UNIVERZITA PALACKÉHO V OLOMOUCI

PEDAGOGICKÁ FAKULTA

Katedra technické a informační výchovy

Diplomová práce

Bc. Jan Sedláček

Tvorba metodických návrhů se zaměřením na problematiku internetové bezpečnosti v kontextu informatických předmětů na 2. stupni ZŠ

Olomouc 2023

vedoucí práce: Mgr. Tomáš Dragon

Prohlášení

Prohlašuji, že jsem tuto bakalářskou práci vypracoval samostatně a veškerou literaturu a ostatní informační zdroje, které v ní byly použity, jsem uvedl na konci této diplomové práce v seznamu použité literatury.

V Olomouci dne …… ……

vlastnoruční podpis

Poděkování

Tímto chci poděkovat mému vedoucímu práce panu Mgr. Tomáši Dragonovi a prof. PhDr. Milanu Klementovi Ph.D. za vedení práce, trpělivost a věcné rady, které mi pomohly k vypracování této práce.

Bc. Jan Sedláček

Obsah

Úvod

Internet do našeho světa přináší mnoho. Od pohodlného nakupování, přes možnosti rychlé komunikace s přáteli, po pracovní a vzdělávací účely. I možná právě proto si přístup k němu dle Českého Statistického Úřadu (2021) pořídilo celkem 83 % českých domácností. Internet však není pouze jen „dobrým sluhou“, ale může být i „zlým pánem“ právě kvůli nebezpečím, která se zde vyskytují. Tato rizika mohou negativně ovlivňovat žáky ve školách, pro které je internet již každodenní záležitostí (vrátíme-li se k výzkumu ČSÚ, dozvíme se, že celkový počet domácností s dětmi, které mají přístup k internetu čítalo v roce 2021 na 99,3 %), a to nejen co se týče zábavy, ale i jejich vlastního vzdělání – je to poměrně nedávno, co se do pomyslného kyberprostoru přesunulo české školství kvůli celosvětové pandemii. Právě z důvodu velkého rozšíření používání internetu je důležité dnešní žáky poučit o jeho nebezpečích už ve školách a například i hodinách informatiky. K tomuto by měla částečně dopomoci i tato práce.

Tato práce je pomyslně rozdělena na dvě části – teoretickou a praktickou.

Ta první, teoretická, se bude nejprve zaměřovat na problematiku internetu, jeho historii, funkce a množství rizik jeho užívání s jejich možnou prevencí. Následně se zaměří na umístění informatiky a bezpečnosti na internetu v aktuálním rámcovém vzdělávacím programu pro základní vzdělávání a další implementaci tohoto tématu ve školách prostřednictvím plánu prevence rizikových chování či mimoškolními projekty a organizacemi. V neposlední řadě bude představen a vysvětlen proces plánování výuky s jeho jednotlivými částmi.

Na tuto část práce bude navazovat část praktická. Ta bude zaměřena přímo na tvorbu a prezentaci metodických návrhů týkající se bezpečnosti na internetu, ve kterých bude využito poznatků z předchozí (teoretické) části práce. Tyto návrhy budou doplněny pracovními listy k jednotlivým tématům, které budou uvedeny v přílohách této práce. Dále bude pokračovat částí ověřovací a částí věnované získání zpětné vazby od žáků.

Cíle práce

Pro vypracování této diplomové práce byly na začátku nejprve stanoveny její cíle. Ty jsou rozděleny na cíl hlavní a cíle vedlejší. Tyto cíle byly vytvořeny v souladu s tématem této práce.

Hlavním cílem je – jak již z názvu této práce vyplývá – **vytvořit metodické návrhy zaměřené na problematiku internetové bezpečnosti v kontextu informatických předmětů na 2. stupni ZŠ.**

Ty budou společně s již zmíněnými doplňujícími pracovními listy vytvořeny za účelem případného zjednodušení výuky o této problematice, její popularizace a předejití nežádoucích rizikových situací spojených s internetem a jeho službami.

Po cíli hlavním byly dále sestaveny cíle vedlejší. Ty mají za úkol doplnit cíl hlavní či dopomoci při jeho plnění. Za vedlejší cíle byly zvoleny.:

1. **Vysvětlení výše zmiňovaných problematik v teoretické části** – z důvodu následné práce s nimi v rámci plnění cíle hlavního při tvorbě vlastních metodických návrhů v praktické části této práce.
2. **Získání a zhodnocení zpětné vazby od žáků** – pro doplnění hlavního cíle z hlediska získání názorů žáků na produkt praktické části.

1 Internet

„Cyberspace. a consensual hallucination experienced daily by billions of legitimate operators, in every nation, by children being taught mathematical concepts... A graphic representation of data abstracted from banks of every computer in the human system. Unthinkable complexity. Lines of light ranged in the nonspace of the mind, clusters and constellations of data. Like city lights, receding.“

- William Gibson, *Neuromancer* (1984)

Pro účely této práce je důležité popsat internet, jelikož vychází z poznatků o něm. I když nám citát zvolený pro započetí této práce z dystopického sci-fi románu Williama Gibsona již trochu naznačil co můžeme pod pojmem internet či v úvodu zmíněného pojmu „kyberprostor“ očekávat, je důležité jej popsat přesněji. Greenlaw a Hepp (Bidgoli, 2002) jej definují jako globální informační systém, který je propojen pomocí unikátních adres internetového protokolu (IP), podporuje komunikaci na bázi protokolu TCP/IP a jejího rozšíření a s pomocí těchto zmíněných protokolů umožňuje fungování služeb. Zjednodušeně řečeno se jedná o globální systém propojených počítačů s uživateli a daty. Jako jedním z důležitých charakteristik internetu uvádějí, že si jeho uživatelé byli schopni vytvořit vlastní online kulturu, a to hlavně díky možnosti komunikovat na dálku a jednoduchému přístupu k informacím. Celý internet takto přirovnávají k takzvané „informační superdálnici“, po které uživatel jede jako řidič svým pomyslným autem. Naučit se toto pomyslné auto řídit je jednoduché, uživatel však může dosáhnout hlubšího porozumění svého „vozidla“ a virtuálního světa kolem něj.

Historie internetu

Předtím než se internet světovým fenoménem byl jeho předchůdce čistě vojenskou záležitostí. Takto o něm mluví autoři Keefer a Baiget (2001), kteří poukazují na fakt, že to, co v dnešní době známe jako internet, byla v samém prvopočátku myšlenkou tajné vojenské sítě pro přenos informací mezi spojovacími centry, kde by přenos dat pokračoval i po vyřazení jedné ze stanic. Vývoje tohoto projektu se ujala Americká DARPA (Defence Advanced Research Projects Agency – agentura ministerstva obrany pro pokročilé výzkumné projekty, dříve ARPA). Portál Internet Society (1997) uvádí, že plán pro tuto síť pracující na technologii přepojování paketů byl sestaven již v roce 1966. Užití této technologie oproti staršímu přepojování okruhů bylo zdůvodněno reliabilitou této nové technologie, a právě již zmíněné ochraně proti výpadku spojení. Tato síť, nazvaná ARPANET, byla postupně zkoušena

na Amerických univerzitách a následně veřejně demonstrována v roce 1972 na ICCC (International Computer Communication Conference – mezinárodní konference pro počítačovou komunikaci).

Keefer a Baiget (2001) uvádí, že ARPANET měl 3 funkce. Těmi byly Telnet (systém pro logování do systému vzdálených počítačů z terminálů pro přístup), FTP (File Transfer Protocol – protokol pro přesouvání souborů mezi počítači) a SMTP (Simple Mail Transfer Protocol – protokol pro přenos jednoduchých zpráv neboli e-mail). Fungování těchto služeb bylo zajištěno pomocí internetového protokolu (IP) a rodinou protokolů TCP/IP (Transmission Control Protocol/Internet Protocol), kde IP má za úkol najít nejvhodnější cestu v síti pomocí routerů (směrovačů) a doručit informace k příjemci za pomoci IP adres (identifikátor zařízení/počítače v síti), a kde TCP/IP zajišťuje rozložení zprávy či přenášených dat do diskrétních balíčků a jejich opětovné sestavení v zařízení příjemce.

Greenlaw a Hepp (Bidgoli, 2002) dále zmiňují, že postupem času se do sítě začaly kromě univerzit a státních podniků dostávat i komerční organizace. K největšímu nárustu došlo v devadesátých letech minulého století, a to především v roce 1992, kdy byl internet zpřístupněn široké veřejnosti. Byly vytvořeny organizace pro standardizaci webu (např. W3C – World Wide Web Consortium) a prostředky a aplikace pro jeho používání (prohlížeče, programovací prostředí atd.) Jako hlavní pozitiva internetu uvádějí jednoduchost a rychlost komunikace, spolehlivost, rozšiřitelnost, pohodlí užívání, možnosti edukace a zábavy a sdílení dat a informací.

Služby internetu

Těch je dosaženo pomocí takzvaných služeb internetu. Těch je podle Hladké a Fouska (MUNI) několik základních. První zmiňovanou službou je WWW (World Wide Web). Zkráceně „web“ (síť) poskytuje uživatelům obsah různého typu (od textového po multimediální) a je tak hlavní složkou internetu, která je přístupná skrze různé webové prohlížeče. Druhou službou je e-mail, jeho podstatou je zasílání zpráv mezi uživateli. Následuje internetové bankovnictví, to – jak již z názvu vyplývá – umožňuje uživateli přístup k penězům pomocí internetu a provádět s nimi různé operace. Čtvrtou službou je cloud. Jedná se o technologii vzdáleného úložiště, ke kterému se uživatel dostane prostřednictvím internetu. Následuje VoIP (Voice over Internet Protocol) a jiné hlasové služby (Discord, Skype atd.), jenž zajišťují přenos hlasových hovorů po internetu. Šestou uváděnou službou je FTP. To již bylo zmíněno jako jedna z původních funkcí APRPANETu a jedná se o protokol určený

k přenosu souborů. Poslední popisovanou službou je peer-to-peer. Jedná se o technologii, která na rozdíl od výše zmiňovaných nepotřebuje centrální server. Uživatelé jsou tak přímo propojeni mezi sebou. Výhoda oproti architektuře klient-server je právě tato decentralizace, která chrání uživatele před výpadky.

I když se tedy může zdát, že internet byl vytvořen pro zjednodušení komunikace, přístupu k informacím, a tedy jinak prospěšným činnostem s pozitivním charakterem, můžeme se zde (ať už my či žáci ve školách) dostat do nebezpečných situací. Tato negativa budou popsána v následující podkapitole.

1.1 Nebezpečí internetu

Velmi důležitou součástí této práce je pochopení jednotlivých nebezpečí, se kterými se žáci na internetu mohou setkat, a tedy obsahu vyučovaných témat. Dle Kopeckého (2015) je internet pro děti každodenní záležitostí, a to jak pro zajištění zábavy, tak pro komunikaci. Šmahel (Ševčíková a kol., 2015) též uvádí, že jsou dnešní děti už od malička obklopeny moderní digitální technikou včetně internetu. To může vést k negativním zkušenostem s online prostředím. Je tedy nutné žáky na tyto rizika připravit i v hodinách informatiky v rámci učiva o bezpečnosti. Potřebu výuky bezpečnosti na internetu nám potvrzuje i výzkum Szotkowskiho a Kopeckého (2019a), podle kterého se žáci s různými (nejen) potenciálními rizikovými situacemi, jež jsou spojeny s internetem opravdu setkávají. Konkrétně zmiňují nebezpečí na sociálních sítích (či jiných komunikačních platformách), prodejních portálech a v prostředí online her.

Kopecký (2015) dále popisuje, proč k těmto nekalým aktivitám na internetu dochází. Za tímto stojí specifičnost internetové komunikace, kdy si jednotliví uživatelé mohou přijít nedotknutelní, za což může například anonymita na internetu – komunikace není takzvaně tváří v tvář, nýbrž skrytá pod přezdívkami, nespojitá v čase a v případech nějakou vymyšlenou osobností či maskou, za kterou může osoba skrývat své reálné úmysly a záměry.

Následně budou popsána jednotlivá nebezpečí, se kterými se žák základní školy může na internetu setkat.

Dezinformace

Dezinformace jsou Ministerstvem Vnitra ČR (portál mvcr.cz) popisovány jako nepravdivé informace, jež jsou šířeny s úmyslem klamat obyvatelstvo. Bývají často využívány v propagandě, což je neobjektivní šíření informací, které má za účel manipulovat s člověkem. Jako nejčastější podoby propagandy jsou zmíněny psychologická válka či politické propagandy.

Kopecký (2022, portál e-bezpeci.cz) jmenuje další druhy dezinformací. První z nich je takzvaný hoax. Jedná se o informaci, jejímž účelem je vyvolat paniku. K hoaxům patří však i žertovné zprávy či legendy a jsou často doplněny i obrazovým materiálem. Další kategorií dezinformací jsou misinformace. Ty jsou rozdílné od hlavního popisu dezinformace tím, že nejsou úmyslné a jsou šířeny nepoučeným propagátorem, který si myslí, že je jeho informace pravdivá. Kopecký dále uvádí termín fake news. Tím označuje lživé zprávy, které nejsou satirické, a média, co je šíří. Právě z důvodu šíření těchto informací internetem je důležité je žákům představit a upozornit na ověřování informací.

Gambling

Licehammerová (Blinka a kol., 2015) popisuje **gambling** jako fenomén, jež obsahuje různé formy hry jejichž cílem je nejčastěji peněžní výhra. Různé formy gamblingu se nacházejí i na internetu či v rámci počítačových her, což přináší pro hráče výhody týkající se dostupnosti, soukromí či anonymity. Podobně jako hazardní hry v kasínech mohou být i tyto aktivity návykové a řadí se mezi nelátkové závislosti. Licehammerová jako příklady online gamblérství zmiňuje například online poker, kurzové a živé sázení či další hry spojené s virtuálními kasíny (např. hrací automaty).

Toto však nejsou jediné rizikové složky internetového hazardu. V současné době se potýkáme například s fenoménem takzvaných „loot boxů“ (krabice či truhly s kořistí/pokladem) ty jsou popisovány autory Zendle, Meyer a Over (2019) jako moderní způsob, jak utrácet peníze ve videohrách. Jedná se o mikrotransakce, které nám zpřístupní pomyslný virtuální výherní automat, jehož cenou je nějaký virtuální předmět, který může mít přiřazenou peněžní hodnotu a je s ním možno dále obchodovat.

Příkladem může být počítačová hra Counter Strike: Global Offensive, která tyto „bedny“ nabízí a za otevření jedné (zakoupení klíče) si účtuje 2,49 euro. Hráči se po zakoupení tohoto klíče a jeho použití na samotné „bedně“ zobrazí grafika podobná právě hernímu

automatu či ruletě, která se zastaví na „vyhraném“ virtuálním předmětu – v případě této videohry se jedná o vzhledy zbraní, které jsou řazeny do kategorií podle vzácnosti, čímž vzniká podobné riziko jako při peněžním hazardu v reálném světě. Tyto vzhledy mohou totiž nabývat hodnot od několika centů po tisíce dolarů u těch nejvzácnějších. Větší problém, než u fyzických automatů nastává v tom, že tyto hry jsou dostupné i mladistvým a nejsou regulované.

Je zmíněn fakt, že tyto videohry se snaží na tuto herní mechaniku nalákat potencionální zákazníky například jedním „zatočením“ zdarma či zobrazením toho že hráč skoro vyhrál hlavní cenu a vybízí ho k dalšímu zakupování klíčů. Důvodů k participaci v tomto hazardu je podle autorů několik – virtuální zboží může být bráno jako status symbol, vidina výdělku na prodeji vzácného předmětu, z vlastního pocitu zábavy z této činnosti, podpoření vývojářů hry či dokonce z důvodu přínosu výhody ve hře. Právě poslední zmiňovaný důvod je dle výzkumu těchto autorů nejčastější motivací.

Dle Licehammerové (Blinka a kol., 2015) má online gambling větší potenciál k vyvolání závislosti právě díky jeho dostupnosti a je proto důležité implementovat její prevenci. Toho může být dosaženo například tvrdým limitem maximálního vkladu na straně poskytovatele služby či celkovým rozšířením finanční gramotnosti v populaci. Případná léčba online gamblérství je dle autorky podobná jako u látkových závislostí (potažmo „offline“ gamblérství) a může být jak individuální, tak skupinová. Principem je postupné přerušení návyků takto nebezpečně hrát.

Grooming

Grooming případně kybergrooming je Kožíškem a Píseckým (2016) popisován jako zneužívání a vylákání uživatele internetu prostřednictvím vyvolání pocitu důvěry za pomoci falešné identity. Agresoři vytvářejí falešné profily, které mají za účel nalákat jejich „kořist“ za účelem další manipulativní komunikace. Finálem tohoto snažení je podle Kopeckého (2015) schůzka, jejímž účelem je sexuální nebo jinak násilného zneužití oběti.

Dále popisuje rysy groomingu, kterými jsou samotná manipulace za pomoci lichotek a dárků, ale i hrozbami jako vydíráním a vyhrožováním. Dalším rysem je navázání důvěrného až intimního vztahu s dítětem a následná nevhodná (například sexuálně orientovaná) komunikace s ním. Zmiňuje (str. 30) také to, že většina obětí groomerů jsou děti ve věku od 13 do 17 let – proto je důležité tuto problematiku žákům objasnit. Kožíšek a Písecký (2016, str. 421) také poukazují na fakt, že oběti jsou poměrně genderově vyrovnané (56 % dívek a 44 % chlapců).

Jak Kopecký (2015), tak Kožíšek s Píseckým (2016) vyjmenovávají podobné strategie pachatelů, Těmi jsou „mirroring“, kde dospělý napodobuje chování dítěte ve stejné věkové kategorii jako je jeho oběť. Z tohoto důvodu je pro pachatele důležitá profilace oběti, kdy zjišťuje citlivé údaje o dítěti a jeho zálibách, což mu umožňuje snadnější manipulaci. S těmito informacemi je dle autorů snadné založit falešný profil tak, aby byl pro oběť zajímavý. Následuje samotné kontaktování oběti a již zmíněná následná manipulace s ní.

Dle Kopeckého (2015) je kybergrooming složité odhalit, pokud se dítě nesvěří samo. Může se totiž obávat pomsty anebo naopak nechtějí agresora prozradit kvůli citům k němu – obě tyto specifika se mohou vztahovat k době před i po osobní schůzce. Je tedy důležitá prevence v podobě varování a upozornění na taktiky těchto pachatelů. Autoři považují za důležité například upozornění na nesrovnalosti na falešných profilech – ověřování identity, lákání na dary či finanční obnosy, zvýšené opatrnosti při žádostech zasílání osobních informací či udržování konverzací v tajnosti, při podezření na nekalou činnost se svěřit, a hlavně jakoukoliv případnou schůzku s člověkem, kterého jsme potkali na internetu prokonzultovat s důvěryhodnou osobou.

Kyberšikana

Kyberšikana je dle Kopeckého (2015) opakované agresivní chování, které může být směřováno jak na jednotlivce, tak skupinu, a při kterém je na rozdíl od tradičního pojetí šikany využito digitálních zařízení. Může se jednat o vyhrožování, vydírání, ponižování či ztrapňování prostřednictvím sociálních sítí a jiných komunikačních prostředků. Kopecký dále jmenuje krádež identity, exkluzi z online komunity, slovní napadání a jiné opakované obtěžování. Zdůrazňuje také, že kyberšikanu může být obtížné rozpoznat. Tuto skutečnost potvrzují i Kožíšek a Písecký (2016), kteří vysvětlují, že kyberšikana nezanechává na oběti fyzické, viditelné znaky, jakým jsou například modřiny. Oběť kyberšikany je týraná psychicky a následky mohou být podobné změnám osobnosti v pubertě či jiné životní události. Příklady mohou být změna chování, uzavřenost nebo zhoršení prospěchu.

Možnosti prevence kyberšikany popisuje Černá (Ševčíková a kol., 2015) a to tak, že oběť šikany tohoto typu by měla ze všeho nejdříve vědět, že na tuto situaci není sama a aby měla prostředky k tomu, aby se mohla se svým problémem svěřit. To je důležité hlavně z důvodu dalšího řešení. Kožíšek a Písecký (2016) rovněž apelují na okamžité řešení situace a v případě eskalace informovat příslušné správní orgány.

