáků vyvolaný v předchozí evokaci [18]. Zásadním specifikem této fáze je aktivní role žáka při konstrukci poznání. Vyučující vstupuje do role průvodce, zatímco žáci samostatně zkoumají předložený obsah a neustále sledují, jak tyto nové informace souvisejí s jejich původními představami z evokace [18]. Právě zde typicky nacházejí uplatnění didaktické analogie, které žákům pomáhají budovat nezbytné kognitivní mosty mezi starými a novými vědomostmi [18]. Dochází ke střetu původních prekonceptů a nových závěrů, přičemž žák by měl být schopen vzniklý nesoulad zpracovat a pospojovat si informace do hlubších souvislostí.

Zásadním bodem učebního procesu je závěrečná fáze reflexe. Během ní si žáci třídí, systematizují a upevňují nové vědomosti, čímž probíhá proces učení vedoucí k trvalému uchování informací [18]. Nejde o pouhé shrnutí probrané látky, ale o okamžik, kdy probíhá skutečná restrukturalizace mentálních modelů. Žáci si nové poznatky zhodnotí a naučí se své nové názory zformulovat vlastními slovy, což je klíčové pro jejich ukotvení. K systematizaci těchto nově zkonstruovaných

poznatků se využívají strukturované diskuze nebo opět myšlenkové mapy, které díky převodu informací do grafické podoby proces konceptuální změny efektivně zakončují [18].

2 Informatika v kurikulu a analýza dostupných zdrojů

Tato kapitola zasazuje výuku počítačových sítí do širšího rámce českého vzdělávacího systému a existující didaktické praxe. Její hlavní ambicí je analyzovat současné požadavky kurikula, zhodnotit reálné možnosti škol a kriticky posoudit výukové materiály, které mají vyučující aktuálně k dispozici.

Text nejprve shrnuje požadavky Rámcového vzdělávacího programu a ukazuje, jak by na sebe mělo ideálně navazovat učivo základní a střední školy. Následně poskytuje rešerši a srovnání dostupných metodických zdrojů. Celá kapitola pak ústí v identifikaci hlavního didaktického problému – tedy absence ucelených, konstruktivisticky laděných materiálů pro výuku počítačových sítí na středních školách.

2.1 Revize RVP pro střední školy a obsahové vymezení

Vzdělávací obor Informatika prošel v českém kurikulu revizí, která reflektuje nutnost posunu od uživatelského ovládání počítače k informatickému myšlení a porozumění principům digitálních technologií. Obsah oboru je nově strukturován do čtyř vzájemně se prolínajících tematických celků: Data, informace a modelování; Algoritmizace a programování; Informační systémy; a Digitální technologie.

Tato práce se zaměřuje na oblast digitální technologie, konkrétně na tematický celek počítačové sítě. Při návrhu výukových materiálů k tomuto středoškolskému učivu je nezbytné nejprve definovat výchozí stav, tedy očekávané znalosti, se kterými by měl žák do prvního ročníku střední školy nastupovat.

2.1.1 Prerekvizity ze ZŠ a požadavky na středoškolské vzdělávání

Podle Rámcového vzdělávacího programu pro základní vzdělávání (RVP ZV) ve znění platném od roku 2023 se žáci s principy fungování sítí seznamují již na prvním stupni [1]. Důraz je zde kladen na základní pochopení propojování technologií a uživatelskou bezpečnost. Očekávaným výstupem je schopnost žáka propojit digitální zařízení, pracovat ve sdíleném prostředí a uvědomovat si možná rizika spojená se sdílením dat [1].

Na druhém stupni ZŠ se téma dále rozšiřuje. Očekávané výstupy stanovují, že žák dokáže vybrat vhodný způsob připojení do sítě, popíše její znaky a orientuje se v metodách zabezpečení přístupu k datům [1]. RVP ZV předepisuje pro druhý stupeň konkrétní technické učivo: od absolventa se formálně očekává znalost architektury klient-server, funkce aktivních síťových prvků (např. switch), konceptu IP adres, struktury a principů internetu, fungování webu (role webového serveru, prohlížeče a URL), principů cloudových aplikací a správy přístupových práv [1]. Zatímco základní školství čeká v rámci revize RVP ZV z roku 2025 změna přístupu, kdy se u vzdělávacího oboru Informatika ustupuje od striktně předepsaného

technického učiva k obecněji formulovaným výstupům (např. výběr připojení a zabezpečení sítě výhradně na základě uživatelského posouzení rizik) [20], pro navazující středoškolské studium zůstávají technologické znalosti a architektura systémů nadále relevantní.

Na tyto výstupy ze základní školy navazuje Rámcový vzdělávací program pro gymnázia (RVP G) a obdobně i RVP pro střední odborné vzdělávání. Středoškolské kurikulum již nebuduje základní představu o existenci sítí, ale předpokládá, že studenti přejdou od uživatelského ovládání k abstraktnějšímu porozumění skrytým mechanismům přenosu dat a kybernetické bezpečnosti [2]. Mezi očekávané výstupy v oblasti Digitálních technologií patří schopnost žáka porovnat jednotlivé způsoby propojení počítačů a vysvětlit, „pomocí čeho a jak je zajištěna komunikace mezi jednotlivými zařízeními v síti“. Žák by měl být rovněž schopen identifikovat a řešit síťové problémy a zodpovědně chránit svá zařízení i data před zneužitím s ohledem na technologický vývoj.

Konkrétní předepsané učivo pro střední školy v této oblasti zahrnuje problematiku lokálních sítí a internetu s důrazem na princip paketového přenosu dat. Dále je vyžadována orientace v zabezpečeném přenosu dat, kam spadá funkce firewallu a principy šifrované komunikace. Žáci by měli chápat principy fungování webu a cloudových služeb a orientovat se v moderních technologiích, což zahrnuje typy a vlastnosti bezdrátových sítí včetně konceptu Internetu věcí. Výuka sítí na středních školách by proto měla poskytnout teoretický i praktický základ, na kterém mohou žáci stavět své technologické kompetence, což vyžaduje budování propracovaných mentálních modelů.

2.1.2 Kurikulární návaznost a reálný stav

Analýza uvedených kurikulárních dokumentů ukazuje, že středoškolské učivo (např. paketový přenos či firewall) je koncipováno jako nadstavba nad znalostním základem ze základní školy (např. klient-server, IP adresa).

Tento předpoklad teoretické návaznosti však v současné transformační fázi českého školství představuje didaktický problém. Vzhledem k probíhajícímu přechodnému období implementace nové informatiky nastupují na střední školy žáci, kteří definovaným učivem druhého stupně ZŠ často vůbec neprošli, nebo si z něj odnesli pouze útržkovité znalosti a nadále u nich přetrvávají mylné prekoncepce. Tvorba středoškolských výukových materiálů tedy nespočívá pouze v naplnění cílů RVP G, ale také v nutnosti integrovat do výuky mechanismy, které dokážou chybějící základy ze základní školy detekovat a doplnit. Mezi tyto tematické okruhy patří schopnost žáků opustit laickou představu o přímém (často pouze bezdrátovém) spojení koncových zařízení a nahradit ji mentálním modelem sítě, v níž komunikaci zprostředkovávají aktivní uzly. Dále je vhodné ukotvit logiku modelu klient-server, aby žáci pochopili fyzickou lokalizaci dat v internetovém prostoru a odbourali mýtus o tom, že webové služby běží přímo v jejich lokálních zařízeních [6]. Důležitou oblastí je samotná podstata síťové komunikace, která vyžaduje uvědomění, že každé zařízení v síti musí být jednoznačně identifikovatelné a že data fyzicky putují přes sdílenou infrastrukturu. Pochopení těchto univerzálních principů tvoří didaktický most pro středoškolskou výuku abstraktnějších konceptů, jako je samotný mechanismus paketového přenosu či šifrování, nezávisle na tom, jak úzce jsou tyto oblasti vymezeny v aktuálních kurikulárních revizích.

2.1.3 Časové vymezení a organizace výuky

Rozsah předepsaného učiva a očekávaných výstupů je nutné vnímat v kontextu časových možností, které mají školy k dispozici. Podle RVP ZV je obor Informatika na prvním stupni realizován s minimální časovou dotací dvou vyučovacích hodin (v praxi tedy typicky jedna hodina týdně ve 4. a jedna v 5. ročníku). Pro celý druhý stupeň jsou pak závazně vyhrazeny minimálně čtyři hodiny. Podobný minimální základ nastavuje i RVP G pro čtyřletá gymnázia. Ačkoliv ředitelé škol mohou tuto dotaci navýšit z rámce disponibilních hodin, v praxi se o tento prostor informatika dělí s ostatními předměty a její výuka tak zůstává u stanoveného minima.

Začlenění všech tematických oblastí do tohoto časového rámce proto představuje pro vyučující značnou výzvu. Samotná oblast Digitální technologie, pod kterou počítačové sítě spadají, je poměrně široká – zahrnuje témata od hardwaru přes operační systémy až po kybernetickou bezpečnost. Ve výuce tak na samotné počítačové sítě zbývá pouze omezená časová dotace (v řádu jednotek vyučovacích hodin). Tato časová tíseň vytváří tlak na efektivitu výuky a činí z pečlivé didaktické redukce učiva klíčový předpoklad pro to, aby bylo téma žákům předáno v souvislostech a v souladu s principy konstruktivistické didaktiky.

Z tohoto důvodu je navrhovaný výukový modul v praktické části této práce koncipován v rozsahu čtyř vyučovacích hodin. Tento časový rámec (odpovídající zhruba jednomu měsíci výuky při standardní dotaci jedné hodiny týdně) představuje na základě výše popsaných kurikulárních limitů jakýsi kompromis. Je dostatečně stručný, aby byl reálně začlenitelný do běžných tematických plánů středních škol, a zároveň poskytuje nezbytné časové minimum pro smysluplnou aplikaci konstruktivistických metod a fyzických simulací, které vyžadují delší časovou dotaci než tradiční frontální výklad.

2.2 Analýza a srovnání dostupných materiálů

Základním předpokladem pro návrh výukového modulu je kritická analýza stávajících vzdělávacích materiálů. Analýza dostupných zdrojů pro výuku počítačových sítí na středních školách ukazuje, že nabídka materiálů je z hlediska metodického i obsahového nehomogenní a v mnoha ohledech nevyhovuje požadavkům moderní informatiky. V kontextu všeobecného gymnaziálního vzdělávání lze identifikovat několik specifických oblastí, které vykazují výrazná metodická omezení.

2.2.1 Metodika analýzy a kritéria výběru zdrojů

Pro zajištění replikovatelnosti a objektivitu analýzy byla pro vyhledávání a následné hodnocení výukových materiálů stanovena metodická kritéria.

Výběr analyzovaných zdrojů byl omezen na materiály splňující následující body:

1. Cílovou skupinou jsou žáci středních škol (primárně gymnázií a SOŠ všeobecného zaměření) nebo žáci druhého stupně ZŠ, pokud dané materiály svým obsahovým rozsahem pokrývají povinné kurikulární základy středoškolského vzdělávání.

2. Obsahové zaměření se věnuje tematické oblasti počítačových sítí a fungování internetu, případně se jedná o ucelené řady učebnic pro novou informatiku, u nichž je pokrytí tohoto povinného celku předpokládáno.
3. Materiály jsou vyučujícím běžně dostupné (ve formě tištěných publikací, schválených učebnic nebo veřejných online platforem).

Vyhledávání probíhalo v období od listopadu 2025 do května 2026 prostřednictvím katalogů pedagogických nakladatelství, oficiálního metodického portálu `dum.rvp.cz` a vyhledávače Google s využitím klíčových slov „počítačové sítě učebnice“, „výuka sítí SŠ“ a „nová informatika učebnice“. Nalezené zdroje byly pro přehlednost rozděleny do tří tematických okruhů:

1. Nové publikace a oficiální metodické portály,
2. online výukové materiály vzniklé jako přímá reakce na nové RVP,
3. inovativní materiály a akademické práce primárně určené pro nižší stupně vzdělávání.

Z těchto okruhů byl vybrán výsledný vzorek relevantních materiálů, které byly následně podrobeny detailní analýze. Každý z vybraných zdrojů byl posuzován a hodnocen podle čtyř stanovených proměnných:

- **Pojetí výuky** – zda materiál předkládá hotová fakta, nebo vede žáka k vlastnímu objevování.
- **Míra didaktické redukce** – zda text nezatěžuje žáky nadbytným technickým detailem a soustředí se na klíčové principy.
- **Aktivizační prvky a simulace** – zda jsou přítomny fyzické či digitální modely a aktivity.
- **Úroveň kognitivních cílů** – jak lze ohodnotit úlohy dle revidované Bloomovy taxonomie.

2.2.2 Absence tématu v nových publikacích a na metodických portálech

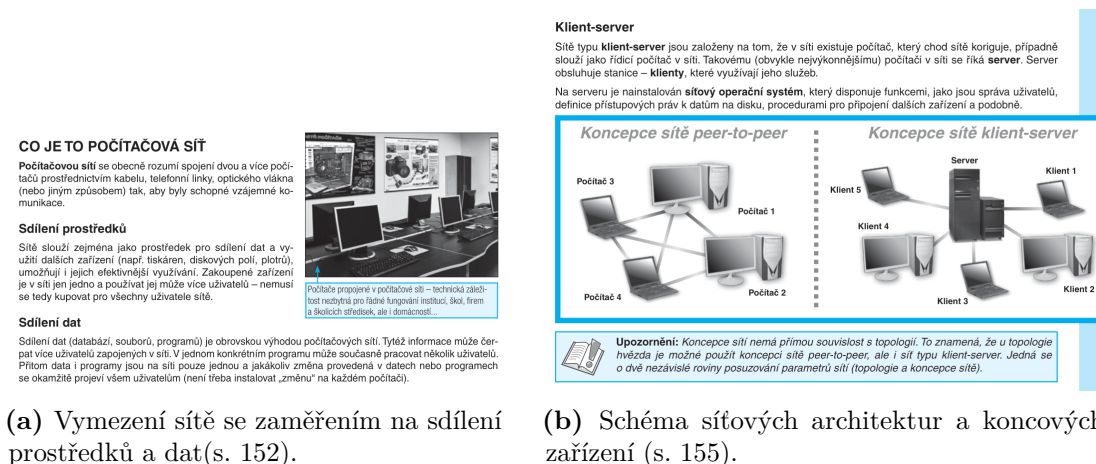
Prvním analyzovaným okruhem jsou nově vydávané publikace a oficiální metodické portály.

Při vyhledávání v katalozích nakladatelství byly nalezeny dvě ucelené tištěné řady reflektující reformu informatiky na středních školách: *Základy informatiky pro střední školy* [21] a první díl publikace *Informatika pro střední školy 1* [22]. Analýzou těchto dostupných zdrojů bylo zjištěno, že tematickou oblast počítačových sítí ani jedna z publikací neobsahuje, protože je nebylo možné podrobit hodnocení podle stanovených proměnných. Z hlediska celkového stavu trhu tak tyto publikace v současné době neposkytují vyučujícím obsahovou oporu a přípravu materiálů přesouvají na samotné učitele.

K téže kategorii tištěné literatury, která se však v praxi z důvodu setrvačnosti stále uplatňuje, patří starší učebnice *S počítačem nejen k maturitě 2. díl* [23]. Tento

materiál již síťovou tematiku obsahuje, a proto mohl být podroben kritické analýze dle všech čtyř sledovaných proměnných. Z hlediska *pojetí výuky* a *didaktické redukce* text neobsahuje vysvětlení principů fungování internetu či mechanismů přenosu dat. Místo budování funkčních mentálních modelů se zaměřuje na deskriptivní přístup na nejnižší úrovni Bloomovy taxonomie, kde jsou žákovi předkládána hotová technická fakta a klasifikace (např. typy kabelů, síťové operační systémy či dělení sítí podle velikosti). Konkrétní příklady této technologické redukce a konzervace historického pohledu na infrastrukturu ilustruje obrázek 2.1.

Autor této práce odhaduje, že text odráží historický, uživatelsko-správcovský pohled na síťovou infrastrukturu, který neodpovídá současným potřebám všeobecného vzdělávání. Síť je zde definována jako prostředek pro sdílení hardwarových zařízení (např. tiskáren) a správu přístupových práv k adresářům. Z hlediska *miskonceptů* navíc učebnice fixuje překonané modely, když věnuje podstatný prostor popisu fyzické topologie sběrnice (BUS), která se v moderní síťové praxi již standardně nevyužívá. V materiálu zcela chybí *aktivizační prvky*, *didaktické analogie* či *simulace*, které by žáky vedly k pochopení procesů, jako je paketový přenos, směrování nebo kybernetická bezpečnost.



(a) Vymezení sítě se zaměřením na sdílení prostředků a dat (s. 152).

(b) Schéma síťových architektur a koncových zařízení (s. 155).

Obrázek 2.1 Ukázky pojetí síťové problematiky v učebnici *S počítačem nejen k maturitě 2. díl* [23]. © Computer Media s.r.o., 2018

Druhým sledovaným zdrojem v této kategorii byl oficiální metodický portál *dum.rvp.cz*. Při vyhledávání pro stupeň vzdělávání *gymnázium* byla v systému zvolena verze filtru *RVP (do 2024)*, která však jako jedinou možnost pro modernizovanou výuku nabízí položku *Informatika (rvp gv 2021)* v kolonce vzdělávacích oblastí. Cílené vyhledávání v této kombinaci parametrů nenalezlo žádné výsledky. Druhá možnost filtru, konkrétně *RVP revidované (od 2025)*, v době vyhledávání nabízela pouze materiály pro mateřské a základní školy, přičemž středoškolské vzdělávání nebylo zahrnuto.

Při změně kritérií na gymnaziální vzdělávací oblast *Informatika a informační a komunikační technologie* databáze nabídla celkem šest materiálů. Analýza jejich obsahu ukázala, že dva z nich tematicky neodpovídají sledované oblasti, neboť se věnují počítačové grafice [24] a tvorbě papírového modelu budovy [25]. Pro přímou výuku počítačových sítí na gymnáziích tak portál obsahuje pouze čtyři izolované dokumenty: úvodní přehled počítačových sítí [26], křížovku obsahující síťové pojmy [27] a dvě navazující prezentace k lokálním sítím LAN [28, 29]. Všechny byly

publikovány v letech 2008 až 2011, což znamená, že reflektují technologický stav a didaktické potřeby předminulého desetiletí.

Při rozšíření vyhledávání na *odborné vzdělávání* v rámci vzdělávací oblasti *Informační a komunikační technologie* portál nabídl celkem 14 materiálů. Analýza jejich obsahu ukázala, že většina z nich tematicky neodpovídá sledované oblasti, neboť se věnuje tvorbě webových stránek v nástroji Google Sites (např. [30]), počítačové grafice [31] či 3D modelování [32]. K samotné tematice počítačových sítí a jejich infrastruktury se v databázi nacházejí pouze dva izolované dokumenty – prezentace zaměřená na síťový hardware z roku 2013 [33] a pracovní list z roku 2014 obsahující síťové pojmy a model ISO/OSI [34].

Z hlediska sledovaných proměnných tyto dostupné materiály na portálu *dum.rvp.cz* (gymnaziální i odborné) podle autora této práce konzervují transmisivní pojetí výuky. Jsou koncipovány pro potřeby starších kurikulárních dokumentů, soustředí se na znalost faktů, konkrétně memorování zkratk a popis hardwaru, přičemž téměř postrádají didaktickou redukci, která by reflektovala současná témata (jako je cloud, VPN či Internet věcí), stejně jako aktivizační prvky či konfrontaci žákovských prekonceptů. Oficiální metodická podpora pro středoškolskou výuku sítí podle nového RVP tak na centrálním portálu zcela chybí.

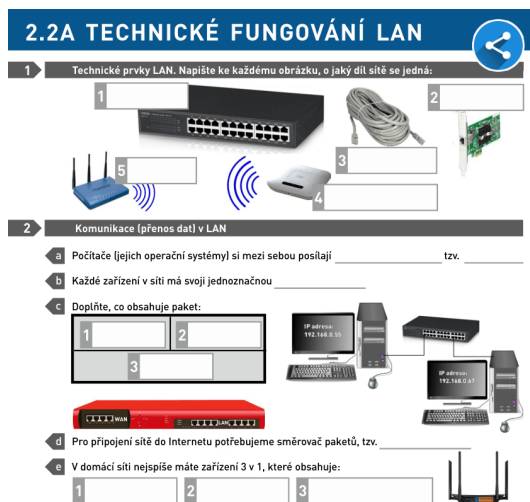
2.2.3 Online materiály pro nové RVP

Druhým analyzovaným okruhem jsou online výukové materiály vzniklé jako přímá reakce na reformu. Tento segment v současnosti reprezentuje zejména tvorba Pavla Roubala na portálu *opocitacich.cz* [8] a vzdělávací portál *Umíme to*.

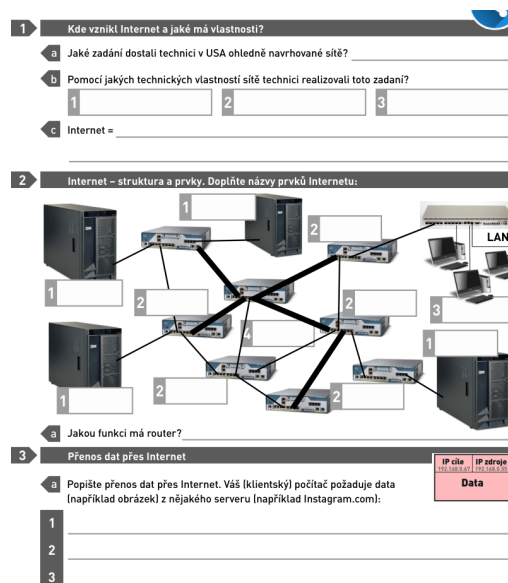
Z hlediska *pojetí výuky* vykazují materiály Pavla Roubala převážně transmisivní charakter. Sledované úlohy v pracovních listech jsou postaveny na mechanickém doplňování termínů, identifikaci hardwarových prvků podle fotografií či na digitálních úlohách typu přiřazování pojmů, což ve spojení s doprovodnými prezentacemi fixuje faktuelní pojetí výuky. Příklad tohoto metodického zpracování ilustrují doplňovací úlohy v pracovních listech na obrázku 2.2, respektive vizuální opora v prezentacích (viz obrázek 2.3). Ačkoliv tento přístup podporuje rozvoj čtenářské gramotnosti a schopnost žáků vyhledávat fakta v textu, z pohledu provedené didaktické analýzy neposkytuje samotná práce s tímto formátem dostatečný prostor pro budování funkčních mentálních modelů ani pro konfrontaci hluboce zakořeněných miskonceptů.

V oblasti *didaktické redukce* sice Roubalovy materiály pokrývají základní tematické okruhy, z pohledu analýzy však žákům neposkytují dostatečný prostor pro logické odvození principů ani pro vyvolání kognitivního konfliktu k překonání chybných prekonceptů. I když žák dokáže reprodukovat definici (např. že VPN tvoří „šifrovaný tunel“), v materiálech chybí *aktivizační prvky a fyzické simulace*, které jsou pro konstruktivistický přístup a dosažení konceptuální změny charakteristické.

Odlišný přístup k online vzdělávání nabízí portál *Umíme informatiku* [35]. Z hlediska pojetí výuky a aktivizace nestaví na čtení souvislých textů, ale na opakovaném procvičování izolovaných faktů, které je doplněno o prvky herního designu. Žáci pracují s uzavřenými interaktivními úlohami, jako jsou pexesa, doplňování textu či rychlé rozhodovačky, jak ilustruje příklad síťového cvičení na obrázku 2.4. Ačkoli tento formát může být pro žáky vizuálně atraktivní, při hodnocení *úrovně kognitivních cílů* aktivity nedosahují vyšších pater Bloomovy



(a) Identifikace síťového hardwaru a doplňování pojmů v kapitole 2.2A.



(b) Doplňování pojmů a textu v kapitole 2.3.

Obrázek 2.2 Ukázky z pracovního sešitu *opocitacich.cz* [8]. © Ing. Pavel Roubal.

Komunikace (přenos dat) v LAN – IP adresy

- **Stručně:**
- **Počítače (jejich operační systémy), si mezi sebou posílají balíčky s daty, tzv. pakety.**
- Je to (z hlediska principu) **opravdu takto jednoduché**. Podobně jako Česká pošta doručuje balíčky se zbožím, stejně putují data v počítačové síti.
- **Jak ale pošta ví, kam má doručit který balíček?**
- Každý odesílatel a příjemce musí **mít svoji (jednoznačnou) adresu**. A stejně to dělají i počítačové sítě:
- **Každý počítač (jeho OS) má v síti jednoznačnou IP adresu [aj pí adresu].**

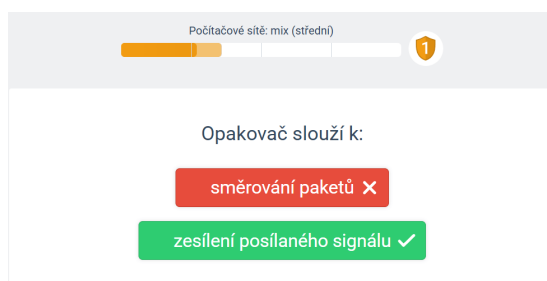
IP (Internet Protocol) adresa se skládá z čísel. IP adresa verze 4 například obsahuje 4 jednobajtová čísla (0–255).

2.2 Technické fungování LAN 4

Obrázek 2.3 Ukázka snímku z materiálu *opocitacich.cz*, prezentace 2.2 – Fungování LAN, pakety, IP [8]. © Ing. Pavel Roubal.

taxonomie. Úlohy testují primárně schopnost vybavit si a přiřadit správný termín či zkratku (např. že P2P znamená peer-to-peer). Limitem tohoto přístupu je navíc absence formativní zpětné vazby – v případě chybné odpovědi systém často poskytuje pouze textové vysvětlení konkrétní zkratky či termínu namísto objasnění celkového síťového principu, což žáky vede spíše k metodě pokus-omyl než k pochopení problému.

Z pohledu *didaktické redukce* vykazuje portál *Umíme informatiku* výrazné nedostatky, neboť žáky zahlučuje encyklopedickým výčtem technických specifikací. Již v modulech pro základní školy se objevují historické fyzické topologie (sběrníková, kruhová) či detailní rozdíly mezi aktivními prvky na nižších vrstvách sítě (rozdíl mezi zařízeními hub, switch a bridge). V modulech určených pro střední školy pak zůstává teoretický základ prakticky totožný se základní školou, je pouze rozšířen o katalogizaci síťových protokolů (např. FTP, SMTP, IMAP, POP3, IRC, SSH). Výuka tak rezignuje na budování celkového mentálního modelu sítě ve prospěch mechanické reprodukce technického slovníku.



Obrázek 2.4 Ukázka cvičení („rozhodovačka“) na portálu *Umíme informatiku* [35].
© Umíme to, s.r.o.

2.2.4 Inovativní materiály pro nižší stupně vzdělávání

Třetím analyzovaným okruhem jsou výukové materiály, akademické práce a komerční sady učebnic z posledních let, které sice primárně cílí na nižší stupně vzdělávání (1. a 2. stupeň ZŠ), avšak pro svou metodickou propracovanost bývají v praxi zvažovány jako alternativa i pro střední školy. Tento segment lze vnitřně rozdělit na výstupy z akademického prostředí a komerční publikace.

V rámci akademické sféry představují významný didaktický posun metodické práce a diplomové projekty. Zatímco Yaghobová [3] zmapovala žákovské prekoncepce, na její zjištění prakticky navázali autoři tvorbou ucelených výukových modulů. Jde zejména o materiály Drobné [36] zacílené na 1. stupeň ZŠ, a dále práce Mazné [5], Petíře [37] a Šmída [4] určené pro 2. stupeň ZŠ.

Z hlediska *pojetí výuky* představují tyto práce posun ke konstruktivistickému přístupu. Výukové moduly (zejména u Mazné a Petíře) jsou explicitně strukturovány podle modelu E-U-R (evokace, uvědomění, reflexe) a využívají badatelské postupy. Výuka nezačíná technickými definicemi, ale mapováním prekonceptů a navazováním na každodenní zkušenosti žáků, což Drobná aplikuje již u dětí mladšího školního věku.

Z pohledu *odborného zaměření na počítačové sítě a didaktické redukce* vykazují práce rozdílný přístup úměrný cílové skupině. Drobná [36] pro 1. stupeň ZŠ redukuje téma sítě do roviny elementární uživatelské bezpečnosti a viditelnosti na

internetu (např. pomocí metafory „domu jako průhledného akvária“), čímž zcela abstrahuje od jakéhokoliv hardwaru. Petříř [37] se ve svém modulu pro 6. a 7. ročník věnuje sítím primárně optikou uživatelské kybernetické bezpečnosti (např. zabezpečení domácího Wi-Fi routeru). Šmíd [4] volí pro vysvětlení síťové infrastruktury cestu metaforických výukových plakátů, kde síťové prvky představuje jako „chytré křižovatky“, čímž buduje intuitivní pochopení směrování bez nutnosti znalosti protokolů. Mazná [5] pak ve svých materiálech nabízí pro starší žáky komplexnější pohled na fyzickou infrastrukturu internetu a mechanismus paketového přenosu.

Při hodnocení *aktivizačních proků a simulací* je u všech autorů patrné systematické zapojení činnostního učení k vizualizaci neviditelných procesů. Drobná využívá k ukotvení abstraktních pojmů kreslení a diskusi nad zmíněnými didaktickými metaforami. Petříř do své výuky integruje fyzickou simulaci spolupráce na cloudu (tzv. sdílenou nástěnku), pomocí které žáci objevují principy přidělování přístupových práv. Mazná naopak využívá unplugged aktivity k modelování samotného síťového provozu prostřednictvím didaktické hry simulující směrování paketů. Šmídovy výukové plakáty, jejichž konkrétní podobu ilustruje obrázek 2.5, pak vedou žáky k samostatnému logickému propojování jednotlivých uzlů sítě.



Obrázek 2.5 Ukázka výukového listu „Servery a křižovatky“ z práce Šmída [4].

Z hlediska *úrovně kognitivních cílů* směřují aplikované úlohy k vyšším procesům Bloomovy taxonomie. Již u Drobné žáci reflektují pozitiva a negativa sdílení dat, u starších žáků pak následuje analýza rizik spojená se zneužitím digitální stopy (Mazná) či hodnocení oprávněnosti přístupů aplikací k periferiím (Petříř). Limitem pro přímé využití těchto prací ve všeobecném středoškolském vzdělávání (gymnáziích) je však právě míra a zacílení jejich didaktické redukce. Ačkoliv navrhovaný středoškolský modul – podobně jako materiály pro základní školy – vynechává zbytečné technické specifikace a vysvětluje síťové mechanismy primárně konceptuálně, musí reagovat na odlišné kognitivní potřeby gymnaziálních žáků. Materiály designované pro nižší stupně nedosahují takové úrovně abstrakce a nepokrývají pokročilejší témata v širších souvislostech. Zcela tak opomíjejí fenomény, se kterými se dnešní středoškolák běžně setkává, jako jsou konceptuální principy

virtuálních privátních sítí (VPN) či bezpečnostní aspekty Internetu věcí (IoT). Právě na didaktické uchopení těchto komplexnějších témat bez zahlcení žáků hardwarovými specifikacemi se zaměřuje tato diplomová práce.

