Oponentský posudek

Ve svém oponentském posudku se zabývám disertační prací pana Ing. Vratislava Žáčka, nazvanou „Prototyp digitalizovaného symptomatického systému".

Cílem práce je vytvoření prototypu webové aplikace zaměřené na diagnostiku škodlivých organismů dle symptomů poškození hostitelské rostliny. Autor neuvádí komu je tato aplikace určena ale z ukázky diagnostického klíče se domnívám, že mělo jít o širokou zemědělskou veřejnost. Zvolené téma považuji za velmi aktuální a přínosné. Podobné webové aplikace budou mimo jiné dobře využitelné v rámci připravovaného portálu „Rostlinolékař".

Literární přehled je zaměřen převážně na citace z oblasti informatiky, které jako fytopatolog nejsem schopen objektivně posoudit. Přesto mě napadá jedna otázka. Z literatury vím, že existují četné pokusy využít pro diagnostické a expertní systémy technologie neuronových sítí, v posuzované práci ale není tato technologie zmíněna.

Kapitoly věnované metodice a výsledkům jsou podrobným popisem systému a návodem k jeho využití, který mohu jen těžko kriticky posoudit. Zaměřím se proto spíše na ukázková dat, kterými je systém naplněn.

Vložená data představují kompilaci různých textů, často bez přímé souvislosti. Například u krytonosce čtyřzubého se v záložce „prognóza a signalizace" doporučuje pozorování v Möríckeho miskách ale indikace ochrany je založena na počtu brouků na 1 m^2. U většiny uvedených škodlivých organismů chybí navigační menu nebo některá z jeho standardních záložek. Předpokládám, že je to v případech, kdy se autorovi nepodařilo získat odpovídající informace.

Považuji také za vhodné aby u položek „prognóza" „pozorovací bod" aj. byly přímo odkazy na vhodné webové aplikace. Například u položky „pozorovací bod" je uveden popis pozorování, které je prováděno v rámci monitoringu SRS ale chybí zde příslušný odkaz na výsledky tohoto monitoringu.

Určité výhrady mám také k určovacímu klíči. Jsou zde uvedeny obecné definice jednotlivých symptomů ale uživatel hledá nepochybně popis symptomů v souvislosti se specifickým projevem na zvolené rostlině nebo její části. Čím je například charakteristická korová nekróza na stonku řepky apod. Některé symptomy vyžadují další, podrobnější úroveň popisu. Například skvrnitost listů končí v podstatě obrazovým atlasem chorob a uživatel je odkázán ve svém konečném rozhodnutí na ne vždy zcela zdařilé fotografie. Nicméně je třeba uznat, že

autor tímto způsobem získal nástroj, použitelný s minimálními úpravami pro celou řadu zemědělských plodin.

Za velmi dobře a nápaditě zpracovaný považuji modul věnovaný ekotoxikologii.

Na celém systému mě naopak vadí poměrně náročný způsob pořizování a vkládání informací. Nebylo by možné některé údaje přebírat z odpovídajících databází? Mám na mysli například informace o účinných látkách přípravků.

V kapitole závěr a diskuse postrádám porovnání vzniklé aplikace s obdobnými webovými aplikacemi a přehledný výčet přínosů, které přináší pro řešení zvolené problematiky.

Není pro mě jednoduché oponovat tento typ disertační práce. Nejedná se zde o provedení experimentu a příslušnou interpretaci výsledků tak, jak jsme na to v oboru rostlinolékařství zvyklí. Napadlo mě, zda by se autor s touto disertační prací neměl ucházet o vědecký titul spíše v oboru informatiky než v oboru ochrany rostlin.

Faktem ale zůstává, že Ing. Žáček velmi dobře splnil zadání a cíl disertační práce a skutečně vytvořil vhodný prototyp diagnostického a faktografického systému, který po naplnění odpovídajícími daty a odkazy bude vyhledávanou internetovou položkou zemědělců.

Ve svém oponentském posudku jsem se zaměřil na kritické výhrady, především pokud jde o ukázku dat. Tyto výhrady ale nejsou v tomto případě podstatné a nemění nic na tom, že disertační práci pana Ing. Vratislava Žáčka hodnotím jako zdařilou a souhlasím aby byla přijata k obhajobě a po jejím úspěšném obhájení byl jmenovanému přiznán akademický titul „PhD".

