POSUDEK VEDOUCÍHO DIPLOMOVÉ PRÁCE "BEZPEČNOST ELEKTRONICKÉHO HLASOVÁNÍ"

BC. PETRY FRITZOVÉ

1. Formulář

Matematická úroveň: vynikající, velmi dobrá, **průměrná**, podprůměrná, nevyhovující;
Grafická, jazyková a formální úroveň: vynikající, **velmi dobrá**, průměrná, podprůměrná, nevyhovující;
Výsledky: originální, původní i převzaté, **netriviální kompilace**, citované z literatury, opsané;
Použité metody: nestandardní, **standardní**, obojí;
Aplikovatelnost: přínos pro teorii, **přínos pro praxi**, přínos pro praxi i teorii, bez přínosu, nedovedu posoudit;
Věcné chyby: téměř žádné, **vzhledem k rozsahu a pojednávanému tématu přiměřený počet**, méně podstatné četné, závažné;
Tiskové chyby: **téměř žádné**, vzhledem k rozsahu a pojednávanému tématu přiměřený počet, četné;
Celková úroveň práce: vynikající, **velmi dobrá**, průměrná, podprůměrná, nevyhovující;

Práci **doporučuji** uznat jako diplomovou. Návrh klasifikace přikládám na zvláštním papíru.

2. Připomínky a vyjádření vedocího práce

V první kapitole autorka nejprve popisuje obecné principy a standardně používané metody kryptografie. Po té diskutuje bezpečnostní hrozby, zejména internetové komunikace. Druhá kapitola je pokusem o definici ideálního volebního systému pomocí vlastností, které by měl takový systém splňovat a následnou diskuzí vzájemného vztahu těchto vlastností. Třetí kapitola je popisem elektronického volebního systému SERVE. Ve čtvrté kapitole se studentka detailně věnuje volebnímu systému v Estonsku. V páté pak autorka srovnává oba předchozí systémy a ideální volební systém definovaný ve druhé kapitole. Nakonec rozebírá možné útoky na tyto systémy a navrhuje způsoby jak se jim bránit.

V práci jsou popsány principy jednotlivých volebních systému, útoků na slabá místa používané internetové komunikace nebo z toho odvozených útoků na navržené volební systémy. Není to detailní matematický popis. Přesto se ale domnívám, že se zakládá na dobrém porozumění problematice. V případě popisu možných útoků v první kapitole také na dobré znalosti principů počítačových sítí. Podobně diskuze jednotlivých vlastností volebního systému ve druhé kapitole je sice elementární, ale ne triviální. Popisy systémů SERVE a volebního systému v Estonsku odpovídají

dosažitelné literatuře. Mohu-li hodnotit přístup studentky, byl jsem s ním velmi spokojen.

V Praze dne 10.5.2013
Mgr. Pavel Růžička, Ph.D.