Paralelně s těmito akademickými výzkumy vznikal v komerční sféře samostatný segment materiálů určených pro základní vzdělávání. Typickými zástupci jsou publikace *Základy informatiky pro 2. stupeň základní školy* [38] vydaná v rámci projektu *iMyšlení*, dále řada *Informatika pro základní školy* od nakladatelství Computer Media a pracovní učebnice *Informatika v pohodě* od nakladatelství Taktik.

Analýza obsahu a struktury tohoto komerčního segmentu učebnic pro 2. stupeň ZŠ odhaluje limity z hlediska míry didaktické redukce a technologické přesnosti. Ačkoliv se jedná o publikace vydávané jako podpůrné materiály pro reformovanou výuku informatiky, jejich nabídka na trhu vykazuje fragmentaci a obsahovou nekonzistentnost. Zatímco některé řady tematickou oblast počítačových sítí ve svém obsahu opomíjejí, jiné se omezují na uživatelsky orientovaný pohled na koncové služby.

V řadě *Informatika pro základní školy* od nakladatelství Computer Media se tematika objevuje pouze v 6. ročníku [39], kde je redukována na základy vyhledávání, e-mailovou komunikaci a bezpečnostní rizika na webu (např. fenomén deepfake), přičemž v 7. a 8. ročníku se již nevyskytuje. Také řada *Základy informatiky pro 2. stupeň základní školy* projektu *iMyšlení* [38], která vyčleňuje kapitolu „Síťové prostředí“, omezuje výuku na identifikaci koncových zařízení (mobil, router), elementární popis cloudu a didaktickou analogii fungování elektronické pošty s klasickou listovní poštou.

Z hlediska rozsahu témat síťové infrastruktury obsahuje pracovní učebnice *Informatika v pohodě 6* od nakladatelství Taktik [40] v bloku „Domácí a školní počítačová síť“ pojmy jako LAN, IP adresa, switch, router, podsítě a výchozí brána. Analýza textu však ukazuje na nedostatky v oblasti didaktické redukce. Zavedení pojmu podsít a vysvětlení její správy vykazuje pro žáky 6. ročníku vysokou kognitivní náročnost. Text popisuje fungování podsítí skrze soustavu propojených switchů a uvádí, že část úkolů routeru může podle nastavených pravidel přebírat switch a naopak, což ilustruje schematické zapojení na obrázku 2.6. Pro dvanáctiletého žáka může být takto abstraktní popis bez funkčních analogií obtížně srozumitelný.

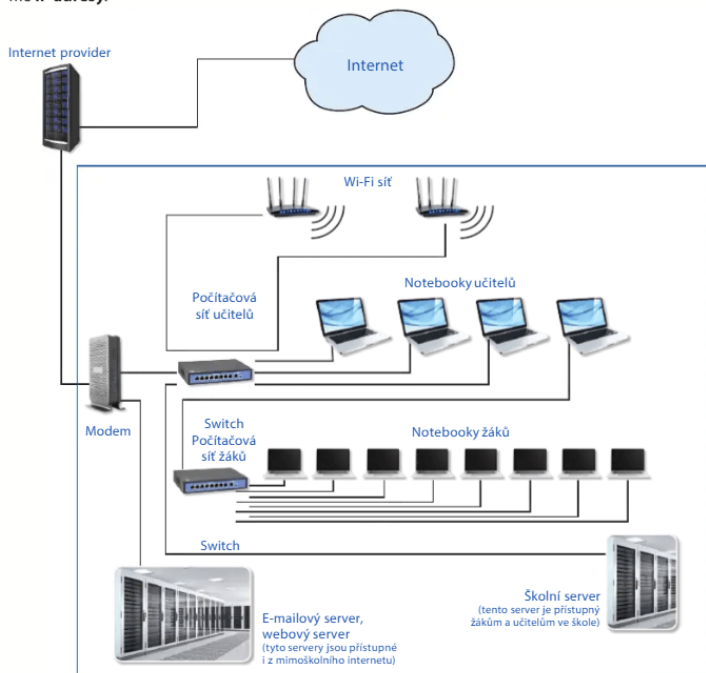
Z hlediska miskoncepcí text obsahuje terminologické nepřesnosti, když definuje switch jako „rozbočovač“ (hub), čímž zaměňuje L2 a L1 prvky¹. Naopak z hlediska úrovně kognitivních cílů podle Bloomovy taxonomie učebnice formuluje badatelské dotazy (např. „Proč se síť rozděluje do podsítí?“), které žáky vedou k aktivnímu hledání odpovědí v rámci diskuse, což stimuluje vyšší kognitivní procesy. Limitem zůstává skutečnost, že v navazujících dílech pro 7. a 8. ročník tato řada na rozpracovaná témata již nenavazuje.

Z hlediska sledovaných proměnných tento komerční segment pro 2. stupeň ZŠ vykazuje snahu o konstruktivistické pojetí výuky, využívá aktivizační prvky (např. kreslení schémat či simulace pošty u Berkiho) a vede žáky k řešení problémů. Pro potřeby všeobecného středoškolského vzdělávání (gymnázií) jsou však tyto materi-

¹Odkazuje na vrstvy referenčního modelu ISO/OSI. Rozbočovač (hub) pracuje na 1. (fyzické) vrstvě, kde kopíruje signál do všech portů, zatímco přepínač (switch) operuje na 2. (datové) vrstvě a směřuje datové rámce podle fyzických (MAC) adres konkrétních zařízení.

Školní počítačová síť

Počítačová síť ve škole je velice podobná té domácí, jen k ní, pokud slouží pro celou školu, může být připojeno mnohem více zařízení. K jednoznačné identifikaci všech zařízení v počítačové síti používáme **IP adresy**.



Obrázek 2.6 Ukázka schematického zapojení podsítě v učebnici *Informatika v pohodě 6* [40]. © TAKTIK Vydavatelství s.r.o., 2022.

ály obsahově neúplné. Neobsahují vysvětlení vnitřních principů internetových protokolů (např. struktura IP adres, mechanismus směrování paketů), problematiku komplexnější kybernetické bezpečnosti (šifrování VPN, symetrická/asymetrická kryptografie) ani síťovou architekturu Internetu věcí (IoT) z pohledu ochrany datového soukromí.

2.2.5 Výhled a připravované publikace

V rámci analýzy trhu byl zkoumán také výhled vydavatelské činnosti pro nejbližší období. Nakladatelství Computer Media avizuje přípravu navazujícího druhého dílu učebnice *Informatika pro střední školy 2*, který by měl podle předběžného obsahu tematiku počítačových sítí pokrývat. Vzhledem k tomu, že recenzní výtisk ani pracovní verze této publikace nebyly v době vzniku této práce dostupné, nebylo možné materiál podrobit analýze podle stanovených proměnných.

Současný trh s literaturou pro střední školy tak z pohledu modernizované výuky počítačových sítí zůstává nedostatečný a nenabízí vyučujícím ucelenou metodickou oporu.

2.3 Identifikace didaktického problému

Z provedené analýzy vyplývá didaktický problém, kterým je nedostatek adekvátní metodické opory pro výuku počítačových sítí ve všeobecném středoškolském vzdělávání.

Vyučující na gymnáziích řeší volbu výukového přístupu. Mohou zvolit tradiční transmisivní výuku, která u žáků často vede k memorování pojmů bez pochopení principů fungování sítí. Druhou možností je přejímat konstruktivistické materiály určené pro základní školy, čímž však riskují, že kognitivní potenciál starších žáků zůstane nevyužit a výuka nepokryje náročnější středoškolská témata.

Tento problém v praxi umocňují dva faktory. Prvním z nich je omezená časová dotace; RVP sice vyžaduje pokrytí tématu sítí, avšak reálná praxe na školách umožňuje tomuto bloku věnovat pouze přibližně čtyři vyučovací hodiny (viz 2.1.3). Alternativní technické materiály (např. certifikační kurzy typu Cisco Networking Academy či vysokoškolská skripta zaměřená na síťovou architekturu) jsou proto v tomto časovém rámci obtížně použitelné. Tyto zdroje jsou určeny pro odbornou přípravu budoucích IT specialistů a kladou důraz na konfiguraci konkrétního hardwaru, ovládání příkazových řádků a detailní implementaci síťových protokolů, což přesahuje potřeby všeobecného středoškolského vzdělávání.

Druhým faktorem je pak rozpor v digitálních kompetencích samotných žáků. Středoškolští žáci přicházejí do hodin jako uživatelé digitálních technologií, avšak jejich každodenní rutina v nich fixuje prekoncepce, jako je představa o přímém datovém spojení či předpoklad soukromí při používání chytrých spotřebičů. Tento rozpor mezi uživatelskou zdatností a absencí konceptuálního porozumění procesům na pozadí online světa dokládají i data z mezinárodního šetření ICILS 2023 [41]. Čeští žáci sice v celkovém hodnocení počítačové gramotnosti dosahují nadprůměrných výsledků v rámci EU, avšak více než čtvrtina z nich (28 %) nedosahuje ani základní úrovně. Výzkum navíc odhaluje metakognitivní zkreslení ve vnímání vlastních kompetencí – v aspektu kritického posuzování informací celých 86 % neúspěšných řešitelů subjektivně deklarovalo, že danou dovednost ovládá. Ačkoliv se šetření ICILS zaměřuje na informační a mediální gramotnost, popsany fenomén (kdy je schopnost zařízení ovládat zaměňována za porozumění principům jeho fungování) může být relevantní i pro oblast síťové infrastruktury. Lze hypoteticky předpokládat, že podobný deficit v hodnocení vlastních znalostí se může projevat i zde, což by u žáků potenciálně fixovalo chybné technologické prekoncepce a snižovalo jejich ostražitost vůči bezpečnostním rizikům. Existenci této korelace v oblasti síťových technologií je však nutné brát jako možný předpoklad, který by vyžadoval samostatné empirické ověření.

Jádrem identifikovaného didaktického problému je tedy otázka, jak v časové dotaci čtyř vyučovacích hodin zprostředkovat žákům téma počítačových sítí tak, aby výuka nebyla omezena na pasivní příjem informací. Je vhodné navrhnout vzdělávací modul, který pomocí cílené didaktické redukce odstraní technické detaily přesahující rámec všeobecného vzdělávání a zároveň si zachová odpovídající úroveň abstrakce. Modul by měl prostřednictvím konstruktivistických metod (např. rámce E-U-R a fyzických simulací) konfrontovat žákovské představy a vytvářet podmínky pro porozumění síťové architektuře.

2.4 Teoretická východiska výzkumu

Tvorba nového výukového modulu a jeho zavádění do praxe není pouze intuitivním pedagogickým procesem, ale vyžaduje jasné ukotvení v metodologii pedagogického výzkumu. Pro účely této práce, jejímž cílem je vytvořit, otestovat a následně optimalizovat didaktické materiály pro střední školy, byla zvolena kom-

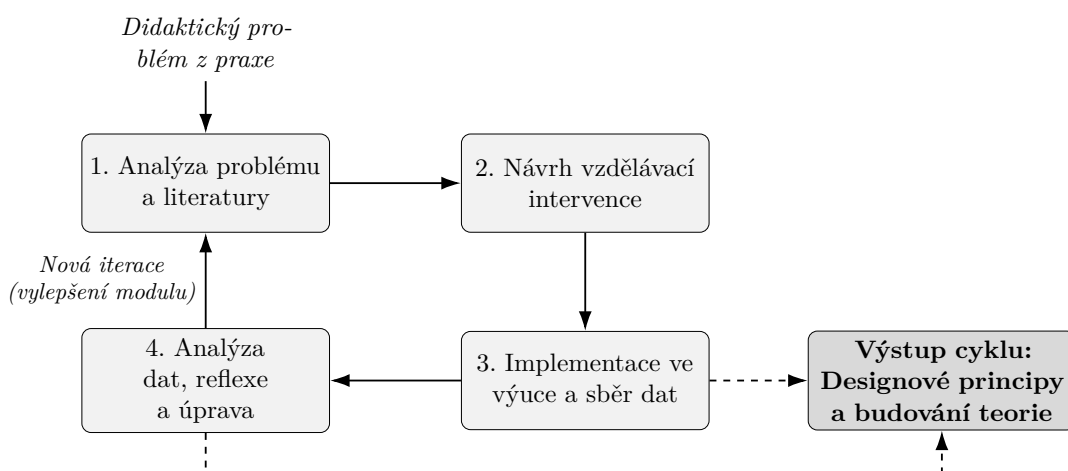
binace dvou komplementárních výzkumných přístupů: konstrukčního a akčního výzkumu.

Toto propojení umožňuje zkoumat vzdělávací realitu přímo z pozice vyučujícího a zároveň systematicky pracovat na iterativním vývoji konkrétního didaktického produktu.

2.4.1 Konstrukční výzkum

Konstrukční výzkum (Design-Based Research, DBR) je výzkumný přístup, který se snaží co nejlépe propojit pedagogickou teorii s každodenní školní praxí. Na rozdíl od klasických experimentů, které často zkoumají izolované jevy v uměle kontrolovaných podmínkách, probíhá DBR přímo ve vzdělávacím prostředí [42].

Základním principem této metodologie je iterativní cyklus. Celý proces začíná analýzou konkrétního problému z praxe a studiem odborné literatury. Následuje fáze návrhu samotné vzdělávací intervence, která je poté implementována do reálné výuky, během které probíhá sběr dat. Na základě analýzy těchto dat dochází k reflexi a následné úpravě výukových materiálů. Celý proces je znázorněn na obrázku 2.7.



Obrázek 2.7 Schéma iterativního cyklu metodologie Design-Based Research

Celý tento cyklus se opakuje tak dlouho, dokud se nedosáhne požadované kvality. V původním akademickém pojetí DBR je zásadní, že cílem není jen vyřešit lokální problém ve výuce, ale také přispět k budování teorie prostřednictvím formulování přenositelných designových principů [42]. V kontextu této práce je však tato teoretická rovina záměrně redukována. Z metodologie DBR je převzat a aplikován především její silný praktický rámec sloužící k iterativnímu vývoji, pilotáži a optimalizaci konkrétního výukového modulu, aniž by primárním cílem byla ambice formulovat nové obecné didaktické teorie. Výhodou tohoto přístupu je i jeho metodologická volnost – typicky využívá smíšené metody (kombinaci kvalitativních a kvantitativních nástrojů), díky čemuž dokáže lépe a pragmatičtěji reagovat na reálné potřeby [42].

2.4.2 Akční výzkum a role učitele-výzkumníka

Zatímco konstrukční výzkum poskytuje rámec pro celkový vývoj materiálů, akční výzkum definuje roli samotného učitele v tomto procesu. Akční výzkum je specifický tím, že jej nerealizuje externí a nezávislý pozorovatel, ale přímo učitel ve své vlastní třídě. Jeho cílem je hlouběji porozumět vlastní pedagogické praxi, identifikovat problematická místa a aktivně je řešit.

Spojení konstrukčního a akčního výzkumu představuje v didaktice přirozený a funkční přístup [42]. Učitel v tomto modelu vystupuje ve dvojí roli: jako výzkumník-designér navrhující vzdělávací materiály a současně jako vyučující, který je přímo aplikuje v praxi. Tradiční výzkum může tuto úzkou vazbu mezi vývojem a realizací výuky vnímat jako hrozbu pro objektivitu. V kontextu DBR je však hluboká znalost prostředí naopak faktorem, který validitu výzkumu posiluje [42]. Učitel v roli výzkumníka dokáže okamžitě zachytit reakce třídy, odhalit žákovské prekoncepce a přímo na ně reagovat. Subjektivní pohled zde tedy není na škodu, ale pomáhá lépe porozumět tomu, co se v hodině skutečně děje.

V praxi se oba přístupy přirozeně doplňují. Konstrukční výzkum dává celému projektu architektonický rámec — určuje, že materiály vyvíjíme v iterativních cyklech od návrhu přes testování až po úpravy. Akční výzkum se pak projevuje při samotné výuce, kterou testuje přímo učitel ve svých vlastních třídách, nikoliv nezávislý pozorovatel. Každá iterace v rámci DBR, jako je pilotáž a následné úpravy aktivit, tak staví na sebereflexi učitele, který funkčnost designu vyhodnocuje přímo v reálném provozu se svými žáky.

2.5 Formativní hodnocení jako nástroj ověřování

Nezbytnou součástí iterativního vývoje v rámci konstrukčního výzkumu je průběžný sběr relevantních dat o tom, zda navržené vzdělávací aktivity skutečně vedou k budování odpovídajících mentálních reprezentací a porozumění učivu. V konstruktivisticky pojaté výuce není vhodné spoléhat se primárně na tradiční sumativní testování (například závěrečný písemný test). Sumativní hodnocení se zaměřuje na zjištění a změření konečného výkonu žáka na konci určitého vzdělávacího období [43]. Ačkoliv kvalitně koncipovaný sumativní test dokáže spolehlivě změřit nejen reprodukci faktů, ale i hlubší úroveň porozumění, jeho limitem pro účely iterativního vývoje je absence průběžné zpětné vazby. Neposkytuje totiž učiteli okamžitý vhled do samotného procesu učení a neumožňuje mu formativně reagovat na příčiny případného nepochopení přímo během vyučovací hodiny. Z tohoto důvodu se jako jeden z klíčových nástrojů ověřování výzkumných cílů v DBR využívá hodnocení formativní.

Zatímco sumativní přístup představuje hodnocení učení (assessment of learning), formativní přístup funguje jako hodnocení pro učení (assessment for learning) [43]. Neplní tak ve výuce pouze roli pedagogickou (tedy poskytování okamžité a konkrétní zpětné vazby žákům pro zefektivnění jejich učení [43]), ale v akčním a konstrukčním výzkumu plní i roli výzkumnou. Slouží jako důležitý diagnostický nástroj učitele-výzkumníka. Sledování žáků během skupinové práce, analýza jejich argumentace při řešení problémů s didaktickými analogiemi nebo rozbor výstupů z pracovních listů poskytují okamžitá data o kognitivním postupu třídy. Vyučující tak v reálném čase vidí, zda žáci správně překonávají své původní prekoncepce,

a v souladu s principy formativního přístupu může operativně přizpůsobit výuku zjištěným potřebám [43].

Aby však bylo možné formativní hodnocení úspěšně aplikovat, musí učitel dokázat specifikovat svá očekávání a jasně definovat, co představuje takzvaný důkaz o učení [43]. Výukové aktivity musí být záměrně designovány tak, aby tyto důkazy přirozeně generovaly – například tím, že nutí žáky své kroky a myšlenkové postupy verbalizovat a obhajovat při fyzických simulacích či řízených diskuzích. Získaná data z tohoto průběžného formativního mapování následně představují primární vstup pro kritickou reflexi odučené hodiny a pro další iteraci a korekci výukových materiálů, čímž se cyklus konstrukčního výzkumu uzavírá [42].

Část II

Praktická část

3 Návrh a popis výukového modulu

Tato kapitola představuje hlavní výstup praktické části práce – kompletní návrh a popis čtyřhodinového výukového modulu zaměřeného na fungování internetu a počítačových sítí. Cílem této části je přenést teoretická východiska, popsaná v předchozích kapitolách, do praxe.

Navržený modul je koncipován primárně pro žáky středních škol a odpovídajících ročníků víceletých gymnázií. Vyučujícím nabízí ucelenou metodickou oporu, která je striktně postavena na konstruktivistických principech a klade si za cíl minimalizovat pasivní frontální výklad ve prospěch budování vlastních mentálních modelů.

Samotný text kapitoly je rozdělen do dvou hlavních bloků. První sekce se věnuje strukturalizaci učiva. Reflektuje omezené časové limity RVP, vysvětluje logickou posloupnost čtyř navržených vyučovacích hodin a vymezuje aplikovanou didaktickou redukci – tedy obhajuje, jaké koncepty byly z výuky vědomě odstraněny, aby žáci získali prostor pro hlubší pochopení celkových souvislostí. Druhá sekce následně obsahuje metodický rozbor všech čtyř vyučovacích bloků. Každá hodina je navržena podle třífázového modelu E-U-R, od úvodní evokace a mapování prekonceptů, přes fázi uvědomění s využitím didaktických analogií a fyzických simulací, až po závěrečnou reflexi.

Pro usnadnění orientace je nutné předeslat, že struktura praktické části záměrně nepostupuje chronologicky podle toho, jak probíhal výzkum. Tato kapitola čtenáři představuje výslednou podobu výukových materiálů v jejich plně odladěné verzi. Metodologický rámec, proces iterativního vývoje modulu, analýza nefunkčních návrhů odhalených během pilotáže a celkové vyhodnocení reálného znalostního posunu žáků jsou podrobně rozebrány až v bezprostředně navazujících kapitolách.

3.1 Výběr a didaktická redukce učiva

Tato kapitola popisuje proces výběru témat, zohlednění časových limitů a provedenou didaktickou redukci.

Časová dotace a limity RVP

Jak bylo analyzováno v teoretické části (viz kapitolu 2.1.3), výuce počítačových sítí lze v rámci celkové dotace informatiky věnovat pouze jednotky vyučovacích hodin. Vytvořený modul v rozsahu čtyř vyučovacích hodin (zhruba jednoho měsíce výuky) proto představuje realistický kompromis. Na jedné straně respektuje omezené časové možnosti škol, na straně druhé však tvoří nezbytné minimum pro smysluplnou aplikaci konstruktivistického přístupu (model E-U-R) a fyzických simulací, které by jinak musely ustoupit pasivnímu frontálnímu výkladu.

Práce s prekoncepty a reálný stav žáků

Teoretická část této práce rovněž identifikovala propast mezi očekávanými výstupy základní školy a reálnými znalostmi žáků. Tato situace byla v rámci

realizovaného testování modulu navíc umocněna faktem, že zapojení žáci během svého předchozího studia neabsolvovali modernizované výukové bloky zaměřené na síť a budování mentálních modelů. Neměli tak možnost projít výukou, která by systematicky pracovala s dětskými prekoncpcemi (jak je pro české prostředí zmapovala např. Yaghobová [3]). Žáci se proto nesetkali s materiály, jež se tento deficit na nižších stupních snaží řešit – ať už jde o aktivity pro první stupeň ZŠ od Drobné [36], nebo o navazující moduly pro druhý stupeň z tvorby Petře [37], Šmída [4] či Mazné [5].

Výuka tak nemohla přímo stavět na znalostech, které by si žáci osvojili v rámci výuky na ZŠ. Z tohoto důvodu není navržený modul koncipován tak, aby předpokládal zvládnutí učiva nižších stupňů. Evokační a úvodní fáze jednotlivých hodin jsou záměrně navrženy tak, aby tyto prerekvizity nejprve zmapovaly, vyrovnaly rozdíly mezi žáky a případně korigovaly chybné laické představy. Teprve na tomto sjednoceném základě jsou následně budována pokročilá středoškolská témata.

3.1.1 Tematická struktura a posloupnost modulu

Výběr a řazení témat sleduje didaktický princip postupu od konkrétního k abstraktnímu. Jednotlivé hodiny na sebe navazují tak, aby každá řešila problém, který přirozeně vyplynul z předchozí hodiny.

První hodina se zaměřuje na lokální síť prostřednictvím žákům známého prostředí domácí Wi-Fi. Cílem je dekonstruovat běžný uživatelský pohled na domácí router a představit jej jako aktivní síťový uzel, který zajišťuje provoz v lokální síti. Žáci tak začínají analýzou technologie, se kterou mají každodenní zkušenost.

Druhá hodina přechází od lokálních sítí k sítím rozlehlým a vysvětluje samotný princip přenosu dat na dálku. Do výuky je zaveden koncept paketového přenosu a směrování (routing). Výklad a aktivity se soustředí na proces fragmentace dat, jejich nezávislé putování přes různé síťové uzly a následnou zpětnou kompletaci v cílovém zařízení.

Třetí hodina přímo reaguje na zranitelnost přenosu dat veřejnou sítí, která vyplynula z předchozí hodiny. Základem je kybernetická bezpečnost. Jakmile žáci porozumí tomu, že pakety putují přes cizí uzly, je zavedena problematika ochrany dat před odposlechem. Hodina se zaměřuje na základní principy šifrování a technické fungování virtuální privátní sítě (VPN).

Čtvrtá hodina celý modul uzavírá problematikou Internetu věcí (IoT), která slouží jako syntéza předchozích poznatků. Žáci zde aplikují nabyté vědomosti na nestandardní koncová zařízení (chytré spotřebiče) a zjišťují, že i tyto prvky fungují jako běžné síťové uzly s IP adresou, odesílají pakety a v případě chybějícího zabezpečení představují kritické zranitelnosti sítě.

3.1.2 Aplikovaná didaktická redukce

Aby bylo možné strukturu v kapitole 3.1.1 v daném čase efektivně odučit a dosáhnout u žáků konceptuální změny, bylo nezbytné přistoupit k didaktické redukci. Cílem kurikula pro gymnázia a střední školy není vychovávat síťové specialisty, ale vybavit žáky představou o tom, jak počítačové sítě fungují. Z obsahu modulu byly proto vědomě odstraněny specializované koncepty. Modul se nezabývá například

detailním rozbohem sedmivrstvého referenčního modelu ISO/OSI, neobsahuje výpočty IP adres a masek podsítí a neřeší technické rozdíly na fyzické vrstvě (např. rozdíl mezi switchem a hubem). Důraz je naopak kladen na celkovou abstrakci a pochopení souvislostí.

Výrazné zjednodušení bylo uplatněno také u tématu paketového přenosu. Z výkladu zcela zmizelo rozdělení na protokoly transportní vrstvy (např. TCP a UDP) i detaily samotného paketu včetně přesné struktury hlaviček a datových polí. Modul zároveň zobecňuje způsob, jakým si routery vyměňují informace o topologii sítě a následně staví směrovací tabulky. Router zde vystupuje jako uzel, který již nezbytnou znalostí o okolí disponuje. Cílem této úpravy je přiblížit žákům samotný princip fragmentace dat a jejich nezávislého putování sítí, aniž by výuka narážela na komplexitu dynamických směrovacích protokolů.

Obdobný přístup byl využit také pro blok věnovaný bezpečnosti. Cíl hodiny ne spočívá ve vysvětlení matematických principů kryptografie nebo přesného průběhu šifrovacích protokolů. Technologie jako HTTPS, VPN či koncové šifrování (E2E) v modulu figurují jako funkční nástroje pro zajištění soukromí a integrity přenášených dat. Redukce záměrně opomíjí technickou implementaci (např. rozdíly mezi symetrickou a asymetrickou kryptografií) a upřednostňuje uživatelský význam těchto technologií. Žák by měl porozumět především tomu, k čemu daný nástroj slouží a kterou část komunikace chrání, nikoliv jakým konkrétním algoritmem šifra pracuje.

V oblasti Internetu věcí (IoT) a chytré domácnosti se redukce projevila snahou nezatěžovat žáky roztržitostí komunikačních standardů. Výklad proto zcela vynechává specifické protokoly jako Zigbee, Z-Wave nebo Matter. Zvolená úroveň abstrakce má své opodstatnění. Pro pochopení síťových principů totiž nehraje roli frekvence nebo konkrétní komunikační vrstva daného senzoru. Klíčový je fakt, že z pohledu topologie jde o další bezdrátový uzel v systému. Výklad se proto soustředí výhradně na obecnou bezdrátovou komunikaci a na roli těchto prvků jako koncových bodů, které v síti generují datový provoz.

Popsaná redukce obsahu nevyplyvá pouze z technické složitosti problematiky, ale úzce souvisí s celkovým metodickým pojetím. Konstruktivistický přístup a rámec E-U-R kladou důraz na hluboké porozumění a dlouhodobou retenci znalostí. Tyto cíle mají přednost před pouhým předáváním velkého objemu informací, které je typické pro tradiční transmisivní výuku. Aby žáci získali dostatečný prostor pro samostatné objevování, diskuzi a vlastní formulaci závěrů, bylo nutné upřednostnit hloubku probírané látky před její šířkou. Výběr zachovaného učiva navíc přímo cílí na nejčastější žakovské prekoncepce. Právě konfrontace těchto mýtů o fungování sítí pak pomáhá nastartovat proces konceptuální změny.

3.2 Detailní rozbor výukových hodin

3.2.1 Hodina 1: Bezdrátové počítačové sítě

Metodický list k této vyučovací hodině je k dispozici v příloze A.3.1. Pracovní list tvoří přílohu A.4.1 a prezentace je v příloze A.2.1.

Tato úvodní hodina se zaměřuje na ukotvení základních prvků síťové architektury na příkladu domácí Wi-Fi sítě, kterou žáci běžně znají ze své každodenní praxe. Hlavním didaktickým záměrem je dekonstruovat laický pohled žáků na

připojení k internetu a ukázat jim skryté technické pozadí. Hodina cíleně pracuje s vyvracením prekoncepce, že data putují z jednoho mobilního zařízení přímo do druhého, a nahrazuje ji funkčním modelem sítě s aktivními uzly. Závěr hodiny navíc slouží jako příprava pro pozdější hlubší probírání kybernetické bezpečnosti.

Cíle a zaměření hodiny

- Žák definuje vlastními slovy pojmy domácí síť a koncové zařízení.
- Žák popíše hlavní funkci Wi-Fi routeru v domácí síti a vysvětlí rozdíl mezi routerem, Wi-Fi routerem a samotnou Wi-Fi sítí.
- Žák vysvětlí na konkrétním příkladu (např. odeslání zprávy), jakou roli hraje v síti router a server.
- Žák porovná rozdíly mezi otevřenou a zabezpečenou Wi-Fi sítí a pojmenuje základní rizika otevřených sítí.

Evokace (5–10 minut)

Cíl: Aktivovat dosavadní znalosti žáků, zjistit jejich prekoncepty a vtáhnout je do tématu.

Výuka je zahájena evokačními otázkami, které vycházejí z běžných zkušeností žáků. Vyučující se ptá, proč bývá Wi-Fi občas pomalá, co v síti funguje v případě výpadku internetu nebo jaká rizika přináší neznámý uživatel v naší síti. U každé otázky je žákům poskytnut prostor pro zamyšlení, na což navazuje krátká řízená diskuze. Zásadním didaktickým krokem v této fázi je neopravovat případné chybné žákovské prekoncepce, jako je například představa, že data létají přímo z jednoho mobilního telefonu do druhého. Vyučující může zaznamenávat zaznívající klíčová slova na tabuli, čímž si připraví podklady pro výklad.

Uvědomění si významu (25–30 minut)

Cíl: Představení nových pojmů a jejich aktivní zpracování žáky.

Hodina plynule přechází k diskuzi o možnostech propojení zařízení, kde žáci porovnávají kabelové a bezdrátové varianty. Ve dvojicích následně vypracovávají první úlohu v pracovním listu A.4.1, do které doplňují výhody a nevýhody obou typů připojení. Vyučující definuje pojmy domácí síť a koncová zařízení. Žáci poté samostatně řeší druhou úlohu v pracovním listu, ve které mají za úkol identifikovat běžná koncová zařízení připojující se v domácnosti k internetu. Vyučující zde dbá na přesah do problematiky Internetu věcí (IoT), aby žáci do svých úvah zahrnuli i spotřebiče typu chytrých žárovek či vysavačů, což je následně shrnuto ve společné diskuzi.

