



Bezpečnostní management organizace



ÚVOD

Lidské zdroje:

- jsou nejcitlivějším místem každé organizace,
- jsou základním kamenem organizace,
- je nutné je kvalifikovaně řídit, a to jak ve smyslu získávání, tak formování,
- rozvíjet jejich pracovní schopnosti,
- zvyšovat kvalifikaci,
- vrcholové vedení organizace ovlivňuje styl řízení organizace a tím ovlivňuje celou organizaci.



ÚVOD

- Všechny úrovně vedení:
 - vycházejí z přidělených úkolů,
 - musí konkrétně zvažovat:
 - kolik pracovníků a
 - jací pracovníci budou ke splnění úkolů v jejich úseku zapotřebí.
- Management musí mít přehled o:
 - stavu,
 - pohybu a
 - využívání pracovníků.
- Vedoucí pracovníci na nejnižší úrovni:
 - bezprostředně plní rozhodující pracovní úkoly,
 - jsou klíčovým prvkem, protože na jejich úrovni pracovní úkoly nabývají konkrétnosti nejvyšší.



Management

Definujeme jako:

- **řízení** (označení funkce),
- **řídící pracovníky**, (skupina lidí vykonávající manažerské funkce),
- **vědní disciplínu**,
- **předmět studia**.



Management

- definujeme také jako **proces**, který charakterizuje management ve vztahu k používání manažerských funkcí tj.:
 - **plánování**, které zahrnuje stanovení cílů a prostředků k jejich dosažení;
 - **organizování**, které znamená uspořádání prvků a vztahů v soustavě;
 - **personalistika**, která znamená obsazování pozic v organizační struktuře nejschopnějšími lidmi;
 - **vedení lidí**, jež znamená schopnost vést, usměrňovat, motivovat a stimulovat;
 - **kontrola**, která zjišťuje skutečný stav a porovnává ho s plánovaným cílem.



Management

• Integrované řízení bezpečnosti organizace je:

- způsob řízení bezpečnosti, který je zaměřen na zajištění:
 - úplnosti,
 - vyváženosti a
 - provázanosti bezpečnostních protopatření.
- charakterizováno následujícími znaky:
 - protopatření pokrývají všechny významné hrozby (úplnost);
 - neexistují podceňovaná nebo přeceňovaná protopatření (vyváženost);
 - protopatření jsou posuzována ve vzájemných souvislostech (provázanost).



Management

- **Řídící pracovníci** v oblasti bezpečnosti:
 - jsou **přímo odpovědní** za splnění požadavků kladených na tuto oblast;
 - jejich činnost by neměla být omezována jen na činnost exekutivní a kontrolní, ale měli by sehrávat významnou roli v oblasti **preventivní a poradenskou** vůči pracovníkům organizace.
 - v současné době je bezpečnost organizace řízena lidmi, kteří jsou do funkcí v bezpečnostním managementu jmenováni svými nadřízenými.
 - s výjimkou kryptografické ochrany není stanovena podmínka odborné způsobilosti





