ICS 35.030 SLOVENSKÁ TECHNICKÁ NORMA Jún 2024

STN	**Kyberbezpečnosť** **Usmernenia pre internetovú bezpečnosť**	**STN** **ISO/IEC 27032** 97 4110

Cybersecurity
Guidelines for Internet security

Cybersécurité
Lignes directrices relatives à la sécurité sur l'internet

Cybersecurity
Leitlinien für die Sicherheit im Internet

Táto slovenská technická norma je slovenskou verziou medzinárodnej normy ISO/IEC 27032: 2023.
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: 2023.
It was translated by Slovak Office of Standards, Metrology and Testing.
STN ISO/IEC 27032 has the same status as the official versions.

Nahradenie predchádzajúcich dokumentov

Táto slovenská technická norma nahrádza STN ISO/IEC 27032 z marca 2023 v celom rozsahu.

138534

Národný predhovor

Obrázky v tejto STN sú prevzaté z elektronických podkladov dodaných z ISO/IEC, © 2023 ISO/IEC, ref. č. ISO/IEC 27032: 2023 E.

Preklad medzinárodnej normy musí získať konsolidovaný význam v obidvoch jazykoch. Nie je vždy možné a žiaduce vykonať preklad odborného kontextu doslovným prekladom, spájaním viet a gramatickými zámenami slov. 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.

Špecifické technické výrazy, ktoré sú aj v anglickom jazyku používané len okrajovo, nedáva význam prekladať do slovenského jazyka a uvádzajú sa v pôvodnom tvare. Prípadne sú u niektorých výrazov ku slovenskému prekladu pridané pôvodné anglické výrazy a naopak.

Ak sa v časti literatúra uvádza taká norma, ktorá je už prevzatá do sústavy STN, je namiesto doslovného prekladu názvu normy použitý jej platný názov, v tvare, v akom bol schválený a publikovaný prostredníctvom portálu noriem ÚNMS.

Niektoré termíny sú preložené v iných normách, ktoré už boli prevzaté do sústavy STN prekladom. Mnohokrát však boli tieto termíny (vrátane ich prípadného použitia v názve normy) preložené nejednoznačne. Ide napríklad o (hrubým písmom je zvýraznená disproporcia na ktorú sa poukazuje):

- STN ISO/IEC 27005: 2023 Informačná bezpečnosť, kybernetická bezpečnosť a ochrana súkromia. **Usmernenie** k riadeniu rizík informačnej bezpečnosti. V niektorých predchádzajúcich verziách noriem 27XXX boli rovnocenne používané preklady „**usmernenie**“ aj „**návod**“ v kontexte termínu „**guidance**“.

V časti literatúra sú uvedené slovenské názvy noriem s názvami, ako boli prevzaté prekladom do sústavy STN. Tieto názvy nie bezpodmienečne lícujú s pôvodnými anglickými názvami nových verzií príslušných noriem ISO/IEC. Z dôvodov zaručenia nadväznosti sú použité novšie, medzičasom opravené slovenské preklady termínov. Ide najmä o nasledujúce:

- STN EN ISO/IEC 27031: 2022 Informačné technológie. Bezpečnostné metódy. Návody pre pripravenosť informačných a komunikačných technológií na zabezpečenie kontinuity činnosti;
- STN EN ISO/IEC 27002: 2023 Informačná bezpečnosť, kybernetická bezpečnosť a ochrana súkromia. Riadenie informačnej bezpečnosti (ISO/IEC 27002: 2022).

Vzhľadom na rozsiahlejšiu slovnú zásobu anglického jazyka majú niektoré výrazy viacnásobný význam, resp. ich preklad by v slovenčine mohol byť nezmyselný. Preto je v týchto prípadoch v preklade použitý ten ekvivalent, ktorý je pre kontext vhodnejší, hoc nie je doslovným prekladom pôvodného výrazu.

V súvislosti s dlhodobo nesprávne interpretovanými pojmami si autor dovolí poukázať na nasledujúce výrazy, ktoré sú v dobrej praxi používané odlišným spôsobom, alebo ktoré nemajú oporu v slovenskom právnom prostredí. V tomto dokumente ide najmä o nasledujúce:

- Consumer – výraz môže mať význam „spotrebiteľ“, aj „zákazník“,
- Exploitations – v informačnej bezpečnosti je výraz chápaný ako „zneužitie“,
- Personnel – výraz chápaný ako „zamestnanci“, „pracovníci“ alebo „osoby“ (nie „personál“),
- Responsibilities – v informačnej bezpečnosti je výraz chápaný ako „zodpovednosti“ (nie „povinnosti“),
- Threat intelligence – v informačnej bezpečnosti je výraz chápaný ako „analýza hrozieb“ (nie „spravodajské informácie o hrozbách“),
- Law enforcement agencies – v slovenskom prostredí je výraz „orgány presadzovania práva“ neobvyklý, ide však o širší pojem, než len „orgány činné v trestnom konaní“.