V Brně dne 11.6.2007

Ing. Rostislav Hrubý, CSc.

Posudek na doktorskou disertační práci Ing. Vratislava Žáčka na téma: „Prototyp digitalizovaného symptomatického systému“

Formální úprava disertační práce

Předložená disertační práce má celkem 98 stran[1] a je standardně členěna na šest hlavních kapitol: úvod, literární rešerše, metodika, výsledky, závěr a diskuse a literatura. Proporce jednotlivých kapitol odpovídají běžným zvyklostem pro psaní vědeckých prací i když vzhledem k tomu, že stěžejním výsledkem práce je počítačová aplikace přístupná na internetu, mohl být rozsah kapitoly výsledky zredukován na nezbytné minimum. Kromě úvodu a dvou posledních kapitol jsou jednotlivé kapitoly dále členěny s využitím číslování jednotlivých oddílů a to až do páté úrovně. V některých případech je tento způsob členění až příliš jemný a oddíl pak představuje pouze jeden odstavec o třech řádkách. Velký počet číslovaných oddílů pak vedl k méně přehlednému třístránkovému obsahu. Naopak barevné odlišení názvů oddílů v textu usnadňuje orientaci. Po formální stránce je disertační práce na velmi vysoké úrovni a graficky je výborně zpracována.

Specifické poznámky k obsahu disertační práce

Zvolené téma je velmi zajímavé a má velký praktický přínost. Není pochyb, že požadavky na obdobné digitální informační systémy budou v nejbližší budoucnosti přibývat. Autor vytvořil prototyp, který lze univerzálně použít v různých oblastech ochrany rostlin. Poněkud komplikovaně vypadá název systému a domnívám se, že by jej bylo možno zjednodušit (např. vypuštěním slova faktografický, neboť slovo informační dostačuje pro popis). Spíše by v názvu měla být zdůrazněna skutečnost, že se jedná o systém pro škůdce a choroby rostlin.

Literární rešerše je věnována zejména informatice, databázovým systémům a určovacím klíčům a v závěru je na konkrétním příkladu řepky olejky uvedena diagnostika škodlivých činitelů. Vzhledem k tomu, že se jedná o disertační práci v oboru rostlinolékařství, zdá se mi, že je až příliš velký důraz v rešerši kladen na informatiku obecně a čtenář může mít problém s hledáním souvislostí textů a cílem práce. Např. definice jednotlivých pojmů jako je SQL či PHP je jistě potřebná, ale chybí informace, zda už těchto prostředků bylo někde v oboru rostlinolékařství použito nebo alespoň proč jsou právě vhodné pro vytvoření digitalizovaného symptomatického systému. Také by bylo možné tuto kapitolu doplnit o některé další expertní systémy navržené pro rostlinolékařství, např. (Woolley and Stone 1987, Kemp et al. 1989, Yialouris and Sideridis 1996, Kaloudis et al. 2005).

[1] Práce je psána základním řádkováním, při přepočtu na tzv. normostrany by byl rozsah práce ještě větší.

V kapitole metodika je popsána aplikace systému pFIDiS. Členění aplikace na jednotlivé moduly je velice žádoucí. Kromě větší přehlednosti toto modulární uspořádání usnadňuje i administraci celého systému. Název modulu Mapa vývojových stádií je poněkud problematický. Snad by byl vhodnější název Vývojový cyklus. Kladně lze hodnotit, že celý systém je vybudován na tzv. „open source" programových prostředcích, ačkoliv autor nijak nezdůvodňuje, proč si vybral právě uvedené nástroje a nezvolil jiné. Validace napsaného kódu pomocí W3C validátorů je počin nadmíru záslužný. Ne každý má totiž možnost či ani nechce používat poslední verzi MSIE a kompatibilita s ostatními prohlížeči je nutná. Programátoři si často zjednodušují práci tím, že svůj program optimalizují a odladí pouze pro jeden prohlížeč. V modulu bibliografické databáze jsou uloženy údaje stažené z komerčních databází. Samozřejmě pro osobní potřebu je to korektní, avšak zveřejňování těchto údajů včetně abstraktů a dokonce celých článků na internetu může narazit na problém s autorskými právy.

