MANAGEMENT KYBERNETICKÉ BEZPEČNOSTI

TÉMA Č. 4
ISO NORMY RODINY 27K

pplk. Ing. Petr HRŮZA, Ph.D.
Univerzita obrany, Fakulta ekonomiky a managementu
Katedra vojenského managementu a taktiky
E-mail.: petr.hruza@unob.cz

Operační program Vzdělávání pro konkurenceschopnost

Projekt: ***Vzdělávání pro bezpečnostní systém státu***

(reg. č.: CZ.1.01/2.2.00/15.0070)

OBSAH

- ✓Co jsou normy.
- ✓Řada ISO/IEC 27k.
- ✓Řada ISO/IEC 27k – připravované normy.
- ✓Popis jednotlivých norem.
- ✓Závěr

Literatura

ČSN ISO/IEC 27000 Datum vydání : 1.5.2010

Informační technologie - Bezpečnostní techniky - Systémy řízení bezpečnosti informací - Přehled a slovník.

ČSN ISO/IEC 27001 Datum vydání : 1.10.2006

Informační technologie - Bezpečnostní techniky - Systémy managementu bezpečnosti informací - Požadavky.

ČSN ISO/IEC 27002 / 17799 Datum vydání : 1.8.2006

Informační technologie - Bezpečnostní techniky - Soubor postupů pro management bezpečnosti informací.

Literatura

ČSN ISO/IEC 27004 Datum vydání : 1.1.2011

Informační technologie - Bezpečnostní techniky - Řízení bezpečnosti informací - Měření

ČSN ISO/IEC 27005 Datum vydání : 1.7.2009

Informační technologie - Bezpečnostní techniky - Řízení rizik bezpečnosti informací.

ČSN ISO/IEC 27006 Datum vydání : 1.4.2008

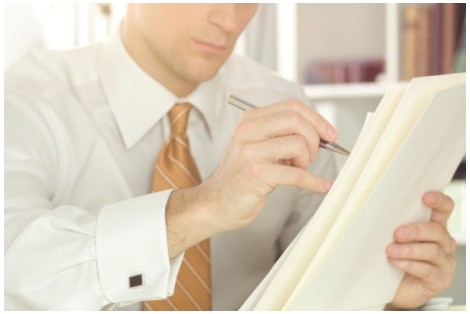
Informační technologie - Bezpečnostní techniky – Požadavky na orgány provádějící audit a certifikaci systémů řízení bezpečnosti informací.

Co jsou normy

Normy jsou definovány jako **směrnice, pravidlo**, jehož zachování je závazné, např. mravní, právní, technické. Technická norma přesně stanovuje požadované vlastnosti, provedení, tvar nebo uspořádání opakujících se předmětů nebo způsobů a postupů práce, popř. vymezuje všeobecně užívané technické pojmy.

Hlavními úkoly normy jsou např.:

- zjednodušování a snižování rozmanitosti výrobků a činností;
- dorozumívací funkce mezi výrobcem a zákazníkem a mezi výrobci v národním i mezinárodním měřítku;
- zavádění symbolů a kódů ke zjednodušení obchodního styku a překonání potíží způsobených rozdílností jazyků;
- zlepšení hospodárnosti;
- ochrana spotřebitele.



Řada ISO/IEC 27k

Do této doby byly publikovány následující normy:

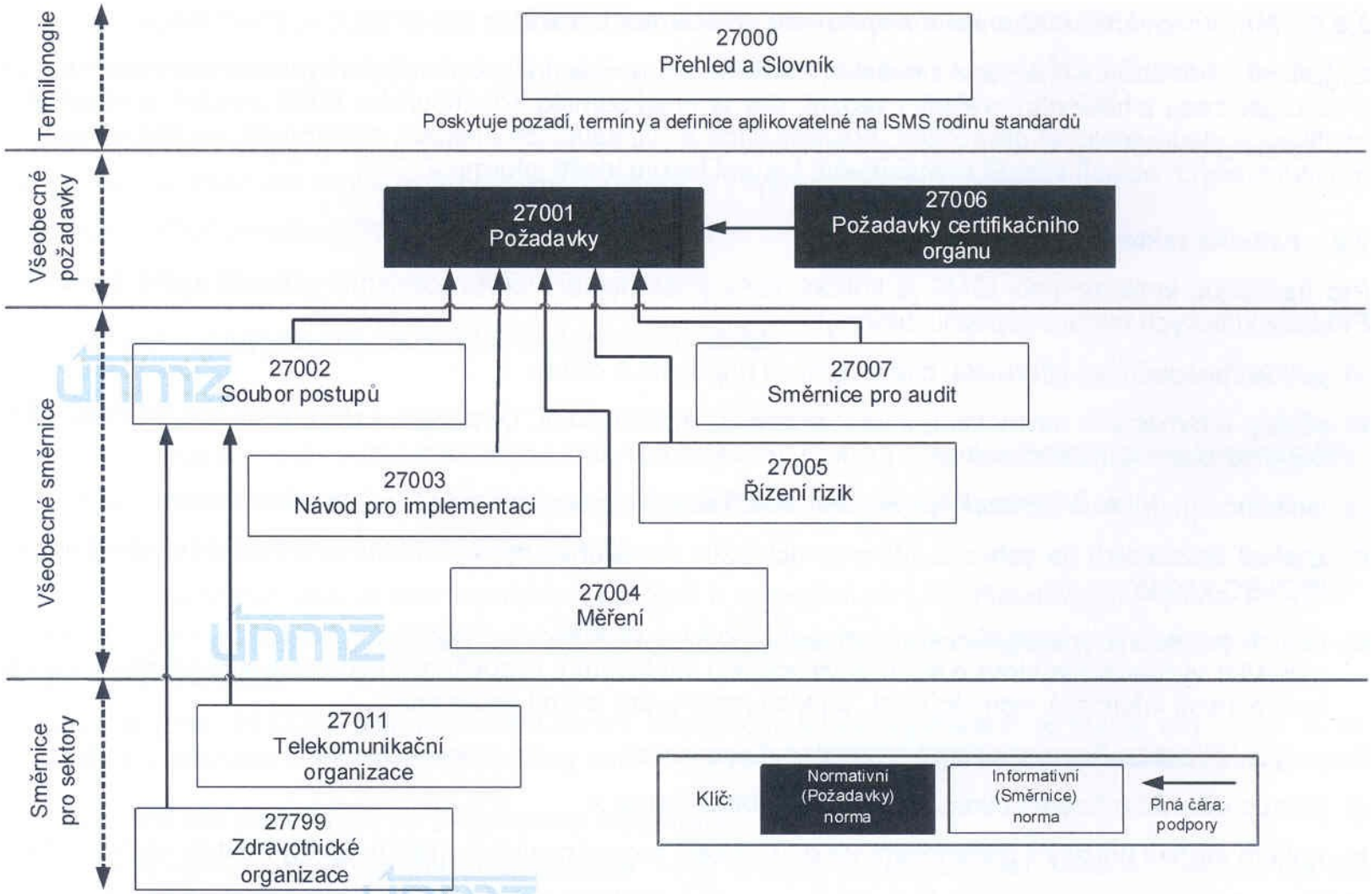
- **ISO 27000** - definice pojmů a terminologický slovník pro všechny ostatní normy z této série byl vydán v květnu 2009.
- **ISO 27001** (BS7799-2) - hlavní norma pro Systém řízení bezpečnosti informací (ISMS), dříve známá jako BS7799 část 2, podle které jsou systémy certifikovány. Norma byla publikována koncem října 2005.
- **ISO 27002** (ISO/IEC 17799 & BS7799-1) - aktuální verze normy byla prvně publikována v červnu 2005 jako ISO/IEC 17799:2005. V červenci 2007 došlo k přejmenování ISO/IEC 17799:2005 na ISO/IEC 27002:2005, obsahově se normy neliší.
- **ISO 27004** - norma byla publikována v prosinci 2009 pod názvem "Information technology - Security techniques - Information security management - Measurement".

Řada ISO/IEC 27k

Do této doby byly publikovány následující normy:

- **ISO 27005** - norma byla publikována v červnu 2008 pod názvem "Information technology - Security techniques - Information security risk management"..
- **ISO 27006** - norma byla publikována v březnu 2007 pod názvem “Information technology - Security techniques - Requirements for bodies providing audit and certification of information security management systems”.
- **ISO 27011** - doporučení a požadavky na řízení bezpečnosti informací v prostředí telekomunikačních operátorů.
- **ISO 27799** - doporučení a požadavky na řízení bezpečnosti informací ve zdravotnických zařízeních.

