Informační podpora bezpečnosti

Téma:

Informační a komunikační systémy podpory bezpečnosti,
zadání témat seminárních prací

Cíl:

- zadání témat seminárních prací;
- informační a komunikační systémy;
- využití informačních a komunikačních systémů pro podporu bezpečnosti.

Úkoly pro samostatnou práci:

- znát co jsou základními registry veřejné správy;
- studium literatury;
- prohloubení informací získaných na hodině;
- vybraní studenti si připraví seminární práci na zadané téma.

Studijní literatura:

- BARTA, Jiří; SVOBODA, Oldřich; URBÁNEK, Jiří; URBÁNEK, Jiří. Krizová interoperabilita. Brno: Univerzita obrany, 2015, 89 s. ISBN 978-80-7231-428-7.
- BARTA, Jiří; LUDÍK, Tomáš. Krizový scénář - modelové řešení havárie. Skripta. Brno: Univerzita obrany, 2012, 47 s.
- JURENKA, Miroslav; MALACHOVÁ, Hana; URBAN, Rudolf. Krizové řízení I. Skripta. Brno: Univerzita obrany, 2016, 129 s. ISBN 978-80-7231-379-2.
- Zákon č. 240/2000 Sb. ze dne 28. června 2000, o krizovém řízení a o změně některých zákonů (krizový zákon)
- Zákon č. 239/2000 Sb., o integrovaném záchranném systému a změně některých zákonů.
- RICHTER; Rostislav. Slovník pojmů krizového řízení. Praha: Ministerstvo vnitra, 2018. ISBN 978-80-87544-91-4.
- Vyhláška Národního bezpečnostního úřadu č. 317/2014 Sb., o významných informačních systémech a jejich určujících kritériích

Obsah:

Pořadové číslo	Název tématu
1.	Prezence, zápis do třídních knih

2.	Zadání seminárních prací
3.	Úvod
4.	Informační systémy
5.	Informační systémy veřejné správy
6.	Využívané informační systémy pro zvýšení bezpečnosti
7.	Úkoly na samostudium
8.	Závěr – shrnutí cvičeného tématu, vyřešení případných dotazů a nejasností

TEXT

Po provedení administrativních prací spojených s praktickým fungováním studijní skupiny bude následovat zadání témat seminárních prací.

Každý student dostane zadáno individuální téma seminární práce na základě aktuálně probíraných témat bezpečnostní situace v ČR. Prezentace seminárních prací budou probíhat na každé hodině (od současné hodiny za dva týdny bude první). V závislosti na počtu studentů bude stanoven minimální počet prezentujících na hodině.

V úvodu do problematiky informačních systémů pro podporu bezpečnosti budou diskutována obecné informační systémy, a jejich využití ve vztahu k zajištění bezpečnosti.

Následujícím tématem budou informační systémy veřejné správy, které jsou hlavními systémy pro evidenci obyvatel, spolků, FO, PO a dalších významných údajů.

Informační systémy veřejné správy

Informační systémy veřejné správy jsou souborem informačních systémů, které slouží pro výkon veřejné správy. Ministerstvo vnitra zajišťuje rozvoj, výstavbu a metodické řízení ISVS. Prostřednictvím atestace dlouhodobého řízení ISVS, atestace způsobilosti k realizaci vazeb ISVS prostřednictvím referenčního rozhraní a kontrolní činnosti realizuje zpětnou vazbu na metodiky a vyhlášky k zákonu č. 365/2000 Sb., o ISVS, ve znění pozdějších předpisů a jejich dodržování v praxi. Projektovým přístupem omezuje vznik duplicit při provozování ISVS. Zabezpečuje reálné požadavky na čerpání financí z veřejných rozpočtů v oblasti ICT. Připravuje technologické podmínky pro efektivnější výkon veřejné moci.

- • Legislativa
- • Metodické pokyny
- • Další dokumenty
- • Povinně zveřejňované informace
- • Atestace a akreditace
- • IS o ISVS a ISDP

Příklad řízení kvality ISVS pro obec s pověřeným obecním úřadem a pro obec vykonávající přenesenou působnost v základním rozsahu

Tento dokument obsahuje příklady, poskytující metodickou podporu zejména obcím, které zajišťují řízení kvality informačních systémů veřejné správy převážně svými zaměstnanci.

Příklady informačních koncepcí

Ministerstvo vnitra v souvislosti s § 5a novely zákona č. 365/2000 Sb., o informačních systémech veřejné správy (ISVS), provedené zákonem č. 81/2006 Sb. (zákon) zveřejňuje příklady zpracovaných inform...