Kapitola výsledky je podrobných popisem struktury a fungování systému. Částečně se překrývá s předchozí kapitolou o metodice. Systém jsem měl možnost si vyzkoušet on-line a měl bych pouze několik následujících poznámek. Poněkud se vytrácí smysl registrace, když se registrovaný uživatel následně dozví: „bohužel Vaše práva jsou minimální" a lze pouze poslat komentáře správci systému. Buď by měl být přístup k informacím pro neregistrované omezen a tak uživatelé motivováni k registraci - to pro případ, že správce chce mít přehled o uživatelích nebo by měla být registrace odstraněna s výjimkou přístupu pro správce a editory dat. Další připomínka se týká obrázků rostliny v levé nabídce v rámci diagnostického modulu. Tyto obrázky jsou příliš malé a špatně rozlišitelné, tedy alespoň na mém monitoru (15 palců, rozlišení 1024x768 bodů, prohlížeč Mozilla Firefox) se tak jevily. Dále jsem si všiml poněkud archaického jazyka v textu, např. „V době silnějšího rozmnožení bývá jich na květech řepky černo a v jediném kvítku často nalezneme i deset broučků". K tomu pravděpodobně došlo doslovným přepisem ze starší literatury. U listu škodlivého činitele je nadbytečná informace o rodu, neboť rodové jméno je již součástí vědeckého jména. V části bionomie nebo popis škodlivého činitele jsou často odkazy na literaturu a je škoda, že tyto odkazy nejsou propojeny s úplnou citací, tj. není hyperlink na modul použitá literatura nebo bibliografie. Usnadnilo by to hledání. Citace, které jsou uloženy a spravovány pomocí programu JabRef[2] představují velký zdroj informací, avšak nejsou součástí systému pFIDiS, což je škoda i když na druhé straně by zde mohl být problém s autorskými právy, jak zmiňuji výše.

Kapitola Závěr a diskuse zaujímá tři strany textu. Je však škoda, že autor vlastně nediskutuje svůj systém s literárními zdroji - v diskusi není jediná citace. Logická posloupnost by měla být obrácená, tedy nejprve diskuse, z níž by měly vzejít závěry - co se liší, v čem je prototyp systému lepší a také jaké jsou výhledy rozšíření a uplatnění systému ať už komerční nebo nekomerční. S tím je spojena i otázka autorských práv, administrace, vývoj dalších jazykových mutací (doporučil bych přeložení systému zejména do angličtiny). Byl bych rád, kdyby vytvořené dílo neza-

[2]Ačkoliv to autor nikde nezmiňuje, jde o grafické prostředí pro správu bibliografické databáze ve formátu systému BibTeX, který např. umožňuje automatické generování seznamu použité literatury při sazbě dokumentu volně dostupným programem LaTeX.

padlo a stalo se vyhledávaným zdrojem informací rostlinolékařů, studentů i zájemců z řad laické veřejnosti nejen u nás, ale i v zahraničí. K tomu může přispět i dosud chybějící publikace v mezinárodním recenzovaném, nejlépe impaktovaném časopise, např. *Computers and Electronics in Agriculture* vydávaný nakladatelstvím Elsevier.

Závěrečné shrnutí

Jedná se o kvalitní doktorskou disertační práci, která sice nepřináší nová experimenální data avšak její výstup v podobě internetové aplikace jistě nalezne mnoho uživatelů. Autor zpracoval zadané téma na velmi dobré úrovni a proto doporučuji předloženou práci k obhajobě.

Literatura

Kaloudis, S., Anastopoulos, D., Yialouris, C., Lorentzos, N. and Sideridis, A. 2005. Insect identification expert system for forest protection. Expert Systems Appl. 28: 445–452.

Kemp, R. H., Stewart, T. M. and Boorman, A. 1989. An expert system for diagnosis of pests, diseases and disorders in apple crops. New Zealand Journal of Crop and Horticultural Science 17(1): 89–96.

Woolley, J. and Stone, N. 1987. Application of artificial intelligence to systematics: systex - a prototype expert system for species identification. Syst. Zool. 36(3): 248–267.

Yialouris, C. and Sideridis, A. 1996. An expert system for tomato diseases. Comp. Electr. Agric. 14: 61–76.

