

# Národní kvalifikační rámec terciárního vzdělávání

## BEZPEČNOSTNÍ OBORY



evropský  
sociální  
fond v ČR



EVROPSKÁ UNIE



MINISTERSTVO ŠKOLSTVÍ,  
MLÁDEŽE A TĚLOVÝCHOVY



OP Vzdělávání  
pro konkurenceschopnost

INVESTICE DO ROZVOJE VZDĚLÁVÁNÍ

SPOLUFINANCOVÁNO EVROPSKÝM SOCIÁLNÍM FONDEM A STÁTNÍM ROZPOČTEM ČESKÉ REPUBLIKY

## **Oblasti vzdělávání v Národním kvalifikačním rámci terciárního vzdělávání**

Oblastí vzdělávání se rozumí ucelený a vzájemně související úsek terciárního vzdělávání, v jehož rámci vznikají a uskutečňují se studijní programy. Oblast vzdělávání přitom není pouhým souhrnem v současnosti uskutečňovaných studijních programů s určitým společným jádrem, ale spíše prostorem, který by měl umožnit flexibilní vývoj studijních programů v budoucnu (integrace a další přeměny existujících programů a vznik programů nových).

Oblast vzdělávání je vymezena především deskriptory popisujícími výstupy z učení, které standardizovanou formou vyjadřují cíle vzdělávání a rovněž odrážejí společný teoretický metodologický, případně také filozofický a hodnotový základ dané oblasti vzdělávání.

**Obecný popis oblasti vzdělávání** zahrnuje zejména:

- jednoduchý a výstižný název oblasti vzdělávání;
- stručný popis historie, povahy a tematického rozsahu oblasti vzdělávání;
- poslání oblasti vzdělávání (co je předmětem a cílem poznávání v dané oblasti);
- uvedení páteřních oborů, které jsou jako akademické disciplíny pro danou oblast vzdělávání charakteristické a určující;
- vymezení cílů vzdělávání v dané oblasti;
- rámcový profil absolventů v dané oblasti vzdělávání s uvedením charakteristických profesí, zejména pak profesí regulovaných, které jsou relevantní;
- vztahy k ostatním oblastem vzdělávání (vč. mezních oborů).

**Deskriptory oblastí vzdělávání** převádějí volněji formulované popisy oblastí vzdělávání do kategorie očekávaných výstupů z učení – znalostí, dovedností a dalších způsobilostí (kompetencí) absolventů, a to v souladu s národními deskriptory kvalifikačního rámce. Zaměřují se přitom na:

- **odborné znalosti** (konkretizace faktických i teoretických znalostí a stupně porozumění typického absolventa páteřního oboru),
- **odborné dovednosti** (konkretizace výzkumných, uměleckých nebo jiných praktických postupů uplatňujících odborné znalosti dané úrovně).

Pokud jde o obecné způsobilosti, tato kategorie vyjadřuje především kontext, v němž se od absolventa očekává, že bude odborné znalosti a odborné dovednosti uplatňovat, a míru samostatnosti a odpovědnosti, s jakou tak bude činit. Obecné způsobilosti jsou obecně popsány národními deskriptory jako společné napříč všemi oblastmi vzdělávání, a deskriptory oblastí vzdělávání proto tento typ výstupů z učení v zásadě nespecifikují.

## **Závaznost oblastí vzdělávání**

Je přirozené, že existující oblasti vzdělávání zahrnují širokou a proměnlivou škálu oborů s různou mírou akademického nebo naopak profesního zaměření, z nichž některé se nacházejí na pomezí dalších oblastí vzdělávání. Účelem formulace deskriptorů oblastí vzdělávání proto zjevně nemůže být stanovení minimálního standardu platného pro všechny obory v dané oblasti vzdělávání, ani stanovení akademicky optimálního profilu absolventa. **Deskriptory oblastí vzdělávání se budou vztahovat k typickému absolventu páteřního oboru oblasti vzdělávání a budou vyvážené brát v úvahu akademický i profesní účel vzdělávání.** V tom se liší od národních deskriptorů, které představují minimální standard, tedy charakterizují odborné znalosti, odborné dovednosti a obecné způsobilosti, které musí absolvent prokazovat při absolvování daného stupně vzdělání.

# BEZPEČNOSTNÍ OBORY

## STRUČNÝ POPIS POVAHY, TEMATICKÉHO ROZSAHU A HISTORIE OBLASTI

Výraz „bezpečnost“ má svůj původ v základu „sine cura“, čili bez starostí, bez problémů, mimo nebezpečí. Bezpečnost je v obecném slova smyslu jedna ze základních vlastností přírodního, technologického nebo společenského systému. Pokud uvedený systém takovou vlastnost má, pak se nachází v nekonfliktní interakci (v rovnovážném stavu) se svým okolím i sám se sebou (vykazuje vnější i vnitřní stabilitu). Za těchto okolností je schopen poskytovat veškeré funkce a vykazovat parametry, pro které byl v reálném i virtuálním světě vytvořen a není hrozbou pro sebe i své okolí. Bezpečnostní obory se věnují systematickému studiu této problematiky v kontextu všech souvislostí, jež vedou ke změně nekonfliktní interakce na interakci konfliktní a současně i vymezují postupy, které umožňují nekonfliktní interakci obnovit.

Historicky tato oblast vzdělávání existuje od doby, kdy se začaly rozvíjet tradiční vědní disciplíny orientované na rozvoj poznání a pochopení zákonitostí, podle kterých se chovají přírodní, technologické nebo společenské systémy. Větší či menší zájem o rozvoj poznání a systematické studium v oblasti bezpečnostních oborů byl v této době obvykle závislý na tom, do jaké míry se konfliktní interakce bezprostředně promítaly do života člověka, jako reálné hrozby. Přitom nebylo podstatné, byl-li shledáván zdroj jejich původu v samotné přírodě, v používaných technologických postupech či materiálech, nebo všech pravděpodobných interakcích, vznikajících při vzájemném ovlivňování se prvků linie člověk – technologie – prostředí. Z historického hlediska je třeba považovat za velmi významné, že se tato oblast vzdělávání postupně začala stávat nástrojem k cílevědomému a záměrnému vyvolávání konfliktních interakcí samotným člověkem. To dalo popud ke vzniku zcela nové kategorie hrozeb, majících svůj původ v antropogenní oblasti. Dlouhodobě získávané zkušenosti v současnosti vedou k tomu, že stát řídí a kontroluje vzdělávání ve vybraných segmentech (armáda, policie, státní správa apod.) této oblasti vzdělávání. Je totiž zřejmé, že stát musí být v obecném slova smyslu odpovědný za vytvoření podmínek vnitřní i vnější bezpečnosti jednotlivce i společnosti jako celku.

Bezpečnostní obory reprezentují oblast vzdělávání, která se zaměřuje na cílevědomě řízené a prováděné lidské činnosti, které zahrnují problematiku interakcí systému se svým okolím i se sebou samým a primárně vedou do nerovnovážného stavu. Přitom obecným cílem poznání v této oblasti vzdělávání, je znát a umět postupovat tak, aby se zachoval systém v nekonfliktní interakci, tedy nestal se hrozbou. Absolventi studia na straně jedné musí disponovat schopností předpovídat, rozpoznávat či preventivně odstraňovat stavy, jež mohou vést ke vzniku konfliktních interakcí. Na straně druhé, musí disponovat schopností analyzovat, nalézat postupy a řešení v situacích, jež umožní náhodně či uvědoměle vzniklé konfliktní interakce eliminovat.

## PÁTEŘNÍ OBORY

Tradiční vědní disciplíny, které jsou především aplikačně rozvíjeny v oblasti vzdělávání „bezpečnostní obory“, jsou přírodní vědy, společenské vědy, technické vědy, zdravotnictví a vojenství. Jejich nadstavbu, společnou všem oborům této oblasti vzdělávání, tvoří páteřní obory. Jsou představovány problematikou vyučovanou v takových disciplínách, jako je bezpečnostní politika, řízení bezpečnosti ve veřejném a soukromém sektoru, metodologie analýzy rizik, právo a normy v oblasti bezpečnosti, společenské aspekty bezpečnosti, logistika v oblas-

ti bezpečnosti a aplikovaná informatika. Obsahové vymezení těchto páteřních oborů představuje minimální společný vzdělávací základ této oblasti vzdělávání. V následující tabulce je uvedeno toto obsahové vymezení na bakalářské úrovni. S tím pak koresponduje patřičně redukované obsahové vymezení pro krátký cyklus a kvalitativně i kvantitativně rozšířené obsahové vymezení pro úroveň magisterskou a doktorskou. S uvedenou změnou obsahového vymezení páteřních oborů korelují především deskriptory oblasti vzdělávání „bezpečnostní obory“, které jsou uvedeny dále. Kromě toho, je za samozřejmost, plynoucí z mezinárodní dimenze této oblasti vzdělávání, považována schopnost absolventa komunikovat v některém ze světových jazyků, kde prioritní postavení přísluší jazyku anglickému.

#### **BEZPEČNOSTNÍ POLITIKA:**

Cílem je podat studentům ucelenou představu o problematice bezpečnostní politiky státu ve stávajícím bezpečnostním prostředí. Pozornost je věnována principům bezpečnostní politiky, základním hodnotám, zájmům, postojům a ambicím České republiky při zajišťování své bezpečnosti, prevenci a eliminaci bezpečnostních hrozeb a z nich vyplývajících rizik, s cílem zajistit vnitřní a vnější bezpečnost, obranu a ochranu občanů a státu. Důraz je kladen na komplexnost přístupu k vnitřní a vnější bezpečnosti, včetně definování bezpečnostního systému, jeho struktury, vymezení povinností, kompetencí a odpovědnosti jeho jednotlivých součástí. Součástí předmětu je seznámení se základními koncepčními a strategickými materiály státu, jako jsou bezpečnostní strategie, strategie udržitelného rozvoje a další strategie.

#### **ŘÍZENÍ BEZPEČNOSTI VE VEŘEJNÉM A SOUKROMÉM SEKTORU:**

Cílem je seznámit studenty se základy krizového managementu a jejich aplikací v oblasti bezpečnostního managementu, včetně pochopení místa a úlohy subjektů „nouzového“ a krizového řízení, součinnosti mezi hlavními aktéry při plánování opatření a zvládání mimořádných událostí a krizových situací. Pozornost je věnována schopnostem zabezpečovat preventivní opatření k ochraně obyvatelstva a jejich majetku, aplikovat poznatky krizového managementu při zabezpečení ochrany osob a majetku, vnitřní bezpečnosti a veřejného pořádku, ochraně ekonomiky a kritické infrastruktury a obrany státu, včetně schopnosti samostatně se rozhodovat a řídit podřízené jednotlivce a činnosti malého kolektivu.