Informace k novele zákona č. 365/2000 Sb., o informačních systémech veřejné správy - zákon č. 81/2006 Sb.

Novela zákona č. 365/2000 Sb., o informačních systémech veřejné správy (zákon č. 81/2006 Sb.), vychází ze zkušeností s aplikací zákona v jeho podobě před novelizací, reaguje na rozvoj informačních a k...

Nařízení vlády č. 594/2006 Sb., o přepisu znaků do podoby, ve které se zobrazují v informačních systémech veřejné správy

Dne 27. 12. 2006 bylo ve Sbírce zákonů, částce 188 zveřejněno nařízení vlády č. 594/2006 Sb., o přepisu znaků do podoby, ve které se zobrazují v informačních systémech veřejné správy. Nařízení bylo no..

Zákon č. 365/2000 Sb., o informačních systémech veřejné správy

Dne 23. 10. 2000 byl ve Sbírce zákonů, částce 99 zveřejněn zákon č. 365/2000 Sb., o informačních systémech veřejné správy. Zákon byl dále novelizován.

Vyhláška č. 64/2008 Sb., o formě uveřejňování informací souvisejících s výkonem veřejné správy prostřednictvím webových stránek pro osoby se zdravotním postižením (vyhláška o přístupnosti)

Dne 28. 2. 2008 byla ve Sbírce zákonů, částce 20 zveřejněna vyhláška č. 64/2008 Sb., o formě uveřejňování informací souvisejících s výkonem veřejné správy prostřednictvím webových stránek pro osoby se...

Vyhláška č. 53/2007 Sb., o referenčním rozhraní

Dne 22. 3. 2007 byla ve Sbírce zákonů, částce 24 zveřejněna vyhláška č. 53/2007 Sb., o technických a funkčních náležitostech uskutečňování vazeb mezi informačními systémy veřejné správy prostřednictví...

Vyhláška č. 52/2007 Sb., o postupech atestačních středisek při posuzování způsobilosti k realizaci vazeb ISVS prostřednictvím referenčního rozhraní

Dne 22. 3. 2007 byla ve Sbírce zákonů, částce 24 zveřejněna vyhláška č. 52/2007 Sb., o postupech atestačních středisek při posuzování způsobilosti k realizaci vazeb informačních systémů veřejné správy...

Vyhláška č. 530/2006 Sb., o postupech atestačních středisek při posuzování dlouhodobého řízení ISVS

Dne 6. 12. 2006 byla ve Sbírce zákonů, částce 172 zveřejněna vyhláška č. 530/2006 Sb., o postupech atestačních středisek při posuzování dlouhodobého řízení informačních systémů veřejné správy.

Vyhláška č. 529/2006 Sb., o dlouhodobém řízení informačních systémů veřejné správy

Dne 6. 12. 2006 byla ve Sbírce zákonů, částce 172 zveřejněna vyhláška č. 529/2006 Sb., o požadavcích na strukturu a obsah informační koncepce a provozní dokumentace a o požadavcích na řízení bezpečnos...

Vyhláška č. 528/2006 Sb., o informačním systému o informačních systémech veřejné správy

Dne 6. 12. 2006 byla ve Sbírce zákonů, částce 172 zveřejněna vyhláška č. 528/2006 Sb., o formě a technických náležitostech předávání údajů do informačního systému, který obsahuje základní informace o ...

Vyhláška č. 469/2006 Sb., o informačním systému o datových prvcích

Dne 24. 10. 2006 byla ve Sbírce zákonů, částce 154 zveřejněna vyhláška č. 469/2006 Sb., o formě a technických náležitostech předávání údajů do informačního systému o datových prvcích a o postupech Min...

Ministerstva a ostatní ústřední správní úřady, správní úřady a orgány územních samosprávných celků jsou povinny při plnění úkolů zajišťování obrany státu **vzájemně spolupracovat a vyměňovat si v nezbytně nutném rozsahu informace z informačních systémů, které vedou**. Při plnění úkolů zajišťování obrany státu využívají pracovišť krizového řízení, pracovních a poradních orgánů zřízených podle krizového zákona. Vzájemnou spolupráci a výměnu informací koordinuje MO.

Za stavu ohrožení státu vyhlášeného v souvislosti se zajišťováním obrany ČR před vnějším napadením a za válečného stavu mohou orgány krizového řízení nařizovat také opatření podle zvláštního právního předpisu, nejsou-li v rozporu se zákonem o zajišťování obrany ČR.

