Přehled norem v oblasti bezpečnosti informačních technologií (normy vyvíjené ISO/IEC JTC1 SC27 a ISO TC 68) zavedených do soustavy českých norem

Do 70tých let bylo používání bezpečnostních, zejména kryptografických technik určených na ochranu informací omezeno na specifické oblasti aplikace. S rozšířením osobních počítačů a počítačových sítí, s nástupem Internetu a prováděním obchodních i dalších činností on-line se tento stav dramaticky změnil. Prudce vzrostla rovněž možná rizika spojená s využíváním těchto progresivních technologií. Proto se začal zejména v posledních letech klást důraz na jejich bezpečnost, tj. na zajištění zejména integrity, důvěrnosti a dostupnosti dat zpracovávaných prostřednictvím těchto technologií. Je zřejmé, že normalizované bezpečnostní techniky (autentizace entit, integrita dat, nepopiratelnost, důvěrnost dat) se stávají povinnými požadavky pro elektronický obchod, zdravotní péči a řadu dalších aplikačních oblastí. Bezpečnost IT se tak stala s ohledem na svůj průřezový charakter významnou částí normalizačních aktivit v celém světě.

Mezinárodní organizace pro normalizaci ISO (International Organisation for Standardisation) vyvíjí normy týkající se bezpečnosti informačních technologií v několika svých komisích a subkomisích. Nejdůležitější jsou vyvíjené pod ISO/IEC JTC1 SC 27 (Informační technologie – Bezpečnostní techniky) a TC 68 (Bankovnictví a související finanční služby).

V oblasti spolupráce s ostatními normalizačními komisemi ISO je cílem zajistit vývoj společných norem, vyhnout se možnému. překrývání a duplicitám ve vyvíjených normách a sdílet expertizy. SC 27 úzce spolupracuje v oblasti bezpečnostních norem s TC 68; za tímto účelem byla zřízena společná koordinační komise. Další spolupráce s ITU-T SG 7/Q20 je zaměřena zejména na vydávání společných norem. Spolupráce s CCIMB (Common Criteria Interpretation Managerial Board) umožňuje národním úřadům, které nejsou členy CCEB (Common Criteria Editorial Board) a CCIMB revidovat, připomínkovat a přispívat k vyvíjeným projektům (např. Common Criteria).

Vzhledem k tomu, že vývoj bezpečnostních norem je velmi náročnou záležitostí nezpracovávají se původní české normy. Vzhledem k úkolům na úseku harmonizace norem a právních dokumentů jsou běžně mezinárodní bezpečnostní normy ISO národními normalizačními orgány přejímány a vydávány jako národní normy. ČSNI plní v této oblasti významnou roli– mezinárodní bezpečnostní normy mající charakter průřezových norem (vyvíjené ISO/IEC JTC1 SC 27) jsou průběžně sledovány, přejímány a vydávány a aktualizovány jako české technické normy již řadu let. ČSNI rovněž zajišťuje mezinárodní spolupráci v této oblasti.

České technické normy přejímané z ISO/IEC JTC1 SC 27 pokrývají problematiku bezpečnosti informačních technologií na průřezové úrovni, jsou tedy všeobecně využitelné. Zajišťují normalizaci generických metod a technik pro bezpečnost informačních technologií. To zahrnuje:

- identifikaci generických požadavků (včetně požadavků na metodologii) pro bezpečnostní služby systémů IT
- vývoj bezpečnostních technik a mechanismů (včetně registračních postupů a vztahů mezi bezpečnostními komponentami)
- vývoj bezpečnostních směrnic (např. interpretační dokumenty)

- vývoj dokumentace a norem určených k podpoře managementu (např. terminologie a kritéria pro hodnocení bezpečnosti, problematika analýzy rizik).

České technické normy přejímané z ISO/IEC JTC1 SC 27 pokrývají normalizaci kryptografických algoritmů pro zajištění služeb integrity, autentizace a nepopiratelnosti. Zahrnují rovněž normalizaci kryptografických algoritmů pro zajištění služeb důvěrnosti a to v souladu s mezinárodně akceptovanými zásadami.

