

### Charakteristika vzdelávacích potrieb

| Kategória používateľov | Popis kategórie používateľov   | Cieľ vzdelávania pre príslušnú kategóriu   |
|------------------------|--|--|
| laik                   | používateľ IKT okrem výkonu konkrétneho povolania  | a) porozumieť vybraným základným pojmom kybernetickej bezpečnosti,<br>b) porozumieť významu osobných údajov a citlivých informačných aktív v mimopracovnej oblasti<br>a osvojiť si základné pravidlá bezpečnej manipulácie a používania IKT.   |
| odborný zamestnanec    | používateľ, ktorý pri výkone povolania využíva sieť alebo informačný systém  | a) porozumieť vybraným základným pojmom kybernetickej bezpečnosti,<br>b) porozumieť svojej úlohe a zodpovednosti v systéme kybernetickej bezpečnosti,<br>c) chápať význam informačných aktív s ktorými zamestnanec pracuje,<br>d) porozumieť potrebe ochrany informácií a informačných aktív,<br>e) osvojiť si základné pravidlá bezpečnej práce s IKT,<br>f) rozpoznať incident a vedieť naň správne reagovať,<br>g) porozumieť bezpečnostným politikám a používaniu bezpečnostných mechanizmov v pracovných procesoch.           |
| manažér                | riadiaci zamestnanec, ktorý nie je IT manažérom alebo manažérom kybernetickej bezpečnosti a ktorý spravdla zodpovedá za príslušný proces alebo skupinu procesov a v rámci nich zodpovedá aj za plnenie úloh v oblasti riadenia rizík kybernetickej bezpečnosti | a) porozumieť vybraným základným pojmom kybernetickej bezpečnosti,<br>b) porozumieť rizikám kybernetickej bezpečnosti v riadených procesoch,<br>c) nadobudnúť schopnosť analyzovať požadovanú úroveň ochrany informačných aktív,<br>d) nadobudnúť schopnosť integrovať požiadavky kybernetickej bezpečnosti do procesov a úloh podriadených zamestnancov,<br>e) naučiť sa definovať a dohliadať na plnenie požiadaviek kybernetickej bezpečnosti pri obstaraní produktov a služieb a pri procesoch podporovaných tretími stranami. |
| IT manažér             | riadiaci zamestnanec organizačných jednotiek zodpovedných za poskytovanie IT služieb, návrh, implementáciu, obstaranie, prevádzku, údržbu a posudzovanie prostriedkov IKT  | a) porozumieť významu kybernetickej bezpečnosti pre činnosť organizácie,<br>b) poznať jednotlivé oblasti kybernetickej bezpečnosti,<br>c) porozumieť systému riadenia bezpečnosti informácií a informačných aktív a osvojiť si ho,<br>d) nadobudnúť schopnosť implementovať bezpečnostné opatrenia v konkrétnom prostredí,   |