Zvláštní skutečnosti

Zvláštními skutečnostmi se rozumí **údaje z oblasti krizového řízení, které by v případě zneužití mohly vést k znemožnění nebo omezení činnosti orgánu krizového řízení, ohrožení života a zdraví osob, majetku, životního prostředí nebo podnikatelského zájmu**

PaPFO vykonávající podnikatelskou nebo jinou obdobnou činnost. Takto označené skutečnosti nenesou statut utajovaných informací podle zvláštního právního předpisu.

Orgány krizového řízení označují krizové plány a ostatní listiny, nosná média a jiné materiály obsahující zvláštní skutečnosti slovy "zvláštní skutečnosti" nebo zkratkou "ZS".

K ochraně ZS je potřeba přijmout i různá režimová opatření – personální, administrativní, objektová a technická bezpečnost a **bezpečnost informačních systémů**. Se ZS se mohou seznamovat jen oprávnění pracovníci, kteří musí být zapsáni ve zvláštním seznamu. Tito jsou povinni zachovávat mlčenlivost, tzn. nesdělovat zvláštní skutečnost osobě, která není oprávněna se s takovou skutečností seznamovat.

Informační systémy využitelné pro krizové řízení

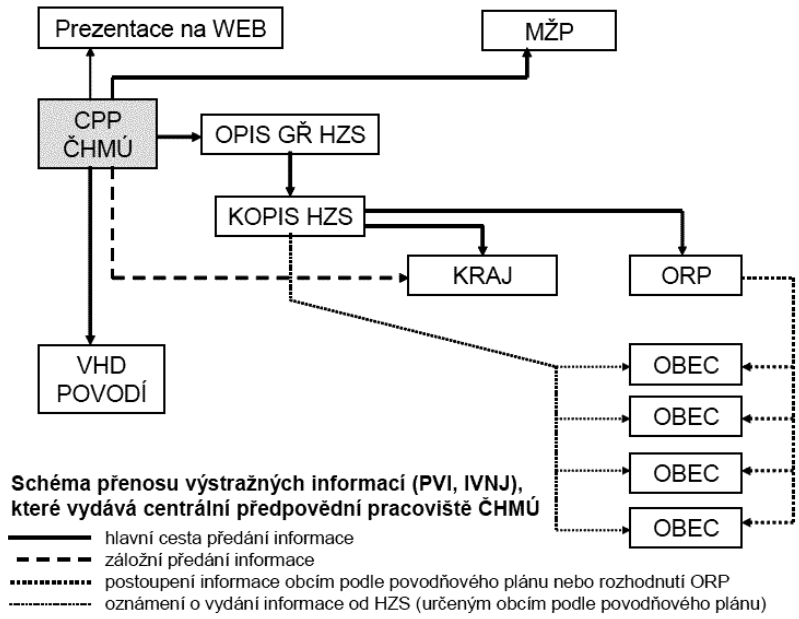
Orgány krizového řízení při plánování krizových opatření a při řešení KS využívají informační systémy krizového řízení a jednotné geografické podklady v analogové nebo digitální podobě. Jednotnými geografickými podklady pro plnění plánovaných opatření a při řešení KS jsou státní mapová díla a další geografické produkty vytvářené pro zajišťování obrany státu.

Mezi celostátní informační systémy využívané při přípravě a při řešení KS je informační systém pro podporu hospodářských opatření pro krizové stavy (IS ARGIS), který spravuje SSHR.

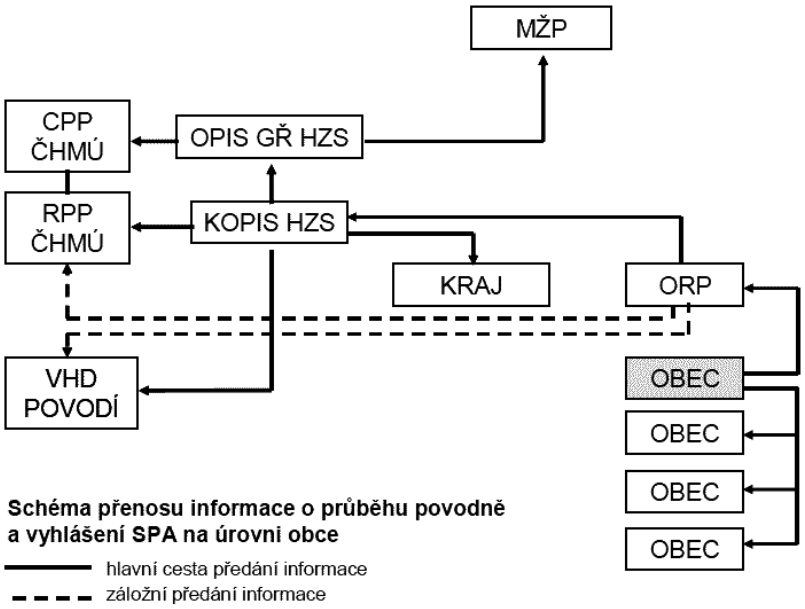
Jednotlivé kraje využívají při plánování krizových opatření a při řešení KS také vlastní informační a geografické systémy.

