ČESKÁ TECHNICKÁ NORMA

ICS 35.040

Září

2004

	Informační technologie - Bezpečnostní techniky - Systémy kontrolních znaků	ČSN ISO/IEC 7064 36 9794

Information technology - Security techniques - Check character systems

Technologies de l’information - Techniques de sécurité - Systèmes de caractères de contrôle

Tato norma je českou verzí mezinárodní normy ISO/IEC 7064:2003. Mezinárodní norma ISO/IEC 7064:2003 má status české technické normy.

This standard is the Czech version of the International Standard ISO/IEC 7064:2003. The International Standard ISO/IEC 7064:2003 has the status of a Czech Standard.

Nahrazení předchozích norem

Touto normou se nahrazuje ČSN ISO 7064 (97 9711) ze srpna 1995.

© Český normalizační institut,
2004
Podle zákona č. 22/1997 Sb. smějí být české technické normy rozmnožovány a rozšiřovány jen se souhlasem Českého normalizačního institutu.

70851

Národní předmluva

Vypracování normy

Zpracovatel: Ing. Vladimír Pračke, IČ 40654419

Technická normalizační komise: TNK 20 Informační technologie

Pracovník Českého normalizačního institutu: Ing. Petr Wallenfels

MEZINÁRODNÍ NORMA
Informační technologie - Bezpečnostní techniky - Systémy kontrolních znaků

ISO/IEC 7064
První vydání
2003-02-15

ICS 35.040

Odmítavé stanovisko k manipulaci s PDF souborem
Tento soubor PDF může obsahovat vložené typy písma. V souladu s licenční politikou Adobe lze tento soubor tisknout nebo prohlížet, ale nesmí být editován, ledaže by typy písma, které jsou vloženy, byly používány na základě licence a instalovány v počítači, na němž se editace provádí. Při stažení tohoto souboru přejímají jeho uživatelé odpovědnost za to, že nebude porušena licenční politika Adobe. Ústřední sekretariát ISO nepřejímá za její porušení žádnou odpovědnost.
Adobe je obchodní značka „Adobe Systems Incorporated“.
Podrobnosti o softwarových produktech použitých k vytváření tohoto souboru PDF lze najít ve Všeobecných informacích, které jsou k souboru připojeny; parametry, pomocí kterých byl PDF soubor vytvořen, byly optimalizovány pro tisk. Soubor byl zpracován s maximální péčí tak, aby ho členské organizace ISO mohly používat. V málo pravděpodobném případě, tj. když vznikne problém, který se týká souboru, informujte o tom na níže uvedené adrese Ústřední sekretariát ISO.

© ISO 2002

Všechna práva vyhrazena. ®ádná část této normy nesmí být reprodukována nebo zpracována jakoukoliv jinou formou, jako například elektronickou, mechanickou, včetně fotokopií a mikrofilmu bez písemného povolení ISO. Povolení lze vyžádat na níže uvedené adrese nebo u členské národní organizace v zemi žadatele.

ISO copyright office
Case postale 56, CH-1211 Geneva 20
Tel. +41 22 749 01 11
Fax. +41 22 734 10 79
e-mail copyright@iso.ch
Web www.iso.ch

Obsah

Předmluva

ISO (Mezinárodní organizace pro normalizaci) a IEC (Mezinárodní elektrotechnická komise) tvoří specializovaný systém světové normalizace. Národní orgány, které jsou členy ISO a IEC, se podílejí na vývoji mezinárodních norem prostřednictvím technických komisí, zřízených dotyčnou organizací a zabývajících se určitou oblastí technické činnosti. Technické komise ISO a IEC spolupracují v oblastech společných zájmů. Práce se zúčastňují i další mezinárodní organizace, vládní i nevládní, s nimiž ISO a IEC navázaly pracovní styk. ISO a IEC ustavily v oblasti informačních technologií společnou technickou komisi, ISO/IEC JTC 1.

Mezinárodní normy jsou navrhovány v souladu s pravidly obsaženými v části 2 Směrnic ISO/IEC.