Řada ISO/IEC 27k



Řada ISO/IEC 27k – připravované normy

- **ISO 27007** - norma bude obsahovat doporučení pro auditování ISMS.
- **ISO 27008** - norma bude obsahovat doporučení auditorům ISMS a bude doplňovat ISO 27007.
- **ISO 27009** - norma bude obsahovat doporučení pro auditování bezpečnostních opatření.
- **ISO 27010** - norma by měla poskytovat doporučení pro vzájemnou komunikaci organizací a komunikaci organizací s vládou nejen v době krize.
- **ISO 27012** - projekt pro tvorbu normy, která měla poskytovat bezpečnostní doporučení pro státní správu při elektronické komunikaci s občany, byl zrušen.
- **ISO 27013** - norma by měla poskytovat doporučení pro implementaci ISO/IEC 20000 a ISO/IEC 27001.
- **ISO 27014** - norma by měla poskytovat doporučení organizacím při návrhu Information Security Governance.
- **ISO 27015** - doporučení a požadavky na řízení bezpečnosti informací v prostředí finančních institucí (banky, pojišťovny apod.).

Řada ISO/IEC 27k – připravované normy

- **ISO 27031** - norma bude obsahovat doporučení pro zajištění kontinuity činností organizace (business continuity).
- **ISO 27032** - pod označení "Guidelines for cybersecurity" vyjde ke konci roku 2010 norma obsahující bezpečnostní doporučení pro poskytovatele internetového připojení.
- **ISO 27033** - soustava norem poskytující doporučení pro implementaci protiopatření vztahujících se k bezpečnosti sítí.
- **ISO 27034** - soustava norem bude publikovaná pod označením "Information technology — Security techniques — Application security".
- **ISO 27035** - pod názvem "Security incident management" by měla vyjít norma vycházející z ISO TR 18044.
- **ISO 27036** - norma bude obsahovat doporučení organizacím pro hodnocení a snižování rizik týkajících se outsourcovaných služeb a pro podporu implementace bezpečnostních opatření podle standardu ISO/IEC 27002.
- **ISO 27037** - norma bude obsahovat doporučení pro zjišťování, sběr a získávání a uchovávání digitálních důkazů.

ČSN ISO/IEC 27000

ČSN ISO/IEC 27000 - Dat.vydání : 1.5.2010
Informační technologie - Bezpečnostní techniky - Systémy řízení bezpečnosti informací - Přehled a slovník.

Tato mezinárodní norma poskytuje přehled systémů řízení bezpečnosti informací , které tvoří předmět rodiny norem ISMS a definuje související termíny. Termíny a definice uvedené v této normě se týkají termínů a definic obecně použitých v rodině norem ISMS, nikoliv všech termínů a definic.

ČSN ISO/IEC 27001

ČSN ISO/IEC 27000 - Dat.vydání : 1.10.2006
Informační technologie - Bezpečnostní techniky - Systémy managementu bezpečnosti informací - Požadavky.

Norma poskytuje doporučení jak aplikovat vybraná opatření ISO/IEC 17799:2005 (do budoucna ISO/IEC 27002) v rámci procesu ustavení, provozu, údržby a zlepšování systému managementu bezpečnosti informací (Information Security Management System, **ISMS**) v organizaci. Norma prosazuje přijetí procesního přístupu k řešení ISMS, zavádí model známý jako Plánuj-Dělej-Kontroluj-Jednej (Plan-Do-Check-Act nebo zkratkou **PDCA**).V hlavní části normy jsou specifikovány požadavky na vybudování, zavedení, provoz, monitorování, přezkoumání, udržování, zlepšování a případnou certifikaci zdokumentovaného systému managementu bezpečnosti informací. Jsou zde specifikovány požadavky na výběr a zavedení bezpečnostních opatření chránících informační aktiva. V **příloze A** jsou uvedeny cíle opatření a jednotlivá opatření. V **příloze B** je uveden vztah mezi principy OECD pro bezpečnost informačních systémů a sítí a fázemi PDCA cyklu. V **příloze C** je uveden vztah mezi ISO/IEC 9001:2000, ISO/IEC 14001:2004 a ISO/IEC 27001:2005.

ČSN ISO/IEC 27002

ČSN ISO/IEC 27002 / 17799 Datum vydání : 1.8.2006
Informační technologie - Bezpečnostní techniky - Soubor postupů pro management bezpečnosti informací.

Tato mezinárodní norma poskytuje doporučení a obecné principy pro vymezení, zavedení, udržování a zlepšování systému managementu bezpečnosti informací v organizaci. Cíle, popsané v normě, poskytují rady o obecně přijímaných cílech managementu bezpečnosti.
Cíle opatření a jednotlivá opatření obsažená v této mezinárodní normě by měla být implementována na základě požadavků zjištěných v rámci analýzy rizik. Norma může sloužit jako praktický průvodce při vývoji bezpečnostních standardů organizace, účinných řídících bezpečnostních postupů a také při budování důvěry mezi organizacemi.