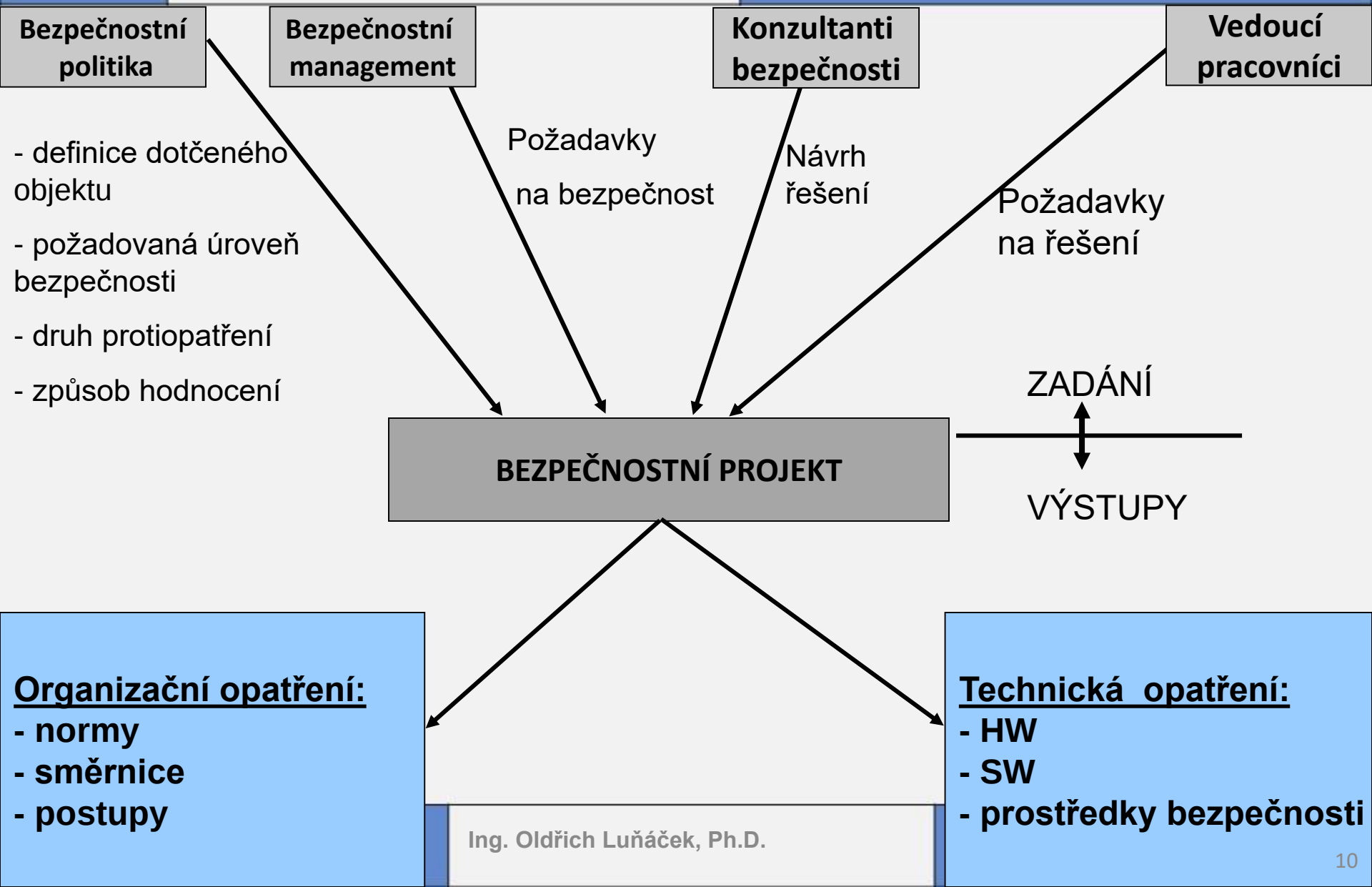
Management

- **Cíl organizace** - integrované řízení bezpečnosti organizace pro ochranu aktiv organizace.
- **Místo v organizaci** – „bezpečnostní“ útvar je samostatný útvar podléhající nejvyššímu vedení organizace.
- Existence bezpečnostního managementu - **definování místa bezpečnostního managementu ve své struktuře organizace.**
 - stanovení **struktury** bezpečnostního managementu;
 - definování **odpovědností** jednotlivých rolí;
 - definování požadavků pro výkon jednotlivých rolí;
 - definování **požadavků na vzdělávání** bezpečnostního managementu organizací.



Management

- **Podřízenost bezpečnostního managementu** - vedoucímu organizace
- **Oblasti odpovědnosti** bezpečnostního managementu:
 - administrativní bezpečnost,
 - fyzická bezpečnost,
 - bezpečnost IKS,
 - kryptografická ochrana,
 - personální bezpečnost,
 - průmyslová bezpečnost.
- **Vykonávané činnosti:**
 - exekutivní,
 - kontrolní,
 - poradenská a
 - analytická.





