

FVL FB

Bezpečnostní normy

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

Osnova

- Úvod
- Vývoj v oblasti bezpečnosti
- Normy OUI zveřejněné ve sbírce zákonů
- Normy NATO
- Normy EU
- Mezinárodní uznávané normy
- Národní normy
- Význam Zákona 412/2006 Sb.



1. ÚVOD

Vztahy mezi lidmi jsou upraveny řadou normativních systémů:

- právní,
- morální,
- náboženské,
- zvykové,
- politické,
- estetické,
- dále např. technické, jazykové či ekonomické.

1. ÚVOD

- Právní normy jsou základním a integrujícím souborem společnosti.
- Zdroje právních norem jsou tzv. prameny práva:
 - právní předpisy,
 - mezinárodní smlouvy,
 - obyčeje,
 - nálezy Ústavního soudu.

1. ÚVOD

- Dále hovoříme o:
 - morálních normách, které jsou jedny z nejvýznamnějších a podporují právo.
 - náboženské normy - hrají takovou roli, jakou roli hraje náboženství ve veřejném životě toho kterého státu.
 - zdvořilostní normy - tato oblast je velmi důležitá jako projev lidských vztahů.



1. ÚVOD

- Oblast ochrany utajovaných informací (OUI) je řešena zákonem a právními prováděcími předpisy.
- V současné době řeší OUI Zákon č. 412/2005 Sb., o ochraně utajovaných informací a bezpečnostní způsobilosti.
- V návaznosti na něj jsou vydávány právní prováděcí předpisy - Vyhlášky NBÚ.
- Musíme respektovat závazky, k nimž se ČR zavázala v dvoustranných či vícestranných smlouvách.



1. ÚVOD

- Při řešení bezpečnosti bychom měli uplatňovat komplexní pojetí a dosáhnout co nevyšší integrace řízení.
- Bezpečnost v praxi musí být jasně definovaná struktura prvků s interaktivními vazbami.
- Zajištění bezpečnosti je velmi dynamický a neustále měnící se proces.

Vývoj v oblasti bezpečnosti informací v posledních letech

- Po skončení 2. světové války byla ČSR přiřazena do sféry vlivu SSSR. Vše z oblasti bezpečnosti státu bylo utajováno.
- Organizace bezpečnosti nebyla jednotná a např. Ministerstvo obrany (MO) používalo pro oblast ochrany utajovaných skutečností předpisy Všeob-70 Práv a posléze Všeob P-38.
- MO prověřovalo osoby, které mohly vejít do styku s utajovanými skutečnostmi na základě svého rozhodnutí.

Vývoj v oblasti bezpečnosti informací v posledních 25 letech

- Zásadní zlom po roce 1989.
- V 90. letech byly zveřejňovány informace do té doby utajované, bez analýzy zda může dojít k újmě.
- Na začátku 90. let šla ČR v oblasti bezpečnosti svou vlastní cestou.
- Postupné zapojování naší země do projektu NATO „Partnerství pro mír“ v polovině 90. let nám zpřístupnilo postupy a procedury od spojenců z NATO.



Vývoj bezpečnostní legislativy a prováděné změny s jejich důsledky

- Zlom nastal po přizvání ČR do NATO. Neexistoval zde žádný právní předpis, který by dával záruky NATO pro OUI.
- Z tohoto důvodu byl přijat Zákon 148/1998 Sb. o ochraně utajovaných skutečností.



Vývoj bezpečnostní legislativy a prováděné změny s jejich důsledky

Proč byla důležitá tato norma:

- legislativní srovnání ČR zejména se státy NATO a EU;
- vytvoření NBÚ;
- vytvoření legislativních úprav cestou NBÚ k řešení problematiky bezpečnosti;
- zaveden systém bezpečnostních prověrek;
- definování prostředků ochrany utajovaných skutečností,
- nastavení pravidel pro umožnění výměny UI v mezinárodním styku;
- zřízení registrů pro shromažďování UI cizí mocí.