Výklad pokračuje principy bezdrátové komunikace prostřednictvím rádiových vln, během kterého žáci průběžně doplňují třetí a čtvrtou úlohu v pracovním listu. Následuje krátká kontrola a poté definice rozdílu mezi technologií Wi-Fi a Wi-Fi routerem.

Zlomovým bodem hodiny je interaktivní dekonstrukce cesty digitální zprávy, kterou vyučující krok za krokem vizualizuje formou nákresu na tabuli. Aktivita

začíná zakreslením dvou mobilních telefonů a příslušných Wi-Fi routerů. Vyučující předkládá žákům problémovou otázku, zda by bylo možné tato zařízení propojit napřímo. Po diskuzi nad limity takového řešení (fyzická neudržitelnost, nerealističnost) je vyvozeno, že síť potřebuje aktivní prvek, který dokáže data poslat správným směrem. Tímto krokem je žákům funkčně definován router, který je následně v několika instancích dokreslen do schématu. Vyučující naznačuje komplexitu sítě přidáním dalších propojovacích cest a případných slepých větví.

Ve chvíli, kdy jsou obě strany komunikace propojeny přes sérii routerů, vyučující proces zastaví a konfrontuje žáky s dalším logickým problémem: „Stačí to k tomu, aby fungoval například WhatsApp? Jak zpráva najde cestu, pokud příjemce není doma, má vybitý telefon, nebo se připojí z úplně jiného místa?“ Tímto cíleným dotazováním je vyvrácena mylná představa, že zprávu uchovává lokální router, a žáci jsou vedeni k uvědomění, že data je nutné někde centrálně uložit. Vyučující zjišťuje, z jakého kontextu žáci znají pojem server (často zmiňují online počítačové hry, kde server udržuje stav hry pro všechny zúčastněné). Na základě této zkušenosti je server definován (zařízení poskytující služby a trvalé uložení dat) a zakreslen do středu budovaného schématu na tabuli. Pro dokreslení reality lze do schématu zanést více nezávislých serverů (např. odděleně pro WhatsApp a Facebook). Na úplný závěr této modelovací aktivity vyučující pomocí odlišné barvy vyznačí skutečnou trasu komunikace: od odesílatele, přes sérii routerů na server, a následně k příjemci.

Poslední část uvědomění je věnována bezpečnosti. Vyučující vysvětluje rozdíly mezi otevřenou a zabezpečenou sítí. Jsou akcentována rizika otevřených sítí (možnost odposlechu, podvržení webových stránek, napadení zařízení), což si žáci bezprostředně upevňují vypracováním poslední úlohy v pracovním listu.

Reflexe (5–10 minut)

Cíl: Upevnit nové poznatky, propojit je a ověřit, zda žáci dosáhli výukových cílů.

Závěr hodiny slouží k formování uceleného obrazu. Vyučující se vrací k původním evokačním otázkám a konfrontuje žáky s tím, jak by na základě nových poznatků opravili své původní chybné prekoncepce. Následuje aktivita nazvaná „Jak spolu souvisejí“, při které jsou žáci rozděleni do dvojic nebo menších skupin. Každá skupina obdrží náhodnou dvojici probraných pojmů (např. mobil – server; otevřená síť – riziko) a má za úkol ve stanoveném časovém limitu (ideálně dvou až čtyř minut) zformulovat a odprezentovat fakticky správnou větu, která tyto pojmy logicky propojuje. Úplný závěr hodiny je věnován formativnímu sebehodnocení, kdy žáci na zadní stranu pracovního listu zapisují, který z pojmů by ještě nedokázali vysvětlit spolužákovi, a formulují, jaká nová informace je v hodině nejvíce překvapila.

3.2.2 Hodina 2: Přenos dat v sítích

Metodický list k druhé vyučovací hodině tvoří přílohu A.3.2, doprovodné karty a materiály k aktivitě jsou v příloze A.3.2. Pracovní list pro žáky je v příloze A.4.2 a prezentace je v příloze A.2.2.

Tato hodina plynule navazuje na předchozí seznámení se síťovou architekturou a zaměřuje se na samotný princip přenosu dat na dálku. Hlavním didaktickým záměrem je vysvětlit proces fragmentace dat, směrování a zavedení pevných komunikačních pravidel. Abstraktní a technicky náročné téma je zde didakticky transformováno pomocí příběhové analogie (stěhování muzejního exponátu) a následně ukotveno prostřednictvím fyzické simulace síťového provozu, ve které žáci na vlastní kůži zažívají zahlcení sítě a ztrátu dat.

Cíle a zaměření hodiny

- Žák definuje účel IP adresy a zdůvodní, proč ji v síti potřebujeme.
- Žák vysvětlí na základě analogie důvody, proč se data před přenosem dělí na menší části (pakety).
- Žák identifikuje v rámci fyzické simulace problémy, které mohou při přenosu dat nastat (např. zahlcení uzlu, ztráta paketu, příchod paketů ve špatném pořadí).
- Žák vysvětlí vlastními slovy pojem síťový protokol jako nezbytnou sadu pravidel pro komunikaci.

Evokace (5–10 minut)

Cíl: Navázat na předchozí hodinu a vytvořit kognitivní konflikt – jak router pozná, kam data poslat, a v jaké formě data cestují?

Výuka je zahájena sérií evokačních otázek spojených s každodenní zkušeností žáků – sledováním videa na platformě YouTube. Vyučující se ptá, odkud se video bere, jak se dostane ze serveru do mobilního telefonu a především, zda přichází celé najednou, nebo po menších částech. Jako vizuální nápověda slouží snímek přehrávače s viditelným pruhem načítání (tzv. buffer). Vyučující rovněž vznáší problémovou otázku, co by měl systém udělat, pokud se některý díl cestou ztratí nebo dorazí pozdě. Odpovědi žáků nejsou v této fázi hodnoceny z hlediska správnosti; vyučující s nimi pracuje pouze jako s výchozími hypotézami a klíčová slova zaznamenává na tabuli jako odrazový můstek pro následný výklad.

Uvědomění si významu (25–30 minut)

Cíl: Pochopení adresování, fragmentace dat a prožití fyzické simulace dynamického směrování a zahlcení.

Fáze uvědomění začíná vyřešením základního problému směrování. Na základě řízené diskuze nad otázkou, podle čeho se router rozhoduje o směru dat, je definován pojem IP adresa jako nezbytný číselný identifikátor. Pro zjednodušení je v rámci modulu operováno pouze se standardem IPv4.

Následně je pozornost přesunuta k problému fyzického doručení velkého objemu dat. Klíčovým prvkem této části je didaktická analogie, vycházející z původního návrhu Drobné [36] a následné modifikace Mazné [5], která je pro potřeby modulu dále adaptována. Vyučující uvádí žáky (pracující ve skupinách po dvou až čtyřech) do role ředitelů muzea, kteří musí zajistit převoz obrovské, křehké a cenné kostry dinosaura do jiné instituce, přičemž originál nesmí opustit depozitář. Žáci pracují s pracovním listem a postupně narážejí na logické problémy. Nejprve odvodí nutnost vytvoření věrné kopie (čímž se vyloučí alternativní neadekvátní návrhy jako virtuální realita nebo vpuštění veřejnosti do depozitáře).

Následně aktivita řeší problém s transportem – kopie se nevejde do jediného kamionu, což si vynutí její rozebrání a uložení do očíslovaných krabic. Vizualizace chaosu mezi neoznačenými zásilkami navede žáky k potřebě balíky popsat, uvést jejich celkové množství a přiložit návod k sestavení. Další krok představuje rozdělení nákladu do více vozidel. Ta volí různé trasy (např. aby se vyhnula dopravní zácpě). Aktivita vrcholí momentem, kdy po doručení a sestavení kostry v cíli jeden kus — konkrétně ocas — chybí. Žáci v této situaci sami odvozují nejúspěšnější řešení: namísto opětovného odeslání celého nákladu si z depozitáře vyžádají pouze tento chybějící díl.

Na vyřešenou analogii plynule navazuje vysvětlení síťové terminologie. Role jednotlivých prvků modelu odpovídají reálným konceptům: dinosaurus reprezentuje přenášený soubor (ze kterého server odesílá vždy pouze kopii), kosti odpovídají samotným datovým paketům a popisky na krabicích představují metadata s informacemi o odesílateli, příjemci a pořadí částí. Skupina aut na různých trasách ilustruje princip dynamického směřování (routing) a dohledání ztraceného ocasu simuluje vyžádání chybějícího paketu poté, co ho přetížený router zahodil.

Teoretický výklad následně přechází do fyzické simulace přímo v prostoru třídy. Deset dobrovolníků se rozestaví podle zadané topologie. Tři žáci zastupují koncová zařízení (klienty K1, K2 a server S), zbylých sedm představuje routery (R1–R7) se specifickými směrovacími tabulkami. Ostatní žáci ve třídě působí jako pozorovatelé. Celá simulace prochází třemi po sobě jdoucími fázemi:

1. **Řízený provoz:** Klient K2 posílá paket přes router R2 k serveru S. Vyučující zpočátku určuje tempo předávání, aby byl proces přehledný. Poté se do komunikace zapojuje také klient K1 se svými pakety.
2. **Zahlcení sítě:** Klient K1 začne v rychlém dvouvteřinovém intervalu odesílat redundantní pakety s označením „#X“. V síti vzniká úzké hrdlo. Routery nestíhají data odbavovat a dochází ke zpoždění. Ztrátu paketu simuluje vyučující tak, že jej zahlcenému žákovi odebere přímo z rukou.
3. **Odpověď:** Server S přijaté pakety postupně kompletuje. Odpověď klientovi K2 odchází až po sestavení celé zprávy, případně po úspěšném vyžádání chybějících dat.

Po ukončení simulace probíhá cílený debriefing. Vyučující se dotazuje konkrétních aktérů na jejich rozhodovací procesy (např. podle čeho R2 volil cestu, proč nemohl K2 komunikovat se serverem napřímo, nebo jak se K1 cítil při zahlcení). Reflektuje se zjištění, že reálný internet se chová identicky – data nechodí popořadě a cesty se ucpávají. Aby mohl takový chaotický systém spolehlivě fungovat, je

nezbytné mít pevně daná pravidla komunikace. Tímto závěrem je plynule zavedena definice síťového protokolu.

Reflexe (5–10 minut)

Cíl: Ověření pochopení hlavních pojmů (IP adresa, paket, protokol).

K závěrečnému upevnění a zhodnocení nabytých znalostí slouží shrnující kvíz (představený v prezentaci). Kvízové otázky jsou zaměřeny na klíčové výstupy hodiny – účel IP adresy, princip rozdělování souboru na pakety, význam pořadových čísel (metadat), reakci sítě na ztracený paket a nutnost existence síťových protokolů pro zamezení chaosu. Společná kontrola a diskuse správných odpovědí uzavírá druhou vyučovací hodinu.

3.2.3 Hodina 3: Bezpečnost v sítích a ochrana dat

Metodické pokyny ke třetí hodině jsou k dispozici v příloze A.3.3. Žákovský pracovní list je přiložen v příloze A.4.3 a prezentace je v příloze A.2.3.

Třetí hodina modulu navazuje na mechaniku síťového přenosu, přičemž se zaměřuje na jeho zranitelnosti a slabá místa. Záměrem výuky je přimět žáky ke kritickému posuzování rizik, která provázejí sdílení dat a pohyb na internetu, a oslabit tak jejich naivní důvěru v bezpečí digitálních systémů. Výklad se opírá o rozbor běžných situací, jako je práce v cloudovém prostředí nebo připojování k otevřeným Wi-Fi sítím. Tyto scénáře slouží k demonstraci možností i reálných limitů konkrétních ochranných nástrojů — konkrétně firewallu, HTTPS, VPN a koncového šifrování.

Cíle a zaměření hodiny

- Žák vysvětlí na základě simulace princip sdíleného cloudového dokumentu a zhodnotí riziko přístupu správce (poskytovatele) k uživatelským datům.
- Žák aplikuje princip fungování firewallu na konkrétní příklady síťového provozu a rozhodne, zda komunikaci propustí nebo zastaví.
- Žák porovná úroveň soukromí při použití nešifrovaného spojení, HTTPS a koncového (E2E) šifrování, přičemž identifikuje, jaká data jsou viditelná pro případného útočníka.
- Žák zvolí a obhájí adekvátní bezpečnostní nástroj (VPN, E2E, HTTPS) pro zadané každodenní situace.

Evokace (5–10 minut)

Cíl: Zopakovat klíčové pojmy z minulých hodin a vytvořit u žáků potřebu poznat mechanismy ochrany dat.

Hodina je zahájena frontální evokací zaměřenou na oživení znalostí z předchozích hodin. Vyučující pokládá žákům sérii otázek týkajících se putování paketů a role routerů v síti. Následně je pozornost přesměrována na problematiku bezpečnosti otázkami typu: „Když vaše zpráva putuje přes cizí routery, může si ji

někdo po cestě přechází?“ Tento dotaz vyvolává u žáků přirozenou nejistotu ohledně soukromí jejich dat a slouží jako efektivní kognitivní přechod k hlavnímu tématu hodiny.

Uvědomění si významu (25–30 minut)

Cíl: Prožití principu fungování cloudových služeb, seznámení se základními nástroji ochrany dat (Firewall, HTTPS, E2E, VPN) a pochopení jejich funkčních limitů.

První část uvědomění je věnována uložení dat. Po krátkém vysvětlení principu komunikace mezi webovým prohlížečem a serverem je zaveden pojem „cloud“. K hlubšímu pochopení tohoto abstraktního konceptu využívá vyučující fyzickou simulaci „Cloudový dokument naživo“. Tato aktivita je inspirována didaktickým konceptem, který ve svých materiálech pro mladší žáky představil Petř [37]. Pro účely tohoto modulu byla původní myšlenka adaptována a modifikována tak, aby odpovídala kognitivním potřebám a znalostem starší cílové skupiny. Žáci jsou rozděleni do skupin, přičemž každá skupina obdrží jeden prázdný papír (reprezentující cloudový dokument) a samolepicí lístky. Jeden žák v roli vlastníka přiděluje ostatním práva editorů (píše přímo do dokumentu) nebo komentátorů (pouze lepí lístky). Skupiny následně kooperují na zadaném tématu, čímž simulují synchronní práci v cloudu.

Během této aktivity vyučující záměrně obchází třídu a bez varování zasahuje do dokumentů jednotlivých skupin (vpisováním textu či vlepováním lístků). V následné reflexi aktivity vyučující analyzuje překvapení žáků a pokládá klíčovou otázku: „Jak je možné, že jsem mohl číst a upravovat váš dokument, aniž byste mi přidělili oprávnění?“. Tato aktivita žákům názorně ukazuje, že vyučující v roli správce simuloval poskytovatele cloudových služeb (např. Google či Microsoft). Ten má k nešifrovaným datům na svých fyzických serverech plný přístup, a to bez ohledu na uživatelské nastavení sdílení v aplikaci.

Další fáze hodiny se zaměřuje na ochranné mechanismy, konkrétně na roli firewallu jako nástroje pro kontrolu a filtraci síťového provozu. Žáci pracují s úlohami v pracovním listu, kde pravidla firewallu aplikují na čtyři modelové situace (nevyžádaný vzdálený přístup, neznámá aplikace odesílající data, stahování systémové aktualizace a přístup na infikovaný HTTPS web). U každého scénáře žáci písemně zdůvodňují své rozhodnutí. Výklad v této části cílí na častou miskoncepci spojenou s posledním scénářem — firewall totiž škodlivý kód z legitimní HTTPS stránky propustí, protože do šifrovaného obsahu paketů ze své pozice nevidí.

Následné vysvětlení šifrovacích standardů se zaměřuje na princip HTTPS a jeho limity (provozovatel serveru má k datům stále přístup). Na toto omezení plynule navazuje koncept koncového šifrování (E2E), u něhož data zůstávají zašifrovaná po celou dobu přenosu a přístup k nim mají výhradně komunikující klienti.

Blok uvědomění uzavírá tematika virtuálních privátních sítí (VPN). Výklad záměrně opouští tradiční, avšak zavádějící představu „zabezpečeného tunelu“ a definuje VPN jako šifrujícího prostředníka v komunikaci. Zásadní je v tomto bodě pochopení, že VPN sice chrání uživatele před odposlechem na lokální (např. veřejné) síti, ale samotný provozovatel VPN serveru má k metadatům o připojení i nadále přístup.

Reflexe (10 minut)

Cíl: Upevnění znalostí prostřednictvím rolové hry a vyvrácení běžných mýtů o absolutní anonymitě na internetu.

Závěr hodiny je strukturován jako analytická hra na internetového detektiva. Žáci se vžívají do role vyšetřovatele a na základě nově nabytých znalostí analyzují provoz na fiktivní veřejné Wi-Fi. Odpovídají na otázky, co by jako detektivové viděli vždy (metadata spojení), co by viděli u nešifrovaného provozu (hesla, obsah) a co by zůstalo skryto i při nejlepší výbavě (zprávy s E2E šifrováním).

Hodina je ukončena cílenou konfrontací dvou velmi častých žákovských miskoncepcí. Vyučující pokládá otázky: „Vyřeší VPN všechny bezpečnostní problémy?“ a „Je anonymní režim v prohlížeči opravdu anonymní?“. Závěrečná diskuze žáky vede k poznání, že VPN nechrání před phishingem a že anonymní režim pouze lokálně maže historii prohlížeče, ale nijak neskrývá aktivitu před poskytovatelem internetu.

3.2.4 Hodina 4: Internet věcí a chytrá domácnost

Metodický list ke čtvrté vyučovací hodině je k dispozici v příloze A.3.4, příslušný pracovní list v příloze A.4.4 a doprovodná prezentace v příloze A.2.4.

Závěrečná hodina celého modulu spojuje předchozí poznatky a přenáší je na nestandardní koncová zařízení v rámci konceptu Internetu věcí (IoT). Hlavním didaktickým záměrem je vyvést žáky z představy, že počítačovou síť tvoří pouze tradiční výpočetní technika jako počítače a telefony. Pozornost se soustředí na kritické zhodnocení chytrých domácností — na logiku jejich síťového propojení, nevyhnutelnou závislost na cloudových službách a bezpečnostní rizika, která s sebou nese sběr osobních dat.

Cíle a zaměření hodiny

- Žák rozliší běžná koncová zařízení od „chytrých“ zařízení na základě jejich schopnosti pracovat a reagovat automaticky.
- Žák porovná možnosti ovládání chytrých zařízení (lokálně z mobilní aplikace vs. vzdáleně přes cloud výrobce) a zhodnotí jejich výhody a rizika.
- Žák vysvětlí tzv. paradox chytré žárovky (závislost na nepřerušném fyzickém napájení).
- Žák identifikuje a kriticky zhodnotí, jaká osobní data vybraná chytrá zařízení sbírají a komu je odesílají.

Evokace (5–10 minut)

Cíl: Identifikace chytrých zařízení v bezprostředním okolí a vymezení jejich základních charakteristik.

Hodina je zahájena evokačními otázkami zaměřenými na přítomnost chytrých zařízení v bezprostředním okolí žáků. Vyučující na tabuli formou brainstormingu zaznamenává jejich nápady. V této úvodní fázi záměrně neprobíhá žádná korekce

ani hodnocení správnosti. Výsledný seznam slouží jako výchozí bod pro další aktivity v hodině, během nichž žáci sami analyzují, zda a kam tato konkrétní zařízení reálně odesílají svá data.

Uvědomění si významu (25–30 minut)

Cíl: Analýza datových toků v IoT, pochopení role cloudových serverů a vymezení limitů chytré domácnosti.

Fáze uvědomění začíná definicí chytrého zařízení. Žáci nejprve v pracovním listu třídí vybrané příklady (notebook, robotický vysavač, dveřní senzor) podle míry jejich autonomie. Cílem je uvědomění, že zatímco tradiční technika (notebook) vyžaduje aktivní povel uživatele, chytré IoT prvky pracují samostatně na pozadí, kde generují datový provoz a reagují na vnější podněty.

Po představení konceptu chytré domácnosti se pozornost přesouvá k samotné síťové infrastruktuře. Vyučující se žáky rekapituluje vlastnosti běžných bezdrátových technologií (Wi-Fi, Bluetooth) z hlediska jejich dosahu a energetické náročnosti. Do tohoto kontextu je následně zasazeno obecné porozumění, že tato koncová chytrá zařízení komunikují bezdrátově, avšak odlišným způsobem než běžná a energeticky náročná Wi-Fi síť.

Klíčovou část hodiny představuje analýza toku dat. Vyučující demonstruje komunikační trasu na příkladu chytrých hodinek. Žáci jsou v této fázi konfrontováni s vlastní prekonceptí, podle které zůstávají veškeré informace z hodinek pouze v jejich mobilním telefonu. Pomocí návodných dotazů (např. na zálohování historie či sdílení sportovních výsledků) žáci sami objevují nutnost zapojení vzdáleného cloudového serveru. Stejnou logiku pak uplatňují na chytrou žárovku. Vyučující pokládá problémovou otázku, proč by odesílání pokynů na vzdálený server mělo mít přednost před přímým spojením s domácím routerem. Žáci si díky tomu uvědomují, že právě cloudová cesta umožňuje dálkové ovládání domácnosti mimo domov. Následně v pracovním listu porovnávají lokální a cloudovou správu z hlediska uživatelského komfortu i bezpečnosti.

Následuje rozbor technických omezení a rizik IoT technologií, který se dělí do čtyř tematických okruhů:

1. **Paradox chytré žárovky:** Manuální vypnutí klasického vypínače odpojí zařízení od napájení a degraduje chytrou žárovku na obyčejný nefunkční hardware.
2. **Závislost infrastruktury:** Výpadek internetového připojení nebo výpadek serverů na straně výrobce znemožní ovládání základních domácích prvků.
3. **Softwarové zastarávání:** Ukončení podpory cloudové aplikace ze strany výrobce mění plně funkční fyzické zařízení v nepoužitelný elektroodpad.
4. **Kybernetická zranitelnost:** Levná a špatně zabezpečená IoT zařízení (kamery, zvonky) představují pro případné útočníky snadný vstupní bod do lokální sítě.

Reflexe (5–10 minut)

Cíl: Kritická analýza osobních dat sbíraných IoT zařízeními a pochopení přesahu digitálních technologií do fyzického soukromí uživatelů.

Závěr hodiny se věnuje vyhodnocení sběru osobních údajů. Vyučující na konkrétních příkladech (chytré hodinky, vysavač či regulace topení) ukazuje, jaká data aplikace ke svému fungování potřebují. Upozorňuje na to, že tyto agregované informace (např. půdorys bytu z vysavače nebo biometrická data) se ukládají na serverech výrobců. Žáci následně ve skupinách vypracovávají finální úkol v pracovním listu. Analyzují tři vybraná zařízení (žárovka, dveřní senzor, chytrá zásuvka) a odvozují, co všechno mohou generovaná data vypovídat o zvyklostech a pohybu členů domácnosti (např. čas odchodu do práce, biorytmus, přítomnost osob v domě). Tato aktivita uzavírá celý výukový modul a podněcuje žáky k kritické reflexi jejich vlastního chování v digitálním prostředí.

4 Metodika výzkumu a testování

Následující kapitola přibližuje metodologický rámec výzkumu, charakteristiku výzkumného vzorku, použité diagnostické nástroje i samotnou organizaci sběru dat. Metodika staví na kombinaci průběžné formativní evaluace a závěrečného sumativního hodnocení. Zatímco formativní část sloužila k postupnému ladění a vylepšování výukových materiálů, sumativní složka měla za úkol kvantifikovat výsledný dopad intervence na vědomosti žáků.

4.1 Cíle a design výzkumu

Výzkum byl navržen na pomezí akčního a konstrukčního výzkumu. Tento přístup byl zvolen pro svou flexibilitu, neboť umožňuje plynule střídat fáze návrhu, testování v praxi a následné reflexe s úpravami.

Hlavním cílem výzkumu bylo zjistit, zda navržený konstruktivistický modul vede k prokazatelnému znalostnímu posunu žáků a k odbourání jejich chybných prekonceptů v oblasti počítačových sítí. Vývoj a testování modulu probíhalo ve třech fázích:

1. **Pilotáž:** Prvotní ověření proveditelnosti modulu v reálné výuce. Cílem nebylo získat statisticky signifikantní data, ale identifikovat kritická místa ve struktuře hodin a v designu výzkumných nástrojů. Na základě této fáze prošel modul i testový nástroj výraznou revizí.
2. **Malé testování:** Ověření upravené verze modulu a stabilizace testových otázek na menším vzorku žáků.
3. **Velké testování:** Finální nasazení modulu se stabilizovaným testovým nástrojem, během kterého docházelo již jen k drobnému ladění (tzv. fine-tuning) výukových postupů směrem k jejich finální podobě.

4.2 Výzkumný vzorek a prostředí

Modul je primárně koncipován pro žáky prvních a druhých ročníků středních škol a odpovídajících ročníků víceletých gymnázií. Výzkumný vzorek byl však cíleně strukturován tak, aby kromě hlavní cílové skupiny pokryl i nižší ročníky, což pomohlo ověřit spodní hranici kognitivní náročnosti navrženého modulu.

Složení výzkumného vzorku se lišilo v závislosti na fázi testování. S ohledem na průběžné změny v docházce a absenci žáků během realizace výzkumu jsou níže uvedeny konečné počty spárovaných pre-testů a post-testů. Tyto dvojice tvoří výsledný vzorek, který byl podroben statistické analýze.

Detailní rozpis finálního výzkumného vzorku pro fázi velkého testování podle jednotlivých škol uvádí tabulka 4.1. Údaje o pohlaví respondentů nebyly záměrně zjišťovány z důvodu zachování maximální anonymity žáků při použití přezdivek a faktu, že genderové rozdíly v porozumění učivu nebyly předmětem výzkumných otázek této práce.

- **Pilotáž** proběhla na jedné střední odborné škole (SOŠ). Po vyřazení nekompletních dat tvořilo finální vzorek pro tuto fázi 22 žáků.
- **Malé testování** proběhlo na jednom pražském gymnáziu. K ověření validity mírně upraveného testového nástroje po pilotáži byl využit vzorek 26 spárovaných žáků.
- **Velké testování** představovalo hlavní fázi sběru dat. Finální výzkumný vzorek tvořilo $N = 154$ žáků z pěti různých gymnázií. Z hlediska věkového rozložení tvořili většinu vzorku žáci kvart a kvint.

Rozpis výzkumného vzorku pro fázi velkého testování, včetně rozdělení podle pohlaví a typů tříd, uvádí tabulka 4.1.

Škola	Třída (stupeň studia)	Pre-test (n)	Post-test (n)	Spárováno (n)
Gymnázium A (pražské)	Tercie (8leté)	25	27	22
Gymnázium B (pražské)	3. ročník (6leté) ¹	30	28	24
Gymnázium C (mimopražské)	Kvarta (8leté)	25	19	15
Gymnázium D (mimopražské)	Kvarta (8leté)	26	26	25
	1. ročník (4leté)	26	30	25
Gymnázium E (mimopražské)	1. ročník (4leté, 2 třídy)	49	44	43
Celkem		181	174	154

¹ Věkově a znalostně odpovídá 1. ročníku čtyřletého SŠ studia.

Tabulka 4.1 Rozpis výzkumného vzorku a úspěšnosti párování dat ($N = 154$)

Zařazení třídy tercie do vzorku bylo motivováno snahou otestovat náročnost modulu u mladších žáků a ověřit kognitivní limity aktivit. Cílem bylo zjistit, zda je zvolená didaktická redukce srozumitelná i pro žáky nižších ročníků, nebo zda jsou koncepty již příliš abstraktní.

4.3 Nástroje sběru dat

Pro zajištění ucelené zpětné vazby a analýzy dat byla využita kombinace kvantitativních a kvalitativních výzkumných nástrojů.

Kvantitativní nástroje: Didaktický test

Znalostní posun žáků byl měřen pomocí nestandardizovaného didaktického testu. Jeho položky byly záměrně konstruovány tak, aby obsahově pokrývaly klíčová témata všech čtyř vyučovacích hodin (bezdrátové počítačové sítě, přenos dat v sítích, bezpečnost v sítích a internet věcí), čímž byla zajištěna obsahová validita nástroje. Ve fázi velkého testování test obsahoval stabilní sadu 30 výroků, které byly tematicky rozděleny do osmi hlavních položek. Každá tato hlavní položka uvozovala specifický síťový či bezpečnostní problém a byla dále rozvedena do 3 až 4 dílčích podotázek (tvrzení). K odpovědím na úrovni jednotlivých výroků byla využita uzavřená třibodová škála s možnostmi „souhlasím“, „nevím“ a „nesouhlasím“.

Pro ilustraci celkové podoby, vnitřní struktury a míry abstrakce výzkumného nástroje je níže uvedena kompletní druhá položka testu, která byla zaměřena na prověření konceptuálního porozumění bezpečnosti bezdrátových technologií:

- „*Heslo k Wi-Fi neslouží jen k přihlášení, ale i k ochraně přenášených dat mezi zařízením a Wi-Fi routerem.*“
- „*Wi-Fi je automaticky bezpečná, není potřeba ji nijak chránit.*“
- „*Antivir na počítači se dokáže postarat i o zabezpečení Wi-Fi.*“
- „*K připojení k Wi-Fi je potřeba nainstalovat speciální aplikaci.*“

Na tomto konkrétním příkladu je patrné, že test neověřoval pouze faktuelní znalosti (např. názvy šifrovacích standardů), ale cílil na odhalení typických žákovských miskoncepcí a prekonceptů (např. záměna role antivirového softwaru a síťového šifrování). Celé znění všech osmi hlavních položek testu je uvedeno v příloze A.1.

Při vyhodnocování byla správná odpověď kódována jako 1 bod, zatímco nesprávná odpověď i volba „nevím“ byly hodnoceny 0 body. Zahrnutí možnosti „nevím“ do designu testu mělo za cíl minimalizovat zkreslení výsledků vlivem náhodného tipování.

K měření efektu výuky a retence znalostí byl využit design tří testování pro každého žáka.

- **Pre-test** zadaný před začátkem výukového modulu ke zjištění výchozích znalostí a prekonceptů (vyplňován v papírové podobě).
- **Post-test** zadaný bezprostředně po ukončení čtvrté vyučovací hodiny k měření okamžitého posunu (vyplňován v papírové podobě).
- **Odložený post-test** zadaný s časovým odstupem dvou až tří měsíců po ukončení výuky k měření trvalosti nabytých poznatků (vyplňován v elektronické podobě).

Sběr dat probíhal ve dvou odlišných formátech. Pretest a post-test byly administrovány v papírové podobě vždy prezenčně pod vedením autora této práce, což zajistilo jednotné instrukce pro všechny zapojené třídy. Následný odložený post-test byl realizován elektronicky a žákům jej distribuovali jejich vyučující informatiky.

Kvalitativní nástroje: Pozorování a sebereflexe

Pro sběr formativních dat nezbytných k iterativnímu vývoji modulu byly využity dva nástroje:

- **Záznamový arch učitele** (viz příloha A.5.1) sloužil k přesnému strukturovanému zápisu o průběhu výuky (např. jaké aktivity byly zrealizovány, reálné časové dotace, odchylky).
- **Pozorovací arch** (viz příloha A.5.2) vyplňovaný přítomnými hospitujícími učiteli, kteří sledovali reakce žáků, srozumitelnost zadání a celkovou dynamiku hodiny nezávislým pohledem.

