Střední škola informatiky, poštovnictví a finančnictví Brno, příspěvková organizace

Témata pro praktickou část maturitní zkoušky z odborných předmětů

Předmět: Praktická zkouška z odborných předmětů

Obor: 37-42-M/01 Logistické a finanční služby

Název ŠVP: **Bezpečnost dat ve veřejné zprávě**

Třída: BD4

Školní rok: 2023/2024

Praktická zkouška bude probíhat 2 dny:

1. **Den**

   Dílčí zkouška I.

   - Evidence aktiv a hodnocení rizik v programu CSA, výpočty hrozeb dopadu.

2. **Den**

   Dílčí zkouška II.

   - Ekonomické výpočty.

V časových limitech jsou zohledněni žáci se specifickými poruchami učení.

Schváleno ředitelem Střední školy informatiky, poštovnictví a finančnictví Brno

dne 27. března 2024 Ing. Olga Hölzlova

Zajištění praktické zkoušky:

Zkoušky budou probíhat v odborné učebně JCEKB a v učebně Fiktivní firmy D3/203.

Zkoušející učitel PV

- Ing. Vladimír Šulc, Ph. D;
- Renata Müllerová;
- Veronika Seidlová.

Hodnocení praktické zkoušky

Dílčí zkouška I.

Počet bodů	Hodnocení
100–88	výborný
87–72	chvalitebný
71–60	dobrý
59–40	dostatečný
39–0	nedostatečný

Dílčí zkouška II.

Počet bodů	Hodnocení
60-55	výborný
54-47	chvalitebný
46-39	dobrý
38-31	dostatečný
30-0	nedostatečný

Celkové hodnocení praktické zkoušky:

Celkové hodnocení se stanoví vážným aritmetickým průměrem z hodnocení jednotlivých dílčích zkoušek. V případě nerozhodného hodnocení se přihlédne k hodnocení dílčí zkoušky I.

Zadání praktické zkoušky

Dílčí zkouška I.

Zkouška má časovou dotaci 2 hodiny, skládá se ze 2 částí. První a druhá část je v délce 1 hodina. V první části student na základě zadaného příkladu doplní a vytvoří model informačního systému v analytickém nástroji. V dalším kroku vytvoří hrozby a přiřadí je v aktivum, na které působí dané hrozby. Uvede možné typy zranitelnosti aktiv, popíše riziko a navrhne dané opatření.

Hodnotí se:

- ✓ Jak je primární aktivum závislé na sekundárním aktivu.
- ✓ Závislost mezi sekundárními aktivy, kterými jsou prostory, HW, SW, síť, lidé.
- ✓ Co se stane, když bude narušena bezpečnost kteréhokoliv sekundárního aktiva, jaký to může mít dopad na primární aktivum.
- ✓ Kdy může dojít k narušení důvěrnosti, integrity a dostupnosti a jak se to projeví? Jaká by mohla vzniknout škoda a komu?
- ✓ Vztah mezi sekundárními aktivy a mezi primárním aktivem.
- ✓ Hrozby, kterým bude tento systém čelit a na jaké aktivum bude hrozba působit, např.: Hacking webového serveru, DOS – odepření služby, krádež osobních údajů ze strany zdravotnického personálu, atd…
- ✓ Jaká je pravděpodobnost těchto hrozeb a proč si to myslíte?
- ✓ Navrhněte opatření, které by organizace měla zavést
- ✓ Proti jakým hrozbám budou daná opatření účinná a zdůvodněte proč.
- ✓ Jak by se dala stanovit účinnost těchto opatření?
- ✓ Vypočítá riziko a vysvětlí, jakou zvolili hodnotu dopadu, zranitelnost.

Část první

Na učebně „Kyber centra“ spustí student webovou aplikaci CSA, kde zadá do systému v rámci daného příkladu fiktivní organizace evidenci aktiv, hrozeb a zranitelnosti a identifikuje rizika a nedostatky ve své kybernetické bezpečnosti. Maximální počet bodů 50.

Část druhá

Výstupem z aplikace CSA bude celkové hodnocení úrovně kybernetické bezpečnosti, které slouží především k nápravě nedostatků v oblasti kybernetické bezpečnosti a zlepšení jejího dosavadního stavu. Uživatel bude disponovat komplexním obrazem o kybernetické bezpečnosti v organizaci. Maximální počet bodů 50.

Dílčí zkouška II.

Zkouška má časovou dotaci 2 hodiny. Žák podle zadání zpracuje účetní příklad. Sestaví počáteční rozvahu obchodní společnosti, provede jednotlivé účetní operace, sestaví výkaz zisku a ztráty, vypočítá hospodářský výsledek obchodní společnosti, vypočítá daňovou povinnost a daňové odpisy DHM. Žák může získat max. 60 bodů.

V časových limitech jsou zohledněni žáci se specifickými poruchami učení.

Hodnotí se:

- správnost řešení;
- logické myšlení;
- znalost problematiky;
- pracovní postupy;
- korektnost jednotlivých operací.