Úřad pro ochranu osobních údajů (ÚOOÚ) změna k 25.5.2018

- je nezávislým orgánem,
- provádí dozor nad dodržováním zákonem stanovených povinností při zpracování osobních údajů,
- vede registr povolených zpracování osobních údajů,
- přijímá podněty a stížnosti občanů na porušení zákona,
- poskytuje konzultace v oblasti ochrany osobních údajů.



Úřad pro ochranu osobních údajů (ÚOOÚ)

- Zákonem se chráněno občan před **neoprávněným zasahováním do jeho soukromého a osobního života a neoprávněným shromažďováním, zveřejňováním nebo jiným zneužíváním osobních údajů.**
- V současné společnosti je vlivem rozvoje informačních technologií toto právo stále více narušováno.



NBÚ

(Národní bezpečnostní úřad)

- je nejvyšší **bezpečnostní autoritou** v oblasti ochrany utajovaných informací (OUI),
- je zřízen jako ústřední správní úřad pro oblast ochrany utajovaných informací (UI),
- v jeho čele NBÚ je **ředitel**, který je jmenován a odvoláván po projednání ve výboru Poslanecké sněmovny,
- **předseda vlády** je služebně nadřízen řediteli NBÚ a vykonává dohled nad činností NBÚ.



NBÚ plní tyto hlavní úkoly:

- zpracovává **konceptci rozvoje** a zajišťuje jednotné provádění OUI;
- vede **ústřední registry** UI v rámci mezinárodních styků;
- povoluje poskytování UI v rámci **mezinárodních styků**;
- připravuje **vládní návrhy zákonů a prováděcích předpisů**;
- zabezpečuje úkoly související se **sjednáváním a plněním mezinárodních smluv**;



NBÚ plní v OUI tyto hlavní úkoly

- stanovuje **pravidla zavádění a používání prostředků a systémů** určených k OUI;
- plní úkoly v oblasti **průmyslového vlastnictví**;
- vykonává **státní dozor a metodickou činnost**;
- zajišťuje a provádí **bezpečnostní prověrky fyzických osob a organizací**;
- provádí nebo zajišťuje **certifikaci technických prostředků**,



NÚKIB

(národní úřad pro kybernetickou a informační bezpečnost)

- je nejvyšší **bezpečnostní autoritou** v oblasti bezpečnosti IS a KS a kryptografické ochrany



NÚKIB

- provádí **certifikace**:
 - IS,
 - kryptografického prostředku,
 - kryptografického pracoviště a
 - stínicí komory,
- pro oblast kryptografické ochrany:
 - zajišťuje:
 - výzkum,
 - vývoj a
 - výrobu národních kryptografických prostředků,
- vyvíjí a schvaluje:
 - národní šifrové algoritmy a
 - vytváří národní politiku kryptografické ochrany.



NÚKIB

- zabezpečuje rozvoj **kryptologie** a **řídí kryptologickou ochranu**;
- zajišťuje a koordinuje **kryptografický výzkum a vývoj**;
- provádí nebo zajišťuje **certifikaci IS** používaných k nakládání s UI a kryptografických prostředků.



Organizace (firma) OOÚ

- subjekt údajů – fyzická osoba , k níž se osobní údaje vztahují,
- správce osobních údajů – určuje účel a prostředky zpracování osobních údajů (na UO rektor –velitel),
- zpracovatel – každý subjekt který zpracovává údaje podle zákona na OOÚ,



Organizace (firma) OUI

- musí určit odpovědnou osobu (odpovědnost ze zákona)
- musí určit bezpečnostního ředitele
- musí určit bezpečnostní správu kryptografické ochrany



Resort MO

- **Úkolem resortu MO je zajištění obranyschopnosti a suverenity ČR.**
- **Závazky plynoucí z našeho členství v NATO, EU a v mezinárodních organizacích nás zavazují k dosažení a plnění bezpečnostních standardů existujících uvnitř těchto organizací.**



Resort MO

- Do popředí vystupuje **výběr** potřebné **kvality** personálu organizací a řízení v jednotlivých oblastech bezpečnosti.
- **Organizace bezpečnosti** je opět hierarchická.
- **Odpovědná osoba** – ministr obrany.



