

Fyzická bezpečnost

Druhy zajištění ochrany utajovaných informací (OUI)

Ing. Oldřich Luňáček, Ph.D.

oldrich.lunacek@unob.cz

Operační program Vzdělávání pro konkurenceschopnost
Projekt: *Vzdělávání pro bezpečnostní systém státu*
(reg. č.: CZ.1.01/2.2.00/15.0070)



INVESTICE DO ROZVOJE VZDĚLÁVÁNÍ

Druhy zajištění ochrany informací

Osnova

1. Základní pojmy
2. Personální bezpečnost (PB)
3. Průmyslová bezpečnost (PrB)
4. Administrativní bezpečnost (AB)
5. Fyzická bezpečnost (FB)
6. Bezpečnost informačních nebo komunikačních systémů(BIKS)
7. Kryptografická ochrana (KO)



Základní pojmy

Utajované informace		Neutajované informace	
Přísně tajné	Chráněné dle zák. č. 412/2005 Sb.	Neklasifikované veřejně přístupné informace	Nepodléhají ochraně
Tajné	Chráněné dle zák. č. 412/2005 Sb.	Skutečnosti na které se vztahuje povinnost mlčenlivosti	Daně, trestní řízení apod.
Důvěrné	Chráněné dle zák. č. 412/2005 Sb.	Osobní údaje	Chráněné dle zák. č. 101/2000 Sb.
Vyhrazené	Chráněné dle zák. č. 412/2005 Sb.	Zvláštní skutečnosti	Chráněné dle zák. č. 240/2000 Sb.,

Druhy informací

- **Osobním údajem** je jakákoliv informace týkající se určeného nebo určitelného subjektu údajů.
- **Subjekt údajů** se považuje za určený nebo určitelný, jestliže lze subjekt údajů přímo či nepřímo identifikovat zejména na základě:
 - čísla,
 - kódu nebo jednoho či více prvků, specifických pro jeho:



Druhy informací

- ***Citlivým údajem je:***

- osobní údaj vypovídající o:

- národnostním,
- rasovém nebo etnickém původu,
- politických postojích,
- členství v odborových organizacích,
- náboženství a filozofickém přesvědčení,
- odsouzení za trestný čin,
- zdravotním stavu a sexuálním životě subjektu údajů a genetický údaj subjektu údajů;
- citlivým údajem je také biometrický údaj, který umožňuje přímou identifikaci nebo autentizaci subjektu údajů.

- ***Anonymním údajem je***

- takový údaj, který buď v původním tvaru, nebo po provedeném zpracování nelze vztáhnout k určenému nebo určitelnému subjektu údajů.



Druhy informací

Zpracováním osobních údajů se rozumí zejména:

- shromažďování,
- ukládání na nosiče informací,
- zpřístupňování,
- úprava nebo pozměňování,
- vyhledávání,
- používání,
- předávání,
- šíření,
- zveřejňování,
- uchovávání,
- výměna,
- třídění nebo kombinování,
- blokování a
- likvidace.



Druhy informací

Citlivé údaje je možné zpracovávat, jen jestliže

- **subjekt údajů dal ke zpracování výslovný souhlas,**
- je to **nezbytné v zájmu zachování života nebo zdraví subjektu údajů** nebo jiné osoby nebo odvrácení bezprostředního závažného nebezpečí hrozícího jejich majetku,
- se jedná o **zpracování při poskytování zdravotních služeb**, ochrany veřejného zdraví, zdravotního pojištění a výkon státní správy v oblasti zdravotnictví
- je zpracování **nezbytné pro dodržení** povinností a práv správce odpovědného za zpracování v oblasti **pracovního práva a zaměstnanosti**,
- jde o zpracování, které sleduje politické, filosofické, náboženské nebo odborové cíle, prováděné v rámci oprávněné činnosti občanského sdružení, nadace nebo jiné právnické osoby nevýdělečné povahy



Druhy informací

Citlivé údaje je možné zpracovávat, jen jestliže

- se jedná o údaje podle zvláštního zákona nezbytné pro provádění nemocenského pojištění, důchodového pojištění (zabezpečení), státní sociální podpory a dalších státních sociálních dávek, sociálních služeb, sociální péče, pomoci v hmotné nouzi a sociálně-právní ochrany dětí,
- se zpracování týká osobních údajů zveřejněných subjektem údajů,
- je zpracování nezbytné pro zajištění a uplatnění právních nároků,
- jsou zpracovány výlučně pro účely archivnictví podle zvláštního zákona, nebo
- se jedná o zpracování podle zvláštních zákonů při předcházení, vyhledávání, odhalování trestné činnosti, stíhání trestných činů a pátrání po osobách.