4.4 Průběh testování a etické zásady

Sběr dat probíhal v období od listopadu 2025 do ledna 2026. Pilotáž i malé testování se uskutečnily v průběhu listopadu, zatímco realizace velkého testování kontinuálně probíhala od listopadu do ledna.

Organizace výuky se v rámci velkého testování mírně lišila v závislosti na rozvrhových možnostech zapojených škol. V jedné třídě (tercie) proběhla výuka standardně formou čtyř oddělených vyučovacích hodin (4×45 minut). Na jednom z gymnázií (vzorek dvou tříd) byl z provozních důvodů celý modul realizován blokově během jediného dne. Na zbylých zapojených školách probíhala výuka ve formě dvou devadesátiminutových bloků (2×90 minut), které byly zpravidla rozloženy do dvou po sobě jdoucích týdnů. Velikost testovaných výukových skupin se přitom pohybovala v rozmezí přibližně od 15 do 30 přítomných žáků. Tato variabilita formátů i velikosti tříd věrně odpovídá realitě běžné školní praxe.

Výuka se ve všech zapojených třídách napříč všemi fázemi výzkumu opírala o jednotnou sadu primárních didaktických materiálů, konkrétně tištěných pracovních listů a výukových prezentací. Tyto materiály byly do výuky nasazeny pokaždé. Vzhledem k iterativnímu charakteru výzkumu se však jejich konkrétní podoba a obsah mezi pilotáží, malým a velkým testováním postupně vyvíjely. Proměnou procházely zejména samotné prezentace – na základě vlastní reflexe z výuky a zpětné vazby od pozorovatelů probíhalo experimentální hledání co nejsrozumitelnějších formulací textu. Během iterací byly některé doplňující informace zkušebně zařazeny a následně opět odebrány, čímž docházelo k průběžné didaktické redukci probírané látky s cílem maximalizovat srozumitelnost a předejít kognitivnímu přetížení žáků. Detailní popis těchto změn a konkrétní podoba inovací napříč fázemi testování jsou následně předmětem kapitoly 5.

Administrace didaktických testů (pre-test i post-test) probíhala systematicky a bez výjimky u všech zapojených skupin. Byla pevnou součástí časového harmonogramu výuky a byla pro ni předem vyhrazena odpovídající časová dotace. Vyplnění pre-testu probíhalo vždy na začátku první vyučovací hodiny a zabralo zpravidla 10 až 15 minut. Shodná časová dotace byla vyhrazena i na konci čtvrté vyučovací hodiny pro administraci post-testu. Z pozorování během výuky vyplynulo, že žáci vyplňovali post-test obvykle o něco rychleji. Tento jev mohl být dán jejich předchozím seznámením s formátem testu, nelze však vyloučit přirozenou snahu žáků o co nejrychlejší dokončení práce ani vliv únavy na konci výukového bloku. Odložený post-test byl administrován elektronicky s odstupem dvou až tří měsíců od poslední odučené hodiny. Jeho zadání probíhalo v rámci běžných hodin informatiky pod dohledem kmenových vyučujících, přičemž časová dotace zůstala obdobná.

Zásadním metodologickým parametrem výzkumu je skutečnost, že výuku všech fází a iterací modulu realizoval výhradně sám autor práce. Díky tomu byla zaručena kontrola nad dodržáním navržených postupů. Průběh výuky byl navíc ve většině případů monitorován dalšími osobami, a to formou průběžných poznámek z náslouchů a následné reflexe bezprostředně po skončení výuky.

Přítomnost pozorovatelů se lišila podle konkrétní fáze výzkumu:

- **Pilotáž a malé testování** proběhly kompletně pod dohledem pozorovatelů z Matematicko-fyzikální fakulty UK (MFF UK), což bylo klíčové pro prvotní odbornou a didaktickou optimalizaci modulu.

- **Velké testování** již probíhalo s variabilní účastí pozorovatelů, danou především časovými a organizačními možnostmi. Na jednom z pražských gymnázií dohlíželi na výuku přímo akademičtí pracovníci z MFF UK. Na dalších dvou školách (jednom pražském a jednom mimopražském gymnáziu) převzali roli pozorovatelů kmenoví vyučující informatiky v daných třídách. Na dalším z mimopražských gymnázií působil jako pozorovatel kolega z pedagogické fakulty. Pouze na jedné ze zapojených škol proběhla výuka zcela samostatně, bez přítomnosti pozorovatele.

Tato kombinace odborného dohledu v raných fázích a samostatnější výuky v závěru testování pomohla zachovat metodologickou správnost. Skutečnost, že všechny hodiny odučil sám autor práce, však přirozeně zůstává jedním z limitů celého testování.

Z hlediska etických zásad a ochrany osobních údajů probíhal výzkum v souladu s vnitřními předpisy zapojených škol. Ve většině případů (zejména u fakultních škol) bylo testování žáků plně pokryto platným generálním souhlasem zákonných zástupců, kterým školy standardně disponují. Pouze v případě jedné zapojené školy byl administrován a vyžadován specifický informovaný souhlas rodičů určený přímo pro účely tohoto výzkumu (vzor viz příloha A.6). Veškerá sebraná data z didaktických testů byla plně anonymizována a spárována (pre-test, post-test, odložený test) výhradně na základě anonymních přezdivek, které si žáci sami vytvořili na začátku prvního testování. Tento postup zaručil, že ani autor práce jako vyučující nemohl zpětně přiřadit konkrétní výsledky k jednotlivým žákům.

5 Výsledky testování

Tato kapitola popisuje výsledky realizovaného výzkumu a je pro přehlednost rozdělena do dvou hlavních bloků. První část se věnuje formativní evaluaci – detailně mapuje iterativní vývoj modulu a popisuje konkrétní didaktické úpravy, kterými jednotlivé vyučovací hodiny prošly na základě zjištění z pilotní fáze, malého testování i následného plného nasazení v praxi. Druhá část má sumativní charakter a zaměřuje se na zhodnocení samotného efektu výuky. Prostřednictvím statistické analýzy dat z pre-testů a post-testů vyhodnocuje reálný znalostní posun žáků, míru dlouhodobé retence učiva a úspěšnost modulu při cíleném odbourávání nejčastějších laických prekonceptů.

5.1 Iterativní vývoj modulu

Zvolená metodologie výzkumu umožnila plynule reagovat na situace vzniklé přímo ve výuce. Původní návrh modulu prošel řadou zásadních strukturálních i obsahových změn, jejichž cílem bylo snížit nadměrnou kognitivní zátěž žáků, posílit konstruktivistický charakter výuky a zajistit lepší proveditelnost pro vyučujícího. Fáze pilotního testování a následného malého testování odhalily několik kritických didaktických i organizačních nedostatků. Na základě hospitačních záznamů a sebereflexe byly provedeny úpravy, které jsou detailně popsány níže.

5.1.1 Úpravy 1. vyučovací hodiny

Původní návrh hodiny počítal s evokační aktivitou, při které měli žáci formou myšlenkové mapy připomenout pojmy spojené s počítačovými sítěmi. V praxi se tento postup ukázal jako neefektivní, a to i při experimentálním přesunutí aktivity na konec vyučovací hodiny. Hlavním problémem byl fakt, že žáci metodu tvorby myšlenkových map dostatečně neovládali. Místo samotné aktivace znalostí tak trávili čas řešením vizuální a strukturální podoby mapy, což vedlo k neúměrné časové ztrátě.

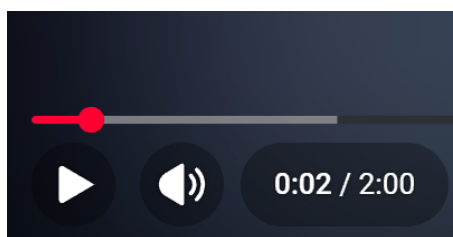
Pro další iterace byla tvorba mapy zcela odstraněna. V úvodu hodiny byla nahrazena řízenými evokačními otázkami z běžné praxe žáků, což zajistilo rychlejší a cílenější aktivaci prekonceptů. Závěr hodiny byl doplněn o reflexní otázky a krátkou aktivitu nazvanou „Jak spolu souvisejí“. V ní dvojice žáků dostávaly dva související pojmy (například *Wi-Fi router* a *domácí síť*) a jejich úkolem bylo naformulovat jedinou větu, která přesně vystihuje vztah mezi nimi. Tento formát se ukázal jako mnohem efektivnější nástroj pro ověření pochopení látky.

Dalším problémem úvodní hodiny byla původní přílišná orientace na frontální předávání informací a kognitivní přehlcení technickými detaily. Z obsahu byly proto pro velké testování plošně odstraněny okrajové koncepty, jako je MAC adresa, captive portál, quishing či bezpečné předávání hesla k Wi-Fi síti. Tato redukce uvolnila prostor pro výrazně konstruktivističtější pojetí výkladu zaměřené čistě na základní principy fungování síťových prvků.

5.1.2 Úpravy 2. vyučovací hodiny

Obsah druhé hodiny vykazoval zpočátku příliš vysokou míru abstrakce, neboť zahrnoval problematiku protokolu IPv6 a strukturu páteřních sítí. V rámci následné didaktické redukce však byla tato témata vyhodnocena jako nadbytečná a z modulu zcela odebrána, což uvolnilo prostor pro klíčové koncepty.

Úpravou prošla již samotná evokace hodiny, do níž bylo doplněno stavění na bezprostřední zkušenosti žáků s každodenním streamováním videa na platformě YouTube. Žáci jsou v rámci diskuze vedeni k uvědomění, že video se do jejich zařízení nestahuje jako jeden celistvý soubor, ale je doručováno postupně. Pro vizuální oporu byl do prezentace doplněn snímek indikátoru přehrávání (viz obrázek 5.1), na kterém je jasně patrný rozdíl mezi aktuálně přehranou částí a daty, která jsou již stažena do vyrovnávací paměti.



Obrázek 5.1 Indikátor přehrávání videa na YouTube

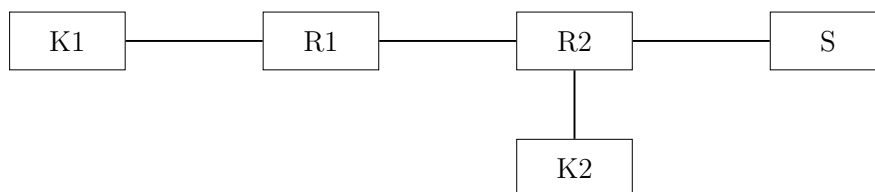
Ačkoliv tato analogie pracuje s odlišnou úrovní abstrakce, neboť videozáznam je technicky dělen na větší segmenty (tzv. chunky), které se až následně rozpadají na jednotlivé síťové pakety, z hlediska evokace slouží jako funkční a intuitivní most k následnému pochopení fragmentace.

Zásadní změnou prošla také didaktická analogie sloužící k vysvětlení principu fragmentace dat. Původní model vysvětloval dělení datových paketů na příkladu „stěhování skříně“. Tato představa se však neukázala jako ideální – jednotlivé díly skříně nemusí mít intuitivní logickou návaznost a především neumožňují dobře demonstrovat vlastnosti digitálního přenosu, neboť ztracené prkno nelze v reálném světě snadno „vyžádat znovu“.

Tento koncept byl proto nahrazen vizuálně atraktivnějším a didakticky ověřeným modelem „stěhování kostry dinosaura“. Aktivita vychází z původního návrhu Drobné [36] a následné modifikace Mazné [5]. Pro potřeby tohoto modulu však byla aktivita autorsky upravena tak, aby co nejpřesněji simulovala reálné digitální prostředí. Už během samotného budování této analogie probíhá se žáky řízená diskuze; řeší se například, proč nelze návštěvníky pustit přímo do depozitáře (což ilustruje oddělení a ochranu dat na serveru) a proč se z něj nestěhuje fyzický originál kostry, ale rovnou se vytváří její identická kopie (princip poskytnutí dat uživateli, zatímco zdrojový soubor zůstává nedotčen na serveru). Tato úprava následně otevírá i prostor pro debatu o tom, co by se stalo, kdyby se po cestě některá část kostry (paket) ztratila, a jak by se situace řešila, čímž žáci přirozeně objevují mechanismus opětovného vyžádání ztracených dat.

Nejvýraznější proměnou však prošla klíčová aktivita zaměřená na fyzickou simulaci síťového provozu. Původní design předpokládal práci ve třech až pěti nezávislých skupinách (v závislosti na velikosti třídy). Žáci ve skupině dostali jednoduchou topologii sítě (viz obrázek 5.2), podle které se rozestavěli. Následně

obdrželi rozstříhaný QR kód, kde každý ústřížek reprezentoval jeden datový paket. Úkolem bylo předat pakety přes žáky (routery) do cíle, tam kód složit a oskenovat mobilním telefonem.



Obrázek 5.2 Zadání topologie sítě pro skupinku 5 žáků



Obrázek 5.3 Čtyři datové pakety složené žáky do výsledného QR kódu

Tento formát v praxi selhal z technických i didaktických důvodů. Mobilní telefony často nedokázaly kód přečíst, protože to vyžadovalo naprosto přesné složení papírků (viz obrázek 5.3). Zároveň žáci nerespektovali stanovená pravidla síťového provozu – místo postupného odesílání paketů předávali všechny ústřížky naráz a zcela ignorovali topologii sítě (předávali si pakety napřímo). Kvůli malému počtu žáků ve skupině byla navíc síť příliš jednoduchá a neumožňovala demonstrovat volbu alternativní cesty při výpadku uzlu. Jeden vyučující přitom nedokázal efektivně monitorovat a korigovat chyby u všech skupin současně.

Aktivita byla proto transformována do podoby řízené celotřídní simulace, do které je fyzicky zapojeno deset žáků reprezentujících složitější síť. Zatímco deset žáků tvořilo fyzickou strukturu sítě, zbytek třídy plnil roli aktivních pozorovatelů – podle zadaných otázek sledovali trasu paketů, činnost jednotlivých síťových uzlů nebo zaznamenávali případné ztráty. Ústřížky QR kódu byly nahrazeny lístky s fragmenty textových zpráv. Zásadní změnou je role učitele, který nyní aktivitu moderuje a diktuje její tempo – odesílatelům nedává všechny pakety naráz, ale distribuuje je postupně. Tím je zajištěno, že zbytek třídy stíhá proces sledovat. Tato řízená forma zvýšila přehlednost celé aktivity a maximalizovala její didaktický potenciál, neboť vyučující mohl efektivně sledovat a okamžitě reflektovat rozhodovací procesy žáků.

5.1.3 Úpravy 3. vyučovací hodiny

Třetí hodina prošla z celého modulu nejrazantnější strukturální i obsahovou redukcí, jejímž hlavním motivem bylo přesnější ukotvení v Rámcovém vzdělávacím programu. Původní návrh hodiny fungoval spíše jako široký katalog kybernetických hrozeb. Evokační fáze pracovala se situacemi jako odemčený mobil v cizích rukou, cizí pohled přes rameno nebo nepozorné kliknutí na podvodný odkaz. Fáze uvědomění pak byla vystavěna na obecném konceptu „Hrozba – Zranitelnost – Ochrana“ (ilustrovaném na podvodných e-mailech a hádání hesel) a následně pokrývala bezpečnost veřejných Wi-Fi sítí, HTTPS, VPN, koncové šifrování, firewall, principy fungování webu a cloudu, cloudová úložiště, metadata a problematiku cookies.

Během pilotáže se ukázalo, že toto pojetí je kognitivně zcela přehlacené a koncepčně se odchyľuje od zamýšleného cíle modulu. Z důkladné analýzy RVP vyplynulo, že řada původně zařazených témat (fyzická bezpečnost zařízení, podvodné e-maily, hesla či cookies) spadá primárně do jiného očekávaného výstupu zaměřeného na obecnou bezpečnost digitálních zařízení. Výukový modul je však primárně zacílen na oblast „lokální počítačové sítě a internet“, u které RVP explicitně vyžaduje pochopení principů „zabezpečeného přenosu dat“ a „firewallu“.

Na základě toho byla hodina zredukována výhradně na síťový přenos. V upravené finální verzi staví evokační fáze na zopakování principu paketového přenosu, přičemž žáci reflektují, zda může datový paket po cestě někdo číst a kdo reálně vidí jejich aktivitu na otevřené Wi-Fi síti. Fáze uvědomění je následně logicky zúžena na vysvětlení toho, jak funguje web a cloud (demonstrováno na živé spolupráci v cloudovém dokumentu), co je to firewall ve smyslu správy přístupu k síti, a jak komunikaci chrání HTTPS, koncové šifrování a VPN.

Spolu s tematickou redukcí probíhalo napříč iteracemi také intenzivní ladění textových formulací na slidech prezentace. Cílem bylo odstranit zažité, avšak pro žáky příliš abstraktní technologické metafory. Typickým příkladem tohoto procesu byla postupná proměna vysvětlení technologie VPN. Původní materiály definovaly VPN tradičně jako „šifrovaný tunel“. Reflexe z výuky však odhalila, že tato zkratkovitá definice nevede u žáků bez hlubší znalosti kryptografie k reálnému porozumění mechanismu. Během iterací byl proto popis na slidech experimentálně upravován a zpřesňován, až se ustálil na mnohem uchopitelnějším vysvětlení. VPN je nově prezentována jako „komunikace s cílovým serverem přes prostředníka, se kterým mám domluvenou vlastní šifru“. Toto přeformulování se ukázalo jako didakticky funkční, neboť žákům jasně ilustruje jak princip šifrování dat, tak mechanismus skrytí původní identity uživatele.

5.1.4 Úpravy 4. vyučovací hodiny

Čtvrtá vyučovací hodina, zaměřená na chytrou domácnost a Internet věcí, prošla napříč testováním zásadním vývojem. Původní návrh modulu zde narazil na didaktický jev známý jako tzv. expertní slepá skvrna (*expert blind spot*). Jde o situaci, kdy vyučující díky své hluboké orientaci v tématu nedokáže přesně odhadnout výchozí úroveň začátečníků a nechtěně přeskočí základní koncepty nezbytné pro jejich porozumění. Vzhledem k vlastní každodenní zkušenosti s pokročilými systémy chytré domácnosti autor primárně předpokládal, že žáci tyto technologie běžně znají a využívají. Tento předpoklad byl navíc umocněn součas-

nou masivní dostupností chytrých zařízení na trhu a věkem žáků, u kterých se přirozeně, avšak mylně, očekávala orientace v těchto moderních trendech. Školní praxe však ukázala pravý opak.

V rámci **pilotního testování** byla evokační fáze vystavěna na nedefinovaném pojmu „chytré zařízení“. Žáci měli uvést nejchytřejší či nejdivnější zařízení ze svého okolí a pokusit se vymyslet zcela nové (např. chytrou skříň). Tato aktivita vyžadovala masivní dopomoc vyučujícího, neboť žáci neměli z čeho vycházet. Následná fáze uvědomění okamžitě přešla k definici IoT a k praktické aktivitě „Kdo dostává data z chytrých zařízení a proč“, kde žáci analyzovali výhody a rizika fiktivní chytré místnosti. Vzhledem k absenci reálných zkušeností žáků s těmito technologiemi však aktivita didakticky silně drhla.

Pro **malé testování** byla proto fáze uvědomění zásadně přepracována a rozšířena o chybějící prerekvizity. Byly zařazeny typy bezdrátových sítí, přes které zařízení reálně komunikují (Wi-Fi, Bluetooth a experimentálně i NFC, jež bylo později pro nadbytečnost opět odebráno). Především však byla se žáky otevřena klíčová diskusní otázka: „Proč vůbec chceme zařízení bez displeje připojovat k internetu a k čemu je mu síť?“ Pozornost se zaměřila na základní logiku toku dat, tedy zda je zařízení posílá přímo do telefonu, nebo do cloudu. Teprve po ukotvení těchto principů následovaly definice IoT, chytré domácnosti a samotná praktická aktivita.

Do finální podoby pro **velké testování** byla hodina dále upravena tak, aby postupovala striktně induktivně od nejjednoduššího ke složitějšímu. Evokace již nestavěla na abstraktním vymýšlení neexistujících věcí, ale na hmatatelné realitě – žáci hledali zařízení ve svém bezprostředním okolí, která neustále sbírají data nebo jsou aktuálně připojena k internetu. Fáze uvědomění následně začínala elementární definicí „chytrého zařízení“, z níž plynule vzešla definice celého ekosystému IoT, přičemž chytrá domácnost posloužila jako jeho specifický příklad.

Výrazně byla ve velkém testování posílena technická a bezpečnostní rovina. Výklad komunikace byl doplněn o zmínku specifických sítí určených výhradně pro chytrou domácnost. Z důvodu prevence kognitivního přetížení nebyly zaváděny konkrétní technické standardy (jako např. Zigbee či Matter), ale žáci byli vedeni k obecnému porozumění, že tato zařízení komunikují bezdrátově, avšak odlišným způsobem než běžná Wi-Fi síť. Se žáky byl řízenou diskusí vybudován mentální model toku dat, na kterém pochopili rozdíl mezi komunikací napřímo a odesláním dat na server výrobce (což jim reálně umožňuje dálkové ovládání mimo domov). Z toho přirozeně vyplynulo zásadní srovnání mezi lokálním a cloudovým řešením chytré domácnosti, s důrazem na rizika a paradoxy IoT, jako je například ztráta funkčnosti drahého hardwaru při ukončení cloudové podpory ze strany výrobce. Teprve s touto teoretickou výbavou žáci úspěšně přistupovali k praktické aktivitě.

Závěrečná reflexe se napříč iteracemi sjednotila do podoby řízené diskuse, v níž žáci hodnotili osobní přínosy a rizika chytré domácnosti, definovali, co jim reálně usnadňuje život, jaká data zařízení plošně sbírají a kdo všechno by k nim měl, či naopak neměl mít přístup.

5.1.5 Reflexe a změny během plného nasazení

Během fáze velkého testování ($N = 154$ na pěti gymnáziích) byl modul z hlediska klíčových konceptů a struktury již stabilizován. Docházelo pouze k drobnému ladění v reálném čase. Tyto úpravy zahrnovaly především optimalizaci časových dotací pro jednotlivé aktivity, drobné přesuny v pořadí prezentovaných témat a úpravy ve formulacích pracovních listů a skupinových cvičení tak, aby zadání byla pro žáky co nejvíce intuitivní.

Významným formativním zjištěním z velkého testování bylo srovnání práce v různých věkových skupinách. Zařazení jedné třídy odpovídající 8. ročníku ZŠ (tercie) potvrdilo teoretické předpoklady o kognitivní náročnosti učiva. Oproti starším žákům postrádali tito respondenti širší technologický rozhled a zkušenosti. Veškeré aktivity vyžadovaly v této třídě delší časovou dotaci, výrazně větší míru podpory ze strany učitele a nutnost využití širšího spektra konkrétních přirovnání a ukázek na úkor abstraktního myšlení. Tento poznatek plně potvrdil a podpořil původní zadání práce cílit modul primárně na žáky 1. a 2. ročníků SŠ (a odpovídající ročníky víceletých gymnázií), pro které je nastavená míra abstrakce plně přiměřená. Výsledky z testování nicméně ukazují, že modul je uplatnitelný i u žáků v závěrečném ročníku základního vzdělávání (respektive v kvartách).

5.2 Zhodnocení efektu výuky

Pro vyhodnocení celkového znalostního posunu žáků byla získaná data analyzována ve statistickém softwaru Jamovi [44]. Z původní sady 30 testových položek byly z hodnocení předem vyřazeny 4 otázky, u nichž medián úspěšnosti v pre-testu činil alespoň 80 %. Tyto položky reprezentovaly koncepty, které byly pro žáky snadné a intuitivní již před začátkem výuky (tzv. efekt stropu). Jejich ponechání v datové sadě by sice analýzu neznemožnilo, ale zbytečně by zvyšovalo míru statistického šumu a snižovalo by citlivost celého testového nástroje na reálný znalostní posun způsobený edukační intervencí. Následující statistická analýza proto pracuje výhradně s očištěnou sadou 26 položek, přičemž maximální dosažitelné skóre je 26 bodů.

Konkrétně se jednalo o vyřazení následujících čtyř tvrzení, u kterých žáci již před výukou prokazovali vysokou míru porozumění. Pro zachování přesného významu jsou tato vyřazená tvrzení níže uvedena v kontextu původních úvodních otázek, ke kterým se v testu vázala:

- **Otázka:** „*Stačí mít doma zapnutou Wi-Fi, abych měl internet?*“
 - Vyřazené tvrzení: „Stačí, protože Wi-Fi je totéž co internet.“
- **Otázka:** „*Co platí o bezpečnosti Wi-Fi sítě?*“
 - Vyřazené tvrzení: „Wi-Fi je automaticky bezpečná, není potřeba ji nijak chránit.“
 - Vyřazené tvrzení: „K připojení k Wi-Fi je potřeba nainstalovat speciální aplikaci.“

- **Otázka:** „Která z následujících tvrzení o ochraně dat na internetu jsou pravdivá?“
- Vyřazené tvrzení: „Když prohlížeč neukáže Nezabezpečeno, je stránka určitě pravá a bezpečná.“

5.2.1 Celkový znalostní posun a retence znalostí

K porovnání výsledků před a po absolvování výukového modulu byla nejprve vypočítána popisná statistika. Do finálního hodnocení byli zařazeni výhradně žáci, u nichž se podařilo bezpečně spárovat výsledky pre-testu a post-testu na základě jejich přezdívky. Celkově bylo od žáků získáno 181 pre-testů a 174 post-testů. Záznamy, které nebylo možné spárovat z důvodu absence žáka v jedné z fází testování či z důvodu chybně vyplněné přezdívky (celkem 47 testů), byly z hodnocení zcela odstraněny, aby nedocházelo ke zkreslení dat.

Konečný výzkumný vzorek pro měření okamžitého posunu tvořilo spárovaných $N = 154$ žáků. Odloženého post-testu (administrovaného online s odstupem 2–3 měsíců) se z tohoto vzorku zúčastnilo $n = 99$ žáků. Tento přirozený úbytek respondentů je standardním jevem, který byl v tomto případě dán absencemi žáků ve výuce a nižší návratností při distančním sběru dat.

Průměrné bodové skóre celého vzorku ($N = 154$) vzrostlo z výchozích 12,9 bodu v pre-testu na 20,9 bodu v okamžitém post-testu (viz tabulku 5.1). U podvzorku žáků, kteří absolvovali i odložený post-test ($n = 99$), činil průměr v pre-testu 13,0 bodu, v okamžitém post-testu 20,5 bodu (viz tabulku 5.2). V odloženém testu skóre u této skupiny kleslo na 18,9 bodu (pokles o 1,6 bodu oproti stavu bezprostředně po výuce). Tento pokles sice odráží přirozené zapomínání, ale celková úroveň znalostí přesto zůstala výrazně nad výchozím stavem.

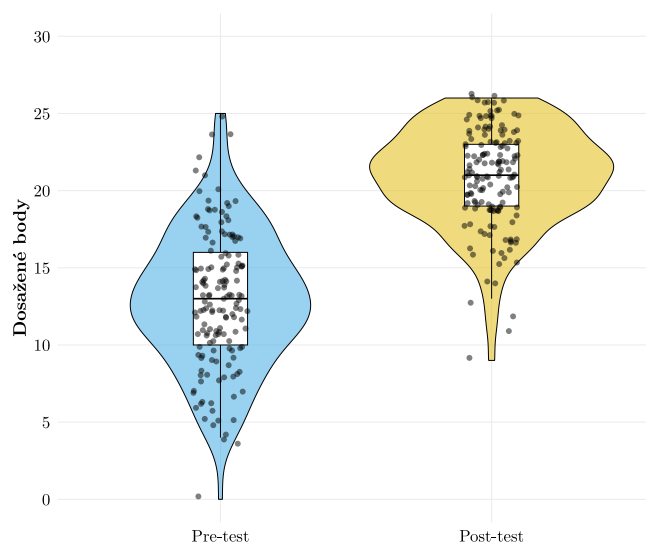
Rozložení bodových zisků zachycují grafy na obrázcích 5.4 a 5.5. Bezprostřední posun po výuce u hlavního vzorku ($N = 154$) znázorňuje obrázek 5.4. Graf ukazuje výrazný posun mediánu k vyšším hodnotám spolu s celkovým zmenšením rozptylu bodů. Data tak dokládají plošné zlepšení výsledků a snížení rozdílů v úrovni znalostí mezi jednotlivými žáky.

Obrázek 5.5 porovnává výchozí stav s odloženým post-testem u podvzorku respondentů ($n = 99$). I přes mírný pokles bodů způsobený časovým odstupem je patrné, že si žáci i po několika měsících udrželi vědomostní úroveň statisticky i vizuálně vysoce nad původním stavem z pre-testu.

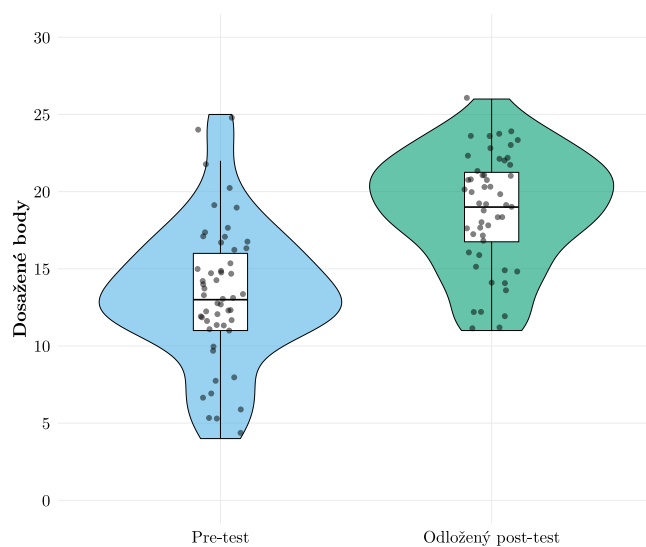
Fáze testování	Průměr	Medián	SD	SE
Pre-test	12,9	13,0	4,45	0,358
Post-test	20,9	21,0	3,26	0,263

Tabulka 5.1 Popisná statistika – okamžitý znalostní posun ($N = 154$)

Pro ověření, zda je zjištěný nárůst znalostí statisticky významný, byl využit párový t-test (Studentovo t). Test potvrdil, že okamžitý rozdíl mezi výsledky pre-testu a post-testu je statisticky vysoce signifikantní, $t(153) = 23,0$, $p < 0,001$. Velikost účinku dosáhla hodnoty Cohenova $d = 1,85$, což představuje velmi silný edukační efekt (viz tabulka 5.3).



Obrázek 5.4 Rozložení celkového skóre: pre-test vs. post-test ($N = 154$)



Obrázek 5.5 Rozložení celkového skóre: pre-test vs. odložený post-test ($n = 99$)

Fáze testování	Průměr	Medián	SD	SE
Pre-test	13,0	13,0	4,51	0,453
Post-test	20,5	21,0	3,31	0,333
Odložený post-test	18,9	19,0	3,93	0,395

Tabulka 5.2 Popisná statistika – retence znalostí s časovým odstupem ($n = 99$)

Dalším krokem bylo zhodnocení dlouhodobého efektu výuky a míry zapamatování učiva. Párový t-test potvrdil, že i po několika měsících od výuky vykazují žáci statisticky významně lepší výsledky oproti svému výchozímu stavu, $t(98) = 12,6$, $p < 0,001$. Velikost účinku u retence znalostí činí Cohenovo $d = 1,27$.