Resort MO

Odbor bezpečnosti (OB MO)

- je organizačním útvarem ministerstva pro plnění úkolů:
 - stanovených zákonem č. 412/2005 Sb. OUI a bezpečnostní způsobilost, a
 - zákonem č. 499/2004 Sb. (Zákon o archivnictví a spisové službě).
- V čele odboru bezpečnosti MO je **ředitel odboru**, který je přímo podřízen ministru obrany.



Resort MO

BŘ MO jako výkonný orgán ministra obrany
zabezpečuje splnění následujících úkolů v oblasti
OUI:

- realizace **systemových opatření** PB, AB, FB, BIKS, KO,
- písemné oznámení NBÚ o schválení uvedení IS do provozu do 30 dnů od tohoto schválení;



Resort MO

BŘ MO jako výkonný orgán ministra obrany zabezpečuje splnění následujících úkolů v oblasti OUI:

- **zabezpečení součinnosti** MO s NBÚ a ostatními orgány státní správy v oblasti OUI;
- **řízení KRYPTO a správy klíčového hospodářství** v rezortu MO;
- **metodické řízení** orgánů bezpečnostní správy OC a zpracovávání odborných vyjádření k problematice OUI v rezortu MO;
- **vyjadřování se ke způsobu OUI** v rámci veřejných zakázek;



Resort MO

BŘ MO jako výkonný orgán ministra obrany zabezpečuje splnění následujících úkolů v oblasti OUI:

- aplikace **právních předpisů** v podmínkách rezortu MO;
- zpracování **plánu kontrol** OUI v rezortu MO;
- zpracování **personálního projektu** rezortu MO;
- vedení přehledu o **projektech FB** v rezortu MO;
- vedení **přehledu oprávněných osob** v rezortu MO, žádostí o vydání OFO a OFO pro cizí moc;



Resort MO

BŘ MO jako výkonný orgán ministra obrany zabezpečuje splnění následujících úkolů v oblasti OUI:

- **schvalování projektů FB**, které se zpracovávají pro zabezpečenou oblast,
- provádění **odborných školení** pracovníků **KOUI**;
- koordinace **výroby, nákupu, přejímky a distribuci** klíčového materiálu pro provoz kryptografických prostředků resortu MO;
- realizace cílů **výstavby** v oblasti BIKS;