Druhy informací

- **Zvláštními skutečnostmi** se rozumí údaje z oblasti krizového řízení, které by v případě zneužití mohly vést:
 - k znemožnění nebo omezení činnosti orgánu krizového řízení,
 - k ohrožení:
 - života a zdraví osob,
 - majetku,
 - životního prostředí nebo podnikatelského zájmu právnické osoby nebo fyzické osoby vykonávající podnikatelskou nebo jinou obdobnou činnost pokud tyto údaje nejsou utajovanými informacemi.
- Pracovníci oprávnění se seznamovat se zvláštními skutečnostmi musí být zapsáni ve zvláštním seznamu, který schvaluje vedoucí orgánu krizového řízení. Musí zachovávat mlčenlivost.



Druhy informací

- **Utajovanou informací (UI) se rozumí informace**
 - **v jakékoliv podobě.**
 - **zaznamenaná na jakémkoliv nosiči.**
 - **označená v souladu se zákonem 412/2005 Sb.,**
 - **jejíž vyzrazení nebo zneužití může způsobit újmu zájmu České republiky (ČR) nebo může být pro tento zájem nevýhodné,**
 - **je uvedena v seznamu utajovaných informací (SUI).**

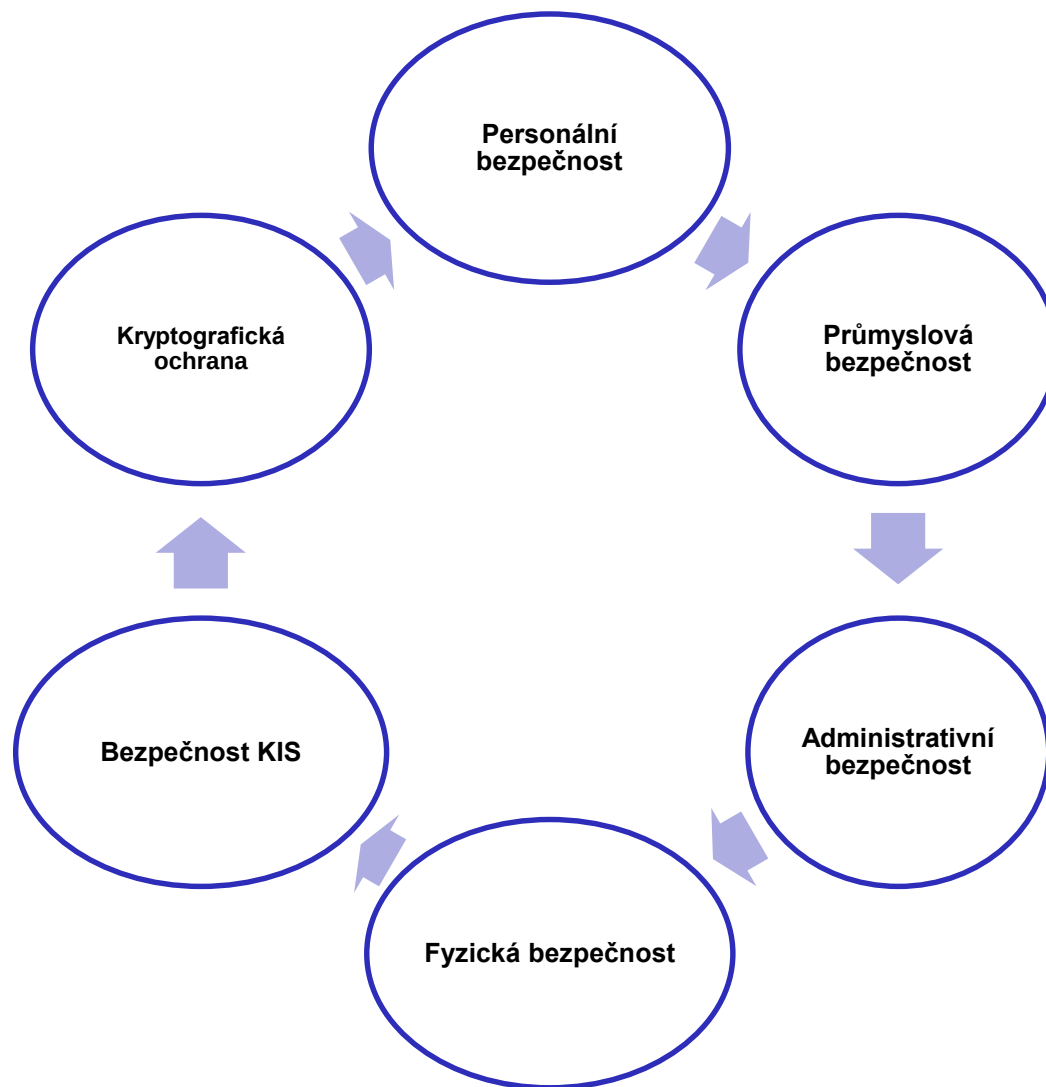
Stupně utajení **PT, T, D a V**



Základní pojmy OUI utajovaná informace (UI)

- klasifikuje se stupněm utajení
 - **Přísně Tajné** (PT), jestliže její vyzrazení neoprávněné osobě nebo zneužití může způsobit mimořádně vážnou újmu zájmům ČR,
 - **Tajné** (T), jestliže její vyzrazení neoprávněné osobě nebo zneužití může způsobit vážnou újmu zájmům ČR,
 - **Důvěrné** (D), jestliže její vyzrazení neoprávněné osobě nebo zneužití může způsobit prostou újmu zájmům ČR,