Bezpečnostní legislativa



A pyramid diagram illustrating the hierarchy of security legislation. The pyramid is divided into five horizontal layers, each with a different color and a specific label. From top to bottom, the layers are: a small cyan triangle labeled 'Zákon', a teal trapezoid labeled 'Nařízení vlády', a green trapezoid labeled 'Vyhlášky NBÚ', a light gray trapezoid labeled 'Rozkaz ministra obrany', and a large yellow trapezoid at the base labeled 'Normativní výnos'.

Zákon

Nařízení vlády

Vyhlášky NBÚ

Rozkaz ministra obrany

Normativní výnos

2. Normy OUI zveřejněné ve sbírce zákonů

- V roce 2005 vydán Zákon 412/2005 Sb., který je platnou normou a řeší problematiku **OUI a bezpečnostní způsobilosti**.
- Tento zákon definuje:
 - stanovení vymezeného časového rámce a zjednodušení bezpečnostních prověrek fyzických osob;
 - zvýšení odpovědnosti každé fyzické osoby – zavedeno poučení fyzické osoby;
 - u fyzických osob již nebude porušení povinností posuzováno jako jiný správní delikt, ale jako přestupek a na jeho projednávání NBÚ se bude vztahovat zákon o přestupcích, nikoli správní řád jako doposud;

2. Normy OUI zveřejněné ve sbírce zákonů

- vymezení okruhu lidí pracujících v:
 - zahraničním obchodu s vojenským materiálem,
 - o osoby pracující v oblasti mírového využití jaderné energie a ionizujícího záření (atomový zákon) a
 - o nakládání s některými věcmi využitelnými k obranným a bezpečnostním účelům na území ČR hornická činnost, výbušniny a státní báňská správa,
 - oblasti veřejných zakázek,
 - v oblasti insolvenčního řízení jako insolvenční správci.
- přesun významu jednotlivých druhů zajištění OUI z vyhlášek do zákona;
- změny v oblasti kryptografické ochrany;
- změna či zavedení nového názvosloví.



2. Normy OUI zveřejněné ve sbírce zákonů

- Další zákony mající vztah k ochraně informací:
 - Zákon č. 101/2000 Sb., o ochraně osobních údajů a změně některých zákonů.
 - Zákon č. 499/ 2004 Sb., o archivnictví, který upravuje ochranu archiválií.
 - **Zákon č. 181/2014 Sb. o kybernetické bezpečnosti a o změně souvisejících zákonů**
 - Zákon č. 137/2006 Sb. o veřejných zakázkách
 - Dále např. Zákon o krizovém řízení, Zákon o elektronickém podpisu apod.



Normy OUI řešící problematiku OUI v ČR – vydané NBÚ

- Vyhláška č. **432/2011** Sb., o zajištění **kryptografické ochrany** utajovaných informací (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



Normy OUI řešící problematiku OUI v ČR – vydané NBÚ

- Vyhláška č. **528/2005** Sb., o **fyzické bezpečnosti** a certifikaci technických prostředků, ve znění vyhlášky č. 19/2008 Sb., č. 454/2011 Sb. a 205/2016 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.
- Vyhláška č. **523/2005** Sb., o **bezpečnosti informačních a komunikačních systémů** (IKS) a dalších elektronických zařízení nakládajících s utajovanými informacemi a o certifikaci stínících komor, ve znění vyhlášky č. **453/2011** Sb.
- Nařízení vlády č. **522/2005** Sb., kterým se stanoví **seznam utajovaných informací** (SUI), ve znění nařízení vlády č. **240/2008** Sb.