ČSN ISO/IEC 27004

ČSN ISO/IEC 27004 - Dat.vydání : 1.1.2011
Informační technologie - Bezpečnostní techniky - Řízení bezpečnosti informací - Měření.

Tato norma poskytuje doporučení pro vývoj a používání metrik a pro měření účinnosti zavedeného systému řízení bezpečnosti informací (ISMS) a účinnosti opatření nebo skupin opatření, jak je uvedeno v ISO/IEC 27001. Implementace těchto doporučení je předmětem programu měření bezpečnosti informací. Program měření bezpečnosti informací zahrnuje procesy rozvoje metrik a měření, provádění měření, analýzu dat a hlášení výsledků měření a dále proces vyhodnocení a zlepšování programu měření bezpečnosti informací. V příloze normy jsou pak uvedeny příklady konceptů měření pro určitá opatření nebo procesy ISMS.

ČSN ISO/IEC 27005

ČSN ISO/IEC 27005 - Dat.vydání : 1.7.2009
Informační technologie - Bezpečnostní techniky - Řízení rizik bezpečnosti informací.

Tato mezinárodní norma poskytuje doporučení pro řízení rizik bezpečnosti informací v rámci organizace, podporuje obecný koncept specifikovaný v ISO/IEC 27001 a je strukturována, aby dostatečně podporovala implementaci informační bezpečnosti založené na přístupu řízení rizik. Nicméně tato mezinárodní norma nenabízí konkrétní metodiku pro řízení rizik bezpečnosti informací. Záleží jen na organizaci, jaký přístup k řízení rizik zvolí, např. v závislosti na rozsahu ISMS, kontextu řízení rizik, průmyslovém odvětví. V souladu s přístupem k řízení rizik popsaným v této normě lze pro implementaci požadavků ISMS použít některou z celé řady existujících metodik pro řízení rizik. Norma je určená manažerům a pracovníkům, kteří jsou v rámci organizace odpovědní za řízení rizik bezpečnosti informací a tam, kde je to relevantní, také externím subjektům. Je aplikovatelná na všechny typy organizací (např. komerční společnosti, vládní organizace, neziskové organizace), které mají v úmyslu řídit rizika, která mohou narušit bezpečnost informací organizace.

ČSN ISO/IEC 27006

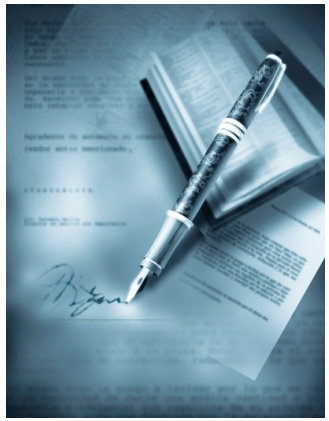
ČSN ISO/IEC 27006 - Dat.vydání : 1.4.2008
Informační technologie - Bezpečnostní techniky - Požadavky na orgány provádějící audit a certifikaci systémů řízení bezpečnosti informací.

Tato norma specifikuje požadavky a poskytuje doporučení pro orgány provádějící audit a certifikaci systému řízení bezpečnosti informací (ISMS) a doplňuje tak požadavky obsažené v ČSN ISO/IEC 17021 a ČSN ISO/IEC 27001. Norma je primárně určená k podpoře procesu akreditace certifikačních orgánů poskytujících certifikace ISMS.

ZÁVĚR

Normy jsou definovány jako **směrnice, pravidlo**, jehož zachování je závazné, např. mravní, právní, technické. Technická norma přesně stanovuje požadované vlastnosti, provedení, tvar nebo uspořádání opakujících se předmětů nebo způsobů a postupů práce, popř. vymezuje všeobecně užívané technické pojmy.

Rodina norem 27k má pomoci organizacím všech typů a velikostí zavést a provozovat systém ISMS. Organizace mohou použitím rodiny norem ISMS vyvinout a implementovat rámec pro řízení bezpečnosti svých bezpečnostních aktiv a připravit nezávislé ohodnocení svých ISMS.



Dotazy?

pplk. Ing. Petr HRŮZA, Ph.D.
Univerzita obrany, Fakulta ekonomiky a managementu
Katedra vojenského managementu a taktiky
E-mail.: petr.hruza@unob.cz