 - **Vyhrazené** (V), jestliže její vyzrazení neoprávněné osobě nebo zneužití může být nevýhodné pro zájmy ČR.

Druhy zajištění OUI



Personální bezpečnost

- výběr fyzických osob, které mají mít přístup k UI,
- ověřování podmínek pro jejich přístup k UI,
- jejich výchova a ochrana.

Personální bezpečnost „Vyhrazené“

Fyzické osobě lze umožnit přístup k UI stupně utajení „V“ :

- nezbytně potřebuje k výkonu své funkce, pracovní nebo jiné činnosti;
- je držitelem:
 - Oznámení o splnění podmínek pro přístup k UI stupně utajení „V“, nebo
 - Osvědčení fyzické osoby nebo
 - Dokladu.
- je poučena.



Personální bezpečnost- „Vyhrazené“

- Oznámení se vydá fyzické osobě, která:
 - je způsobilá k právním úkonům v plném rozsahu,
 - dosáhla alespoň 18 let věku,
 - je bezúhonná.
- Splnění podmínek ověřuje a oznámení fyzické osobě vydává ten, kdo je vůči ní:
 - odpovědnou osobou v rámci služebního poměru nebo pracovněprávního, či obdobného vztahu, nebo
 - odpovědnou osobou určená osoba.



Personální bezpečnost „Vyhrazené“

- Podmínka způsobilosti k právním úkonům se prokazuje prohlášením fyzické osoby o způsobilosti k právním úkonům.
- Podmínka věku se prokazuje občanským průkazem nebo cestovním dokladem fyzické osoby.
- Podmínka bezúhonnosti se prokazuje výpisem z evidence Rejstříku trestů :
 - osoba nesmí být pravomocně odsouzena za spáchání úmyslného trestného činu nebo
 - trestného činu vztahujícího se k ochraně UI, pokud se na ni nehledí, jako by odsouzena nebyla.

Doklady k ověření bezúhonnosti nesmějí být starší než 3 měsíce od jejich vydání.



