

Posudek vedoucího diplomové práce

Název: Základy kryptografie jako téma výuky informatiky na 2. stupni ZŠ
Autor: Bc. Sabina Hájková
Vedoucí: PhDr. Michal Musílek, Ph.D.
Oponent: doc. RNDr. Štěpán Hubálovský, Ph.D.

Práce volně navazuje na bakalářskou práci diplomantky s názvem Luštění transpozičních šifer s podporou počítače, která se zabývala vybranými transpozičními šiframi, především jednoduchou sloupcovou transpozicí s úplnou tabulkou a Fleissnerovou otočnou mřížkou, jejich principem, vlastnostmi, postupy šifrování a dešifrování a metodami jejich luštění. Výsledky této bakalářské práce v diplomové práci využívá jen částečně, výrazně je rozšiřuje a doplňuje je o obecně pedagogický a oborově didaktický pohled.

Vlastní práce má 51 stran textu, doplněného 23 stranami příloh. Text je stručný, jasný a výstižný. V úvodu autorka vhodně formuluje cíle práce a stanovuje kontrolovatelná kritéria jejich splnění. Teoretická část práce podává nejprve přehled všech podstatných základních pojmů souvisejících s tématem práce, zabývá se formami a metodami výuky s důrazem na aktivizující metody, pokračuje přehledem typů ručních šifer (tedy nejen transpozičních, ale i substitučních), grafických systémů a steganografických metod. Tuto část práce uzavírá zhodnocením přínosu výuky kryptologie pro rozvoj logického a kritického myšlení, budování mezipředmětových vztahů informatiky s dějepisem, matematikou, výtvarnou výchovou a jazyky a pro podtržení významu tématu počítačové bezpečnosti.

Velmi zajímavě je postavena empirická část práce, která popisuje dotazníkové šetření mezi žáky vybrané základní školy, které mělo za cíl zmapovat předpoklady a motivovanost respondentů k luštění šifer. Protože luštění šifer není obvyklým koníčkem ani u dospělých, natož u dětí, zaměřila autorka pozornost výzkumu především na luštění křížovek a osmismerek a dalších klasických „slovních hádanek“, přičemž zjišťovala nejen samotný fakt, zda žáci křížovky a osmisměrky luští, ale také, zda je to baví, jaký způsob luštění preferují, který typ „slovních hádanek“ mají nejraději apod. Otázky na vybrané kryptologické pojmy se v dotazníku také objevují, ale jsou spíše doplňkem. Tento přístup se mi zdá být velmi chytře zvolený, podává totiž ucelenou výchozí představu pro stavbu následující praktické části práce.

Praktickou částí a prakticky použitelným výstupem práce je příprava na dvojici vyučovacích hodin z nichž první je věnována seznámení žáků se základními pojmy kryptologie a s různými typy ručních šifer a druhá má podobu hry *Cesta za pokladem*, kde k postupu na další krok je vždy třeba vyluštit konkrétní šifrový text, případně obrázek (grafickou šifru). K přípravě na první vyučovací hodinu se váže pečlivě připravená počítačová prezentace, k přípravě na druhou hodinu sada pracovních listů. Obě hodiny byly také realizovány v rámci souvislé praxe studentky a byly následně vyhodnoceny a porovnány v rámci dvou skupin žáků. Experimentální skupina žáků 6. ročníku ZŠ absolvovala obě vyučovací hodiny, zatímco kontrolní skupině žáků 7. ročníku ZŠ byla hra *Cesta za pokladem* předložena bez předchozího seznámení s různými typy šifer. Zajímavý byl výsledek experimentu, kdy žáci 7. ročníku zvládali úkoly o něco lépe, přestože neabsolvovali přípravnou vyučovací hodinu. Autorka práce vyslovuje hypotézu, že by to mohlo být způsobeno rozvojem abstraktního myšlení právě v tomto období psychického vývoje dítěte, a přestože by tato hypotéza zasloužila ověření, je velmi pravděpodobné, že do značné míry správně vystihuje skutečnost.

V závěru práce autorka konstatuje splnění vytyčených cílů a diskutuje závěry provedeného dotazníkového šetření a experimentální výuky. Celá práce má dobrou grafickou úroveň.

Rozsah práce: 51 stran textu, 23 stran příloh
Formální úprava: odpovídá vnitřním předpisům UHK
Logická struktura: práce je vhodně členěna do kapitol a podkapitol
Bibliografické citace: odpovídají normě ČSN ISO 690, 8 zdrojů různého typu (knihy, články v časopisech, články ve sbornících, on-line zdroje)
Cíle práce: cíle práce jsou jasně deklarovány v úvodu práce, v závěru práce autorka konstatuje jejich splnění

Z hlediska vlastního přínosu autorky je kvalitní jak empirická, tak praktická část práce. Na základě předložené práce konstatuji, že autorka splnila vytyčené cíle. Práci doporučuji připustit k obhajobě a navrhuji hodnocení A.

V Hradci Králové dne 15. 4. 2017