Hlavním úkolem společné technické komise je příprava mezinárodních norem. Návrhy mezinárodních norem, přijaté společnou technickou komisí, se rozesílají národním orgánům k hlasování. Vydání návrhu jako mezinárodní normy vyžaduje souhlas alespoň 75 % hlasujících členů.

Pozornost je nutno věnovat možnosti, že některé prvky této mezinárodní normy mohou být předmětem patentových práv. ISO a IEC nelze považovat za odpovědné za identifikování některých nebo všech takových patentových práv.

ISO/IEC 7064 byla připravena společnou technickou komisí ISO/IEC JTC 1, *Informační technologie*, subkomise SC 27, *Bezpečnostní techniky IT*.

První vydání ISO/IEC 7064 ruší a nahrazuje ISO 7064:1983, která byla předmětem technické revize. Implementace, které vyhovují ISO 7064:1983, budou vyhovovat i ISO/IEC 7064:2003.

Úvod

Potřeba normalizace systémů kontrolních znaků byla vyvolána následujícími úvahami:

a) z množství systémů, které jsou používány, má mnoho z nich velmi podobné charakteristiky a mnoho z nich nepřináší žádný výrazný užitek;

b) málokterý z existujících systémů byl důkladně matematicky verifikován a některé mají podstatné vady;

c) různost systémů ničí ekonomickou stránku produktů, které generují nebo validují kontrolní znaky, a často brání kontrole vzájemně vyměňovaných dat.

Proto byl vybrán malý soubor kompatibilních systémů, který je schopen se vypořádat s potřebami různých aplikací; tyto systémy byly ověřeny a v rámci omezení, danými aplikací, poskytují vysokou ochranu proti typickým chybám plynoucím z přepisů a vstupů z klávesnice.

Existující systémy kontrolních znaků, specifikované v ISO 2108, ISO 2894 a ISO 6166, jsou používány ve speciálních oblastech aplikací (ISO 2894 byla zrušena). Tyto systémy ale nedosahují takové míry detekce chyb jako systémy specifikované v této mezinárodní normě.

Příloha A shrnuje kritéria, která by měla být vzata v úvahu při výběru systému kontrolních znaků, specifikovaných v této mezinárodní normě, pro jednotlivé aplikace.

Příloha B uvádí příklad metody, jak může být tato norma aplikována v případě abeced, které mají více než 26 znaků.

1 Předmět normy

1.1 Tato mezinárodní norma specifikuje sadu systémů kontrolních znaků, schopných chránit řetězce vůči chybám, které vznikají při kopírování nebo zadávání dat uživateli. Řetězce mohou mít pevnou nebo proměnnou délku a mohou vycházet ze znakových sad

a) číselných (10 číslic: 0 až 9);

b) abecedních (26 písmen: A až Z); a

c) alfanumerických (písmena a číslice).

Vložené mezery a zvláštní znaky jsou ignorovány.

1.2 Tato mezinárodní norma specifikuje požadavky na shodu pro metody, které generují kontrolní znaky nebo kontrolní řetězce s využitím systémů, popsaných v této mezinárodní normě.

1.3 Tyto systémy kontrolních znaků mohou detekovat:

a) všechny jednotlivé substituční chyby (substituce jednotlivého znaku za jiný, např. „4234“ místo „1234“);

b) všechny nebo téměř všechny jednotlivé (místní) transpoziční chyby (transpozice dvou jednotlivých znaků, buď sousedících nebo s jedním znakem mezi sebou, např. „12354“ nebo „12543“ místo

„12345“);

c) všechny nebo téměř všechny chyby s kruhovým posuvem (kruhové posuvy celého řetězce vlevo nebo vpravo);

d) velký podíl chyb dvojité substituce (dvě oddělené jednotlivé substituční chyby ve stejném řetězci, např. „7234587“ místo „1234567“); a

e) velký podíl všech ostatních chyb.

1.4 Tato mezinárodní norma vylučuje specificky navržené systémy, které

a) připouští jak detekci chyb tak automatické opravy;

b) detekují úmyslné padělání; a

c) kontrolují řetězce vyměňované výhradně mezi stroji.

1.5 Tato mezinárodní norma je určena k použití při výměně informací mezi organizacemi. Je rovněž důrazně doporučena k použití v interních informačních systémech.

-- Vynechaný text --