Srovnání	Rozdíl průměrů	t	df	p	Cohenovo d
<i>Celkový výzkumný vzorek ($N = 154$)</i>					
Post-test vs. pre-test	8,00	23,0	153	$< 0,001$	1,85
<i>Podvzorek retence znalostí ($n = 99$)</i>					
Post-test vs. pre-test	7,58	17,2	98	$< 0,001$	1,73
Odložený test vs. pre-test	5,92	12,6	98	$< 0,001$	1,27

Tabulka 5.3 Výsledky párového t-testu pro srovnání edukačního posunu

Z kvantitativního hlediska lze shrnout, že navržený výukový modul vedl k výraznému počátečnímu nárůstu porozumění zkoumaným konceptům. Ačkoliv s odstupem času došlo k přirozenému úbytku zapamatovaných informací (o 1,6 bodu), celková retence znalostí zůstala velmi vysoká.

5.2.2 Odbourávání žákovských prekonceptů

Kvantitativní analýza sice dokládá celkový edukační přínos modulu, pro posouzení jeho didaktické funkčnosti je však nutné analyzovat posun u konkrétních žákovských prekonceptů. Sledování úspěšnosti u jednotlivých testových položek ukazuje, kde navržené aktivity nejúčinněji korigovaly původní mylné představy.

Následující rozbor se detailně zaměřuje na tři oblasti, v nichž žáci zaznamenali nejvýraznější posun v porozumění.

Mýtus přímého spojení a nepochopení síťové infrastruktury

Vstupní test odhalil hluboce zakořeněnou představu žáků, že data v síti putují nejkratší možnou cestou a zcela bez prostředníků. V úloze „*Pošlu zprávu z mobilu na mobil přes internet. Jak zpráva cestuje?*“ zpočátku velká část respondentů souhlasila s chybným tvrzením 3.b („*Letí přímo: mezi telefony existuje přímé propojení.*“). Správný nesouhlas zde v pre-testu vyjádřilo pouze 42 % žáků. S fakticky správným tvrzením 3.a („*Putuje přes různá zařízení, která ji předávají dalším zařízením, dokud zpráva nedorazí do cíle.*“) pak před výukou souhlasilo pouhých 26 % respondentů.

Po absolvování modulu se situace změnila. Úspěšnost při vyvracení mýtu o přímém propojení (položka 3.b) vzrostla na 94 % a správné pochopení principu předávání dat (položka 3.a) stoupl na 73 %. Tento nárůst mohla způsobit například fyzická simulace síťového provozu, během níž si žáci ve třídě data sami předávali přes simulované uzly (routery). Lze předpokládat, že k tomuto posunu přispěla právě hmatatelná zkušenost s přenosem dat, která žákům pomohla nahradit abstraktní představu o neviditelném spojení konkrétnějším obrazem uzlové struktury sítě.

Koncept paketového přenosu

Vůbec nejvýraznější edukační posun v rámci celého výzkumného nástroje byl zaznamenán u položky 3.c, která zkoumala pochopení fragmentace dat: „*Ve skutečnosti se rozloží na malé kousky a pošle se po těchto kouskách, které se v cíli složí zpátky.*“

Před výukou tomuto neintuitivnímu konceptu rozumělo pouze 40 % žáků. Většina žáků se domnívala, že soubory cestují sítí vcelku. Po výuce se úspěšnost u tohoto tvrzení výrazně zvýšila na 96 % (nárůst o 56 procentních bodů). Pro tento markantní posun se nabízí vysvětlení spočívající ve využití didaktické metafory „stěhování kostry dinosaura“ a následné aktivity s doručováním QR kódů, která princip paketového přenosu převedla do snadno uchopitelné podoby.

Iluze datového soukromí u Internetu věcí (IoT)

Značný posun byl zaznamenán rovněž v bloku věnovaném chytré domácnosti. Na úvodní otázku „*Co z následujícího platí o chytrých zařízeních připojených k internetu?*“ navazovalo tvrzení 7.a: „*Chytré zařízení nikdy nezasílá výrobci informace o tom, jak ho používáme.*“

V pre-testu dokázalo tento mýtus o absolutním soukromí identifikovat a správně s ním nesouhlasit pouze 26 % žáků. Po čtvrté vyučovací hodině se úspěšnost zvýšila na 69 %. Z výzkumného hlediska je však nutné k výchozím 26 % přistupovat kriticky. Jak ukázala formativní evaluace hodin, nízká úspěšnost v pre-testu nemusela pramenit výhradně z naivní důvěry žáků v ochranu soukromí, ale spíše z fundamentální neznalosti samotného pojmu „chytré zařízení“. Žáci před výukou často netušili, že zařízení jako žárovka či vysavač vůbec nějakou datovou komunikaci provádějí. Až cílená analýza datových toků (komu a proč IoT zařízení data odesílají) ve čtvrté hodině jim umožnila tento mýtus racionálně dekonstruovat.

6 Diskuze a limity

Sběr kvantitativních i kvalitativních dat potvrzuje, že navržený konstruktivistický modul dosahuje stanovených didaktických cílů. Výrazný bezprostřední znalostní posun žáků ($d = 1,85$) vykazuje i s odstupem několika měsíců vysokou míru retence ($d = 1,27$). Kromě samotných kvantitativních výsledků však testování přineslo podstatné informace o fungování jednotlivých didaktických nástrojů a o tom, jak žáci vnímali vybrané síťové abstrakce.

Zaznamenané výsledky naznačují, že fyzické simulace mohou představovat účinnou cestu k narušení chybných prekonceptů. Lze předpokládat, že konkrétní pohybová aktivita žákům pomáhá vizualizovat jinak neviditelné síťové pochody. Výrazný nárůst porozumění paketovému přenosu (z původních 40 % na 96 %) tak mohl být podpořen právě odvozením principu na základě fyzické zkušenosti, což odpovídá didaktickému záměru této aktivity a teorii konceptuální změny. Získaná data odpovídají závěrům mezinárodních šetření [45, 46]. Botturi [45] upozorňuje, že bez cílené didaktické intervence vnímají dospívající internet pouze skrz povrchovou vrstvu izolovaných aplikací a procesní tok dat na pozadí zcela opomíjejí. Zatímco v zahraničním výzkumu [46] téměř polovina respondentů věřila v existenci centrálního počítače, který celý internet řídí, zapojená pohybová simulace nabídla žákům přímou zkušenost s decentralizovanou architekturou. Následný růst úspěšnosti z 26 % na 73 % u příslušných testových položek ukazuje, že zprostředkování decentralizované povahy sítě pomocí skupinové hry je pro žáky kognitivně dobře uchopitelné. Vzhledem k absenci kontrolní skupiny však nelze vliv samotné simulace striktně izolovat od působení ostatních prvků výukového modulu.

Výsledky výzkumu dále konfrontují mýtus o přirozené digitální gramotnosti tzv. digitálních domorodců v oblasti Internetu věcí (IoT). Ukázalo se, že každodenní užívání technologií nevede automaticky k pochopení jejich vnitřního fungování — v pre-testu činila úspěšnost v této oblasti pouhých 26 % (viz kapitola 5.2.2). Tento rozpor mezi uživatelskou suverenitou a nízkým konceptuálním porozuměním síťové infrastruktury potvrzuje také přehledová studie Broma [6]. Ta na základě analýzy mezinárodních dat dokládá, že adolescenti sice spolehlivě ovládají běžné webové služby, jejich představy o fyzické povaze sítě, ukládání dat či roli infrastruktury (kabelů, satelitů) jsou však často fragmentované a naivní. Nárůst úspěšnosti na 69 % v post-testu tak ukazuje, že zařazení témat jako IoT a datové soukromí do středoškolské informatiky představuje nezbytný krok k rozvoji skutečné, nikoliv pouze konzumní digitální gramotnosti.

Z pedagogického pozorování a zpětné vazby během testování vyplynulo, že pro věkovou skupinu tercie víceletých gymnázií se náročnost abstraktního učiva pohybovala na hranici srozumitelnosti. U těchto žáků bylo v průběhu výuky patrné, že při expozici komplexnějších síťových konceptů častěji docházelo ke kognitivnímu přetížení, což naznačuje, že pro tuto věkovou skupinu by modul vyžadoval další didaktickou redukci a delší časovou dotaci.

Z didaktického hlediska však taková redukce v kontextu celého vzdělávacího systému postrádá smysl. Pro 6. a 7. ročníky (resp. sekundu a tercii) již existují validované výukové moduly, které s touto věkovou skupinou pracují cíleně a efektivně [37, 4, 5]. Namísto dublování těchto materiálů je tedy vhodnější využít existující

výukové materiály, které pro tyto ročníky využívají adekvátní didaktické analogie a unplugged aktivity. Zvolené zacílení této diplomové práce na 1. a 2. ročníky SŠ tak reflektuje potřebu diferenciací výuky a přirozeně navazuje na stávající výukové moduly pro základní školy, v nichž středoškolský modul přebírá žáky již vybavené základním mentálním modelem sítě, na němž může dále budovat pokročilejší koncepty.

Z hlediska samotné realizace modelových hodin se jako největší úskalí ukázala časová a kognitivní náročnost komplexních aktivizačních metod. Průběžná reflexe v průběhu výzkumu odhalila, že zařazení otevřených evokačních technik (jako je například tvorba myšlenkových map) v praxi selhávalo. Pozornost žáků se totiž tříštila mezi snahu pochopit samotný formát metody a přemýšlení nad probíraným tématem, což v kombinaci s abstraktní povahou sítí vedlo ke kognitivnímu přehlcení a ztrátě cenného času. Výraznou překážkou se v počátečních fázích stala také expertní slepá skvrna vyučujícího, která vedla k nadhodnocení vstupních znalostí žáků a k přehlcení hodin okrajovými technickými detaily.

Jako významný prvek se naopak ukázalo následné uplatnění didaktické redukce a přechod k vysoce strukturovanému vedení výuky. Úprava modulu, která nahradila volné skupinové experimenty plně moderovanými celotřídními simulacemi, umožnila žákům udržet pozornost na hlavní síťové koncepty. Z průběhu testování tak lze vyvodit, že konstruktivistický model E-U-R je pro výuku počítačových sítí v rámci standardní 45minutové vyučovací hodiny efektivní, avšak vyžaduje, aby vyučující minimalizoval nadbytečné technické detaily a udržoval pevnou organizaci výuky.

6.1 Limity výzkumu a navrženého modulu

Při interpretaci výsledků testování je nezbytné zohlednit několik metodologických a organizačních limitů, které mohly získaná data do určité míry ovlivnit.

6.1.1 Efekt výzkumníka a absence kontrolní skupiny

Významným metodologickým limitem tohoto šetření je skutečnost, že výuku všech 154 žáků realizoval výhradně autor modulu. Vzhledem k autorově detailní znalosti materiálů a orientaci v tématu nelze garantovat stejnou míru efektivity v případě, kdy by modul implementoval jiný vyučující pouze na základě předložených metodických listů. Výzkumný design navíc nezahrnoval kontrolní skupinu a neporovnával tak výsledky modulu s tradiční transmisivní výukou. Z výsledků lze vyvodit, že navržený postup je didakticky funkční, data však neumožňují jeho přímé statistické srovnání s jinými metodami.

Určitým limitem je rovněž složení výzkumného vzorku z hlediska jeho celkové reprezentativnosti. Školská zařízení do výzkumu nebyla vybrána na základě striktního statistického klíče, ale na základě jejich dobrovolné účasti a vzájemné spolupráce. Lze však konstatovat, že výzkum nebyl izolován pouze na specifické prostředí hlavního města Prahy, ale zahrnoval jak pražská, tak mimopražská gymnázia. Tato geografická variabilita sice zvyšuje věrohodnost získaných dat v kontextu běžné školní praxe, vzorek pěti institucí však přesto nelze považovat za plošně reprezentativní vzorek středoškolské populace v České republice.

6.1.2 Limity plynoucí z organizace výuky a časových rozestupů

Ačkoliv byla administrace didaktických testů u všech výzkumných skupin sjednocena, dalším limitem zůstává variabilita v celkovém rozvržení výuky. U většiny zapojených tříd probíhala výuka ve dvou blocích rozložených do dvou po sobě jdoucích týdnů. V případě jedné ze škol však byla z provozních důvodů realizována blokově během jediného dne.

Tento rozdíl ovlivňuje časový rozestup mezi pre-testem a post-testem. Zatímco u žáků s blokovou výukou měřil post-test bezprostřední poznatky s odstupem pouhých několika hodin, u žáků s rozloženou výukou mohly do výsledků zasáhnout faktory jako samostudium mezi bloky či zapomínání v čase. U blokové výuky bylo naopak nutné počítat s vyšším rizikem kognitivní únavy žáků na konci testovacího dne. Ačkoliv tato proměnná ztěžuje přímou komparabilitu okamžitého znalostního posunu mezi konkrétními školami, z širšího pohledu tato variabilita zvyšuje věrohodnost výzkumu, neboť přibližuje podmínky testování nehomogenní realitě běžné školní praxe. Tyto metodologické i organizační limity však bezprostředně formují podněty pro navazující výzkumnou činnost.

6.1.3 Podněty pro budoucí výzkum

Popsané limity otevírají několik směrů, kterými by se měl budoucí výzkum v oblasti didaktiky počítačových sítí ubírat. Prvním logickým krokem v navazující práci by mělo být ověření přenositelnosti navrženého výukového modulu. To v praxi znamená předat vytvořené metodické a pracovní listy kmenovým učitelům informatiky na různých typech středních škol, kteří by výuku realizovali samostatně, bez přímého zasahování autora práce. Následné měření znalostního posunu žáků u těchto nezávislých vyučujících by umožnilo eliminovat efekt výzkumníka a potvrdilo by, zda jsou materiály dostatečně robustní, intuitivní a univerzálně použitelné v běžném pedagogickém provozu.

Druhý krok pro navazující výzkum představuje úprava výzkumného designu na pedagogický experiment s využitím kontrolní a experimentální skupiny. Takové uspořádání by umožnilo statisticky porovnat efektivitu navrženého konstruktivistického modulu s tradiční transmisivní výukou, která se opírá o standardní učebnice. Výzkumný vzorek by bylo vhodné rozšířit o střední odborné školy ne-technického zaměření a realizovat sběr dat i v dalších krajích ČR pro dosažení vyšší reprezentativnosti. Budoucí práce by tak mohla exaktně ověřit, zda a do jaké míry přináší zvolená didaktická redukce vyšší míru retence učiva v porovnání s klasickým encyklopedickým výkladem síťového hardwaru.

Třetím krokem je další rozvoj a rozšíření samotných výukových materiálů. Současný modul se kvůli časovým limitům běžné výuky musel zaměřit pouze na nejkritičtější koncepty. Navazující práce by však mohla tento základní čtyřhodinový blok doplnit o volitelné nadstavbové moduly. Ty by pokrývaly například principy kryptografie, směrovací protokoly nebo praktické základy lokálního řízení chytré domácnosti bez závislosti na cloudu. Vyučující by je pak mohli snadno zařadit v případě vyšší časové dotace nebo v rámci specializovaných informatických seminářů.

Z hlediska formátu materiálů představuje slibnou cestu částečná digitalizace pracovních listů a vytvoření interaktivního webového prostředí. To by žákům umožnilo samostatně krokovat a vizualizovat síťový přenos, například v podobě zjednodušeného digitálního simulátoru. Východiskem v tomto směru může být výuková aplikace Ondřeje Kohuta [47], která úspěšně vizualizuje základní principy internetu pro žáky základních škol. Budoucí rozšíření středoškolského modulu může na tento koncept přímo navázat, adaptovat jeho vizuální prvky pro vyšší úroveň kognitivních cílů gymnazistů a prohloubit možnosti samostatného experimentování.

6.2 Doporučení pro pedagogickou praxi

Zkušenosti získané během iterativního vývoje a testování modulu umožňují zformulovat klíčová doporučení pro výuku počítačových sítí na středních školách.

Podle zkušeností autora je častým nedostatkem školní praxe snaha předat žákům nadměrné množství technických specifikací (např. detailní rozbor vrstev modelu ISO/OSI, výpočty IP masek či výčty portů), které pro všeobecné vzdělávání postrádají širší kontext. Pedagogická reflexe i výsledky testování ukazují, že takový přístup klade na žáky neúměrné kognitivní nároky. Výsledkem pak bývá spíše mechanické memorování faktů namísto hlubšího porozumění. Žáci se v záplavě technických detailů snadno ztrácejí, což prokazatelně snižuje jejich motivaci a vede k povrchnímu osvojení látky. Na základě zkušeností z ověřování navrženého modulu proto autor doporučuje provést didaktickou redukci. Výuka by se měla zaměřit primárně na principy s přímým dopadem na uživatelskou bezpečnost a porozumění toku dat. Pochopení mechanismu, jakým data cestují přes uzly v síti, má pro žáky v rámci všeobecného vzdělávání výrazně vyšší prioritu než detailní znalost teoretických vrstev síťových modelů.

6.2.1 Zapojení fyzických simulací (unplugged aktivity)

Z výsledků výzkumu i pedagogické reflexe vyplývá, že počítačové sítě představují pro žáky značně abstraktní systém. Vstupní testování odhalilo hluboce zakořeněné žákovské miskoncepce, jako je například představa o přímém izolovaném spojení mezi dvěma mobilními telefony, které pravděpodobně přetrvávají kvůli převážně teoretickému pojetí běžné výuky. V pedagogické praxi lze proto doporučit pravidelné zařazování unplugged aktivit a fyzických simulací. Fyzické modelování procesů (např. předávání papírových zpráv simulující principy paketového přenosu a zahlcení sítě, nebo manuální zásah vyučujícího do struktury dat) vytváří pro žáky hmatatelnou oporu, která usnadňuje pochopení skrytých mechanismů a podporuje kognitivní procesy nezbytné pro dosažení trvalé konceptuální změny.

6.2.2 Kritický přístup k Internetu věcí a soukromí

Jak ukazují výsledky testování a analýza žákovských prekonceptů, je vhodné, aby se vyučující v pedagogické praxi vyvarovali předpokladu, že současná generace žáků automaticky rozumí vnitřním principům zařízení, která denně používá. Výuka sítí by proto neměla končit pouze u tradiční výpočetní techniky, jako jsou osobní počítače a mobilní telefony, ale měla by koncepčně přesahovat do problematiky

Internetu věcí (např. chytré domácnosti či nositelné elektroniky). Na základě dat z ověřování modulu se jeví jako žádoucí cíleně otevírat diskuzi o povaze osobních dat, která tato specifická zařízení plošně sbírají a odesílají na servery výrobců. Ukázalo se totiž, že počáteční nekritická uživatelská důvěra žáků často neodpovídá reálným bezpečnostním a soukromým rizikům spojeným s provozem IoT infrastruktury.

6.2.3 Práce s prekoncepty a formativní hodnocení

V souladu s modelem E-U-R se doporučuje nezačínat výuku pouhými definicemi, ale cíleným mapováním prekonceptů. Žáci do hodin přicházejí s vlastními, často nepřesnými představami o fungování internetu. Pokud učitel tyto představy v úvodu neidentifikuje, vzniká riziko, že si žáci i přes formální osvojení nového učiva paralelně zachovají svůj původní chybný mentální model světa.

6.3 Shrnutí diskuze a naplnění cílů výzkumu

Vzhledem k výše uvedeným zjištěním, limitům i pedagogickým implikacím lze konstatovat, že stanovené cíle diplomové práce byly naplněny. Hlavní záměr, kterým byl návrh, praktická realizace a následné ověření čtyřhodinového konstruktivistického modulu pro výuku počítačových sítí, se ukázal jako didakticky funkční řešení současného deficitu středoškolských výukových materiálů. Získaná kvantitativní data dokládají, že i přes výraznou didaktickou redukci technických podrobností (jako je vynechání vrstev ISO/OSI modelu či detailní struktury paketů) vede vhodně zvolená forma výuky k trvalému porozumění síťovým principům. Propojení unplugged simulací s rámcem E-U-R se v praxi ukázalo jako funkční cesta, která u středoškoláků podporuje dlouhodobou retenci klíčových znalostí.

Praktické ověření v reálné výuce ukazuje, že k trvalé konceptuální změně a odbourání zažitých miskonceptů netřeba žáky zahlcovat memorováním technických specifikací. Rozhodujícím faktorem je naopak aktivní zapojení do fyzického modelování procesů a přímá konfrontace s jejich uživatelskými návyky — především v tématech kybernetické bezpečnosti a Internetu věcí. Navržený výukový modul, upravený na základě několika výzkumných iterací, tak nabízí prakticky využitelnou a metodicky ukotvenou oporu pro učitele středních škol, která přímo reaguje na probíhající kurikulární reformu v České republice.

Závěr

Cílem této diplomové práce bylo navrhnout, v praxi otestovat a vyhodnotit konstruktivistický výukový modul pro výuku počítačových sítí na středních školách a víceletých gymnáziích. Práce představuje reakci na nedostatek metodických materiálů, které by naplňovaly požadavky revidovaného Rámcového vzdělávacího programu a nabízely funkční alternativu k tradiční transmisivní výuce.

Hlavním výstupem práce je čtyřhodinový vzdělávací modul. Ten pokrývá klíčová témata od bezdrátových lokálních sítí a paketového přenosu dat po kybernetickou bezpečnost a Internet věcí (IoT). Výukový obsah prošel důslednou didaktickou redukcí. Vynecháním vybraných technických detailů, jako je rozbor vrstev ISO/OSI modelu nebo výpočty IP masek, se otevřel prostor pro pochopení samotných principů síťové architektury. Využití modelu E-U-R a pohybových simulací (unplugged aktivit) pomohlo převést abstraktní procesy v síti do konkrétní podoby, která je pro žáky kognitivně uchopitelná.

Ověřování v reálné výuce na vzorku 154 žáků potvrdilo didaktickou účinnost navrženého řešení. Kvantitativní analýza prokázala statisticky významný znalostní posun, přičemž získané vědomosti vykazovaly vysokou míru retence i s odstupem několika měsíců. Srovnání pre-testů a post-testů potvrdilo, že navržený modul účinně koriguje zažitě žakovské miskoncepce, především představu o přímém propojení mezi koncovými zařízeními. Lekce zaměřené na Internet věcí pak ukázaly, že samotné rutinní užívání technologií nevede automaticky k porozumění ochraně dat. Tyto výsledky doplňují diskuzi o tom, že uživatelská suverenita adolescentů často zakrývá hluboké konceptuální mezery.

Práce přináší aplikovatelný výstup pro pedagogickou praxi. Vytvořené metodické a pracovní listy, prezentace a nástroje pro formativní hodnocení tvoří ucelenou sadu materiálů pro okamžité nasazení do výuky. Modul nabízí vyučujícím prověřený postup, jak omezit mechanické memorování technických pojmů a směřovat výuku k rozvoji funkční digitální gramotnosti. Zvolený konstruktivistický přístup spolu s zapojením fyzických simulací se v praxi ukázal jako opodstatněný a účinný nástroj pro nastartování konceptuální změny.

Literatura

1. MINISTERSTVO ŠKOLSTVÍ, MLÁDEŽE A TĚLOVÝCHOVY. *Rámcový vzdělávací program pro základní vzdělávání* [online]. Verze platná od 1. 9. 2023. Praha: MŠMT, 2023 [cit. 2026-04-13]. Dostupné z: <https://edu.gov.cz/dokumenty/rvp-ramcove-vzdelavaci-programy/rvp-zv-ramcove-vzdelavaci-program-pro-zakladni-vzdelavani/>.
2. MINISTERSTVO ŠKOLSTVÍ, MLÁDEŽE A TĚLOVÝCHOVY. *Rámcový vzdělávací program pro gymnázia* [online]. Verze platná od 1. 9. 2022. Praha: MŠMT, 2021 [cit. 2026-04-13]. Dostupné z: <https://edu.gov.cz/dokumenty/rvp-ramcove-vzdelavaci-programy/rvp-g-ramcove-vzdelavaci-programy-pro-gymnazia/>.
3. YAGHOBOVÁ, Anna. *Prekoncepce žáků druhého stupně o fungování internetu*. 2021. Dostupné také z: <http://hdl.handle.net/20.500.11956/127858>. Diplomová práce. Univerzita Karlova, Matematicko-fyzikální fakulta.
4. ŠMÍD, Radek. *Digitální technologie: tvorba didaktických materiálů pro 2. stupeň ZŠ*. 2023. Dostupné také z: <https://hdl.handle.net/20.500.11956/180713>. Diplomová práce. Univerzita Karlova, Pedagogická fakulta.
5. MAZNÁ, Michaela. *Základy fungování internetu: didaktické materiály pro 2. stupeň ZŠ*. 2024. Dostupné také z: <http://hdl.handle.net/20.500.11956/188536>. Diplomová práce. Univerzita Karlova, Matematicko-fyzikální fakulta.
6. BROM, Cyril; YAGHOBOVÁ, Anna; DROBNÁ, Anna; URBAN, Marek. ‘The internet is in the satellites!’: A systematic review of 3–15-year-olds’ conceptions about the internet. *Education and Information Technologies*. 2023, roč. 28, č. 11, s. 14639–14668. Dostupné z DOI: 10.1007/s10639-023-11775-9.
7. BABARI, Parvaneh; HIELSCHER, Michael; EDELSBRUNNER, Peter; CONTI, Martina; DÖBELI HONEGGER, Beat; MARINUS, Eva. A literature review of children’s and youth’s conceptions of the internet. *International Journal of Child-Computer Interaction*. 2023, roč. 37, s. 100595. Dostupné z DOI: 10.1016/j.ijcci.2023.100595.
8. ROUBAL, Pavel. *O počítačích* [online]. [cit. 2026-07-01]. Dostupné z: <https://opocitacich.cz>.
9. DiSESSA, Andrea. A friendly introduction to “knowledge in pieces”: Modeling types of knowledge and their roles in learning. In: KAISER, G.; FORGASZ, H.; GRAVEN, M.; KUZNIAK, A.; SIMMT, E.; XU, B. (ed.). *Invited lectures from the 13th international congress on mathematical education*. Springer International Publishing, 2018, s. 65–84. Dostupné z DOI: 10.1007/978-3-319-72170-5_5.
10. DUIT, Reinders; GROPENGIESSER, Harald; KATTMANN, Ulrich; KOMOREK, Michael; PARCHMANN, Ilka. The model of educational reconstruction – a framework for improving teaching and learning science. In: JORDE, Doris; DILLON, Justin (ed.). *Science education research and practice in Europe: Retrospective and prospective*. SensePublishers, 2012, s. 13–37. Dostupné z DOI: 10.1007/978-94-6091-900-8_2.

11. DIETHELM, Ira; HUBWIESER, Peter; KLAUS, Robert. Students, teachers and phenomena: Educational reconstruction for computer science education. In: *Proceedings of the 12th Koli Calling International Conference on Computing Education Research*. 2012, s. 164–173. Dostupné z DOI: 10.1145/2401796.2401823.
12. KALHOUS, Zdeněk; OBST, Otto. *Školní didaktika* [online]. 1. vyd. Praha: Portál, 2002 [cit. 2026-05-29]. ISBN 80-7178-253-X. Dostupné z: <https://www.digitalniknihovna.cz/mzk/uuid/uuid:cfe789e0-5b61-11e3-ae93-001018b5eb5c>.
13. ČÁP, Jan; MAREŠ, Jiří. *Psychologie pro učitele*. 2. vyd. Praha: Portál, 2007. ISBN 978-80-7367-273-7.
14. POSNER, George J.; STRIKE, Kenneth A.; HEWSON, Peter W.; GERTZOG, William A. Accommodation of a scientific conception: Toward a theory of conceptual change. *Science Education*. 1982, roč. 66, č. 2, s. 211–227. Dostupné z DOI: 10.1002/sce.3730660207.
15. DUIT, Reinders. On the role of analogies and metaphors in learning science. *Science Education*. 1991, roč. 75, č. 6, s. 649–672. Dostupné z DOI: 10.1002/sce.3730750606.
16. GLYNN, Shawn M.; YEANY, Russell H.; BRITTON, Bruce K. (ed.). *The Psychology of Learning Science*. Hillsdale: Lawrence Erlbaum Associates, 1991. ISBN 0-8058-0668-7.
17. JELEMENSKÁ, Patrícia; SANDER, Elke; KATTMANN, Ulrich. Model didaktickéj rekonštrukcie: impulz pre výskum v odborových didaktikách. *Pedagogika*. 2003, č. 2, s. 190–201. ISSN 2336-2189.
18. ZORMANOVÁ, Lucie. *Výukové metody v pedagogice: S praktickými ukázkami*. 1. vyd. Grada, 2012. ISBN 9788024778457.
19. MAŇÁK, Josef; ŠVEC, Vlastimil. *Výukové metody*. Brno: Paido, 2003. ISBN 80-7315-039-5.
20. NÁRODNÍ PEDAGOGICKÝ INSTITUT ČESKÉ REPUBLIKY; MINISTERSTVO ŠKOLSTVÍ, MLÁDEŽE A TĚLOVÝCHOVY. *Rámcový vzdělávací program pro základní vzdělávání* [online]. 2025. [cit. 2026-06-28]. Dostupné z: <https://prohlednout.rvp.cz/zakladni-vzdelavani>. Ve znění Opatření ministra školství, mládeže a tělovýchovy č. j. MSMT-11173/2025-4 ze dne 24. 6. 2025.
21. LESSNER, Dan; LÁNA, Martin; PODRÁZKÁ TOMKOVÁ, Michala; HAUT, Jiří. *Základy informatiky pro střední školy* [online]. Jihočeská univerzita v Českých Budějovicích, Pedagogická fakulta, 2020 [cit. 2026-06-25]. ISBN 978-80-7394-785-9. Dostupné z: <https://archiv-ismysleni.npi.cz/ucebnice/zaklady-informatiky-pro-stredni-skoly.html>. Online učebnice, projekt PRIM.
22. NAVRÁTIL, Pavel. *Informatika pro střední školy 1. díl*. 1. vyd. Computer Media, 2025. ISBN 978-80-7402-517-4.
23. NAVRÁTIL, Pavel; JIŘÍČEK, Michal. *S počítačem nejen k maturitě 2*. 10. vyd. Computer Media, 2018. ISBN 978-80-7402-355-2.