Resort MO

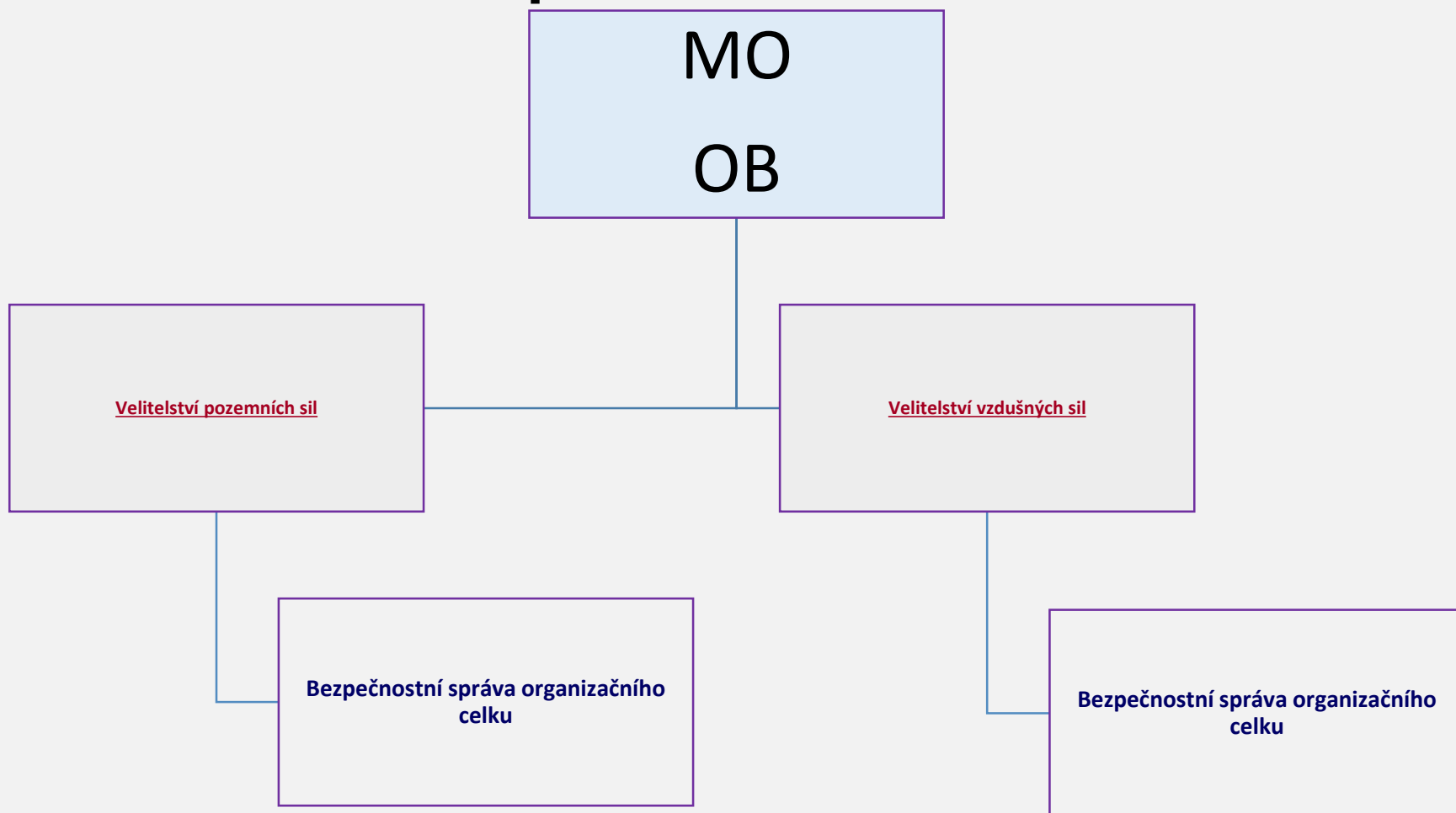
BŘ MO jako výkonný orgán ministra obrany zabezpečuje splnění následujících úkolů v oblasti OUI:

- **stanovení politiky a koncepce bezpečnosti KIS a KOUI v resortu MO;**
- **stanovení vnitřních předpisů a odborných instrukcí v oblasti BIKS a KOUI;**
- **stanovení zásad a norem pro certifikaci a akreditaci KIS a KOUI;**
- **kontrolování dodržování norem a zásad bezpečnosti KIS a KOUI v resortu MO.**





Struktura bezpečnosti v resortu MO





Organizační celek (OC)

Vedoucí organizačního celku (VOC):

- zajišťuje, aby v jednacích oblastech **nedocházelo k ohrožení nebo úniku projednávaných UI**;
- plní **povinnosti provozovatele** objektu;
- zajišťuje, aby **nedocházelo k nakládání s UI** v IKS, které neakreditoval vedoucí OC odpovědný za IKS;
- **schvaluje místní provozní bezpečnostní dokumentace** IKS;
- schvaluje **přístup uživatelů** do IKS;
- **pověřuje osoby k výkonu uživatelských funkcí** provozní obsluhy kryptografického prostředku;



Organizační celek (OC)

Vedoucí organizačního celku:

- **určuje pracovníka kryptografické ochrany** ke konkrétní činnosti BS KO;
- **pověřuje osobu, která doprovází kurýra KM;**
- **podepisuje administrativní pomůcky KO** při jejich autentizaci;
- **písemně povoluje přenášení a zapůjčování nosičů UI** stupně utajení T a PT;
- **jako původce UI povoluje zhotovení kopií, opisů a překladů** utajovaných dokumentů stupně utajení PT nebo výpisů z nich;
- **určuje při personální změně osoby pověřené vedením jednacího protokolu** minimálně **tříčlennou komisi k předání nosičů UI** a příslušných administrativních pomůcek.