#### **METODOLOGIE ANALÝZY RIZIK:**

Cílem je seznámit studenty s terminologií a klasifikačními aspekty rizik, významem a místem analýzy rizika v procesu zajišťování bezpečnosti procesů, systémů, organizace a regionu, s formulací zásad při sestavování rozsahu a cíle analýzy rizika, prezentací obecného postupu analýzy rizika, včetně základních metod užívaných při sběru vstupních dat. Pozornost je věnována výkladu nejobecnějších metod užívaných k sestavení registru nebezpečí, screeningu rizik, případových studií, modelování scénářů řešení rizik a posouzení jejich akceptovatelnosti, za účelem stanovení kritických rizik systému, organizace a regionu, s akcentem na praktickou využitelnost v oblasti veřejné správy, bezpečnostních služeb a bezpečnosti informačních a komunikačních technologií.

#### **PRÁVO, PRÁVNÍ A TECHNICKÉ PŘEDPISY A METODIKY V OBLASTI BEZPEČNOSTI:**

Cílem je poskytnout studentům základní znalosti o právní úpravě zajištění bezpečnosti ČR v oblasti ochrany obyvatelstva, společnosti a veřejného pořádku, ekonomiky, kritické infrastruktury a obrany státu, s obecnými pojmy a instituty práva obrany a bezpečnosti a se základními právními úpravami vnitřní a vnější bezpečnosti ČR. Pozornost je věnována rovněž výkladu podstaty a tvorby právní a technické normotvorné základny v oblasti bezpečnosti a její návaznosti na mezinárodní, smluvní, normotvorné a zákonné instituty.

**SPOLEČENSKÉ ASPEKTY BEZPEČNOSTI:**

Cílem je seznámit studenty s ochranou společnosti zejména ve vztahu k sociální a společenské problematice, v návaznosti na lidská práva, mezi něž patří lidská bezpečnost, zajištění svrchovanosti a územní celistvosti politického a demokratického zřízení a další práva a povinnosti v návaznosti na ochranu ekosystému, kritické infrastruktury a ochranu obyvatelstva. Pozornost je věnována orientaci v problematice ochrany společnosti jako celku, ve vztahu k ochraně společenských vztahů, závazků a obyvatelstva, seznámení s východisky, principy a metodami rozvoje individuálních a týmových profesních kompetencí, úlohou a funkcí bezpečnostních systémů a bezpečnostních služeb v sociálním prostředí.

**LOGISTIKA V OBLASTI BEZPEČNOSTI:**

Cílem je seznámit studenty se znalostmi z tvorby podpůrných zdrojů v oblasti personálního, materiálního, finančního, komunikačního a dalšího zabezpečení, ekonomické teorie, podnikové ekonomiky a managementu, sloužících k zpracovávání návrhů na implementaci logistických systémů v oblasti bezpečnosti. Pozornost je věnována vyhodnocování úrovně fungování logistiky, řízení logistických řetězců ve vazbě na zajišťování požadavků, optimalizaci nákladů, naplňování logistických koncepcí souvisejících s tvorbou a užitím zdrojů, s manipulací materiálů, umožňující orientaci v řízení logistických procesů, vztahujících se k bezpečnosti.

**APLIKOVANÁ INFORMATIKA:**

Cílem je poskytnout potřebné teoretické vědomosti a praktické dovednosti v oblasti aplikované informatiky, nezbytně nutné pro práci bezpečnostního a krizového manažera, které představují nadstavbu nad vědomostmi a dovednostmi, získanými studiem základního vysokoškolského kurzu v oblasti informatiky. Pozornost je věnována získání schopností a dovedností studentů samostatně navrhovat, vyhodnocovat a argumentačně hájit základní informačně-bezpečnostní řešení při využívání informačních a komunikačních technologií a osobních informačních systémů v oblastech svého profesního působení v oblasti bezpečnostního managementu.

**VYMEZENÍ CÍLŮ**

Předmětem a cílem poznávání v oblasti vzdělávání „bezpečnostní obory“ jsou hrozby, které ohrožují bezpečnost člověka a společnosti, a které mají svůj původ v přírodní, technologické a antropogenní oblasti.

Změny v klimatu a jeho důsledky v podobě např. povodní, větrných smrští, ale i další přírodní katastrofy, jako je zemětřesení, tsunami, sopečné výbuchy apod., jsou stále častějším jevem, který mnohdy nelze přesně lokalizovat a definovat. Závažné hrozby představují rovněž technologické havárie různých typů. V jejich rámci často dochází k narušení životně důležitých infrastruktur společnosti, jako je přerušení dodávek elektrické energie, plynu, k výpadkům komunikačních a informačních sítí apod., které jsou obvykle doprovázeny jak ekonomickými, tak i politickými dopady na život společnosti. Mezi hrozby, které mají svůj původ v antropogenní oblasti, patří vzrůstající a stále intenzivnější mezinárodní terorismus, neřešená problematika národnostních menšin, vzniklých v důsledku dlouhodobé a stále se zvyšující migrace, konflikty nepřizpůsobivých etnik s majoritami, proliferace zbraní hromadného ničení apod. Další hrozby pro člověka vyplývají z interakce člověk – stroj, resp. člověk – prostředí v rámci jeho pracovní činnosti, a to zejména s ohledem na zavádění nových technologií a široké používání řady nebezpečných látek.

Těmto negativním skutečnostem se musí přizpůsobit člověk jako jedinec, tak i činnost pevných a flexibilních bezpečnostních struktur veřejného i soukromého sektoru, a to jak v preventivní, tak v represivní oblasti. To vyžaduje mimo jiné také koncepční, cílevědomý a dlouhodobý přístup ke vzdělávání všech osob profesně působících v této oblasti. Většina evropských států si tyto skutečnosti plně uvědomuje a za tím účelem má vybudovaný, či buduje, sofistikovaný systém vzdělávání na všech jeho úrovních.

V kontextu uvedených skutečností je proto možné konstatovat, že poslání oblasti vzdělávání „bezpečnostní obory“ vyplývá z potřeby naplňovat ustanovení Listiny základních práv a svobod, dalších ústavních zákonů, obecně závazných právních předpisů, vyhlášek, norem i řady mezinárodních smluv, k jejichž dodržování se Česká republika zavázala, a které reflektují velice pestré spektrum hrozeb, kterým je člověk jako samostatný jedinec nebo příslušník lidské komunity vystaven.

Cílem vzdělávání v oblasti vzdělávání „bezpečnostní obory“, z pohledu pospolitosti, je příprava vysokoškolsky kvalifikovaných odborníků, kteří budou schopni působit na pracovních pozicích ve všech sektorech bezpečnosti. To znamená jak v tradičních sektorech vojenském a veřejnoprávním, tak i doplňujících sektorech, např. ekonomickém, environmentálním, společenském, energetickém, technologickém či kulturním.

Cílem vzdělávání v oblasti vzdělávání „bezpečnostní obory“, z pohledu studujícího jednotlivce, je získat schopnosti identifikace, prevence, predikce a eliminace celého spektra bezpečnostních hrozeb a rizik a současně i získat schopnosti zobecňování poznatků a zkušeností pro rozvoj teorie a praxe v oblasti bezpečnosti.

Současně je v uvedeném kontextu nutné, jak z pohledu pospolitosti, tak i jednotlivce, aby absolvent byl vzděláván v duchu vlastenectví, demokracie, humanismu a občanské odpovědnosti, s politickým, právním, etickým a kulturním rozhledem. V tomto rozšířeném pojetí bezpečnosti je kladen důraz na bezpečí lidí jako konkrétních jedinců. Prosazení tohoto konceptu ve společnosti se jeví jako nezbytné.

#### **RÁMCOVÝ PROFIL ABSOLVENTŮ**

Oblast vzdělávání „bezpečnostní obory“ má výrazný multidisciplinární charakter. V současnosti se jeví, že je strukturována celkem do tří podoblastí, které lze označit jako podoblast "ochrana osob a majetku", "bezpečnost a ochrana zdraví při práci" a "vojsko a obrana". Z tohoto důvodu se proto jeví nezbytné, aby absolventi studijních oborů v oblasti vzdělávání „bezpečnostní obory“ disponovali určitým společným „standardem znalostí“, který budou následně rozšiřovat podle své specializace v konkrétní bezpečnostní problematice, určené studovaným studijním oborem. Za uvedený společný „standard znalostí“ je možné považovat „Společné minimum pro potřeby vzdělávání odborníků v oblasti bezpečnosti“, schválené Bezpečnostní radou státu 3. července 2007, na jehož základě byly vymezeny i výše uvedené páteří obory. Předpokládá se, že tento společný „standard znalostí“ bude představovat u oborů krátkého cyklu až polovinu, u oborů bakalářských až jednu třetinu a u oborů magisterských a doktorských jednu čtvrtinu až jednu pětinu konkrétně studovaného studijního oboru.

Celkově je třeba mít na paměti, že vymezení profilu absolventů v oblasti vzdělávání „bezpečnostní obory“, je vzhledem k jeho multidisciplinarní problematice. Je zřejmě nereálné snažit se vygenerovat tzv. „univerzálního pracovníka“ v oblasti bezpečnosti. Profil absolventa konkrétního studijního oboru se bude muset odvíjet od základního kurikula předmětů společného základu. To v praxi bude znamenat, bude-li např. společný vědní základ na bázi věd přírodních, bude absolvent uplatnitelný zejména ve firmách a v těch institucích, kde se předpokládá řešit bezpečnostní problematiku v návaznosti na mimořádné či krizové situace. Půjde-li o společenské vědy (např. oblast veřejné správy) bude absolvent uplatnitelný především ve veřejné správě. Obdobně u technických, vojenských, lékařských věd atd.

Z uvedeného úhlu pohledu bude profil absolventa zaměřen na znalosti, které uplatní v profesních funkcích všude tam, kde bude nezbytné zabezpečovat opatření vztahující se na konfliktní interakce. Na základě získaných znalostí bude absolvent schopen provádět analýzu rizik, vypracovávat programy prevence a eliminace rizik, zpracovávat bezpečnostní dokumentaci. Dále bude schopen vypracovat predikci možných následků, provést analýzu vývoje konfliktních interakcí a navrhnout způsoby jejich řešení.