Malware

Mezi řadu nebezpečí pocházející z internetu, které mohou žáci nalézt se řadí i **malware** (složenina: mal – malicious – škodlivý, ware – software). Ten je popisován Kolouchem (2017) jako jakýkoliv software určený k narušení normální funkce počítače, získání dat v něm uložených nebo k přístupu do jeho systému. Malware je tedy označení pro řadu nebezpečných softwarů, které můžeme dále řadit do podkategorií. Nejméně nebezpečným malwarem je adware (ad – advertisement – reklama). Jedná se o software, jehož úkolem je šířit nechtěnou reklamu například vyskakujícími okny na obrazovce počítače. Spyware (spy - špeh) zajišťuje útočníkovi získat data o počítači bez vědomí uživatele jejich automatickým odesíláním. Virus je programem či kódem, který se dokáže připojit k počítačovému souboru a dokáže se tak šířit sám. Viry mohou být různé severity a mohou sahat od praktických vtipů po celkovou destrukci systému. Červ (worm) bývá označován jako virus, rozdílem je však fakt, že červ ke svému šíření nepotřebuje připojení k souboru (hostiteli) a dokáží se šířit samostatně. Takzvaný Trojský kůň je malware, který se vydává za normální software, ale ve své skutečnosti dokáží způsobit nepříjemnosti bez vědomí uživatele. Stejně tak jako v legendě mají za úkol vpravit k uživateli zkázu. Jedním takovým typem trojského koně jsou takzvané backdoors (zadní vrátka), jejichž úkolem je nepozorovaně usnadnit dalším malwarům přístup do počítače.

Další Kolouchem popisovaným typem malwaru je rootkit. Jejich cílem je změnit chování operačního systému či jeho složek tak, aby nedošlo k objevení malwarů v systému. Keylogger je program, který zaznamenává údery na klávesnici a ty odesílá útočníkovi. Posledním zmiňovaným malwarem je ransomware (ransom - výkupné), jehož úkolem je vymáhat peníze po uživateli například pro opětovné zpřístupnění jeho dat. Vydírání však může být různého typu.

Phishing

Jedním z dalších nebezpečí internetu je **phishing**. Ten Kožíšek a Písecký (2016) popisují jako podvod, jehož cílem je získání citlivých údajů zejména určeným pro přístup k uživatelským účtům či penězům poškozeného. Je to ve své podstatě metoda sociálního inženýrství s prvky manipulace, kterou můžeme přirovnat k rybaření (odkud také název pochází). „Návnadou“ nám může být například spamový email, který je dle Kopeckého (2015) nejefektivnější způsob, jak se dostat k co nejvíce uživatelům. Obsah tohoto emailu klade důraz na zaslání tajných informací (hesel, čísel kreditních karet atd.) původnímu odesílateli či jejich vyplnění do elektronického formuláře. Tyto elektronické zprávy mohou dle autorů nabývat

různého charakteru, a to od falešných zpráv od banky a exekucí po neexistující zásilky, výhry v loteriích. Nemusí se však jednat pouze o zprávy. Kopecký (2015, str. 97) uvádí například i podvodné aplikace, které dokáží skrytě pracovat v chytrých telefonech a bez vědomí uživatele zasílat nechtěná data mimo zařízení a do pomyslných rukou pachatelů.

Internetové podvody

Zmíněný phishing patří do kategorie **internetových podvodů**. K těm Kožíšek s Píseckým (2016) dále řadí například i internetové obchody a prodejce, kteří po zaslání peněz nezašlou kupované zboží či v případě falešných inzerátů, kdy zásilka sice dorazí, ale s úplně jiným obsahem. Dalším příkladem podvodů můžou být ty, které cílí na city a dobré skutky lidí. K takovým patří i případ ženy, která zaslala více jak dva miliony korun českých neznámému muži, jenž se na seznamce vydával za vojáka v nouzi. (Bartosz, 2022, Novinky.cz)

Kopecký (2015) i Kožíšek s Píseckým (2016) uvádí možnosti prevence. Těmi jsou hlavně informování o možných typech podvodů, nezasílání citlivých informací či peněz nedůvěryhodným (neověřeným) osobám, v podvodných emailech sledovat, zda se v nich nenachází překlepy, používat antivirový software, který dokáže podvody odhalit, neotvírat přílohy z podezřelých emailů či webových stránek a ověřovat si informace (u nákupů například stránky prodejce, jejich registrace v rámci státu atd.).

Sexting

Sexting je dle Kopeckého (2015) popisován jako internetová komunikace se sexuálním podtextem, která může být doprovázena sdílením vlastních videí či fotografií s obsahem tomu podobným. K této komunikaci většinou dochází na sociálních sítích, ale není zcela vázána. Ačkoliv se zprvu může zdát, že je sexting zcela bezpečnou aktivitou, co se týče například dospělých párů, vystavuje nebezpečí (nejen) pro děti. Sexting a komunikace jemu podobná byla již částečně zmíněna v podkapitole o groomingu a může být tedy brána i jako jeho součást. Rizikům však nejsou vystaveny pouze děti, ale dle Kožíška a Píseckého (2016) také i ostatní, kteří jej provozují. Zmiňují, že pokud tato data (fotografie, videa) odešleme jakékoliv jiné osobě, jsou mimo náš dosah a již nemůžeme kontrolovat jejich další šíření. Tohle může být následně zneužito například při vydírání, znectění či jiném nátlaku na poškozenou osobu. Kopecký (2015) dále zmiňuje možnost objevení tohoto materiálu širokou veřejností, které může vést k následkům jako ztráta prestiže, vztahů či zaměstnání. V případě sextingu u dětí takto může dojít i k trestnému činu šíření dětské pornografie.

Stalking

Macháčková (Ševčíková a kol., 2015) zmiňuje nebezpečí zneužití informací uváděných na internetu a sociálních sítích – zejména o aktuální poloze, pohybu a bydliště. Tyto informace jsou hlavními prostředky využívanými ke stalkingu. **Stalking** (popřípadě též nazývaný **kyberstalking**, pokud je provozovaný v prostředí internetu) je Kožíškem a Píseckým (2016) popisován jako nechtěné pronásledování osoby, u které dochází k trestné činnosti. Může se projevovat vyhrožováním osobě, neustálým kontaktováním, sledováním z dáli, omezováním v pohybu, zneužíváním osobních údajů oběti nebo šířením lží o ní. Jako obranu proti stalkingu autoři zmiňují apelaci na stalkera, aby přestal, nepřistupování na jeho návrhy, nepublikování informací o aktuální poloze a nepravidelné střídání pohybu, zablokování možnosti komunikace a oznámení policii.

Závislost na internetu

Jako riziko používání internetu je také zmiňována **závislost** na něm. Ta má dle Škařupové (Blinka a kol., 2015) i Kopeckého (2015) podobné symptomy jako jiné látkové či nelátkové závislosti uváděné v DSM-V (APA, Diagnostický a statistický manuál duševních poruch). Těmi jsou stavy, kdy uživatel internetu nad ním a jejím používáním neustále přemýšlí, změny nálady, potřeba neustálého navyšování „dávky“, abstinenční příznaky, konflikty s různými součástmi života jedince (okolí, osobní život atd.) a následným opakováním zmíněných jevů po neúspěšném odvykání.

Závislost na internetu je Kopeckým (2011) označována za netolismus, a to společně s dalšími „virtuálními drogami“ jako jsou počítačové hry či sociální sítě. Dle K. S. Young (2004) se však může jednat i o závislostní chování spojené s online nakupováním, pornografií či virtuálním vztahům. Szotkowski a Kopecký (2019b) uvádějí také příklady dalších nemocí s netolismem spojených. Mohou to být nemoci týkající se jak fyzického stavu jedince (bolesti krční páteře, ramen či rukou), tak stavy mysli jako například strach z toho, že zařízení / internet nebudeme moci používat a nebudeme mít aktuální informace (FOMO – fear of missing out) či neustálé nutkání kontrolovat vlastněné digitální zařízení a přerušovat tak aktuálně konanou činnost.

Závislost na internetu takto můžeme dále částečně spojit se závislostí na počítačových hrách – především z hlediska online her pro více hráčů. Hraní počítačových her popisuje Basler a Mrázek (2018) jako potenciálně rizikovou aktivitu, která může kromě závislosti vést například

k epilepsii, nadměrným zatěžováním očí, virtuální nevolnosti, obezity a dalším nejen fyzickým potížím.

Dle Szotkowskiho a Kopeckého (2019b) je internetová závislost brána jako vážný problém především v Asii, kde dle výzkumů trpí tímto typem závislosti až 39 % dospívajících dětí (zmiňováno je Japonsko), nicméně Sedláček (2021) ve svém bakalářském výzkumu zjistil, že závislostí na internetu může v České republice trpět až 26 % žáků – tyto výsledky je však dle autora nutné brát s nadsázkou z důvodu poměrně malého výzkumného vzorku a dobou, kdy byl výzkum realizován (plošná online výuka z důvodu pandemie Covid-19).

Jako prevenci tohoto typu závislosti uvádí Žufníček (MŠMT, 2013) sledování dítěte a jeho pohyb v online prostředí, stanovení limitů a přestávek, podporování dítěte, co se týče jiných koníčků a jeho sebevědomí a zjištění, zda dítě nepoužívá internet a online hry jako únik před jinými problémy.

Společné znaky a prevence

Při listování mezi jednotlivými internetovými nebezpečími můžeme narazit na společné znaky. Tím hlavním, význačným u velké části nebezpečí, je však potřeba neustálého ověřování informací. Od vyhledávání akademických zdrojů pro ověření, zda je na zdánlivém HOAXu či dezinformaci něco pravdivého, přes ověření si identity přátelského cizince na internetu, než mu zašleme svá data či fotky, po vypočítání si, jestli je výhra ve virtuálním herním automatu opravdu dosažitelná nebo zda námi používaná aplikace nezasílá data z našeho zařízení potenciálním pachatelům ať už úplně bez našeho vědomí či po pořádném nepřečtení podmínek jejího užívání. Právě z tohoto důvodu je asi nejlepší prevencí samotné ověřování informací (je zmiňováno různými autory u výše uvedených rizik internetu). To sice může být odrazující co se týče při něm strávené doby, ale je důležité pro bezpečný pohyb (nejen) v kyberprostoru. Prevenci provádíme či můžeme provádět i v rámci výuky na základních školách. Umístění a ukotvení této problematiky (nejen) ve školách je vysvětleno v kapitole 2.

1.2 Anonymita a digitální stopa

S internetovými nebezpečími je spojena anonymita uživatelů na internetu, ať už co se týče v předchozí podkapitole falešných identit používaných útočníky, tak po ochranu vlastních citlivých informací. Celková anonymita je dle Koloucha (2017) však spíše naivní představou uživatelů internetu, a to především z toho důvodu, že se právě tito uživatelé v některých případech vůbec nezajímají o fungování internetu a jeho služeb.

Ty totiž v kombinaci s poskytovateli internetu shromažďují o jednotlivcích velké množství informací, a to jak osobních (jména, příjmení, adresy atd.), tak dalších citlivých informací jako jsou například GPS souřadnice či informace o systému uživatelova zařízení, které mohou být využity potenciálním útočníkem, anebo na druhé straně ochránci zákona.

Digitální stopa

Tyto informace zanechané uživateli můžeme nazvat **digitální stopou**. Ta může být neovlivnitelná nebo uživatelem ovlivnitelná. Součástí neovlivnitelné stopy jsou především informace o zařízení a jeho interakcí s online prostředím. Můžeme zde zařadit IP adresu či MAC adresu zařízení, která je pevně svázána se zařízením. Je zmíněn také virtuální otisk užívaného webového prohlížeče, ten totiž také automaticky předává informace o uživateli jako je například e-mail přihlášeného uživatele (Kolouch, 2017).

Na druhou stranu však existuje digitální stopa, která je uživatelem ovlivnitelná. Jedná se o dobrovolné zveřejnění jakýchkoliv informací jednotlivcem na internetu s jeho vědomím pomocí sociálních sítí, datových úložišť, jiných internetových stránek (blogů, fór) atd. A právě sociální sítě jsou dle Kožíška a Píseckého (2016) v tomto zejména nebezpečné z hlediska hledání obětí a informací o nich. Je tedy nutné dávat si pozor, jaké informace dobrovolně sdílíme.

Dle Koloucha (2017) je tedy nutné dbát na pravidlo, které praví, že cokoliv vložíme na internet, to už tam zůstane napořád i když je sami odstraníme či zneviditelníme. Vždy totiž bude existovat nějaká jejich záloha či kopie – takto sdílená data si už někdo mohl „stáhnout“ či byla zálohována systémem automaticky. Právě z tohoto důvodu Kolouch radí důkladné pročtení smluvních podmínek využívané služby a dále i Kožíškem a Píseckým (2016) zmiňované kladení důrazu na to dávat si pozor kde a komu sdílíme informace o sobě.

2 Informatika a internetová bezpečnost ve školách

Pro tvorbu metodických návrhů zaměřených na bezpečnost na internetu v oblasti výuky informatiky je také důležité nastínit umístění informatiky jako oboru v českém školství a jejího obsahu. Tyto informace jsou dohledatelné v rámcovém vzdělávacím programu pro základní školy (MŠMT, 2021). Informatika je zde vedena jako předmět určený pro rozvoj informatického myšlení a porozumění digitálním zařízením (po úpravách z roku 2021 zde nahrazuje původní předmět informační a komunikační technologie).

Pro tuto výuku je využito praktických úkolů za účelem hledání řešení a efektivního využívání informačních technologií. Na obou stupních je vzdělávací obsah rozdělen do čtyřech kategorií. Těmi jsou 1) data, informace a modelování, 2) algoritmizace a programování, 3) informační systémy a 4) digitální technologie.

Data, informace a modelování

Na prvním stupni základní školy se v první kategorii žáci věnují jednoduchému sběru dat a informací a jejich hodnocení (uveden je například jednoduchý dotazník). Využití jednoduchých piktogramů či značek a kódů pro učivo kódování a přenos dat, kde je zmíněna i ochrana informací, její sdílení a záznam. V části modelování se pak objevuje tvorba obrazových modelů jako jsou jednoduché grafy a myšlenkové mapy. Toto učivo je na druhém stupni rozšířeno o vyhledávání dat a jeho ukládání v počítači a jejich interpretaci, možnosti standardizovaného kódování dat a jednoduché šifry a v neposlední řadě tvorba složitějších grafů či vývojových diagramů.

Algoritmizace a programování

V kategorii **algoritmizace a programování** se na prvním stupni objevuje jednoduchá algoritmizace (krokování) pomocí obrázků či jiných symbolů a textu pro jednoduché postupy. Oblast programování je řešena experimentováním v jednoduchém blokovém programovacím jazyce. Poslední částí je kontrola řešení s následnou případnou opravou programu nebo jeho zjednodušováním. Na druhém stupni je algoritmizace rozšířena o další přizpůsobování programu. Do samotného programování pak přibývají složitější funkce jako například cykly. Rozšířena je i kontrola řešení dalšími způsoby hledání chyby. Přidána je část tvorby digitálního obsahu, ve které si žáci vyzkouší vytvořit vlastní jednoduchou aplikaci. V této části je zmíněna i etická a právní stránka programování.

Informační systémy

Předposlední součástí informatiky na základních školách je učivo o **informačních systémech**. Systémy a jejich součásti jsou popsány na příkladech z reálného života. Druhou složkou je práce se strukturovanými daty, porovnávání vlastností objektů, jejich řazení do seznamů či jednoduchých tabulek. Výuka na druhém stupni na toto navazuje strukturou datových tabulek a jejich úpravou a nastavováním pravidel. Je představeno zpracování dat pomocí funkcí či vzorců, filtrování dat a jejich vizualizace. Zmíněna je i funkce informačních systémů ve společnosti a ochrana dat.

Digitální technologie

Finální součástí učiva informatiky je učivo o **digitálních technologiích**. To je na prvním stupni rozděleno na hardware a software, kde jsou vysvětleny jak jednotlivé součásti počítače, tak ovládání uživatelského rozhraní aplikací, ukládání a otevírání souborů. Dalším tématem jsou počítačové sítě a síťová připojení. V tomto tématu je uveden i internet a práce s ním. Nakonec je zmíněna bezpečná práce se zařízeními, uživatelská hesla a účty. Druhý stupeň opět rozšiřuje poznatky stupně prvního. Téma hardwaru a softwaru je rozšířeno a dále doplněno o operační systémy a jejich funkci, kompresi dat, správu souborů a jejich formáty. V tématu počítačových sítí je popsána funkce webu, internetu a podmínky a specifika jeho fungování. Zmíněny jsou například i další typy sítí, internetové služby či cloudové aplikace. Učivo o bezpečnosti je obohaceno o poznatky ze světa malwaru (vir, antivir atd.), zálohování dat či další typy zabezpečení. Oproti prvnímu stupni je přidáno učivo zaměřené na řešení problémů s technikou a digitální identitě, v jejímž obsahu najdeme jak sledování polohy a internetem dále uchovávané záznamy, tak práci sociálních sítí.

Z této koncepce tedy vyplývá, že už na prvním stupni jsou žáci s problematikou informatiky seznamováni pomocí her a experimentů, a tedy svojí vlastní aktivitou. Své postupy a myšlení si mohou ihned prakticky ověřovat technikou dostupnou na školách a dospívají tak k základnímu porozumění konceptu informatiky a bezpečnému a efektivnímu používání digitálních technologií. V tomto ohledu se nic nemění ani na druhém stupni základní školy – aktivita a vlastní tvorba žáků je dále primární složkou výuky. Jsou však rozšiřovány jejich vědomosti a dovednosti z prvního stupně a tím pádem jejich povědomí o výše zmíněných tématech informatiky, digitálních technologií a bezpečnosti.

Z výše uvedeného se tedy dozvídáme, že problematika informační a dále internetové bezpečnosti je deklarována jako důležitou součástí předmětu informatika a je nutné s ní žáky obeznámit. Součástí jsou témata jako zabezpečení dat a informací jak v počítači, tak na internetu pomocí hesel a šifrování, ochrana proti nežádoucím softwarům nebo téma zahrnující digitální identitu jedince a jeho pohyb na internetu a jeho službách. Tato témata jsou rozložena jak na prvním stupni základní školy, tak na stupni druhém, kdy jsou rozvíjeny dále.

Národní strategie prevence rizikového chování

Prevence s internetem spojených rizikových chování je uváděna i v národní strategii primární prevence rizikového chování dětí a mládeže (MŠMT, 2019), která se kromě jiných zaměřuje i na prevenci závislostnímu chování, netolismu, gamblingu, agrese či rizikovému sexuálnímu chování, které jsou spojeny s internetem. Cíli této strategie jsou vytvoření systému pro prevenci, koordinace vzdělávacích systémů prevence, aktualizace právního rámce, zkvalitnění a zefektivnění vzdělávání pedagogických a jiných pracovníků v oblasti prevence, financování tohoto systému a jeho sledování a hodnocení.

Tento systém primární prevence je dále rozdělen na prevenci všeobecnou pro nedělenou populaci dětí a mládeže jejíž výhodou je oslovení velkého počtu jedinců, prevenci v rámci rizikových skupin a v neposlední řadě indikovanou prevenci zaměřenou na konkrétního jednotlivce (či skupinu), které jsou bezprostředně vystaveny rizikovým faktorům s posouzením individuální situace. U všeobecné prevence je možné organizovat akce nebo výukové programy s lektory z praxe (např. policie). Pokud se však jedná o indikovanou prevenci u jedince, je vyžadován speciální přístup osoby se speciálně-pedagogickým, psychologickým či jiným podobným vysokoškolským vzděláním.

V rámci školy se primární prevencí zabývá školní metodik prevence, jež se zabývá tvorbou preventivního programu ve škole, jeho kontrolou, vedením a koordinaci metodiky pedagogických pracovníků v oblasti prevence, spoluprací školy a jiných státních orgánů a vedením zápisů. Další, čeho může metodik využít, jsou mimoškolní projekty zabývající se problematikou internetové bezpečnosti.

2.1 Mimoškolní projekty zabývající-se internetovou bezpečností

Problematika internetové bezpečnosti není řešena pouze jednotlivými školami v rámci RVP či jiných národních strategií. Zdrojem informací (nejen) pro žáky mohou být také webové projekty, které se zabývají jak bezpečným užíváním internetu a jeho služeb, tak prevencí zmiňovaného rizikového chování s ním spojeným.

Jedním z takových projektů je Projekt E-Bezpečí realizovaný Centrem prevence rizikové virtuální komunikace (PRVoK) Pedagogické fakulty Univerzity Palackého v Olomouci. Zabývá se prevencí, výzkumem, a popularizací internetové bezpečnosti. Konkrétně se zabývá tématy kyberšikany, groomingu, stalkingu, sextingu, dezinformacemi, závislostmi na digitálních technologiích a riziky užívání sociálních sítí. Součástí projektu není pouze informační webová stránka, ale také terénní práce s cílovými skupinami různých věkových kategorií a povolání, celorepublikové výzkumy a vlastní vydavatelská činnost různého charakteru (e-bezpeci.cz).

Za zmínění stojí také projekty Nebuď oběť (nebudobet.cz), Bezpečně online (bezpecne-online.ncbi.cz), Internetem bezpečně (internetembezpecne.cz) či projekty zaměřené na internetovou bezpečnost od portálu Seznam.cz (např. Seznam se s médii, Bezpečně online a Seznam se bezpečně), které se zabývají podobnou tématikou a prevencí nebezpečného chování v online prostředí. Webové stránky některých z těchto projektů sice nebyly již několik let aktualizovány, to však nemění fakt, že mohou být ve výuce užitečné.