24. KŘÍŽ, Pavel. *Základní pojmy z počítačové grafiky* [online]. 2011-12-05. [cit. 2026-07-01]. Dostupné z: <https://dum.rvp.cz/materialy/zakladni-pojmy-z-pocitacove-grafiky.html>.
25. TALÁČEK, Milan. *Tvorba papírového modelu budovy* [online]. 2011-11-30. [cit. 2026-07-01]. Dostupné z: <https://dum.rvp.cz/materialy/tvorba-papiroveho-modelu-budovy.html>.
26. NĚMEC, Petr. *Úvod do počítačových sítí* [online]. 2008-12-16. [cit. 2026-07-01]. Dostupné z: <https://dum.rvp.cz/materialy/uvod-do-pocitacovych-siti.html>.
27. ČIŽMÁROVÁ, Lenka. *Informatická křížovka – počítačové sítě* [online]. 2011-06. [cit. 2026-07-01]. Dostupné z: <https://dum.rvp.cz/materialy/informaticka-krizovka-pocitacove-site.html>.
28. NĚMEC, Petr. *Počítačové sítě LAN I* [online]. 2009-07-20. [cit. 2026-07-01]. Dostupné z: <https://dum.rvp.cz/materialy/pocitacove-site-lan-i-2.html>.
29. NĚMEC, Petr. *Počítačové sítě LAN II* [online]. 2010-01-26. [cit. 2026-07-01]. Dostupné z: <https://dum.rvp.cz/materialy/pocitacove-site-lan-ii-2.html>.
30. JURAJDOVÁ, Zuzana. *Google Sites 2* [online]. 2018-05-15. [cit. 2026-07-01]. Dostupné z: <https://dum.rvp.cz/materialy/google-sites-2-3.html>.
31. VLČKOVÁ, Jitka. *Počítačová grafika* [online]. 2016-02-26. [cit. 2026-07-01]. Dostupné z: <https://dum.rvp.cz/materialy/pocitacova-grafika-2.html>.
32. GOTTFRIED, Lukas. *3D modelování X – Test 1 Rhino* [online]. 2014-09-17. [cit. 2026-07-01]. Dostupné z: <https://dum.rvp.cz/materialy/3d-modelovani-x-test-1-rhino.html>.
33. VLACH, Josef. *Stavba PC – síťové karty* [online]. 2013-03-13. [cit. 2026-07-01]. Dostupné z: <https://dum.rvp.cz/materialy/stavba-pc-sitove-karty.html>.
34. GABRIEL, Jan. *ICT: síť (pracovní list)* [online]. 2014-06-23. [cit. 2026-07-01]. Dostupné z: <https://dum.rvp.cz/materialy/ict-site-pracovni-list.html>.
35. UMÍME TO. *Umíme informatiku* [online]. [cit. 2026-07-10]. Dostupné z: <https://www.umimeinformatiku.cz/>.
36. DROBNÁ, Anna. *Základy fungování počítačů - didaktické materiály pro 1. stupeň ZŠ*. 2021. Dostupné také z: <http://hdl.handle.net/20.500.11956/147973>. Diplomová práce. Univerzita Karlova, Pedagogická fakulta.
37. PETÍŘ, Ondřej. *Digitální technologie - didaktické materiály pro 6. a 7. třídu ZŠ*. 2025. Dostupné také z: <http://hdl.handle.net/20.500.11956/198686>. Diplomová práce. Univerzita Karlova, Pedagogická fakulta.
38. BERKI, Jan; DRÁBKOVÁ, Jindra. *Základy informatiky pro 2. stupeň základní školy* [online]. Liberec: Technická univerzita v Liberci, 2020 [cit. 2026-06-30]. ISBN 978-80-7494-521-2. Dostupné z: <https://imysleni.cz/ucebnice/zaklady-informatiky-pro-zakladni-skoly>.

39. NAVRÁTIL, Pavel. *Informatika pro 6. ročník ZŠ*. 1. vyd. Computer Media, 2024. ISBN 978-80-7402-472-6.
40. IŠTOK, Milan; HYNEK, Miroslav; BALLA, David; HRNČIŘÍKOVÁ, Marcela; JAGER, Karel. *INFORMATIKA V POHODĚ 6: Pracovní učebnice pro 6. ročník ZŠ a víceletá gymnázia*. 1. vyd. Praha: Taktik International, s.r.o., 2022. ISBN 978-80-7563-488-7.
41. HALBOVÁ, Barbora; BIRD, Lucie; HAVLÍČKOVÁ, Martina; ŠŤASTNÝ, Vít; BASL, Josef. *Národní zpráva ICILS 2023: Počítačová a informační gramotnost, Informatické myšlení*. Praha, 2024. Národní zpráva. Česká školní inspekce. ISBN 978-80-88492-95-5. Dostupné také z: <https://www.csicr.cz>. 1. vydání. Licence: CC BY-SA 4.0.
42. ANDERSON, Terry; SHATTUCK, Julie. Design-Based Research: A Decade of Progress in Education Research? *Educational Researcher*. 2012, roč. 41, č. 1, s. 16–25. Dostupné z DOI: 10.3102/0013189X11428813.
43. LAUFKOVÁ, Veronika. *Formativní hodnocení*. Praha, 2016. Dizertační práce. Univerzita Karlova, Pedagogická fakulta (Oddělení pro vědeckou činnost). Vedoucí práce Karel STARÝ.
44. THE JAMOVİ PROJECT. *jamovi (Version 2.7) [Computer Software]* [online]. 2025. [cit. 2026-02-14]. Dostupné z: <https://www.jamovi.org>.
45. BOTTURI, Luca. "Draw the internet": A visual exploration of how children imagine an everyday technology. *Journal of Media Literacy Education*. 2021, roč. 13, s. 35–48. Dostupné z DOI: 10.23860/JMLE-2021-13-3-3.
46. DIETHELM, Ira; WILKEN, Henning; ZUMBRÄGEL, Stefan. An investigation of secondary school students' conceptions on how the internet works. In: 2012, s. 67–73. ISBN 9781450317955. Dostupné z DOI: 10.1145/2401796.2401804.
47. KOHUT, Ondřej. *Základy fungování internetu - výuková webová aplikace* [online]. Praha, 2023 [cit. 2026-07-10]. Dostupné z: <http://hdl.handle.net/20.500.11956/196387>. Bakalářská práce. Univerzita Karlova, Matematicko-fyzikální fakulta, Katedra softwaru a výuky informatiky. Vedoucí práce Anna YAGHOBOVÁ.

Seznam obrázků

2.1	Ukázky pojetí síťové problematiky v učebnici <i>S počítačem nejen k maturitě 2. díl</i> [23]. © Computer Media s.r.o., 2018	20
2.2	Ukázky z pracovního sešitu <i>opocitacich.cz</i> [8]. © Ing. Pavel Roubal.	22
2.3	Ukázka snímku z materiálu <i>opocitacich.cz</i> , prezentace 2.2 – Fungování LAN, pakety, IP [8]. © Ing. Pavel Roubal.	22
2.4	Ukázka cvičení („rozhodovačka“) na portálu <i>Umíme informatiku</i> [35]. © Umíme to, s.r.o.	23
2.5	Ukázka výukového listu „Seraery a křiřovatyky“ z práce Šmída [4].	24
2.6	Ukázka schematického zapojení podsítě v učebnici <i>Informatika v pohodě 6</i> [40]. © TAKTIK Vydavatelství s.r.o., 2022.	26
2.7	Schéma iterativního cyklu metodologie Design-Based Research	28
5.1	Indikátor přehrávání videa na YouTube	50
5.2	Zadání topologie sítě pro skupinku 5 žáků	51
5.3	Čtyři datové pakety složené žáky do výsledného QR kódu	51
5.4	Rozložení celkového skóre: pre-test vs. post-test ($N = 154$)	56
5.5	Rozložení celkového skóre: pre-test vs. odložený post-test ($n = 99$)	56

Seznam tabulek

4.1	Rozpis výzkumného vzorku a úspěšnosti párování dat ($N = 154$)	45
5.1	Popisná statistika – okamžitý znalostní posun ($N = 154$)	55
5.2	Popisná statistika – retence znalostí s časovým odstupem ($n = 99$)	56
5.3	Výsledky párového t-testu pro srovnání edukačního posunu	57

A Přílohy

A.1 Didaktický test

Poznámka: Pre-test a post-test byly shodné, závěrečný test byl doplněn o zpětnou vazbu a podněty žáků k výuce.

ÚVODNÍ DOTAZNÍK

Přezdívká: _____

v4 2025-11-17

Stačí mít doma zapnutou Wi-Fi, abych měl internet?

	Souhlasím	Nejsem si jistá/y	Nesouhlasím
1.a Stačí, protože Wi-Fi je totéž co internet.	☐	☐	☐
1.b Nestačí, protože Wi-Fi je jen způsob bezdrátového propojení digitálních zařízení.	☐	☐	☐
1.c Pokud je Wi-Fi router připojený k internetu (připojení funguje) a mé zařízení je k němu připojeno, mám přístup k internetu.	☐	☐	☐
1.d Nestačí, ale zařízení se přes Wi-Fi mohou propojit i bez internetu (např. tiskárna s počítačem).	☐	☐	☐

Co platí o bezpečnosti Wi-Fi sítě?

	Souhlasím	Nejsem si jistá/y	Nesouhlasím
2.a Heslo k Wi-Fi neslouží jen k přihlášení, ale i k ochraně přenášovaných dat mezi zařízením a Wi-Fi routerem.	☐	☐	☐
2.b Wi-Fi je automaticky bezpečná, není potřeba ji nijak chránit.	☐	☐	☐
2.c Antivir na počítači se dokáže postarat i o zabezpečení Wi-Fi.	☐	☐	☐
2.d K připojení k Wi-Fi je potřeba nainstalovat speciální aplikaci.	☐	☐	☐

Pošlu zprávu z mobilu na mobil přes internet. Jak zpráva cestuje?

	Souhlasím	Nejsem si jistá/y	Nesouhlasím
3.a Putuje přes různá zařízení, která ji předávají dalším zařízením, dokud zpráva nedorazí do cíle.	☐	☐	☐
3.b Letí přímo: mezi telefony existuje přímé propojení.	☐	☐	☐
3.c Ve skutečnosti se rozloží na malé kousky a pošle se po těchto kouskách, které se v cíli složí zpátky.	☐	☐	☐

Co dalšího musí mít textová zpráva posílaná přes internet, aby dorazila do cíle a adresát na ni mohl odpovědět?

	Souhlasím	Nejsem si jistá/y	Nesouhlasím
4.a Zpráva musí obsahovat informaci o cíli své cesty – tedy adresu příjemce nebo jiný údaj, podle kterého ji lze doručit.	☐	☐	☐
4.b Zpráva obsahuje nejen text (obsah), ale i doplňující informace (metadata), bez kterých by doručení ani odpověď na zprávu nebyla možná.	☐	☐	☐
4.c Pokud zpráva neobsahuje informaci, kdo ji poslal (odesílatele), příjemce neví, komu odpovědět.	☐	☐	☐
4.d Zpráva se doručí vždy sama bez jakýchkoliv dalších údajů — stačí pouze text zprávy (čili její obsah).	☐	☐	☐

Která z následujících tvrzení o ochraně dat na internetu jsou pravdivá?

	Souhlasím	Nejsem si jistá/y	Nesouhlasím
5.a Na Wi-Fi síti bez hesla může někdo v dosahu Wi-Fi signálu číst nešifrovaná data, která já přes tuto Wi-Fi síť posílám i přijímám.	☐	☐	☐
5.b Zařízení, která hlídají síť, většinou vidí, odkud a kam data jdou. Pokud však data nejsou skrytá, mohou vidět i jejich obsah.	☐	☐	☐
5.c Když prohlížeč neukáže „Nezabezpečeno“, je stránka určitě pravá a bezpečná.	☐	☐	☐
5.d Přihlašovací stránka veřejné Wi-Fi znamená, že je použití Wi-Fi bezpečné.	☐	☐	☐

Co z následujícího platí o komunikaci na internetu?

	Souhlasím	Nejsem si jistá/y	Nesouhlasím
6.a Pokud je přenos dat po internetu šifrovaný, obsah zprávy není čitelný, ale ostatní mohou vidět, s kým a kdy odesílatel zprávy komunikuje.	☐	☐	☐
6.b U všech běžných chatů platí, že obsah vidí jen účastníci; provozovatel služby ho číst nemůže.	☐	☐	☐
6.c Pokud si pustím anonymní okno v prohlížeči, na internetu se můžu pohybovat anonymně; weby a služby nedokážou poznat, kdo jsem.	☐	☐	☐
6.d Když mám soubor uložený někde na internetu, může se k němu ten, kdo tu službu provozuje, technicky dostat.	☐	☐	☐

Co z následujícího platí o chytrých zařízeních připojených k internetu (např. žárovka, televize, vysavač nebo hodinky, které lze ovládat přes aplikaci)?

	Souhlasím	Nejsem si jistá/y	Nesouhlasím
7.a Chytré zařízení nikdy nezasílá výrobci informace o tom, jak ho používáme.	☐	☐	☐
7.b Chytré zařízení výrobcí může posílat data o tom, kdy a jak často ho používáme.	☐	☐	☐
7.c I když je zařízení užitečné, může ohrozit naše soukromí.	☐	☐	☐
7.d Odvolání souhlasu v aplikaci způsobí, že výrobce vždy přestane používat naše osobní data.	☐	☐	☐

Máte doma chytrá světla ovládaná aplikací přes internetové servery výrobce. Nástěnný vypínač přerušuje napájení světla. Internet vypadne.

	Souhlasím	Nejsem si jistá/y	Nesouhlasím
8.a Ovládání přes aplikaci přestane fungovat; běžným nástěnným vypínačem ale světla budu moci vypnout nebo zapnout.	☐	☐	☐
8.b Všechno bude fungovat úplně stejně, jako když byl internet zapnutý, včetně ovládání přes aplikaci.	☐	☐	☐
8.c Světla úplně přestanou fungovat a nezapnu je ani nástěnným vypínačem.	☐	☐	☐

A.2 Prezentace

A.2.1 Prezentace pro 1. hodinu

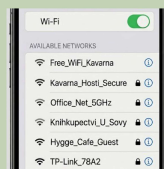
Bezdrátové počítačové sítě

Jste doma připojeni na Wi-Fi, ale internet nefunguje.
Co bude fungovat dál a co ne?

Když pošlete zprávu kamarádovi, kudy
ta zpráva putuje, než mu dorazí?

Co by se mohlo stát, kdyby vaši domácí Wi-Fi
používal někdo úplně cizí?

Když vám dojdou data, jakou síť z nabídky si hned vyberete?
A proč to vlastně nemusí být dobrý nápad?



Možnosti propojení zařízení

- Aby zařízení mohla komunikovat, musí být propojená.
- Jak se zařízení mohou propojit?



Možnosti propojení zařízení

Kabelové připojení

- Rychlé, stabilní, spolehlivé.
- Omezené kabelem.

Bezdrátové připojení

- Pohodlné, mobilní.
- Pokryje celý prostor.
- Snadné připojení nových zařízení.
- Rušení okolními sítěmi.
- Omezený dosah.

V praxi se často **kombinují**.

Domácí síť

- Virtuální prostor, kde se „potkávají“ zařízení např. mobil, notebook a televize.
- Umožňuje zařízením, aby o sobě věděla, mohla si mezi sebou posílat data a společně využívala jeden přístup k internetu.



Z izolovaných přístrojů se stává **jeden funkční celek**.

Koncová zařízení

- Jsou „na konci“ sítě, komunikují pomocí sítě s ostatními.
- Přijímají nebo odesílají data.



Která **koncová zařízení** se doma
běžně připojují k internetu?

Bezdrátová komunikace

- Zařízení spolu komunikují **pomocí rádiových vln**.
 - Nepotřebují kabel – data se přenášejí „vzduchem“.
- Aby si rozuměla, potřebují **společnou bezdrátovou síť**.



Co je to Wi-Fi

- Wi-Fi umožňuje propojení zařízení **bezdrátově**.

Jde pouze o **místní propojení** mezi zařízeními.

Sama o sobě nás ještě **nepřipojí** k internetu.

Wi-Fi ≠ Internet!

Wi-Fi router

- **Vytváří (domácí) Wi-Fi síť**.
- Propojuje bezdrátová a kabelová zařízení.
- Propojuje domácí síť s internetem.
- Řídí tok dat – rozhoduje, kam se která data pošlou.
- **Komunikace je obousměrná**.



Jste doma, připojeni k vaší Wi-Fi.

Kamarád je u babičky, na její Wi-Fi.

Kudy cestuje zpráva, přes jaká zařízení?



Další zařízení v síti

Router (směrovač)

- „Inteligentní křižovatka pro síť“
- **Řídí provoz v síti** a posílá data správným směrem.
- Určuje, kudy mají data projít.



Jste doma, připojeni k vaší Wi-Fi.

Kamarád je u babičky, na její Wi-Fi.

Kudy cestuje zpráva, přes jaká zařízení?



Další zařízení v síti

Server

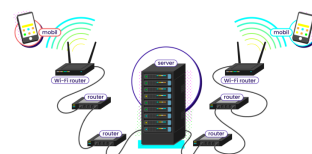
- Počítač **zpracovávající data** nebo **poskytující služby** (např. web, e-mail, WhatsApp).
- **Neustále zapnutý**.



Jste doma, připojeni k vaší Wi-Fi.

Kamarád je u babičky, na její Wi-Fi.

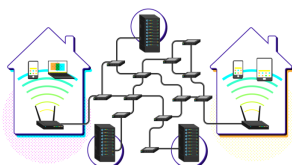
Kudy cestuje zpráva, přes jaká zařízení?



Jste doma, připojeni k vaší Wi-Fi.

Kamarád je u babičky, na její Wi-Fi.

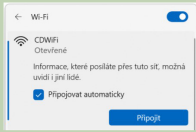
Kudy cestuje zpráva, přes jaká zařízení?



Otevřená síť

- **Otevřená síť** – připojení **bez hesla**.
- Výhody: snadné připojení, není třeba nic zadávat.
- **Řada nevýhod a rizik**
 - kdokoli se může připojit,
 - kdokoli ve stejné síti může sledovat provoz,
 - může nám podvrhnout weby,
 - hrozí napadení zařízení.



Zabezpečená síť Díky heslu se zařízení a router domluví na kódu, kterým si kommunikaci mezi sebou zašifrují. Kdo by to odposlouchával, uvidí jen zmatek znaků. Heslo = vstupní brána a klíč pro šifrování dat.	Jaké zařízení musí doma fungovat, aby se všechna zařízení mohla vzájemně propojit?
Co by se stalo, kdyby doma přestal fungovat Wi-Fi router?	Jste doma připojeni na Wi-Fi, ale internet nefunguje. Co bude fungovat dál a co ne?
Proč je otevřená Wi-Fi síť riziková? 	Když pošlete zprávu kamarádovi, kudy ta zpráva putuje, než mu dorazí?
Jak spolu souvisejí? 1) Wi-Fi router – domácí síť 2) Router – internet 3) Wi-Fi – internet 4) Mobil – Wi-Fi 5) Mobil – server 6) Domácí síť – heslo 7) Otevřená síť – riziko 8) Koncové zařízení – router 9) Wi-Fi – šifrování 10) Domácí Wi-Fi – pokrytí	Použité ilustrace a grafika Obrázky 1, 5, 6, 9, 11, 14: Ilustrace vygenerované pomocí AI (Google Gemini, 2023-2024). Obrázek 8: Ilustrace koncového zařízení (laptop) s otevřenou sítí (Wi-Fi) a routerem. Zdroj: https://commons.wikimedia.org/wiki/File:Ethernet_router_connected_to_laptop.jpg. Obrázky 9, 13, 15, 17: Ilustrace zařízení (laptop) s otevřenou sítí (Wi-Fi) a routerem. Zdroj: https://commons.wikimedia.org/wiki/File:Ethernet_router_connected_to_laptop.jpg. Obrázky 16, 18, 19: Ilustrace zařízení (laptop) s otevřenou sítí (Wi-Fi) a routerem. Zdroj: https://commons.wikimedia.org/wiki/File:Ethernet_router_connected_to_laptop.jpg. Obrázek 20: Ilustrace vygenerovaná AI.

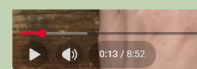
A.2.2 Prezentace pro 2. hodinu

Přenos dat v sítích

Pustíte si video na YouTube.
Odkud se to video vlastně bere?

Jak se video dostane ze serveru až do vašeho mobilu?

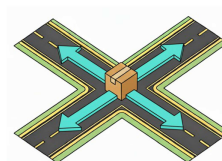
Myslíte, že video přichází celé najednou,
nebo po menších částech?



Když se některý díl ztratí nebo dorazí pozdě,
co by měl systém udělat?

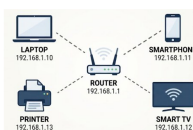
Jak se data dostanou k cíli?

Když data dorazí do routeru,
podle čeho se rozhoduje,
kterým směrem pokračují?



IP adresa

- Každé zařízení v síti má svoji IP adresu, jinak by routery nevěděly, kam data směřovat.
- Číselná adresa zařízení v síti, typicky **čtyři čísla oddělená tečkami**
 - Např.: 192.168.0.12
 - Každé číslo může být od 0 do 255.

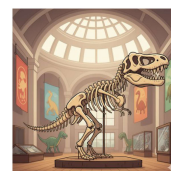


Jak převést kostru?

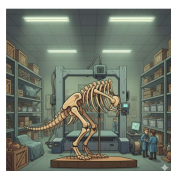
V depozitáři máte obří a velmi křehkou
dinosauří kostru.

Veřejnost ji chce vidět v muzeu, ale originál
je příliš cenný a riskantní na přesun.

Jak byste to vyřešili?

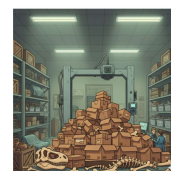


Jak převést kostru?



Uděláme kopii, kterou můžeme vystavit.

Jak převést kostru?



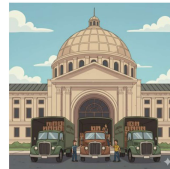
Kopie kostry se rozdělí na části a každá se zabalí zvlášť.

Jak převést kostru?



Části očíslovujeme a uděláme plánek.

Jak převést kostru?



Části naložíme do aut.

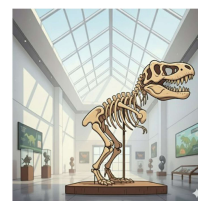
Jak převést kostru?



Auta jedou různými cestami...
V cíli se všechny sejdou a dají dohromady.

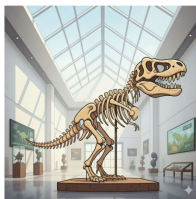
Jak převést kostru?

Může se nějaká část kostry ztratit?
Co udělat když se ztratí?



Jak převést kostru?

Z muzea nám pošlou novou část.



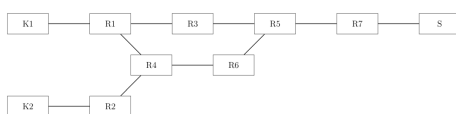
Jak data cestují v síti?

Odesílaná data rozdělí na menší kousky – **pakety**.
Každý paket obsahuje dvě části:

- **přenášenou informaci** – kousek samotných dat,
- **doplňující informace** (metadata) – kdo to posílá, komu, v jakém pořadí to má být složeno, ...

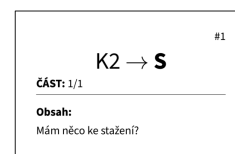
Simulace paketového přenosu

• Mapa sítě



Simulace paketového přenosu

• Posílané zprávy



Simulace paketového přenosu

• Směrovací tabulky

Směrovací tabulka pro R1	
Podmínka	Akce
Paket míří do S	Předej do R3 pak R4
Paket míří do K1	Předej K1
Jinak	Předej R4

Simulace paketového přenosu

- K1 ukládá na server S zprávu pro K2.
- K2 se doptává, jestli má něco na serveru.
 - Pokud ano, zprávu dostane.
- K2 odpoví na zprávu a nechá uložit další na server.

Jak je možné, že dopis umíme všichni číst stejným způsobem – poznáme adresu, obsah i podpis?

Bez pravidel by byla v síti džungle

Při posílání dopisu každý ví, kam napsat adresu, kam známku, kam text – jinak by pošta nefungovala.



Bez pravidel by byla v síti džungle

Síťový protokol – domluvená pravidla pro komunikaci mezi počítači.

Díky nim obě strany vědí

- co mají dělat,
- v jakém pořadí,
- jak má vypadat zpráva.

Různé služby používají různá pravidla (jiný protokol).

Bez pravidel by byla v síti džungle

Síťový protokol – domluvená pravidla pro komunikaci mezi počítači.

Příklad z praxe:

IP adresa → Internet Protocol

(Základní pravidla pro doručování na internetu)

Závěrečný kvíz

1) K čemu slouží IP adresa?

- Umožňuje jednoznačně identifikovat zařízení v síti.
- Určuje rychlost přenosu dat mezi zařízeními.
- Slouží jako heslo pro připojení k Wi-Fi.
- Označuje typ použitého protokolu.

2) Proč má každé zařízení v síti jedinečnou adresu?

- Aby zařízení mohlo mít rychlejší internet.
- Aby router věděl, kam data správně poslat.
- Aby mohla zařízení sdílet mezi sebou hesla.
- Aby se odstranila potřeba routerů.

3) Jak se data posílají přes internet?

- Posílají se vždy jako jeden velký blok.
- Každý paket obsahuje celý soubor.
- Všechny části musí jet po stejné trase a ve správném pořadí.
- Rozdělí se na malé části (pakety), které mohou jet různými cestami.

4) Co se stane, když se paket po cestě ztratí?

- Celá komunikace se automaticky zastaví.
- Odesílatel okamžitě znovu pošle všechny pakety.
- Příjemce zjistí, že něco chybí, a vyžádá si chybějící části znovu.
- Příjemce si domyslí chybějící obsah.

5) K čemu slouží pořadové číslo v paketech?

- Umožňuje příjemci správně poskládat data ve správném pořadí.
- Určuje, přes kterou Wi-Fi se mají data odeslat.
- Slouží jako kontrola, zda má zařízení správnou IP adresu.
- Označuje, která část dat je určena pro který server.

6) Proč jsou protokoly v síti nezbytné?

- a) Bez společných pravidel by zařízení nevěděla, jak komunikovat.
- b) Protokoly přidávají internetu ochranu proti virům.
- c) Zajišťují, že všechna zařízení mají stejnou IP adresu.
- d) Umožňují přenášet data bez potřeby směrování.

Správné odpovědi

- 1 a)
- 2 b)
- 3 d)
- 4 c)
- 5 a)
- 6 a)

Použité ilustrace a grafika

Obrazek 4, 17, 18, 19, 20, 22: Vlastní zpracování.
Obrazek 5, 11, 6, 9, 10, 11, 12, 13, 14, 15: Ilustrace vygenerované pomocí AI (Google Gemini, 2025-10-26).

A.2.3 Prezentace pro 3. hodinu

Bezpečnost v sítích a ochrana dat	K čemu server v síti slouží?
Proč se data neposílají jako jeden kus, ale rozdělují se na pakety a co každý paket obsahuje?	Jak je možné, že pakety jedou různými cestami a nemusí dorazit ve správném pořadí?
Může paket po cestě někdo přechít?	Když se připojíte na otevřenou Wi-Fi, může někdo vidět, co na ní děláte? Kdo?
Jak funguje web Co se stane, když napíšu adresu do prohlížeče?	Jak funguje web Co se stane, když napíšu adresu do prohlížeče? • Prohlížeč pošle žádost na konkrétní server. • Server má uloženou stránku a pošle zpět části stránky (texty, obrázky...). • Prohlížeč je poskládá dohromady.
Cloud • Více serverů navzájem propojených do jednoho celku. • Nemusí být všechny na jednom místě. • Na těchto serverech jsou provázány služby a uložena naše data. • Provozovatel se stará o chod, zálohy, opravy. • Dostupný odkudkoli přes internet. 	Cloudový dokument naživo • Simulace dokumentu v cloudu • Jeden ze skupinky – vlastník dokumentu. • Ostatní editoři / komentující. • Vlastník může cokoli + přiděluje oprávnění • Editoři píšou do dokumentu – naráz. • Komentátoři lepí poznámky. • Úkol: Jaké používání mobilů ve škole je podle vás přijatelné? 

Brána do sítě

Firewall

- **Kontroluje** síťový provoz podle pravidel.
- Může být v routeru, v serveru nebo **v počítači**.
- Pracuje s **metadaty**.
- Podle předem daných pravidel rozhoduje, **co projde a co se zastaví**.



Zabezpečení webové stránky

HTTPS

- Šifruje přenos **mezi prohlížečem a serverem**.
- Nezajišťuje důvěryhodnost webu.
- Brání odposlechu.



Zabezpečené zprávy

Koncové šifrování (E2E)

- Zprávu dokáže přečíst **jen odesílatel a příjemce**.
- **Provozovatel služby obsah nevidí**.
- Implementováno vývojářem.
- Kdokoli cizí vidí pouze změť znaků.



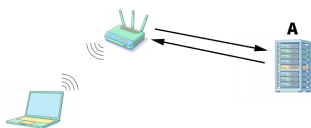
Když používám cizí Wi-Fi...

VPN

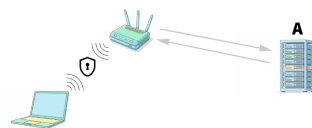
- Šifruje spojení **mezi mým zařízením a VPN serverem**.
- Komunikace jde šifrovaně na VPN server, a až potom na stránky, které používám.
- Zabraňuje, aby někdo na otevřeném Wi-Fi viděl můj provoz.

VPN ≠ úplná anonymita

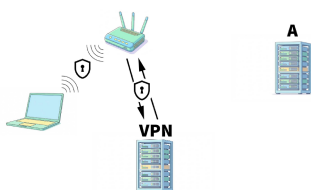
Když používám cizí Wi-Fi...



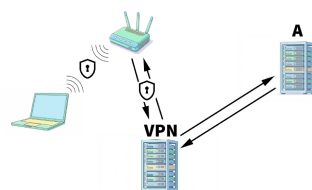
Když používám cizí Wi-Fi...



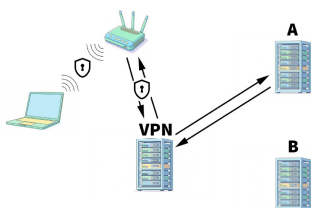
Když používám cizí Wi-Fi...



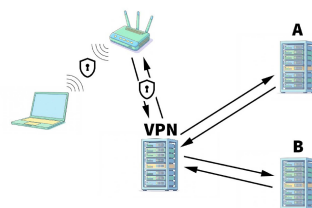
Když používám cizí Wi-Fi...



Když používám cizí Wi-Fi...



Když používám cizí Wi-Fi...



*Představte si, že jste internetový detektiv.
Snažíte se zjistit, co dělá člověk připojený k veřejné Wi-Fi.*

Co můžete vidět vždy – i když se komunikuje šifrovaně?
Co vidíte jen tehdy, pokud není použito žádné šifrování?
Co nevidíte nikdy – i kdybyste měli nejlepší vybavení?

Vyřeší VPN všechny bezpečnostní problémy?

Je anonymní režim opravdu anonymní?

Použité ilustrace a grafika

Snímek 9: Datacenter (z Google). Oficiální materiály společnosti Google.
Snímek 10: Vlastní fotografie.
Snímky 11: Ilustrace vygenerovány pomocí AI (Google Gemini, 2025-2026).
Snímky 12, 13: Vlastní tvorba.
Snímky 15, 16, 17, 18, 19, 20: Ilustrace vygenerovány pomocí AI (Google Gemini, 2025-2026) + vlastní tvorba.

A.2.4 Prezentace pro 4. hodinu

Internet věcí a chytrá domácnost

Která zařízení kolem vás právě teď **sbírají nějaké informace**,
aby je později předala dál?

Jaká zařízení kolem sebe máte,
která **mají přístup na internet**?