**DESKRIPTORY OBLASTI VZDĚLÁVÁNÍ**

	Program krátkého cyklu	Bakalářský studijní program	Magisterský studijní program	Doktorský studijní program
	Absolventi studijního programu			
<b>Odborné znalosti</b>	<ul style="list-style-type: none"> <li>vysvětlí místo a úlohu specializovaných subjektů krizového řízení (např. znají úlohu ozbrojených sil v rámci integrovaného záchranného systému),</li> <li>charakterizují krizový management (např. znalost obecných zásad krizového řízení v podmínkách ozbrojených sil),</li> <li>vysvětlí logistiku v oblasti bezpečnosti, vázanou zejména k materiálnímu, technickému a finančnímu zabezpečení řešení mimořádných událostí a krizových situací, narušení vnitřního pořádku a bezpečnosti, včetně zajištění připravenosti pro tato řešení (např. znají zásady a principy realizace logistické podpory na/mimo území vysílajícího státu),</li> <li>znají možnosti aplikované informatiky nezbytné pro práci bezpečnostního manažera (např. základní znalost práce s počítačem a možnosti využití textových a tabulkových procesorů, elektronické pošty a internetu pro svoji práci),</li> <li>vysvětlí terminologii a klasifikační aspekty rizika (např. znalosti bezpečnostních a vojenských rizik),</li> <li>objasní význam a místo analýzy rizika v procesu zajišťování krizového řízení a bezpečnosti,</li> <li>vysvětlí obecný postup analýzy rizika, včetně základních metod získávání vstupních dat,</li> <li>objasní zásady sestavování rozsahu a cíle analýzy rizika (např. znalosti zásad tvorby variant v rámci rozhodovacího procesu),</li> <li>vysvětlí bezpečnostní systém ČR, jeho struktury, vymezení povinností, kompetencí a odpovědností jednotlivých sou-</li> </ul>	<ul style="list-style-type: none"> <li>reprodukují bezpečnostní politiku státu, organizace anebo jiného celku (např. znají strukturu bezpečnostního systému ČR, kompetence jeho jednotlivých prvků, nebo bezpečnostní politiku státu, organizace v oblasti ochrany kritické infrastruktury, majetku a osob, BOZP, požární ochrany, nebo topologii bezpečnostního systému organizace, systémové charakteristiky jednotlivých prvků a jejich vzájemné vazby, nebo Bezpečnostní strategii ČR, Vojenskou strategii ČR),</li> <li>vysvětlí problematiku prevence rizik a krizového managementu ve veřejném anebo soukromém sektoru (např. znají problematiku prevence rizik bezpečnosti silniční a letecké dopravy, nebo bezpečnosti informačních a komunikačních systémů, nebo bezpečnosti práce, ochrany obyvatelstva, požární ochrany, bezpečnosti průmyslu, nebo prevence a uspořádávání sporů a zajišťování bezpečnosti v post-konfliktních oblastech, nebo prevence rizik vyplývajících z použití vojenských a bezpečnostních technologií),</li> <li>vysvětlí obecný postup analýzy rizika, včetně sběru vstupních dat (např. mají relevantní znalosti matematiky, statistiky a metod sběru dat, metod verifikace dat),</li> <li>popíší právní, předpisovou a normativní úpravu v oblasti bezpečnosti státu anebo organizace (např. ústavní zákony, nebo zákony a předpisy související s ochranou majetku a osob, nebo předpisy a normy vymezující zásady použití bezpečnostních technologií, nebo obecně závazné právní předpisy, technické normy a vnitřní předpisy organizace, nebo zákony a předpisy související se zajištěním bezpečnosti při používání vojenských technologií),</li> <li>popíší psychologické aspekty bezpečnosti a zásady interpersonální komunikace (např. do-</li> </ul>	<ul style="list-style-type: none"> <li>vysvětlí a interpretují bezpečnostní politiku státu, organizace anebo jiného celku (např. široce znají strukturu bezpečnostního systému ČR, kompetence jeho jednotlivých prvků, nebo bezpečnostní politiku státu, organizace v oblasti ochrany kritické infrastruktury, majetku a osob, BOZP, požární ochrany, nebo topologii bezpečnostního systému organizace, systémové charakteristiky jednotlivých prvků a jejich vzájemné vazby, nebo Bezpečnostní strategii ČR, Vojenskou strategii ČR),</li> <li>vyjadřují a interpretují problematiku prevence rizik a krizového managementu ve veřejném anebo soukromém sektoru (např. široce znají problematiku bezpečnosti silniční a letecké dopravy, nebo bezpečnosti informačních a komunikačních systémů, nebo bezpečnosti práce, ochrany obyvatelstva, požární ochrany, bezpečnosti průmyslu, nebo prevence a uspořádávání sporů a zajišťování bezpečnosti v post-konfliktních oblastech, nebo prevence rizik vyplývajících z použití vojenských a bezpečnostních technologií),</li> <li>vyjadřují a interpretují obecný postup analýzy rizika, včetně sběru vstupních dat a koncepce řešení bezpečnosti v podoblasti podle zaměření studia (např. mají relevantní široké znalosti matematiky, statistiky, operační analýzy a metod sběru dat, metod verifikace dat, nebo rozhodovacího procesu velitele při plánování operace),</li> <li>vysvětlí právní, předpisovou a normativní úpravu v oblasti bezpečnosti státu anebo organizace (např. ústavní zákony, nebo zákony a předpisy související s ochranou majetku a osob, nebo předpisy a normy vymezující zásady použití bezpečnostních technologií, nebo obecně závazné právní předpisy, technické normy a vnitřní předpisy organizace, nebo zá-</li> </ul>	<ul style="list-style-type: none"> <li>zdůvodní bezpečnostní politiku státu, organizace anebo jiného celku, bezpečnostního systému organizace, systémové charakteristiky jeho jednotlivých prvků a jejich vzájemné vazby (např. hluboce a systematicky znají strukturu bezpečnostního systému ČR, kompetence jeho jednotlivých prvků, nebo bezpečnostní politiku státu, organizace v oblasti ochrany kritické infrastruktury, majetku a osob, BOZP, požární ochrany, nebo topologii bezpečnostního systému organizace, systémové charakteristiky jednotlivých prvků a jejich vzájemné vazby, nebo Bezpečnostní strategii ČR, Vojenskou strategii ČR),</li> <li>diskutují a opoují problematiku prevence rizik a krizového managementu ve veřejném anebo soukromém sektoru (např. hluboce a systematicky znají metody prevence rizik a krizového managementu, nebo standardní operační postupy, nebo metody posouzení prevence napadení kritické infrastruktury v případě teroristického útoku či havárie dopravního prostředku, nebo metody posouzení prevence rizik vyplývajících z použití vojenských a bezpečnostních technologií),</li> <li>diskutují a identifikují obecný postup analýzy rizika, včetně sběru vstupních dat a koncepce řešení bezpečnosti v podoblasti podle zaměření studia (např. mají relevantní hluboké a systematické znalosti možnosti využití matematických nástrojů při modelování dějů s vysokou mírou neurčitosti, nebo samostatně zvládají rozhodovací proces velitele při plánování operace),</li> <li>interpretují a diskutují právní, předpisovou a normativní úpravu v oblasti bezpečnosti státu anebo organizace (např. ústavní zákony, nebo zákony a předpisy související s ochranou majetku a osob, nebo předpisy a normy vymezují-</li> </ul>