R. Zemek

R. Zemek

V Českých Budějovicích
dne 15.6.2007

Ing. Rostislav Zemek, CSc.

Oponentský posudek

disertační práce

PROTOTYP DIGITALIZOVANÉHO SYMPTOMATICKÉHO SYSTÉMU

Autor práce: Ing. Vratislav Žáček

Posudek zpracovala: Doc. Ing. Evženie Prokinová, CSc.

Předložená disertační práce ing. V. Žáčka se zabývá vývojem programu využitelného mimo jiné pro diagnostiku poškození rostlin, jako modelovou rostlinu si autor vybral řepku. Vzhledem k tomu posuzuji pouze část práce týkající se uvedených údajů o konkrétních poškozeních řepky a výsledný program posuzuji výhradně jako jeho případný uživatel.

Autor pečlivě zpracoval část Literární přehled. Od věci se mi jeví informace uvedené v kapitole 2.7, ale jejich uvedení určitě není na škodu. Informace uvedené v kapitole literární přehled považuji za velmi užitečné pro celou odbornou veřejnost. V práci je též přehledně uveden návod k používání programu.

K vlastnímu výslednému programu mám následující připomínky:

- v odkazu podle výběru původce poškození rostliny konstatuji nejednotné členění: u některých původců jsou uvedeny informace v kategoriích diagnostika, prognóza a signalizace a bibliografie, u některých je jen jedna z uvedených kategorií nebo dokonce žádná. Jestliže jde o otevřený systém, který má být doplňován – jak autor uvádí – mělo by členění být všude stejné, i s tím, že někde bude dočasně pouze uvedeno, že informace zatím není k dispozici, sledování se neprovádí apod.
- autor jako základní zdroj informací pro informace o původcích použil publikace z let 1956 (Miller F.), 1959 a 1962 (Baudyš a kol.). Tyto publikace jsou jako celek doposud skutečně nepřekonané, ale řada informací v nich je již zastaralá a neodpovídá skutečnosti. To vedlo k tomu, že jsou uvedeny faktické chyby. Např. není pravda, že bejlomorka kapustová není schopna klást vajíčka do nepoškozených šešulí – to neodpovídá potvrzené skutečnosti, u černě řepkové chybí údaj o možnosti přenosu osivem, resp. se uvádí, že se osivem nepřenáší, což není pravda. Není jasně uveden příznak na listech. U fomové hniloby je diskutabilní zařazení obrázku č. 4 – není typický pro fomovou hnilobu, ale pro botrytidu. U *Sclerotinia sclerotiorum* se uvádí, že sucho snižuje výskyt choroby, což není pravda – viz i letošní rok. U *Botrytis cinerea* se uvádí, že ochrana není – všichni pěstitelé ale vědí, že přípravky určené proti *S. sclerotiorum* mají vedlejší účinek i proti *B. cinerea*. Mimo to by zde vzhledem ke koncepci práce zmínka o ochraně ani neměla být. Dále se zde uvádí jako jeden z možných způsobů šíření botrytidy přenos sadbou, což mi u řepky připadá kuriózní. U dvou ze tří obrázků k cylindrosporióze řepky je chybně uvedeno cilindrosporióza. *Peronospora brassicae* není již řadu let řazena do říše Fungi. Fakt, že to některé servery a informační zdroje nerespektují není důvod k tomu jejich chybu opakovat a dále šířit. Také u tohoto patogena chybí zmínka o přenosu osivem. Popis *Pseudocercosporella capsellae* je velmi nepřesný. Podle mého názoru je diskutabilní i

zařazení obrázků, i když v tomto případě autor pouze převzal již určené fotky a případná záměna tedy není jeho vina. Konstatuji ale značnou nepřesnost vyjadřování – nepřezimuje choroba, ale patogen, spory netvoří skvrny, ale houba. V běžné mluvě se sice běžně užívá výrazů tak, jak je použil i autor práce, v oficielním odborném textu jde ale o chybu. U řady původců, resp. chorob či škůdců nejsou uvedeny další rostliny, na kterých mohou škodit, přesto že příslušná část je na stránce vidět. To si lze vyložit i tak, že uvedené organismy škodí pouze na řepce.

