Vysoká škola: Žilinská univerzita v Žiline, KC KYB UNIZA	
Kód kurzu: MKBVS	**Názov kurzu:** Manažér kybernetickej bezpečnosti vo verejnej správe
Druh, rozsah a metóda vzdelávacích činností:	
Týždenný počet hodín výučby vo forme prednášky, cvičenia, semináre	priebežne
Kapacita kurzu	Max. 25
Metóda, akou sa vzdelávacia činnosť uskutočňuje	Výučba sa uskutočňuje prezenčne
Metódy dosiahnutia výsledkov vzdelávania	Odporúčané metódy a techniky vyučovania: Prednáška: motivačné rozprávanie (možnosti využitia výsledkov vzdelávania v praxi), výklad, problémový výklad, prezentácia, prezentácia s podporou multimédií, interaktívna prednáška s diskusiou, metóda otázok a odpovedí. Diskusia a praktické cvičenia: diskusia a práca v skupine, riešenie problémov, príprava zadaní, testovanie nadobudnutých vedomostí a zručností.
Záťaž študenta: 50 hodín.	

Podmienky na absolvovanie kurzu:

Vstupné hodnotenie:

- Overenie vstupných vedomostí:
- Nástroj hodnotenia: Absolvovanie vstupného elektronického testu

Priebežné hodnotenie:

- Vedomosti z obsahu prednášok a skúsenosti z praktických cvičení
- Nástroj hodnotenia: 4x elektronický test po skončení každého bloku

- Účasť na kurze: minimálne 75 % (37,5hodiny z 50).
- Nástroj hodnotenia: prezenčná listina

Záverečné hodnotenie:

- Podmienkou pre úspešné absolvovanie kurzu je získanie minimálne 55 % správnych odpovedí z každého zo 4 priebežných elektronických testov
- Nástroj hodnotenia: osvedčenie

Formy a metódy hodnotenia	Váha %	Oblasť vedomostí, zručností, kompetentností
Elektronický test – Blok I	25	Právny rámec, organizácia KB a strategické plánovanie
Elektronický test – Blok II	25	Organizačné opatrenia
Elektronický test – Blok III	25	Personálne a fyzické opatrenia
Elektronický test – Blok IV	25	Technické opatrenia

Výsledky vzdelávania:

Kurz Manažér kybernetickej bezpečnosti vo verejnej správe poskytuje rozsiahle vedomosti v oblasti informačnej a kybernetickej bezpečnosti (KB), pričom účastníci získajú prehľad o národnom a európskom normatívnom rámci a reguláciách, vrátane legislatívy (napr. NIS2, GDPR) a technických predpisov (napr. rada noriem STN ISO/IEC 27000). Budú rozumieť úlohám a zodpovednostiam v kybernetickej bezpečnosti a osvoja si princípy riadenia informačnej bezpečnosti, vrátane systémov manažérstva informačnej bezpečnosti (ISMS), bezpečnostnej dokumentácie a metodík hodnotenia bezpečnosti.

Dôležitou súčasťou je správa aktív a ochrana informácií, kde sa účastníci naučia klasifikovať a označovať informácie, pracovať s manažmentom aktív a rozumieť atribútom informačnej bezpečnosti. Kurz sa venuje aj manažmentu rizík KB, pričom účastníci získajú znalosti o metódach posudzovania rizík, stratégiách ich ošetrenia a procesoch monitorovania. Osobitná pozornosť je venovaná bezpečnosti dodávateľského reťazca a auditu kybernetickej bezpečnosti, kde účastníci pochopia normatívne požiadavky na dodávateľov, hodnotenie ich dôveryhodnosti a zásady compliance v oblasti KB. Súčasťou kurzu je aj kontinuita činností a krízové riadenie, kde sa účastníci naučia tvoriť plány kontinuity činností, obnovy systémov po havárii a testovať manažment kontinuity činností (BCM). Po technickej stránke kurz zahŕňa témy ako sieťová bezpečnosť, kryptografia, správa identít, hardening systémov, aplikačná bezpečnosť a ochrana proti škodlivému kódu. Účastníci sa zoznámia s princípmi bezpečného vývoja softvéru, testovania bezpečnosti systémov a správou bezpečnostných konfigurácií.

V oblasti praktických zručností kurz pripravuje účastníkov na aplikáciu bezpečnostných štandardov, implementáciu ISMS a používanie bezpečnostnej dokumentácie. Osvoja si metódy riadenia kybernetických rizík, analýzu a návrh opatrení a riešenie kybernetických incidentov. Kurz ich naučí aj hodnotiť bezpečnosť dodávateľského reťazca, implementovať opatrenia na zvýšenie bezpečnosti a testovať plány kontinuity činností. Dôležitou súčasťou sú praktické zručnosti v konfigurácii a hardeningu systémov, posudzovaní zraniteľností, monitorovaní bezpečnostných udalostí a vykonávaní penetračných testov. Absolventi budú schopní realizovať bezpečnostné audity, kontrolovať súlad s legislatívou a používať bezpečnostné nástroje na ochranu informačných systémov. Tento kurz poskytuje komplexné vedomosti a praktické zručnosti potrebné pre efektívne riadenie informačnej a kybernetickej bezpečnosti vo verejnom sektore.

Stručná osnova kurzu:

1. Právny rámec, organizácia KB a strategické plánovanie (Blok I):
    a. Organizácia a riadenie informačnej bezpečnosti a kybernetickej bezpečnosti
    b. Správa aktív, ochrana záznamov, súkromia a označovanie informácií
    c. Riadenie kybernetických hrozieb a rizík
2. Organizačné opatrenia (Blok II):
    a. Dodávateľský reťazec
    b. Riadenie udalostí a kybernetických bezpečnostných incidentov
    c. Riadenie kontinuity činností, zálohovanie, obnova systémov po havárii a krízové riadenie
    d. Postupy posudzovania účinnosti opatrení, riadenie súladu a kontrolné činnosti
3. Personálne a fyzické opatrenia (Blok III):
    a. Bezpečnosť a spôsobilosti ľudských zdrojov
    b. Fyzická bezpečnosť, bezpečnosť prostredia a správa koncových zariadení
4. Technické opatrenia (Blok IV):
    a. Úvod k prevádzke elektronických komunikačných systémov
    b. Bezpečnosť pri nadobúdaní, vývoji a údržbe IS a siete, komunikačná bezpečnosť
    c. Kryptografické opatrenia a zásady používania kryptografie

d. Správa zraniteľností a kybernetických hrozieb e. Správa identít a prístupov f. Bezpečnosť konfigurácií g. Monitorovanie, zaznamenávanie a hlásenie udalostí h. Aplikačná bezpečnosť a bezpečnosť cloudových systémov i. Podniková a bezpečnostná architektúra j. Bezpečný vývoj a testovanie softvéru k. Ochrana proti škodlivému kódu a nežiaducemu obsahu
Odporúčaná literatúra: N/A
Jazyk, ktorého znalosť je potrebná na absolvovanie kurzu: slovenský
Poznámky:
Vyučujúci: viď. príloha
Dátum poslednej zmeny: 2025
Garant kurzu: prof. Ing. Tomáš Loveček, PhD.
Schválil: prof. Ing. Tomáš Loveček, PhD. (garant ŠP)