2. Normy OUI vydané v resortu Ministerstva obrany

- RMO 16/2013 Ochrana určených neutajovaných informací v resortu MO
- **RMO 14/2013 Ochrana utajovaných informací v resortu MO**
- **RMO 33/2012 o personální bezpečnosti v resortu MO**
- RMO 6/2010 ve znění RMO 14/2011 Zřízení rady pro kybernetickou bezpečnost
- RMO 11/2010 ve znění RMO 42/2010 a RMO 17/2013 Spisový řád
- RMO 18/2006 ve znění RMO 44/2010 a RMO 16/2012 Seznam zvlášť určených pracovišť
- RMO 25/2007 Stanovení stupňů utajení

2. Normy OUI vydané v resortu Ministerstva obrany

- NV 85/2013 **BIKS a EZ nakládajících s UI**
- NV 77/2013 **Fyzická bezpečnost v rezortu MO**
- NV 20/2013 BIKS a EZ, které nakládají s určenými neutajovanými informacemi (UNI) v rezortu MO
- NV 19/2013 Technické standardy pro přenosy dat prostřednictvím data linků
- NV 18/2013 OUI poskytovaných podnikatelům
- NV 60/2012 **Administrativní bezpečnost**
- NV 33/2010 OUI před KEV
- NV 12/2010 **Spisová služba** ve znění NV 61/2012
- NV 111/2013 **Kryptografická ochrana**

3. Normy NATO

- **CM 2002 49 „Bezpečnost v rámci organizace Severoatlantické smlouvy“,** definuje bezpečnostní požadavky a procedury pro OUI a jednání v rámci NATO.
- **CM 2002 49 je rozdělen do příloh:**
 - Příloha A - Bezpečnostní dohoda
 - Příloha B - Základní principy bezpečnosti
 - Příloha C - Personální bezpečnost
 - Příloha D - Fyzická bezpečnost
 - Příloha E - Bezpečnost informací
 - Příloha F - INFOSEC
 - Příloha G - Průmyslová bezpečnost
 - Výkladový slovník
- **AD 70-1 Bezpečnostní předpis**

4. Normy EU

Dokumenty EU:

- **Rozhodnutí rady** (2001/264/ES) ve znění pozdějších novelizací (2004/194/EC), (2005/571/ES) a (2005/952/ES);
- **Rozhodnutí komise** (2001/844/ES, ESUO, Euratom), (2005/94/ES, Euratom) a (2006/70/ES, Euratom);
- **Nařízení rady** č. 3 roku 1958.



5. Mezinárodní uznávané normy

Mezinárodní uznávané normy zakotvené v českých právních dokumentech:

- Pro potřeby řízení bezpečnosti informačních systémů lze využít, technickou zprávu typu 3, ČSN ISO/IEC TR 13335 Informační technologie – Směrnice pro řízení bezpečnosti:
- Pro hodnocení bezpečnosti IS se využívá ČSN ISO/IEC 15408 Informační technologie – Bezpečnostní techniky – Kritéria pro hodnocení bezpečnosti (známá jako Common Criteria)
- Normy ISO řady 9000 pro řízení kvality v organizaci
- Normy ISO 27000 týkající se Information systems management security



6. Národní normy

- Národní instituty zabývající se problematikou řízení bezpečnosti. Velmi aktivní je např. americký institut pro standardizaci a technologie NIST:
 - **NIST Speciální publikace 800-100** – určen pro manažery odpovědné za vypracování bezpečnostního programu organizace.
 - **NIST Speciální publikace 800-55** – je zaměřen na oblast IT. Reaguje na požadavek měření výkonu bezpečnosti. Zabývá se vytvářením metrik a způsobem použití těchto metrik pro efektivní posouzení systému s cílem směřování zdrojů. podrobně analyzovat a využít.
 - **NIST Speciální publikace 800-53 Revize 2** – zabývá se problematikou bezpečnosti IT. Používá systém bezpečnostních kontrol, popisuje druhy kontrol a jejich využití
 - **NIST Speciální publikace 800-33** – je určen pro nestátní organizace nakládající s citlivými informacemi.
 - **NIST Speciální publikace 800-80** – zabývá se problematikou vytváření a implementace metrik informační bezpečnosti. Řeší problematiku informační bezpečnosti v souvislosti s kontrolami a strategickým plánováním.
 - **NIST Speciální publikace 800-55 Revize 1. (Návrh)** – zabývá se opatřeními na zvýšení odpovědnosti při sběru, analýze a zpracování zpráv či relevantních informací cestou implementace efektivního informačního systému a programu bezpečnostních kontrol organizace v kritických aktivitách.