|   |   |   |
|---|---|---|
|   |   | <p>e) nadobudnúť schopnosť určiť zodpovednosti zamestnancov organizácie vo vzťahu k informačným a komunikačným technológiám,</p> <p>f) osvojiť si metódy vyhodnocovania efektívnosti prijatých bezpečnostných opatrení,</p> <p>g) vedieť definovať a kontrolovať plnenie požiadaviek kybernetickej bezpečnosti pri obstarávaní, dodávaní, správe, prevádzke, údržbe a rozvoji sietí a informačných systémov a ich komponentov,</p> <p>h) nadobudnúť schopnosť presadzovať politiky kybernetickej bezpečnosti v organizácii.</p>   |
| informatik                              | zamestnanec zodpovedný za poskytovanie IT služieb, návrh, implementáciu, obstaranie, prevádzku, údržbu a posudzovanie IKT   | <p>a) doplniť vlastné odborné znalosti špecificky pre oblasť kybernetickej bezpečnosti,</p> <p>b) porozumieť podstate bezpečnostných požiadaviek na IKT a IT služby,</p> <p>c) porozumieť zraniteľnostiam, hrozbám a rizikám spojeným s používanými IKT a IT službami,</p> <p>d) nadobudnúť schopnosť navrhnúť, implementovať, udržiavať a prevádzkovať mechanizmy na naplnenie bezpečnostných požiadaviek na IKT a IT služby,</p> <p>e) nadobudnúť zručnosť kvalifikovane komunikovať a spolupracovať so špecialistami kybernetickej bezpečnosti, formulovať problémy, posudzovať a implementovať navrhované opatrenia.</p>  |
| zamestnanec v kybernetickej bezpečnosti | zamestnanec špecializovaný na oblasť bezpečnosti informácií a riadenia rizík kybernetickej bezpečnosti, zodpovedný za návrh, implementáciu, obstaranie, prevádzku, údržbu a posudzovanie bezpečnostných mechanizmov a riešení | <p>a) poznať a osvojiť si právne a etické požiadavky na zaručenie bezpečnosti informačných aktív,</p> <p>b) rozumieť zraniteľnostiam, hrozbám a rizikám v informačnej a kybernetickej bezpečnosti,</p> <p>c) nadobudnúť schopnosť navrhnúť, implementovať, udržiavať a prevádzkovať bezpečnostné mechanizmy a riešenia,</p> <p>d) nadobudnúť schopnosť navrhovať a prezentovať bezpečnostné stratégie, bezpečnostné politiky a bezpečnostnú architektúru,</p> <p>e) nadobudnúť znalosti o technikách a metódach vyhodnocovania efektívnosti bezpečnostných mechanizmov a riešení a uplatňovať ich v procesoch organizácie,</p> <p>f) nadobudnúť zručnosť kvalifikovane komunikovať a spolupracovať s informatikmi, formulovať problémy, posudzovať a implementovať navrhované opatrenia,</p> <p>g) nadobudnúť schopnosť navrhovať procesy riadenia rizík v informačnej a kybernetickej bezpečnosti.</p> |

|  |  |   |
|--|--|---|
| <p>manažér kybernetickej bezpečnosti</p>             | <p>riadiaci zamestnanec špecializovaný na oblasť bezpečnosti informácií a riadenia rizík kybernetickej bezpečnosti, vlastníci bezpečnostných procesov</p>  | <ul style="list-style-type: none"> <li>a) nadobudnúť schopnosť vytvoriť rámec riadenia kybernetickej bezpečnosti v organizácii,</li> <li>b) nadobudnúť schopnosť riadiť procesy súvisiace s informačnou a kybernetickou bezpečnosťou v organizácii,</li> <li>c) nadobudnúť schopnosť formulovať návrhy a odporúčania na obstaranie, implementáciu, prevádzku a vyhodnocovanie bezpečnostných mechanizmov a riešení a navrhovať a manažovať procesy riadenia rizík v informačnej a kybernetickej bezpečnosti,</li> <li>d) nadobudnúť schopnosť navrhovať, implementovať, udržiavať a prevádzkovať bezpečnostné mechanizmy a riešenia,</li> <li>e) nadobudnúť znalosti o právnych a etických požiadavkách na zaručenie bezpečnosti informačných aktív,</li> <li>f) nadobudnúť schopnosť navrhovať a prezentovať bezpečnostné stratégie, bezpečnostné politiky a bezpečnostnú architektúru,</li> <li>g) nadobudnúť a osvojiť si znalosti o technikách a metódach vyhodnocovania efektívnosti bezpečnostných mechanizmov a riešení a schopnosť uplatňovať ich v procesoch organizácie,</li> <li>h) nadobudnúť schopnosti pri presadzovaní bezpečnostných opatrení.</li> </ul> |
| <p>auditor a výskumník kybernetickej bezpečnosti</p> | <p>odborný zamestnanec špecializovaný na oblasť výskumu alebo posudzovania kybernetickej bezpečnosti, analýzy rizík, testovania a vyhodnocovania efektivity bezpečnostných opatrení, posudzovania zhody a súladu</p> | <ul style="list-style-type: none"> <li>a) nadobudnúť schopnosti v rozsahu podľa predchádzajúcich cieľov platných pre všetky ostatné kategórie,</li> <li>b) vykonať audit kybernetickej bezpečnosti a posúdiť efektívnosť prijatých bezpečnostných opatrení podľa vyhlášky Národného bezpečnostného úradu č. 436/2019 Z. z. o audite kybernetickej bezpečnosti a znalostnom štandarde audítora a platných auditných metodík.</li> </ul>  |