Organizační celek (OC)

VOC je povinen:

- stanovit **BS OC** v čele s bezpečnostním manažerem (BM) OC a zajistit podmínky pro její výkon;
- pro **oblast BIKS určit zaměstnance** a obsadit role v místním systému BS IKS, který řídí;
- zabezpečit **zpracování bezpečnostních provozních směrnic pro zpracování UI** v elektronické podobě na elektronickém zařízení;
- zajistit **podmínky pro výkon KO**, manipulaci a hospodaření s KM a jeho přepravu;



Organizační celek (OC)

VOC je povinen:

- žádat BŘ MO o **vyškolení pracovníka KO** a o pověření tohoto pracovníka k výkonu KO;
- **ověřovat podmínky pro přístup fyzické osoby k UI „V“**,
- **vydávat oznámení** o splnění podmínek pro přístup k UI „V“ a
- **vydávat písemně oznámení** o jeho zániku;
- **zaslat BŘ MO žádost** o vydání souhlasného nebo nesouhlasného stanoviska k žádosti o vydání OFO, kterou fyzická osoba předkládá NBÚ;



Organizační celek (OC)

VOC je povinen:

- **poučit zaměstnance před prvním přístupem k UI.** (Poučení podepisuje zaměstnanec a vedoucí OC, který zaměstnance poučil).
- 1x ročně zabezpečit proškolení zaměstnance, který má přístup k UI, z právních předpisů v oblasti OUI. Záznam o účasti na proškolení uchovat u OC po dobu 3 let;
- 1x ročně zabezpečit zpracování personálního projektu za OC, který řídí;





Organizační celek (OC)

VOC je povinen:

- poučit odpovědné osoby, které jednají za podnikatele v rámci realizace veřejné zakázky, pokud tyto osoby nebyly již poučeny;
- **zabezpečit zpracování a uložení projektu FB;**
- **zabezpečit vedení přehledu systemizovaných míst a seznamu fyzických osob určených nebo poučených pro styk s UI a tento přehled schvalovat;**
- **poučit držitele uznání bezpečnostního oprávnění,** které vydal úřad cizí moci, a to tehdy, poskytuje-li mu UI a nebyl-li již poučen.



Bezpečnostní správa OC (BS OC)

- K plnění povinností v oblasti OUI vytváří VOC bezpečnostní správu (BS).
- BS OC vykonává povinnosti ve prospěch svého OC či jiného celku.



Bezpečnostní správa OC (BS OC)

- BS OC tvoří následující role:
 - bezpečnostní manažer organizačního celku;
 - bezpečnostní a provozní správa IS, KS a EZ;
 - bezpečnostní správa kryptografické ochrany;
 - registr nebo pomocný registr;
 - pracoviště ochrany informací (POI);
 - bezpečnostní pracovník pro personální bezpečnost;
 - správce technických prostředků.





Provozní a bezpečnostní správa IS, KS a EZ

- **provozní správa systému**
 - gestor systému;
 - manažer systému;
 - provozovatel systému;
 - správce systému;
 - místní správce systému



Provozní a bezpečnostní správa IS, KS a EZ

Projektová **bezpečnostní správa** systému se uplatňuje

- zejména ve fázích:
 - plánování,
 - vývoje,
 - testování,
 - implementace
- rozvoje systému a realizují ji tyto role:
 - bezpečnostní manažer systému;
 - bezpečnostní architekt systému.





Provozní a bezpečnostní správa IS, KS a EZ

Provozní bezpečnostní správu systému realizují role vystupující současně v rolích bezpečnostní správy organizačního celku:

- bezpečnostní správce systému;
- bezpečnostní správce kryptografické ochrany systému;
- místní bezpečnostní správce systému;
- místní bezpečnostní správce kryptografické ochrany systému;
- bezpečnostní správce terminálové oblasti systému.