Personální bezpečnost- „Vyhrazené“

- Poučení provede před prvním přístupem k UI stupně „V“ ten, kdo je vůči fyzické osobě v rámci služebního poměru nebo pracovněprávního, členského či obdobného vztahu osobou odpovědnou.
- Kontrola podmínek pro Oznámení - kdo vydal oznámení, je povinen každých 5 let ode dne jeho vydání ověřovat splnění podmínek



Personální bezpečnost – PT, T, D

- Fyzické osobě lze umožnit přístup k UI stupně utajení PT, T, D jestliže:
 - jej nezbytně potřebuje k výkonu své funkce, pracovní nebo jiné činnosti,
 - je držitelem platného osvědčení fyzické osoby příslušného stupně utajení,
 - je poučena.
- Před prvním přístupem k UI stupně utajení PT, T, D - ten, kdo je vůči fyzické osobě v rámci služebního poměru nebo pracovněprávního, členského či obdobného vztahu osobou odpovědnou, zajistí její poučení.

Personální bezpečnost

Přísně tajné, Tajné, Důvěrné

- NBÚ vydá Osvědčení fyzické osoby (OFO) fyzické osobě, která:
 - je státním občanem ČR nebo státním občanem členského státu EU, nebo NATO,
 - bezúhonná,
 - způsobilá k právním úkonům,
 - 18 let věku,
 - je osobnostně způsobilá,
 - je bezpečnostně spolehlivá.



Personální bezpečnost – PT, T, D

Osobnostní způsobilost:

- osoba netrpí poruchou či obtížemi, které mohou mít vliv na její spolehlivost nebo schopnost utajovat informace,
- se ověřuje na základě prohlášení k osobnostní způsobilosti a v případech stanovených zákonem i na základě znaleckého posudku o osobnostní způsobilosti.

Bezpečnostní spolehlivost:

- u osoby není zjištěno bezpečnostní riziko, za které lze považovat:
 - závažná nebo opakovaná činnost proti zájmům ČR, nebo
 - činnost, spočívající v potlačování základních práv a svobod, anebo podpora takové činnosti.



Personální bezpečnost

Bezpečnostní způsobilost

- týká se citlivých oblastí z hlediska zájmu státu
- zaměřuje se na oblast:
 - mírové využití jaderné energie
 - obchod se vojenským materiálem
 - problematika báňského zákona
- oprávněné osoby jsou držiteli – DOKLAD
- platnost tohoto dokumentu je 5 let



Průmyslová bezpečnost

- tvoří systém opatření k zjišťování a ověřování podmínek pro přístup podnikatele k UI a k zajištění nakládání s UI u podnikatele
- podnikateli lze umožnit přístup k UI jestliže:
 - jej nezbytně potřebuje k výkonu své činnosti a
 - je držitelem platného osvědčení podnikatele příslušného stupně utajení.



Průmyslová bezpečnost

- Podmínky pro vydání osvědčení podnikatele:
 - je ekonomicky stabilní,
 - je bezpečnostně spolehlivý,
 - je schopen zabezpečit ochranu UI a
 - pokud odpovědná osoba a prokuristé jsou držiteli platného OFO nejméně pro takový stupeň utajení, pro který žádá podnikatel o vydání osvědčení podnikatele, nebo jsou držiteli platného oznámení v případě, že má být vydáno osvědčení podnikatele pro stupeň utajení Vyhrazené.



Administrativní bezpečnost

System opatření při:

- tvorbě,
- příjmu,
- evidenci,
- zpracování,
- odesílání,
- přepravě,
- přenášení,
- ukládání,
- skartačním řízení,
- archivaci,
- případně jiném nakládání s UI.



Administrativní bezpečnost

- Na UI je původce povinen vyznačit:
 - svůj název,
 - stupeň jejího utajení,
 - její evidenční označení,
 - datum jejího vzniku, není-li dále stanoveno jinak.
- UI se eviduje v administrativních pomůckách, kde se rovněž zaznamenává předávání, přebírání nebo jiný pohyb UI.