7. Význam Zákona 412/2005 Sb.

- legislativní základ pro srovnání s ostatními státy,
- existence nezávislého státního orgánu pro oblast OUI – NBÚ,
- systém bezpečnostních prověrek,
- stanovení základní terminologie,
- stanovení druhů zajištění UI:
 - personální,
 - průmyslová,
 - administrativní,
 - fyzická,
 - bezpečnost IKS
 - kryptografická ochrana
- výměna UI v mezinárodním styku,
- vytýčení citlivých činností z hlediska státu.



7. Význam Zákona 412/2005 Sb.

Povinnosti při OUI:

- Obecné povinnosti
- Povinnosti odpovědné osoby
- Povinnosti fyzických osob
- Povinnosti podnikatele



7. Význam Zákona 412/2005 Sb.

OBECNÉ POVINNOSTI

- Každý je povinen **neprodleně odevzdat nalezenou UI** nebo UI získanou v rozporu s 412/2005 anebo OFO, osvědčení podnikatele, OFO pro cizí moc nebo osvědčení podnikatele pro cizí moc NBÚ, policii nebo zastupitelskému úřadu ČR.
- Každý, kdo měl nebo má přístup k UI, je povinen zachovávat o ní mlčenlivost a nesmí k ní umožnit přístup neoprávněné osobě.
- Každý, kdo podal žádost je povinen neprodleně **oznámit NBÚ změny údajů**, které jsou v ní uvedeny.
- Každý je povinen při výkonu státní kontroly NBÚ plnit pokyny kontrolního pracovníka při provádění neodkladných opatření.

7. Význam Zákona 412/2005 Sb.

Fyzická osoba, která má přístup k UI je povinna:

- **dodržovat povinnosti** při OUI,
- **odevzdat tomu, kdo osvědčení fyzické osoby vydal, do 5 dnů své OFO**, jehož platnost zanikla podle § 56 odst. 1 písm. b), f) a g),
- **neprodleně písemně oznámit** tomu, kdo OFO nebo OFO pro cizí moc vydal, ztrátu nebo odcizení svého osvědčení fyzické osoby nebo osvědčení fyzické osoby pro cizí moc,
- **neprodleně oznámit NBÚ změny** údajů, které byly uvedeny v její žádosti fyzické osoby,
- **neprodleně oznamovat tomu**, kdo provedl její poučení porušení povinností stanovených Zákonem 412/2005,
- **účastnit se proškolení**



7. Význam Zákona 412/2005 Sb.

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 informaci 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.



7. Význam Zákona 412/2005 Sb.

Určení postupu 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



7. Význam Zákona 412/2005 Sb.

Stupně bezpečnostních prověrek

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



7. Význam Zákona 412/2005 Sb.

- Jsou-li při provádění bezpečnostní prověrky zjištěny skutečnosti, které mohou být na překážku vydání osvědčení, provádí se **bezpečnostní pohovor**. V případě PT vždy. V bezpečnostním pohovoru má navrhovaná osoba možnost vyjádřit se ke zjištěným skutečnostem.
- V případě, že NBÚ bezpečnostní prověrkou ověří, že navrhovaná osoba splňuje podmínky může vydat **osvědčení**, které této osobě doručí.
- **Poučení** před prvním kontaktem s utajovanou informací **provádí odpovědná osoba**. O Poučení se provede záznam.