Nyní je nám již známa problematika nebezpečí na internetu a její zakotvení v rámci českých škol. Abychom však toto téma mohli kvalitně vyučovat, je za potřebí si naplánovat výuku.

3 Plánování výuky

Další velmi důležitou částí přípravy učitele na výuku a vůbec tvorby metodických návrhů je plánování výuky. Plánování nám tedy napomůže vzít zmíněné informace o internetové bezpečnosti a převést jej do formy, kterou můžeme předat žákům.

Výuka je popisována Šafránkovou (2019) jako složitý systém vzájemně propojených, navzájem závislých prvků společně s vnějším prostředím a jde tedy o lidskou činnost umožňující rozvoj jejich aktérů za pomoci stanovených cílů. Samotný proces výuky je pak uspořádán logicky do pěti prvků. Těmi jsou cíle a kompetence žáka, obsah učiva, spolupráce mezi učitelem a žáky, prostředky výuky (formy, metody, pomůcky atd.) a podmínky, za kterých výuka probíhá. Skalková (2007) shrnuje proces výuky jako součinnost učitele a žáka, kteří mají učivo jako společný předmět činnosti. Obě strany musí k výuce přistupovat aktivně.

Efektivitu takovéto systematizované výuky potvrzují i autorky Stará, Zemanová a Horská (2020), podle kterých je důležité plánovat výuku tak, aby byla konzistentní. Důležitost kladou také na správné rozložení učiva do jednotlivých ročníků. Takto systematizující a plánující učitelé jsou pak schopni volit vhodné strategie pro přiblížení-se výukovým cílům s jejich následným splněním. Zmiňují také pozitivum promýšlení výuky z hlediska diferenciace ve třídě, kde je potřeba brát ohledy na žáky nadané, se speciálními vzdělávacími potřebami, různých úrovní znalostí či preferovaných stylů učení. Plánovaná výuka rovněž dává učiteli možnost reflexe, a to jak z hlediska splnění krátkodobých, tak dlouhodobých cílů.

Vališová a Kovaříková (2021) dále doplňují, že plánování je procesem začlenění vzdělávacího oboru do školy, který začíná analýzou potřeb žáků, následuje samotným plánováním, které by mělo obsahovat formální a neformální kurikulum a je zakončeno hodnocením.

Didaktická analýza učiva

Zormanová (2014) uvádí, že hlavní součástí jakéhokoliv plánování výuky je samotná didaktická analýza učiva, kterou popisuje jako myšlenkovou činnost učitele, pomocí které pronikne do učební látky z pedagogického hlediska, za účelem vypracování tematického plánu a vlastní přípravy výuky. Učitel zde využívá učebnic a kurikulárních dokumentů (rámcové a školní vzdělávací plány). Pomocí nich je učitel schopen provést rozbor vyučovaného tématu a jeho další přetvoření na učivo s výchovnou a vzdělávací hodnotou.

Didaktická analýza je rozdělená na tři typy. Tím prvním je **analýza pojmová**, zabývající-se – jak již z názvu vyplývá – analýzou pojmů týkajících se učiva zprostředkovávaného žákům, které vkládáme do logické struktury a popisujeme vztahy mezi nimi. Součástí učitelovy práce a také tyto pojmy rozřadit na nadřazené, podřazené, hlavní a doplňující. Druhá je **analýza operační**. Ta se zabývá samotnými činnostmi, pomocí kterých si žáci učivo osvojí a dosáhli vzdělávacího cíle. Poslední je **analýza z hlediska mezipředmětových vztahů**, která nám zajišťuje vhodné propojení učiva mezi jednotlivými vyučovanými předměty.

S tímto souhlasí i Skalková (2007), která dále vysvětluje, že je nutné věnovat pozornost nejen věcným znalostem, ale také těm operacionálním a procesuálním. Ty žákům dopomohou v tvoření schopností a dovedností, které přesahují hranice vyučovaného předmětu. Rozvíjíme totiž schopnosti jako jsou analýza, indukce, dedukce, plánování atd.

Vališová a Kovaříková (2021) didaktickou analýzu shrnují jako činnost přemýšlení na straně učitele, zabývající se tématem výuky a tím, co je potřeba žáky naučit a jakým způsobem toho co nejefektivněji dosáhnout. Samotný průběh této analýzy rozdělují do několika bodů. Těmi jsou konkretizace cíle výuky tematického celku, rozbor učiva tematického celku, vymezení základní činnosti studentů, volba metod, forem a materiálních prostředků a formulace učebních otázek a úkolů.

Didaktická transformace

Po didaktické analýze následuje didaktická transformace. Tu Skalková (2007) popisuje jako hledání cesty k uvedení probíraných problému do reálného života. Uplatňujeme zde jak obsah předmětu, tak jeho vztah k žákovi. Je tedy možné říct, že při didaktické transformaci učitel přemýšlí nad tím, jakým způsobem (v jakém pojetí) žákovi informace či dovednosti předat. Musí tedy být schopen učivo transformovat a přeorganizovat tak, aby odpovídalo žákovým předchozím dovednostem, zkušenostem a věku – jedná se tedy o nějakou tvůrčí činnost učitele, při které proniká do učiva hlouběji a přetváří jej pro zjednodušení pochopení probíraného tématu žákem. K tomuto procesu mohou pedagogovi dopomoci učebnice či jiné výukové materiály.

Příprava učitele

Právě k efektivitě v průběhu samotné vyučovací hodiny dopomáhá příprava učitele. Postup tvorby přípravy rozděluje Zormanová (2014) do pěti etap. Tou první je **stanovení cílů výuky**. V této fázi si učitel uvědomuje, co nového si má žák osvojit. Je nutné brát v potaz předchozí výuku a vycházet tak z předchozích vědomostí a dovedností žáků a uvědomit si, zda je nutné s žáky něco zopakovat či vysvětlit znovu. Samotné cíle by měly být stanoveny konkrétně, abychom zajistili kontrolovatelnost jejich splnění na konci hodiny.

Druhou fází je **výběr učebních úloh**, kde na schopností, zkušeností a věku žáků zvolíme vhodné aktivity, pomocí kterých budeme schopni splnit stanovený výukový cíl. Tyto aktivity by měly vést jak k představení nových pojmů a osvojení dovedností, tak k aktivizaci žáků.

Třetí fází je **sestavení časového plánu**. Jak již z názvu vyplývá – v této části učitel vytvoří pořadí zvolených aktivit a uvede, kolik času ve výuce zaberou.

Předposlední fází je již samotné připravení či **vytvoření učebních pomůcek** k aktivitám.

Poslední fáze je věnována **doladění přípravy**, jejímž účelem je její finální uzpůsobení pro získání zpětné vazby či přizpůsobení pro žáky se speciálními potřebami.

S touto strukturou přípravy plánu výuky souhlasí i Vališová a Kovaříková (2021). Doplňují však, že je vhodné promyslet vhodné motivační prostředky, promyslet uspořádání místa výuky (učebny) či najít způsob sledování pokroku žáka ve výuce. Zmiňují však také, že efektivita výuky závisí i na tom, jak je učitel schopen přizpůsobovat tento plán přímo ve vyučovací hodině a reagovat tak na aktuální dění ve třídě. Pedagog se totiž může dopustit hned několika chyb spojených s přípravami. Jsou uvedeny příklady jako snaha dodržovat písemnou přípravu bez jakékoliv průběžné úpravy, špatný časový odhad u aktivit, vynechání některé z fází výuky, nedostatečné didaktické prostředky či očekávání stejných výsledků při používání přípravy na výuku opakovaně.

Tato učitelská příprava by však také měla dodržovat nějaké zásady – konkrétně ty didaktické.

3.1 Didaktické zásady

Zmiňovanou důležitou součástí plánování a přípravy výuky je dodržování takzvaných didaktických zásad. Ty popisuje Kurelová (Kalhous, Obst a kol., 2002) jako obecné požadavky vztahující se na všechny části výuky a určují tak její charakter v souladu s výchovně-vzdělávacími cíli. Tyto zásady mají jak stránku objektivní (objektivní zákonitosti výuky), tak subjektivní, kde záleží přímo na učiteli a jeho zkušenostech. Zormanová (2014) doplňuje, že se jedná o možná doporučení pro pedagogy pro dosáhnutí maximální efektivity výuky. Zmiňuje také fakt, že tyto zásady či principy vznikaly již v historii a jejich forma se vyvíjela.

Kurelová (Kalhous, Obst a kol., 2002) zasazuje didaktické zásady do přehledu.:

1. **Zásada komplexního rozvoje osobnosti žáka** – Tato zásada se zabývá nutností komplexního přístupu k výuce. Je vyžadováno žáka rozvíjet ve všech rovinách. Těmi jsou rovina kognitivní, afektivní a psychomotorická.
2. **Zásada vědeckosti** – Druhá zmiňovaná zásada klade důraz na vyučování vědecky podložených poznatků a učitelovu soustavnou práci při jejich aktualizaci, aby nevyučoval podle zastaralých informací.
3. **Zásada individuálního přístupu k žákům** – Touto zásadou je třeba se řídit zejména z toho důvodu, že každý žák je vlastní osobnost. I když mohou mít žáci ve třídě společné znaky (Zormanová (2014) uvádí například přibližně stejný věk), je nutné brát ohledy na jejich jednotlivé schopnosti, dovednosti, znalosti či zájmy a další odlišnosti.
4. **Zásada spojení teorie s praxí** – Čtvrtá zásada hovoří o propojení teoretických poznatků a dovedností se samotnou praktickou činností žáka a aby si žák mezi teorií a praxí byl schopen utvářet vazby.
5. **Zásada uvědomělosti a aktivity** – Tato zásada se vztahuje na žákův zodpovědný vztah k výuce. Žák se do výuky aktivně zapojuje, osvojuje si znalosti a dovednosti.
6. **Zásada názornosti** – Šestá zásada popisuje nutnost názorné výuky pro lepší pochopení probíraného tématu žáky. Učitel by při výuce měl využít srozumitelných příkladů a pojmů, které žáci už znají. Dle Zormanové (2014) tak žák získává znalosti přímým stykem a více smysly zároveň.

7. **Zásada soustavnosti a přiměřenosti** – Poslední Kurelovou (Kalhous, Obst a kol., 2002) zmiňovanou zásadou je ta týkající se potřeby logického uspořádání výuky tak, aby její posloupnost dávala smysl žákům. Výuka by také měla být přiměřená věku a dosavadním znalostem žáků.

Zormanová (2014) však tento seznam didaktických zásad doplňuje o některé další. Těmi jsou následující zásady.:

1. **Zásada emocionálnosti** – Týká se faktu, že učitel i žáci jsou ovlivňováni emocemi. Z tohoto důvodu je nutné navození pozitivní atmosféry pro zkvalitnění jak výuky, tak vztahu mezi pedagogem a žákem.
2. **Zásada trvalosti** – Tato zásada se týká potřeby pevného a trvalého osvojení-si tématu žáky, a ne pouze mechanickým memorováním. Součástí práce učitele by tedy mělo být i zjišťování, zda žáci téma pochopili za pomoci opakování učiva.
3. **Zásada zpětné vazby** – Třetí a poslední doplňovanou zásadou je zásada zpětné vazby. Pomocí ní pedagog získává náhled na plnění cílů a dokáže tak diagnostikovat porozumění probíraného tématu.

3.2 Učební úlohy

Současně s dodržováním didaktických zásad je vybrání správných učebních úloh. Dle *Pedagogického slovníku* (Průcha, Walterová a Mareš, 2009) je učební úloha *„každá pedagogická situace, která se vytváří proto, aby zajistila u žáků dosažení určitého učebního cíle“* a je *„zaměřena na pět aspektů: obsahový, stimulační (motivační), operační, formativní a regulativní.“* S tímto souhlasí i Zormanová (2014), která je dále popisuje jako pomůcku pro naplňování a ověřování výukových cílů a nástroj pro řízení výuky, s jejichž pomocí žáci získávají či upevňují znalosti a dovednosti. Jsou tedy i prostředkem vlastní aktivizace žáka ve výuce. Můžeme je též popsat jako nějaký požadavek směřující žáka od zadání k cíli.

Podobně o tomto tématu hovoří i Kalhous (Kalhous, Obst a kol., 2002), který popisuje, že aby se žák byl schopen něco efektivně naučit, je třeba, aby s učivem něco dělal sám (aktivně). Vyzdvihuje učební úlohy jako nejdůležitější a nejúčinnější nástroj v arzenálu učitele co se týče aktivizace žáka a ověřování plnění cílů. Podotýká, že při řešení učební úlohy by měl žák získávat nové vědomosti a dovednosti i opakovat a upevňovat ty předchozí. Zároveň by však měly rozvíjet všechny tři jeho osobnostní složky (kognitivní, afektivní a psychomotorickou).

Těmi nejpoužívanějšími učebními úlohami jsou Zormanovou (2014) jmenovány úlohy analytické (analýza jevu), doplňující (doplnění údajů), domácí (samostatná práce doma, nejčastěji kontrolní), problémové (řešení problému), reproduktivní, slovní (verbální), srovnávací (srovnávání dvou (a více) jevů) a úlohy zjišťovací zaměřené na samostatné zjišťování a ověřování faktů žákem.

Kalhous (Kalhous, Obst a kol., 2002) dále vysvětluje roli učebních úloh ve výuce. Těchto rolí je hned několik. Učební úlohy by měly být protkány celým procesem výuky, jsou pouze jednou složkou a neměly by tedy být čistě autonomní, měly by být podávány v systémech (různorodě), učitel může při jejich tvorbě improvizovat, ale musí být předem plánované, musí být stanoveny konkrétní cíle a měly by být součástí učitelova „mistrovství" a odrazem jeho profesionality v oboru.

Maňák a Švec (2003) dále uvádí tři parametry učebních úloh. Těmi jsou parametr stimulační, který ovlivňuje to, jak u žáka vzbudí zájem ke studiu. Učební úloha by tedy měla žáka motivovat aktivizovat a pobídat k tvořivosti. Druhý zmíněný je parametr regulační. Ten se týká řízení činnosti žáka. Poslední uváděný je parametr operační, jež popisuje vlastní operace, kterých musí žák využít, aby úspěšně vyřešil zadanou úlohu. Právě k tomuto nám dopomůže taxonomie učebních úloh.

3.2.1 Taxonomie učebních úloh

K tomu, abychom pro naše žáky vybrali co nejvhodnější soubor úloh, nám pomůže je nějakým způsobem rozřadit. Typy učebních úloh byly seřazeny podle náročnosti D. Tollingerovou v roce 1970, která vycházela z Bloomovy taxonomie kognitivních cílů z 50. let 20. století. Tato původní taxonomie byla dle Skalkové (2007) rozdělena do šesti cílových kategorií osvojení. Kategorie jsou seřazeny následovně.:

1. **Zapamatování** – Žák dokáže doplnit, napsat, definovat, pojmenovat, popsat, … – týká se faktů, termínů, rozpoznání informací.
2. **Pochopení** – Žák dokáže objasnit, dokázat, ilustrovat, jinak formulovat, vysvětlit, … - týká se jednoduché interpretace, pochopení významu.
3. **Aplikace** – Žák dokáže aplikovat, demonstrovat, použít, diskutovat, navrhnout, … - týká se použití abstrakce a zobecňování, použití informací.
4. **Analýza** – Žák dokáže analyzovat, provést rozbor, rozlišit, rozčlenit, specifikovat, … - týká se rozboru komplexní informace na jednotlivé prvky, pochopení vztahů mezi nimi.

5. **Syntéza** – Žák dokáže kombinovat, modifikovat, organizovat, shrnout, vytvořit závěr, … - týká se složení z jednotlivých prvků do jiného (nového) celku.
6. **Hodnotící posouzení** – argumentovat, provést kritiku, ocenit, oponovat, obhájit, … - týká se posouzení z různých hledisek.

Tato taxonomie byla následně zrevidována Andersonem a Krathwohlem (2001) z důvodů vyzdvihnutí původní Bloomovy verze a její autory zmiňované nadčasovosti a dále pro zavedení nových poznatků v oblasti pedagogiky do následující podoby s podkategoriemi:

1. **Pamatovat** – vybavit si znalosti z dlouhodobé paměti.
   1.1 Rozpoznávání – identifikování
   1.2 Vybavování – opětovné získání z paměti
2. **Porozumět** – sestavit si význam se sdělení (grafických, psaných, ústních).
   2.1 Interpretování – vysvětlování, parafrázování, zjednodušování
   2.2 Dávání příkladů – ilustrování, podávání příkladů
   2.3 Klasifikování – kategorizování, zařazování
   2.4 Sumarizování – generalizování, zobecňování
   2.5 Odvozování – vyvozování logických závěrů, předpovídání
   2.6 Srovnávání – rozlišování, přiřazování, hledání shod
   2.7 Vysvětlování – vytváření modelů situací, vysvětlování příčin
3. **Aplikovat –** použít proceduru v dané situaci.
   3.1 Provádění – provádění, uskutečňování, použití procedury v povědomé úloze
   3.2 Realizování – používání znalostí v neznámé úloze
4. **Analyzovat** – rozebrat celek na základní složky a najít mezi nimi vztahy a strukturu celku.
   4.1 Rozlišování – hledaní rozdílů, rozeznávání, vybírání důležitých/nedůležitých částí
   4.2 Uspořádání – strukturování, načrtávání, integrování, určení fungování v rámci struktury
   4.3 Přisuzování – provádění dekonstrukce, určování předsudků, názorů u předloženému materiálu

5. **Hodnotit** – hodnotit na základě kritérií a standardů.
    5.1 Kontrolování – testování, monitorování, koordinování, zjišťování chyb v procesu nebo výsledku práce
    5.2 Kritizování – provádění kritiky, detekování inkonzistencí mezi výstupem a vstupními kritérii
6. **Tvořit** – skládat jednotlivé části tak, aby vytvořili funkční celek nebo reorganizovat jednotlivé části do celku nového.
    6.1 Generování – tvoření hypotéz, vytváření alternativních hypotéz
    6.2 Plánování – navrhování, tvorba postupu pro úspěšné dokončení práce
    6.3 Budování – konstruování, vynalézání

Vraťme se však zpět k taxonomii učebních úloh dle D. Tollingerové z roku 1970 adaptovanou pro české školy. Ta má dle Kalhouse (Kalhous, Obst a kol., 2002) výhodu v tom, že neudává konkrétní seznamy učebních úloh, nýbrž se zabývá jejich obecným tříděním – jednotlivými typy učebních úloh. Tyto typy úloh jsou tak seřazeny podle náročnosti poznávacích operací, které jsou nutné provést žákem pro úspěšné řešení. Znění této taxonomie je následující (Tollingerová, 1986). Popisují ji však i Zormanová (2014) a Kalhous (Kalhous, Obst a kol., 2002).:

1. **Úlohy vyžadující pamětní reprodukci poznatků:**
    1.1 Úlohy na znovupoznání
    1.2 Úlohy na reprodukci jednotlivých faktů, čísel, pojmů apod.
    1.3 Úlohy na reprodukci zákonů, definic, norem, pravidel apod.
    1.4 Úlohy na reprodukci větších textových celků
2. **Úlohy vyžadující jednoduché myšlenkové operace s poznatky:**
    2.1 Úlohy na zjišťování faktů (např. měření, vyhledávání apod.)
    2.2 Úlohy na vyjmenování a popis faktů (výčet, soupis apod.)
    2.3 Úlohy na vyjmenování a popis procesů a způsobů činností
    2.4 Úlohy na rozbor a skladbu (analýza a syntéza)
    2.5 Úlohy na porovnávání a rozlišování (komparace a diskriminace)
    2.6 Úlohy na třídění (kategorizace a klasifikace)
    2.7 Úlohy na zjišťování vztahů mezi fakty (příčina, následek, vliv apod.)
    2.8 Úlohy na abstrakci, konkretizaci a zobecňování
    2.9 Řešení jednoduchých příkladů s neznámými veličinami

3. **Úlohy vyžadující složité myšlenkové operace s poznatky:**
   - 3.1 Úlohy na překlad (translace a transformace)
   - 3.2 Úlohy na výklad (interpretace, vysvětlení a zdůvodnění)
   - 3.3 Úlohy na vyvozování (indukce)
   - 3.4 Úlohy na odvozování (dedukce)
   - 3.5 Úlohy na dokazování a ověřování
   - 3.6 Úlohy na hodnocení
4. **Úlohy vyžadující sdělení poznatků:**
   - 4.1 Úlohy na vypracování přehledu, výtahu, obsahu apod.
   - 4.2 Úlohy na vypracování zprávy, pojednání, referátu apod.
   - 4.3 Samostatné písemné práce, výkresy, projekty apod.
5. **Úlohy vyžadující tvořivé myšlení:**
   - 5.1 Úlohy na praktickou aplikaci (řešení praktických situací)
   - 5.2 Řešení problémových situací
   - 5.3 Kladení otázek a formulace úloh
   - 5.4 Úlohy na objevování na základě vlastního pozorování
   - 5.5 Úlohy na objevování na základě vlastních úvah

Posouzení souboru učebních úloh

Pomocí této taxonomie můžeme dle Kalhouse (Kalhous, Obst a kol., 2002) posoudit celý soubor učebních úloh, což je vhodné pro plánování vyučovací hodiny. Pro tuto činnost bychom měli dle autora stanovit **poznávací náročnost** jednotlivých učebních úloh. Toho dosáhneme roztřízením jednotlivých zvolených úloh do podkategorií podle zmiňované taxonomie pomocí jejich akčních sloves. Příkladem zde můžou být akční slovesa zdůvodněte (3.2), vyjmenujte (2.2) či vyhledejte a následně vypracujte (4.2).