Bezpečnostní správa KO (BS KO)

BS KO v resortu MO je tvořena:

- bezpečnostní správce kryptografické ochrany;
- správce kryptografického materiálu;
- zástupce správce kryptografického materiálu;
- bezpečnostní správce kryptografické ochrany systému;
- pracovník určený k vedení dokumentů KRYPTO;
- speciální obsluha kryptografického prostředku;
- kurýr určený k přepravě kryptografického materiálu;



Příprava bezpečnostního managementu

- Chce-li organizace efektivně pracovat, musí mít sestaven personální plán na obsazení jednotlivých míst.
- Každý je nahraditelný, na jednom člověku nemůže stát celá bezpečnost.
- Vrcholový management musí vidět bezpečnost jako jednu z hlavních priorit.
- Zkušenost pracovníků organizace bude posilovat ve vědomí pocit zodpovědnosti i za výsledek toho druhého.
- Vzdělávání pracovníků bezpečnostního managementu není nijak legislativně stanoveno.





Příprava bezpečnostního managementu

- Výjimkou je pouze oblast kryptografické ochrany utajovaných informací.
- Záleží na organizaci, co bude vyžadovat po bezpečnostním managementu za odborné vzdělání.
- Nezajištění, podcenění úlohy vzdělávání či nedostatečná podpora pro zdokonalování bezpečnostního managementu je pro organizaci kontraproduktivní.



Příprava bezpečnostního managementu

- Osoba přijímací nového pracovníka, by měla zjistit skutečný stav vědomostí, znalostí a zkušeností přijímaného pracovníka, zejména s poukázáním na silné a slabé stránky nového zaměstnance.
- Velmi účelné je, když se přijetím nového pracovníka zabývá jak **personalista**, tak **bezpečnostní manažer**.



Příprava bezpečnostního managementu

Příprava může být rozdělena na několik druhů:

- teoretická globální příprava, kdy dochází k seznámení s organizací, dochází také k seznámení s bezpečnostní globální dokumentací;
- teoretická příprava, týkající se organizace, dochází k seznámení s vnitřní strukturou organizace a vztahů mezi základními prvky a dále k seznámení s organizací bezpečnosti organizace, je objasněna bezpečnostní dokumentace organizace;



Příprava bezpečnostního managementu

- praktická příprava zaměřená na výkon na dané funkci, za použití trenažérů k nácviku reakcí a řešení skutečných problémů, seznámení s používanými technickými prostředky zajišťujícími bezpečnost;
- praktická příprava s lektorem, výkon funkce s pomocí lektora;
- samostatný výkon funkce;
- Délka jednotlivých fází se může velmi podstatně lišit.
- Záleží na schopnostech, dovednostech a také na motivaci nově příchozího zaměstnance.



Povinnosti při ochraně UI

Každý:

- Je povinen neprodleně odevzdat nalezenou UI nebo UI získanou v rozporu se Zákonem 412/2005 Sb. anebo Osvědčení (všechny druhy) NBÚ nebo Policii ČR,
- kdo měl nebo má přístup k UI, musí zachovávat o ní mlčenlivost a nesmí k ní umožnit přístup neoprávněné osobě,
- kdo podal žádost, musí neprodleně oznámit NBÚ změny údajů, které jsou v ní uvedeny,
- je povinen při výkonu státní kontroly NBÚ plnit pokyny kontrolního pracovníka při provádění neodkladných opatření k nápravě, tj. k zajištění OUI.



Povinnosti při ochraně UI

Povinnosti osoby mající přístup k UI:

- dodržovat povinnosti při ochraně UI,
- neprodleně NBÚ písemně oznámit ztrátu nebo odcizení svého OFO,
- neprodleně oznámit změny údajů NBÚ, které byly uvedeny v její žádosti (v dotazníku),
- neprodleně oznamovat tomu, kdo provedl její poučení, porušení povinností stanovených Zákonem 412/2005 Sb.,
- účastnit se proškolení 1x ročně.