7. Význam Zákona 412/2005 Sb.

Druhy zajištění OUI

- **personální bezpečnost**, je tvořena výběrem fyzických osob, které mají mít přístup k UI, ověřování podmínek pro jejich přístup k UI, jejich výchova a ochrana,
- **průmyslová bezpečnost**, která je tvořena systémem opatření k zjišťování a ověřování podmínek pro přístup podnikatele k UI a k zajištění nakládání s UI u podnikatele v souladu s 412/2005,
- **administrativní bezpečnost**, která je tvořena systémem opatření při tvorbě, příjmu, evidenci, zpracování, odesílání, přepravě, přenášení, ukládání, skartačním řízení, archivaci, případně jiném nakládání s UI,
- **fyzická bezpečnost**, která je tvořena systémem opatření, která mají neoprávněné osobě zabránit nebo ztížit přístup k UI, popřípadě přístup nebo pokus o něj zaznamenat,
- **bezpečnost IKS**, kterou 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,
- **kryptografická ochrana**, kterou tvoří systém opatření na ochranu UI použitím kryptografických metod a kryptografických materiálů při zpracování, přenosu nebo ukládání UI.



7. Význam Zákona 412/2005 Sb.

Mezinárodní styky

- Zákon 412/2005 o OUI a bezpečnostní způsobilosti, stanoví podmínky poskytování UI v mezinárodním styku.
- UI je možné poskytovat pouze na základě písemné žádosti a povolení za podmínek stanovených zákonem 412/2005.
- Orgány státu, právnické osoby a podnikající fyzické osoby evidují, ukládají nebo odesílají UI registrech.



7. Význam Zákona 412/2005 Sb.

Výkon státního dozoru, pokuty a řízení

- **Státním dozorem** v oblasti OUI a bezpečnostní způsobilosti je dozor nad tím, jak orgány státu, podnikatelé a fyzické osoby **dodržují právní předpisy** v této oblasti.
- Při výkonu státního dozoru se postupuje přiměřeně podle zákona upravujícího státní kontrolu.
- **Zaměstnanci NBÚ** mají při výkonu státního dozoru přístup k UI v rozsahu prováděné kontroly, prokáží-li se **platným OFO** pro příslušný stupeň utajení.
- NBÚ cizí moci, který má v působnosti OUI, je oprávněn účastnit se státního dozoru v oblasti OUI, které jsou jím poskytnuty ČR, vyplývá-li to ze záazku členství ČR v EU, nebo stanoví-li tak mezinárodní smlouva, kterou je Česká republika vázána.
- Státnímu dozoru podle tohoto zákona nepodléhá činnost zpravodajských služeb a činnost Ministerstva vnitra.



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.
- Dobda, L.: Ochrana dat v IS
- Předpis NATO AD 70-1.
- Dokument NATO C-M(2002)49 Security within NATO. 2002.
- ČSN ISO/IEC 15408 Informační technologie – Bezpečnostní techniky – Kritéria pro hodnocení bezpečnosti IT
- ČSN ISO/IEC 17799 Informační technologie – Soubor postupů pro řízení informační bezpečnosti
- Normy řady ISO/IEC 27000 - 27006 ISMS
- www.nbu.cz
- www.nist.gov



Literatura

- Zákon č. 101/2000 Sb., o ochraně osobních údajů a změně některých zákonů.
- Zákon č. 499/ 2004 Sb., o archivnictví, který upravuje ochranu archiválií.
- Zákona č. 137/2006 Sb. o veřejných zakázkách
- Zákon o krizovém řízení,
- Zákon o elektronickém podpisu



Literatura

- Vyhláška č. **432/2011** Sb., o zajištění **kryptografické ochrany** utajovaných informací (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



Literatura

- 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.
- 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.
- Nařízení vlády č. **522/2005** Sb., kterým se stanoví **seznam utajovaných informací** (SUI), ve znění nařízení vlády č. **240/2008** Sb.