- Hledání příznaků podle lokalizace na rostlině je značně zavádějící. Např. při volbě „stonek" se objeví nabídka: symptomy vyvolané škůdci, odumírání, znaky patogena, změna tvaru, změna zbarvení. Za prvé, odumírání, změna tvaru a (nebo) barvy mohou být také vyvolány škůdci. Mimo to postrádám popis poškození sáním. Pod heslem odumírání je nekróza a na dalším obrázku kolonie mšic? Pod heslem znak patogena jsou nepopsané obrázky – zde by měly být obrázky s popisem: mycelium, sklerocium, pyknidy, ... U změny tvaru je jen praskání stonků. Zelenokvětost, hálky nejsou změnami tvaru? Pod heslem změna zabarvení nejsou diskolorace, ale nekrózy.
- Ve výčtu původců poškození, resp. chorob chybí padlí.
- Při volbě „kořen" – povlaky se objeví obrázek nekrózy, praskání pletiv.

Podobné nedostatky lze najít i u dalších hesel, není účelem posudku je vypisovat po jednom.

Zařazení bibliografie k jednotlivým původcům poškození rostlin je určitě pozitivem práce, ale domnívám se, že vzhledem k charakteru prací (vědecké, odborné) a jejich četnosti bude aktualizace této části systému velmi problematická a zbytečně náročná. Pro nalezení relevantních prací existují uživatelsky jednodušší cesty.

Vysoce oceňuji zařazení informací z ekotoxikologie. Bylo by užitečné v tomto směru doplnit údaje i z jiných zdrojů.

Autor uvádí, že cílem systému není poskytovat informace o možnostech ochrany. Zde odkazuje uživatele na stránky Státní rostlinolékařské správy. Odkaz je ale na Registr přípravků na ochranu rostlin, což je část, ve které se pěstitel požadovanou informaci nedozví. Měl by zde být odkaz na Přípravky na OR – registrace – Věstník.

K práci mám následující dotazy:

- jestliže autor předkládá prototyp otevřeného systému, o kterém předpokládá široké využití, proč jeho funkci omezuje vybavením ZF JU?

- systém počítá s účastí více administrátorů a editorů. Jak bude zajištěna faktická správnost vkládaných údajů? (Bez toho by systém nebyl dostatečně validní a tedy použitelný).

Přestože je autor absolventem ZF JU oboru rostlinolékařství, orientuje se na práci programátora. Nepřesnosti a chyby v textu naznačují, že autor se vlastním oborem příliš nezabýval. To jistě není zásadní chyba, ale domnívám se, že práce zabývající se vývojem databázového programu nespadá do oboru Rostlinolékařství a to ani v případě, že modelovým objektem je polní plodina a její poškození. Podle mého soudu jde spíše o informatiku. (Zcela něco jiného jsou samozřejmě systémy prognózy a signalizace škodlivých činitelů, epidemiologické modely, … které jsou nedílnou součástí oboru a při jejichž tvorbě musí autor prokázat hluboké znalosti oboru). Protože podstatou práce je vývoj databázového programu, domnívám se, že by alespoň jeden z oponentů měl být specialista – programátor.

Práce má velmi dobrou grafickou úpravu, je přehledná. Také jazyková úroveň je odpovídající, až na několik překlepů (z nich doporučuji opravit „molibden").

Autor si vytyčil nelehký úkol vypracovat systém, který by výrazně rozšířil informační zdroje v oboru Rostlinolékařství. V zásadě je předložený prototyp pro daný účel využitelný. Ve fázi, v jaké je předložen, je však pro laika zatím nepoužitelný a pro specialistu nerelevantní, s faktickými chybami, nepřesnou terminologií. Prototyp by měl být pro jednu modelovou rostlinu plně dokončený, bez chyb, s informacemi aktuálními v době dokončení práce.

Předložená disertační práce odpovídá požadavkům zákona č. 111/1998 Sb., o vysokých školách ve znění pozdějších předpisů, § 47, odst. 4. Práci doporučuji opravit, doplnit. Doporučuji i přihlédnout k připomínkám programátorů, které nejsou součástí tohoto posudku a byly autorovi poskytnuty samostatně. Po odstranění nedostatků doporučuji práci k obhajobě.