Přehled ČSN z oblasti bezpečnosti informačních technologií

ČSN ISO/IEC	2382-1	Informační technologie - Slovník - Část 1: Základní termíny
ČSN ISO/IEC	2382-8	Informační technologie - Slovník - Část 8: Bezpečnost
ČSN ISO/IEC	2382-14	Informační technologie - Slovník - Část 14: Spolehlivost
ČSN ISO/IEC	10116	Informační technologie - Bezpečnostní techniky - Módy činnosti pro n-bitovou blokovou šifru
ČSN ISO/IEC	10118-1	Informační technologie - Bezpečnostní techniky - Hašovací funkce - Část 1: Všeobecně
ČSN ISO/IEC	10118-2	Informační technologie - Bezpečnostní techniky - Hašovací funkce - Část 2: Hašovací funkce používající n-bitovou blokovou šifru
ČSN ISO/IEC	10118-3	Informační technologie - Bezpečnostní techniky - Hash funkce - Část 3: Dedikované hash funkce
ČSN ISO/IEC	10118-4	Informační technologie - Bezpečnostní techniky - Hašovací funkce - Část 4: Hašovací funkce používající modulární aritmetiku
ČSN ISO	10126-1	Bankovnictví - Postupy pro šifrování zpráv (bankovní služby pro velkou klientelu) - Část 1: Obecné zásady
ČSN ISO	10126-2	Bankovnictví - Postupy pro šifrování zpráv (bankovní služby pro velkou klientelu). Část 2: Algoritmus DEA
ČSN ISO	10202-1	Identifikační karty. Karty pro finanční transakce. Bezpečnostní architektura systémů finančních transakcí využívajících karty s integrovanými obvody. Část 1: Životní cyklus karty
ČSN ISO	11131	Bankovnictví - Autentizace přihlášením
ČSN ISO	11166-1	Bankovnictví - Správa klíčů prostřednictvím asymetrických algoritmů - Část 1: Zásady, postupy a formáty
ČSN ISO	11166-2	Bankovnictví - Správa klíčů pomocí asymetrických algoritmů - Část 2: Schválené algoritmy používající kryptosystém RSA
ČSN EN ISO	11568-1	Bankovnictví - Správa klíčů (bankovní služby pro drobnou klientelu) - Část 1: Úvod do správy klíčů
ČSN EN ISO	11568-2	Bankovnictví - Správa klíčů (bankovní služby pro drobnou klientelu) - Část 2: Techniky správy klíčů pro symetrickou šifru
ČSN EN ISO	11568-3	Bankovnictví - Správa klíčů (bankovní služby pro drobnou klientelu) - Část 3: Životní cyklus klíče pro symetrickou šifru
ČSN ISO/IEC	11770-1	Informační technologie - Bezpečnostní techniky - Správa klíčů - Část 1: Struktura
ČSN ISO/IEC	11770-2	Informační technologie - Bezpečnostní techniky - Správa klíčů - Část 2: Mechanismy používající symetrické techniky
ČSN ISO/IEC	11770-3	Informační technologie - Bezpečnostní techniky - Správa klíčů - Část 3: Mechanismy používající asymetrické techniky
ČSN ISO/IEC	13335-1	Informační technologie - Směrnice pro řízení bezpečnosti IT -

TR		Část 1: Pojetí a modely bezpečnosti IT
ČSN ISO/IEC TR	13335-2	Informační technologie - Směrnice pro řízení bezpečnosti IT - Část 2: Řízení a plánování bezpečnosti IT
ČSN ISO/IEC TR	13335-3	Informační technologie - Směrnice pro řízení bezpečnosti IT - Část 3: Techniky pro řízení bezpečnosti IT
ČSN ISO/IEC TR	13335-4	Informační technologie - Směrnice pro řízení bezpečnosti IT - Část 4: Výběr ochranných opatření
ČSN ISO/IEC	13888-1	Informační technologie - Bezpečnostní techniky - Nepopiratelnost - Část 1: Všeobecně
ČSN ISO/IEC	13888-2	Informační technologie - Bezpečnostní techniky - Nepopiratelnost - Část 2: Mechanismy používající symetrické techniky
ČSN ISO/IEC	13888-3	Informační technologie - Bezpečnostní techniky - Nepopiratelnost - Část 3: Mechanismy používající asymetrické techniky
ČSN ISO/IEC	14888-1	Informační technologie - Bezpečnostní techniky - Digitální podpisy s dodatkem - Část 1: Všeobecně
ČSN ISO/IEC	14888-2	Informační technologie - Bezpečnostní techniky - Digitální podpisy s dodatkem - Část 2: Mechanismy založené na identitě
ČSN ISO/IEC	14888-3	Informační technologie - Bezpečnostní techniky - Digitální podpisy s dodatkem - Část 3: Mechanismy založené na certifikátu
ČSN ISO/IEC	15408-1	Informační technologie - Bezpečnostní techniky - Kritéria pro hodnocení bezpečnosti IT - Část 1: Úvod a všeobecný model
ČSN ISO/IEC	15408-2	Informační technologie - Bezpečnostní techniky - Kritéria pro hodnocení bezpečnosti IT - Část 2: Bezpečnostní funkční požadavky
ČSN ISO/IEC	15408-3	Informační technologie - Bezpečnostní techniky - Kritéria pro hodnocení bezpečnosti IT - Část 3: Požadavky na záruky bezpečnosti
ČSN ISO/IEC	17799	Informační technologie - Soubor postupů pro řízení informační bezpečnosti
ČSN ISO	6166	Cenné papíry a příbuzné finanční nástroje - Mezinárodní systém identifikačního číslování cenných papírů (ISIN)
ČSN ISO	7775	Bankovnictví - Cenné papíry - Schéma pro typy zpráv
ČSN ISO	8372	Zpracování informací - Módy činnosti pro algoritmus 64-bitové blokové šifry
ČSN ISO	8730	Bankovnictví - Požadavky na autentizaci zprávy (bankovní služby pro velkou klientelu)
ČSN ISO	8731-1	Bankovnictví - Schválené algoritmy pro autentizaci zprávy - Část 1: DEA
ČSN ISO	8731-2	Bankovnictví - Schválené algoritmy pro autentizaci zprávy - Část 2: Algoritmus autentikátora zprávy
ČSN ISO	8732	Bankovnictví - Správa klíčů (bankovní služby pro velkou klientelu)
ČSN ISO	8908	Bankovnictví a souvisící finanční služby - Slovník a datové prvky
ČSN ISO	9564-1	Bankovnictví - Řízení a bezpečnost osobních identifikačních čísel. Část 1: Principy a techniky ochrany PIN
ČSN ISO	9564-2	Bankovnictví - Řízení a bezpečnost osobních identifikačních

