POSUDEK VEDOUCÍHO BAKALÁŘSKÉ PRÁCE

Jméno a příjmení autora:	**Jana Soukupová**
Název práce:	**Softwarové zabezpečení dat**

I. Volba tématu:

1. mimořádně aktuální
2. aktuální, málo frekventované
3. aktuální, pracné
4. frekventované s dostatkem literatury

II. Cíl práce a jeho naplnění:

1. vhodně zvolený cíl, který byl naplněn
2. vhodně zvolený cíl, částečně naplněn
3. vhodně zvolený cíl, který nebyl naplněn
4. nevhodně zvolený cíl

III. Struktura práce:

1. originální – zdařilá
2. logická – systémová
3. logická – tradiční
4. pro dané téma tradiční
5. pro dané téma nevhodná

IV. Práce s literaturou:

1. vynikající, použity dosud neběžné prameny
2. velmi dobrá, použity nejnovější dostupné prameny
3. dobrá, běžně dostupné prameny
4. slabá, zastaralé prameny

V. Vybavení práce (data, tabulky, grafy, přílohy):

1. mimořádné, funkční
2. velmi dobré, funkční
3. odpovídá nutnému doplnění textu
4. nedostačující

VI. Přínosy práce:

1. originální, inspirativní názory
2. ne zcela běžné názory
3. vlastní názor argumentačně podpořený
4. vlastní názor chybí

VII. Uplatnění práce v praxi a ve výuce:

1. práci lze uplatnit v praxi
2. práci lze uplatnit ve výuce
3. práce nelze příliš využít ani v praxi ani při výuce

VIII. Formální stránka:

1. výborná
2. přijatelná
3. nevyhovující

IX. Jazyková stránka

1. stylistika
   a) výborná
   b) velmi dobrá
   c) dobrá
   d) nevyhovující

2. gramatika
   a) výborná
   b) dobrá
   c) nevyhovující

X. Zásadní připomínky k práci: **1. nemám**

XI. Další hodnocení:

Autorka ve své bakalářské práci představuje ty z možností zabezpečení počítačových dat, které jsou běžně dostupné pro kteréhokoliv uživatele výpočetní techniky, ale které jsou začasté zcela na okraji jeho zájmu. Důležitost ochrana vlastních dat se pak bohužel často v plné nahotě objeví až v okamžiku, kdy je uživatel okraden o svůj počítač, nebo kdy „pouze" ztratí svůj USB disk.

Předložená práce má tradiční, logickou strukturu. Na začátku autorka zavede pojmy a základní terminologii, seznámí čtenáře s historií kryptologie a představí současný stav. Zabývá se přitom základními technologiemi a algoritmy, přičemž ale (správně pro účely bakalářské práce) nezabíhá do zvláštních podrobností.

Hlavní část práce pak tvoří představení několika nástrojů, které jsou pro (v teoretické části představené) šifrování a ochranu dat vhodné pro obyčejného smrtelníka. Autorka se přitom zabývá různými typy aplikací: TrueCrypt pro šifrování celých disků nebo diskových oddílů, SecurEngine jako představitele steganografických nástrojů či PGP (resp. GPG) jako nástroje, který kvalitní šifrování dat na principu dvojice veřejný-soukromý klíč přinesl mezi obyčejné uživatele počítačů. Autorka popisuje možnosti (a zejména vhodnost nasazení) jednotlivých nástrojů a je zřetelně vidět, že se jim skutečně prakticky věnovala. Na závěr pak nezapomíná ani na velmi širokou problematiku bezpečnosti hesel, kdy jednak uvádí základní principy tvorby hesel, jednak také představuje aplikace pro generování/správu/odhalení počítačových hesel.

Osobně bych zejména praktickou část práce doporučil všem, kteří si alespoň trochu dokáží představit, jak cenná jsou jejich data, a chtěli by se dozvědět, co pro jejich ochranu mohou udělat; a bohužel, takových uživatelů výpočetní techniky je dodnes drtivá většina…

Z hlediska stylistiky i gramatiky je práce na dobré úrovni, autorka píše lehkým (někdy možná až příliš) stylem, který se velmi dobře čte. Dobrá je i práce se zdroji a také kvalita doprovodných grafických objektů je dobrá.

Vzhledem k výše uvedeným faktům mi nezbývá, než navrhnout hodnocení práce stupněm „výborně" a těšit se na budoucí možné rozpracování do podoby již více teoreticky zaměřené diplomové práce.

Datum: 1. 6. 2007 **Podpis vedoucího práce: Jiří Přibil**