## Národní kvalifikační rámec terciárního vzdělávání

	<p>části a prvků (např. znalosti místa a úlohy ozbrojených sil v rámci bezpečnostního systému státu),</p> <ul style="list-style-type: none"> <li>• popíší zájmy, postoje a ambice ČR při zajišťování své bezpečnosti (např. znalosti zapojení ČR do mezinárodních bezpečnostních organizací),</li> <li>• vymezí prevenci a eliminaci bezpečnostních hrozeb a z nich vyplývajících rizik,</li> <li>• reprodukují společenské aspekty bezpečnosti vztahující se k problematice ochrany společnosti ve vztahu k sociální problematice a v návaznosti na lidská práva, zejména ochranu obyvatelstva a životního prostředí při mimořádných událostech, ochranu kritické infrastruktury a zajištění vnitřního pořádku a bezpečnosti (např. znalosti praktického uplatnění bezpečnostních zásad),</li> <li>• reprodukují právní úpravu a normy pro zajištění bezpečnosti ČR s důrazem na krizové řízení, vnitřní bezpečnost, ochranu obyvatelstva a integrovaný záchranný systém.</li> </ul>	<p>pady na psychiku osob postižených mimořádnou událostí, nebo příbuzných a známých obětí událostí a záchranářů, nebo psychologické aspekty použití technologií pro ochranu kritické infrastruktury, majetku a osob, nebo psychologické aspekty bezpečnosti práce, nebo psychologické aspekty použití zbraní a vojenské techniky)</p> <ul style="list-style-type: none"> <li>• definují prvky materiálního, technického a finančního zabezpečení řešení mimořádných událostí a krizových situací, narušení vnitřního pořádku a bezpečnosti, včetně zajištění připravenosti pro toto řešení (např. při koordinaci a řízení záchranných a likvidačních prací, nebo při zabezpečování ochrany obyvatelstva, nebo při aplikaci technologií pro ochranu majetku a osob, při haváriích, požárech, povodních, evakuacích zaměstnanců a souvisejících činnostech a postupech, nebo při tvorbě krizových plánů, nebo standardních operačních postupů, nebo při použití vojenské techniky),</li> <li>• popíší softwarové produkty pro podporu analýzy rizik, prevence rizik a komunikačních a počítačových systémů řízení (např. znají informační systémy a databáze pro podporu analýzy a prevence rizik, nebo nebezpečných látek, nebo BOZP, nebo štabní informační systém, nebo právní informační systém, nebo systémy pro počítačovou podporu návrhu technologií pro ochranu majetku a osob, nebo vojenské techniky, nebo znalostního managementu v organizaci),</li> <li>• popíší principy a koncepty bezpečnostní politiky státu, organizace anebo jiného celku (např. znají principy a koncepce efektivního použití bezpečnostních technologií pro ochranu kritické infrastruktury, majetku a osob, nebo systémů managementu BOZP, nebo bezpečnostních kategorií v rámci organizace a jejich vzájemné vazby, nebo základních doktrínálních předpisů AČR, NATO, nebo vojenské techniky v mírových i válečných operacích),</li> <li>• definují metody prevence rizik a koncepty krizového managementu ve veřejném anebo soukromém sektoru (např. znají metody prevence rizik v silniční a letecké dopravě, nebo</li> </ul>	<p>kony a předpisy související se zajištěním bezpečnosti při používání vojenských technologií),</p> <ul style="list-style-type: none"> <li>• vysvětlí psychologické aspekty bezpečnosti a zásady interpersonální komunikace (např. dopady na psychiku osob postižených mimořádnou událostí, nebo příbuzných a známých obětí událostí a záchranářů, nebo psychologické aspekty použití technologií pro ochranu kritické infrastruktury, majetku a osob, nebo psychologické aspekty bezpečnosti práce, nebo psychologické aspekty použití zbraní a vojenské techniky),</li> <li>• vypočítají a vyjadřují prvky materiálního, technického a finančního zabezpečení řešení mimořádných událostí a krizových situací, narušení vnitřního pořádku a bezpečnosti, včetně zajištění připravenosti pro toto řešení (např. při koordinaci a řízení záchranných a likvidačních prací, nebo při zabezpečování ochrany obyvatelstva, nebo při aplikaci technologií pro ochranu majetku a osob, při haváriích, požárech, povodních, evakuacích zaměstnanců a souvisejících činnostech a postupech, nebo při tvorbě krizových plánů, standardních operačních postupů, nebo řízení technického zabezpečení ekologické ochrany při haváriích, nebo při analýze krizové situace, nebo při řízení a odstraňování následků živelných pohrom),</li> <li>• vysvětlí a interpretují softwarové produkty pro podporu analýzy rizik, prevence rizik a komunikačních a počítačových systémů řízení (např. široce znají informační systémy a databáze pro podporu analýzy a prevence rizik, nebo nebezpečných látek, nebo BOZP, nebo štabní informační systém, nebo právní informační systém, nebo systémy pro počítačovou podporu návrhu technologií pro ochranu majetku a osob, nebo vojenské techniky, nebo znalostního managementu v organizaci),</li> <li>• vysvětlí a interpretují principy a koncepty bezpečnostní politiky státu, organizace anebo jiného celku (např. široce znají principy a koncepce efektivního použití bezpečnostních technologií pro ochranu kritické infrastruktury, majetku a osob, nebo systémů managemen-</li> </ul>	<p>ci zásady použití bezpečnostních technologií, nebo obecně závazné právní předpisy, technické normy a vnitřní předpisy organizace, nebo zákony a předpisy související se zajištěním bezpečnosti při používání vojenských technologií),</p> <ul style="list-style-type: none"> <li>• identifikují a diskutují psychologické aspekty bezpečnosti a zásady interpersonální komunikace (např. dopady na psychiku osob postižených mimořádnou událostí, nebo příbuzných a známých obětí událostí a záchranářů, nebo psychologické aspekty použití technologií pro ochranu kritické infrastruktury, majetku a osob, nebo psychologické aspekty bezpečnosti práce, nebo psychologické aspekty použití zbraní a vojenské techniky),</li> <li>• interpretují a oponují prvky materiálního, technického a finančního zabezpečení řešení mimořádných událostí a krizových situací, narušení vnitřního pořádku a bezpečnosti, včetně zajištění připravenosti pro toto řešení (např. při koordinaci a řízení záchranných a likvidačních prací, nebo při zabezpečování ochrany obyvatelstva, nebo při aplikaci technologií pro ochranu majetku a osob, při haváriích, požárech, povodních, evakuacích zaměstnanců a souvisejících činnostech a postupech, nebo při tvorbě krizových plánů, standardních operačních postupů, nebo řízení technického zabezpečení ekologické ochrany při haváriích, nebo při analýze krizové situace, nebo při řízení a odstraňování následků živelných pohrom),</li> <li>• zdůvodní softwarové produkty pro podporu analýzy rizik, prevence rizik a komunikačních a počítačových systémů řízení (např. hluboce a systematicky znají SW produkty pro podporu vývoje a návrhu technologií pro ochranu kritické infrastruktury, majetku a osob, nebo pro řízení systémů fyzické ochrany, nebo pro podporu vývoje a návrhu zbraní a vojenské techniky, nebo pro sledování a vyhodnocování spolehlivosti vojenské techniky v provozu a pro řízení její údržby),</li> <li>• znají a diskutují principy a koncepty bezpečnostní politiky státu, organizace anebo jiného celku v kontextu nejnovějších poznatků (např. hluboce a systematicky znají bezpečnostní</li> </ul>
--	---	---	---	--

## Národní kvalifikační rámec terciárního vzdělávání

		<p>metody prevence rizik s využitím technologií pro ochranu majetku a osob, nebo teorii krizového managementu, nebo teorii a principy národní bezpečnosti, nebo metody prevence rizik vyplývajících z používání vojenských technologií),</p> <ul style="list-style-type: none"> <li>• definují terminologicky a klasifikačně aspekty rizika a rizikové faktory (např. znají terminologické a klasifikační aspekty rizika, včetně strategie výběru rizikových faktorů vyplývajících z použití bezpečnostních technologií dle zaměření studia, nebo metody identifikace bezpečnostních hrozeb a bezpečnostních rizik),</li> <li>• popíší právní systém ČR v oblasti bezpečnosti a jemu odpovídající legislativní nebo technické a normotvorné postupy (např. znají správní právo, nebo právo obrany, nebo bezpečnost technických zařízení SOD),</li> <li>• popíší metody školení a ověřování znalostí ve vztahu k sociální a společenské problematice v návaznosti na lidská práva (např. znají základní metody leadershipu),</li> <li>• popíší personální politiku organizace pro oblast bezpečnosti vycházející z principů podnikové ekonomiky a managementu (např. znají zásady personální politiky, nebo ekonomiky obrany státu, nebo ekonomiky ozbrojených sil s ohledem na požadavky personální bezpečnosti organizace),</li> <li>• vysvětlí koncepty a metody aplikované informatiky využitelné v práci vedoucího pracovníka (např. široce znají pojetí manažerské informatiky, nebo možnosti využití práce v síti, nebo problematiku algoritmizace úloh, nebo prezentací, nebo některých specifických informačních systémů využívaných v ozbrojených silách, nebo SW produkty využitelné při návrhu a použití vojenských technologií, nebo koncepty a metody aplikované informatiky využitelné při řízení technologií pro ochranu kritické infrastruktury, majetku a osob),</li> <li>• vysvětlí mezinárodní aspekty bezpečnosti, postoje a ambice ČR (např. široce znají požadavky na bezpečnost kritické infrastruktury, majetku a osob, nebo zajištění bezpečnosti</li> </ul>	<p>tu BOZP, nebo bezpečnostních kategorií v rámci organizace a jejich vzájemné vazby, nebo základních doktrinárních předpisů AČR, NATO, nebo vojenských techniky v mírových i válečných operacích),</p> <ul style="list-style-type: none"> <li>• vysvětlí a interpretují metody prevence rizik a koncepty krizového managementu ve veřejném anebo soukromém sektoru (např. široce znají metody prevence rizik v silniční a letecké dopravě, nebo metody prevence rizik s využitím technologií pro ochranu majetku a osob, nebo teorii všech fází krizového řízení, nebo teorii a principy národní bezpečnosti, nebo metody prevence rizik vyplývajících z používání vojenských technologií),</li> <li>• vysvětlí terminologicky a klasifikačně aspekty rizika a rizikové faktory (např. široce znají terminologické a klasifikační aspekty rizika, včetně strategie výběru rizikových faktorů vyplývajících z použití bezpečnostních technologií dle zaměření studia, nebo metody identifikace bezpečnostních hrozeb a rizik, nebo postupy přípravy, plánování a realizace rozhodovacího procesu velitele),</li> <li>• vysvětlí a interpretují právní systém ČR v oblasti bezpečnosti a jemu odpovídající legislativní nebo technické a normotvorné postupy (např. široce znají správní právo, nebo právo obrany, nebo bezpečnost technických zařízení SOD) identifikují a vysvětlí metody školení a ověřování znalostí ve vztahu k sociální a společenské problematice v návaznosti na lidská práva (např. široce znají metody leadershipu),</li> <li>• vysvětlí personální politiku organizace pro oblast bezpečnosti vycházející z principů podnikové ekonomiky a managementu (např. široce znají zásady personální politiky, nebo ekonomiky obrany státu, nebo ekonomiky ozbrojených sil s ohledem na požadavky personální bezpečnosti organizace),</li> <li>• zdůvodní koncepty a metody aplikované informatiky využitelné v práci vedoucího pracovníka (např. hluboce znají pojetí manažerské informatiky, nebo možnosti využití práce v síti, nebo problematiku algoritmizace úloh, nebo prezentací, nebo některých specifických</li> </ul>	<p>strategii ČR, nebo principy a koncepce efektivního použití bezpečnostních technologií pro ochranu kritické infrastruktury, majetku a osob, nebo mezinárodní aspekty bezpečnostní politiky státu, obrany země, nebo principy a koncepce efektivního použití vojenské techniky v mírových i válečných operacích),</p> <ul style="list-style-type: none"> <li>• znají a diskutují metody prevence rizik a koncepty krizového managementu ve veřejném a eventuálně soukromém sektoru v kontextu nejnovějších poznatků (např. hluboce a systematicky znají metody prevence rizik v silniční a letecké dopravě, nebo metody prevence rizik s využitím technologií pro ochranu majetku a osob, nebo teorii všech fází krizového řízení, nebo teorii a principy národní bezpečnosti, nebo metody prevence rizik vyplývajících z používání vojenských technologií),</li> <li>• znají a diskutují terminologicky a klasifikačně aspekty rizika a rizikové faktory v kontextu nejnovějších poznatků (např. hluboce a systematicky znají terminologické a klasifikační aspekty rizika, včetně strategie výběru rizikových faktorů vyplývajících z použití bezpečnostních technologií dle zaměření studia, nebo metody identifikace bezpečnostních hrozeb a rizik, nebo postupy přípravy, plánování a realizace rozhodovacího procesu velitele),</li> <li>• znají a diskutují právní systém ČR v oblasti bezpečnosti a jemu odpovídající legislativní, eventuálně technické a normotvorné postupy v kontextu nejnovějších poznatků (např. hluboce a systematicky znají správní právo, nebo právo obrany, nebo bezpečnost technických zařízení SOD),</li> <li>• znají a diskutují metody školení a ověřování znalostí ve vztahu k sociální a společenské problematice v návaznosti na lidská práva v kontextu nejnovějších poznatků (např. hluboce a systematicky znají metody leadershipu, nebo metody výcviku vojáků z hlediska jejich chování v krizových situacích),</li> <li>• znají a diskutují personální politiku organizace pro oblast bezpečnosti vycházející z principů podnikové ekonomiky a managementu v kontextu nejnovějších poznatků (např. hluboce a systematicky znají zásady personální politiky,</li> </ul>
--	--	---	--	---

