ICS 35.040 SLOVENSKÁ TECHNICKÁ NORMA Marec 2023

STN	**Informačné technológie Bezpečnostné metódy Návody pre kybernetickú bezpečnosť**	**STN ISO/IEC 27032 97 4110**

Information technology
Security techniques
Guidelines for cybersecurity

Technologies de l'information
Techniques de sécurité
Lignes directrices pour la cybersécurité

Informationstechnik
Sicherheitsverfahren
Leitfaden für Cybersicherheit

Táto slovenská technická norma je slovenskou verziou medzinárodnej normy ISO/IEC 27032: 2012.
Preklad zabezpečil Úrad pre normalizáciu, metrológiu a skúšobníctvo Slovenskej republiky.
STN ISO/IEC 27032 má rovnaké postavenie, ako majú oficiálne verzie.

This standard is the Slovak version of the International Standard ISO/IEC 27032: 2012.
It was translated by Slovak Office of Standards, Metrology and Testing.
STN ISO/IEC 27032 has the same status as the official versions.

136248

Národný predhovor

Obrázky v tejto STN sú prevzaté z elektronických podkladov dodaných z ISO/IEC, © 2012 ISO/IEC, ref. č. ISO/IEC 27032 E.

Norma obsahuje 3 národné poznámky.

Slovenský jazyk a anglický jazyk majú výrazne rozdielnu slovnú zásobu a odborná angličtina má určité špecifické vlastnosti. Naviac mnohé technické výrazy, najmä v odbore informačná a kybernetická bezpečnosť vznikli až v novom tisícročí, bez toho, aby sa boli tieto výrazy ustálené v slovenskom jazyku. Preto nie je vždy možné a žiaduce vykonať preklad odborného kontextu doslovným prekladom, spájaním viet a gramatickými zámenami slov.

Medzinárodná norma musí získať konsolidovaný význam v obidvoch jazykoch. Z toho dôvodu boli pri preklade tejto medzinárodnej normy použité aj lexikálno-gramatické postupy, najmä explikácia (opisný preklad), s cieľom čo najväčšieho zachovania významovej stránky obsahu za cenu zmien jeho výrazovej stránky za použitia primeraných výrazových prostriedkov. Tým sa do slovenského technického jazyka formálne, prostredníctvom technickej normalizácie dostávajú niektoré slovné novotvary, najmä „kyberbezpečnosť“, „kyberochrana“, „kyberpriestor“, „haktivizmus“, „hekovanie“, „malvér“ a ďalšie, ako aj mnohé ich morfologické tvary. Špecifické technické výrazy, ktoré sú aj v anglickom jazyku používané len okrajovo, nedávalo význam prekladať do slovenského jazyka a uvádzajú sa v pôvodnom tvare – napr. termín „sinkhole“.

Technická komisia ISO/IEC JTC 1/SC 27 ohlásila prípravu novej verzie normy ISO/IEC 27032 Informačné technológie. Bezpečnostné metódy. Návody pre kybernetickú bezpečnosť, po jej oficiálnom publikovaní bude taktiež vydaná prekladom do štátneho jazyka.

Základným cieľom tejto medzinárodnej normy je venovať sa problémom bezpečnosti informácií so zameraním na premostenie rozdielov medzi rôznymi bezpečnostnými doménami v kybernetickom priestore.

Ako pravopisné zdroje boli pri preklade použité Krátky slovník slovenského jazyka a Slovenský národný korpus zo Slovníkového portálu Jazykovedného ústavu Ľ. Štúra SAV, a terminologické databázy, najmä Terminologický portál Jazykovedného ústavu Ľ. Štúra SAV a Terminologická databáza Úrad pre normalizáciu, metrológiu a skúšobníctvo SR.

Normatívne referenčné dokumenty

Nasledujúce dokumenty, celé alebo ich časti, sú v tomto dokumente normatívnymi odkazmi a sú nevyhnutné pri jeho používaní. Pri datovaných odkazoch sa použije len citované vydanie. Pri nedatovaných odkazoch sa použije najnovšie vydanie citovaného dokumentu (vrátane všetkých zmien).