Chytré zařízení

- **Běžný předmět** (hodinky, žárovka), který **má vlastní procesor a senzory**.
- Dokáže **vnímat okolí** (teplotu, pohyb) a na základě toho se samo rozhodnout nebo vykonat akci.
- Je připraveno komunikovat s okolím.



Internet věcí (IoT)

- **Sít fyzických zařízení**, která jsou vybavena softwarem a senzory, aby se mohla připojit k internetu.
- Zařízení komunikují **mezi sebou** a se vzdálenými servery **automaticky**.
- Cíl: sběr dat, která se pak vyhodnocují.

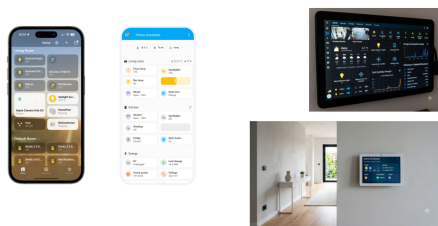
Chytrá domácnost

Jeden konkrétní příklad IoT.

Cílem je **pohodlí, automatizace a úspora**.



Chytrá domácnost



Jak chytrá zařízení komunikují

Každé chytré zařízení posílá informace.
Podle potřeby používá různé způsoby bezdrátové komunikace.

Jak chytrá zařízení komunikují

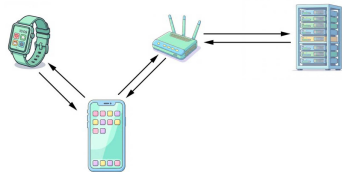
Každé chytré zařízení posílá informace.
Podle potřeby používá různé způsoby bezdrátové komunikace.

- **Wi-Fi**
 - Pro zařízení se stálým napájením, velká spotřeba, vysoká rychlost.
- **Bluetooth**
 - Propojení na krátkou vzdálenost (v rámci místnosti), velmi nízká spotřeba.
- **Sítě pro chytrou domácnost**
 - Protokoly navržené pro efektivní předávání dat mezi zařízeními v rámci domu.

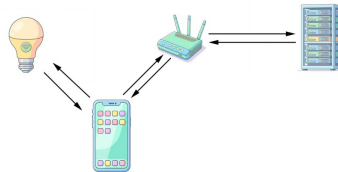
Kam zařízení posílá data?



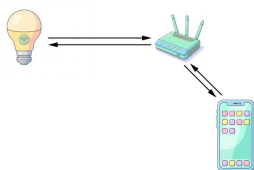
Kam zařízení posílá data?



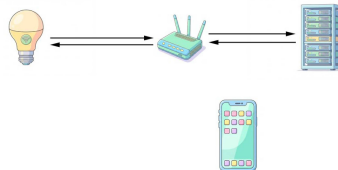
Kam zařízení posílá data?



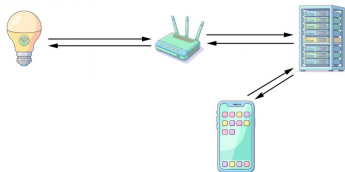
Kam zařízení posílá data?



Kam zařízení posílá data?



Kam zařízení posílá data?



Chytrá domácnost: lokální vs. cloudová

Lokální ovládání

- data zůstávají doma,
- funguje i bez připojení k internetu,
- méně „chytrých“ funkcí,
- jednodušší, bezpečnější.

Cloudové ovládání

- chytré funkce, plánování, ...
- závislost na výrobci a na internetu,
- data mimo vaši kontrolu.

Rizika a paradoxy

- Paradox chytré žárovky
- Závislost na cloudu a na mobilu.
- Konec podpory aplikace.
- Zranitelné zařízení (kamera, zvonek).

Chytré věci = pohodlí, ale platíme za něj daty a bezpečností.

Kdo dostává data a proč

Zařízení	Co odesílá	Komu	Proč
Hodinky			
Žárovka			
Robotický vysavač			
Termostát			

Kdo dostává data a proč

Zařízení	Co odesílá	Komu	Proč
Hodinky	kroky; tep; fáze spánku		
Žárovka			
Robotický vysavač			
Termostát			

Kdo dostává data a proč

Zařízení	Co odesílá	Komu	Proč
Hodinky	kroky; tep; fáze spánku	výrobci nebo aplikaci v mobilu	
Žárovka			
Robotický vysavač			
Termostát			

Kdo dostává data a proč

Zařízení	Co odesílá	Komu	Proč
Hodinky	kroky; tep; fáze spánku	výrobci nebo aplikaci v mobilu	statistiky a dlouhodobé trendy
Žárovka			
Robotický vysavač			
Termostat			

Kdo dostává data a proč

Zařízení	Co odesílá	Komu	Proč
Hodinky	kroky; tep; fáze spánku	výrobci nebo aplikaci v mobilu	statistiky a dlouhodobé trendy
Žárovka	stav; jas/barva; spotřeba	aplikaci výrobce	dálkové ovládání, sledování spotřeby
Robotický vysavač			
Termostat			

Kdo dostává data a proč

Zařízení	Co odesílá	Komu	Proč
Hodinky	kroky; tep; fáze spánku	výrobci nebo aplikaci v mobilu	statistiky a dlouhodobé trendy
Žárovka	stav; jas/barva; spotřeba	aplikaci výrobce	dálkové ovládání, sledování spotřeby
Robotický vysavač	mapa bytu; délka úklidu; stav	výrobci nebo aplikaci	přehled o úklidu, automatizace
Termostat			

Kdo dostává data a proč

Zařízení	Co odesílá	Komu	Proč
Hodinky	kroky; tep; fáze spánku	výrobci nebo aplikaci v mobilu	statistiky a dlouhodobé trendy
Žárovka	stav; jas/barva; spotřeba	aplikaci výrobce	dálkové ovládání, sledování spotřeby
Robotický vysavač	mapa bytu; délka úklidu; stav	výrobci nebo aplikaci	přehled o úklidu, automatizace
Termostat	aktuální teplota; stav topení; režim;	aplikaci výrobce	vzdálené ovládání, úspora energie

Co je pro vás **největší výhoda** a co **největší riziko** chytré domácnosti?

Chtěli byste mít doma chytrou domácnost?

Kdo má mít přístup k datům?

- Jenom my
- Rodina
- Výrobce
- Stát
- Cizí člověk

Chytrá zařízení v domácnosti

- Jaké jsou výhody chytrých zařízení? (Co usnadní?)

Chytrá zařízení v domácnosti

- Jaké jsou výhody chytrých zařízení? (Co usnadní?)
- Co o vás zařízení může prozradit? (Jaké informace sbírá?)

Chytrá zařízení v domácnosti

- Jaké jsou výhody chytrých zařízení? (Co usnadní?)
- Co o vás zařízení může prozradit? (Jaké informace sbírá?)

Chytré věci usnadňují život, ale vždy zanechávají digitální stopu.

Použité ilustrace a grafika

Obrazek 2: Obrazek ilustrace vytvořené autorem.

Obrazek 3: Obrazek vygenerovaný pomocí AI (Google Gemini, 2025, 2026).

Obrazek 4: Obrazek vygenerovaný pomocí AI (Google Gemini, 2025, 2026).

Obrazek 5: Obrazek vygenerovaný pomocí AI (Google Gemini, 2025, 2026).

A.3 Metodické listy

A.3.1 Metodické listy pro 1. hodinu

Metodický list k vyučovací hodině č. 1

Bezdrátové počítačové sítě

Cílová skupina: 1. a 2. ročník SŠ (víceletá gymnázia)

Čas: 45 minut

Klíčové pojmy: domácí síť, koncové zařízení, Wi-Fi, router, server, zabezpečení

Potřebné pomůcky: prezentace č. 1, pracovní list č. 1 (PL)

Legenda značení v textu

- **sn. X** – snímek č. X v prezentaci (např. **sn. 2–5** = snímky 2 až 5)
- **PL 👥 X.** – úkol č. X v pracovním listu pro práci ve dvojicích či skupinách
- **PL X.** – úkol č. X v pracovním listu pro samostatnou práci žáka

Výukové cíle

Po skončení této vyučovací hodiny žák:

- **definuje** vlastními slovy pojmy domácí síť a koncové zařízení,
- **popíše** funkci Wi-Fi routeru a **vysvětlí** rozdíl mezi routerem a Wi-Fi,
- **objasní** roli serveru v procesu odesílání zpráv,
- **porovná** otevřenou a zabezpečenou Wi-Fi a pojmenuje rizika.

Evokace (5–10 minut)

Cíl: Aktivovat dosavadní znalosti žáků.

- **sn. 2–5** Otevřete hodinu evokačními otázkami z prezentace.
- Pro každou otázku nechte žáky chvíli přemýšlet a následně vyvolejte krátkou diskuzi.

V této fázi žáky **neopravujte**. Zapište klíčová slova na tabuli jako odrazový můstek.

Uvědomění (25–30 minut)

Cíl: Představení nových pojmů a jejich aktivní zpracování.

1. Typy připojení a koncová zařízení

- **sn. 6–7** Zahajte diskuzi o tom, jak se zařízení připojují k síti. Vyzvěte žáky, aby porovnali kabelové a bezdrátové připojení.
- **PL 👥 1.** Žáci vypíší ve dvojicích nebo skupinkách výhody a nevýhody obou typů připojení. Následuje krátké společné shrnutí.
- **sn. 8–9** Definujte pojmy *domácí síť* a *koncová zařízení*.
- **PL 👥 2.** Žáci identifikují běžná koncová zařízení. Doplnují je ve skupinkách, nebo dvojicích, do pracovního listu.

• **Na co se doptávat:**

- „Většina z vás napsala mobil, notebook nebo televizi. Připojuje se dnes k domácí Wi-Fi ještě něco jiného?“
Očekávané odpovědi: chytré hodinky, herní konzole.
- „A co v kuchyni nebo při úklidu? Slyšeli jste o chytrých domácnostech?“
- Žáci by si měli uvědomit, že v síti komunikují i chytré žárovky, robotické vysavače nebo ledničky.

Pojem Internet věcí (IoT) zatím nezmiňujte. Dbejte, aby žáci rozlišovali mezi např. běžnou „hloupou“ televizí (bez konektivity k internetu) a chytrou televizí s konektivitou. Podobně např. u robotického vysavače nebo jiného chytrého zařízení.

2. Bezdrátový přenos a Wi-Fi

- **sn. 11** Vysvětlete principy bezdrátové komunikace (využití rádiových vln).
- **PL 3.** Během výkladu, nebo po něm, žáci průběžně doplňují princip bezdrátové komunikace.
- **sn. 12–13** Definujte a ujasněte rozdíl mezi *technologií Wi-Fi* (samotný způsob bezdrátového přenosu) a *Wi-Fi routerem* (fyzické zařízení, krabička).
- **PL 4.** Během výkladu, nebo po něm, žáci doplní, které vytváří domácí síť.

3. Interaktivní dekonstrukce cesty zprávy

- **Cíl aktivity:** Žáci pochopí nutnost existence aktivních síťových prvků (routerů) a centrálních bodů (serverů).
- **Postup na tabuli:** Začněte tím, že na okraje tabule nakreslíte dva mobilní telefony (odesílatel a příjemce).

Krok 1: Lze zařízení propojit napřímo?

sn. 14 Zeptejte se žáků: „Představte si, že chci poslat zprávu tady z mého mobilu do mobilu někoho z vás. Můžeme se spojit úplně napřímo, bez ničeho dalšího?“

Diskuze: Žáci mohou navrhnout Bluetooth nebo kabel. Přiveďte je k limitům: „A co když kamarád bydlí na druhém konci republiky? Dosáhne tam Bluetooth? Natáhneme kabel?“

Vyvození: Přímé spojení je fyzicky neudržitelné a nerealistické. Potřebujeme v síti aktivní prvek, který data převezme a pošle správným směrem → **sn. 15** představení **routeru**. Do schématu přikreslete k mobilům Wi-Fi routery a několik dalších routerů mezi ně (můžete využít **sn. 16**). Volitelně naznačte také slepé větve a „zkratky“, abyste ukázali komplexitu sítě.

Poznámka

V této fázi budování schématu záměrně vůbec **nezmiňujte** zařízení jako je **switch**. Pro pochopení základního konceptu doručování dat by to odvádělo pozornost od hlavního principu směrování.

Krok 2: Kde zpráva čeká?

Proces doručování na tabuli v polovině zastavte a předložte žákům zásadní logický problém.

Zeptejte se žáků: „Stačí nám k doručení WhatsApp zprávy jen tyhle routery? Co když má příjemce zrovna vybitý telefon, nebo vůbec není doma?“

Mylná představa: Žáci odpoví, že si zprávu pamatuje lokální router u příjemce nebo odesílatele.

Zeptejte se žáků: „Dobře, řekněme, že zpráva čeká v mém domácím routeru. Co když si ale kamarád nabije telefon a připojí se k úplně jiné Wi-Fi síti, třeba v kavárně na druhém konci města? Jak by z mého routeru tu zprávu dostal?“

Žáci si musí uvědomit, že data je nutné centrálně uložit. Zeptejte se jich, z jakého kontextu znají slovo **server** (často zmíní online hry, kde server udržuje svět pro všechny).

sn. 17 Formálně definujte server (zařízení poskytující služby a trvalý uložení dat). Doprostřed schématu na tabuli dokreslete server (**sn. 18** ; případně více pro různé služby – např. jeden pro WhatsApp, druhý pro Facebook, lze využít **sn. 19**).

- **Dokončení:** Vezměte barevnou křídu/fix a vyznačte skutečnou trasu komunikace: **odesílatel → routery → server (uložení)**.

Druhá cesta, kdy příjemce zjišťuje přítomnost nových zpráv: **příjemce → routery → server**. Pokud zpráva existuje, pak **server → routery → příjemce**.

4. Bezpečnost v síti

- **sn. 20–21** Vysvětlíte rozdíly mezi otevřenou (např. veřejná Wi-Fi v kavárně bez hesla) a zabezpečenou sítí (domácí Wi-Fi chráněná heslem).
- **Na co se doptávat:**
 - „Proč může být nebezpečné připojit se k volné Wi-Fi v nákupním centru a přihlásit se tam do banky nebo na sociální síť?“
- Zdůrazněte rizika: možnost odposlechu komunikace, podvržení falešných webových stránek, napadení samotného zařízení.
- **PL 5.** Žáci na závěr určí, čím je otevřená Wi-Fi síť riziková, čímž si rizika prakticky zafixují.

Reflexe (5–10 minut)

Cíl: Upevnit nové poznatky, propojit je a ověřit, zda žáci dosáhli výukových cílů.

- **sn. 22–26** Shrnutí pomocí otázek z prezentace.

Na **sn. 25** upozorněte na dialogové okno systému Windows při připojování se k otevřené Wi-Fi a hlášku „Informace, které posíláte přes tuto síť, možná uvidí i jiní lidé.“ Zároveň s žáky vedte krátký dialog o automatickém připojování k Wi-Fi – kdy ano (důvěrné, zabezpečené síť) a kdy ne (veřejné, nezabezpečené síť – otevřenou Wi-Fi může útočník vytvořit kdekoli, jejich mobil se pak sám připojí a začne komunikovat; u zabezpečené síť musí útočník nastavit stejné heslo).

Jak spolu souvisejí

sn. 27 Dvojicím nebo skupinám zadejte dvojice (např. *router – internet*).

Úkol: Během 2 minut vymyslet jednu větu, která oba pojmy logicky a fakticky správně propojuje.

A.3.2 Metodické listy pro 2. hodinu

Metodický list k vyučovací hodině č. 2

Přenos dat v sítích

Cílová skupina: 1. a 2. ročník SŠ (víceletá gymnázia)

Čas: 45 minut

Klíčové pojmy: IP adresa, paket, směrování, síťový protokol

Potřebné pomůcky: prezentace č. 2, pracovní list č. 2 (PL), 1 × aktivita s pakety

Legenda značení v textu

- **sn. X** – snímek č. X v prezentaci (např. **sn. 2–5** = snímky 2 až 5)
- **PL  X.** – úkol č. X v pracovním listu pro práci ve dvojicích či skupinách
- **PL X.** – úkol č. X v pracovním listu pro samostatnou práci žáka

Výukové cíle

Po skončení této vyučovací hodiny žák:

- **definuje** účel IP adresy a zdůvodní, proč ji v síti potřebujeme,
- **vysvětlí** na základě analogie důvody, proč se data před přenosem dělí na menší části (pakety),
- **identifikuje** v rámci fyzické simulace problémy, které mohou při přenosu dat nastat (např. zahlcení uzlu, ztráta paketu, příchod paketů ve špatném pořadí),
- **vysvětlí** vlastními slovy pojem síťový protokol jako nezbytnou sadu pravidel pro komunikaci.

Evokace (5–10 minut)

Cíl: *Navázat na předchozí hodinu a vytvořit kognitivní konflikt – jak router pozná, kam data poslat?*

- **sn. 2–5** Otevřete hodinu evokačními otázkami z prezentace.
- Pro každou otázku nechte žáky chvíli přemýšlet a následně vyvolejte krátkou diskuzi.

sn. 4 Zde může být žákům nápovědou screenshot YouTube přehrávače a linky indikující, jaká část videa je načtena ale ještě nepřehrána (světle šedý pruh).

V této fázi žáky **neopravujte**. Zapište klíčová slova na tabuli jako odrazový můstek.

Uvědomění (25–30 minut)

Cíl: *Pochopení adresování, fragmentace dat a prožití fyzické simulace směrování.*

1. Paketový přenos

- **sn. 6 Zeptejte se žáků:** „Když data dorazí do routeru, podle čeho se rozhoduje, kterým směrem pokračují?“
Na základě jejich úvah a návrhů plynule přejděte k definici IP adresy – **sn. 7** (zmiňte pouze IPv4 pro jednoduchost).

Žáci v tuto chvíli již vědí, podle čeho síť pozná, kam má data doručit. Nyní je potřeba vyřešit problém, jak se tam data fyzicky dostanou, když je odesílaný soubor příliš velký na to, aby prošel sítí naráz. K tomu slouží následující příběh.

Převoz dinosaura (6 minut)

sn. 8 Uvedte žáky do role: „Představte si, že jste ředitelé muzea...“.

PL  **1.** Nechte žáky ve skupinkách (2–4 žáci) pracovat na úloze **a)** a **b)**. Následně se žáky diskutujte jimi navrhovaná řešení.

Očekávané řešení: Žáci by měli přijít na to, že je nutné vytvořit věrnou fyzickou kopii (např. 3D tiskem) a tu převézt.

Jak reagovat na alternativní nápady:

- *Návrh VR (virtuální realita):* Odmítněte s tím, že muzeum trvá na hmatatelném fyzickém zážitku v reálném měřítku.
- *Návrh pustit lidi přímo do depozitáře:* Zamítněte z bezpečnostních důvodů (nutnost udržovat přísné klimatické podmínky pro ochranu křehkého originálu).

Jakmile máte od žáků očekávané řešení, přejděte na **sn. 9**.

Než přejdete k dalšímu obrázku, uvedte problém – celá kopie dinosaura se nevejde do kamionu a neprojde dveřmi muzea.

sn. 10 Žáci logicky navrhnou, že se model musí rozebrat na menší části (kosti) a dát do krabic.

Nyní položte návodnou otázku: „*Skvělé, rozložili jsme ho do krabic. Ale podívejte se na ten zmatek. Co se stane, až tuhle hromadu kostí dovezeme na místo? Jak poznají, co kam patří?*“ Tím si perfektně připravíte půdu pro další nezbytný krok – nutnost krabice očíslovat a opatřit instrukcemi. Než začnete cokoli společně řešit, vyzvěte žáky, ať ve skupinkách vypracují **podúlohu c)** v PL.

sn. 11 Očekávané řešení: Během následného sdílení odpovědí by žáci měli přijít s nápadem, že krabice se musí nejen očíslovat, ale ideálně i označit celkovým počtem (např. „krabice 5 ze 120“), a že se k nim musí přiložit plánek či návod.

Zde je cílem, aby si žáci sami odvodili naprostou logickou nutnost pořadových čísel a informace o celkovém množství. Zdůrazněte jim, že bez tohoto řešení by v muzeu buď vznikl zmutovaný dinosaur, nebo by při přebírání vůbec nepoznali, že jim cestou jedna krabice vypadla.

Zeptejte se třídy: „*Máme desítky očíslovaných krabic. Naložíme je všechny do jednoho obrovského kamionu, nebo je pošleme více menšími auty? A musí jet všechna auta stejnou trasou?*“

sn. 12–13 Očekávané řešení: Žáci zpravidla odvodí, že použití více aut je flexibilnější. Stejně tak by měli navrhnout, že auta mohou jet různými cestami (např. aby se vyhnula zácpě na dálnici nebo nehodě).

Nechte žáky, ať si sami obhájí, že rozdělení nákladu do více nezávislých vozidel, která mohou měnit trasu podle aktuální situace, je to nejchytřejší a nejrychlejší řešení.

sn. 14 Dramatizujte situaci: „*Ale ne! Auta dojela, muzeum kostru složilo podle návodu, ale dinosaurovi chybí ocas! Jedno auto mělo po cestě nehodu (nebo uvízlo v zácpě). Co teď?*“

sn. 15 Očekávané řešení: Žáci logicky navrhnou, že muzeum zavolá zpět do depozitáře, nahlásí chybějící čísla krabic a nechá si poslat **pouze ten chybějící ocas** (nikoliv celého dinosaura znovu).

Zde aktivita vrcholí. Upozorněte žáky na to, jak geniální řešení právě vymysleli – když se cestou ztratí jedna krabice, nemusíme převážet celou kostru znovu od začátku, ale vyžádáme si jen ten jeden malý chybějící kousek. Zároveň depozitář má stále z čeho vyrobit další repliky, nepřišlo se o originál.

- **sn. 16** Definujte nový pojem – **paket** a jaké má základní části.
- Nechte žáky vypracovat ve skupinkách úlohu **PL** **2.** a **PL** **3.**
- Krátce přeložte nápady žáků z reálného světa do síťové terminologie:
 - **Kostra dinosaura** Představuje jakýkoliv soubor (fotku, video, webovou stránku), který chceme poslat.
 - **Věrná kopie v depozitáři:** Síť neposílají originály (ty zůstávají u odesílatele/na serveru), ale tvoří a odesílají jejich kopie.
 - **Rozebrání na kosti:** Soubor nelze poslat v kuse. Odesílaná data se dělí na menší kousky – **pakety**.
 - **Očíslování krabic:** Kosti bez návodu by byly k ničemu. Každý paket má proto i druhou část – **doplňující informace (metadata)**. To je „popisek na krabici“: kdo to posílá, komu a v jakém pořadí se to má složit.
 - **Auta na různých trasách:** Pakety neputují jednou fixní trasou. Síť (routery) jim dynamicky hledá cestu.
 - **Chybějící ocas:** Pokud paket cestou „odpadne“ (např. ho zahlcený router zahodí), cílové zařízení si vyžádá jeho opětovné zaslání.

S žáky můžete rozvést krátkou diskusi na téma, jestli se může nějaký paket ztratit a co by k tomu mohlo vést.

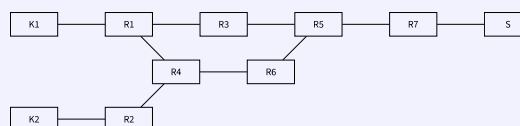
2. Směrování dat

Fyzická simulace sítě (klíčová aktivita – 15 min)

Příprava a pravidla:

- **Role a rozestavení:** Do prostoru třídy je rozmístěno 10 dobrovolníků podle schématu topologie.
 - **Koncová zařízení:** **K1**, **K2** (klienti) a **S** (server).
 - **Směrovače:** Sedm žáků v rolích **R1** až **R7**.
- **Vybavení uzlů:** Každý směrovač obdrží svou specifickou **směrovací tabulku** (viz příloha), která definuje jeho rozhodovací logiku.
- **Role pozorovatelů:** Ostatní studenti sledují tok dat a zaznamenávají anomálie (např. čekací doby nebo kumulaci paketů).

Schéma



Průběh aktivity

- Zahajte aktivitu tím, že lísteček (paket) **#1** dáte žákovi **K2**, necháte ho přecházet komu paket posílá. Následně se ho zeptejte „Komu paket budeš předávat? Můžeš ho předat přímo příjemci?“ – Nemůže, předá jej **R2**.
- Žáka **R2** zastavte v moment, kdy obdrží paket. Zeptejte se ho, s kým může komunikovat přímo (pouze **K2** a **R4**) a komu paket předá – podle směrovací tabulky **R4**, protože paket míří do **S**.

Minimálně v začátku udávejte „takt“, jakým si mají pakety předávat, aby nevznikl chaos.

- Jakmile paket **#1** dorazí k **R5**, předejte **K1** paket **#2**.

Toto vyčkání je důležité, aby **S** v úvodu mylně neinterpretoval první část zprávy jako hotovou odpověď.

- Mezitím dorazí paket **#1** k žákovi **S**. Jelikož je žák **S** příjemce, měl by si sám přecházet zprávu. Pokud to neudělá, vyzvěte jej. Také se ho zeptejte, jestli pro **K2** má jak odpovědět – nemá, předáte mu paket **#3**.
- Žákovi **K1** předejte postupně pakety **#4**, **#5** a **#6**.
- Žákovi **K1** předejte všechny pakety s označením **#X**. Dejte mu pokyn, aby je postupně posílal do sítě (např. každé dvě vteřiny).
- Jakmile paket **#6** má žák **R3**, můžete žákovi **K2** předat paket **#7**.
- Jakmile paket **#6** má žák **S**, můžete předat žákovi **S** paket **#8**.
- Server **S** nyní na (opakovanou) žádost **K2** (paket **#7**) může odpovědět, postupně mu předejte pakety **#9** a **#10**.
- Po obdržení **#10** žákem **K2** mu předejte k odeslání **#11**.

Debriefing simulace: Ptejte se pozorovatelů i aktérů:

- **Pro žáka K2:** „Když jsi dostal paket 1, mohl jsi ho předat příjemci S přímo? Pokud ne, přes koho musela tvoje zpráva jít?“
- **Pro žáka R2:** „Podle čeho jsi věděl, že máš paket od K2 předat právě uzlu R4, a ne někomu jinému?“
- **Pro žáka S:** „Když ti dorazil paket 1 (ten první), věděl jsi hned, jak na něj odpovědět? Co jsi k tomu potřeboval?“
- **Pro žáka K1:** „Co se začalo v síti dít v momentě, kdy jsi začal posílat pakety X?“
- **Pro aktéry i pozorovatele:** „Na základě této zkušenosti – co se pravděpodobně děje v reálném internetu, když se data (např. video) načítají pomalu nebo se přenos zastaví?“

Zreflektujte, že přesně takto se chová reálný internet (data nechodí popořadě, cesty se ucpávají). Nechte žáky vyplnit **PL 4**.

sn. 21–24 Po simulaci se zeptejte žáků, jakými pravidly se museli při předávání lístečků řídit (např. znát cíl, posílat postupně). Vysvětlete, že v reálném světě se těmito dohodnutým pravidlům říká **síťový protokol**. Upozorněte na přímou spojitost s tím, co už znají: Zkratka IP znamená „Internet Protocol“ – tedy

přesně ten základní soubor pravidel pro adresování a doručování paketů, který si právě fyzicky vyzkoušeli. Žáci vyplní **PL 5.** a **PL  6.** .

Reflexe (odhad: 5–10 minut)

Cíl: *Ověření pochopení hlavních pojmů.*

- **sn. 25–31** Spustte připravený kvíz, který zopakuje základní definice z této hodiny.

Materiály k aktivitě pro 2. hodinu

Poznámka: Níže uvedené výukové materiály a karty slouží k realizaci simulace síťového provozu (směrování paketů) v rámci 2. vyučovací hodiny.

Směrovací tabulky Karty pro žáky v roli síťových routerů.

Směrovací tabulka pro R1 <table><tr><th>Cíl</th><th>Akce</th></tr><tr><td>S</td><td>R3 (při frontě R4)</td></tr><tr><td>K1</td><td>K1</td></tr><tr><td>Jinak</td><td>R4</td></tr></table>	Cíl	Akce	S	R3 (při frontě R4)	K1	K1	Jinak	R4	Směrovací tabulka pro R2 <table><tr><th>Cíl</th><th>Akce</th></tr><tr><td>S</td><td>R4</td></tr><tr><td>K2</td><td>K2</td></tr></table>	Cíl	Akce	S	R4	K2	K2
Cíl	Akce														
S	R3 (při frontě R4)														
K1	K1														
Jinak	R4														
Cíl	Akce														
S	R4														
K2	K2														
Směrovací tabulka pro R3 <table><tr><th>Cíl</th><th>Akce</th></tr><tr><td>S</td><td>R5</td></tr><tr><td>Jinak</td><td>R1</td></tr></table>	Cíl	Akce	S	R5	Jinak	R1	Směrovací tabulka pro R4 <table><tr><th>Cíl</th><th>Akce</th></tr><tr><td>K1</td><td>R1</td></tr><tr><td>K2</td><td>R2</td></tr><tr><td>Jinak</td><td>R6 (při frontě R2)</td></tr></table>	Cíl	Akce	K1	R1	K2	R2	Jinak	R6 (při frontě R2)
Cíl	Akce														
S	R5														
Jinak	R1														
Cíl	Akce														
K1	R1														
K2	R2														
Jinak	R6 (při frontě R2)														
Směrovací tabulka pro R5 <table><tr><th>Cíl</th><th>Akce</th></tr><tr><td>S</td><td>R7</td></tr><tr><td>Jinak</td><td>R3 (při frontě R6)</td></tr></table> Router je velmi pomalý. Než předáš zprávu, napočítej do 5.	Cíl	Akce	S	R7	Jinak	R3 (při frontě R6)	Směrovací tabulka pro R6 <table><tr><th>Podmínka</th><th>Akce</th></tr><tr><td>S</td><td>R5</td></tr><tr><td>K1 nebo K2</td><td>R4</td></tr><tr><td>Jinak</td><td>R5</td></tr></table>	Podmínka	Akce	S	R5	K1 nebo K2	R4	Jinak	R5
Cíl	Akce														
S	R7														
Jinak	R3 (při frontě R6)														
Podmínka	Akce														
S	R5														
K1 nebo K2	R4														
Jinak	R5														
Směrovací tabulka pro R7 <table><tr><th>Podmínka</th><th>Akce</th></tr><tr><td>S</td><td>S</td></tr><tr><td>K1 nebo K2</td><td>R5</td></tr></table>	Podmínka	Akce	S	S	K1 nebo K2	R5									
Podmínka	Akce														
S	S														
K1 nebo K2	R5														

Pakety Fyzické reprezentace posílaných dat (zpráv), které kolují v síti mezi žáky a jsou přenášeny podle pokynů ve směrovacích tabulkách.

#1 $K2 \rightarrow S$ ČÁST: 1/1 Obsah: Mám něco ke stažení?	#2 $K1 \rightarrow S$ ČÁST: 1/4 Obsah: Mám pro K2 důležitou zprávu. Ulož...
#3 $S \rightarrow K2$ ČÁST: 1/1 Obsah: Nemáš žádné nové zprávy.	#4 $K1 \rightarrow S$ ČÁST: 3/4 Obsah: Týká se našeho společného...
#5 $K1 \rightarrow S$ ČÁST: 2/4 Obsah: ...ji, aby si ji mohl stáhnout...	#6 $K1 \rightarrow S$ ČÁST: 4/4 Obsah: projektu Omega. Schůzka bude v pět.
#7 $K2 \rightarrow S$ ČÁST: 1/1 Obsah: Mám něco ke stažení?	#8 $S \rightarrow K1$ ČÁST: 1/1 Obsah: Uloženo!

