

Ing. Jaroslav Šmíd
1. náměstek ředitele Úřadu

Praha 19. srpna 2021
Č.j.: 6931/2021-NÚKIB-E/440

Věc: Stanovisko a doporučení k programu Kybernetická bezpečnost

Vážený pane řediteli,

na základě Vaší žádosti ze dne 10. 6. 2021 jsme provedli posouzení zaslaného návrhu vzdělávacího programu Kybernetická bezpečnost pro VOŠ PRIGO (obor informační bezpečnost, 26-47-N/04, denní i kombinovaná forma) a zasíláme Vám naše stanovisko s doporučeními.

Vzhledem k obecnému a dlouhodobému nedostatku odborníků v oblasti kybernetické a informační bezpečnosti tuto Vaši aktivitu, která rozšiřuje kapacity České republiky v oblasti přípravy specialistů kybernetické a informační bezpečnosti, vítáme.

Vámi navržený vzdělávací program je celkově vhodnou alternativou k vysokoškolskému studiu kybernetické bezpečnosti navazující po střední škole.

Zaslané materiály prostudovali naši odborníci a sestavili stručný souhrn komentářů a doporučení k programu, který Vám zasíláme v příloze tohoto dopisu.

Pro zkvalitnění obsahu vzdělávacího programu a navýšení uplatnitelnosti absolventů na trhu práce Vám doporučujeme zpracovat navrhovaná doporučení.

Věříme, že Váš vzdělávací program akreditaci získá a jeho absolventi budou v budoucnu platným přínosem při zajišťování, výstavbě a posilování kybernetické bezpečnosti České republiky a našich spojenců.

S přátelským pozdravem a přáním hezkého dne

Ing. Rudolf Macek, Ph.D.

ředitel

Vyšší odborná škola a Jazyková škola s právem
státní jazykové zkoušky PRIGO, s.r.o.

Mojmírovců 1002/42

709 00 Ostrava-Mariánské Hory

Příloha: Komentáře a doporučení k programu

Obecně:

1. Návrh vzdělávacího programu a popis absolventa (včetně jeho očekávaných dovedností, znalostí a způsobilostí) reaguje na poptávku tržního prostředí v podobě nedostatečného počtu odborníků v oblasti kybernetické bezpečnosti.
2. Absolventi denní formy studijního programu absolvují 911 hodin teoretické výuky (vč. cvičení) a 408 hodin praktické výuky u firem, které se zabývají bezpečností informačních systémů a technologií, což z hlediska získávání praxe u absolventů hodnotíme jako zajímavý koncept.
3. Pozitivně také hodnotíme sekci *Bb) Kompetence a možnosti uplatnění absolventa* (Profil znalostí, dovedností a způsobilostí absolventa). Profil absolventa je zaměřen prakticky.
4. Kladnou stránkou návrhu vzdělávacího programu je také důraz na kybernetickou bezpečnost, což dobře dokládá skladba závěrečných zkoušek a její okruhy, které jsou vypsány v sekci *Cb) hodnocení výsledků studentů*.
5. Přínosem jsou dále:
 - a. Orientace absolventů v problematice digitalizace státní správy a vazby na kybernetickou bezpečnost.
 - b. Zařazení IT terminologie do výuky anglického jazyka.
 - c. Výuka etických a morálních aspektů auditů informačních systémů.
 - d. Zahrnutí problematiky elektronického podpisu a jeho využití ve veřejné správě.
 - e. Zařazení problematiky dokazování v prostředí elektronických dokumentů.
 - f. Výuka právních základů e-governmentu v České republice.

Doporučení NÚKIB k možnému provedení změn:

1. Doplnit Národní úřad pro kybernetickou a informační bezpečnost mezi organizace, které se podílí na zajištění a rozvoji systému bezpečnosti České republiky (sekce *Cd, předmět Základy bezpečnosti státu*). Kybernetická bezpečnost, kterou v České republice zajišťuje Národní úřad pro kybernetickou a informační bezpečnost, je součástí systému bezpečnosti státu. Národní úřad pro kybernetickou a informační bezpečnost v této části návrhu v tuto chvíli nijak nefiguruje.

2. Položit vyšší důraz na síťové a bezpečnostní protokoly obecně. Předmět Datové sítě se podle obsahu věnuje ve velké míře různým Cisco řešením, aniž by studenti znali základy. Důvodem pro toto doporučení je skutečnost, že je tento předmět povinně volitelný, takže z VOŠ může vyjít absolvent, který tento předmět neabsolvoval, a takový absolvent by nemusel získat potřebné základní znalosti fungování sítí, které jsou pro činnost v oblasti kybernetické bezpečnosti klíčové.
3. Věnovat vyšší pozornost typům útoků v rámci předmětu Základy kybernetické bezpečnosti. Předmět se podle obsahu věnuje virům, ale ne útokům obecně. Útoky jsou s největší pravděpodobností řešeny v předmětu Bezpečnostní technologie, ale obecný úvod by měl zaznít již v předmětu Základy kybernetické bezpečnosti, aby si student mohl udělat ucelenější přehled již v této fázi studia.
4. Doplnit do programu problematiku znalosti finančních trhů. Obecné povědomí o finančních trzích absolventům umožní lépe pochopit problematiku kryptoměn v předmětu Kryptoměny.

Závěr:

Po zapracování doporučení Národního úřadu pro kybernetickou a informační bezpečnost má vzdělávací program kybernetické bezpečnosti VOŠ PRIGO potenciál být zajímavou možností pro další vzdělávání absolventů středních škol v oblasti kybernetické bezpečnosti a dalším zdrojem pro zvýšení počtu kvalitně připravených specialistů kybernetické bezpečnosti pro organizace zajišťující kybernetickou bezpečnost státu jak ve státním, tak i soukromém sektoru.