POZNÁMKA 1. – Ak bola medzinárodná publikácia zmenená spoločnými modifikáciami, čo je indikované označením (mod), použije sa príslušná EN/HD.

POZNÁMKA 2. – Aktuálne informácie o platných a zrušených STN a TNI možno získať na webovom sídle www.unms.sk.

ISO/IEC 27000 prijatá ako STN EN ISO/IEC 27000 Informačné technológie. Bezpečnostné metódy. Systémy riadenia informačnej bezpečnosti. Prehľad a slovník (ISO/IEC 27000) (97 4170)

Vypracovanie slovenskej technickej normy

Spracovateľ: Ing. Ivan Makatura, CIRISC, CDPSE, RATIO SERVICES s. r. o., Bratislava

Technická komisia: TK 37 Informačné technológie

Informačné technológie
Bezpečnostné metódy
Návody pre kybernetickú bezpečnosť

ISO/IEC 27032
Prvé vydanie
2012-07

ICS 35.040

Obsah

Contents

Predhovor

ISO (medzinárodná organizácia pre normalizáciu) a IEC (Medzinárodná elektrotechnická komisia) tvoria špecializovaný systém celosvetovej normalizácie. Národné orgány, ktoré sú členmi ISO alebo IEC, sa zúčastňujú na tvorbe medzinárodných noriem prostredníctvom technických komisií zriadených týmito organizáciami pre jednotlivé oblasti technickej činnosti. Technické komisie ISO a IEC vzájomne spolupracujú v oblasti spoločného záujmu. S ISO a IEC spolupracujú aj iné medzinárodné vládne a mimovládne organizácie. V oblasti informačných technológií vytvorili ISO a IEC spoločnú technickú komisiu ISO/IEC JTC 1.

Medzinárodné normy sú vypracované v súlade s redakčnými pravidlami smerníc ISO/IEC, časť 2.

Hlavnou úlohou spoločného technického výboru je príprava medzinárodných noriem. Návrhy medzinárodných noriem prijaté spoločnou technickou komisiou sa rozposielajú národným orgánom na hlasovanie. Publikácia ako medzinárodná norma vyžaduje schválenie najmenej 75 % hlasujúcich národných orgánov.

Upozorňuje sa na možnosť, že niektoré časti tohto dokumentu môžu byť predmetom patentových práv. ISO a IEC nezodpovedajú za identifikáciu ktoréhokoľvek ani všetkých takýchto patentových práv.

ISO/IEC 27032 vypracovala spoločná technická komisia ISO/IEC JTC 1, *Informačné technológie, Podvýbor SC 27, techniky bezpečnosti IT*.

Foreword

ISO (the International Organization for Standardization) and IEC (the International Electrotechnical Commission) form the specialized system for worldwide standardization. National bodies that are members of ISO or IEC participate in the development of International Standards through technical committees established by the respective organization to deal with particular fields of technical activity. ISO and IEC technical committees collaborate in fields of mutual interest. Other international organizations, governmental and non-governmental, in liaison with ISO and IEC, also take part in the work. In the field of information technology, ISO and IEC have established a joint technical committee, ISO/IEC JTC 1.

International Standards are drafted in accordance with the rules given in the ISO/IEC Directives, Part 2.

The main task of the joint technical committee is to prepare International Standards. Draft International Standards adopted by the joint technical committee are circulated to national bodies for voting. Publication as an International Standard requires approval by at least 75 % of the national bodies casting a vote.

Attention is drawn to the possibility that some of the elements of this document may be the subject of patent rights. ISO and IEC shall not be held responsible for identifying any or all such patent rights.

ISO/IEC 27032 was prepared by Joint Technical Committee ISO/IEC JTC 1, *Information technology*, Subcommittee SC 27, *IT Security techniques*.