IS pro řešení povodní

Organizaci hlásné a předpovědní povodňové služby metodicky řídí MŽP jako ústřední povodňový orgán ČR, který je také garantem **povodňového informačního systému (POVIS),** který soustřeďuje data potřebná pro tvorbu povodňových plánů obcí, ORP a krajů. Jeho účelem je zlepšení přístupu k informacím a umožnění jejich sdílení a aktualizaci. V systému je uložen Digitální povodňový plán ČR a také další povodňové orgány v něm mohou mít uloženy svůj digitální povodňový plán a digitální povodňovou knihu. Administrátorem tohoto systému je ČHMÚ. Odborné pokyny pro hlásnou povodňovou službu vydává ČHMÚ a obsahují odborná pravidla pro provozování a hlášení povodňových stavů, doporučená kritéria pro výběr hlásných profilů a další doporučení pro povodňové orgány týkající se vyhlašování SPA podle množství srážek a podle ledových jevů na vodních tocích.



Příloha č. 3



IS přeprava nebezpečných věcí

Přeprava nebezpečných věcí je ošetřena mezinárodními dohodami ADR a RID. ADR je Evropská dohoda o mezinárodní silniční přepravě, která ukládá podmínky přepravy nebezpečného nákladu po silnicích. RID je Řád pro mezinárodní železniční přepravu nebezpečných věcí, který ukládá podmínky přepravy nebezpečných věcí po železnici. Obě dohody zavádí pojem nebezpečná věc, který je totožný s pojmem nebezpečné látky.

V silniční přepravě jsou údaje o charakteru nebezpečného nákladu v nákladním listu a písemných pokynech pro případ nehody. V rámci železniční dopravy je základním dokumentem rovněž nákladní list, který je k dispozici u vlakvedoucího.

Na základě smluvního vztahu mezi Svazem chemického průmyslu ČR a MV – GŘ HZS ČR poskytuje **transportní a informační systém (dále „TRINS“)** pomoc OPIS IZS při řešení MU spojených s přepravou a skladováním nebezpečných látek na území ČR. Činnost TRINS je organizována republikovým koordinačním střediskem a regionálními středisky. Jedná se o otevřený systém, který se neustále rozvíjí, a do kterého jsou rovněž zapojeny jako regionální střediska členské společnosti chemického průmyslu. TRINS poskytuje OPIS IZS zejména údaje k výrobkům, látkám a jejich bezproblémové přepravě a skladování, praktické zkušenosti s manipulací nebezpečnou látkou nebo s likvidací MU spojených s nebezpečnou látkou, praktickou pomoc při odstraňování škod a likvidaci MU spojených s nebezpečnou látkou.

Při zásazích s nebezpečnou látkou má významnou roli OPIS HZS kraje, které zajišťuje nejen vysílání SaP, ale rovněž **poskytuje informační podporu veliteli zásahu**. Zdrojem dat jsou zejména VněHP, havarijní karty, databáze a softwary pro modelování úniků nebezpečných látek.

Každý HZS kraje je vybaven elektronickou databází nebezpečných látek **MedisAlarm**. Při vyhledávání není třeba znát přesný název látky, vyhledávat lze látku i zadáním synonyma, CAS, čísla ES, indexového čísla nebo UN kódu. Databáze obsahuje údaje o identifikaci, základní vlastnosti, způsoby hašení a skladování, fyzikálně chemické vlastnosti, pokyny pro přepravu dle ADR/RID, první pomoc a zdravotní ošetření, údaje o toxicitě, legislativní limity a předpisy ČR a EU.