Povinnosti při ochraně UI

Povinnosti odpovědné osoby:

- zajistit poučení fyzické osoby,
- zajistit jednou ročně provedení proškolení fyzických osob, které mají přístup k UI, z právních předpisů v oblasti OUI,
- zajistit ověřování splnění podmínek pro přístup fyzické osoby k UI informací stupně utajení Vyhrazené,
- schválit IS do provozu a písemně tuto skutečnost oznámit NBÚ,
- pověřit fyzickou osobu k činnosti nebo k výkonu kryptografické ochrany,
- kontrolovat dodržování dalších povinností stanovených zákonem.



Postup při určení osob pro seznamování s UI:

- Výběr navrhované osoby
- Splnění podmínek pro vydání osvědčení:
 - způsobilost k právním úkonům,
 - 18 let věku,
 - bezúhonnost,
 - občan ČR/ EU/ NATO,
 - osobnostní způsobilost ,
 - bezpečnostní spolehlivost.
- Provedení bezpečnostní prověrky
 - vyplnění bezpečnostního dotazníku,
 - provedení vlastní prověrky,
 - založení bezpečnostního spisu
- Vydání osvědčení
- Poučení navrhované osoby



Stupně bezpečnostních prověrek

- I. stupeň pro stupeň utajení „VYHRAZENÉ“
 - provádí statutární orgán, po 5 letech kontrola a aktualizace dokumentů,
- II. stupeň pro stupeň utajení „DŮVĚRNÉ“
 - doba platnosti osvědčení je 9 let
 - provádí NBÚ
- III. stupeň pro stupeň utajení „TAJNÉ“
 - doba platnosti osvědčení je 7 let
 - provádí NBÚ
- IV. stupeň pro stupeň utajení „PŘÍSNĚ TAJNÉ“
 - doba platnosti osvědčení je 5 let
 - provádí NBÚ



Otázky samostudium

- Jaké je postavení NBÚ, NÚKIB a ÚOOÚ k fyzickým osobám a právnickým osobám z hlediska své působnosti?
- Jaké role bezpečnostního managementu by si měla každá organizace vytvářet a z jakého důvodu?





Literatura

- LUKÁŠ, Luděk. Bezpečnostní technologie, systémy a management. Zlín: Radim Bačuvčík - VeRBuM, 2011-2015. 5 svazků. 978-80-87500-05-7, 978-80-87500-19-4, 978-80-87500-35-4, 978-80-87500-57-6, 978-80-87500-67-5
- LUKÁŠ, Luděk. Teorie bezpečnosti I. Zlín: Radim Bačuvčík - VeRBuM, 2017. ISBN 978-80-87500-89-7.
- NEČAS, Stanislav. Management rizika a management bezpečnosti v organizacích. Praha: Vysoká škola Karlovy Vary, 2013. ISBN 978-80-87236-17-8.
- POŽÁR, Josef a Milan KNY. Reflexe funkcí bezpečnostního managementu: Výzkumné centrum bezpečnostního managementu. Praha: Policejní akademie České republiky v Praze, 2015. ISBN 978-80-7251-445-8.
- DRASTICH, Martin. Systém managementu bezpečnosti informací. 1. vyd. Praha: Grada, 2011, 126 s. Průvodce. ISBN 978-80-247-4251-9.
- RODRYČOVÁ, Danuše a Pavel STAŠA. Bezpečnost informací jako podmínka prosperity firmy. Praha: Grada, 2000. Manažer. ISBN 80-7169-144-5. Dostupné také z: <http://www.digitalniknihovna.cz/mzk/uuid/uuid:89b88500-535e-11e4-bc71-005056827e52>
- DVOŘÁK, Jan. Zákon o ochraně utajovaných informací a o bezpečnostní způsobilosti: komentář. Praha: Wolters Kluwer, 2018. Komentáře Wolters Kluwer. ISBN 978-80-7598-016-8.