Následně bychom při posuzování rozhodli o **pestrosti** souboru úloh. Tu určíme pohledem na soubor kategorizovaných úloh – čím méně se nám čísla podkategorií opakují, tím lépe. Musíme však samozřejmě dbát na přiměřenost úloh u konkrétní třídy (např. nezadávat příliš obtížné úlohy). Proto pokračujeme zjištěním **operační (poznávací) hodnoty** (obtížnosti) souboru úloh zjištěním toho, ve které kategorii nám úlohy převládají.

Nakonec porovnáváme poznávací hodnotu se zvoleným výukovým cílem. Toto nám udá **didaktickou hodnotu** našeho souboru úloh – ověříme si tak, zda jsme pomocí souboru úloh splnit výukový cíl hodiny (Kalhous, Obst a kol., 2002).

S informacemi o nebezpečích internetu, umístění problematiky ve školním prostředí a plánováním výuky již můžeme začít sestavovat metodické návrhy.

4 Metodické návrhy

Jak již z názvu práce vyplývá, praktická část se zabývá vlastní tvorbou metodických návrhů týkající se bezpečnosti na internetu v rámci informatických předmětů na druhém stupni základních škol. Tyto metodické návrhy jsou vypracovány v návaznosti na poznatky o internetových nebezpečích z teoretické části této práce a vycházejí z úpravy koncepce „nové informatiky“ RVP ZV z roku 2021 a klíčových kompetencí (MŠMT, 2021). Pro tvorbu těchto materiálů je dále brána v potaz prevence nežádoucích rizikových chování dětí a mládeže ve spojení s prostředím internetu, která je uváděna v národní strategii (MŠMT, 2019).

Z větší části se tyto metodické listy budou zabývat problematikou ověřování informací a hazardem s osobními informacemi a jejich sdílením, které jsou společné pro velkou část zmíněných nebezpečí na internetu (dezinformace, phishing, podvody – ověřování informací; grooming – ověřování informací o lidech; stalking, sexting – hazard s osobními informacemi a jejich sdílením). Budou ovšem zahrnovat i jiná témata jako je například hazardní hraní na internetu, vyzkoušení-si dotazníku týkajícího-se závislosti na internetu či pojmy týkající se ochrany vlastních zařízení.

Nutné je však podotknout, že tyto metodické návrhy jsou vytvořeny bez konkrétní cílové skupiny žáků, a je tedy na samotném pedagogovi, aby rozhodl, pro kterou věkovou skupinu žáků/ročník jsou vhodné – popřípadě jakým způsobem návrh modifikovat tak, aby mu co nejlépe zapadal do výuky. Případné pracovní listy týkající se jednotlivých témat jsou umístěny v přílohách této práce.

4.1 Návrh 1 – Dezinformace 1

Tento návrh se týká dezinformací a konkrétně HOAXů, lží a dalších s dezinformacemi spojených pojmů. Cílem tohoto cvičení je rozeznat lživou informaci od pravdy. Žáci zde nejprve spolupracují s učitelem pro nastínění tématiky hoaxů, vysvětlení jejich funkce a představení několika slavných. Následně žáci pracují ve dvojicích či skupinách s pracovními listy, kde si pomocí jednoho vyzkouší ověřování informací sami. Druhý list slouží pro zopakování pojmů.

Tematický celek a učivo (RVP ZV):

Data, informace a modelování – data, informace; Digitální technologie – bezpečnost

Cíl práce a metodika:

Cílem práce s tímto metodickým návrhem je představení problematiky dezinformací prostřednictvím HOAXů a dalších internetových lží. V první části vyučování se zabýváme nastíněním zmíněné problematiky společně se třídou prostřednictvím webové aplikace určené pro rozeznávání pravdy od lži. Následně žáci pracují ve dvojicích s pracovními listy, na kterých si vyzkouší dohledávání informací z internetu. Po vyplnění pracovního listu se navracíme opět do diskuse s učitelem. Druhý pracovní list může být použit při tvoření zápisu či pro zopakování tématu.

Organizační forma:

Hromadná (frontální) výuka

Metody výuky:

Práce s textem (vyhledávání informací), diskuse (diskuse o nalezených informacích), skupinová a kooperativní výuka (práce ve dvojicích) a vysvětlování (uvedení do tématu).

Mezipředmětové vztahy:

Občanská výchova, mediální výchova

Pomůcky:

Vybavená počítačová učebna s projektorem

Webová aplikace - https://www.e-bezpeci.cz/hoaxy/

Pracovní listy (viz. příloha 1, 2)

Otázky a úlohy:

Co je to HOAX?

Znáte nějaké příklady HOAXů?

Znáte jiné lživé informace podobné těm z pracovního listu?

Průběh výuky:

1. Představení výukového cíle žákům.
2. Žáci společně s učitelem prochází webovou aplikaci a snaží se poznávat lživé informace od pravdivých. Webová aplikace nás sama opraví a uvede vysvětlení zobrazovaného HOAXu.

3. Rozdělení třídy do dvojic a rozdání pracovních listů.
4. Žáci postupně reagují na uvedené dezinformace v pracovním listu a dohledávají informace pravdivé. V případě použití pracovního listu 2 doplňují žáci vlastní poznatky z hodiny.
5. Následuje diskuse jednotlivých dvojic s učitelem o nalezených informacích.
6. Výuka je zakončena sebereflexí žáků.

4.2 Návrh 2 – Dezinformace 2

Tento návrh se týká dezinformací a konkrétně fenoménu „fake news“ a propagandy. Cílem tohoto cvičení je rozeznat lživou informaci od pravdy. Žáci zde nejprve spolupracují s učitelem pro nastínění (případně zopakování) tématiky „fake news“ a propagandy. Následně žáci pracují ve dvojicích či skupinách na tvorbě vlastní falešné zprávy či propagandy.

Tematický celek a učivo (RVP ZV):

Data, informace a modelování – data, informace; Digitální technologie – bezpečnost

Cíl práce a metodika:

Cílem práce s tímto metodickým návrhem je představení (či zopakování) problematiky dezinformací prostřednictvím „fake news“ a jinak nebezpečných lží ve formě propagandy. V první části vyučování se zabýváme nastíněním zmíněné problematiky společně se třídou. Následně žáci pracují ve dvojicích (malých skupinách) s počítači, na kterých si vyzkouší tvorbu vlastní falešné zprávy potažmo propagandy. Po jejím vytvoření ji žáci formou jednoduché inscenace odprezentují před třídou.

Pro tvorbu lživých zpráv je možno využít počítačových aplikací jako jsou například MS Word, MS PowerPoint či jiných podobných. Témata práce si skupiny žáků mohou po konzultaci s učitelem vybrat sami – popřípadě přiděluje sám učitel (náměty na témata jsou uvedeny v příloze 3).

Organizační forma:

Hromadná (frontální) výuka

Metody výuky:

Diskuse (diskuse o tématu a následně zprávách jednotlivých skupin), skupinová a kooperativní výuka (práce ve dvojicích či malých skupinách), inscenační metoda (žáci inscenují (hrají) lživé zpravodaje) a vysvětlování (uvedení do tématu).

Mezipředmětové vztahy:

Občanská výchova, mediální výchova

Pomůcky:

Vybavená počítačová učebna s projektorem

„Kancelářské“ aplikace

Otázky a úlohy:

Co jsou to fake news?

V jakých případech mluvíme o propagandě?

Jaké falešné zprávy jste slyšeli?

Průběh výuky:

1. Představení výukového cíle žákům.
2. Učitel vysvětluje žákům problematiku.
3. Krátká diskuse týkající se problematiky.
4. Rozdělení do skupin a zadání práce v nich.
5. Žáci pracují na počítačích, kde společnými silami vypracovávají své zadané téma.
6. Žáci představují své výtvory pomocí jednoduché inscenace – zpravodajové, náboráři atd.
7. Následuje diskuse o jednotlivých představeních. Diskuse může být například o tom, která zpráva byla nejvíce přesvědčivá.
8. Výuka je zakončena sebereflexí žáků.

4.3 Návrh 3 – Grooming a podobné nebezpečné interakce

Tento návrh se týká nebezpečí groomingu a možných nebezpečných interakcí na internetu. Cílem tohoto cvičení je rozeznat lži groomera a podtrhnout nesrovnalosti na uživatelském profilu. Žáci zde nejprve spolupracují s učitelem pro nastínění tématiky groomingu. Následně žáci pracují v pracovním listu. Téma částečně navazuje na tématiku dezinformací – nyní se však žáci zaměří na ověření informací o člověku.

Tematický celek a učivo (RVP ZV):

Data, informace a modelování – data, informace; Digitální technologie – bezpečnost

Cíl práce a metodika:

Cílem práce s tímto metodickým návrhem je představení problematiky a nebezpečí groomingu. V první části vyučování se zabýváme nastíněním zmíněné problematiky společně s žáky – varováním před potenciálními zločinci a jak postupovat při jeho odhalování. Následně žáci pracují samostatně v pracovních listech týkajících se postupu odhalování falešného profilu a potenciálně nebezpečných otázek.

Organizační forma:

Hromadná (frontální) výuka

Metody výuky:

Diskuse (diskuse o tématu v rámci pracovních listů), samostatná práce (práce v pracovním listě) a vysvětlování (uvedení do tématu).

Mezipředmětové vztahy:

Občanská výchova

Pomůcky:

Pracovní list (viz. příloha 4)

Otázky a úlohy:

Co je to grooming?

Proč „groomeři“ napodobují chování někoho jiného?

Můžeme ověřit identitu někoho, koho neznáme?

Průběh výuky:

1. Představení výukového cíle žákům.
2. Učitel vysvětluje problematiku žákům, varuje před potenciálním nebezpečím a poukazuje na to, jak se mu můžou vyhnout.
3. Rozdání pracovních listů.
4. Žáci postupně reagují na uvedené otázky v pracovním listu a vyplňují je podle informací, co se dozvěděli od učitele.
5. Následuje společná diskuse s učitelem o pro zopakování učiva.
6. Výuka je zakončena sebereflexí žáků.

4.4 Návrh 4 – Digitální stopa

Tento návrh se týká problematiky digitální stopy a toho, co od nás aplikace odesílají dál. Cílem tohoto cvičení je uvědomit si, jaká povolení dáváme aplikacím například v chytrých telefonech či osobních počítačích. Žáci zde nejprve spolupracují s učitelem pro nastínění tématiky digitální stopy a jejích součástí. Následně žáci pracují v pracovním listu.

Tematický celek a učivo (RVP ZV):

Digitální technologie – bezpečnost, digitální identita

Cíl práce a metodika:

Cílem práce s tímto metodickým návrhem je představení tématu digitální stopy a součástí k ní náležící (IP a MAC adresa, cookies, lokační data a metadata). V první části vyučování se zabýváme nastíněním zmíněné problematiky společně s žáky. Následně žáci pracují ve dvojicích v pracovních listech týkajících se vyhledávání ve vlastních mobilních zařízeních (mobilech, tabletech či laptopech).

Organizační forma:

Hromadná (frontální) výuka

Metody výuky:

Diskuse (diskuse o tématu v rámci pracovních listů), skupinová a kooperativní výuka (práce ve dvojicích, práce v pracovních listech) a vysvětlování (uvedení do tématu).

Mezipředmětové vztahy:

Občanská výchova

Pomůcky:

Pracovní list (viz. příloha 5)

Žákovská zařízení

Otázky a úlohy:

Co je to MAC adresa?

Co je to IP adresa?

Můžeme ze souboru fotografie vyčíst i jiná data než samotný obraz?

Co (někdy) musíme aplikacím v chytrých telefonech povolit?

Průběh výuky:

1. Představení výukového cíle žákům.
2. Učitel vysvětluje problematiku žákům.
3. Rozdání pracovních listů.
4. Žáci postupně reagují na uvedené otázky v pracovním listu a vyplňují je podle informací, co se dozví z vlastních mobilních zařízení.
5. Následuje společná diskuse s učitelem o výsledcích vlastního bádání.
6. Výuka je zakončena sebereflexí žáků.

4.5 Návrh 5 – Online gambling a internetová závislost

Tento návrh se týká problematiky online hazardního hráčství a (nejen) s ním spojenou internetovou závislostí. Cílem tohoto cvičení je najít příklady online gamblingu, matematicky si vyzkoušet pravděpodobnosti výhry a případně vyzkoušet svoji vlastní internetovou závislost. Žáci zde nejprve spolupracují s učitelem pro nastínění zmíněné a následně pracují v pracovním listu.

Tematický celek a učivo (RVP ZV):

Data, informace a modelování – data, informace; Digitální technologie – bezpečnost

Cíl práce a metodika:

Cílem práce s tímto metodickým návrhem je představení tématu internetové závislosti a problematiky online gamblingu, jemuž mohou být žáci vystaveni v rámci některých videoher. V první části vyučování se zabýváme nastíněním zmíněné problematiky společně s žáky. Následně žáci pracují ve dvojicích či skupinkách v pracovních listech týkajících se vyhledávání informací na internetu a následné práce s nimi.

Pro zjednodušení práce při výpočtech a ukládání dat si můžeme dopomoci například softwarem MS Excel případně jiným tabulkovým procesorem.

Organizační forma:

Hromadná (frontální) výuka

Metody výuky:

Diskuse (diskuse o tématu po vypracování pracovních listů), skupinová a kooperativní výuka (práce ve dvojicích či skupinkách, práce v pracovních listech/na počítačích) a vysvětlování (uvedení do tématu).

Mezipředmětové vztahy:

Občanská výchova, matematika

Pomůcky:

Pracovní list (viz. příloha 6)

Vybavená počítačová učebna

Kalkulačka či počítačový software schopný výpočtů

Pro otestování internetové závislosti webovou stránku

https://poradna.adiktologie.cz/otestujte-se/?poll_id=5

Otázky a úlohy:

Kde se můžeme setkat s gamblingem na počítačích?

Slyšeli jste pojem „lootbox“?

Průběh výuky:

1. Představení výukového cíle žákům.
2. Učitel vysvětluje problematiku žákům.
3. Rozdání pracovních listů.
4. Žáci postupně reagují na uvedené otázky v pracovním listu a vyplňují je (či případnou tabulku v tabulkovém procesoru) pomocí samostatně vyhledaných informací z internetu a vlastních výpočtů.
5. Následuje společná diskuse s učitelem o výsledcích vlastního bádání.
6. Možnost vyzkoušení svojí internetové závislosti na přiloženém webu.
7. Výuka je zakončena sebereflexí žáků.

4.6 Návrh 6 – Internetové podvody

Tento návrh se týká internetových podvodů a toho, jak je rozeznat. Cílem tohoto cvičení je rozeznat falešné oznámení, zprávu či web od reálné(ho). Žáci zde nejprve spolupracují s učitelem pro nastínění tématiky internetových podvodů a jejich druhy (phishing, falešné inzeráty, spamové emaily atd.). Následně žáci pracují samostatně či dvojicích s pracovním listem, ve kterém odpovídají na dané otázky k tématu.

Tematický celek a učivo (RVP ZV):

Digitální technologie – bezpečnost

Cíl práce a metodika:

Cílem práce s tímto metodickým návrhem je představení problematiky internetových podvodů. V první část zabýváme nastíněním zmíněné problematiky společně s žáky prostřednictvím reálných zpráv o těchto typech podvodů. Následně žáci pracují ve dvojicích (popřípadě samostatně) s pracovními listy, ve kterých zodpovídají na otázky a pracují s textem. Po vyplnění pracovního listu se navracíme opět do diskuse s učitelem.

Organizační forma:

Hromadná (frontální) výuka

Metody výuky:

Diskuse (diskuse o tématu), samostatná práce či skupinová a kooperativní výuka (práce ve dvojicích či samostatně, práce v pracovních listech) a vysvětlování (uvedení do tématu).

Mezipředmětové vztahy:

Občanská výchova

Pomůcky:

Pracovní list (viz. příloha 7)

Vybavená počítačová učebna s projektorem

Otázky a úlohy:

Jak si ověříme, zda je email pravý? (od banky atd.)

Co je to „phishing“? Proč se tak nazývá?

Průběh výuky:

1. Představení výukového cíle žákům.
2. Učitel vysvětluje problematiku žákům.
3. Rozdání pracovních listů.
4. Žáci postupně reagují na uvedené otázky v pracovním listu a vyplňují je. Součástí je i jednoduchá práce s textem.
5. Následuje společná diskuse s učitelem o výsledcích pracovních listů.
6. Výuka je zakončena sebereflexí žáků.

4.7 Návrh 7 – Malware

Tento návrh se týká problematiky různých druhů malwaru (virus, červ, adware, keylogger atd.). Cílem tohoto cvičení je pochopit funkci jednotlivých zmiňovaných malwarů a jak se proti nim můžeme bránit. Žáci zde nejprve spolupracují s učitelem pro vysvětlení tématiky škodlivých softwarů a následně pracují v pracovním listu.

Tematický celek a učivo (RVP ZV):

Digitální technologie – bezpečnost

Cíl práce a metodika:

Cílem práce s tímto metodickým návrhem je představení tématu malwaru a jak se proti jeho různým typům bránit. V první části vyučování se zabýváme nastíněním zmíněné problematiky společně s žáky, představíme jednotlivé typy malwarů a zmíníme možné obrany proti nim. Následně žáci pracují ve dvojicích v pracovních listech s možným použitím internetu jako zdroje informací.

Organizační forma:

Hromadná (frontální) výuka

Metody výuky:

Diskuse (diskuse o vypracovaných pracovních listech), skupinová a kooperativní výuka (práce ve dvojicích, práce v pracovních listech, vyhledávání na internetu) a vysvětlování (uvedení do tématu).

Mezipředmětové vztahy:

Občanská výchova

Pomůcky:

Pracovní list (viz. příloha 8)

Vybavená počítačová učebna

Otázky a úlohy:

Co je to malware?

Může se malware šířit sám?

Kde na malware můžeme narazit?

Čím se proti malwaru můžeme bránit?

Průběh výuky:

1. Představení výukového cíle žákům.
2. Učitel vysvětluje problematiku žákům.
3. Rozdání pracovních listů.
4. Žáci postupně odpovídají na uvedené otázky v pracovním listu a vyplňují je podle informací, co se dozvěděli od učitele (případně internetu).
5. Následuje společná diskuse s učitelem o výsledcích vlastního bádání.
6. Výuka je zakončena sebereflexí žáků.

4.8 Návrh 8 – Kyberšikana a sociální sítě

Tento návrh se týká kyberšikany, toho, jak ji rozeznat od standartní šikany a následně v jakém prostředí ji najdeme (sociální sítě). Cílem tohoto cvičení je pochopit jak rozdíly mezi šikanou a kyberšikanou, tak seznámit se s nejznámějšími sociálními sítěmi. Žáci zde nejprve spolupracují s učitelem pro nastínění tématiky a následně pracují ve dvojicích s pracovním listem, ve kterém vyplňují zadané úkoly.

Tematický celek a učivo (RVP ZV):

Digitální technologie – bezpečnost, digitální identita

Cíl práce a metodika:

Cílem práce s tímto metodickým návrhem je představení problematiky kyberšikany a sociálních sítí (nejen jako prostor, kde se tento typ šikany projevuje). V prvopočátku se zabýváme nastíněním zmíněné problematiky společně s žáky, představení sociálních sítí může probíhat s pomocí projektoru. Následně žáci pracují ve dvojicích s pracovními listy, ve kterých zodpovídají na otázky a plní úkoly. Po vyplnění pracovního listu se navracíme opět do diskuse s učitelem.

Organizační forma:

Hromadná (frontální) výuka

Metody výuky:

Diskuse (diskuse o tématu), skupinová a kooperativní výuka (práce ve dvojicích, práce v pracovních listech) a vysvětlování (uvedení do tématu).

Mezipředmětové vztahy:

Občanská výchova

Pomůcky:

Pracovní list (viz. příloha 9)

Vybavená počítačová učebna s projektorem

Otázky a úlohy:

Jaký je rozdíl mezi „normální“ šikanou a kyberšikanou?

