

POSUDEK OPONENTA DIPLOMOVÉ PRÁCE

Autor diplomové práce:

Vojtěch Draganov

Téma diplomové práce:

Zákon o kybernetické bezpečnosti a jeho dopady na povinné subjekty

Cíle diplomové práce:

Cílem práce bylo nejprve provést rozbor ZKB za účelem zjištění dopadů tohoto zákona na povinné subjekty a následně na základě tohoto rozboru pak navrhnout a provést dotazníkový průzkum, který ověří zjištěné dopady na krajských úřadech ČR a zjistí základní fakta o stavu kybernetické bezpečnosti na těchto úřadech.

Vedlejším cílem je dále také uvedení základních informací o české legislativě kybernetické bezpečnosti, vzniku zákona o kybernetické bezpečnosti a jeho kontextu.

HODNOCENÍ DIPLOMOVÉ PRÁCE	
Kritéria	Hodnocení
1. Vymezení cíle práce a jeho naplnění	vynikající
2. Náročnost tématu na teoretické znalosti	dobré
3. Náročnost tématu na praktické dovednosti	dobré
4. Adekvátnost použitých metod, způsob jejich použití	vynikající
5. Hloubka a správnost provedené analýzy	vynikající
6. Vlastní přínos k řešené problematice	dobré
7. Práce s informačními zdroji, relevance, rozsah, rešerše odb. prací	vynikající
8. Adekvátnost a srozumitelnost závěrů práce	vynikající
9. Logická struktura práce a její členění	vynikající
10. Jazyková a terminologická úroveň práce	vynikající
11. Formální úprava a náležitosti práce	vynikající
Navržená známka	výborně (1)

Celkové zhodnocení práce a případné otázky pro diskusi (případně na další samostatný list):

Autor si v úvodu vytyčuje cíle, které v rámci své práce naplňuje. Kladně hodnotím rešerši, nacházející se v úvodu práce, kde hodnotí stávající práce jiných autorů a bystře identifikuje hlavní aktivity patrné v oblasti regulace kybernetické bezpečnosti. Problematiku autor vhodně začleňuje do kontextu kybernetické bezpečnosti prosazované na úrovni státu, nesměšuje pojmy počítačové kriminality a kybernetické bezpečnosti, ochrany dat a ochrany kybernetického prostoru. Taktéž vhodně komentuje "okolí" zákona o kybernetické bezpečnosti (vazbu na ústavní zákony i zákony související - např. zákon o krizovém řízení). Za rozumné považuji rovněž to, že se autor věnuje základním pojmům uvedeným v zákoně a uvádí je do souladu s pojmy běžně užívanými v oblasti ICT bezpečnosti (hrozba, riziko, incident, atd.) - tam, kde je to účelné. Následuje exkurz do historie a zasazení ochrany kybernetického prostoru do rámce aktivit EU. V následující kapitole (kapitola 4) se autor zabývá obsahem ZKB a prokazuje, že porozuměl jeho účelu a obsahu (včetně návazných vyhlášek).

Zmíněné kapitoly hodnotím jako přehledný a rozumně podaný úvod do problematiky zákona o kybernetické bezpečnosti, včetně shrnutí hlavních dopadů zákona na povinné subjekty.

Samotný průzkum je popsán v kapitole 5. Průzkum je proveden metodicky správně a dle mého názoru nevykazuje formální chyby. Osobně považuji za nejzajímavější otázky ty, které se týkají možnosti outsourcingu a financování zaváděných opatření z fondů IROP. U dotazů na očekávanou organizační či finanční zátěž zavádění opatření, stejně jako na přiměřenost lhůty pro jejich implementaci bylo dle mého názoru poměrně nasnadě predikovat odpovědi respondentů. Nicméně pro účely diplomové práce považuji i takto formulované otázky za relevantní - jistě pomohou autorovi (a nejen jemu) pochopit realitu ochrany kybernetického prostoru v nekomerční sféře.

Jméno oponenta diplomové práce:

David C. HÁJÍČEK

Datum: 19.05.16

Podpis oponenta diplomové práce