ČESKÁ NORMA

35.040

Únor 1994

Zpracování informací. Šifrování dat. Požadavky na součinnost fyzických vrstev

ČSN ISO 9160

36 9627

Information processing - Data encipherment - Physical layer interoperability requirements

Traitement de l'information - Chiffrement de données - Caractéristique interfonctionnement dans la couche physique

Informationsverarbeitung - Datenverschlüsselung - Datenschlüsselungsanforderungen für Kommunikation in der Bit-Übertragungsschicht

Tato norma obsahuje ISO 9160:1988.

Tato norma je přeložena z anglického znění bez redakčních změn. V případě, že by vznikl spor o výklad, použije se původního anglického znění normy.

This standard contains the International Standard ISO 9160:1988, first edition.

This standard is translated from the English version without editorial changes. In all cases of interpretation disputes, the English version applies.

Národní předmluva

Citované normy

ISO 2382-9 zavedena v ČSN ISO 2382-9 Zpracování dat. Slovník. Část 9: Datová komunikace (36 9001)

ISO 7498 dosud nezavedena[1])

ISO 7498-2 dosud nezavedena[1])

ISO 8372 dosud nezavedena

ANSI X3.92-198 1 dosud nezavedena

CCITT Doporučení X.20, X.20bis, X.21, X.2lbis - Červená kniha VIII.3 - 1984

dosud nezavedena

CCITT Doporučení V.24, V.54 - Červená kniha VIII.1 - 1984 dosud nezavedena

Obdobné mezinárodní, regionální a zahraniční normy

ISO 9160:1988 Information processing - Data encipherment - Physical layer interoperability requirements (Zpracování informací - šifrování dat - požadavky na součinnost fyzických vrstev)

BS 7112:1991; ISO 9160:1988 Procedures for achievement of interoperability and security by use of encipherment at the physical layer of OSI in telecommunication systems conveying Automatic Data Processing information (Procedury k dosažení součinnosti a bezpečnosti při použití šifrování ve fyzické vrstvě OSI v telekomunikačních systémech přenášejících informace strojového zpracování dat (ADP))

Tato norma obsahuje národní přílohu se seznamem pojmů a jejich překladů.

[1]) Norma se zpracovává.

Vypracování normy

Zpracovatel: TESLA TELEKOMUNIKACE. spol. s r. o. IČO 41194403, Ing. Otokar Buzek. CSc.

Technická normalizační komise: TNK 20 Informační technika

Pracovník Českého normalizačního institutu: Ing. Natálie Mišeková

ZPRACOVÁNÍ INFORMACÍ ŠIFROVÁNÍ DAT. POŽADAVKY NA SOUČINNOST FYZICKÝCH VRSTEV ISO 9160

První vydání

1988-02-01

MDT 681.3.04:621.39:654.028:003.26

Deskriptory: data processing, information interchange, open system interconnection, telecommunications, coded representation, data converting

Předmluva

ISO (mezinárodní organizace pro standardizaci) je celosvětovou federací národních normalizačních organizací (členů ISO). Na mezinárodních normách pracují technické komise ISO. Každý člen ISO, který se zajímá o předmět, pro který byla vytvořena technická komise, má právo být zastoupen v této

technické komisi. Práce se zúčastňují i mezinárodní organizace, vládní i nevládní, s nimiž ISO navázala pracovní styk.

Návrhy mezinárodních norem přijaté technickými komisemi se rozesílají členům ISO ke schválení před jejich přijetím jakožto mezinárodních norem radou ISO. Jsou schvalovány podle postupů ISO, požadujících schválení alespoň 75 % členů ISO.

Mezinárodní norma ISO 9160 byla připravena společnou technickou komisí ISO/TC 97 - *Systémy na zpracování informací*.

Uživatelé si musí uvědomit, že všechny mezinárodní normy jsou čas od času revidovány a že veškeré odkazy v této normě na jinou mezinárodní normu, pokud není uvedeno jinak, se týkají jejího posledního vydání.

0 Úvod

Tato mezinárodní norma specifikuje požadavky na součinnost a bezpečnost při použití šifrování na fyzické vrstvě referenčního modelu propojení otevřených systémů (OSI) ISO v telekomunikačních systémech přenášejících informace automatického zpracování dat (ADP).

Tato mezinárodní norma usnadní součinnost zařízení pro šifrování dat, používaných v komunikačních prostředcích a systémech, které vyžadují ochranu šifrováním.

Účelem šifrování ve fyzické vrstvě je ochrana proti všem formám pasivního napadení včetně analýzy provozu. Úplná ochrana před analýzou provozu může být zajištěna pouze při synchronním provozu, ve kterém lze šifrovat všechny bity, na rozdíl od asynchronního provozu, v němž nelze nikdy zašifrovat bity start a stop. Tato norma nezajišťuje ochranu zřízení fyzického spoje.

Tato mezinárodní norma obsahuje dvě přílohy A a B. Příloha A netvoří nedílnou část této mezinárodní normy. Příloha B tvoří nedílnou část této mezinárodní normy.

1 Předmět normy

Tato mezinárodní norma se vztahuje na systémy sloužící k šifrování informací automatického zpracování dat (ADP) ve fyzické vrstvě datové komunikace.

Tato norma je stejně použitelná jak v případě, kdy je datové šifrovací zařízení (DEE) realizováno jako fyzicky oddělená část zařízení nebo kdy je realizováno jako část koncového zařízení přenosu dat (DTE), tak i v případě kdy tvoří část ukončujícího zařízení datového okruhu (DCE). Je-li šifrování zabudováno do DTE nebo DCE, týká se tato norma těch částí DTE nebo DCE, které realizují požadavky této mezinárodní normy. Požadavky na součinnost jsou specifikovány pro následující definice fyzických rozhraní: V.24, X.20bis, X.21bis, X.20 a X.21.

Fyzická vrstva je popsána v referenčním modelu propojení otevřených systémů, ISO 7498. Při šifrování ve fyzické vrstvě je celá SDU normálně zašifrována. Požadavky na součinnost popsané v této mezinárodní normě se týkají jak synchronního a asynchronního provozu, tak i úplného duplexního a poloviční duplexního režimu.

Hlavní část této normy specifikuje požadavky, které jsou použitelné při využívání různých šifrovacích algoritmů. Příloha B specifikuje další požadavky pro použití DEA (ANSI X3.92-1981).

Tato norma také specifikuje dva alternativní režimy synchronního provozu a sice volitelný režim se zpožděním a volitelný režim bez zpoždění, které jsou vzájemně nekompatibilní.

Tato mezinárodní norma také specifikuje dva alternativní režimy BREAK při asynchronním provozu - Třída A a Třída B, které jsou vzájemně nekompatibilní.