## Národní kvalifikační rámec terciárního vzdělávání

		<p>pozemní a letecké dopravy, nebo bezpečnost vojenské techniky vyplývající z evropské legislativy a mezinárodních standardů, nebo požadavky na BOZP, bezpečnost výrobků a technických zařízení vyplývající z mezinárodních smluv a úmluv, nebo angažovanost ČR v mezinárodních bezpečnostních organizacích),</p> <ul style="list-style-type: none"> <li>• definují místo a úlohu subjektů krizového řízení na jednotlivých úrovních (např. znají činnost krizových štábů, nebo jednotlivých pracovníků v systémech na ochranu kritické infrastruktury, majetku a osob, nebo krizového řízení podniku zejména v reakci na živelní pohromy, havárie a další mimořádné události, nebo prvků integrovaného záchranného systému ČR, nebo součástí ozbrojených sil státu v operacích probíhajících pod vedením mezinárodních organizací),</li> <li>• vysvětlí možnosti a omezení hodnocení rizik a stanovování priorit v rozhodovacích procesech (např. specifikaci požadavků na bezpečnost a spolehlivost technologií pro ochranu kritické infrastruktury, majetku a osob, nebo zásady přípravy, plánování a realizace rozhodovacího procesu velitele),</li> <li>• vysvětlí obecné pojmy a instituty práva v oblasti bezpečnosti a základní právní úpravy vnitřní anebo vnější bezpečnosti ČR, organizace anebo jiného celku (např. co to je bezpečnost, krizová situace, mimořádná událost, nebo jaké jsou kompetence orgánů veřejné správy, nebo práva a povinnosti příslušníků některých bezpečnostních sborů, nebo kompetence orgánů veřejné správy při vymezování požadavků na bezpečnost technických systémů a kontrolu jejich naplňování, nebo zásady práva na úseku vnitřní a vnější bezpečnosti státu),</li> <li>• vysvětlí alternativy problematiky ochrany společnosti ve vztahu k sociální problematice a v návaznosti na lidská práva, zejména ochranu obyvatelstva a životního prostředí při mimořádných událostech, ochrany kritické infrastruktury a zajištění vnitřního pořádku a bezpečnosti (např. znají možnosti efektivního využití moderních technologií na ochranu kritické infrastruktury, majetku a osob, nebo</li> </ul>	<p>informačních systémů využívaných v ozbrojených silách, nebo SW produkty využitelné při návrhu a použití vojenských technologií, nebo koncepty a metody aplikované informatiky použitelné při řízení technologií pro ochranu kritické infrastruktury, majetku a osob,</p> <ul style="list-style-type: none"> <li>• rozlišují a interpretují mezinárodní aspekty bezpečnosti, postoje a ambice ČR (např. hluboce znají požadavky na bezpečnost kritické infrastruktury, majetku a osob, nebo zajištění bezpečnosti pozemní a letecké dopravy, nebo bezpečnost vojenské techniky vyplývající z evropské legislativy a mezinárodních standardů, nebo požadavky na BOZP, bezpečnost výrobků, technických zařízení vyplývající z mezinárodních smluv a úmluv, nebo angažovanost ČR v mezinárodních bezpečnostních organizacích),</li> <li>• vysvětlí místo a úlohu subjektů krizového řízení na jednotlivých úrovních (např. široce znají činnost krizových štábů, nebo jednotlivých pracovníků v systémech na ochranu kritické infrastruktury, majetku a osob, nebo krizového řízení podniku zejména v reakci na živelní pohromy, havárie a další mimořádné události, nebo prvků integrovaného záchranného systému ČR, nebo součástí ozbrojených sil státu v operacích probíhajících pod vedením mezinárodních organizací),</li> <li>• vyjádří a identifikují možnosti a omezení hodnocení rizik a stanovování priorit v rozhodovacích procesech (např. specifikaci požadavků na bezpečnost a spolehlivost technologií pro ochranu kritické infrastruktury, majetku a osob, nebo zásady přípravy, plánování a realizace rozhodovacího procesu velitele),</li> <li>• interpretují obecné pojmy a instituty práva v oblasti bezpečnosti a základní právní úpravy vnitřní anebo vnější bezpečnosti ČR, organizace anebo jiného celku (např. co to je bezpečnost, krizová situace, mimořádná událost, nebo jaké jsou kompetence orgánů veřejné správy, nebo práva a povinnosti příslušníků některých bezpečnostních sborů, nebo kompetence orgánů veřejné správy při vymezování požadavků na bezpečnost technických systémů a kontrolu jejich naplňování, nebo zásady</li> </ul>	<p>nebo ekonomiky obrany státu, nebo ekonomiky ozbrojených sil s ohledem na požadavky personální bezpečnosti organizace),</p> <ul style="list-style-type: none"> <li>• znají a diskutují koncepty a metody aplikované informatiky využitelné v práci vedoucího pracovníka v kontextu nejnovějších poznatků (např. hluboce a systematicky znají použití konkrétních informačních systémů a možnosti využití SW aplikací při řešení bezpečnostních úloh, nebo koncepty a metody aplikované informatiky použitelné při řízení technologií pro ochranu kritické infrastruktury, majetku a osob, nebo některých specifických informačních systémů využívaných v ozbrojených silách, nebo koncepty a metody aplikované informatiky použitelné při řízení technologií pro ochranu kritické infrastruktury, majetku a osob),</li> <li>• diskutují a oponují mezinárodní aspekty bezpečnosti, postoje a ambice ČR (např. hluboce a systematicky znají činnost orgánů Evropské unie, nebo angažovanost ČR v mezinárodních bezpečnostních organizacích a uskupeních),</li> <li>• interpretují místo a úlohu subjektů krizového řízení na jednotlivých úrovních (např. hluboce a systematicky znají činnost krizových štábů, nebo havarijních, povodňových a nálezových komisí na ústřední a regionální úrovni, nebo jednotlivých pracovníků v systémech na ochranu kritické infrastruktury, majetku a osob, nebo prvků integrovaného záchranného systému ČR),</li> <li>• oponují možnosti a omezení hodnocení rizik a stanovování priorit v rozhodovacích procesech (např. specifikaci požadavků na bezpečnost a spolehlivost technologií pro ochranu kritické infrastruktury, majetku a osob, nebo zásady přípravy, plánování a realizace rozhodovacího procesu velitele, včetně příslušných vazeb a návazností),</li> <li>• diskutují obecné pojmy a instituty práva v oblasti bezpečnosti a základní právní úpravy vnitřní anebo vnější bezpečnosti ČR, organizace anebo jiného celku (např. co to je bezpečnostní rada, veřejná správa a její vztah k bezpečnosti, nebo mezinárodní organizace v oblasti bezpečnosti a jejich závazné směrnice či</li> </ul>
--	--	--	--	---