Administrativní bezpečnost

- **Opis, kopie nebo překlad UI** stupně utajení PT nebo výpis z ní mohou být vyhotoveny pouze na základě **písemného souhlasu původce**
- Jde-li o UI stupně utajení T, D mohou být vyhotoveny pouze s **písemným souhlasem přímo nadřízené osoby.**

Administrativní bezpečnost

- UI lze přepravovat nebo přenášet pouze:
 - v **přenosných schránkách** nebo v **uzavřeném obalu** v závislosti na jejím stupni utajení a na jejím nosiči;
 - přepravovat ji lze pouze prostřednictvím **kurýrní služby** nebo držitele poštovní licence.



Administrativní bezpečnost

- UI lze v průběhu její skartační lhůty, **zapůjčit pouze fyzickým osobám**, které jsou k orgánu státu, právnické osobě nebo podnikající fyzické osobě ve služebním poměru nebo v pracovněprávním, členském či obdobném vztahu.
- Stupeň utajení se na UI vyznačí při jejím vzniku.



Administrativní bezpečnost

- **Vyznačení stupně utajení** na UI musí být zachováno po celou dobu trvání důvodů utajení. Bez souhlasu původce nebo poskytující cizí moci nesmí být stupeň utajení změněn nebo zrušen.
- Vyžaduje-li to charakter UI, musí původce vyznačit na UI dobu, po kterou bude informace utajována; stupeň utajení zaniká uplynutím vyznačené doby.
- **Stupeň utajení původce neprodleně zruší nebo změní po zjištění, že pominul důvod** pro utajení informace, důvody pro utajení neodpovídají stanovenému stupni utajení nebo byl-li stupeň utajení stanoven neoprávněně, a na UI toto zrušení nebo změnu jejího stupně utajení vyznačí.

Administrativní bezpečnost

- Původce je povinen prověřit, zda důvod pro utajení informace trvá, a to nejméně **jednou za 5 let** ode dne jejího vzniku.
- Provedl-li původce zrušení nebo změnu stupně utajení oznámí tuto skutečnost neprodleně písemně adresátům UI.
- Adresáti UI oznámí neprodleně písemně tuto skutečnost všem dalším adresátům, kterým utajovanou informaci zpřístupnili.
- Adresát po obdržení oznámení na UI zrušení nebo změnu stupně utajení vyznačí.



Administrativní bezpečnost

- u organizačních celků (OC) sehrává důležitou roli pracoviště ochrany informací (POI)
- u některých OC se můžeme setkat s registry (informace cizí moci)
- administrativní pomůcky za účelem vedení evidence:
 - jednacích protokol
 - doručovací kniha
 - manipulační kniha



Fyzická bezpečnost (FB)

- FB tvoří systém opatření která mají neoprávněné osobě:
 - zabránit nebo ztížit přístup k UI,
 - popřípadě přístup nebo pokus o něj zaznamenat

Fyzická bezpečnost

Pro zabezpečení OUI se v rámci fyzické bezpečnosti určují:

- objekty,
- zabezpečené oblasti (ZO)
- jednacích oblasti (JO)



Fyzická bezpečnost

- Objektem je ohraničený prostor, ve kterém se nachází zabezpečená oblast nebo jednací oblast, zde se UI zpracovávají.
- Zabezpečenou oblastí (ZO) - je ohraničený prostor v objektu, zde se UI ukládají.
- Jednací oblastí (JO) je ohraničený prostor v objektu, zde se UI pravidelně projednávají
 - UI stupně utajení PT nebo T lze pravidelně projednávat pouze v jednací oblasti.

Fyzická bezpečnost

UI se zpracovává:

- v ZO,
- v objektu mimo ZO, pokud je zajištěno, že k UI nemá přístup neoprávněná osoba, nebo
- v odůvodněných případech s písemným souhlasem odpovědné osoby nebo bezpečnostního ředitele mimo objekt, pokud je zajištěno, že k UI nemá přístup neoprávněná osoba.
- UI se ukládá v ZO a v ní popřípadě v úschovném objektu, trezoru, zamykatelné skříni nebo jiné schránce.

Fyzická bezpečnost

Kategorie zabezpečených oblastí:

- Přísně Tajné,
- Tajné,
- Důvěrné,
- Vyhrazené.

ZO se podle možnosti přístupu k UI zařazují do tříd:

- třída I, kdy **vstupem** do této oblasti **dochází k seznámení s UI**,
- třída II, kdy **vstupem** do této oblasti **nedochází k seznámení s UI**.



