EVROPSKÁ UNIE
Evropské strukturální a investiční fondy
Operační program Výzkum, vývoj a vzdělávání

MINISTERSTVO ŠKOLSTVÍ, MLÁDEŽE A TĚLOVÝCHOVY

VSTUPNÍ ČÁST

Název modulu

Bezpečnostní politika a řízení rizik v IT

Kód modulu

18-m-4/AD91

Typ vzdělávání

Odborné vzdělávání

Typ modulu

(odborný) teoreticko–praktický

Využitelnost vzdělávacího modulu

Kategorie dosaženého vzdělání

M (EQF úroveň 4)

Skupiny oborů

18 - Informatické obory

Komplexní úloha

Metody analýzy rizik - Bezpečnostní politika

Obory vzdělání - poznámky

18-20-M/01 – Informační technologie

Délka modulu (počet hodin)

24

Poznámka k délce modulu

Platnost modulu od

30. 04. 2020

Platnost modulu do

Vstupní předpoklady

Základní práce se standardním aplikačním programovým vybavením (textový editor, tabulkový editor, grafický editor); základní znalosti pojmů informačních a operačních systémů; znalost UML (use case, sekvenční diagram).

JÁDRO MODULU

Charakteristika modulu

Modul představuje základní pojmy v oblasti bezpečnostní politiky, a to včetně metod používaných pro analýzu rizik. Jádro modulu tvoří problematika útoků v síťovém prostředí a metody kvantifikace a kvalifikace rizik.

Očekávané výsledky učení

Žák:

- definuje pojmy bezpečnostní politiky (BP): certifikace, role, akreditace, audit, evaluace, risk management, reakce na výjimečné situace, dozor;
- popíše na příkladech 4 druhy BP dle úrovně požadovaného zabezpečení;
- popíše na příkladu auditní postup;
- vysvětlí rozdíl mezi rizikem a hrozbou;
- uvede příklady rizik v oblasti informačních technologií;
- zařadí riziko dle kvantifikovaných ukazatelů do mapy rizik a na příkladu vysvětlí tzv. mez akceptovatelnosti.

(RVP) aby absolventi:

- navrhovali a aplikovali vhodný systém zabezpečení dat před zneužitím a ochrany dat před zničením
- dbali na zabezpečování parametrů (standardů) kvality procesů, výrobků nebo služeb, zohledňovali požadavky klienta (zákazníka, občana)
- si byli vědomi možností a výhod, ale i rizik (zabezpečení dat před zneužitím, ochrana dat před zničením, porušování autorských práv) a omezení (zejména technických a technologických) spojených s používáním výpočetní techniky;
- aplikovali výše uvedené – zejména aktivně využívá prostředky zabezpečení dat před zneužitím a ochrany dat před zničením;

Obsah vzdělávání (rozpis učiva)

- Obsah bezpečnostní politiky
- Druhy BP
- Auditní postup
- Útoky v síťovém prostředí
- Hrozba, Riziko – Mapa rizik

Učební činnosti žáků a strategie výuky

Metody názorně demonstrační:

- příklady reálných aplikací na definice jednotlivých částí BP;
- ukázka možných rizik a jejich zařazení do mapy rizik;
- rozdělení rizik do jednotlivých kategorií s ohledem na možné dopady pro chod firmy.

Metody praktické:

- nácvik určení druhu BP podle podmínek ve firmě;
- vyhledání možných rizik a jejich zařazení do mapy rizik;
- sestavení auditního postupu na konkrétní oblast zabezpečení.

Žáci v rámci praktické výuky provádí následující činnosti:

- sestaví mapu rizik;
- na ukázkovém případu popíší jednotlivé kroky auditního postupu.

Zařazení do učebního plánu, ročník

Informační systémy - 3. ročník

VÝSTUPNÍ ČÁST

Způsob ověřování dosažených výsledků

Žák pracuje samostatně na výstupní práci, výsledek prezentuje ve skupině, která (pod dohledem pedagoga) hodnotí výstup viz. kritéria hodnocení.

Výsledky jsou tak ověřovány výstupní prací, ve které žáci dovedou:

1. definovat pojmy bezpečnostní politiky (certifikace, role, akreditace, audit, evaluace, risk management, reakce na výjimečné situace, dozor) a k jednotlivým pojmům na internetu vyhledat související problematiku;
2. popsat na reálném příkladu (EZS) jednotlivé kroky auditního postupu (využití UML, znalost auditního postupu).

Kritéria hodnocení

Svou výstupní práci obhajuje žák ve skupině.

Pedagog (za možného přispění členů skupiny) během obhajoby hodnotí přesnost definice (maximálně 2 body) a za vhodnost příkladů udělením dalších maximálně 2 bodů pro každou část – části jsou:

- 9× za pojmy BP (certifikace, role, akreditace, audit, evaluace, risk management, reakce na výjimečné situace, dozor) tj. celkem 36 b.
- 4× za druhy BP (4 základní druhy bezpečnostní politiky) tj. celkem 16 b.
- 7× za auditní postup (7 kroků auditního postupu) tj. celkem 28 b.
- 2× za srozumitelnost UML (vhodnost diagramu, přesnost popisu) tj. celkem 8 b.
- 2× za detailnost UML tj. celkem 8 b.
- 1× za uvádění „zdrojů – citací“ v práci. tj. za správné citace 4 b.

Žák je hodnocen dle celkového součtu dosažených bodů (max. 100 bodů): 50 až 60 % (dostatečný), 61 až 70 % (dobrý), 71 až 85 % (chvalitebný) a 86 až 100 % (výborný).

Doporučená literatura

KORECKÝ, Michal a Václav TRKOVSKÝ. *Management rizik projektů: se zaměřením na projekty v průmyslových podnicích*. Praha: Grada, 2011. Expert (Grada). ISBN 978-80-247-3221-3.

GÁLA, Libor, Jan POUR a Prokop TOMAN. *Podniková informatika: počítačové aplikace v podnikové a mezipodnikové praxi, technologie informačních systémů, řízení a rozvoj podnikové informatiky.* Praha: Grada, 2006. Management v informační společnosti. ISBN 80-247-1278-4.

KAFKA, Tomáš. *Průvodce pro interní audit a risk management.* Praha: C.H. Beck, 2009. C.H. Beck pro praxi. ISBN 978-80-7400-121-5.

Poznámky

Obsahové upřesnění

OV RVP - Odborné vzdělávání ve vztahu k RVP