## Národní kvalifikační rámec terciárního vzdělávání

		<p>BOZP a bezpečnost organizace, nebo hrozeb a jejich dopadů na environmentální bezpečnost, nebo soudobou vojenskou techniku a možnosti jejího využití),</p> <ul style="list-style-type: none"> <li>• vysvětlí podle potřeb možnosti, podmínky a omezení využití specifických norem pro řízení logistického, finančního a personálního managementu bezpečnostní organizace (např. využití hospodářských opatření pro krizové stavy, nebo prvky logistických řetězců a jejich vazby, nebo bezpečnost logistických řetězců, nebo finanční standardy řízení zdrojů),</li> <li>• vysvětlí podle potřeb možnosti, podmínky a omezení pro využití počítačových systémům při hodnocení bezpečnostních hrozeb a rizik (např. dodržování zásad počítačové bezpečnosti v oblasti infrastruktury pro krizové řízení, nebo řízení systémů pro ochranu kritické infrastruktury, majetku a osob, nebo v oblasti infrastruktury pro řízení ozbrojených sil či krizové řízení).</li> </ul>	<p>práva na úseku vnitřní a vnější bezpečnosti státu),</p> <ul style="list-style-type: none"> <li>• interpretují alternativy problematiky ochrany společnosti ve vztahu k sociální problematice a v návaznosti na lidská práva, zejména ochranu obyvatelstva a životního prostředí při mimořádných událostech, ochrany kritické infrastruktury a zajištění vnitřního pořádku a bezpečnosti (např. široce znají možnosti efektivního využití moderních technologií na ochranu kritické infrastruktury, majetku a osob, nebo BOZP a bezpečnost organizace, nebo hrozeb a jejich dopadů na environmentální bezpečnost, nebo soudobou vojenskou techniku, možnosti jejího využití),</li> <li>• interpretují podle potřeb možnosti, podmínky a omezení využití specifických norem pro řízení logistického, finančního a personálního managementu bezpečnostní organizace (např. využití hospodářských opatření pro krizové stavy, nebo prvky logistických řetězců a jejich vazby, nebo bezpečnost logistických řetězců, nebo finanční standardy řízení zdrojů),</li> <li>• interpretují podle potřeb možnosti, podmínky a omezení pro využití počítačových systémům při hodnocení bezpečnostních hrozeb a rizik (např. dodržování zásad počítačové bezpečnosti v oblasti infrastruktury pro krizové řízení, nebo řízení systémů pro ochranu kritické infrastruktury, majetku a osob, nebo v oblasti infrastruktury pro řízení ozbrojených sil či krizové řízení).</li> </ul>	<p>doporučení, nebo kompetence orgánů veřejné správy při vymezování požadavků na bezpečnost technických systémů a kontrolu jejich naplňování),</p> <ul style="list-style-type: none"> <li>• diskutují problematiku ochrany společnosti ve vztahu k sociální problematice a v návaznosti na lidská práva, zejména ochranu obyvatelstva a životního prostředí při mimořádných událostech, ochrany kritické infrastruktury a zajištění vnitřního pořádku a bezpečnosti (např. hluboce a systematicky znají možnosti efektivního využití moderních technologií na ochranu kritické infrastruktury, majetku a osob, nebo hrozeb a jejich dopadů na environmentální bezpečnost, nebo soudobou vojenskou techniku, možnosti jejího využití),</li> <li>• diskutují podle potřeb možnosti, podmínky a omezení využití specifických norem pro řízení logistického, finančního a personálního managementu bezpečnostní organizace (např. využití hospodářských opatření pro krizové stavy, nebo finanční zdroje pro řešení mimořádných událostí, nebo alokace věcných zdrojů, nebo prvky logistických řetězců a jejich vazby, nebo bezpečnost logistických řetězců, nebo finanční standardy řízení zdrojů),</li> <li>• diskutují podle potřeb možnosti, podmínky a omezení pro využití počítačových systémům při hodnocení bezpečnostních hrozeb a rizik (např. vyhodnocování bezpečnostní situace v souladu s platnými národními a mezinárodními normami, nebo dodržování zásad počítačové bezpečnosti v oblasti infrastruktury pro krizové řízení, nebo spolehlivost informačních systémů v podmínkách úmyslného nebo neúmyslného rušení komunikací a působení výkových elektromagnetických polí).</li> </ul>
<b>Odborné dovednosti</b>	<ul style="list-style-type: none"> <li>• určí nebezpečí a rizika na své pracovní úrovni v určených a známých souvislostech,</li> <li>• ovládají řízení bezpečnosti podle vymezeného zadání (např. praktické schopnosti vedení komunikace v krizových situacích),</li> <li>• ovládají plánování opatření a zvládání mimořádných událostí v určených a známých souvislostech,</li> </ul>	<ul style="list-style-type: none"> <li>• určí bezpečnostní politiku ve své organizaci (např. se podílí na zpracování plánu krizové připravenosti, vnitřního havarijního plánu, nebo zásad zajišťování fyzické ochrany a bezpečnosti majetku a osob při využití bezpečnostních technologií, nebo topologií bezpečnostního systému organizace, nebo zásad ochrany a obrany jednotek a využití zbraní a vojenské techniky),</li> <li>• aplikují řízení bezpečnosti ve své organizaci</li> </ul>	<ul style="list-style-type: none"> <li>• analyzují bezpečnostní politiku ve své organizaci (např. samostatně zpracovávají plány krizové připravenosti, vnitřní havarijní plány, nebo zásady zajišťování fyzické ochrany a bezpečnosti majetku a osob při využití bezpečnostních technologií, nebo topologie bezpečnostního systému organizace, nebo zásady ochrany a obrany jednotek a využití zbraní a vojenské techniky),</li> <li>• testují a naplňují řízení bezpečnosti ve své</li> </ul>	<ul style="list-style-type: none"> <li>• oponují a vytváří původním výzkumem teorie, koncepty a metody prevence a eliminace bezpečnostních hrozeb a z nich vyplývajících rizik vnitřní a vnější bezpečnosti státu anebo organizace, či občana (např. územní a regulační plány a jejich vztah k zajištění bezpečnosti, nebo krizové, havarijní, obranné a civilní nouzové plány, nebo opatření k ochraně obyvatelstva, nebo teorie, koncepty a zásady uplatňované při zajišťování fyzické ochrany a bezpečnosti majet-</li> </ul>

## Národní kvalifikační rámec terciárního vzdělávání

	<ul style="list-style-type: none"> <li>• aplikují zabezpečování preventivních opatření a poznatků krizového řízení v určených a známých souvislostech,</li> <li>• ovládají sestavování rozsahu a cílů analýzy rizik, stanovení metod pro sběr vstupních dat, sestavení registru nebezpečí, screeningu rizik a posouzení jejich akceptovatelnosti na své pracovní pozici,</li> <li>• navrhnou materiální, technické a finanční zabezpečení řešení mimořádných událostí a krizových situací, včetně zajištění připravenosti pro tato řešení podle vymezeného zadání,</li> <li>• ovládají odpovídající právní a technické normy na své pracovní úrovni (např. Český obranný standard Manipulace s materiálem v poli),</li> <li>• analyzují na své pracovní úrovni rizika v určených a známých souvislostech,</li> <li>• ovládají na své pracovní úrovni informační a komunikační technologie a informační systémy pro informačně-bezpečnostní řešení,</li> </ul> <p>(např. využití počítače ke sběru, zpracování, vyhledání, využití a přenosu dat na své pracovní úrovni).</p>	<p>(např. se podílí na výběru technologií pro zajištění ochrany kritické infrastruktury, majetku a osob, nebo principech nasazení ozbrojených sil v krizovém regionu, nebo zpracování zásad použití vojenské techniky),</p> <ul style="list-style-type: none"> <li>• určí nebezpečí a rizika ve své organizaci (např. se podílí na určování metod identifikace a hodnocení rizik vyplývajících z využití technologií pro ochranu kritické infrastruktury, majetku a osob, nebo z použití zbraní),</li> <li>• využijí a navrhnou relevantní ustanovení právních a technických předpisů a norem ve svém organizačním celku při řešení bezpečnostní problematiky v podoblasti podle zaměření studia s využitím standardních i nestandardních postupů (např. se podílí na zpracování relevantních právních a technických předpisů a norem souvisejících s užíváním bezpečnostních technologií)</li> <li>• realizují a řídí vzdělávání a výchovu v oblasti bezpečnosti ve své organizaci (např. se podílí na vzdělávání a výchově v oblasti bezpečného využívání technologií pro ochranu kritické infrastruktury, majetku a osob, nebo na velení a řízení při vzdělávání a výcviku v oblasti bezpečného využívání zbraní a vojenské techniky),</li> <li>• určí prvky logistických řetězců v oblasti bezpečnosti ve své organizaci (např. se podílí na určení hospodářských opatření pro krizové stavy, nebo určení prvků logistických řetězců pro zabezpečení systémů ochrany kritické infrastruktury, majetku a osob, zabezpečení použití zbraní a vojenské techniky),</li> <li>• realizují a řídí využívání informačních a komunikačních technologií ve své organizaci (např. se podílí na použití konkrétních informačních systémů a SW aplikací při řešení bezpečnostních úloh podle zaměření studia),</li> <li>• využijí informace pro řešení prevence a eliminace bezpečnostních hrozeb ve své organizaci (např. interpretují vliv přírodních pohrom, nebo mimořádných událostí antropogenní povahy na možnosti vzniku provozní havárie),</li> <li>• využijí informace pro použití bezpečnostního</li> </ul>	<p>organizaci (např. se samostatně podílejí na plánování technologií pro zajištění ochrany kritické infrastruktury, majetku a osob, nebo plánování opatření k zajištění bezpečnosti při výcviku, bojovém použití a údržbě zbraní a vojenské techniky),</p> <ul style="list-style-type: none"> <li>• analyzují nebezpečí a rizika ve své organizaci (např. samostatně analyzují nebezpečí a rizika vyplývajících z využití technologií pro ochranu kritické infrastruktury, majetku a osob, nebo z použití zbraní),</li> <li>• analyzují a sestaví relevantní ustanovení právních a technických předpisů a norem ve svém organizačním celku při řešení bezpečnostní problematiky v podoblasti podle zaměření studia s využitím standardních i nestandardních postupů (např. samostatně zpracovávají relevantní právní a technické předpisy a normy související s užíváním bezpečnostních technologií),</li> <li>• analyzují a vyhodnocují vzdělávání a výchovu v oblasti bezpečnosti ve své organizaci (např. samostatně realizují vzdělávání a výchovu v oblasti bezpečného využívání technologií pro ochranu kritické infrastruktury, majetku a osob, nebo na velení a řízení při vzdělávání a výcviku v oblasti bezpečného využívání zbraní a vojenské techniky),</li> <li>• analyzují prvky logistických řetězců v oblasti bezpečnosti ve své organizaci (např. samostatně určují hospodářská opatření pro krizové stavy, nebo prvky logistických řetězců pro zabezpečení systémů ochrany kritické infrastruktury, majetku a osob, zabezpečení použití zbraní a vojenské techniky),</li> <li>• analyzují a vyhodnocují využívání informačních a komunikačních technologií ve své organizaci (např. samostatně používají konkrétní informační systémy a SW aplikace při řešení bezpečnostních úloh podle zaměření studia),</li> <li>• analyzují a vyhodnocují informace pro řešení prevence a eliminace bezpečnostních hrozeb ve své organizaci (např. samostatně řeší bezpečnost a ochranu osob, materiálu a techniky),</li> <li>• analyzují a vyhodnocují informace pro použití bezpečnostního managementu ve své organi-</li> </ul>	<p>ku a osob a při využití bezpečnostních technologií, nebo topologie bezpečnostního systému organizace, nebo rizika BOZP, BTZ, závažných havárií, ekoterorismu, nebo zásady ochrany a obrany vojenských jednotek, využití zbraní a vojenské techniky),</p> <ul style="list-style-type: none"> <li>• porovnávají a vytváří původním výzkumem koncepty a metody zajištění a hodnocení bezpečnosti ve vazbě na obecné teorie řízení a systémy integrované bezpečnosti (např. koncepty a metody hodnocení odolnosti systémů pro ochranu kritické infrastruktury, majetku a osob proti působení úmyslných i neúmyslných vnějších vlivů),</li> <li>• formulují výzkumné postupy umožňující rozšiřovat poznání v oblasti metodologie analýzy rizik (např. postupy identifikace a hodnocení nebezpečí a rizika vyplývajících z využití technologií pro ochranu kritické infrastruktury, majetku a osob, nebo z použití zbraní a vojenské techniky a z činností souvisejících s jejich údržbou),</li> <li>• formulují a zdůvodňují výzkumné postupy rozšiřující poznání v oboru a v konečném efektu umožňující i návrh nových metodik, postupů a normativních a technických úprav v oblasti bezpečnosti (např. metodiky, postupy a normativní a technické úpravy související s využíváním bezpečnostních technologií podle zaměření studia),</li> <li>• formulují a zdůvodňují výzkumné postupy při řešení bezpečnosti, svrchanosti a územní celistvosti, politického a demokratického zřízení, ochranu ekosystému, kritické infrastruktury a ochranu obyvatelstva (např. výzkum metod modelování fyzické ochrany kritické infrastruktury a hodnocení její efektivity, nebo výzkum metod zvyšování bojové efektivity a spolehlivosti zbraní a vojenské techniky),</li> <li>• formulují a zdůvodňují výzkumné postupy, analyzovat a vyhodnocovat aspekty zajišťování bezpečnosti při vytváření a řízení prvků logistického řetězce realizovaného např. až do podmínek mezinárodního bezpečnostního prostředí (např. výzkum metod hodnocení odolnosti zabezpečovacích systémů v dopravě v podmínkách úmyslného nebo neúmyslného</li> </ul>
--	--	---	--	--