Na internetu je rovněž řada databází, z nichž nejznámější je **Dopravní a informační systém DOK** provozovaný MD. Databáze obsahuje modul havárie, kontrola, legislativa, statistika a mobilní verze. Součástí jsou informace kanadské ERG. Cenné jsou zejména informace o nebezpečnosti látky, reakci s vodou, vzdálenosti pro vytvoření nebezpčené zóny, doporučení pro likvidaci daného typu havárie. Příklady databází nebezpečných látek dostupné na internetu:

- IS DOK (http://cep.mdcr.cz/dok2/DokPub/dok.asp),
- Plumbum (http://www.piskac.cz/ETD/DEFAULT.HTM),
- IRIS (www.epa.gov/iris/index.htm),
- HSDB (http://www.nlm.nih.gov/pubs/factsheets/hsdbfs.html)
- TOXNET (http://toxnet.nlm.nih.gov),
- ASTDR (http://www.atsdr.cdc.gov/toxfaq.html).

Pro modelování následků havárií existuje řada SW nástrojů. V rámci HZS krajů je nejužívanější SW Aloha, který je podrobněji popsán v kapitole 3.3.3 části II. Pro hodnocení dosahů účinků havarijních projevů v rámci havarijního plánování je doporučováno využití metodického přístupu podle vyhlášky č. 226/2015 Sb.

Varování a informování obyvatelstva

Pro zabezpečení varování a vyrozumění je na území ČR budován a provozován JSVV. Je tvořen vyrozumívacími centry (celostátní, krajské a tzv. úrovně dalších provozovatelů), datovými a rádiovými sítěmi a koncovými prvky varování a vyrozumění. Koncovými prvky varování jsou sirény rotační (elektromechanické, dále „ROT“), sirény elektronické (dále „ENS“) a místní informační systémy = obecní rozhlasy připojené do JSVV (dále „MIS“). V posledních letech bývá často užíván pojem jednotný systém varování a informování (dále „JSVI“), jehož úkolem je nejen vyhlašování varovného signálu a předávání tísňových informací obyvatelstvu, nýbrž i následné informování obyvatelstva o charakteru ohrožení a režimových opatřeních v území.

Infrastruktura JSVV je v ČR tvořena:

- systémem selektivního rádiového návěštění (dále „SSRN“), kterým je zabezpečováno ovládání koncových prvků varování a vyrozumění a
- koncovými prvky varování a vyrozumění, kterými je zabezpečováno vlastní varování a vyrozumění obyvatelstva.

SSRN je neveřejný digitální systém, který je určen pro zabezpečení specifických úkolů varování obyvatelstva a vyrozumění osob zařazených do složek IZS. Je budován a provozován na krajské úrovni (10 krajských subsystémů). Základními prvky SSRN jsou:

- vysílací infrastruktura realizující datové spoje mezi jednotlivými částmi SSRN (tvořena sítí základových stanic, které zabezpečují pokrytí zájmových oblastí radiovým signálem),
- zadávací terminály a přenosové cesty (umožňující vstup z vyrozumívacích center jednotlivých úrovní do SSRN) a
- koncové prvky SSRN, tj. přijímače pro ovládání sirén se sirénami a dalšími prvky varování (např. MIS) a osobních přijímačů (pagerů).

Zatímco SSRN je jednosměrný systém, který zajišťuje pouze předávání aktivačních příkazů pro varování a vyrozumění koncovými prvky (sirény, pagery) a neumožňuje získat přehled o tom, zda koncové prvky provedly požadovanou činnost a v jakém provozním stavu se nacházejí, monitorovací systém koncových prvků je systémem obousměrným. Monitorovací systém koncových prvků představuje integrální rozšíření stávajícího systému JSVV-SSRN o paralelní systém umožňující sběr, přenos, zpracování, archivaci a zobrazení informací od koncových prvků varování a koncových prvků měření (senzorů).

Místní informační systémy

Jedná se především o bezdrátové rozhlasy, okrajově o rozhlasy se 100V rozvody a kabelové televize. Společným principem MIS je to, že signál je zpravidla reprodukován z audiopaměti řídící jednotky, nebo ze zvukových souborů řídícího počítače, distribuován příslušnou

technologií a na zvuk přeměněn v elektroakustických měničích. MIS jsou vhodné do lokalit, kde se nachází nízká koncentrace obyvatelstva na velké ploše. U řady zařízení je možno akustický signál distribuovat až do domácností, veřejných budov atd. Typy MIS, začleněných do JSVV jsou uvedeny v technických požadavcích na koncové prvky varování připojované do JSVV.

Organizace prevence závažných havárií

Výkon veřejné správy na úseku PZH vykonávají zákonem určené orgány státní správy, tj. MŽP, MV, ČBÚ a obvodní báňské úřady, ČIŽP, Státní úřady inspekce práce a oblastní inspektoráty práce, HZS krajů a krajské hygienické stanice a krajské úřady (v přenesené působnosti).

