

## I. OSOBNÍ A STUDIJNÍ ÚDAJE

Příjmení: **Miženko** Jméno: **Petr** Osobní číslo: **491717**  
Fakulta: **Fakulta biomedicínského inženýrství**  
Studijní program: **Ochrana obyvatelstva**  
Studijní obor: **Plánování a řízení krizových situací**  
Název práce: **Kybernetická bezpečnost z pohledu podnikové infrastruktury**

## II. HODNOCENÍ BAKALÁŘSKÉ PRÁCE

Kritéria hodnocení práce		Počet bodů
1.	Splnění cíle a vhodnost struktury obsahu bakalářské práce z hlediska zadaného tématu (splnění zadání). (0 - 30)*	25
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)*	8
4.	Rozsah realizačních prací, aplikovaných vědomostí a znalostí, úroveň metodologického zpracování a závěrů práce. (0 - 40)*	30
5.	<b>Celkový počet bodů</b>	<b>79</b>

\* Slovní hodnocení uveďte v komentáři.

## III. NÁVRH OTÁZEK K OBHAJOBĚ

1. Jaká evropská norma zapříčinila zrušení zákona č. 101/2000 Sb., o ochraně osobních údajů? A který zákon jej nahradil?

2. V kapitole 3.5 byly zmíněny jen některé metody zabezpečení podnikové infrastruktury, které ovšem samy o sobě nestačí pro bezpečný provoz IT. Jmenujte a popište další nezbytné metody a nástroje zajištění bezpečnosti IT.

3. Jaké dopady měla evropská směrnice NIS na povinnosti subjektů v kapitole 3.3? A jaké očekáváte dopady evropské směrnice NIS2 na tyto subjekty?

#### IV. 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
	<input type="checkbox"/>	<input type="checkbox"/>	X	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

\*\* v případě hodnocení F (nedostatečně) uveďte podrobný komentář

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

#### V. KOMENTÁŘ

Práce je psána srozumitelně pro širokou veřejnost a to na úkor úrovně technických detailů. Nicméně je napsána s malým množstvím gramatických chyb a na úrovni odpovídající bakalářskému studiu.

Práce bohužel obsahuje nepřesnosti či neúplnosti ve výčtech v kapitolách 3.1 či 3.5, a co je možná horší, používá některé pojmy bez bližšího vysvětlení.

V kapitole 3.1 mi chybí zmíněné tyto tři hrozby: nepoučený (liknavý) uživatel, insider a krádež pověření. To navzdory faktu, že tyto pojmy se v práci později vyskytnou např. v kapitole 6.

Ve výčtech technických řešení či odkazovaných norem by bylo vhodné doporučit další, aktuální, ideálně z best-practise v oblasti kybernetické bezpečnosti.

Pozitivně lze hodnotit čerpání a uplatnění čerstvých informací z bakalářských a diplomových prací z jiných univerzit.

Zvolená metodika SWOT je pro daný use-case vhodná, přičemž student ji správně uchopil a zpracoval.

Dotazník, který je jinak dobře zpracován z pohledu grafického vyhodnocení či výsledných doporučení, byl dle mého názoru nevhodně zvolen. Konkrétně pro zaměstnance společnosti bez IT zaměření s dotazy na pojmy typu RBAC, POSL či vícefaktorovou autentizaci nemohly generovat korektní výsledky, protože cílová skupina těmito pojmy nemohla rozumět.

Jako neodpustitelnou chybu vnímám citaci již tři roky neplatného zákona č. 101/2000 Sb., o ochraně osobních údajů, v kapitolách 3.2.2. a 3.3.2.

Jméno a příjmení: Ing. Michal Kopřiva  
Organizace: Ministerstvo Obrany  
Kontaktní adresa: Tychonova 1, 160 00 Praha 6

Podpis: .....

Datum: .....