V Praze 17. 5. 2007

Doc. Ing. Evženie Prokinová, CSc.

2.3.3 – databáze

Poněkud nepřesná terminologie. Autor spojuje relační model s jeho fyzickou realizací. Na úrovni relačního modelu lze hovořit pouze o relaci, jejích atributech a doménách atributů. Pojmy entita, vztah a atribut patří do definice ERA modelu. Termíny Tabulka, sloupec, řádek (záznam) jsou konečnou realizací na úrovni fyzického DB systému. Jednotlivá označení nelze mezi sebou takto jednoduše vzájemně převádět, jde o různé věci. Autor vychází z fyzického schématu databáze a snaží se k nim přiřadit odpovídající ERA a relační pojmy. Takto to ovšem nelze jednoduše provést, otázka převodů je mnohem složitější. Nelze říci, že entita vždy odpovídá tabulce. Už vůbec neplatí, že atribut = entita.

2.5.3

Chybí zmínka o MySQL5, který existuje od 12/2005. Poskytuje všechny funkce, které postrádá v posledním odstavci kapitoly 2.5.3. MySQL5 je nyní použitelný (a používá se) i pro značně rozsáhlé a složité systémy.

3.2 – volba softwaru

Kombinace Apache 1.3.33, MySQL verze 3.23.56, PHP 4.3.10-2 je velmi zastaralá a pro daný účel nevhodná. Zřejmě za to nemůže autor – vybavení serveru je věcí katedry. Každopádně autor si měl zajistit provoz na odpovídajícím současném stroji a aplikaci psát pro něj. Jsou zde velké otazníky zejména ohledně databáze MySQL 3.x.x a víceuživatelského přístupu.
V situaci, kdy více než jeden uživatel budou zároveň editovat stejnou věc, dojde ke kolizi a poškození integrity dat. Navíc MySQL 3 vůbec neposkytuje ani základní databázové nástroje pro kontrolu správnosti dat vkládaných aplikací.
V 7/2004 byla vydána ostrá verze PHP5, MySQL4 vydáno 3/2003. Což odpovídá začátkům práce na systému. Autor proto měl zvážit použití nových (a velmi rozdílných) verzí.

Hašovací funkce, MD5

Hašovací funkce je algoritmus, kterému se předá řetězec (téměř) libovolné délky (v tomto případě přihlašovací heslo) a výstupem je řetězec pevné délky (128 bitů pro MD5). Důležité je, že z tohoto řetězce zpětně nejde v rozumném čase získat originál (tedy uživatelovo heslo). Pokud tedy někdo zcizí hašovaná hesla, tak mu nejsou k ničemu dobrá, protože není schopen z nich získat vstupní podobu.
Není to ale tak docela pravda: Uvedl jsem, že funkce redukuje řetězec téměř libovolné délky na 128bitů. Dochází zde tedy ke značné ztrátě informace. Je jasné, že existuje velké množství tzv. kolizí – tj. situace, kdy 2 různé vstupy generují stejný výstup (u MD5 pro takový 1 výstup existuje 10^18 vzorů!!!). Finta je v tom, že u ideální hašovací funkce nejde v rozumném čase najít 2 různé vzory, které by generovaly stejný výstup. Pokud se toto podaří, hašovací funkce se označí za prolomenou – a MD5 prolomená je! Sice způsobem, který zatím (doufejme) nejde pro případ ukládání hesla zneužít, ale i tak se krajně nedoporučuje MD5 používat. Není vyloučeno, že se někomu podaří nacházet vzory k danému hašovému kódu. Doporučuje se používat funkce SHA1, SHA256, SHA384, SHA512, neměly by se používat MD4, MD5, SHA0.
Je zde další riziko. Uživatelé používají jako hesla slova, která lze snadno uhodnout (jména, datumy, čísla, názvy věcí, atd.) Není jich (z pohledu počítače) mnoho. Existují slovníky těchto hesel. Pokud bych se dostal k souboru, kde jsou uložena hašovaná hesla, provedu jednoduchý postup: vezmu slovník často se vyskytujících hesel, zhašuji ho a porovnám s hesly, která jsem odcizil ze systému.