MŽP spravuje a provozuje **veřejný informační systém PZH, tzv. MAPIS** (Major Accident Prevention Information System), který slouží ke shromažďování údajů o objektech a souvisejících činnostech. V MAPIS je veden rejstřík objektů, včetně informací o jejich provozovatelích, činnostech a nebezpečných látkách v nich umístěných a dokumentaci zpracované dle zákona o PZH. Dále je v něm registr závažných havárií, registr plánovaných a provedených kontrol, prostorová data o objektech a jejich okolí a informace pro veřejnost zpracované dle zákona o PZH. Systém je určen nejen orgánům veřejné zprávy (tedy i HZS kraje) a provozovatelům, ale rovněž veřejnosti.

Elektronická informace pro veřejnost s možností dálkového přístupu je povinně publikována prostřednictvím informačního systému PZH (MAPIS). Dále je vhodné ji publikovat prostřednictvím krajského geoportálu, na internetových stránkách krajského úřadu, HZS kraje, dotčených obcí a jednotlivých provozovatelů nebo na cílených portálech sloužících občanům pro získávání informací z oblasti bezpečnosti.

Evidence a způsob vyřazení úkrytů z evidence

Dlouhá doba potřebná ke zpohotovení a také nerovnoměrné rozmístění stálých úkrytů civilní ochrany, které byly budovány a předurčeny k ochraně obyvatelstva před účinky ZHN, vede k tomu, že při MU a KS nevojenského charakteru nelze počítat s jejich využitím. Ze strany MV-GŘ HZS ČR bylo proto upřesněno, že nebudou uváděny v HPK.

Přesto mají podle zákona o IZS obecní úřady obcí a HZS krajů povinnost vést evidenci těchto staveb. Základem je vedení evidenčních listů jednotlivých úkrytů (listinná podoba). Z této kartotéky vychází **digitální evidence stálých úkrytů v informačním systému GIS OO**, případně další pomocná evidence sloužící potřebám orgánů státní správy a samosprávy na úseku ochrany obyvatelstva. HZS kraje vede evidenční listy úkrytů v kraji (včetně již vyřazených), evidenci stálých úkrytů v informačním systému GIS OO (včetně již vyřazených), evidenci rozestavěných staveb civilní ochrany na evidenčních listech a v informačním systému GIS OO a evidenci státních dotací rekonstrukcí úkrytů v informačním systému GIS OO. Obce vedou ve svých plánech ukrytí evidenční listy úkrytů a seznamy úkrytů v obci.

Nouzové základní služby obyvatelstvu

Zabezpečení nouzových základních služeb je plánováno zejména v těchto komoditách: ošacení, hygienické potřeby, lékárny, veterinární ambulance, sklenářství, pokrývačství, truhlářství, prádelny a čistírny, tuhá paliva, pohonné hmoty, pohřební služby, ostatní služby.

HZS kraje může s některými významnými dodavateli uzavřít písemnou dohodu podle paragraf 15, písm. b) krizového zákona a sjednat tak předem způsob a rozsah pomoci. Přehled zdrojů na území kraje je uveden v HPK, v krizovém plánu kraje (Plán nezbytných dodávek) a **v informačním systému Argis**, jehož provozovatelem je SSHR. Významnou oblastí základních služeb obyvatelstvu je nepřetržité zajištění poskytování potřebných sociálních služeb (osobní asistence, pečovatelská služba, sociálně-zdravotní služby apod.) a to jak na postiženém území, tak i v místech, kam byli občané evakuováni.

Informační systém pro města a obce

HZS Karlovarského kraje ve spolupráci s Asociací „Záchranný kruh“ o. s. vytvořil „Informační systém pro města a obce“, který zajišťuje ty nejdůležitější rady, návody a informace ze světa rizik a nebezpečí pro obyvatele (návštěvníky stránek) obce, města.

V rámci Integrovaného projektu „Záchranný kruh″ vznikly tyto dílčí projekty:

- „Bezpečnostní portál“ – účinný nástroj edukace první pomoci dětí a mládeže a jejich rodičů a pedagogů“,
- „Internetový bezpečnostní portál“ – vzdělávací, informační, komunikační a evaluační nástroj pro život, v rámci kterého byl rozšířen bezpečnostní portál www.zachrannykruh.cz na celostátní úroveň a byly vytvořeny nebo rozšířeny zejména publikační a zpravodajský systém,
- „Chraň svůj svět, chraň svůj život“ je zaměřen na aktivity ve vztahu ke školám a školským zařízením, dětem a mládeži,
- „Rizika silniční a železniční dopravy“, jehož výstupem je Interaktivní multimediální příručka dopravní výchovy,
- „Včas umět a znát je napořád“, jehož výstupem jsou didaktické a metodické pomůcky pro mateřské školy, zpracované i pro interaktivní výuku.