Co je to sociální síť?

Proč se na sociálních sítích může kyberšikana vyskytovat?

Jaké sociální sítě používáš?

Průběh výuky:

1. Představení výukového cíle žákům.
2. Učitel vysvětluje problematiku žákům.
3. Rozdání pracovních listů.
4. Žáci postupně vyplňují jednotlivé úkoly v pracovním listu a vyplňují je. Porovnávají rozdíly mezi šikanou a kyberšikanou a dále popisují své zkušenosti se sociálními sítěmi.
5. Následuje společná diskuse s učitelem o výsledcích pracovních listů.
6. Výuka je zakončena sebereflexí žáků.

4.9 Návrh 9 – Zabezpečení, zálohování a hesla

Tento návrh se týká metod zabezpečení počítače (antivirus, svědomité stahování souborů atd.), zálohování a metod, kterými je možno ho docílit a v neposlední řadě jsou zmíněna hesla a jejich tvorba. Cílem tohoto cvičení je seznámit žáky s těmito pojmy a docílit toho, aby tyto znalosti aktivně používali. Žáci zde nejprve spolupracují s učitelem pro nastínění tématiky a následně pracují samostatně i či ve dvojicích s pracovním listem, ve kterém vyplňují zadané úkoly.

Tematický celek a učivo (RVP ZV):

Digitální technologie – bezpečnost

Cíl práce a metodika:

Cílem práce s tímto metodickým návrhem je představení problematiky zabezpečení účtů a souborů v počítači (nejen) pomocí hesel a zálohování vlastních dat na externí úložiště. V první části se zabýváme nastíněním zmíněné problematiky společně s žáky. Následně žáci pracují ve dvojicích (popřípadě samostatně) s pracovními listy, na kterém vyplní křížovku týkající se nově naučených pojmů. Po vyplnění pracovního listu se vracíme opět do diskuse s učitelem.

Pokud má škola možnost cloudového úložiště pro žáky, je také možné, aby si ukládání na vzdálené úložiště vyzkoušeli sami – například v rámci uložení zmíněné křížovky či jiného úkolu zadaného učitelem.

Organizační forma:

Hromadná (frontální) výuka

Metody výuky:

Diskuse (diskuse o tématu), samostatná práce či skupinová a kooperativní výuka (práce ve dvojicích, práce v pracovních listech) a vysvětlování (uvedení do tématu).

Mezipředmětové vztahy:

Občanská výchova

Pomůcky:

Pracovní list (viz. příloha 10)

Vybavená počítačová učebna s projektorem

Otázky a úlohy:

Co je to cloud?

Proč zálohujeme data?

Jakým způsobem vytvoříme silné heslo?

Co je to antivirus a proti čemu nás chrání?

Průběh výuky:

1. Představení výukového cíle žákům.
2. Učitel vysvětluje problematiku žákům.
3. Rozdání pracovních listů.
4. Žáci postupně vyplňují křížovku v pracovním listu. Ta se týká nových pojmů zmíněných ve vyučování.
5. *Samostatné vyzkoušení-si zálohování.*
6. Následuje společná diskuse s učitelem o výsledcích pracovních listů.
7. Výuka je zakončena sebereflexí žáků.

4.10 Návrh 10 – Nebezpečí sextingu

Tento návrh se týká, jak již z názvu vyplývá nebezpečí sextingu. Cílem tohoto cvičení je seznámit žáky s tímto pojmem, riziky zasílání fotografií, návazností na grooming, rolemi respektu a souhlasu, peer pressure (tlaku vrstevníků) či právní následky. Žáci zde nejprve spolupracují s učitelem pro nastínění tématiky a následně pracují samostatně i či ve dvojicích s pracovním listem, ve kterém vyplňují zadané úkoly.

Tematický celek a učivo (RVP ZV):

Digitální technologie – bezpečnost, digitální identita

Cíl práce a metodika:

Cílem práce s tímto metodickým návrhem je představení problematiky sextingu a jeho nebezpečí, které může být spojené s groomingem či vydírání (sextortion). Žáci by měli být seznámeni s právními následky, možnostmi ochrany (ověření-si uživatele, jak zacházet s vlastními fotografiemi atd.) a s pravidly souhlasu a respektu potřebného od všech účastnících-se stran. V první části se zabýváme nastíněním zmíněné problematiky společně s žáky. Následně žáci pracují ve dvojicích či samostatně s pracovními listy, které se týkají zopakování pojmů a bezpečného chování. Po vyplnění pracovního listu se vracíme opět do diskuse s učitelem.

Organizační forma:

Hromadná (frontální) výuka

Metody výuky:

Diskuse (diskuse o tématu), samostatná práce či skupinová a kooperativní výuka (práce ve dvojicích, práce v pracovních listech) a vysvětlování (uvedení do tématu).

Mezipředmětové vztahy:

Občanská výchova

Pomůcky:

Pracovní list (viz. příloha 11)

Otázky a úlohy:

Co je to sexting?

Jaká jsou jeho nebezpečí?

Jak si ověříme identitu člověka na internetu?

Průběh výuky:

1. Představení výukového cíle žákům.
2. Učitel vysvětluje problematiku žákům.
3. Rozdání pracovních listů.
4. Žáci postupně vyplňují úkoly v pracovním listu.
5. Následuje společná diskuse s učitelem o výsledcích pracovních listů.
6. Výuka je zakončena sebereflexí žáků.

5 Ověření a získání zpětné vazby

Důležitou součástí tvorby metodických návrhů je jejich praktické ověření. Můžeme na něj pohlížet jako na plnění již zmíněné zásady zpětné vazby, kterou uvádí Zormanová (2014). Pomocí této didaktické zásady získává učitel náhled na plnění výukových cílů a na porozumění probíraného tématu žáky.

V této části tedy konkrétně zjistíme, zda je zvolený návrh a jeho příslušný pracovní list vhodný k použití ve výuce a zda s jeho využitím došlo ke zlepšení povědomí o probíraném tématu. Následně od žáků zjistíme, zda byla forma pracovního listu zajímavá, líbivá či co by na něm změnili nebo poupravili.

Z důvodu našich možností bylo toto ověření provedeno v rámci **neformálního vzdělávání** – tudíž v rámci mimoškolní vzdělávací aktivity volnočasové neziskové organizace. Pro účely ověření byl po domluvě s organizátory zvolen návrh 1 týkající se problematiky dezinformací s pracovním listem 2 (příloha 2). Tento návrh byl společně se zmíněným listem zvolen z důvodu zájmu organizátora a dostupných časových prostředků.

Profil vyučované skupiny

Jak již bylo zmíněno, ověření bylo provedeno v rámci mimoškolní aktivity (konkrétně skautský oddíl). Dotazovaní žáci byli ve věku 11 – 15 let (2. stupeň ZŠ), navštěvující různé základní školy v okolí měst Prostějov a Plumlov. Celkový počet respondentů čítal 19 žáků – z toho 6 dívek a 13 chlapců.

Úskalí ověřování

U tohoto druhu ověřování je nutné zdůraznit několik potenciálních úskalí. Jako první dva můžeme zmínit relativně malý počet respondentů a pouze jeden v praxi vyzkoušený návrh To je zapříčiněno formou ověřování, možnostmi výzkumníka a oslovené organizace. Dalším by mohl být lišící-se věk žáků v dotazované skupině a fakt, že ne všichni žáci jsou na stejné vědomostní úrovni.

Ověření však bylo provedeno i s těmito ne příliš ideálními limitacemi. Domníváme se totiž, že tyto návrhy mohou být užitečné, jak pro vyučující při sestavování plánu vyučovacích hodiny, tak jako základ pro další potenciální výzkum či ověřování.

5.1 Průběh ověřování

Ověření metodického návrhu týkajícího se problematiky dezinformací a pojmů s nimi spojených probíhal ve třech fázích, které byly od sebe vzdáleny přesně týden – jinak řečeno – tři po sobě jdoucí týdny v období květen až červen roku 2023.

První fáze byla věnována zjištění dosavadních znalostí žáků. Pro tuto fázi bylo využito krátkého nestandardizovaného didaktického testu. Tento jinak řečeno učitelský či neformální test označuje Chráska (2016) jako test, který si vyučující připravuje pro svoji vlastní potřebu (například zjištění a vyzkoušení znalostí u dané skupiny žáků) a nebyl ověřen na větším vzorku žáků. Nebyly zde tedy provedeny všechny kroky důležité pro tvorbu testu standardizovaného (důkladné ověření, vytvoření testové normy pro hodnocení či testové příručky).

V našem případě se jednalo o krátký test zaměřený na znalosti z probírané oblasti. Tento test (příloha 12) byl sestaven z otevřených úloh se stručnou odpovědí a úloh s výběrem odpovědí – konkrétně úloh s jednou správnou odpovědí. Otázky a úlohy byly sestaveny tak, aby reflektovaly poznatky z teoretické části této práce.

Druhá fáze se týkala výuky tématu s použitím zvoleného návrhu a pracovního listu přímo s žáky ve skupině v rámci časové dotace poskytnuté oslovenou organizací.

Poslední fáze byla věnována testování pokroku žáků s použitím stejného testu jako ve fázi první. Stejný test byl využit z důvodu možného porovnání dvou stavů znalostí žáků.

Následně si detailně rozebereme jednotlivé fáze ověřování a jejich výsledky.

5.1.1 Fáze 1 – Test

Jak již bylo zmíněno, v první fázi bylo využito krátkého testu na 10 – 15 minut. Tento test byl složen z osmi otázek/úloh z nichž 6 bylo otevřených úloh se stručnou odpovědí a 2 „kroužkovací“ s výběrem jedné správné odpovědi. Tento test byl zcela anonymní a po odevzdání byl zhodnocen. Za správnou odpověď byly přiřazeny 2 body, pro částečně správnou odpověď byl přiřazen 1 bod a za špatnou odpověď 0 bodů. Výsledky jednotlivých otázek/úkolů a podoba testu vypadaly následovně:

Co jsou to dezinformace?

Správná odpověď: Úmyslně lživé a klamavé informace.

Na tuto otázku odpověděli správně 4 žáci, částečně správně 11 žáků a nesprávně 4 žáci. Mezi částečně správné odpovědi se řadily: *lživé informace, lživé zprávy, nepravdivé informace a deformované informace*. Jako nesprávné byly označeny nevyplněné odpovědi.

Kde se s dezinformacemi můžeme setkat? (uveď alespoň 3 možnosti)

Správná odpověď: *Výpis 3 zdrojů dezinformací.* Například televize, média, internet, rádio atd.

Na tuto otázku odpovědělo správně 10 žáků, částečně správně 4 žáci a nesprávně 5 žáků. Nejčastěji se objevovaly odpovědi: *televize, internet, Facebook, sociální sítě, rádio a noviny.* Ke snížení počtu bodů došlo v případě nesplnění požadavku 3 možností. Nesprávné odpovědi byly opět nevyplněné.

Co je cílem HOAXů?

Správná odpověď: Šířit paniku.

U téhle otázky bylo 5 odpovědí správných, 6 částečně správných a 8 špatných. Mezi částečně správné odpovědi byly zařazeny: *aby je vidělo co nejvíce lidí, manipulace s lidmi či šířit se internetem.* Odpovědi ohodnocené 0 body byly nevyplněné.

Uveď příklad nějakého HOAXu.:

Správná odpověď: *Příklad jakéhokoliv známého HOAXu.* Například konec světa v roce 2012.

U tohoto úkolu si 8 žáků vybavilo nějaký HOAX a získali tak 2 body. Zbytek žáků (11) položku nevyplnil. Objevovaly se příklady: *plochá země, HOAXy týkající se blokování účtů, překrucování slov prezidenta, HOAXy týkající-se koronaviru* či například *exploze břicha po zapití bonbónů Mentos colou.*

Jak nazýváme informace, které mají za cíl někoho poškodit?

Správná odpověď: c) malinformace

Zde se jednalo o výběr z šesti možností. Správně odpověděli 4 žáci, nesprávně 15 žáků. Bodování u této odpovědi bylo pro jednoduchost nastaveno na 2 body za správnou odpověď a 0 bodů za odpověď špatnou.

Jak nazýváme neověřené informace, které někdo (neúmyslně) šíří jako pravdivé?

Správná odpověď: b) misinformace

Podobně jako u předchozí otázky se jednalo o výběr mezi šesti možnostmi se stejným hodnocením. Zde však byly pouze 2 správné odpovědi. Zbylých 17 bylo nesprávných.

Co v překladu znamená anglický termín „FAKE NEWS“?

Správná odpověď: Falešné zprávy.

Na tuto otázku odpovědělo správně 18 žáků. Jeden žák nevyplnil odpověď.

S čím v současnosti nejčastěji spojujeme termín PROPAGANDA?

Správná odpověď: Válka *nebo* politický nátlak/přesvědčování.

Na tuto otázky odpovědělo 8 žáků správně, 5 částečně správně a 6 žáků nesprávně. Mezi částečně správné odpovědi byly řazeny odpovědi *komunismus, sovětský svaz* či *Rusáci.* Mezi nesprávné odpovědi byly zařazeny prázdné kolonky a odpověď *LGBT propagace.*

5.1.2 Fáze 2 – Výuka

Týden po předchozí fázi přišla na řadu fáze výuky. Pro tuto fázi nám byla umožněna stejná časová dotace jako pro vyučovací hodinu – tedy 45 minut. Metodický návrh 1 byl zpracován do následující podoby podle potřeb místa výuky.:

Věk žáků: 11 – 15 let (6. – 9. ročník ZŠ)

Tematický celek: Internetová bezpečnost

Téma výuky: Dezinformace a jiné internetové lži

Cíle výuky:

1. Žák dokáže vysvětlit pojmy dezinformace, HOAX, Fake News, malinformace, misinformace a propaganda.
2. Žák dokáže uvést příklady internetových nepravd.
3. Žák dokáže popsat proces ověření informace.

Organizační forma: Hromadná (frontální) výuka

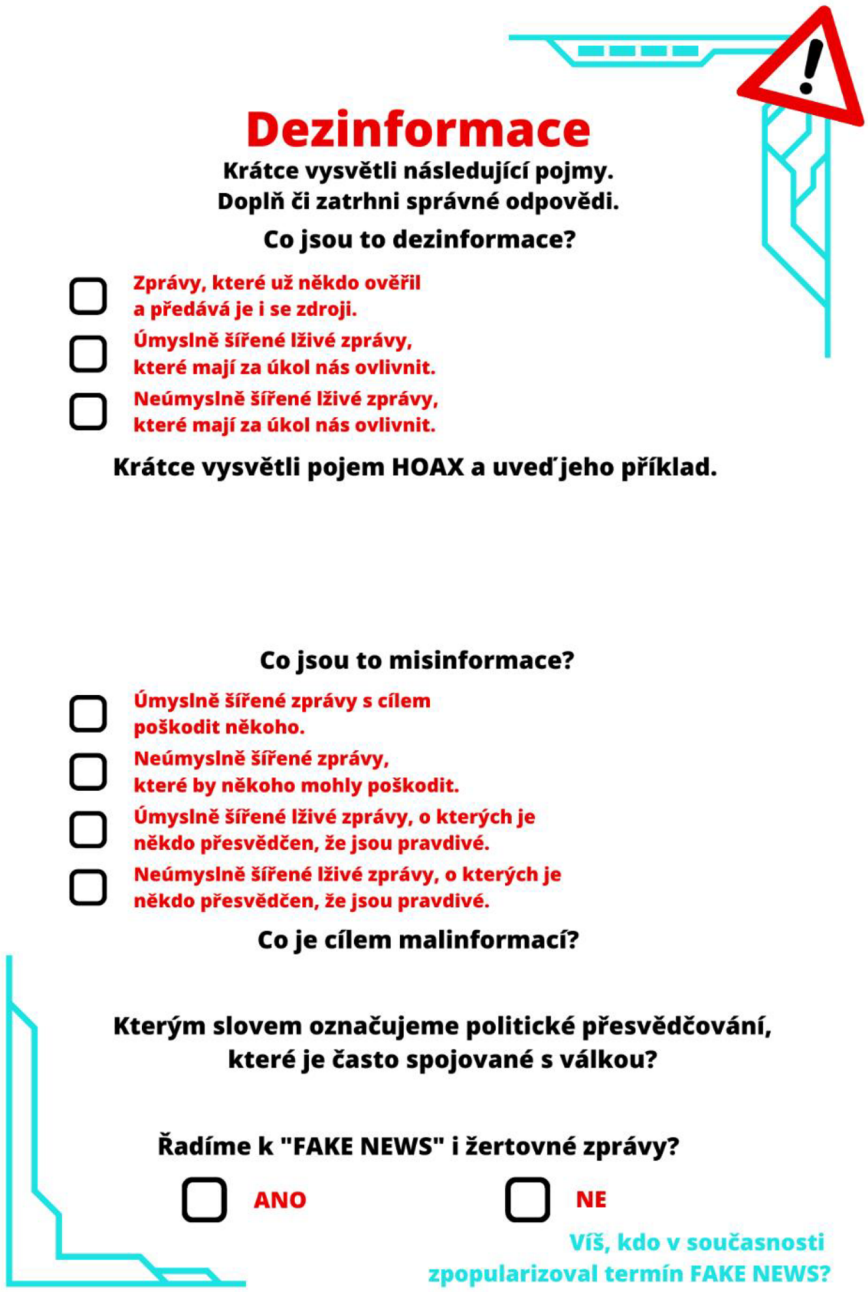
Metody výuky:

1. Vysvětlování (uvedení do tématu)
2. Samostatná práce (práce v pracovních listech)
3. Diskuse (průběžná diskuse s žáky o tématu a vypracovaných listech)

Mezipředmětové vztahy: Mediální výchova, občanská výchova

Pomůcky:

1. Krátká prezentace s pojmy
2. Laptop
3. Online aktivita - https://e-bezpeci.cz/hoaxy/
4. Pracovní listy (příloha 2):



Obrázek 1 - Použitý pracovní list

(Zdroj: vlastní zpracování v aplikaci Canva)

Fáze hodiny:

3. ~ 3 minuty – pozdrav a organizace
4. ~ 2 minuty – motivace
5. ~ 15 minut – prezentace nového učiva a průběžná diskuse
6. ~ 2 minuty – zadání samostatné práce
7. ~ 10 minut – samostatná práce žáků
8. ~ 5 minuty – krátká diskuse k pracovnímu listu
9. ~ 8 minut – online aktivita, sebehodnocení a zakončení

Průběh hodiny:

1. **Motivace** – Motivací v tomto případě může být aktuálnost tématu dezinformací a použití nových informací v reálném světě.
2. **Nové učivo** – Nové učivo je vysvětleno za pomoci krátké prezentace s definicemi z laptopu. Vysvětlování doprovází otázky vyučujícího a diskuse s žáky o tématu.
3. **Samostatná práce** – Samostatnou prací je voleno vyplnění pracovních listů – to především pro shrnutí probíraného tématu. Pracovní list však také může posloužit jako jednoduchý zápis z výuky.
4. **Online aktivita** – Online aktivita je zařazena na konec jako hlasovací hra. Na obrazovce je zobrazena zpráva z webové aplikace, která je přečtena nahlas. Žáci hlasují, zda je informace pravdivá či nepravdivá. Aktivita je zakončena sebehodnocením žáků, které se týká jejich schopnosti pracovat s dezinformacemi (např. jak se jim dařilo při vyplňování pracovních listů, jak byli úspěšní při odhadování pravdy od lži a jak jsou toto schopni dělat v reálném životě).

Možné otázky a úlohy:

Co jsou to dezinformace?

Co je to HOAX? Jaký je jeho cíl?

Jak byste vysvětlili pojem „fake news“?

Jaký je rozdíl mezi mal- a mis- informací?

Jak si můžeme ověřit informaci?

Poznámky:

Žáci jsou uspořádáni do půlkruhu, aby viděli na obrazovku z důvodu nepřítomnosti projektoru.

5.1.3 Fáze 3 – Test

Týden po výukové hodině byly opět ověřeny znalosti žáků pomocí stejného testu jako v první fázi tohoto ověřování. Toto testování bylo použito pro porovnání s předchozím pro určení pokroku žáků. Hodnocení probíhalo také stejným způsobem. Výsledky testování vypadaly následovně.:

Co jsou to dezinformace?

Správná odpověď: Úmyslně lživé a klamavé informace.

Na první otázku odpovědělo správně 7 žáků, 12 částečně správně a nikdo nesprávně. Mezi částečně správné odpovědi byly řazeny nekompletní odpovědi typu: *lživé informace, lži cestující internetem, deformované informace* či *falešné informace.*

Kde se s dezinformacemi můžeme setkat? (uveď alespoň 3 možnosti)

Správná odpověď: *Výpis 3 zdrojů dezinformací.* Například televize, média, internet, rádio atd.

