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, b) porozumieť významu osobných údajov a citlivých informačných aktív v mimopracovnej oblasti 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, b) porozumieť svojej úlohe a zodpovednosti v systéme kybernetickej bezpečnosti, c) chápať význam informačných aktív s ktorými zamestnanec pracuje, d) porozumieť potrebe ochrany informácií a informačných aktív, e) osvojiť si základné pravidlá bezpečnej práce s IKT, f) rozpoznať incident a vedieť naň správne reagovať, 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 spravidla 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, b) porozumieť rizikám kybernetickej bezpečnosti v riadených procesoch, c) nadobudnúť schopnosť analyzovať požadovanú úroveň ochrany informačných aktív, d) nadobudnúť schopnosť integrovať požiadavky kybernetickej bezpečnosti do procesov a úloh podriadených zamestnancov, 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, b) poznať jednotlivé oblasti kybernetickej bezpečnosti, c) porozumieť systému riadenia bezpečnosti informácií a informačných aktív a osvojiť si ho, d) nadobudnúť schopnosť implementovať bezpečnostné opatrenia v konkrétnom prostredí,

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

manažér kybernetickej bezpečnosti	riadiaci zamestnanec špecializovaný na oblasť bezpečnosti informácií a riadenia rizík kybernetickej bezpečnosti, vlastníci bezpečnostných procesov	a) nadobudnúť schopnosť vytvoriť rámec riadenia kybernetickej bezpečnosti v organizácii, b) nadobudnúť schopnosť riadiť procesy súvisiace s informačnou a kybernetickou bezpečnosťou v organizácii, 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, d) nadobudnúť schopnosť navrhovať, implementovať, udržiavať a prevádzkovať bezpečnostné mechanizmy a riešenia, e) nadobudnúť znalosti o právnych a etických požiadavkách na zaručenie bezpečnosti informačných aktív, f) nadobudnúť schopnosť navrhovať a prezentovať bezpečnostné stratégie, bezpečnostné politiky a bezpečnostnú architektúru, g) nadobudnúť a osvojiť si znalosti o technikách a metódach vyhodnocovania efektívnosti bezpečnostných mechanizmov a riešení a schopnosť uplatňovať ich v procesoch organizácie, h) nadobudnúť schopnosti pri presadzovaní bezpečnostných opatrení.
audítor a výskumník kybernetickej bezpečnosti	odborný zamestnanec špecializovaný na oblasť výskumu alebo posudzovania kybernetickej bezpečnosti, analýzy rizík, testovania a vyhodnocovania efektivity bezpečnostných opatrení, posudzovania zhody a súladu	a) nadobudnúť schopnosti v rozsahu podľa predchádzajúcich cieľov platných pre všetky ostatné kategórie, 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.