Úvod

Kyberpriestor je komplexné prostredie, ktoré je výsledkom interakcie ľudí, softvéru a služieb na internete, podporované celosvetovo distribuovanými fyzickými informačnými a komunikačnými technológiami (IKT), zariadeniami a pripojenými sieťami. Existujú však bezpečnostné problémy, ktoré nie sú pokryté najlepšou praxou informačnej bezpečnosti, internetovej bezpečnosti, sieťovej bezpečnosti a bezpečnosti IKT, keďže medzi týmito doménami existujú určité rozdiely. Zároveň je tu aj nedostatočná komunikácia medzi organizáciami a poskytovateľmi v kyberpriestore. To je spôsobené tým, že zariadenia a pripojené siete ktoré podporujú kyberpriestor, majú viacerých vlastníkov a každý z nich má svoje vlastné obchodné, prevádzkové a regulačné záujmy. Rôzne zameranie každej organizácie a poskytovateľa v kyberpriestore v relevantných bezpečnostných doménach, kde sa len minimálne, alebo vôbec neberú do úvahy vstupy od iných organizácií resp. poskytovateľov, má za následok roztrieštený stav bezpečnosti pre kyberpriestor.

Vzhľadom k tomu je základným zameraním tejto medzinárodnej normy venovať sa problémom bezpečnosti kyberpriestoru alebo kyberbernetickej bezpečnosti, ktoré sa sústreďujú na premostenie rozdielov medzi rôznymi bezpečnostnými doménami v kyberpriestore. Konkrétne táto medzinárodná norma poskytuje technické návody pre riešenie bežných kyberbezpečnostných rizík, vrátane:

- útokov za použitia techník sociálneho inžinierstva,
- hekingu,
- šírenia škodlivého softvéru („malvéru“),
- spywaru, a
- iného potenciálne škodlivého softvéru.

Technické usmernenie poskytuje opatrenia na riešenie týchto rizík vrátane opatrení na:

- prípravu na útoky napr. malvéru, individuálnych podvodníkov alebo zločineckých organizácií na internete,
- detekovanie a monitorovanie útokov, a
- reakciu na útoky.

Druhou oblasťou, na ktorú sa táto medzinárodná norma zameriava, je spolupráca, keďže je potrebné úspešné a účinné zdieľanie informácií, koordinácia a riešenie incidentov medzi zainteresovanými stranami v kyberpriestore. Táto spolupráca musí prebiehať bezpečným a spoľahlivým spôsobom, ktorý zároveň chráni súkromie dotknutých osôb.

Introduction

The Cyberspace is a complex environment resulting from the interaction of people, software and services on the Internet, supported by worldwide distributed physical information and communications technology (ICT) devices and connected networks. However there are security issues that are not covered by current information security, Internet security, network security and ICT security best practices as there are gaps between these domains, as well as a lack of communication between organizations and providers in the Cyberspace. This is because the devices and connected networks that have supported the Cyberspace have multiple owners, each with their own business, operational and regulatory concerns. The different focus placed by each organization and provider in the Cyberspace on relevant security domains where little or no input is taken from another organization or provider has resulted in a fragmented state of security for the Cyberspace.

As such, the first area of focus of this International Standard is to address Cyberspace security or Cybersecurity issues which concentrate on bridging the gaps between the different security domains in the Cyberspace. In particular this International Standard provides technical guidance for addressing common Cybersecurity risks, including:

- social engineering attacks,
- hacking,
- the proliferation of malicious software (“malware”),
- spyware, and
- other potentially unwanted software.

The technical guidance provides controls for addressing these risks, including controls for:

- preparing for attacks by, for example, malware, individual miscreants, or criminal organizations on the Internet,
- detecting and monitoring attacks, and
- responding to attacks.

The second area of focus of this International Standard is collaboration, as there is a need for efficient and effective information sharing, coordination and incident handling amongst stakeholders in the Cyberspace. This collaboration must be in a secure and reliable manner that also protects the privacy of the individuals concerned.