Na tuto otázku tentokrát již byli schopni odpovědět všichni žáci. Bylo zaznamenáno 17 správných vyplnění a 2 částečné, které nesplnily minimum tří vypsaných možností. Nejčastěji se objevovaly odpovědi, o kterých se hovořilo na provedené hodině – *internet, média, sociální sítě a televize.*

Co je cílem HOAXů?

Správná odpověď: Šířit paniku.

Na třetí otázku odpovědělo správně 8 žáků, 10 částečně správně a 1 nesprávně (nevyplněná odpověď). Mezi částečně správné odpovědi byly zařazeny: *šířit se/cestovat internetem, aby si je přečetlo co nejvíce lidí, manipulovat s lidmi.*

Uveď příklad nějakého HOAXu.:

Správná odpověď: *Příklad jakéhokoliv známého HOAXu.* Například konec světa v roce 2012.

Na příklad HOAXu si z 19 žáků vzpomnělo 15. Nejčastěji padaly HOAXy, které byly zmíněny ve výuce v předchozím týdnu. Těmi byly: *konec světa 2012, mayský kalendář, Bigfoot, Herobrine z Minecraftu.*

Jak nazýváme informace, které mají za cíl někoho poškodit?

Správná odpověď: c) malinformace

V první výběrové otázce tentokrát odpovědělo správně 12 žáků a nesprávně 7 žáků. Je nutné podotknout, že ve třech případech si žáci zaměnili pojem misinformace za pojem malinformace.

Jak nazýváme neověřené informace, které někdo (neúmyslně) šíří jako pravdivé?

Správná odpověď: b) misinformace

Ve druhé výběrové otázce bylo ohodnoceno 11 odpovědí jako správných a 8 jako nesprávných. Jak již bylo zmíněno, u předchozí a této otázky byla zpozorována záměna pojmů u tří žáků.

Co v překladu znamená anglický termín „FAKE NEWS“?

Správná odpověď: Falešné zprávy.

Na otázku týkající se pojmu fake news ve druhém testování odpovědělo všech 19 žáků správně.

S čím v současnosti nejčastěji spojujeme termín PROPAGANDA?

Správná odpověď: Válka *nebo* politický nátlak/přesvědčování.

Na poslední otázky odpovědělo 17 žáků správně, 1 žák částečně správně a 1 žák odpověď nenapsal. Jako částečně správná odpověď byla hodnocena odpověď *Rusko*.

5.1.4 Výsledky ověřování

Po zpracování hodnocení ze třetí fáze ověřování byly výsledky jednotlivých otázek porovnány s výsledky z fáze první. Co se týče celkové úspěšnosti žáků v první fázi ověřování – minimální získaný počet bodů byl 2 body a nejvyšší 16 bodů. Průměrný počet získaných bodů byl tedy 7,58 bodu s procentuální úspěšností 47,37 %. Dle tohoto výsledku můžeme soudit, že se žáci již s tématem někdy v minulosti setkali.

	VÝSLEDKY																			PRŮMĚR
BODY	4	2	13	7	4	6	2	5	13	6	11	11	6	6	16	6	10	13	3	7,58
%	25	12,5	81,25	43,75	25	37,5	12,5	31,25	81,25	37,5	68,75	68,75	37,5	37,5	100	37,5	62,5	81,25	18,75	47,37

Tabulka 1 - Bodování první fáze

(Zdroj: vlastní zpracování v MS Excel)

Ve druhé fázi byl minimální počet získaných bodů 6 a nejvyšší 16. Průměrný počet získaných bodů byl tedy 12,47 s procentuální úspěšností 77,96 %.

	VÝSLEDKY																			PRŮMĚR
BODY	16	12	16	8	12	15	11	11	15	12	15	6	15	10	12	15	11	14	11	12,47
%	100	75	100	50	75	93,75	68,75	68,75	93,75	75	93,75	37,5	93,75	62,5	75	93,75	68,75	87,5	68,75	77,96

Tabulka 2 - Bodování třetí fáze

(Zdroj: vlastní zpracování v MS Excel)

Z tabulek a průměrného počtu bodů v obou fázích můžeme usoudit, že se skupina žáků při provedené výuce byla schopna přiučit novým vědomostem. Průměrný počet získaných bodů se zvedl o 4,89 bodu. Domníváme se tedy, že výuka založená na metodickém návrhu podpořená zvoleným pracovním listem je alespoň z části efektivní.

Posun u jednotlivých otázek

Obrátíme-li se na posun ve vědomostech u jednotlivých testových otázek, zjistíme, že se zvětšil počet správných a částečně správných odpovědí oproti počtu odpovědí nesprávných. Toto je zřejmé i z následujících tabulek udávající tyto počty. Můžeme tedy soudit, že měla provedená výuka na žáky opravdu nějaký vliv a byli si schopni poznatky týkající se dezinformací zapamatovat a následně reprodukovat ve druhém testování.

	OTÁZKA							
	1)	2)	3)	4)	5)	6)	7)	8)
SPRÁVNĚ	4	10	5	8	4	2	18	8
ČÁSTEČNĚ	11	4	6	0	0	0	0	5
ŠPATNĚ	4	5	8	11	15	17	1	6

Tabulka 3 - Správnost odpovědí z první fáze

(Zdroj: vlastní zpracování v MS Excel)

	OTÁZKA							
	1)	2)	3)	4)	5)	6)	7)	8)
SPRÁVNĚ	7	17	8	15	12	11	19	17
ČÁSTEČNĚ	12	2	10	0	0	0	0	1
ŠPATNĚ	0	0	1	4	7	8	0	1

Tabulka 4 - Správnost odpovědí ze třetí fáze

(Zdroj: vlastní zpracování v MS Excel)

Můžeme pozorovat, že žáci byli u otevřených otázek 1, 3 a 8 po proběhlé výuce schopni lépe formulovat své odpovědi, odpovídat na dané otázky přesněji či odlišit nuance jednotlivých pojmů. Žáci, co nebyli schopni odpovědět při prvním testování byli rovněž schopni odpovědět alespoň částečně při opakovaném ověřování znalostí.

Zlepšení jsme zaznamenali také u otevřených otázek týkajících se výpisu příkladů (otázky 2 a 4). Tento posun můžeme přisoudit udáním či u otázky týkající se HOAXů ukázáním a vysvětlením několika falešných příběhů v proběhlé výuce.

Výsledky otázky 7 zůstaly přibližně stejné. To nejspíše z důvodu správného vyplnění odpovědi žáky již při prvním testování. Zde můžeme soudit, že byla otázka možná až příliš jednoduchá a bylo ji možno vyřešit jak vědomostmi o internetových lžích, tak pouhým překladem z anglického jazyka, který se ve školách v současnosti učí všichni žáci.

Nejproblémovější byly pro žáky otázky týkající se výběru správné odpovědi (otázky 5 a 6). Zlepšení je sice v tabulkách viditelné, je zde však oproti ostatním stále poměrně velké množství odpovědí špatných. Možným vysvětlením pro tento stav je částečná podobnost vysvětlovaných pojmů (zjednodušeně se jedná o lži šířící se internetem). Jak již však bylo zmíněno, při druhém testování byla při hodnocení u tří žáků detekována záměna pojmů (podobná slova – malinformace a misinformace).

Pokud opět nahlédneme k hodnocení jako na celek – především na testování v první fázi, zjišťujeme možnost, že se většina žáků se pojmy z některých otázek (konkrétně 1, 3, 7 a 8) již někde setkala a dokázala sama uvést konkrétní případy.

5.2 Dotazníkové šetření

Po části týkající se ověřování metodického návrhu nás dále zajímaly názory žáků na proběhlou hodinu a konkrétně na vzhled a strukturu použitého pracovního listu. Pro toto zjišťování byla zvolena kvantitativní metoda dotazníku vytvořeného na platformě Google Forms. Ten je popisovaný Chráskou (2016) jako častou metodou určenou pro získávání dat, a to konkrétně získávání písemných odpovědí od dotazovaných respondentů. Vytvořený dotazník (příloha 13) obsahoval uzavřené položky a škálové položky pro zjištění názorů na vzhled pracovního listu. Z důvodu zjištění předchozích vědomostí o tématu v první fázi ověřování byly také vytvořeny výčtové položky týkající se toho, odkud žáci tyto vědomosti nabyli. Dotazník byl žákům zaslán pomocí e-mailu ihned po tom, co proběhla výuková hodina.

5.2.1 Výzkumné předpoklady

Vzhledem k tomu, že bylo při testování žáků zjištěno, že již o tématu nějaké vědomosti mají, byly sestaveny dva výzkumné předpoklady.:

Vp1: Žáci se o tématu nejčastěji dozvěděli ve škole.
Vp2: Žáci se o tématu nejčastěji dozvěděli v hodinách informatiky.

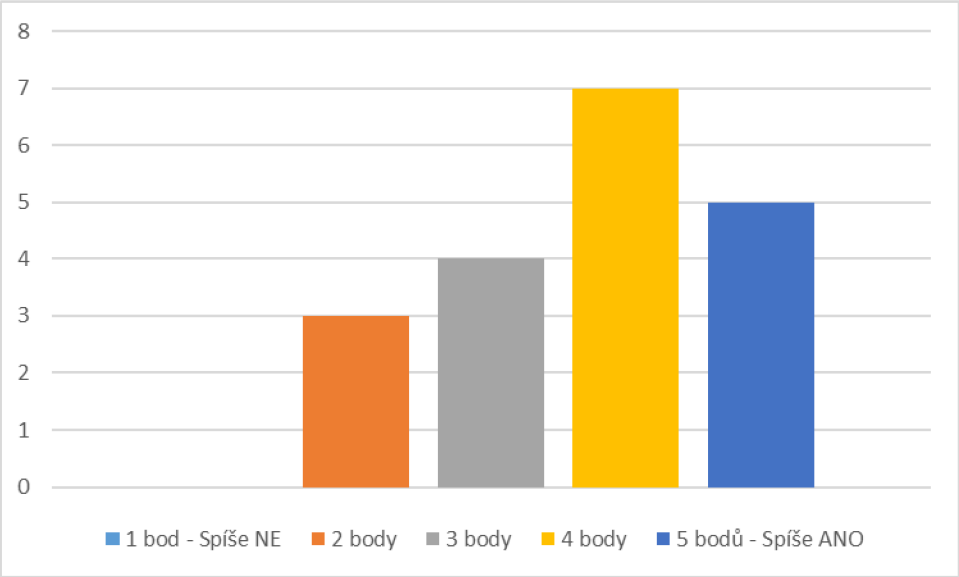
Tyto výzkumné předpoklady vycházejí z faktu, že je problematika internetové bezpečnosti v hodinách informatiky ve školách zavedena v rámci RVP ZV (jak bylo popsáno v kapitole 2) a dále toto konkrétní téma můžeme zařadit do průřezového tématu „*Mediální výchova*“, které může být (nejen) propojeno právě s digitálními technologiemi v rámci výuky informatiky (MŠMT, 2021).

5.2.2 Vyhodnocení dotazníku

Po shromáždění dotazníků od žáků byly jednotlivé odpovědi zpracovány do tabulek a grafů. Dotazník byl složen z 8 otázek – šesti tázajících se na názory ohledně pracovního listu a dvě dotazujících se na předešlé znalosti žáků. Jednotlivé otázky s odpověďmi budou v následujících odstavcích doplněny komentářem. Odpovědi na dotazník jsme obdrželi od všech devatenácti žáků.

Otázka č. 1 – Líbila se Vám grafická úprava pracovního listu?

První otázka se týkala názoru na samotný vzhled či grafickou úpravu pracovního listu. Na tuto otázku odpovídali žáci formou pětibodové stupnice, která sahala od odpovědi *1 – Spíše NE* po *5 – Spíše ANO*. Z tabulky a grafu můžeme vidět, že grafickou úpravu hodnotili žáci spíše kladně. Z 19 žáků volilo možnost s maximálním počtem bodů 26,3 % (5 žáků) a možnost se čtyřmi body 36,8 % (7 žáků). Neutrální postoj zaujmuli 4 žáci (21,1 %) a třem žákům (15,8 %) se pracovní list spíše nelíbil. Nikdo však nezvolil položku s nejméně body.



Graf 1 - Líbivost pracovního listu

(Zdroj: vlastní zpracování v MS Excel)

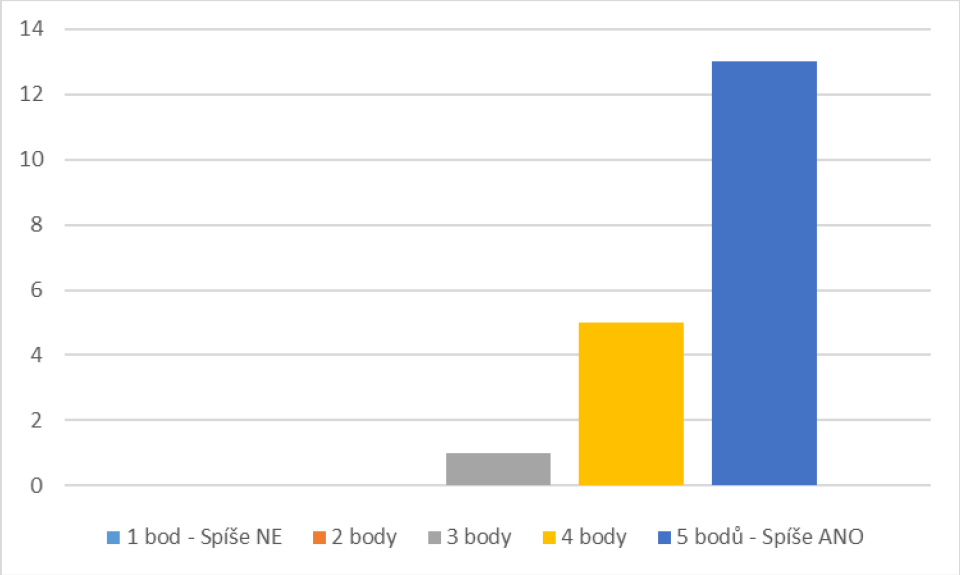
	Počet	%
1 bod - **Spíše NE**	0	0
2 body	3	15,8
3 body	4	21,1
4 body	7	36,8
5 bodů - **Spíše ANO**	5	26,3
CELKEM	19	100

Tabulka 5 - Líbivost pracovního listu

(Zdroj: vlastní zpracování v MS Excel)

Otázka č. 2 – Byl pracovní list přehledný?

V následující otázce jsme se ptali, zda žákům přišel pracovní list dostatečně přehledný. Zde žáci opět odpovídali pomocí pětibodové stupnice. Zde můžeme vidět, že pro většinu žáků byl pracovní list dostatečně přehledný, jelikož 13 z nich (68,4 %) volilo odpověď pětibodovou. Pět žáků (26,3 %) hodnotilo přehlednost čtyřmi body a pouze jeden žák (5,3 %) třemi body. Pro nikoho z žáků nebyl pracovní list tak nepřehledný, aby udělili pouze jeden nebo dva body.



Graf 2 - Přehlednost pracovního listu

(Zdroj: vlastní zpracování v MS Excel)

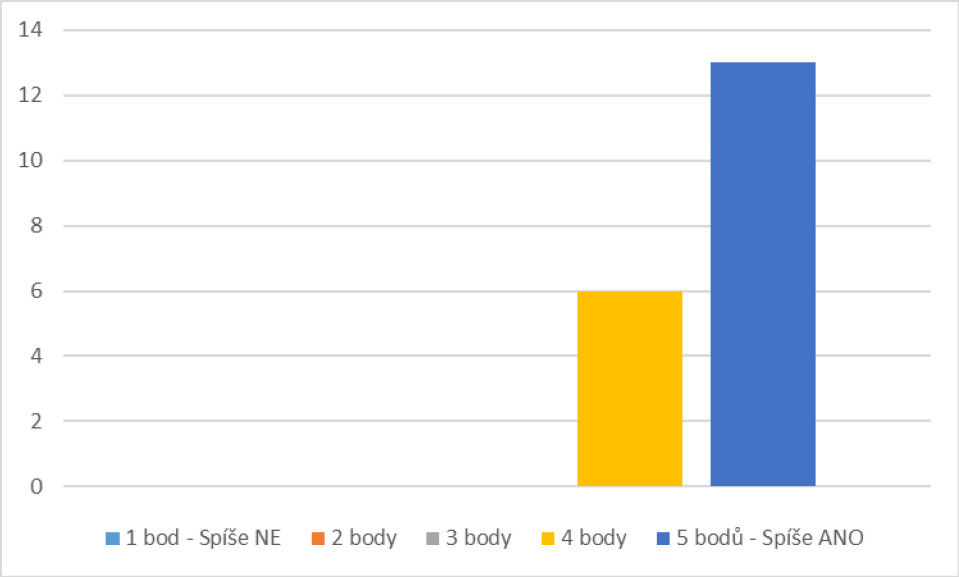
	Počet	%
1 bod - **Spíše NE**	0	0
2 body	0	0
3 body	1	5,3
4 body	5	26,3
5 bodů - **Spíše ANO**	13	68,4
CELKEM	19	100

Tabulka 6 - Přehlednost pracovního listu

(Zdroj: vlastní zpracování v MS Excel)

Otázka č. 3 – Byly otázky a úlohy napsané a vysvětlené srozumitelně?

V následující otázce jsme se žáků dotazovali na srozumitelnost textů otázek a úloh. Odpovědi byly opět děleny do pěti možných kategorií jako u předešlých otázek. Třináct žáků (68,4 %) hodnotilo srozumitelnost velmi kladně (pěti body) a šest žáků (31,6 %) ji hodnotilo čtyřmi body. Nezaznamenali jsme horší bodování.



Graf 3 - Srozumitelnost pracovního listu

(Zdroj: vlastní zpracování v MS Excel)

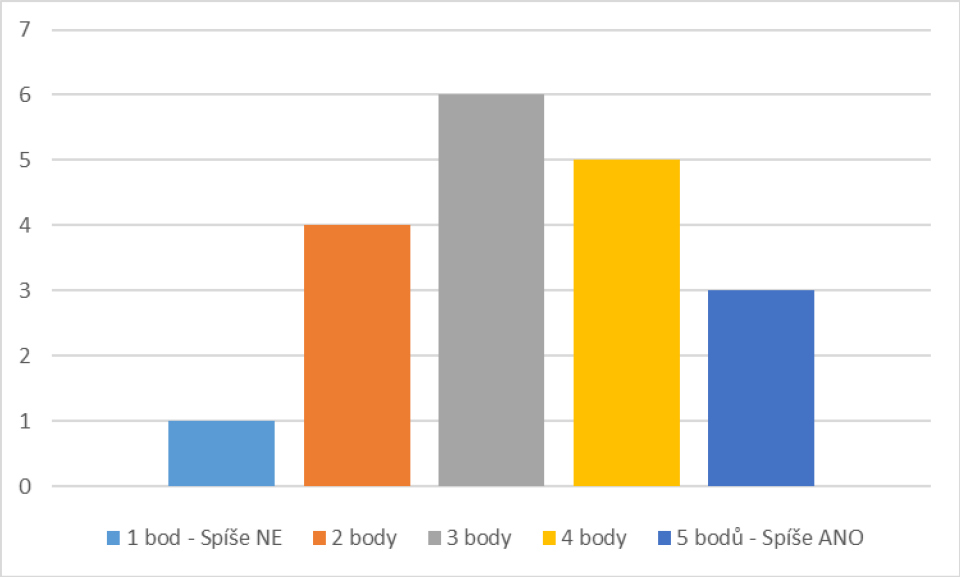
	Počet	%
1 bod - **Spíše NE**	0	0
2 body	0	0
3 body	0	0
4 body	6	31,6
5 bodů - **Spíše ANO**	13	68,4
CELKEM	19	100

Tabulka 7 - Srozumitelnost pracovního listu

(Zdroj: vlastní zpracování v MS Excel)

Otázka č. 4 – Myslíte si, že pro Vás byla práce s pracovním listem přínosná?

Poslední otázkou stejného charakteru byla otázka týkající se přínosnosti pro jednotlivé žáky. Zde 3 žáci (15,7 %) hodnotili nejvyšším počtem bodů, 5 žáků (26,3 %) hodnotilo čtyřmi body, 6 žáků (31,6 %) sáhlo po tříbodové kolonce, 4 žáci (21,1 %) udělilo 2 body a pro jednoho žáka nebyla práce s pracovním listem dostatečně přínosná.