A další projekty na podporu vzdělávání

Mechanismus civilní ochrany

Stěžejním dokumentem EU v oblasti naší kompetence je tzv. Mechanismus civilní ochrany, který byl zřízen v roce 2001 Rozhodnutím Rady 2001/792/ES, Euratom na podporu zesílené spolupráce mezi Společenstvím a členskými státy při asistenčních zásazích v oblasti civilní ochrany v případě výskytu závažných mimořádných událostí nebo bezprostředního nebezpečí jejich výskytu uvnitř nebo vně Společenství. V roce 2007 byla Rozhodnutím Rady

2007/779/ES, Euratom přijata přepracovaná verze mechanismus civilní ochrany Společenství, která novelizovala původní Rozhodnutí dle nabytých zkušeností a tehdejších požadavků.

V roce 2013 byl za účelem posílení účinnosti, efektivnosti a soudržnosti evropské odezvy na katastrofy přijat Rozhodnutím Evropského parlamentu a Rady 1313/2013/EU nový mechanismus civilní ochrany Unie. Jeho cílem je podporovat, koordinovat a doplňovat činnosti členských států v oblasti civilní ochrany a zlepšovat účinnost systémů v oblasti prevence, připravenosti a odezvy. Jednou z důležitých změn je uvedení mechanismu civilní ochrany Unie do souladu s článkem 196 Smlouvy o fungování EU, který se zasazuje o integrovaný přístup k zvládání katastrof. Mechanismus civilní ochrany Unie nabyl účinnosti dne 1. ledna 2014 a je platný pro celou finanční perspektivu 2014-2020. V současné době se vztahuje na 31 států, z toho 28 členských států EU, Island, Lichtenštejnsko a Norsko. Využití některých opatření je však umožněno i ostatním kandidátským zemím a potenciálním kandidátům, jakož i zemím, které jsou součástí evropské politiky sousedství. Stěžejními prvky mechanismu civilní ochrany Unie jsou **středisko pro koordinaci odezvy na mimořádné události (ERCC) a společný komunikační a informační systém pro mimořádné události (CECIS),** díky nimž lze operativně koordinovat a komunikovat poptávanou a nabízenou pomoc a zároveň řešit logistiku této pomoci. Hlavním nástrojem mechanismu civilní ochrany Unie jsou evropské kapacity pro odezvu na mimořádné události (EERC), které se budou sestávat z dobrovolného souboru předem vyčleněných kapacit členských států pro odezvu a zahrnovat moduly (viz níže), další kapacity pro odezvu a odborníky. Za účelem posílení spolupráce v oblasti civilní ochrany a zajištění efektivnější a rychlejší odezvy implementuje Mechanismus civilní ochrany Unie řadu nových prvků a opatření, k nimž například náleží:

- zavedení nové kapitoly v oblasti prevence, s cílem posílit význam rámce politiky prevence EU a efektivně jej navázat na opatření připravenosti a odezvy,
- zřízení **střediska pro koordinaci odezvy na MU** (ERCC). Středisko navazuje na původní **monitorovací a informační středisko (MIC)**, které bylo posíleno, aby zajišťovalo nepřetržitou provozní kapacitu 24 hodin denně, 7 dní v týdnu,
- zřízení evropské kapacity pro odezvu na MU (EERC), které se budou sestávat z dobrovolného souboru předem vyčleněných kapacit členských států pro odezvu a zahrnovat moduly, další kapacity pro odezvu a odborníky,
- změna a zjednodušení finančních ustanovení, které byly původně samostatným finančním nástrojem, ale v současné době jsou zařazeny přímo do Rozhodnutí Evropského parlamentu a Rady 1313/2013/EU,
- vytváří další podpůrná opatření v oblasti prevence, připravenosti a odezvy (například rozšíření opatření v oblasti odborné přípravy, vytvoření plánovacího rámce pro operace odezvy na katastrofy, zavedení možnosti dočasného předběžného umístění kapacit pro odezvu ve výjimečných situacích zvýšeného rizika v členských státech, podpora rozvoje doplňkových kapacit financovaných z prostředků mechanismu civilní ochrany Unie, atd.).

