Univerzita Tomáše Bati ve Zlíně
Fakulta aplikované informatiky

POSUDEK OPONENTA DIPLOMOVÉ PRÁCE

Student: **Bc. Jaroslav Krajča** **Oponent:** **doc. Ing. Zdeněk Čujan, CSc.**

Studijní program: **Inženýrská informatika**
Studijní obor: **Bezpečnostní technologie, systémy a management**
Akademický rok: **2010/2011**

Téma diplomové práce: **Metody analýzy rizik podnikových informačních systémů - učební pomůcka pro předmět Bezpečnost informačních systémů**

Hodnocení práce:

Předložená diplomová práce se zabývá návrhem řešení učební pomůcky pro výuku akreditovaného předmětu „Bezpečnost informačních systémů“.

Práce je zpracována v rozsahu potřebném pro navazující magisterské studium. Téma práce úzce souvisí s problematikou, která je zejména v současné době postupující digitalizace, informatiky, využívání PC a sítí velmi aktuální. Zvyšující se trend ve využívání informačních technologií, které nabízejí stále širší možnosti jejich praktického využití a tím uspokojení potřeb uživatelů, zvětšuje existenci hrozeb a útoků všeho druhu na bezpečnost systémů.

Teoretická část je věnována základním pojmům, jejich pojmenování a definování, jako jsou riziko, aktivita, hrozba, zranitelnost, protiopatření a metody analýzy rizik. Obsah teoretické je tematicky zaměřen na praktickou aplikaci poznatků v navazující části praktické.

Úvod praktické části je věnován zpracování analýzy hrozeb a návrhů opatření, na základě kterých jsou zpracovány matice posuzující hrozby v případě možných útoků na podnikový informační systém. Dílčími nedostatky práce jsou chybějící odkazy na citační normy a také u některých uváděných tabulek a obrázků není uveden zdroj (není zřejmé, zda se jedná o převzatý zdroj nebo je to vlastní tvorba diplomanta. Ve vztahu k definici ochrany dat mohl diplomant použít zákon č. 412/2005 Sb. „O ochraně utajovaných skutečností“ a v souladu s použitou literaturou mohl vhodně definovat zranitelné místo a útočníka – viz literatura číslo [6]). V návrhové části diplomové práce mohl diplomant pro názornou ilustraci zpracovat některý z uvedených druhů působení hrozeb na aktiva tak, aby pro potřeby výuky a snadnější pochopení, byla navrhovaná metodická pomůcka úplná.

Práce jako celek působí vyváženě a to jak po stránce teoretické, tak po stránce analytické i návrhové.

Práci doporučuji k obhajobě.

Univerzita Tomáše Bati ve Zlíně
Fakulta aplikované informatiky

Otázky k obhajobě:

1. Definujte útočníka, druhy a speciální programové kódy.
2. Definujte v souladu se zákonem 412/2005 Sb. a souvisejícími vládními nařízeními, stupně utajení informací.

Celkové hodnocení práce:
Známku uvede vedoucí dle svého uvážení dle klasifikační stupnice ECTS:
A – výborně, B – velmi dobře, C – dobře, D – uspokojivě, E – dostatečně , F – nedostatečně.
Stupeň F znamená též „nedoporučuji práci k obhajobě“.

Předloženou diplomovou práci nedoporučuji k obhajobě a navrhuji hodnocení

B - velmi dobře.

V případě hodnocení stupněm „F – nedostatečně“ uveďte do připomínek a slovního vyjádření hlavní nedostatky práce a důvody tohoto hodnocení.

Datum 30.5.2011 Podpis oponenta diplomové práce