Řešením je použití „soli“. V databázi uložím jako otevřený text náhodně generovaný řetězec (=sůl). Vezmu heslo, připojím za něj sůl, zhašuji, uložím jako další údaj do databáze. Pokud dojde k odcizení obou údajů, útočník má mnohem složitější situaci (dá se říct, že neřešitelnou).

Závěrem:

1. Neměla by být použita MD5 (i když pro to v současnosti není jednoznačný důvod)
2. U hesel by měla být použita sůl (nevím, jestli tomu tak není, na to bych potřeboval vidět kód programu. Tipuji ale, že na to dotyčný nemyslel)

Často se v textu vyskytuje pojem „kódování MD5“

Termín kódování je pro spojení s MD5 krajně nevhodný! Je třeba rozlišovat kódování, šifrování a hašování – vše znamená něco jiného. Kódování je pouze změna zprávy do jiného tvaru (např. vhodného pro uložení v souboru, přenos přes síť atd.). Nemění se informační obsah. Cílem kódování není utajení zprávy. Šifrování má zajistit skrytí informace, bez klíče nejme schopni informaci obnovit. Hašování je teoreticky jedinečný „otisk“ zprávy. Originál zprávy z jejího haše nezískáme (protože „originálů“ existuje obrovské množství, zobrazení není jednoznačné), můžeme si ale být s velmi vysokou pravděpodobností jistí, že nikdo nedokáže najít jinou zprávu, která má stejný haš (pojem kolizí 2. řádu).

Závěr:

Namísto termínu „kódování“ by se v textu mělo hovořit o „hašování“ nebo anglicky „hashování“.

3.2.4, 4.2.2.4

Hodnota počítadla se zobrazuje pouze na úvodní stránce, proč?

4.2.2.1

HTML kód dostupný nepřihlášenému/neregistrovanému uživateli ke dni 7.6.2007 16h není validní podle autorem uvedeného nástroje http://validator.w3.org ani podle jiných nástrojů autorizovaných konsorciem w3c. Stránky navíc nemají základní strukturu HTML dokumentu podle doporučení w3c. Chybí strukturování pomocí HTML značek <h1>, <h2>, ..., pro obsahové zvýraznění jsou použity značky <b>, <i> namísto , .
Celý layout (rozvržení) stránky je realizováno pomocí tabulky (<table>), což je také nevhodné, jak z technických, tak z obsahových důvodů (viz. w3c).
Tyto skutečnosti mají vliv zejména na hodnocení kvality stránky, které provádějí roboti – stroje firem provozujících internetové vyhledávače a katalogy. To při vyhledávání způsobí, že stránka bude zobrazena ve výpisu na nižších pozicích. Rovněž stručný popis stránky ve vyhledávačích či katalozích nebude patrně vystihovat obsah stránek. Toto jsou hlediska, která nelze podceňovat – stejně důležité je kromě existence kvalitního datového zdroje i jeho identifikace a možnost nalezení v Internetu.

5. k závěru:

cituji:
V systému pFIDiS je i přes tyto známé chyby použit algoritmus MD5 a to z několika důvodů. Za prvé se u systému pFIDiS nejedná o žádnou bankovní či jinak striktně zabezpečenou aplikaci, proto se tento druh zabezpečení jeví jako dostačující. Za druhé tento způsob kódování hesel je jednoduše použitelný v PHP skriptech, jenž jsou součástí internetových stránek systému.

-problém zneužití hesla nelze podceňovat. Jednak z hlediska záměrného poškození systému, neméně však z vědomí, že většina uživatelů používá jediné heslo pro velké množství aplikací. Vyzrazením hesla z jakéhokoli, byť nevýznamného, systému dává útočníkovi velké možnosti pro zneužití ostatních aplikací, do kterých uživatel vstupuje. Příklad – kdyby uživatel, zaměstnanec univerzity, v této aplikaci použil stejné heslo, které používá pro přístup do univerzitních aplikací, vzniklo by riziko, že útočník z řad studentů získá databázi hašovaných hesel, heslo dešifruje a zneužije.
-použití SHA-1 a bezpečnějších funkcí (SHA128,384,512) není v této aplikaci o mnoho náročnější na výpočetní výkon a už vůbec ne pro programátora. Práce je v principu stejná, jako s funkcí MD5.