Mnohé z týchto zainteresovaných strán môžu sídliť v rôznych geografických oblastiach a časových pásmach a pravdepodobne sa budú riadiť rôznymi regulačnými požiadavkami. Medzi zainteresované strany patria:

– spotrebitelia, ktorými môžu byť rôzne typy organizácií alebo jednotlivcov, a

– poskytovatelia, ku ktorým patria aj poskytovatelia služieb.

Táto medzinárodná norma teda poskytuje aj rámec pre:

– zdieľanie informácií,

– koordináciu, a

– riešenie incidentov.

Rámec zahŕňa:

– kľúčové prvky hľadísk na vytvorenie dôvery,

– potrebné procesy pre spoluprácu a výmeny a zdieľania informácií, ako aj

– technické požiadavky na integráciu systémov a interoperabilitu medzi rôznymi zainteresovanými stranami.

Vzhľadom k rozsahu tejto medzinárodnej normy sú opatrenia nevyhnutne navrhované z nadhľadu. Podrobné technické špecifikácie noriem a návodov platných pre každú oblasť sú uvedené v tejto medzinárodnej norme ako ďalší návod.

Many of these stakeholders can reside in different geographical locations and time zones, and are likely to be governed by different regulatory requirements. Stakeholders include:

– consumers, which can be various types of organizations or individuals, and

– providers, which include service providers.

Thus, this International Standard also provides a framework for:

– information sharing,

– coordination, and

– incident handling.

The framework includes:

– key elements of considerations for establishing trust,

– necessary processes for collaboration and information exchange and sharing, as well as

– technical requirements for systems integration and interoperability between different stakeholders.

Given the scope of this International Standard, the controls provided are necessarily at a high level. Detailed technical specification standards and guidelines applicable to each area are referenced within this International Standard for further guidance.

1 Predmet normy

Táto medzinárodná norma poskytuje návod na zlepšenie stavu kyberbezpečnosti, pričom uvádza jedinečné aspekty tejto činnosti a jej závislosti od iných bezpečnostných domén, najmä:

- informačnej bezpečnosti,
- sieťovej bezpečnosti,
- internetovej bezpečnosti, a
- ochrany kritickej informačnej infraštruktúry (CIIP).

Zahŕňa základné bezpečnostné postupy pre zainteresované strany v kyberpriestore. Táto medzinárodná norma poskytuje:

- prehľad o kyberbezpečnosti,
- vysvetlenie vzťahu medzi kyberbezpečnosťou a inými typmi bezpečnosti,
- definíciu zainteresovaných strán a opis ich úloh v oblasti kyberbezpečnosti,
- usmernenia na riešenie bežných problémov kyberbezpečnosti, a
- rámec umožňujúci zainteresovaným stranám spolupracovať pri riešení problémov kyberbezpečnosti.

1 Scope

This International Standard provides guidance for improving the state of Cybersecurity, drawing out the unique aspects of that activity and its dependencies on other security domains, in particular:

- information security,
- network security,
- internet security, and
- critical information infrastructure protection (CIIP).

It covers the baseline security practices for stakeholders in the Cyberspace. This International Standard provides:

- an overview of Cybersecurity,
- an explanation of the relationship between Cybersecurity and other types of security,
- a definition of stakeholders and a description of their roles in Cybersecurity,
- guidance for addressing common Cybersecurity issues, and
- a framework to enable stakeholders to collaborate on resolving Cybersecurity issues.

2 Použiteľnosť

2.1 Adresáti

Táto medzinárodná norma je uplatniteľná pre poskytovateľov služieb v kyberpriestore. Adresáti však zahŕňajú aj spotrebiteľov, ktorí tieto služby využívajú. Ak organizácie poskytujú služby v kyberpriestore ľuďom na používanie v domácnosti alebo iným organizáciám, títo možno budú potrebovať usmernenie založené na tejto medzinárodnej norme, ktoré bude obsahovať dodatočné vysvetlenia alebo príklady dostatočné na to, aby ich čitateľ pochopil a mohol podľa nich konať.

