České vysoké učení technické v Praze, Fakulta biomedicínského inženýrství
Katedra zdravotnických oborů a ochrany obyvatelstva, nám. Sítná 3105, 272 01 Kladno
tel.: +420 224 359 973, fax: +420 312 608 204, www.fbmi.cvut.cz

# POSUDEK OPONENTA BAKALÁŘSKÉ PRÁCE

studenta: Jan Dovrtěl
s názvem: Kybernetické hrozby relevantní pro kritickou infrastrukturu České republiky

## Hodnocení bakalářské práce dosahuje následující úrovně:

| | | |
|---|---|---|
| 1. | Splnění cíle a vhodnost struktury obsahu bakalářské práce z hlediska zadaného tématu (splnění zadání). (0 – 30) | 27 |
| 2. | Teoretická úroveň a využití dostupné literatury v bakalářské práci. (0 – 20) | 16 |
| 3. | Formální náležitosti a úprava obsahu bakalářské práce (úroveň psaní, označení struktury textu, grafy, tabulky, citace v textu, seznam použité literatury apod.). (0 – 10) | 9 |
| 4. | Rozsah realizačních prací, aplikovaných vědomostí a znalostí, úroveň metodologického zpracování a závěrů práce. (0 – 40) | 31 |
| 5. | **Celkový počet bodů** | 83 |

## Návrh otázek k obhajobě

1. Jakým způsobem je rozdělena odpovědnost mezi vládní a národní CERT/CSIRT?

2. Na základě jakých kritérií jsou určovány informační systémy do kritické informační infrastruktury?

3. Které jsou hlavní hrozby, jímž čelíme v kyberprostoru?

## Celkové hodnocení úrovně vypracování bakalářské práce:

| Hodnocení**: | A (výborně) | B (velmi dobře) | C (dobře) | D (uspokojivě) | E (dostatečně) | F (nedostatečně) |
|---|---|---|---|---|---|---|
| Počet bodů: | 100 - 90 | 89 - 80 | 79 - 70 | 69 - 60 | 59 - 50 | < 50 |
| | □ | X | □ | □ | □ | □ |

** v případě hodnocení F (nedostatečně) uveďte komentář

Bakalářskou práci hodnotím výše uvedeným klasifikačním stupněm a doporučuji/~~nedoporučuji~~ k obhajobě.

## Komentář

Autor bakalářské práce s názvem "Kybernetické hrozby relevantní pro kritickou infrastrukturu České republiky" se svého úkolu zhostil dobře. Po odborné stránce lze práci vytknou ne zcela aktuální popis stavu implementace zákona č.181/2014 Sb., o kybernetické bezpečnosti a o změně souvisejících zákonů (ZKB), zejména procesu určování kritické informační infrastruktury (KII). Opomenuta byla také, dnes velmi aktuální, zranitelnost SCADA (Supervisory Control And Data Acquisition) systémů využívaných při monitorování a řízení např. technologických procesů. Větší prostor by si také zasloužil, vzhledem k názvu bakalářské práce, výčet prvků kritické infrastruktury, jejichž informační a komunikační systémy jsou důležité pro zajištění chodu státu. Vzhledem k relativní novosti problematiky je možno konstatovat, že se autor v problematice dostatečně zorientoval. Autorův pohled na trendy v oblasti nárůstu hrozeb v kybernetickém prostoru je v souladu s oficiálními postoji odpovědných institucí k dané problematice. Optimismus, s kterým očekává účinnost opatření vyplývající ze ZKB je možná poněkud přehnaný, byť ambice autorů ZKB byly obdobné. Pozitivně hodnotím, že v práci nebyl opomenut mezinárodní aspekt problematiky i přesto, že tématem jsou jen hrozby kritické infrastruktuře ČR. Pokud se týká souvisejících prováděcích předpisů ZKB, autor zmiňuje obě vyhlášky, avšak bez uvedení čísel a názvů těchto vyhlášek. Dobře zpracovaná je kapitola, která se věnuje dohledovým pracovištím typu CERT/CSIRT jako prostředků k předcházení a minimalizaci dopadů kybernetických útoků. Uvedené příklady jednotlivých typů kybernetických útoků a jejich původců dobře demonstrují možnosti napadení široké škály cílů, včetně KII. V práci je pomocí kontextové analýzy vytvořen graf vazeb mezi jednotlivými hackery v rámci hackerské operace AntiSec s využitím otevřených zdrojů. Tato metoda je vhodná pro zpracování velkého objemu dat a autor zde ukázal, že ji lze aplikovat na různé zdroje informací např. při stanovování potenciálních cílů kybernetických útočníků a lze ji tudíž využít v činnosti dohledových pracovišť typu CERT/CSIRT. Na vybraném vzorku kybernetických útoků ze zvolené hackerské operace byla demonstrována celá škála cílů a typů kybernetických útoků, četně útoků na systémy z kritických infrastruktur, byť ne v ČR. Největší kybernetický útok, který byl veden proti cílům v ČR, je v práci uveden.

Deklarované cíle práce byly do značné míry naplněny. Absence konkrétních příkladů kybernetických útoků na kritickou infrastrukturu nelze považovat za nedostatek, neboť KII ČR není dosud zcela definována (25. 5. 2014 vláda schválila prvních 25 informačních systémů zahrnutých do KII). Autor si v práci položil otázku, zda existuje příčinná souvislost mezi podnětem a realizací kybernetického útoku, podobně jako tomu bylo např. v Estonsku v roce 2007. Osobně se ztotožňuji s jeho názorem, že takovou souvislost nelze jednoznačně prokázat.

Formální úroveň práce je odpovídající, pokud se týká grafické úpravy i členění práce. Témata jednotlivých kapitol byla volena vhodným způsobem a pokrývají danou tématiku. Zdroje, ze kterých autor čerpal, byly relevantní v době, kdy práci začal tvořit a lze konstatovat, že pro daný typ práce byly dostatečné. U citací je pečlivě uváděn autor vybrané stati. V textu se nachází minimum překlepů a drobných formulačních pochybení.

Podle mého názoru autor dostál požadavku na obsahovou i formální úroveň bakalářské práce. Přes výše uvedené drobné nedostatky proto doporučuji tuto práci k obhajobě a hodnotím ji stupněm velmi dobře.

Jméno a příjmení: Ing. Jaroslav Šmíd
Organizace: Národní bezpečnostní úřad

Podpis: .....
Datum: .....