RIZIKÁ IKT – 1. HODINA

PRE KOHO SOM ZAUJÍMAVÝ/ZAUJÍMAVÁ?

Tematický celok /Téma	*ISCED /Odporúčaný ročník*
Komunikácia a spolupráca – práca s nástrojmi na komunikáciu; Informačná spoločnosť – bezpečnosť a riziká/***Riziká IKT – pre koho som zaujímavý/zaujímavá***: • pravidlá a odporúčania pre bezpečné profily, pre príjem správ/dokumentov a pre ochranu súkromia; rešpektovanie súkromia ostatných, • hrozby webových kontaktov s neznámymi ľuďmi, nekritické preberanie webového obsahu, • … .	**ISCED 2**/7. – 8. Ročník 1. vyučovacia hodina
Požiadavky na vstupné vedomosti a zručnosti	
• základy práce s počítačom, • ovládanie operačného systému na používateľskej úrovni, • základy práce v prostredí internetu, • základy používania elektronickej pošty (prijímanie/odosielanie správ),	
Ciele	
Žiakom osvojované vedomosti a zručnosti	***Žiakom rozvíjané spôsobilosti***
Analýza problému • **opísať vzťahy medzi informáciami vlastnými slovami,** • **uviesť kontra príklad, keď niečo neplatí, nefunguje,** • **uvažovať o rôznych riešeniach.** **Informačná spoločnosť – digitálne technológie v spoločnosti** • **digitálne technológie okolo nás.** **Hľadanie a opravovanie chýb** • **diskutovať a argumentovať o správnosti riešenia,** • **navrhnúť vylepšenie.** Analýza možných bezpečnostných rizík a problémov • opísanie ohrození elektronickej komunikácie, • pozitívne/negatívne príklady/vlastné skúsenosti, • možné/alternatívne bezpečné riešenia, tvorba a údržba bezpečného hesla. Digitálne riziká na internete • ne/bezpečné správanie sa na internete, • ne/poskytovanie osobných údajov/fotografií. Hľadanie bezpečných riešení • aplikovanie pravidiel a odporúčaní.	Informatické myslenie: • (LOG4) **vyvodzovať** (logicky zdôvodňovať) **závery** z **pozorovaní** a **experimentov** (aj myšlienkových), • (VZO3) **rozpoznať** rovnaké**/podobné vlastnosti/pravidlá správania** sa **v častiach rôznych** objektov/problémov/procesov (napr. časť jedného problému je časťou druhého problému), • (ABS1) **určiť**, ktoré detaily/prvky/vlastnosti/vzťahy objektov/problémov/procesov sú v danej situácii **podstatné** a ktoré môžeme zanedbať (objem motora <-> farba jeho náteru, prezentovanie informácií <-> nástroj na tvorbu prezentácií), • (VYH1) **vybrať kritériá** pre vyhodnotenie priebehu alebo výsledkov projektu/programu/algoritmu/situácie (napr. rýchlosť vykonania, bezpečnosť systému, náročnosť na zdroje, efektívnosť algoritmu, kvalita zdrojového kódu), • (VYH3) **posúdiť kvalitu/správnosť/efektívnosť/vhodnosť** objektu/systému/postupu/nástroja

	na základe **vybraných/definovaných kritérií** (napr. posúdiť efektívnosti algoritmov, posúdiť bezpečnosť systému, posúdiť správnosť dekompozície, posúdiť presnosť a úplnosť algoritmu/programu/postupu, testovať program/výrobok, posúdiť/dokázať pravdivosť tvrdenia).

Riešený didaktický problém

Problematika výchovy a vzdelávania na podporu rozvoja gramotnosti v okruhoch informačnej bezpečnosti je dnes do ZŠ vzdelávania začlenená plošne. Znamená to, že **každý žiak/absolvent daného stupňa vzdelávania musí byť s ňou v určenom rozsahu oboznámený** (nepostačuje realizácia len v časti triedy alebo v krúžkoch). **Osvojenie si podstaty gramotnosti v okruhoch informačnej bezpečnosti je veľmi dôležité.** Ak učiteľ pochopí, čo gramotnosťou v okruhoch informačnej bezpečnosti je (a čo nie je), lepšie vyberie spôsob výučby, tiež to, do ktorých predmetov/tém ju začlení a akú konkrétnu metódu/konkrétne metódy vo výučbe bude uplatňovať.

Webová komunikácia sa v súčasnosti stala už samozrejmým spôsobom medziľudskej komunikácie. Dostala sa aj do života žiakov základných škôl. Žiaci navzájom a aj so svojím učiteľom alebo rodičom pomerne často komunikujú prostredníctvom rôznych webových služieb. V tejto metodike vychádzame z analýzy výučby a hľadania prvkov, ktoré jednotlivý učiteľ vo vyučovaní presadzuje už teraz. Následne sa **zameriavame na prvky, ktoré je v záujme bezpečnosti potrebné do daného predmetu/tematického celku začleniť navyše**.

Dominantné vyučovacie metódy a formy	***Príprava učiteľa a pomôcky***
Bádateľsky orientovaná metodika 5E. **Sprievodnými metódami tém bezpečnosti** sú: • Inscenačné metódy – založené na simulácii a hraní rolí. Sú jednou z možností, ako žiakov vtiahnuť do bezpečnostnej informatickej problematiky. Je možné tak rozvíjať bezpečnostné stratégie, ale zároveň nepracovať s citlivými údajmi. Aj z tohto dôvodu majú tieto metódy vo vzdelávaní v otázkach informačnej bezpečnosti široké uplatnenie. Umožňujú hlbšie porozumenie vzdelávaciemu obsahu, ale sú vhodné aj/najmä pre rozvoj sociálnych zručností, kedy sa žiaci učia rozhodovať. • Situačné metódy – majú veľmi blízko k životnej realite. Ich podstatou je riešenie istej problémovej bezpečnostnej situácie, ktorá je zrkadlom skutočnej udalosti. Žiaci potom používajú svoje vedomosti a zručnosti, pracujú s informačnými zdrojmi, ale zohľadňujú aj svoje skúsenosti, názory a postoje. Spoločne diskutujú o možných (bezpečných, najbezpečnejších) riešeniach, posudzujú/hľadajú ich výhody a nevýhody a rozhodujú sa pre najlepšie riešenie.	**a) Pracovný list 1.** **b) Pracovný list 2.** **c) Pracovný list 3.** **d) Pracovný list 4 – Sebahodnotenie.**

Diagnostika splnenia vzdelávacích cieľov

Sebahodnotiaci test (viď. **Pracovný list 4**).