Kybernetická bezpečnost

Dnem 1. ledna 2009 vstoupila v platnost směrnice Rady 2008/114/ES, o určování a označování evropských kritických infrastruktur a posuzování potřeby zvýšit jejich ochranu. Implementace

členskými státy EU měla proběhnout do 12. ledna 2011. Řešení tohoto úkolu bylo v zásadě možné dvěma způsoby – buď přijetím samostatného zákona o kritické infrastruktuře, nebo zapracováním této problematiky do jiného právního předpisu. V podmínkách ČR byla implementace směrnice vyřešena cestou novelizace krizového zákona a novelizace nařízení vlády č. 462/2000 Sb.

Dnem 1. ledna 2011 současně nabylo účinnosti nové nařízení vlády č. 432/2010 Sb., o kritériích pro určení prvku KI. Tím byla problematika KI zapracována do českého právního a vytvořeny podmínky pro její řešení na národní úrovni. Po přijetí zákona o kybernetické bezpečnosti a prováděcích právních předpisů k němu bylo nutné novelizovat odvětvová kritéria pro určování prvků KI, zejména v odvětví komunikačních a informačních systémů.

Dne 1. ledna 2015 nabyl účinnosti zákon o kybernetické bezpečnosti [16], který upravuje práva a povinnosti osob a působnost a pravomoci orgánů veřejné moci v této oblasti. Jedná se o první právní předpis, který v ČR tuto problematiku reguluje. Ústředním správním úřadem, do jehož působnosti oblast kybernetické bezpečnosti spadá, je Národní bezpečností úřad (dále NBÚ″), který je také gestorem uvedeného zákona. Zákon vymezuje základní pojmy, jako jsou kybernetický prostor, kritická informační infrastruktura nebo významný informační systém, dále definuje systém zajištění kybernetické bezpečnosti, kdy se bezpečnostním opatřením rozumí souhrn úkonů, jejichž cílem je zajištění bezpečnosti informací v informačních systémech a dostupnosti a spolehlivosti služeb a sítí elektronických komunikací v kybernetickém prostoru.

Z hlediska krizového řízení respektive, KI, je zásadní vazba zákona o kybernetické bezpečnosti a krizového zákona. Zákon o kybernetické bezpečnosti vymezuje kritickou informační infrastrukturu jako prvek nebo systém prvků KI v odvětví komunikační a informační systémy (oblast kybernetické bezpečnosti). Kritická informační infrastruktura je tedy součástí KI vymezené podle krizového zákona. Prvek kritické informační infrastruktury musí splňovat průřezová a odvětvová kritéria (odvětví VI. Komunikační a informační systémy/G. Oblast kybernetické bezpečnosti) v souladu s nařízením vlády o kritériích pro určení prvku KI. Prvky kritické informační infrastruktury jsou pak určovány postupem stanoveným v krizovém zákoně. NBÚ (jako ústřední správní úřad) zasílá MV návrh prvků KI v odvětví komunikační a informační systémy v oblasti kybernetické bezpečnosti, jejichž provozovatelem je OSS. MV po obdržení seznamu prvků tyto zařadí do celkového seznamu všech státních prvků KI, který je předkládán vládě ke schválení (formou usnesení vlády). Prvky kritické informační infrastruktury, jejichž provozovatelem není OSS, určuje NBÚ formou opatření obecné povahy.

Vedle prvků kritické informační infrastruktury definuje zákon o kybernetické bezpečnosti tzv. významné informační systémy, kterými jsou informační systémy spravované orgánem veřejné moci, které nejsou kritickou informační infrastrukturou a u kterých narušení bezpečnosti informací může omezit nebo výrazně ohrozit výkon působnosti orgánu veřejné moci. Významné informační systémy tedy nespadají do působnosti krizového zákona, ale řídí se vedle zákona o kybernetické bezpečnosti vyhláškou o významných informačních systémech a jejich určujících kritériích. Jedná se o samostatnou množinu informačních sytému, která je na kritické informační infrastruktuře nezávislá.

V závěru hodiny bude provedeno shrnutí, zopakována probraná témata s důrazem na problematiku bezpečnosti, krizového řízení a odpovězeny případné dotazy.

Úkoly na samostudium:

- znát co jsou základními registry veřejné správy;
- studium literatury;
- prohloubení informací získaných na hodině;
- vybraní studenti si připraví seminární práci na zadané téma.

Na závěr bude studentům dán prostor na dotazy týkající se úkolů na samostudium a celkového probraného tématu.