		čísel. Část 2: Schválené algoritmy pro šifrování PIN
ČSN ISO	9735-5	Elektronická výměna dat pro správu, obchod a dopravu (EDIFACT) - Pravidla syntaxe aplikační úrovně (Číslo verze syntaxe: 4) - Část 5: Pravidla bezpečnosti pro dávkovou EDI (autentičnost, integrita a nepopření původu)
ČSN ISO	9735-6	Elektronická výměna dat pro správu, obchod a dopravu (EDIFACT) - Pravidla syntaxe aplikační úrovně (Číslo verze syntaxe: 4) - Část 6: Bezpečnostní autentizace a potvrzení (Zpráva AUTACK)
ČSN ISO/IEC	9796-2	Informační technologie - Bezpečnostní techniky - Schémata digitálního podpisu umožňující obnovu zprávy - Část 2: Mechanismy využívající hash funkci
ČSN ISO/IEC	9796-3	Informační technologie - Bezpečnostní techniky - Schémata digitálních podpisů umožňující obnovu zprávy - Část 3: Mechanismy založené na diskrétních logaritmech
ČSN ISO/IEC	9797	Informační technologie - Bezpečnostní techniky - Mechanismus integrity dat používající kryptografickou kontrolní funkci s využitím algoritmu blokové šifry
ČSN ISO/IEC	9797-1	Informační technologie - Bezpečnostní techniky - Kódy pro autentizaci zprávy (MAC) - Část 1: Mechanismy používající blokovou šifru
ČSN ISO/IEC	9798-1	Informační technologie - Bezpečnostní techniky - Mechanismy autentizace entit - 1. část: Obecný model
ČSN ISO/IEC	9798-2	Informační technologie - Bezpečnostní techniky - Autentizace entit - Část 2: Mechanismy používající symetrické šifrovací algoritmy
ČSN ISO/IEC	9798-3	Informační technologie - Bezpečnostní techniky - Mechanismy autentizace entit - Část 3: Autentizace entit používající algoritmus s veřejným klíčem
ČSN ISO/IEC	9798-4	Informační technologie - Bezpečnostní techniky - Autentizace entit - Část 4: Mechanismy používající kryptografickou kontrolní funkci
ČSN ISO/IEC	9798-5	Informační technologie - Bezpečnostní techniky - Autentizace entit - Část 5: Mechanismy používající techniku nulových znalostí
ČSN ISO	9807	Bankovnictví - Požadavky na autentizaci zpráv (bankovní služby pro drobnou klientelu)
ČSN ISO/IEC	9979	Informační technologie - Bezpečnostní techniky - Postupy pro registraci kryptografických algoritmů

Ing. Petr Wallenfels (petr.wallenfels@csni.cz) , zveřejněno v e-zinu Crypto-World 3/2003 (http://crypto-world.info)