#9 $S \rightarrow K2$ ČÁST: 1/2 Obsah: Máš tu zprávu od K1 k projektu Omega.	#10 $S \rightarrow K2$ ČÁST: 2/2 Obsah: Zpráva: Schůzka bude v pět.
#11 $K2 \rightarrow S$ ČÁST: 1/1 Obsah: Vše doručeno. Děkuji.	#X $K1 \rightarrow K3$ ČÁST: 1/1 Obsah: Aktualizace systému 1.0.4.
#X $K1 \rightarrow K3$ ČÁST: 1/1 Obsah: Hledám uzel K3.	#X $K1 \rightarrow K3$ ČÁST: 1/1 Obsah: Ping
#X $K1 \rightarrow K3$ ČÁST: 1/1 Obsah: Odesílání diagnostických dat 84 %	#X $K1 \rightarrow K3$ ČÁST: 1/1 Obsah: Kontrola dostupnosti tiskárny v síti.

#X K1 → K3 ČÁST: 1/1 Obsah: RE: Nabídka výhodného pojištění.	#X K1 → K3 ČÁST: 1/1 Obsah: Požadavek na synchronizaci času.
#X K1 → K3 ČÁST: 1/1 Obsah: Hledám nejbližší volný server.	

Checklist pro pozorovatele Seznam cílených otázek a úkolů pro žáky, kteří se přímo neúčastní aktivní simulace. Slouží k zaznamenávání chování sítě, sledování chyb v přenosu a udržení pozornosti celé třídy.

Pozorovatel klientů

Sleduj

- že klient dostává pakety postupně a nemá přehled o celé zprávě,
- jak reaguje na každý jednotlivý paket.

Otázky

- Jak klient poznal, že už dostal všechna data, i když neviděl jejich cestu?
- Co by se stalo, kdyby potvrzení o uložení nepřišlo, i když data k **S** dorazila?

Pozorovatel serveru

Sleduj

- na základě čeho server reaguje,
- jestli řeší cestu a pořadí paketů.

Otázky

- Co všechno server **nemusel vědět**, aby mohl správně odpovědět?
- Reagoval by server jinak, kdyby data přišla jinou cestou?

Pozorovatel routeru

Sleduj jeden z routerů R1, R4 nebo R5

- podle čeho router rozhodoval, kam paket pošle,
- jestli kouká obsah zprávy.

Otázky

- Na základě jaké informace se router rozhodoval?
- Věděl router, jestli paket skutečně dorazí do cíle?

Pozorovatel cesty paketů

Sleduj

- jestli pakety chodí stejnou nebo různou cestou,
- kde se nejvíc zdržují.

Otázky

- Proč nemusely všechny pakety jít stejnou cestou?
- Co síť získá tím, že existuje víc možných cest?

Pozorovatel chování sítě

Sleduj

- situace, kdy pakety nepřijdou hezky po sobě nebo hned,
- co se s takovou situací stane dál.

Otázky

- Co se v síti stalo, když pakety dorazily pozdě, víckrát, nebo v jiném pořadí?
- Jak síť poznala, že má počkat, zopakovat přenos, nebo pokračovat?

Pozorovatel provozu v síti

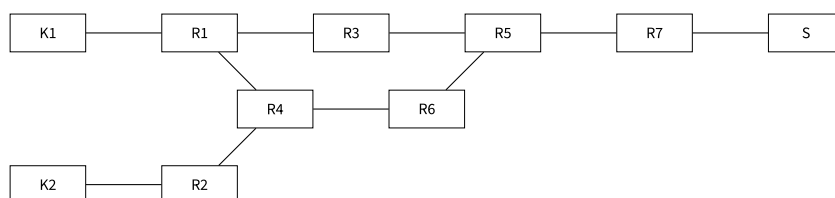
Sleduj

- kde se pakety hromadí,
- které části sítě jsou málo využité.

Otázky

- Kde byla síť nejvíc zatížená a proč právě tam?
- Znamená málo využitý router, že je zbytečný?

Mapa sítě Schéma rozestavení jednotlivých žáků (uzlů) v učebně, které definuje topologii simulované sítě a představuje oporu pro úvodní instruktáž.



A.3.3 Metodické listy pro 3. hodinu

Metodický list k vyučovací hodině č. 3

Bezpečnost v sítích a ochrana dat

Cílová skupina: 1. a 2. ročník SŠ (víceletá gymnázia)

Čas: 45 minut

Klíčové pojmy: cloud, přístupová práva, firewall, HTTPS, koncové šifrování, VPN

Potřebné pomůcky: prezentace č. 3, pracovní list č. 3 (PL), čisté papíry a lepidlo (post-it)

Legenda značení v textu

- **sn. X** – snímek č. X v prezentaci (např. **sn. 2–5** = snímky 2 až 5)
- **PL  X.** – úkol č. X v pracovním listu pro práci ve dvojicích či skupinách
- **PL X.** – úkol č. X v pracovním listu pro samostatnou práci žáka

Výukové cíle

Po skončení této vyučovací hodiny žák:

- **vysvětlí** na základě simulace princip sdíleného cloudového dokumentu a zhodnotí riziko přístupu správce (poskytovatele) k uživatelským datům,
- **aplikuje** princip fungování firewallu na konkrétní příklady síťového provozu a rozhodne, zda komunikaci propustí nebo zastaví,
- **porovná** úroveň soukromí při použití nešifrovaného spojení, HTTPS a E2E šifrování (identifikuje, co vidí útočník),
- **zvolí** a obhájí adekvátní bezpečnostní nástroj (VPN, E2E, HTTPS) pro zadané každodenní situace.

Evokace (5–10 minut)

Cíl: Zopakovat klíčové pojmy z minulých hodin a otevřít téma odposlechu dat.

- **sn. 2–6** Otevřete hodinu evokačními otázkami z prezentace.

Odpovědi na poslední dvě otázky vytvoří přirozený přechod k dnešnímu tématu bezpečnosti.

Uvědomění (25–30 minut)

Cíl: Prožít principu cloudu a seznámení se základními nástroji ochrany dat.

1. Jak funguje web

- **sn. 7–8** Krátce vysvětlíte princip komunikace prohlížeč-server. Žáci následně samostatně vyplní **PL 1.**
- **sn. 9** Představte žákům pojem cloud.

Cloudový dokument naživo (5 minut)

- **sn. 10** Rozdělte žáky do skupinek. Každé skupině dejte jeden čistý papír a post-it lístečky – papír představuje jejich sdílený cloudový dokument. Určete jednoho žáka ve skupině jako **vlastníka**. Vlastník rozdělí role
 - **editor** – do dokumentu píše vlastní tužkou,
 - **komentující** – do dokumentu psát nesmí, může pouze lepit lístečky s vlastním komentářem.
- Zadejte téma, které podnítl diskusi mezi žáky (např. „Jaká pravidla pro mobily by měla platit ve škole?“). Všichni editoři i vlastník mohou do papíru psát současně – simulují tak společnou práci v reálném čase z různých zařízení. Komentující do dokumentu nahlíží a lepí lístečky se svým komentářem k výročkům spolužáků.
- V průběhu práce nenápadně pobídněte některé editory, aby začali tvorbu dokumentu úmyslně „sabotovat“ (např. psát nesmysly).

Cílem je vyvolat situaci, kdy musí vlastník dokumentu zasáhnout a reálně snížit jejich oprávnění (např. jim sebrat propisku a povolit jen čtení/komentování).

- Zatímco skupiny pracují, procházejte třídou. Zcela bez komentáře občas do některého dokumentu něco připište nebo do něj nalepte barevný „post-it“ lísteček.

Své zásahy nijak nevysvětľujte, tvoříte tím klíčovou nahrávku pro následnou reflexi.

Reflexe aktivity:

- Ptejte se žáků na otázky
 - „Kdo všechno viděl do vašeho dokumentu?“
Očekávaná odpověď: My ve skupině.
 - „A mohli by nahlížet spolužáci z jiné skupiny?“
Očekávaná odpověď: Ne, nemají oprávnění
 - „A jak je možné, že já jsem do něj mohl psát a číst ho, i když jste mi nedali oprávnění?“
- Dovedte žáky k uvědomění, že učitel v této hře představoval poskytovatele cloudu (Google/Microsoft), který má k datům na svých serverech fyzický přístup vždy, pokud nejsou šifrována na straně klienta.

2. Ochranné mechanismy

- **sn. 11** Plynujte navažte na řízení přístupu. Vysvětlete funkci firewallu.
- **sn. 12** Na základě jedné z otázek v úvodu vysvětlete potřebu šifrování komunikace mezi serverem a prohlížečem (HTTPS). **Zmiňte, že HTTPS je protokol.**
- Žáci vypracují **PL**  **2.** .

U každé otázky požadujte od žáků odůvodnění jejich závěru.

Navrhované řešení:

a) Nová aplikace odesílá velké množství dat na cizí službu.

- Rozhodnutí: Zastavit (nebo se alespoň dotázat uživatele).
- Odůvodnění: Je to podezřelé chování. Může jít o spyware nebo virus, který se snaží ukrást vaše soukromá data (hesla, fotky) a odeslat je útočníkovi.

b) Někdo se pokouší vzdáleně přistoupit k vašemu počítači.

- Rozhodnutí: Zastavit.
- Odůvodnění: Neautorizovaný přístup zvenčí je největší bezpečnostní riziko. Firewall by měl standardně blokovat všechny nevyžádané příchozí pokusy o spojení, aby se hacker nedostal do systému.

c) Operační systém chce stáhnout oficiální aktualizaci.

- Rozhodnutí: Pustit.
- Odůvodnění: Jde o důvěryhodný zdroj. Aktualizace jsou nezbytné pro opravu chyb a zabezpečení systému. Firewall má tyto známé procesy výrobce na seznamu povolených výjimek.

d) Uživatel otevírá webovou stránku přes HTTPS, ale obsah je škodlivý.

- Rozhodnutí: Pustit (Tady pozor!).
- Odůvodnění: Firewall kontroluje „dopravu“ (odkud a kam data jdou), ale nevidí dovnitř zašifrovaného obsahu stránky. Firewall pozná, že jdete na web, a povolí to. Samotný škodlivý kód (virus na stránce) musí zachytit až antivirus nebo prohlížeč.

- Zeptejte se žáků, jestli si myslí, že HTTPS postačuje na bezpečné zasílání zpráv po internetu – nepostačuje, do zprávy může vidět provozovatel serveru.
- **sn. 13** Zavedte pojem „koncové šifrování“, k popsání využijte obrázek v prezentaci. Upozorněte žáky, že pokud vývojář neimplementoval koncové šifrování, oni jako uživatelé nemají možnost si je zapnout; stejně jako HTTPS. Zároveň žáky upozorněte, že koncové šifrování **není protokol**, ale pouze způsob zabezpečení komunikace. Můžete se odkázat na populární komunikátory (např. WhatsApp, Viber), které koncové šifrování mají.
- Žáci zpracují **PL**  **3.**
- **sn. 14** Při popisování VPN se vyhněte abstraktnímu IT pojmu „zabezpečený tunel“. Vysvětlíte VPN raději jako **prostředníka**. Zmiňte, že VPN také není protokol, jde o službu/koncept zabezpečení dat. *K navázání a udržení tohoto spojení však VPN používá konkrétní síťové protokoly.* Demonstrujte jak taková komunikace probíhá (**sn. 15–20**).

Jak žákům představit princip VPN

- Když jste na veřejné Wi-Fi (např. v kavárně), VPN vezme vaše data, zašifruje je a pošle je na svůj vlastní bezpečný server. Až z tohoto serveru je pošle dál na web, který chcete navštívit. Případný útočník na kavárenské síti vidí jen to, že od vás odchází data, ale nevidí, co je uvnitř ani kam to ve finále jede. Vidí pouze že „nějaká“ data odchází na VPN server.
- Zásadní moment hodiny: důrazně žáky vyvedte z omylu, že VPN znamená absolutní anonymitu. Hacker v kavárně vaše data sice nevidí, ale samotný provozovatel VPN serveru ano. Nejsou na internetu neviditelní.

Můžete také zmínit vedlejší efekt použití VPN – změna zdánlivé polohy uživatele podle IP adresy VPN serveru.

Reflexe (odhad: 10 minut)

Cíl: Upevnění znalostí prostřednictvím rolové hry na „internetového detektiva“ a vyvrácení běžných mýtů o anonymitě.

sn. 21 Zadejte třídě roli: „Představte si, že jste internetový detektiv. Snažíte se zjistit, co dělá člověk připojený k veřejné Wi-Fi.“ Pokládejte otázky a vedte diskuzi:

- *Co můžete vidět vždy – i když se komunikuje šifrovaně?* (Např. metadata, velikost paketů, s kým probíhá spojení).
- *Co vidíte jen tehdy, pokud není použito žádné šifrování?* (Přesný obsah zpráv, hesla, prohlížené obrázky).
- *Co neuvídíte nikdy – i kdybyste měli nejlepší vybavení?* (Obsah zpráv chráněných E2E šifrováním).

Vyvrácení miskoncepce: Na závěr hodiny položte dvě kritické otázky:

- „Vyřeší VPN všechny bezpečnostní problémy?“ (Ne, chrání jen přenos po server VPN, nezabrání např. phishingu nebo stažení viru).
- „Je anonymní režim v prohlížeči opravdu anonymní?“ (Ne, pouze neukládá historii do vašeho počítače. Poskytovatel internetu i navštívený web vás stále vidí).

Zakončete hodinu otázkami z **sn. 22**.

A.3.4 Metodické listy pro 4. hodinu

Metodický list k vyučovací hodině č. 4

Internet věcí a chytrá domácnost

Cílová skupina: 1. a 2. ročník SŠ (víceletá gymnázia)

Čas: 45 minut

Klíčové pojmy: chytré zařízení, Internet věcí (IoT), chytrá domácnost, cloudové a lokální ovládání, sběr osobních dat

Potřebné pomůcky: prezentace č. 4, pracovní list č. 4

Legenda značení v textu

- **sn. X** – snímek č. X v prezentaci (např. **sn. 2–5** = snímky 2 až 5)
- **PL  X.** – úkol č. X v pracovním listu pro práci ve dvojicích či skupinách
- **PL X.** – úkol č. X v pracovním listu pro samostatnou práci žáka

Výukové cíle

Po skončení této vyučovací hodiny žák:

- **rozlíší** běžná koncová zařízení od „chytrých“ zařízení na základě jejich schopnosti pracovat a reagovat automaticky.
- **porovná** možnosti ovládání chytrých zařízení (přímo z mobilu lokálně vs. přes cloud výrobce) a zhodnotí jejich výhody a rizika.
- **vysvětlí** tzv. paradox chytré žárovky (závislost na nepřerušném fyzickém napájení).
- **identifikuje** a kriticky **zhodnotí**, jaká osobní data vybraná chytrá zařízení sbírají a komu je odesílají.

Evokace (5–10 minut)

Cíl: *Uvědomění si všudypřítomnosti chytrých zařízení a definování jejich základních znaků.*

- **sn. 1–2** Otevřete hodinu evokačními otázkami z prezentace.

Zapište všechny úvodní nápady žáků na tabuli, aniž byste je hned opravovali. Tento seznam pak využijte jako živý příklad pro zbytek hodiny, na kterém si žáci sami odvodí, zda a komu jimi zmíněná zařízení data skutečně posílají.

Uvědomění (odhad: 25–30 minut)

Cíl: *Pochopení principů komunikace v IoT, závislosti na cloudu a analýza toků dat.*

- **sn. 3** Definujte pojem „chytré zařízení“.
- **PL  1.** Žáci roztřídí seznam zařízení podle toho, zda je člověk používá aktivně (např. notebook, mobil), nebo zda pracují a reagují sama (chytrá žárovka, senzor, robotický vysavač).

Mobil, notebook – vyžadují aktivní povel člověka. Bez něj samostatně neplní svůj hlavní účel. dveřní senzor, teploměr v chytré meteostanici, robotický vysavač – přesně splňují definici (samy posílají data a přijímají pokyny). Pracují samostatně na pozadí. Chytrá žárovka, chytrá zásuvka, smartwatch (chytré hodinky) – u těchto zařízení uznejte žákům obě odpovědi, pokud je dokážou logicky obhájit. Právě na nich lze nejlépe demonstrovat podstatu chytré domácnosti.

- **PL 2.** Žáci vyplní samostatně. Zcela postačující je definice z prezentace.
- **sn. 4** Definujte pojem „internet věcí“ a uveďte příklad – **sn. 5–6** chytrá domácnost.
- **sn. 7–8** Krátce diskutujte se žáky, jaké bezdrátové možnosti propojení znají (Wi-Fi, Bluetooth). Na základě jejich zkušeností dejte dohromady vlastnosti technologií (rychlost vs. spotřeba). Na závěr zmiňte síť pro chytrou domácnost (např. Zigbee). Jde o specifické síť navržené pro efektivní dosah v budovách – zařízení si data předávají navzájem (tzv. mesh topologie), takže zpráva „doskáče“ i do vzdálených koutů domu.

Diskuze: kam putují data z chytrých zařízení? **sn. 9–15** Zahajte s žáky postupné budování komunikační cesty. Záměrně vynechte složité technické protokoly a soustředte se čistě na logiku toho, kudy data putují (lokální síť vs. internet).

- **sn. 9–10** Ukažte komunikaci chytrých hodinek s telefonem a zeptejte se: „*Zůstávají data jen v telefonu, nebo jdou někam dál?*“ Žáci většinou tvrdí, že nikam dál nejdou.
Jak reagovat: Zeptejte se jich, jak je tedy možné, že v aplikaci vidí srovnání aktivity se svými přáteli, nebo mají zálohovanou historii kroků při koupi nového telefonu. Dovedte je k uvědomění, že data musí odcházet na **server** (do cloudu).
- **sn. 11** Přeneste tuto logiku na chytrou domácnost. Zeptejte se: „*Komunikuje nám žárovka stejně jak hodinky?*“ Nejčastěji nekomunikuje. Stejně tak by bylo nekomfortní neustále se připojovat k žárovce při potřebě změnit její barvu.
- **sn. 12** Častěji se uplatňuje varianta, kdy žárovky jsou připojeny k centrálnímu vysílači – Wi-Fi router, přes který jsou ovládány z telefonu.
- Zeptejte se: „*Potřebujeme u žárovky, aby svá data o svícení posílala někam na server?*“
Očekávaná reakce: Žáci budou namítat, že je to zbytečné.
Jak reagovat: Naveďte je na myšlenky dlouhodobých statistik, měření spotřeby elektřiny nebo nutnosti ovládat světlo z jiného zařízení (např. z notebooku, který s žárovkou není přímo spárovaný).
- **sn. 13** Naveďte žáky k myšlenkám na způsoby, jak se data ze žárovky dostanou na server. Nejsnazší cesta je, že tam žárovka data pošle sama.
- **sn. 14** Když žárovka umí na server data zapisovat, co brání tomu, aby jí server dával pokyny. Položte třídně zásadní otázku: „*Co získáme tím, když nebudeme dávat pokyny domácímu routeru, ale pošleme pokyn na server někde v internetu, který pak sám nařídí naší žárovce, aby se rozsvítila?*“ Žáci musí přijít na to, že toto je ten moment, který nám umožňuje **ovládat domácnost na dálku**, i když jsme zrovna na druhém konci světa a nejsme připojeni na domácí Wi-Fi.

Brainstorming: způsoby ovládání a rizika

Nyní nechte žáky ve skupinách vypracovat **PL 3.** Na základě předchozí diskuze by už měli být schopni jasně odlišit **lokální ovládání** (jsem doma na stejné Wi-Fi) a **cloudové ovládání** (ovládám zvenčí přes server). Provedte s nimi brainstorming o výhodách a především bezpečnostních rizicích obou přístupů. Případně můžete žákům shrnout zásadní rozdíly pomocí **sn. 15**.

Zajímavá diskuse může vyplynout z otázky „U kterých zařízení vám vadí, že posílají data pryč? A u kterých ne?“

Rizika a paradoxy chytré domácnosti

sn. 16 Přejděte od nadšení z ovládaní na dálku k reálným limitům a hrozbám IoT technologií. Postupně s žáky rozeberte čtyři hlavní problémy:

- **Paradox chytré žárovky:** Zeptejte se žáků: „Co se stane s naší chytrou domácností, když někdo jednoduše cvakne fyzickým vypínačem na zdi?“ Ukažte na tom limity technologií – fyzické přerušení napájení znamená okamžitou ztrátu spojení a z chytrého zařízení je rázem „hloupý“ kus skla.
- **Závislost na cloudu a mobilu:** Položte třídě otázku, co se stane, když vypadne domácí Wi-Fi, nebo když má výpadek server výrobce kdesi v zahraničí. Žáci by si měli uvědomit, že bez připojení často nezapnou ani pračku, pokud ji nelze ovládat lokálně.
- **Konec podpory aplikace:** Zeptejte se, jak dlouho vydrží svítit běžná LED žárovka (klidně 10 let). Ale co se stane, když výrobce za dva roky zkrachuje nebo přestane aktualizovat aplikaci pro nové telefony? Zařízení sice fyzicky funguje, ale softwarově se z něj stane nepoužitelný elektroodpad.
- **Zranitelná zařízení (kamery, zámky a zvonky):** Upozorněte na bezpečnostní stránku věci. Levná IoT zařízení často nemají téměř žádné zabezpečení. Chytrá kamera v obýváku nebo domovní zvoněk se tak mohou velmi snadno stát vstupem pro hackery přímo do jejich soukromí.

Kdo dostává data a proč

- **sn. 17–23** Zobrazte tabulku. S žáky postupně diskutujte a doplňujte tabulku.
Návodné otázky:
 - Na **sn. 17** „Co musí hodinky odeslat, aby aplikace zobrazila graf spánku nebo kroků?“
 - Na **sn. 20** „Jak ví aplikace, že žárovka právě svítí?“
 - Na **sn. 21** „Odkud aplikace pozná, že vysavač uklízel a kde byl?“
 - Na **sn. 22** „Jak aplikace ví, jak je doma teplo a kdy se topení zapíná?“
- Upozorněte, že data (mapa bytu, tep) často nekončí jen u nás, ale u výrobce.
- **PL 🧑 4.** Žáci ve skupinkách podobně analyzují žárovku, dveřní senzor a chytrou zásuvku (zda přijímají/odesílají data a co o nás reálně prozrazují).

A.4 Pracovní listy

A.4.1 Pracovní list pro 1. hodinu

Bezdrátové počítačové sítě

v2 2025-11-27

 **1.** Uvedte výhody a nevýhody způsobů připojení k internetu.

Způsob připojení	Výhody	Nevýhody
Kabelové		
Bezdrátové		

 **2.** Která koncová zařízení se doma běžně připojují k internetu?

.....
.....

3. Bezdrátová komunikace funguje na základě

4. Zařízení, které vytváří **domácí síť** a připojuje ji k internetu, se nazývá

.....

5. Proč je otevřená Wi-Fi síť riziková?

- ☐ Může se k ní připojit kdokoli v dosahu.
- ☐ Je vždy pomalejší než zabezpečená síť.
- ☐ Někdo může odposlouchávat přenos dat mezi zařízeními.
- ☐ Útočník může zfalšovat webové stránky.
- ☐ Přenos dat není šifrován.
- ☐ Připojuje se k ní málo lidí.

A.4.2 Pracovní list pro 2. hodinu

Přenos dat v sítích

v1 2025-11-17

 **1.** Představte si, že jste ředitel muzea. V depozitáři máte velkou kostru dinosaura. Chcete ji lidem ukázat, ale kostra je velmi křehká a cenná.

a) Jaké máte možnosti, jak to udělat?

.....
.....
.....

b) Která z navržených možností je podle vás nejlepší? Proč?

.....

c) Jak bychom mohli zajistit, že bude opravdu celá — že nic nechybí a že části půjdou správně dohromady?

.....
.....

 **2.** Co kostra dinosaura v této představě znamená, když mluvíme o přenosu dat po internetu?

.....

 **3.** Co se stane se souborem, než se pošle?

4. Každý paket obsahuje:

.....

5. Vyber správné tvrzení.

Síťový protokol funguje v počítačové síti podobně jako

a) **motor v autě**, dodává datům energii, aby se mohla v kabelech pohybovat rychleji.

b) **pravidla silničního provozu**, určuje přesný řád, jak se mají data v síti pohybovat.

c) **paměťová karta**, dohlíží na to, aby se všechny odeslané zprávy natrvalo uložily.

 **6.** Zařízení v síti se identifikují pomocí IP adresy. Co přesně znamená písmeno „P“ v této zkratce a jak to souvisí s tím, co jste dělali při simulaci sítě?

.....

A.4.3 Pracovní list pro 3. hodinu

Bezpečnost v sítích a ochrana dat

v4 2025-12-11

1. Doplňte věty:

- a) Když do prohlížeče zadám adresu webu, můj počítač se spojí se, který má stránku uloženou.
- b) Server neposílá stránku jako celek – posílá a prohlížeč je poskládá.

 2. Rozhodněte, co by měl firewall „pustit“ nebo „zastavit“. Uveďte proč.

- a) Nová aplikace odesílá velké množství dat na nějakou cizí internetovou službu.
.....
- b) Někdo se pokouší vzdáleně přistoupit k vašemu počítači.
.....
- c) Operační systém chce stáhnout oficiální aktualizaci ze serveru výrobce.
.....
- d) Uživatel otevírá webovou stránku přes HTTPS, ale její obsah je škodlivý.
.....

 3. Doplňte.

Situace	Co útočník vidí? (1–3 slova)
Nešifrovaný přenos (HTTP)	
Šifrovaný přenos (HTTPS)	
Koncové šifrování (E2E)	

4. Ke každé situaci vyberte co **nejvhodnější ochranu**.

	HTTPS	E2E	VPN
Píšu kamarádovi přes chat.	☐	☐	☐
Přihlašuji se na web do školního systému.	☐	☐	☐
Používám veřejnou Wi-Fi v kavárně.	☐	☐	☐
Píšu kamarádovi přes chat, ale používám veřejnou Wi-Fi v obchodním centru.	☐	☐	☐

A.4.4 Pracovní list pro 4. hodinu

Internet věcí a chytrá domácnost

v3 2025-12-07

 1. Ke každému zařízení určete jestli ho

A) používá ho člověk aktivně,

B) pracuje samo (zjišťuje něco a automaticky reaguje).

☐ chytrá žárovka

☐ notebook

☐ mobil

☐ teploměr v chytré meteostanici

☐ dveřní senzor

☐ smartwatch

☐ chytrá zásuvka

☐ robotický vysavač

2. Jak poznáte, že je **zařízení chytré**?

.....

3. Ke každému způsobu, jak zařízení může posílat data napište **jednu výhodu** a **jednu nevýhodu** pro uživatele.

a) Přímou do mobilu:

.....

b) Přes cloud výrobce:

.....

 4. Doplňte tabulku.

Zařízení	Posílá data?	Přijímá pokyny?	Jaký údaj o mně sbírá?
Chytrá žárovka			
Dveřní senzor			
Chytrá zásuvka			

 5. Jakou **výhodu** chytrých zařízení považujete za nejdůležitější? Jaké **riziko** je podle vás největší?

.....

.....

6. Které zařízení podle vás sbírá nejcitlivější údaj? Proč?

.....

A.5 Protokoly

A.5.1 Protokol ke třídě

PROTOKOL – TŘÍDA

v1 2025-11-06

Škola	
Třída, skupina¹	
Celkový počet žáků	

	1. hodina	2. hodina	3. hodina	4. hodina
Datum				
Začátek				
Počet žáků				
Počet žáků s OMJ ²				
Počet žáků s SVP ³				
Pozorovatel				

Specifika třídy, vnější vlivy, poznámky vyučujícího:

Celkový dojem z výuky:

1. hodina:

2. hodina:

3. hodina:

4. hodina:

Osobní dojem:

¹v případě dělení na skupiny

²odlišný mateřský jazyk

³speciální vzdělávací potřeby

A.5.2 Protokol pro pozorovatele

Poznámka: Otevřený pozorovací arch pro 1. vyučovací hodinu, určený k chronologickému zápisu průběhu výuky a reakcí žáků. Pro zbylé hodiny byl arch obsahově identický, lišil se pouze v čísle hodiny a tématu.

PROTOKOL – POZOROVATEL

v1 2025-11-07

1. hodina

Téma: Bezdrátové počítačové sítě

A.6 Informovaný souhlas

Poznámka: Informovaný souhlas mohl být po dohodě se školou modifikován (např. doplněním pole pro vyjádření nesouhlasu s účastí na výzkumu či řešením přeřazení žáků do jiné třídy).



Informovaný souhlas

Dobrý den,
vaše dítě se ve dnech _____ zúčastní výukového bloku „Internet a sítě“ v rámci školního vyučování. Tento blok je součástí výzkumné studie realizované na Matematicko-fyzikální fakultě Univerzity Karlovy, která se zaměřuje na výuku počítačových sítí na středních školách.

Výukový blok povede externí vyučující z Matematicko-fyzikální fakulty Univerzity Karlovy. Součástí výuky může být také pozorovatel, který sleduje průběh hodiny a zaznamenává si poznámky o tom, jak jsou jednotlivé aktivity vedeny a jak na ně žáci reagují. Pozorovatel nehodnotí žáky a nezasahuje do výuky.

Na začátku a na konci výukového bloku žáci vyplní krátký anonymní dotazník, který slouží k vyhodnocení srozumitelnosti a přínosu výuky. Účast na vyplnění dotazníků je dobrovolná – pokud neudělíte souhlas s využitím anonymních dat, žák se výuky zúčastní běžným způsobem a nebude dotazníky vyplňovat.

Během výuky nebudou pořizovány žádné zvukové ani obrazové záznamy. Program nepředstavuje pro žáky žádné jiné riziko než běžná výuka v odborné učebně.

Získané informace budou využity výhradně pro potřeby výzkumné studie realizované na Matematicko-fyzikální fakultě Univerzity Karlovy, pro účely přípravy vzdělávacích materiálů pro výuku informatiky v ČR a pro účely případných prezentací na odborných akcích (např. konferencích pro učitele informatiky). Všechny výsledky budou zpracovány anonymně a prezentovány pouze ve zobecněné podobě, bez možnosti identifikace konkrétních žáků.

Účast na výuce je povinná. Účast na výzkumu je dobrovolná a závisí na souhlasu zákonného zástupce. Materiály vzniklé v rámci projektu budou po dokončení výzkumu volně dostupné pro další školy a učitele.

Svým podpisem stvrzujete, že jste byli informováni o průběhu výuky a dobrovolně souhlasíte s tím, aby se Vaše dítě za výše uvedených podmínek této výzkumné studie zúčastnilo.

Děkuji za spolupráci.

Bc. Adam Papula

Jméno a příjmení dítěte:

Jméno a příjmení zákonného zástupce:

V dne

.....
podpis dítěte

.....
podpis zákonného zástupce