## Národní kvalifikační rámec terciárního vzdělávání

		<p>managementu ve své organizaci (např. utřídí a interpretují informace z krizových anebo havarijních štábů, jednotek ozbrojených sil, nebo soukromých bezpečnostních agentur),</p> <ul style="list-style-type: none"> <li>• využijí management rizika k posouzení nebezpečí a hodnocení rizika ve své organizaci (např. utřídí prediktivní hodnocení bezpečnosti a spolehlivosti užitých bezpečnostních technologií, nebo vojenských technologií),</li> <li>• kategorizují a navrhnou právní anebo technické předpisy či normy ve své organizaci (např. se podílí na interpretaci technických předpisů či norem pro použití technologií na ochranu kritické infrastruktury, majetku a osob),</li> <li>• aplikují a praktikují prostředky pro komunikaci v oblasti krizového řízení ve své organizaci (např. se podílí na využití radiokomunikačních a telekomunikačních prostředků),</li> <li>• aplikují a praktikují principy a postupy logistiky v oblasti bezpečnosti ve své organizaci (např. interpretují principy a postupy logistiky pro zabezpečení systémů ochrany kritické infrastruktury, majetku a osob, nebo metody diverzifikace rizik, deterministických a stochastických metod řízení zásob),</li> <li>• kategorizují a navrhnou využití informačních a komunikačních technologií ve své organizaci (např. se podílí na užití nástrojů manažerské informatiky pro sběr, zpracování, zhodnocení a prezentaci dat, nebo využití systémů pro počítačovou podporu návrhu technologií pro ochranu majetku a osob, zbraní a vojenské techniky a sledování její spolehlivosti v provozu),</li> <li>• posoudí koncepty bezpečnostní politiky k prevenci a eliminaci bezpečnostních hrozeb ve své organizaci (např. se podílí na užití konceptů bezpečnostních technologií k ochraně kritické infrastruktury, majetku a osob, nebo dostupných zbraní a vojenské techniky),</li> <li>• posoudí postupy bezpečnostního managementu ve své organizaci (např. se podílí na součinnosti se složkami integrovaného záchranného systému, s orgány veřejné správy, nebo na vedení a řízení v podmínkách ozbrojených sil),</li> <li>• srovnávají koncepty managementu rizik k</li> </ul>	<p>zaci (např. samostatně využijí informace z krizových anebo havarijních štábů, jednotek ozbrojených sil, nebo soukromých bezpečnostních agentur),</p> <ul style="list-style-type: none"> <li>• navrhnou a řídí management rizika k posouzení nebezpečí a hodnocení rizika ve své organizaci (např. samostatně využijí prediktivní hodnocení bezpečnosti a spolehlivosti užitých bezpečnostních technologií, nebo vojenských technologií),</li> <li>• aplikují a posuzují právní anebo technické předpisy či normy ve své organizaci (např. samostatně používají technické předpisy či normy pro použití technologií na ochranu kritické infrastruktury, majetku a osob),</li> <li>• analyzují a vyhodnocují prostředky pro komunikaci v oblasti krizového řízení ve své organizaci (např. samostatně používají radiokomunikační a telekomunikační prostředky),</li> <li>• analyzují a vyhodnocují principy a postupy logistiky v oblasti bezpečnosti ve své organizaci (např. samostatně používají principy a postupy logistiky pro zabezpečení systémů ochrany kritické infrastruktury, majetku a osob, nebo metody diverzifikace rizik, deterministických a stochastických metod řízení zásob),</li> <li>• aplikují a posuzují využití informačních a komunikačních technologií ve své organizaci (např. samostatně užívají nástroje manažerské informatiky pro sběr, zpracování, zhodnocení a prezentaci dat, nebo systémy pro počítačovou podporu návrhu technologií pro ochranu majetku a osob, zbraní a vojenské techniky a sledování její spolehlivosti v provozu),</li> <li>• analyzují a navrhnou koncepty bezpečnostní politiky k prevenci a eliminaci bezpečnostních hrozeb ve své organizaci (např. samostatně užívají koncepty bezpečnostních technologií k zajištění kritické infrastruktury, majetku a osob, nebo dostupné zbraně a vojenskou techniku, nebo plány krizové připravenosti, vnitřní havarijní plány, nebo operační plány),</li> <li>• analyzují a navrhnou postupy bezpečnostního managementu ve své organizaci (např. samostatně realizují postupy ochrany kritické infra-</li> </ul>	<p>rušení a působení výkonových elektromagnetických polí, nebo aplikace deterministických a stochastických metod řízení zásob v podmínkách nejistoty),</p> <ul style="list-style-type: none"> <li>• analyzují a vytvářejí původním výzkumem podpůrné informačně komunikační nástroje hodnocení rizik, vyhodnocování dat a stanovování priorit, podporujících řízení organizace anebo pracovních týmů (např. analyzují a vytvářejí informační systémy pro sledování a vyhodnocování provozní spolehlivosti systémů pro ochranu kritické infrastruktury, majetku a osob, nebo zbraní a vojenské techniky, nebo navrhnou systémy pro řízení systémů fyzické ochrany),</li> <li>• posuzují a oceňují výzkumné postupy umožňující definovat požadavky kladené na bezpečnostní systém, kompetence, povinnosti a odpovědnost jeho dílčích částí navzájem mezi sebou (např. vyhodnocují postupy specifikace požadavků na spolehlivost, bezpečnost a odolnost systémů fyzické ochrany a jejich prvků, nebo bezpečnost zbraní a vojenské techniky),</li> <li>• oponují výzkumné postupy umožňující rozšiřovat poznání vnitřní bezpečnosti a veřejného pořádku, ochrany ekonomiky, kritické infrastruktury a obrany státu při mimořádných událostech a krizových stavech (např. rozvíjí výzkum možností detekce pohybu osob v perimetru, nebo výzkum použití bezpečnostních zařízení pro omezení pohybu techniky v okolí prvků kritické infrastruktury),</li> <li>• zdůvodňují a zhodnocují výzkumné postupy v oblasti metodologie analýzy rizik při jejím využívání k zajišťování bezpečnosti na strategické úrovni veřejné správy, bezpečnostních a záchranných složek a bezpečnostních informačních a komunikačních technologií (např. vyhodnocují výzkumné postupy pro hodnocení počítačové bezpečnosti v oblasti infrastruktury pro krizové řízení, nebo řízení systémů pro ochranu kritické infrastruktury, majetku a osob, nebo výzkumné postupy pro hodnocení spolehlivosti systému člověk-technika-prostředí),</li> <li>• posuzují a oceňují aspekty a dopady právní úpravy a norem při zajišťování bezpečnosti ČR</li> </ul>
--	--	---	---	---

## Národní kvalifikační rámec terciárního vzdělávání

		<p>identifikaci nebezpečí a hodnocení rizika ve své organizaci (např. se podílí na tvorbě konceptů užití bezpečnostních technologií k ochraně kritické infrastruktury, majetku a osob, nebo managementu rizik bezpečnosti práce, bezpečnosti technických zařízení, nebo konceptů užití zbraní a vojenské techniky),</p> <ul style="list-style-type: none"> <li>• srovnávají postupy plynoucí z ustanovení právních a technických předpisů a norem v oblasti krizového řízení ve své organizaci (např. se podílí na tvorbě postupů užití technologií k ochraně kritické infrastruktury, majetku a osob, nebo postupů aplikované kryptografie, nebo postupů užití zbraní a vojenské techniky),</li> <li>• posoudí koncepty ochrany společnosti ve vztahu k sociální problematice a v návaznosti na lidská práva ve své organizaci (např. postupy logistického zabezpečení v oblasti používání zbraní a vojenské techniky),</li> <li>• srovnávají postupy logistického zabezpečení k aplikaci ekonomických aspektů zajišťování bezpečnosti ve své organizaci (např. se podílí na setřídění postupů logistického zabezpečení ochrany kritické infrastruktury, majetku a osob, nebo identifikaci úrovně bezpečnosti při vynaložených disponibilních zdrojích, nebo zabezpečení při užití zbraní a vojenské techniky),</li> <li>• posoudí postupy aplikované informatiky ve své organizaci (např. se podílí na využití SW nástrojů pro krizové řízení, nebo řešení záchranných a likvidačních prací, nebo užití počítačové podpory návrhu technologií pro ochranu majetku a osob a sledování její spolehlivosti v provozu, nebo užití počítačové podpory návrhu zbraní a vojenské techniky a sledování její spolehlivosti v provozu).</li> </ul>	<p>struktury, majetku a osob, nebo taktiku používání techniky při zvýšeném riziku),</p> <ul style="list-style-type: none"> <li>• analyzují a vytváří koncepty managementu rizik k identifikaci nebezpečí a hodnocení rizika ve své organizaci (např. samostatně realizují koncepty užití bezpečnostních technologií k zajištění ochrany kritické infrastruktury, majetku a osob),</li> <li>• analyzují a vytváří postupy plynoucí z ustanovení právních a technických předpisů a norem v oblasti krizového řízení ve své organizaci (např. samostatně realizují postupy užití technologií k ochraně kritické infrastruktury, majetku a osob, nebo postupů aplikované kryptografie, nebo užití zbraní a vojenské techniky),</li> <li>• analyzují a navrhuji koncepty ochrany společnosti ve vztahu k sociální problematice a v návaznosti na lidská práva ve své organizaci,</li> <li>• analyzují a vytváří postupy logistického zabezpečení k aplikaci ekonomických aspektů zajišťování bezpečnosti ve své organizaci (např. samostatně provádí postupy logistického zabezpečení ochrany kritické infrastruktury, majetku a osob, nebo plánování logistické podpory vojenské operace, nebo zabezpečení při užití zbraní a vojenské techniky),</li> <li>• analyzují a navrhuji postupy aplikované informatiky ve své organizaci (např. samostatně využívají SW nástroje pro krizové řízení, nebo řešení záchranných a likvidačních prací, nebo užití počítačové podpory návrhu technologií pro ochranu majetku a osob a sledování její spolehlivosti v provozu, nebo užití počítačové podpory návrhu zbraní a vojenské techniky a sledování její spolehlivosti v provozu).</li> </ul>	<p>a eventuálně instituce v návaznosti na mezinárodní normotvorné a zákonné instituty (např. vyhodnocují aspekty a dopady právních a technických norem pro použití technologií na ochranu kritické infrastruktury, majetku a osob, nebo zbraní a vojenské techniky v ČR v návaznosti na mezinárodní legislativu),</p> <ul style="list-style-type: none"> <li>• posuzují a oceňují aspekty a dopady vztahu člověk – bezpečnost (např. rozvíjí výzkum vlivu lidského faktoru na efektivnost a spolehlivost technologií pro ochranu kritické infrastruktury, nebo majetku a osob, nebo vojenské techniky),</li> <li>• zdůvodňují a revidují širší souvislosti aplikací teorie logistických řetězců umožňujících optimalizovat disponibilní zdroje a koordinovat činnost týmu při eliminaci bezpečnostních hrozeb a minimalizaci dopadů bezpečnostních rizik (např. vyhodnocují koncepce, metody a postupy zajišťování bezpečnosti v pozemní a letecké dopravě, nebo aplikace opatření pro eliminaci teroristických hrozeb, nebo metody identifikace, analýzy a reakce na interní a externí rizika logistických řetězců),</li> <li>• oponují a zhodnocují metody aplikované informatiky v oblasti řízení bezpečnosti v podmínkách představujících nestabilní bezpečnostní prostředí (např. vyhodnocují využití systémů pro počítačovou podporu návrhu technologií pro ochranu majetku a osob, nebo zbraní a vojenské techniky a sledování její spolehlivosti v provozu, nebo systémů pro řízení fyzické ochrany, nebo využití nástrojů manažerské informatiky pro řešení pracovních úkolů, včetně klasifikace algoritmů jejich řešení).</li> </ul>
--	--	--	--	--