Fyzická bezpečnost

Opatřeními FB jsou:

- ostraha,
- režimová opatření,
- technické prostředky.



Fyzická bezpečnost

PFB v případech, kdy se v objektu nachází ZO kategorie V obsahuje:	určení objektu a ZO, včetně jejich hranic a určení kategorií a tříd ZO,	způsob použití opatření fyzické bezpečnosti,
PFB objektu kategorie „V“ bez ZO obsahuje:	určení objektu včetně jeho hranic.	

PFB - Projekt fyzické bezpečnosti



INVESTICE DO ROZVOJE VZDĚLÁVÁNÍ

Fyzická bezpečnost

PFB kdy se v objektu nacházejí ZO kategorie PT, T, D obsahuje:	určení objektu a ZO, včetně jejich hranic a určení kategorií a tříd ZO	vyhodnocení rizik,	způsob použití opatření fyzické bezpečnosti,	provozní řád objektu	plán zabezpečení objektu a ZO v krizových situacích.
PFB objektu kategorie PT, T, D bez ZO nebo JO obsahuje:	určení objektu včetně jeho hranic,		způsob použití opatření fyzické bezpečnosti,	provozní řád objektu	plán zabezpečení objektu v krizových situacích.

Bezpečnost IKS

- tvoří systém opatření, jejichž cílem je zajistit:
 - důvěrnost,
 - integritu a
 - dostupnost UI s nimiž tyto systémy nakládají, a
 - odpovědnost správy a uživatele za jejich činnost v IKS



Bezpečnost IKS

IS nakládající s UI se rozumí:

- 1 nebo více počítačů,
- programové vybavení,
- periferní zařízení,
- správa tohoto IS a
- k tomuto systému se vztahující procesy nebo prostředky schopné provádět sběr, tvorbu, zpracování, ukládání, zobrazení nebo přenos UI

Bezpečnost IKS

- IS systém musí být certifikován NBÚ a písemně schválen do provozu odpovědnou osobou.
- Nakládat s UI lze pouze v IS, který je certifikován.



Bezpečnost IKS

KS nakládajícím s UI se rozumí systém zajišťující přenos těchto informací mezi koncovými uživateli a zahrnující:

- koncové komunikační zařízení,
- přenosové prostředí,
- kryptografické prostředky,
- obsluhu a
- provozní podmínky a postupy.



Bezpečnost IKS

- KS nelze provozovat bez projektu bezpečnosti KS schváleného NBÚ.
- O schválení projektu bezpečnosti KS písemně žádá u NBÚ orgán státu, právnická osoba nebo podnikající fyzická osoba, která jej bude provozovat.



Bezpečnost IKS

Projekt bezpečnosti KS obsahuje:

- bezpečnostní politiku KS ,
- organizační a provozní postupy provozování KS,
- provozní směrnice pro bezpečnostní správu KS,
- provozní směrnice uživatele KS.



Kryptografická ochrana

- tvoří systém opatření na ochranu UI použitím kryptografických metod a kryptografických materiálů při:
 - zpracování,
 - přenosu nebo
 - ukládání UI.

Kryptografická ochrana

- Kryptografickým materiálem je:
 - **kryptografický prostředek,**
 - je hardwarový nebo softwarový produkt určený ke kryptografické ochraně.
 - musí být certifikován NBÚ.
 - **materiál k zajištění funkce kryptografického prostředku,**
 - je klíčový materiál a heslový materiál pro kryptografickou operaci.
 - **klíčový materiál je** kryptografický klíč na nosiči
 - **kryptografický klíč je** utajovaný proměnný parametr nezbytný k jednoznačnému zašifrování a odšifrování dat.
 - **heslový materiál je** utajovaný znakový řetězec na nosiči, ze kterého je odvozován kryptografický klíč nebo který je použit k autentizaci.
 - **kryptografický dokument**
 - je listina nebo jiný nosič informací obsahující UI kryptografické ochrany.