Graf 4 - Přínosnost pracovního listu

(Zdroj: vlastní zpracování v MS Excel)

	Počet	%
1 bod - **Spíše NE**	1	5,3
2 body	4	21,1
3 body	6	31,6
4 body	5	26,3
5 bodů - **Spíše ANO**	3	15,7
CELKEM	19	100

Tabulka 8 - Přínosnost pracovního listu

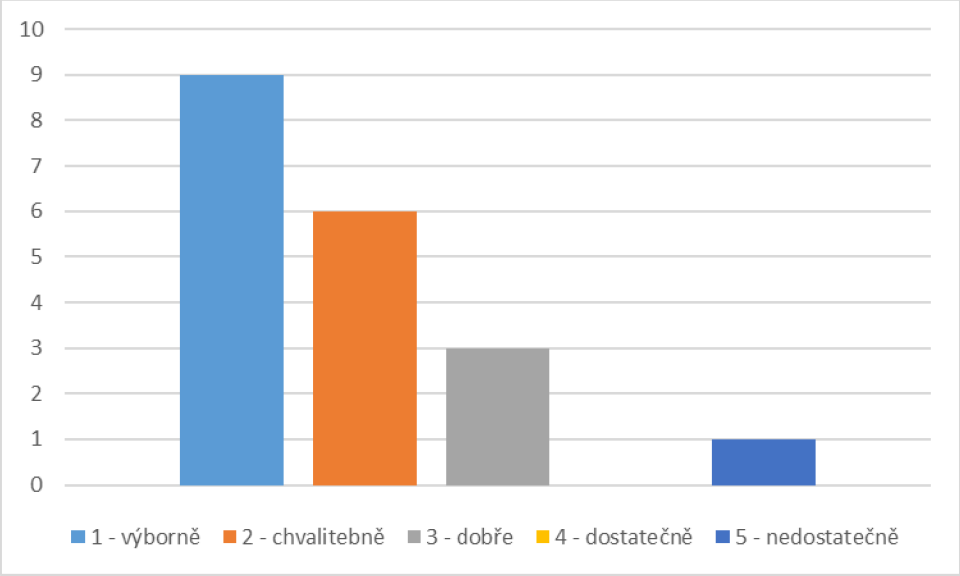
(Zdroj: vlastní zpracování v MS Excel)

Otázka č. 5 – Nalezli jste v pracovním listu něco, co byste rádi upravili či změnili?

Pátá otázka byla otázkou otevřenou a nepovinnou, která dotazovala se žáků na to, co by do pracovního listu rádi doplnili. Na tuto otázku odpovědělo 7 žáků. Čtyři odpověděli slovy *„nevím“* či *„nic“*, ve dvou případech by žáci rádi upravili pracovní list tak, aby byl barevnější a jeden žák by doplnil obrázky.

Otázka č. 6 – Ohodnoťte (celkově) pracovní list známkou jako ve škole.

V otázce číslo 6 jsme po žácích chtěli, aby shrnuli své dojmy z pracovního listu a oznámkovali jej jako ve škole na stupnici 1 (výborně) až 5 (nedostatečně). Velká část dotazovaných žáků (9; 47,4 %) hodnotila jedničkou, 6 žáků (31,6 %) dvojkou, 3 žáci (15,7 %) trojkou a obdrželi jsme jednu pětku (1 žák; 5,3 %). Zde však podle předchozích odpovědí můžeme soudit, že se jedná buď o překlep či vtip od jednoho z žáků.



Graf 5 - Hodnocení žáky

(Zdroj: vlastní zpracování v MS Excel)

	Počet	%
1 - výborně	9	47,4
2 - chvalitebně	6	31,6
3 - dobře	3	15,7
4 - dostatečně	0	0
5 - nedostatečně	1	5,3
CELKEM	19	100

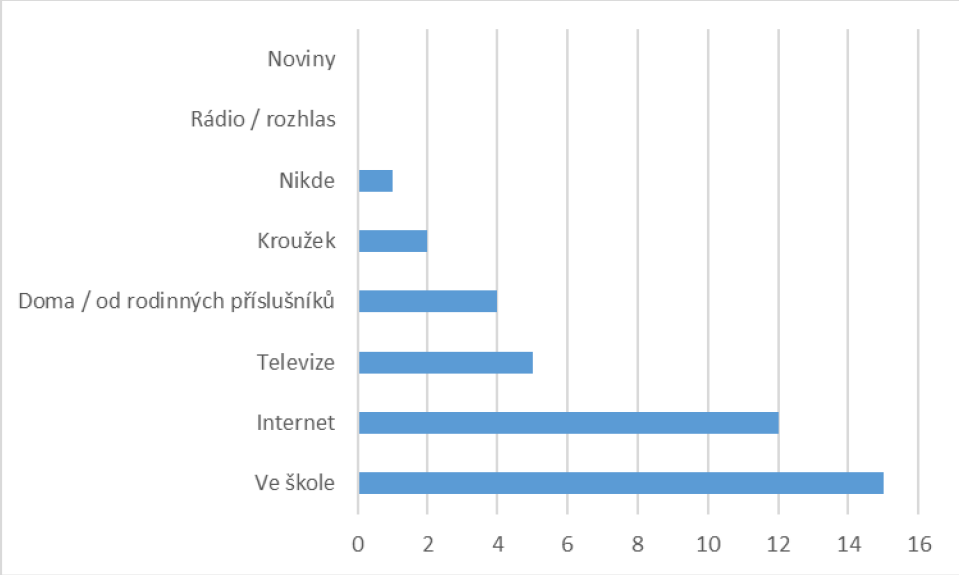
Tabulka 9 - Hodnocení žáky

(Zdroj: vlastní zpracování v MS Excel)

Otázka č. 7 – Kde / jak jste se před proběhlou hodinou dozvěděli o dezinformacích?

Následující dvě otázky se již netýkaly názorů na použitý pracovní list, nýbrž navazovaly na poznatky z první fáze ověřování – tedy na zjištění předchozích vědomostí žáků. Otázka číslo 7 se zabývala tím, kde žáci k vědomostem spojeným s dezinformacemi přišli. Jednalo se o výčtovou otázku s možností více odpovědí a doplnění vlastní odpovědi.

Co se týče konkrétních odpovědí – 15 oslovených žáků se ke znalostem dostalo ve škole, 12 na internetu, 5 v televizi, 4 žáci uvedli odpověď *„doma / od rodinných příslušníků“*, dva žáci využili možnosti doplnit odpověď vlastní a připsali možnost *„kroužek“* a jeden žák zvolil *možnost „nikde“*.



Graf 6 - Kde žáci nabyli znalostí

(Zdroj: vlastní zpracování v MS Excel)

	Počet
Ve škole	15
Internet	12
Televize	5
Doma / od rodinných příslušníků	4
Kroužek	2
Nikde	1
Rádio / rozhlas	0
Noviny	0

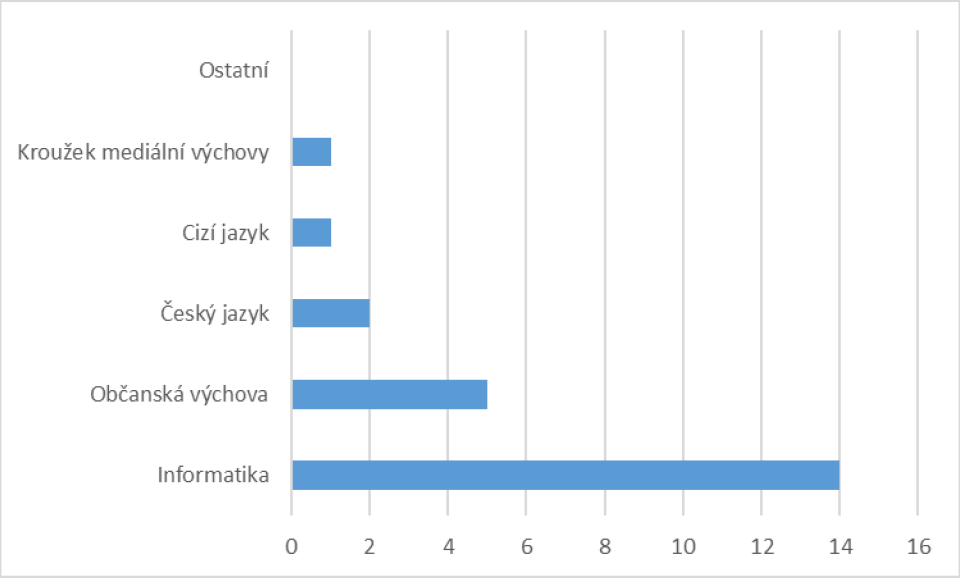
Tabulka 10 - Kde žáci nabyli znalostí

(Zdroj: vlastní zpracování v MS Excel)

Otázka č. 8 – Pokud jste zvolili možnost *„Ve škole“* – v jakém to bylo předmětu?

Poslední otázka rozšiřovala otázku předchozí a doptávala se žáků, kteří zvolili odpověď ve škole, v jakých předmětech se těchto vědomostí naučili či kde o těchto pojmech slyšeli. Opět se jednalo o výčtovou otázku s možností více odpovědí či případné vlastní odpovědi.

Většina žáků (14) odpověděla, že se o tématu již něco dozvěděla v hodinách informatiky, 5 žáků zatrhlo rámeček občanské výchovy, 2 žáci předmět český jazyk a jeden žák společnou položku pro cizí jazyky. Poslední odpověď byla opět připsaná – tentokrát se jednalo o *„kroužek mediální výchovy“*. Byly uvedeny i další možné odpovědi / předměty, ty však byly z následující tabulky a grafu vyřazeny z důvodu žádné odpovědi (pro přehled byly nahrazeny položkou *„ostatní“*).



Graf 7 – Předměty, kde žáci nabyli znalostí

(Zdroj: vlastní zpracování v MS Excel)

	Počet
Informatika	14
Občanská výchova	5
Český jazyk	2
Cizí jazyk	1
Kroužek mediální výchovy	1
Ostatní	0

Tabulka 11 - Předměty, kde žáci nabyli znalostí

(Zdroj: vlastní zpracování v MS Excel)

5.2.3 Interpretace výsledků

Jelikož byl dotazník rozdělen na dvě části, zaměříme se nejprve na tu první, a tedy tu týkající se získání zpětné vazby na použitý pracovní list. Z pohledu na výsledky z této části zjišťujeme, že žáci na formu pracovního listu reagovali převážně kladně až velmi kladně (otázky 1, 2, 3 a 6), a to především co se týče jeho designové stránky, srozumitelnosti textů a přehlednosti. Byla nám však v několika případech (otázka 5) vytknuta nedostatečná barevnost (možná i hravost) – to jak týkající se vlastních barev předloženého listu, tak nedostatek (či spíše jejich celková absence) obrázků.

Toto jsou však poměrně jednoduché úpravy, které by bylo možno provést například v případné budoucí revizi pracovních listů. Je pravda, že pracovní listy byly navrženy především z hlediska přehlednosti a podpora naučného obsahu ve vyučovacích hodinách. Samotná grafická úprava byla tedy při jejich konstrukci brána jako vedlejší, a tudíž poměrně minimalisticky.

Na výsledky otázky týkající se přínosnosti pracovního listu pro jednotlivé žáky (otázka 4) můžeme pohlížet z několika úhlů. Průměrné bodové hodnocení mohlo způsobit to, že žáci již měli o probíraném tématu nějaké povědomí, a tudíž si nemysleli, že je pracovní list naučil něco nového. Další možností mohou být rozdílné preference žáků týkající se způsobu výuky (např. jeden žák preferuje výklad, druhý samostatnou práci a třetí výuku formou hry). Z tohoto důvodu je na samotném učiteli, jakým způsobem by náš pracovní list (potažmo celý metodický návrh) upravil (individualizoval) pro třídu, ve které vyučuje.

Celkově tedy hodnotíme pracovní list i přes drobné nedostatky jako úspěšný a vhodný pro výuku. Tato zpětná vazba a vlastní reakce žáků byly velice potěšující.

Druhá část dotazníku byla věnována potvrzení či vyvrácení výzkumných předpokladů, které vznikly po prvním testování žáků při ověřování metodického návrhu.

Vp1: Žáci se o tématu nejčastěji dozvěděli ve škole.

První výzkumný předpoklad vyplýval z poznatků z teoretické části, které mluví o zavedení internetové bezpečnosti jako tématu ve výuce informatiky a dále v rámci průřezového tématu mediální výchova, který vzděláním na 2. stupni ZŠ prostupuje.

Z výsledků šetření je zřejmé, že nejvíce žáků se o tématu dozvědělo ve škole, jak bylo předpokládáno – můžeme tedy říci, že náš **předpoklad byl potvrzen**.

Není však zanedbatelná položka internetu, která byla druhá nejčastěji volená. Vzhledem k formulaci otázky však nemůžeme zjistit, zda se jedná o obecné informační zdroje či zdroje zabývající se přímo internetovou bezpečností. Část žáků se však dozvěděla o dezinformacích (a jiných lžích publikovaných na internetu) i od rodinných příslušníků či televize.

Možným vysvětlením toho, proč se o tomto tématu žáci dozvěděli i z jiných zdrojů je vzestup dezinformací týkající se současných světových krizí (jako příklad můžeme uvést poměrně nedávnou pandemii či stávající válku na Ukrajině).

Poměrně překvapivou odpovědí byla ta, kterou si žáci doplnili sami. Dva žáci uvedli, že mají tyto znalosti z kroužku. Zde však bohužel nevíme, zda se jedná o kroužek školní či mimoškolní.

Vp2: Žáci se o tématu nejčastěji dozvěděli v hodinách informatiky.

Druhý výzkumný předpoklad měl za úkol rozšířit ten první a dotazoval se na konkrétní předměty, ve kterých se žáci o dezinformacích učili. Tento předpoklad byl stejně jako ten předchozí založen na poznatcích z kapitoly 2.

Z výsledků se dozvídáme, že se opravdu většina žáků o tématu dozvěděla od vyučujících v hodinách informatiky – náš druhý předpoklad je tedy **potvrzen**.

Informatika však nebyla jediná, kde se ve školách o dezinformacích mluvilo. Dále byly uváděny předměty občanská výchova a český či cizí jazyk, ovšem ne v takové míře. Poslední odpověď *„kroužek mediální výchovy“* nám pak naznačuje, že alespoň jeden kroužek zmíněný v předchozí otázce byl kroužkem školním.

Závěr

Tato diplomová práce se zabývala tématem tvorby metodických návrhů, a to konkrétně návrhů týkající se výuky internetové bezpečnosti v hodinách informatických předmětů vyučovaných na druhém stupni základních škol. Práci můžeme pomyslně rozdělit na část teoretickou a praktickou.

Teoretická část práce se zabývala v první řadě vysvětlením základních pojmů spojených s internetem, jeho historií a službami, kde bylo následnou velkou podkapitolou vysvětlení různých nebezpečí, se kterými se žáci na internetu mohou setkat. Následující kapitola se zabývala zasazením informatiky ve školských dokumentech, a právě výukou zmíněného tématu v nich. Třetí a poslední teoretická kapitola se týkala samotnému plánování výuky, které nám mělo dopomoci vytvořit metodické návrhy.

Následně jsme pomyslně překročili do části praktické, která se nejprve zabývala prezentací vytvořených návrhů pro výuku jednotlivých témat nebezpečí na internetu, které byly díky přílohám doplněny pracovními listy. Jeden z těchto návrhů byl dále společně s pracovním listem zvolen k ověření v praxi, zpracován a předveden.

Toto ověření proběhlo ve třech fázích. Těmi byly první testovací fáze určená ke zjištění předchozích znalostí žáků. Následovala výuka s využitím metodického návrhu, která byla podpořena vytvořeným pracovním listem a celá fyzická část ověřování byla zakončena druhým testováním, které nám zajistilo fyzicky přímo před skupinou žáků. Výsledky obou testování byly ohodnoceny, zaznamenány v tabulkách a porovnány. Ve výsledku bylo zjištěno zlepšení týkající povědomí o zvoleném tématu (dezinformace).

V poslední praktické části jsme se zabývali žákovskými názory na použitý pracovní list ve fázi výuky. Tato zpětná vazba byla spíše kladná. Dále jsme také potvrdili dva výzkumné předpoklady týkající se již probíhající výuky bezpečnosti na internetu ve školách.

Díky výsledkům z ověřování a zpětné vazby se domníváme, že i další z návrhů by mohly být užitečné a pomoci učitelům při plánování výuky na jednotlivá témata. Tohle by však bylo vhodné dále ověřit například v rámci další potenciální práce.

Z výše uvedeného tedy **můžeme označit cíle práce uvedené v úvodu jako splněné.**

Toto téma bylo vybráno především z důvodu neustále pokračující integrace internetu a jeho služeb do našeho života. Současní žáci se s jeho přítomností stýkají již od dětství a práce s ním je zahrnuta i v prostředí základních škol. Samotný internet je plný (mohli bychom říci, že dokonce občas i přesycený) zábavy, pohodlí zlepšujících vychytávek a poznání, ale i kriminality, podvodů a dalších nebezpečí.

I o tomhle zpíval Americký komik Bo Burnham ve své písni *„Welcome to the Internet“*, který v roli pochybného obchodníka zosobňující internet jako celek zmiňuje a shrnuje, že je nám schopný přinést a ochotný prodat opravdu cokoliv – kdykoliv.

„Could I interest you in everything?
All of the time.
A little bit of everything.
All of the time.“

- Bo Burnham, *Welcome to the internet* (2021)

Z těchto uvedených důvodu je na místě žáky informovat nejen o tom, jak je užitečný, ale i varovat a poučit tom, jak se na něm bezpečně pohybovat. Právě toto propojení školy a problematiky internetové bezpečnosti žáků bylo velkou inspirací pro vypracování této práce stejně tak jako potenciální pomoc dalším vyučujícím, kteří si neví rady, jak zmíněné téma do svých hodin zakomponovat.

Seznam použitých zdrojů

Literatura

AMERICAN PSYCHIATRIC ASSOCIATION. *Diagnostic and Statistical Manual of Mental Disorders: DSM-V.* Washington, D.C.: American Psychiatric Publishing, 2013. ISBN 978-0-89042-555-8.

ANDERSON, Lorin W. a David R. KRATHWOHL. *A Taxonomy for Learning, Teaching, and Assessing: A Revision of Bloom's Taxonomy of Educational Objectives.* Longman, 2001. ISBN 0-8013-1903-X.

BASLER, Jaromír a Michal MRÁZEK. *Počítačové hry a jejich místo v životě člověka.* Olomouc: PdF UP, 2018. ISBN 978-80-244-5405-4.

BIDGOLI, Hossein. *Encyclopedia of Information Systems*. Elsevier, 2002. ISBN 978-0-12-227240-0.

BLINKA, Lukáš a kol. *Online závislosti*. Praha: Grada, 2015. ISBN 978-80-210-7975-5.

ČADÍLEK, Miroslav a Aleš LOVEČEK. *Didaktika odborných předmětů*. Brno: MUNI, 2005. ISBN 978-80-87063-25-5.

CHRÁSKA, Miroslav. *Metody pedagogického výzkumu: základy kvantitativního výzkumu*. Praha: Grada, 2016. ISBN 978-80-247-5326-3.

KALHOUS, Zdeněk, OBST, Otto a kol. *Školní didaktika*. Praha: Portál, 2002. ISBN 80-7178-253-X.

KEEFER, Alice a Tomas BAIGET. *How it all began: a brief history of the Internet*. Emerald Publishing, 2001. DOI:10.1108/03055720010804221

KOLOUCH, Jan. *CyberCrime*. Praha: CZ.NIC, 2017. ISBN 978-80-88168-15-7.

KOPECKÝ, Kamil a kol. *Rizikové formy chování českých a slovenských dětí v prostředí internetu*. Olomouc: UPOL, 2015. ISBN 978-80-244-4868-8

KOŽÍŠEK, Martin a Václav PÍSECKÝ. *Bezpečně na Internetu*. Praha: Grada, 2016. ISBN 978-80-271-9075-1.

MAŇÁK, Josef a Vlastimil ŠVEC. *Výukové metody*. Brno: MUNI, 2003. ISBN 80-7315-039-5.

PRŮCHA, Jan, WALTEROVÁ, Eliška, MAREŠ, Jiří a kol. *Pedagogický slovník*. Praha: Portál, 2009. ISBN 978-80-7367-546-2.

SKALKOVÁ, Jarmila. *Obecná didaktika*. Praha: Grada, 2007. ISBN 978-80-247-1821-7.

STARÁ, Jana, ZEMANOVÁ, Blanka a Petra HORSKÁ. *Obecná didaktika I. - Plánování výuky*. Praha: PdF UK, 2020. ISBN 978-80-7603-245-3.

ŠAFRÁNKOVÁ, Dagmar. *Pedagogika*. Praha: Grada, 2019. ISBN 978-80-247-5511-3.

ŠEVČÍKOVÁ, Anna a kol. *Děti a dospívající online*. Praha: Grada, 2015. ISBN 978-80-247-9646-8.

TOLLINGEROVÁ, Dana. *K teorii učebních činností*. Praha: Státní pedagogické nakladatelství, 1987. ISBN neuvedeno.

VALIŠOVÁ, Alena a Miroslava KOVAŘÍKOVÁ. *Obecná didaktika a její širší pedagogické souvislosti v úkolech a cvičeních*. Praha: Grada, 2021. ISBN 978-80-271-3249-2.

