

Vysoká škola: Žilinská univerzita v Žiline, KC KYB UNIZA	
Kód kurzu: OZKBVS	Názov kurzu: Odborný zamestnanec kybernetickej bezpečnosti vo verejnej správe
Druh, rozsah a metóda vzdelávacích činností:	
Týždenný počet hodín výučby vo forme prednášky, cvičenia, semináre	23.5.2025 30.5.2025 6.6.2025 13.6.2025 20.6.2025 27.6.2025
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 zadání, 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: 8x 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 z 8 priebežných elektronických testov - Nástroj hodnotenia: osvedčenie	

Formy a metódy hodnotenia	Váha %	Oblasť vedomostí, zručností, kompetentností
Eletronický test – Blok I	12,5	Úvod do kybernetickej bezpečnosti
Eletronický test – Blok II	12,5	Bezpečnostné riziká, opatrenia a prevencia
Eletronický test – Blok III	12,5	Identifikácia a autentizácia
Eletronický test – Blok IV	12,5	Autorizácia, monitorovanie a riešenie incidentov
Eletronický test – Blok V	12,5	Ochrana koncových zariadení v LAN a online bezpečnosť
Eletronický test – Blok VI	12,5	Bezpečnosť pri bezdrôtovej komunikácii, vzdialenom prístupe, využívaní cloudu a IoT zariadení
Eletronický test – Blok VII	12,5	Ochrana dát a súkromia
Eletronický test – Blok VIII	12,5	Sociálne inžinierstvo a reakcie na incidenty ním spôsobené

Výsledky vzdelávania:

Kurz „Odborný zamestnanec kybernetickej bezpečnosti vo verejnej správe“ poskytuje účastníkom základné vedomosti z oblasti kybernetickej bezpečnosti, pričom sa zameriava na jej aplikáciu vo verejnom sektore. Študenti získajú prehľad o národných a európskych normatívnych rámcoch. Kurz sa venuje úvodu do kybernetickej bezpečnosti a jej významu vo verejnej správe, pričom účastníci pochopia základné pojmy, koncepty a bezpečnostné princípy.

Dôležitou témou je manažment rizík, ktorý zahŕňa identifikáciu kybernetických hrozieb a analýzu bezpečnostných opatrení, vrátane testovania zraniteľností. Kurz sa venuje aj identifikácii a autentizácii, kde účastníci získajú prehľad o technikách overovania identity a metódach riadenia prístupu. V oblasti autorizácie a monitorovania sa účastníci oboznámia s riešením kybernetických incidentov a zásadami kontroly prístupu.

Veľká pozornosť sa venuje ochrane koncových zariadení v LAN sieťach a online bezpečnosti. Účastníci kurzu získajú znalosti o počítačových sieťach, spôsoboch ochrany systémov a zariadení, ako aj o bezpečnosti pri bezdrôtovej komunikácii, vzdialenom prístupe a využívaní cloudových služieb či IoT zariadení. Kurz sa zaoberá aj témami digitálneho súkromia, kybernetickej bezpečnosti v trestnom práve a ochranou osobných údajov, pričom účastníci sa naučia zásady ochrany dát a používania digitálnych podpisov.

Významnou časťou kurzu je sociálne inžinierstvo a reakcie na incidenty, ktoré s ním súvisia. Študenti sa naučia rozpoznávať pokusy o manipuláciu, pochopia ochranné opatrenia a budú sa venovať simuláciám sociálneho inžinierstva v praxi. Kurz tiež poskytuje základné vedomosti o kryptografii, digitálnej bezpečnosti a metodikách zabezpečenia citlivých informácií.

V rámci praktických zručností účastníci získajú schopnosť aplikovať bezpečnostné opatrenia v praxi, analyzovať a riešiť bezpečnostné incidenty, testovať zraniteľnosti systémov a identifikovať riziká spojené s používaním rôznych technológií. Oboznámia sa so zásadami bezpečnej správy identít a prístupov, ako aj s monitorovaním bezpečnostných udalostí. Dôležitou súčasťou je aj implementácia bezpečnostných politík a testovanie reakcií na kybernetické hrozby.

Program poskytuje komplexné vedomosti a praktické zručnosti potrebné pre odborných zamestnancov verejnej správy, ktorí sa venujú kybernetickej bezpečnosti a ochrane informačných systémov.

Stručná osnova kurzu:

1. Úvod do kybernetickej bezpečnosti (KB) (Blok I):
 - a. Úvod do kurzu a základné pojmy a koncepty KB
 - b. KB vo verejnej správe
2. Bezpečnostné riziká, opatrenia a prevencia (Blok II):
 - a. Manažment rizík
 - b. Typy KB hrozieb a útokov
 - c. Bezpečnostné opatrenia, test zraniteľností
3. Identifikácia a autentizácia (Blok III):
 - a. Základy identifikácie, autentizácie a autorizácie
 - b. Techniky autentizácie a overovania
4. Autorizácia, monitorovanie a riešenie incidentov (Blok IV):
 - a. Autorizácia a riadenie prístupu
 - b. Monitorovanie a riešenie incidentov
5. Ochrana koncových zariadení v LAN a online bezpečnosť (Blok V.):
 - a. Základy počítačových sietí a komunikácie
 - b. Ochrana systémov a koncových zariadení
6. Bezpečnosť pri bezdrôtovej komunikácii, vzdialenom prístupe, využívaní cloudu a IoT zariadení (Blok VI.):
 - a. Bezdrôtové siete a ich zabezpečenie
 - b. Bezpečnosť mobilných zariadení
 - c. Vzdialený prístup a VPN
 - d. Zraniteľnosti IoT zariadení
 - e. Cloudové služby a ich bezpečnosť
7. Ochrana dát a súkromia (Blok VII.):
 - a. Digitálne súkromie
 - b. Základné zásady (kyber)bezpečnosti
 - c. Základné zásady ochrany osobných údajov
 - d. Kybernetická bezpečnosť a trestné právo
 - e. Digitálny podpis
 - f. Základy kryptografie
8. Sociálne inžinierstvo a reakcie na incidenty ním spôsobené (Blok VIII.):
 - a. Úvod do sociálneho inžinierstva
 - b. Rozpoznávanie sociálneho inžinierstva v praxi, ochrana a prevencia
 - c. Simulácie sociálneho inžinierstva
 - d. Overenie vedomostí

Garant kurzu: prof. Ing. Milan Kubina, PhD.

Schválil: prof. Ing. Milan Kubina, PhD. (garant ŠP)