Posudek oponenta bakalářské práce

Autor/autorka práce: **Pavel Hvězda**

Název práce: **Analýza a vytvoření automatického systému sledování logů.**

Práce se zabývá návrhem systému pro filtrování logů přicházejících z různých zařízení počítačové sítě Západočeské univerzity. Logy se zachycují standardním protokolem SYSLOG, předávají aplikaci, fitrují, třídí a ukládají do databáze. Pro zobrazování logů a zadávání parametrů filtrování se používá webový prohlížeč. Student realizoval webové rozhraní s požadovanými formuláři.

Struktura bakalářské práce se mi jeví jako poněkud nepřehledná. Jednotlivé kapitoly nesou názvy „Úvod, Technologie, Instalace a konfigurace, Zpracování logů, Statistiky dat, Filtry, Regulární výrazy, Webové rozhraní, Moduly a Závěr". Podle mého názoru chybí jasné oddělení teoretické části od části realizační. Navíc první bod zadání zní „Analyzujte a porovnejte dostupné systémy pro zpracování logů ze syslogu a vytvořte webové uživatelské rozhraní pro jejich filtraci". V práci toto porovnání uvedené není. V jednotlivých kapitolách textu autor rozebírá jednotlivé komponenty navrženého systému a zdůvodňuje jejich použití. Vzhledem k tomu, že chybí teoretická část, tak také chybí kapitola, zabývající se jádrem řešeného problému, tj. jak se z textových logů přejde k informaci, uložené v databázi. Princip filrování je uveden nesystematicky, spíše je rozebíráno to, co jednoduše realizovat nelze. Je zde pouze uvedeno, že k analýze logů se musí použít syntaktický analyzátor. Práce má 48 stran textu.

Navržený systém byl realizován a jeho funkčnost odzkoušena na pracovišti zadavatele. Student nainstaloval a nakonfiguroval všechny použité komponenty, tj. webový server Apache, databázi MySQL i server pro zachycování logů. V práci jsou uvedeny i fragmenty realizovaného kódu a příklady konfiguračních souborů.

Po formální stránce práce obsahuje velké množství zbytečných překlepů a chyb. Dovolil jsem si zatrhnout je tuškou přímo v práci. Některé chyby jsou však až nepochopitelné. Na str. 2 se mluví o 9 úrovních priorit, ve výčtu je jich uvedeno pouze 8. Na stránce 3 se mluví o 12 kategoriích logů, ve výčtu je jich uvedeno 13. Vzhledem k tomu, že priority i kategorie se uvažují při filtrování, tak není jasné, co se vlastně filtruje. Na str. 9 se mluví o 2 vrstvách MySQL, o kousek dál se uvádí i třetí vrstva.

Student čerpal z tištěné i v elektronické podobě přístupné literatury. Celkem seznam čítá 20 titulů. Všechny se týkají řešené problematiky.

Lze říci, že cíle zadání byly naplněny. Z předložené práce je zřejmé, že se student zaměřil zejména na vlastní realizaci systému, který musel být funkční, protože jinak by nesplnil zadání bakalářské práce. Podle vyjádření studenta byl systém odzkoušen v reálném provozu s kladným ohlasem zadavatele. Výhradu mám k nenaplnění prvního, teoretického, bodu zadání. Rovněž se mi nelíbí řazení jednotlivých kapitol, které patrně přesně kopíruje postup řešení. Celkově lze ale konstatovat, že zadání bylo splněno. Zejména si vážím toho, že výsledkem je funkční program.

Dotazy k práci: Víte něco o existenci obdobných systémů? Co Vás vedlo k tomu, že jste do přehledu možností „jak zadaný problém řešit" nezahrnul realizaci pomocí servletů v Javě.

Navrhuji hodnocení známkou **velmi dobře** a práci doporučuji k obhajobě.

V Plzni 31.5.2013

Ing. Jiří Ledvina, CSc.