YOUNG, Kimberly S. *Internet Addiction: A New Clinical Phenomenon and Its Consequences*. American Behavioral Scientist, 2004. 48(4). 402–415. DOI:10.1177/0002764204270278

ZENDLE, David; MEYER, Rachel a Harriet OVER. *Adolescents and loot boxes*. Royal Society Open Science, 2019. DOI:10.1098/rsos.190049

ZORMANOVÁ, Lucie. *Obecná didaktika*. Praha: Grada, 2014. ISBN 978-80-247-4590-9.

ZORMANOVÁ, Lucie. *Výukové metody v pedagogice*. Praha: Grada, 2012. ISBN 978-80-247-4100-0.

Elektronické zdroje

BARTOSZ, Jakub. *Další falešný voják se srdceryvnou legendou, žena z Náchodska mu poslala dva miliony*. In: *Novinky.cz* [Online]. Novinky.cz, 2022. [cit. 22.2.2023]. Dostupné z: https://www.novinky.cz/clanek/krimi-dalsi-falesny-vojak-se-srdceryvnou-legendou-zena-z-nachodska-mu-poslala-dva-miliony-40407441

ČESKÝ STATISTICKÝ ÚŘAD. *Využívání informačních a komunikačních technologií v domácnostech a mezi jednotlivci - 2021*. [online]. Český statistický úřad, 2021. [cit. 8. 4. 2023]. Dostupné z: https://www.czso.cz/csu/czso/vyuzivani-informacnich-a-komunikacnich-technologii-v-domacnostech-a-mezi-jednotlivci-2021

E-BEZPECI.CZ. *Projekt E-Bezpečí*. [online]. Olomouc: Centrum PRVoK, 2023. [cit: 11.3.2023]. Dostupné z: https://www.e-bezpeci.cz/

HLADKÁ, Eva a Jan FOUSEK. *Základy IT Gramotnosti - Služby internetu*. In: *is.muni.cz*. [online]. Brno: Fakulta informatiky MUNI. [cit. 16.3.2023]. Dostupné z: https://is.muni.cz/do/ics/el/sitmu/law/html/sluzby-internetu.html

INTERNET SOCIETY. *Brief History of the Internet.* [online]. Internet Society, 1997. [cit. 16.3.2023] https://www.isoc.org/internet/history-internet/brief-history-internet/

KOPECKÝ, Kamil. *Co je to vlastně ten hoax, dezinformace, misinformace nebo třeba fake news? Čím se tyto termíny liší a co mají společného?* In: *E-Bezpeci.cz*. [online]. Olomouc: Centrum PRVoK, 2022. [cit. 20.2.2023] Dostupné z: https://www.e-bezpeci.cz/index.php/clanky-komentare/2864-co-je-to-vlastne-ten-hoax-dezinformace-misinformace-nebo-treba-fake-news-cim-se-tyto-terminy-lisi-a-co-maji-spolecneho

KOPECKÝ, Kamil. *Úvod do netolismu*. In: *E-Bezpeci.cz*. [online]. Olomouc: Centrum PRVoK, 2011. [cit. 15.2.2023]. Dostupné z: http://www.e-bezpeci.cz/index.php/temata/dali-rizika/331-uvod-do-problematiky-netolismu

MŠMT. *Národní strategie primární prevence rizikového chování dětí a mládeže na období 2019-2027*. [online]. Ministerstvo školství, mládeže a tělovýchovy, 2019. [cit. 10.3.2023]. Dostupné z: https://www.msmt.cz/uploads/narodni_strategie_primarni_prevence_2019_27.pdf

MŠMT. *Rámcový vzdělávací program pro základní vzdělávání.* [online]. Ministerstvo školství, mládeže a tělovýchovy, 2021 [cit. 7.2.2023]. Dostupné z: https://revize.edu.cz/files/rvp-zv-2021-s-vyznacenymi-zmenami.pdf

MVČR. *Definice dezinformací a propagandy*. [Online] Ministerstvo vnitra České republiky - Centrum proti hybridním hrozbám, 2023. [cit. 20.2.2023]. Dostupné z: https://www.mvcr.cz/chh/clanek/definice-dezinformaci-a-propagandy.aspx

SZOTKOWSKI, René a Kamil KOPECKÝ. *České děti v kybersvětě (výzkumná zpráva).* [online]. Olomouc: Centrum PRVoK, 2019a. [cit. 19.2.2023]. Dostupné z: https://www.e-bezpeci.cz/index.php/ke-stazeni/vyzkumne-zpravy/117-ceske-deti-v-kybersvete/file

SZOTKOWSKI, René a Kamil KOPECKÝ. *Kybernemoci a netolismus (průvodce studiem)*. [online]. Pdf UP Olomouc, 2019b. [cit. 19.2.2023]. Dostupné z: https://www.pdf.upol.cz/fileadmin/userdata/PdF/VaV/2019/odborne_seminare/2._Kybernemoci_a_netolismius.pdf

ŽUFNÍČEK, Jan. *Příloha č.15 - Netolismus | Metodické dokumenty (doporučení a pokyny).* [online]. Ministerstvo školství, mládeže a tělovýchovy, 2013. [cit. 19.2.2023]. Dostupné z: https://www.msmt.cz/vzdelavani/socialni-programy/metodicke-dokumenty-doporuceni-a-pokyny

Kvalifikační práce

SEDLÁČEK, Jan. *Závislost na internetu u žáků 2. stupně základních škol*. Olomouc, 2021. Bakalářská práce. Univerzita Palackého, Pedagogická fakulta, Katedra technické a informační výchovy. Vedoucí práce: Ing. Mgr. Michal Sedláček, Ph.D.

Seznam obrázků

Seznam grafů

Seznam tabulek

Seznam příloh

Příloha 1

Dezinformace

Pomocí internetu ověř pravdivost následujících tvrzení.

U nepravdivých informací zakresli do rámečku křížek a krátce vysvětli proč je tvrzení nepravdivé.

☐ **Ježci si na bodlinách nosí jablka.**

☐ **Vikingové měli rohaté přilby.**

☐ **Pštrosi strkají hlavu do písku, když se bojí.**

☐ **Chameleon mění barvu podle toho, kde stojí.**

☐ **Po mrkvi se nám zlepší zrak.**

Znáš ještě nějaká podobná tvrzení?

Příloha 2

Dezinformace

Krátce vysvětli následující pojmy.
Doplň či zatrhni správné odpovědi.

Co jsou to dezinformace?

- ☐ Zprávy, které už někdo ověřil a předává je i se zdroji.
- ☐ Úmyslně šířené lživé zprávy, které mají za úkol nás ovlivnit.
- ☐ Neúmyslně šířené lživé zprávy, které mají za úkol nás ovlivnit.

Krátce vysvětli pojem HOAX a uveď jeho příklad.

Co jsou to misinformace?

- ☐ Úmyslně šířené zprávy s cílem poškodit někoho.
- ☐ Neúmyslně šířené zprávy, které by někoho mohly poškodit.
- ☐ Úmyslně šířené lživé zprávy, o kterých je někdo přesvědčen, že jsou pravdivé.
- ☐ Neúmyslně šířené lživé zprávy, o kterých je někdo přesvědčen, že jsou pravdivé.

Co je cílem malinformací?

Kterým slovem označujeme politické přesvědčování, které je často spojované s válkou?

Řadíme k "FAKE NEWS" i žertovné zprávy?

☐ ANO ☐ NE

Víš, kdo v současnosti zpopularizoval termín FAKE NEWS?

Příloha 3

Náměty na aktivitu

Seznam námětů na aktivitu týkající se fake news a propagandy.

Nábor do galaktického impéria (propaganda se Star Wars tématikou)

Hmyz cestující v banánech (fake news)

Lední medvěd procestoval na kusu ledovce půl světa a ohrožuje obyvatele (fake news)

Nová politická strana láká na čerstvé sušenky (propaganda)

Vláda USA cvičí holuby pro špionáž (fake news)

Garfield je ve skutečnosti reálný kryptid (fake news/vymyšlená legenda)

Mezinárodní zákaz špaget v zemích, které nejsou Itálie. (fake news)

...

Příloha 4

Grooming

Odpověz na následující otázky.

Existují nějaké znaky, pomocí kterých zjistíme, že je uživatelský profil falešný?

Jakým způsobem si pomocí jediné fotografie ověříme, že mluvíme se člověkem, se kterým chceme?

Zamysli se, proč by se tě někdo neznámý ptal na následující otázky.

Kam chodíš do školy?

Kontrolují ti rodiče mobil?

Máš vlastní počítač nebo máte doma společný?

Chodíš do školy sám/sama nebo s doprovodem?

Jak by jsi zareagoval/a, kdyby ti napsala nějaká známá osobnost a chtěla se například sejít?

Příloha 5

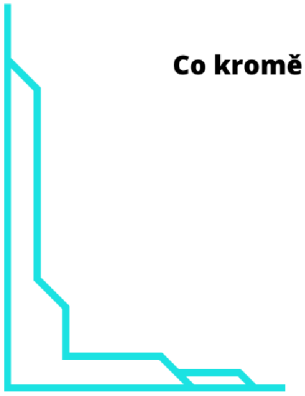
Digitální stopa

Odpověz na následující otázky a vypracuj úkoly.
Můžeš použít vlastní mobilní zařízení.

Vypiš, co o nás aplikace odesílají.

Jaké aplikace z tvého mobilu vyžadují povolení odesílání informací o poloze?

Co je to MAC adresa a jak se k ní dostaneme?



Co kromě MAC adresy patří do digitální stopy?

Příloha 6

Gambling a závislost

Vypracuj následující úkoly.
Pro výpočty můžeš použít
kalkulačku či tabulkový procesor.

Na internetu najdi počítačovou hru,
která obsahuje "lootboxy".
Najdi, jaká je pravděpodobnost výhry nejvzácnějšího předmětu.
Následně vyhledej ceny jednotlivých "lootboxů" a vypočítej,
kolik by jsi musel/a utratit, aby jsi jej měl/a šanci získat.
Zvolenou hru, cenu otevření 1 "lootboxu" a finální cenu si zapiš.

Na následujícím odkazu si vyzkoušej svoji závislost na internetu.:

https://poradna.adiktologie.cz/otestujte-se/?poll_id=5

Příloha 7

Phishing a podvody

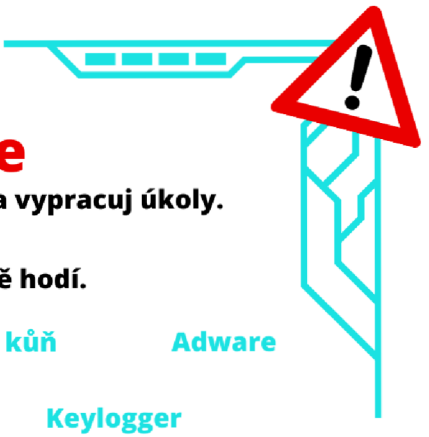
Vypracuj následující úkoly.

Přišel ti e-mail od banky.
V e-mailu se píše, že dlužíš 100 000 Kč.
Jsi si však jistý/á, že sis nikde peníze nepůjčoval/a.
V e-mailu se nachází číslo účtu,
na který máš zaslat peníze a odkaz,
na který se dá kliknout.
Jak se zachováš? Podle čeho si ověříš pravost informací?

Přečti si následující článek a popiš, co žena udělala špatně.

https://www.novinky.cz/clanek/krimi-dalsi-falesny-vojak-se-srdceryvnou-legendou-zena-z-nachodska-mu-poslala-dva-miliony-40407441

Příloha 8



Malware

Odpověz na následující otázky a vypracuj úkoly.

Propoj to, co se k sobě hodí.

Malware Spyware Trojský kůň Adware

Červ Virus Keylogger

na první pohled neškodný, ale hledá zadní vrátka

k šíření potřebuje hostitele

souhrnný název pro škodlivý software

zaznamenává údery na klávesnici

zobrazuje nevyžádané reklamy

dokáže se šířit samostatně

odesílá informace bez vědomí uživatele

Na internetu najdi alespoň 3 antiviry zdarma a vypiš je.

Jak budeš postupovat, když najdeš na ulici pohozenou "flashku"?

Příloha 9

Sociální sítě a kyberšikana

Odpověz na následující otázky a vypracuj úkoly.

Vypiš, jaké používáš sociální sítě.
Označ hvězdičkou tu, kterou používáš nejčastěji.

Proč tuto (označenou) sociální síť používáš?

Vypiš rozdíly mezi tradiční šikanou (v reálném životě)
a kyberšikanou (tou na internetu).
Možná ti poradí následující otázky.

Kde? **Jak může probíhat?** **Kdy?** **Víme, kdo je agresorem?**

Může šikanovat skupina lidí? **Proč?** **Mohou z ní být fyzická zranění?**

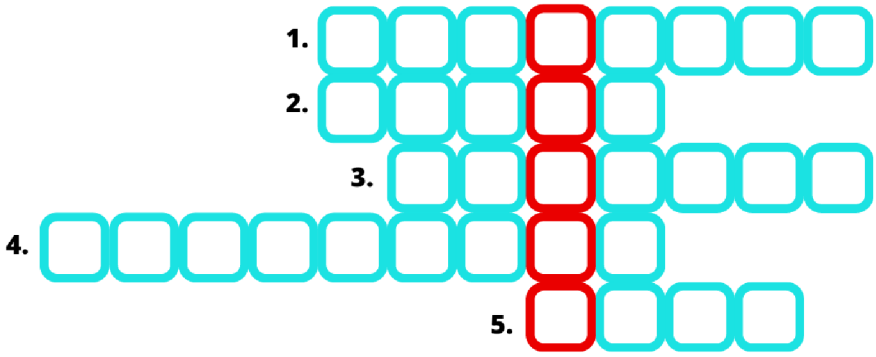
Příloha 10

Zabezpečení

Odpověz na následující otázky a vypracuj úkoly.

Vyplň křížovku.

1. **Mozek počítače.**
2. **Řada znaků určená k zabezpečení např. účtů.**
3. **Kůň patřící do rodiny malwarů.**
4. **Chrání nás před malwarem.**
5. **Může být pevný, externí, flash či kompaktní.**

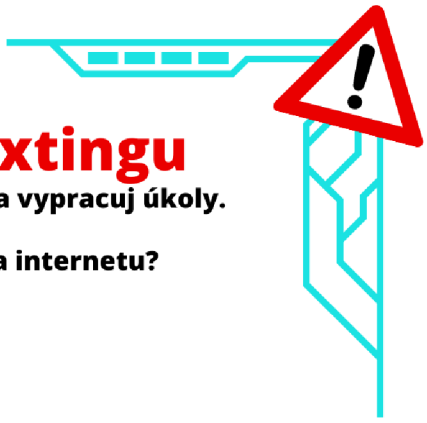


Popiš, na co poukazuje slovo z tajenky.

Jakým způsobem můžeme vytvořit poměrně bezpečné, ale zapamatovatelné heslo?

Napadají tě i jiné možnosti tvorby hesla?

Příloha 11



Nebezpečí sextingu

Odpověz na následující otázky a vypracuj úkoly.

Jak si ověříme uživatele na internetu?

Co je to "peer pressure"?

Kdo všechno musí souhlasit před navázáním sextingu?

Jaká jsou nebezpečí sdílení fotografií na internetu?

Příloha 12

Co jsou to dezinformace?

Kde se s dezinformacemi můžeme setkat? (uveď alespoň 3 možnosti)

Co je cílem HOAXů?

Uveď příklad nějakého HOAXu.:

Jak nazýváme informace, které mají za cíl někoho poškodit?

a) dezinformace b) misinformace c) malinformace

d) fake news e) propaganda f) hoax

Jak nazýváme neověřené informace, které někdo (neúmyslně) šíří jako pravdivé?

a) dezinformace b) misinformace c) malinformace

d) fake news e) propaganda f) hoax

Co v překladu znamená anglický termín „FAKE NEWS“?

S čím v současnosti nejčastěji spojujeme termín PROPAGANDA?

Příloha 13

Dotazník k proběhlé hodině *"Internetové lži"*

Dobrý den,

Jak již víte z proběhlé hodiny týkající se Dezinformací, první část tohoto krátkého dotazníku se bude týkat především **Vašeho názoru** na pracovní list, který jste vyplňovali. Ve druhé části pak naleznete několik otázek týkajících se Vašich zkušeností s probíraným tématem.

Stejně jako proběhlý test, budou i výsledky tohoto dotazníku součástí mé diplomové práce na téma *"Tvorba metodických návrhů se zaměřením na problematiku internetové bezpečnosti v kontextu informatických předmětů na 2. stupni ZŠ"*.

Tento dotazník je stejně jako proběhlý test **zcela anonymní**.

Předem děkuji za vyplnění a přeji pohodový zbytek dne,
Bc. Jan Sedláček

* Označuje povinnou otázku

Názor na pracovní list

1. Líbila se Vám grafická úprava pracovního listu? *

Označte jen jednu elipsu.

Spíše NE	
1	◯
2	◯
3	◯
4	◯
5	◯
Spíše ANO	

2. Byl pracovní list přehledný? *

Označte jen jednu elipsu.

Spíše NE

1 ◯

2 ◯

3 ◯

4 ◯

5 ◯

Spíše ANO

3. Byly otázky a úlohy napsané a vysvětlené srozumitelně? *

Označte jen jednu elipsu.

Spíše NE

1 ◯

2 ◯

3 ◯

4 ◯

5 ◯

Spíše ANO

4. Myslíte si, že pro Vás byla práce s pracovním listem přínosná? *

Označte jen jednu elipsu.

Spíše NE

1 ◯

2 ◯

3 ◯

4 ◯

5 ◯

Spíše ANO

5. Nalezli jste v pracovním listu něco, co byste rádi upravili či změnili?

6. Ohodnoťte (celkově) pracovní list známkou jako ve škole. *

Označte jen jednu elipsu.

◯ 1 - výborně

◯ 2 - chvalitebně

◯ 3 - dobře

◯ 4 - dostatečně

◯ 5 - nedostatečně

Předchozí znalosti

7. *Kde / jak* jste se před proběhlou hodinou dozvěděli o dezinformacích? *(můžete zvolit více odpovědí)* *

Zaškrtněte všechny platné možnosti.

- [ ] Ve škole
- [ ] Doma / od rodinných příslušníků
- [ ] Internet
- [ ] Televize
- [ ] Noviny
- [ ] Rádio / rozhlas
- [ ] Nikde
- [ ] Jiné: _____

8. Pokud jste zvolili možnost ***"Ve škole"*** - v jakém to bylo předmětu? *(můžete zvolit více možností)*

Zaškrtněte všechny platné možnosti.

- [ ] Český jazyk
- [ ] Cizí jazyk (angličtina, němčina atd.)
- [ ] Dějepis
- [ ] Zeměpis
- [ ] Matematika
- [ ] Informatika
- [ ] Fyzika
- [ ] Chemie
- [ ] Občanská výchova
- [ ] Tělesná výchova
- [ ] Výtvarná výchova
- [ ] Hudební výchova
- [ ] Pracovní činnosti
- [ ] Jiné: _____

Anotace

Jméno a příjmení:	Bc. Jan Sedláček
Katedra:	Katedra technické a informační výchovy
Vedoucí práce:	Mgr. Tomáš Dragon
Rok obhajoby:	2023

Název práce:	Tvorba metodických návrhů se zaměřením na problematiku internetové bezpečnosti v kontextu informatických předmětů na 2. stupni ZŠ
Název v angličtině:	Creation of methodological proposals with focus on the issue of Internet security in the context of computer science subjects at lower secondary schools
Anotace práce:	Tato diplomová práce se zaměřuje na tvorbu metodických návrhů se zaměřením na problematiku internetové bezpečnosti v kontextu informatických předmětů na druhém stupni základních škol. Teoretická část popisuje internet, nebezpečí internetu, zavedení informatiky ve školských dokumentech a plánování výuky. Praktická část se zabývá tvorbou a prezentací metodických návrhů, jejich ověřením a získáním zpětné vazby k vytvořeným pracovním listům.
Klíčová slova:	internet, nebezpečí internetu, plánování výuky, metodické návrhy, 2. stupeň ZŠ
Anotace v angličtině:	This diploma thesis focuses on the creation of methodological proposals with focus on the issue of Internet security in the context of computer science subjects at lower secondary schools. The theoretical part characterizes the Internet, the dangers of Internet usage, embedment of computer science in school documents and teaching planning. The practical part is focused on the creation and presentation of methodological proposal, their verification and getting feedback for created worksheets.
Klíčová slova v angličtině:	Internet, dangers of internet, teaching planning, methodological proposals, lower secondary school
Přílohy vázané v práci:	13 příloh: 11 pracovních listů, ověřovací test, dotazník
Rozsah práce:	79 stran + 16 stran příloh (96 stran)
Jazyk práce:	čeština