Univerzita Tomáše Bati ve Zlíně
Fakulta aplikované informatiky

POSUDEK OPONENTA DIPLOMOVÉ PRÁCE

Student: **Bc. Ondřej Martinec** **Oponent:** **Mgr. Tomáš Kužel, DiS.**

Studijní program: **Bezpečnostní technologie, systémy a management**
Studijní obor/Specializace: **Bezpečnostní management**
Akademický rok: **2023/2024**

Téma diplomové práce: **Implementace systému řízení bezpečnosti informací podle ISO 27001:2022**

Hodnocení práce:

Úplnost vypracování, aktuálnost a obtížnost řešeného úkolu
Diplomová práce s názvem „Implementace systému řízení bezpečnosti informací podle ISO 27001:2022“ se dělí na dvě části. V teoretické části popisuje autor vývoj informační bezpečnosti, vymezuje systém řízení bezpečnosti informací v kontextu mezinárodně platných a uznávaných standardů řady ISO/IEC 27001. V dalších teoretických částech se autor věnuje velmi okrajově aktuálnímu zákonu č. 181/2014 Sb., o kybernetické bezpečnosti a platné směrnici Evropského parlamentu a rady (EU) 2022/2555 ze dne 14. prosince 2022 o opatřeních k zajištění vysoké společné úrovně kybernetické bezpečnosti v Unii a poukazuje na její východiska při určování směru v této oblasti. Praktická část je členěna do pěti kapitol. Nosným bodem praktické části je provedená zpětná kompatibilita platné normy ISO/IEC 27002:2022 s ISO/IEC 27002:2013, týkající se opatření informační bezpečnosti. Nová opatření autor prezentuje standardizovanou formou v kapitole 4. Značnou část práce tvoří autorem navržený a realizovaný softwarový nástroj, který je detailně popisován v kapitole 5.

Lze konstatovat, že téma diplomové práce, je i vzhledem k rostoucím požadavkům, které jsou kladeny na oblast informační a kybernetickou bezpečnost, stále aktuální. Autorem stanovené hlavní cíle práce byly splněny.

Způsob a úroveň pojetí řešeného úkolu
Celkově přináší diplomová práce komplexní pohled na danou problematiku a svým obsahem může být značným přínosem zejména pro organizace, které již mají zaveden systém řízení bezpečnosti informací dle ISO/IEC 27001:2013. Přínosem je bezpochyby zpracovaná analýza současného stavu ISMS v konkrétním podniku na základě vytvořených kontrolních otázek vycházející ze znění norem řady ISO/IEC 27001:2022. Z provedené analýzy však není zřejmé, jakým způsobem se v daném podniku naplňují bezpečnostní opatření, na které se autor dotazuje skrze kontrolní otázky.

Autorem vytvořený praktický nástroj v Microsoft Access umožňuje provést základní analýzu stavu a úroveň plnění bezpečnostních opatření v rámci organizace s ohledem na platnou normu ISO/IEC 27001:2022. Rozsah, návrh a popis uvedeného nástroje je považován za dostačují.

Úroveň zpracování tématu, přínos diplomanta
Zvláštně pozitivně hodnotím návrh a realizaci nástroje, který může sloužit jako sebehodnotící prostředek pro dotčené organizace. Nástroje převádí teoretické poznatky a může obsahově, ale i prakticky pomoct organizacím se zásadními změnami při přechodu z ISO/IEC 27001:2013 na

ISO/IEC 27001:2022, které organizace budou muset promítnout do příslušné bezpečnostní politiky a vnitřních procesů. Je zjevné, že autor využil poznatků získaných v rámci své dosavadní praxe v rámci výrobní společnosti, kde byla provedena analýza současného stavu ISMS.

Formální náležitosti práce, chyby a omyly v technické zprávě
Diplomové práce je věcná, logicky strukturovaná a rozsahem dostatečná k tomu, aby představila komplexní pohled na autorem zvolené téma. K osnově práce není zásadnějších připomínek. Autor se v rámci práce dopouští drobných gramatických chyb a terminologických nesprávností. Celkově to však nemá vliv na celkovou úroveň předkládané práce. Použité metody v této práci autor využívá vhodným způsobem. Autor je schopen interpretace vlastního názoru.

Předložený text dokazuje dobrou orientaci autora v oblasti informační a kybernetické bezpečnosti a schopnost autora syntetizovat zdroje z relevantních oblastí. Předloženou práci **doporučuji** k obhajobě a navrhuji hodnocení **B – velmi dobře.**

Dotazy k obhajobě

1. V práci se věnujete analýze současného stavu ISMS v konkrétním podniku. Popište, jakým způsobem bylo vyhodnoceno plnění či neplnění bezpečnostních opatření v rámci daného podniku.
2. V předložené práci se okrajově věnujete ekonomickému pohledu na zavedení systému ISMS. Jak vnímáte účelnost technických opatření a řešení za účelem zabezpečení chráněných aktiv? Jaký je podle vás ideální poměr technických a organizačních opatření v celkovém systému řízení bezpečnosti informací?
3. Vysvětlete, jaký význam a roli má klasifikace informací v rámci ISMS. V čem spatřujete úskalí zavádění klasifikace informací?

Celkové hodnocení práce:
Známku uvede oponent 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 doporučuji 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 04.06.2024 Podpis oponenta diplomové práce