Kryptografická ochrana

- Kryptografické pracoviště:
 - pracoviště určené k výrobě nebo testování klíčových materiálů,
 - ukládání kryptografického materiálu nebo
 - k distribuci a evidenci kryptografického materiálu.
- Kryptografické pracoviště musí splňovat bezpečnostní standardy a musí být do provozu schváleno odpovědnou osobou.



Literatura

- Zákon 412/2005 Sb. o ochraně utajovaných informací a o bezpečnostní způsobilosti
- POŽÁR, J.: Informační bezpečnost. Vydavatelství a nakladatelství Aleš Čeněk,s.r.o.. Plzeň 2005.
- Dokument NATO C-M(2002)49 Security within NATO. 2002.
- RODRYČOVÁ, J., STAŠA, P.: Bezpečnost informací jako podmínka prosperity firmy. Grada, Praha 2000.



Literatura

- Zákon č. 412/2005 Sb., o ochraně utajovaných informací a bezpečnostní způsobilosti (aktuálně novelizováno Zákonem 255/2011Sb.)
- Nařízení vlády č. 522/2005 Sb., kterým se stanoví SUI, ve znění nařízení vlády č. 240/2008 Sb.
- Vyhláška č. 523/2005 Sb., o bezpečnosti informačních a komunikačních systémů (IKS) a dalších elektronických zařízení nakládajících s utajovanými informacemi a o certifikaci stínicích komor, ve znění vyhlášky č. 453/2011 Sb.
- Vyhláška č. 432/2011 Sb., o zajištění KOUI.
- Vyhláška č. 525/2005 Sb. o provádění certifikace při zabezpečování KOUI, ve znění vyhlášky č. 434/2011 Sb.
- Vyhláška č. 405/2011 Sb., o průmyslové bezpečnosti
- Vyhláška č. 363/2011 Sb., o personální bezpečnosti a o bezpečnostní způsobilosti
- Vyhláška č. 528/2005 Sb., o fyzické bezpečnosti a certifikaci technických prostředků, ve znění vyhlášky č. 19/2008 Sb. a vyhlášky č. 454/2011 Sb.
- Vyhláška č. 529/2005 Sb., o administrativní bezpečnosti a o registrech utajovaných informací, ve znění vyhlášky č. 55/2008 Sb. a vyhlášky č. 433/2011 Sb.



Literatura

- RMO 18 2006 Vytvoření a vedení Seznamu zvlášť určených zařízení nebo pracovišť rezortu Ministerstva obrany, změněn RMO44/2010, RMO 16/2012,
- RMO 25 2007 Stanovení stupňů utajení některých informací v rezortu Ministerstva obrany
- RMO 6 2010 Zřízení Rady pro kybernetickou obranu Ministerstva obrany, změněn RMO 14/2011, 86/2013, RMO 50/2014,

Literatura

- RMO 11 2010 Spisový řád rezortu Ministerstva obrany, změněn RMO 42/2010, 17/2013, 121/2013 (bude novelizován)
- RMO 33 2012 o personální bezpečnosti
- RMO 14 2013 Ochrana utajovaných informací v rezortu Ministerstva obrany
- RMO 16 2013 o ochraně určených neutajovaných informací v rezortu Ministerstva obrany, změněn RMO 73/2014

Literatura

- NVMO 12 2010 Spisová služba, změněn NV 61/2012, 84/2013
- NVMO 60 2012 Administrativní bezpečnost v rezortu Ministerstva obrany, změněn NV 35/2014
- NVMO 18 2013 Ochrana utajovaných informací poskytovaných podnikatelům
- NV MO 20 2013 Bezpečnost informačních a komunikačních systémů a elektronických zařízení, které nakládají s určenými neutajovanými informacemi v rezortu Ministerstva obrany, změněn NV 15/2014

Literatura

- NV MO 39 2013 Ochrana utajovaných informací před jejich únikem vlivem kompromitujícího vyzařování, změněn NV 84/14
- NV MO 77 2013 Fyzická bezpečnost v rezortu Ministerstva obrany
- NV MO 85 2013 Bezpečnost informačních a komunikačních systémů a elektronických zařízení nakládajících s utajovanými informacemi v rezortu Ministerstva obrany
- NV MO 111 2013 Kryptografická ochrana utajovaných informací v rezortu Ministerstva obrany