Národní úřad
pro kybernetickou
a informační bezpečnost

NÚKIB

Seifert Petr
vedoucí oddělení
Oddělení vzdělávání

Praha 13. října 2023
Č. j.: 8251/2023-NÚKIB-E/620

Věc: Stanovisko ke vzdělávacímu programu Kybernetická bezpečnost

Vážená paní ředitelko,

na základě Vaší žádosti ze dne **14. 9. 2023** jsme provedli opětovné posouzení zaslaného návrhu vzdělávacího programu **Kybernetická bezpečnost pro Vyšší odborná škola Praha, s.r.o. (obor informační technologie, 26-47-N/.., denní i kombinovaná forma)** a stejně jako v loňském roce Vám zasíláme naše kladné stanovisko.

Zvýšení počtu odborníků v oblasti kybernetické a informační bezpečnosti je stále více aktuální téma a z tohoto důvodu Vaši aktivitu, která v tomto směru rozšiřuje kapacity České republiky vítáme. Vámi navržený a od loňska aktualizovaný vzdělávací program je celkově velmi vhodnou alternativou k vysokoškolskému studiu kybernetické bezpečnosti.

Pro Vámi zaslané materiály platí stejná doporučení, která jsme Vám zasílali v loňském roce. Naleznete je v příloze tohoto stanoviska.

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

S přátelským pozdravem a přáním hezkého dne,

Mgr. Lenka Rejdová
ředitelka
Vyšší odborná škola Praha, s.r.o.
Myslíkova 1998/30
120 00 Praha 2 – Nové Město

Mučednická 1125/31, 616 00 Brno
tel.: 541 110 777, e-mail: posta@nukib.cz, datová schránka: zzfnkp3, www.nukib.cz

Příloha: Komentáře a doporučení k programu

Obecně:

1. Návrh vzdělávacího programu a popis absolventa (včetně jeho očekávaných dovedností, znalostí a způsobilostí) vhodně reaguje na poptávku tržního prostředí v podobě nedostatečného počtu odborníků v oblasti kybernetické bezpečnosti.

2. Absolventi denní formy studijního programu absolvují celkem 2 400 hodin teoretické výuky (vč. všech povinně volitelných i volitelných předmětů) a 680 hodin praktické výuky ve vybraných institucích a podnicích, nebo alespoň na dvou odlišných pozicích, 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 opět zaměřen prakticky stejně jako v předchozím návrhu.

4. Vítáme také doplnění Národního úřadu pro kybernetickou a informační bezpečnost – NÚKIB a jeho role v rozvoji systému bezpečnosti státu v sekci *Cc) Základy bezpečnosti státu*.

5. 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*.

6. **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 správný název zkratky NÚKIB – Národní úřad pro kybernetickou a informační bezpečnost v sekci *Cc) Základy bezpečnosti státu*. Je zde chybně uveden název Národní úřad pro Kybernetickou ochranu – NÚKIB.

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.

Závěr:

Po zapracování doporučení Národního úřadu pro kybernetickou a informační bezpečnost má vzdělávací program kybernetické bezpečnosti Vyšší odborná škola Praha, s.r.o. potenciál být zajímavou možností pro navazující 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.

Elektronický podpis - 13.10.2023
Certifikát autora podpisu :
Jméno : Petr Seifert
Vydal : I.CA EU Qualified CA2/RSA 06/2022
Platnost do : 4.6.2024 13:12:47 +02:00