2.2 Obmedzenia

Táto medzinárodná norma nerieši:

- kyberochranu,
- kyberzločin,
- ochranu kritickej informačnej infraštruktúry (CIIP),
- ochranu na internete, a
- internetovú kriminalitu.

2 Applicability

2.1 Audience

This International Standard is applicable to providers of services in the Cyberspace. The audience, however, includes the consumers that use these services. Where organizations provide services in the Cyberspace to people for use at home or other organizations, they may need to prepare guidance based on this International Standard that contains additional explanations or examples sufficient to allow the reader to understand and act on it.

2.2 Limitations

This International Standard does not address:

- Cybersafety,
- Cybercrime,
- CIIP,
- Internet safety, and
- Internet related crime.

Je všeobecne známe, že medzi uvedenými doménami a kyberbezpečnosťou existuje vzťah. Je však nad rámec tejto medzinárodnej normy zaoberať sa týmito vzťahmi a zdieľaním opatrení medzi týmito oblasťami.

Je dôležité poznamenať, že koncept kyberkriminality, hoci sa spomína, sa tu nerieši. Táto medzinárodná norma neposkytuje návod na právne aspekty kyberpriestoru alebo reguláciu kyberbezpečnosti.

Návod v tejto medzinárodnej norme je obmedzený na realizáciu kyberpriestoru na internete vrátane koncových bodov. Netýka sa však rozšírenia kyberpriestoru na iné priestorové reprezentácie prostredníctvom komunikačných médií a platforiem, ani ich aspekty fyzickej bezpečnosti.

PRÍKLAD 1

Ochrana prvkov infraštruktúry, ako sú komunikačné nosiče, ktoré sú základom kyberpriestoru, nie je riešená.

PRÍKLAD 2

Fyzická bezpečnosť mobilných telefónov, ktoré sa pripájajú do kyberpriestoru z dôvodu sťahovania obsahu a/alebo manipulácie s nimi, nie je riešená.

PRÍKLAD 3

Funkcie textových správ a hlasového četu poskytované pre mobilné telefóny, nie sú riešené.

It is recognized that relationships exist between the domains mentioned and Cybersecurity. It is, however, beyond the scope of this International Standard to address these relationships, and the sharing of controls between these domains.

It is important to note that the concept of Cybercrime, although mentioned, is not addressed. This International Standard does not provide guidance on law-related aspects of the Cyberspace, or the regulation of Cybersecurity.

The guidance in this International Standard is limited to the realization of the Cyberspace on the Internet, including the endpoints. However, the extension of the Cyberspace to other spatial representations through communication media and platforms are not addressed, nor the physical security aspects of them.

EXAMPLE 1

Protection of the infrastructure elements, such as communications bearers, which underpin the Cyberspace are not addressed.

EXAMPLE 2

The physical security of mobile telephones that connect to the Cyberspace for content download and/or manipulation is not addressed.

EXAMPLE 3

Text messaging and voice chat functions provided for mobile telephones are not addressed.

3 Normatívne odkazy

Na nasledujúce dokumenty sa odkazuje v texte takým spôsobom, že časť ich obsahu alebo celý obsah predstavuje požiadavky tohto dokumentu. Pri datovaných odkazoch sa používa len citované vydanie. Pri nedatovaných odkazov sa používa najnovšie vydanie citovaného dokumentu (vrátane akýchkoľvek zmien).

ISO/IEC 27000 Informačné technológie. Bezpečnostné metódy. Systémy riadenia informačnej bezpečnosti. Prehľad a slovník.

3 Normative references

The following documents are referred to in the text in such a way that some or all of their content constitutes requirements of this document. For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments) applies.

ISO/IEC 27000, *Information technology – Security techniques – Information security management systems – Overview and vocabulary*