## **VZTAHY K OSTATNÍM OBLASTEM VZDĚLÁVÁNÍ**

Jak již bylo uvedeno, typickou charakteristikou oblasti vzdělávání „bezpečnostní oborů“ je její multidisciplinarita. Tato skutečnost má za následek, že nelze vyloučit žádnou další oblast vzdělávání, která by jí nebyla dotčena. Studijní obory v rámci bezpečnostních oborů v řadě případů představují speciální „nadstavbu“ disciplín spadajících do jiných oblastí vzdělávání, které však výrazně aplikují a doplňují v oblasti bezpečnosti, a to nejen obsahově, ale metodologicky. V současnosti je možné tyto vazby nalézt k oblastem vzdělávání: ekonomické obory, chemie, vědy o Zemi, stavebnictví, elektrotechnika, informační technologie a kybernetika, strojírenství a materiály, těžba a zpracování nerostných surovin, zpracovatelský průmysl, všeobecné a zubní lékařství, farmacie, zdravotnické obory, dopravní a přepravní služby.

## **CHARAKTERISTICKÉ PROFESE A RELEVANTNÍ REGULOVANÉ PROFESE**

Tyto profese jsou uvedeny v následující tabulce. Údaje jsou kompatibilní se současnou terminologií používanou v klasifikaci zaměstnání (KZAM) vedenou Českým statistickým úřadem a databází regulovaných povolání a činností v ČR vedenou MŠMT.

<b>kód</b>	<b>charakteristické profese</b>
112	Vyšší státní úředníci: 112 7 Vedoucí pracovníci orgánů státní správy, správních úřadů; 112 8 Vyšší úředníci bezpečnosti a ochrany;
114	Vedoucí pracovníci politických, zájmových a odborových organizací: 114 2 Vedoucí pracovníci zájmových, odborových a společenských organizací; 114 3 Vedoucí pracovníci humanitárních a podobných organizací;
115	Přednostové, tajemníci a vedoucí pracovníci okresních a obecních úřadů: 115 0 Přednostové (vč. zástupců), tajemníci a vedoucí pracovníci okresních a obecních úřadů;
122	Vedoucí pracovníci výrobních a provozních dílčích celků velkých organizací, podniků apod.: 122 9 Vedoucí pracovníci dílčích celků jinde neuvedení;
123	Vedoucí pracovníci univerzálních dílčích celků: 123 2 Vedoucí pracovníci personálních útvarů a útvarů průmyslových vztahů; 123 9 Vedoucí pracovníci ostatních útvarů jinde neuvedení;
131	Vedoucí, ředitelé malých podniků, organizací: 131 9 Vedoucí, ředitelé malých podniků, organizací ostatní jinde neuvedení (školství, kultura, sport, zdravotnictví apod.);
211	Vědci a odborníci ve fyzikálních, chemických a příbuzných oborech: 211 9 Ostatní vědci a odborníci v příbuzných oborech jinde neuvedení;
212	Vědci a odborníci v oblasti matematiky, statistiky a v příbuzných oborech: 212 9 Vědci a odborníci v příbuzných oborech jinde neuvedení;
213	Vědci a odborníci v oblasti výpočetní techniky: 213 9 Ostatní odborníci zabývající se výpočetní technikou jinde neuvedení;
214	Architekti, projektanti, konstruktéři techničtí vědci a inženýři (tvůrčí pracovníci): 214 1 Hlavní architekti, architekti a plánovači měst, urbanisté, projektanti měst, obcí, dopravních sítí; 214 2 Projektanti staveb a areálů, stavební inženýři; 214 3 Projektanti elektrotechnických zařízení, elektroinženýři; 214 4 Projektanti elektronických systémů a telekomunikačních sítí, inženýři – elektronici; 214 5 Projektanti a konstruktéři strojních zařízení, strojní inženýři; 214 6 Chemičtí inženýři, technologové; 214 7 Důlní a hutní inženýři, technologové, metalurgové; 214 9 Ostatní architekti, projektanti, konstruktéři a techničtí inženýři jinde neuvedení;
221	Vědci, odborníci a inženýři v biologických a příbuzných oborech: 221 1 Bakteriologové, biologové, ekologové, zoologové a odborníci v příbuzných oborech; 221 2 Farmakologové, anatomové, biochemici, fyziologové, patologové a odborníci v blízkých oborech;
222	Odborní zdravotničtí a veterinární pracovníci: 222 1 Lékaři, ordináři (kromě zubních lékařů); 222 2 Zubní lékaři (dentisté); 222 3 Veterinární lékaři;

*Národní kvalifikační rámec terciárního vzdělávání*

	222 4 Farmaceuti, magistři v lékárně, lékárníci; 222 5 Hygienici;
231	Vědeckopedagogičtí pracovníci a učitelé na vysokých školách: 231 1 Vědeckopedagogičtí pracovníci; 231 9 Ostatní učitelé na vysokých školách;
232	Učitelé středních škol: 232 2 Učitelé odborných předmětů; 232 3 Učitelé praktického vyučování (kromě mistrů - skupina 334);
233	Učitelé základních škol a předškolní výchovy: 233 1 Učitelé základních škol;
235	Učitelé a odborní pedagogičtí pracovníci jinde neuvedení: 235 2 Školní inspektoři; 235 9 Ostatní odborní pedagogičtí pracovníci jinde neuvedení;
315	Bezpečnostní, protipožární, kolaudační technici a technici kontroly zdravotní nezávadnosti a jakosti: 315 1 Kolaudační technici a technici protipožární ochrany, specialisté pro prevenci požárů a zjišťování příčin požárů (kromě hasičů - hl. třída 5); 315 2 Bezpečnostní technici a technici pro kontrolu zdravotní nezávadnosti a jakosti;
322	Zdravotničtí asistenti, optici a rehabilitační pracovníci: 322 9 Zdravotnický záchranář;
343	Odborní administrativní pracovníci: 343 4 Pracovníci v oblasti statistiky a matematiky; 343 9 Ostatní odborní administrativní pracovníci jinde neuvedení;
344	Celní a daňoví pracovníci a pracovníci v příbuzných oborech: 344 1 Celní pracovníci;
345	Policejní inspektoři a detektivové: 345 1 Policejní inspektoři, komisaři; 345 2 Vyšetřovatelé; 345 3 Detektivové, kriminalisté;
348	Profesionální sportovci a pracovníci ve sportu: 348 2 Trenéři, cvičitelé a úředníci sportovních podniků a klubů;
516	Pracovníci ochrany a ostrahy: 516 1 Hasiči, požárníci; 516 2 Pracovníci bezpečnostních orgánů; 516 5 Pracovníci ochrany v dopravě; 516 9 Ostatní pracovníci ochrany a ostrahy jinde neuvedení;
010	Příslušníci armády
<b>kód</b>	<b>regulované profese</b>
69	Mezinárodní přeprava radioaktivních odpadů v rozsahu stanoveném prováděcím právním předpisem
103	Technik požární ochrany
106	Technik speciálních služeb jednotky HZS podniku
132	Technicko-organizační činnost v oblasti požární ochrany
147	Poskytování služeb v oblasti bezpečnosti a ochrany zdraví při práci
157	Výroba nebezpečných chemických látek a nebezpečných chemických přípravků a prodej chemických látek a chemických přípravků klasifikovaných jako vysoce toxické a toxické
251	Zpracování hodnocení rizika
297	Nakládání s vysoce nebezpečnými látkami zneužitelnými k porušování zákazu chemických zbraní
407	Poskytování technických služeb k ochraně majetku a osob
409	Ostraha majetku a osob
458	Bezpečnostní poradce pro přepravu nebezpečných věcí na silnici
459	Bezpečnostní poradce pro přepravu nebezpečných věcí pro železniční dopravu
567	Bezpečnostní poradce pro přepravu nebezpečných věcí
570	Kontrolní technik typu „ADR“
613	Nákup a prodej, půjčování, vývoj, výroba, opravy, úpravy, uschovávání, skladování, přeprava, znehodnocování a ničení bezpečnostního materiálu
615	Pověření k hodnocení nebezpečných vlastností odpadů uvedených v příloze č. 2 k zákonu č. 185/2001 Sb. pod označením kódem H1, H2, H3-A, H3-B, H12, H13 a H14
616	Pověření k hodnocení nebezpečných vlastností odpadů uvedených v příloze č. 2 k zákonu č. 185/2001 Sb.

*Národní kvalifikační rámec terciárního vzdělávání*

625	Koordinátor BOZP na staveništi
650	Služby soukromých detektivů