V tomto dokumente je na niekoľkých miestach v pôvodnej jazykovej verzii normy používaný výraz „dôkaz“, alebo „digitálny dôkaz“. Správnejšie by však bolo používať výraz „stopa“, alebo „digitálna stopa“. Je potrebné zdôrazniť, že výraz „stopa“ označuje jedinečnú množinu vystopovateľných digitálnych aktivít, činností, príspevkov a komunikácie na internete a/alebo pomocou zariadení informačných a komunikačných technológií. Stopa je len indikáciou, ktorá môže viesť k neskoršiemu pochopeniu skutkového stavu a vykonaniu potenciálneho dôkazu pomocou dôkazných prostriedkov. Dôkazom sa stopa stane, až keď súd, vykonávajúci dokazovanie, rozhodne o prípustnosti dôkazov predložených v dôkaznom konaní. Preklad výrazu „evidence“ je však jednoznačne „dôkaz“, nie „stopa“.

Základným cieľom tejto medzinárodnej normy je venovať sa vysvetleniu vzťahu medzi internetovou bezpečnosťou, webovou bezpečnosťou, sieťovou bezpečnosťou a kyberbezpečnosťou, poskytnúť zainteresovaným stranám prehľad v oblasti internetovej bezpečnosti v súvislosti s riešením bežných problémov internetovej bezpečnosti.

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 Úradu pre normalizáciu, metrológiu a skúšobníctvo SR.

Normatívne referenčné dokumenty

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 odkazoch sa používa najnovšie vydanie citovaného dokumentu (vrátane akýchkoľvek 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: RATIO SERVICES s. r. o., Bratislava; Ing. Bc. Ivan Makatura, CRISC, CDPSE

Technická komisia: TK 37 Informačné technológie

Kyberbezpečnosť
Usmernenia pre internetovú bezpečnosť

ISO/IEC 27032
Druhé vydanie
2023-06

Obsah

strana

Predhovor ... 7

Úvod ... 9

1 Predmet ... 11

2 Normatívne odkazy ... 11

3 Termíny a definície ... 11

4 Skrátené výrazy ... 17

5 Vzťah medzi internetovou bezpečnosťou, webovou bezpečnosťou, sieťovou bezpečnosťou a kyberbezpečnosťou ... 18

6 Prehľad internetovej bezpečnosti ... 21

7 Zainteresované strany ... 24

7.1 Všeobecne ... 24

7.2 Používatelia ... 24

7.3 Koordinačné a normalizačné organizácie ... 26

7.4 Vládne orgány ... 26

7.5 Orgány presadzovania práva ... 27

7.6 Poskytovatelia internetových služieb ... 27

8 Posudzovanie a ošetrovanie rizík internetovej bezpečnosti ... 28

8.1 Všeobecne ... 28

8.2 Hrozby ... 28

8.3 Zraniteľnosti ... 30

8.4 Vektory útoku ... 31

Contents

page

Foreword ... 7

Introduction ... 9

1 Scope ... 11

2 Normative references ... 11

3 Terms and definitions ... 11

4 Abbreviated terms ... 17

5 Relationship between Internet security, web security, network security and cybersecurity ... 18

6 Overview of Internet security ... 21

7 Interested parties ... 24

7.1 General ... 24

7.2 Users ... 24

7.3 Coordinator and standardization organi-sations ... 26

7.4 Government authorities ... 26

7.5 Law enforcement agencies ... 27

7.6 Internet service providers ... 27

8 Internet security risk assessment and treatment ... 28

8.1 General ... 28

8.2 Threats ... 28

8.3 Vulnerabilities ... 30

8.4 Attack vectors ... 31

9 Bezpečnostné návody pre internet 33
9.1 Všeobecne 33
9.2 Opatrenia pre internetovú bezpečnosť 34
9.2.1 Všeobecne 34
9.2.2 Politiky internetovej bezpečnosti 35
9.2.3 Riadenie prístupov 35
9.2.4 Vzdelávanie, zvyšovanie povedomia a odborná príprava 36
9.2.5 Riadenie bezpečnostných incidentov 37
9.2.6 Správa aktív 39
9.2.7 Riadenie dodávateľov 40
9.2.8 Kontinuita činností cez internet 42
9.2.9 Ochrana súkromia na internete 43
9.2.10 Riadenie zraniteľnosti 44
9.2.11 Správa siete 45
9.2.12 Ochrana pred malvérom 47
9.2.13 Riadenie zmien 49
9.2.14 Identifikácia uplatniteľných právnych predpisov a požiadavky na súlad 50
9.2.15 Používanie kryptografie 50
9.2.16 Aplikačná bezpečnosť pre aplikácie orientované na internet 51
9.2.17 Správa koncového zariadenia 54
9.2.18 Monitorovanie 55

Príloha A (informatívna) – Krížové odkazy medzi týmto dokumentom a normou ISO/IEC 27002 56

Literatúra 61

9 Security guidelines for the Internet 33
9.1 General 33
9.2 Controls for Internet security 34
9.2.1 General 34
9.2.2 Policies for Internet security 35
9.2.3 Access control 35
9.2.4 Education, awareness and training 36
9.2.5 Security incident management 37
9.2.6 Asset management 39
9.2.7 Supplier management 40
9.2.8 Business continuity over the Internet 42
9.2.9 Privacy protection over the Internet 43
9.2.10 Vulnerability management 44
9.2.11 Network management 45
9.2.12 Protection against malware 47
9.2.13 Change management 49
9.2.14 Identification of applicable legislation and compliance requirements 50
9.2.15 Use of cryptography 50
9.2.16 Application security for Internet-facing applications 51
9.2.17 Endpoint device management 54
9.2.18 Monitoring 55

Annex A (informative) – Cross-references between this document and ISO/IEC 27002 56

Bibliography 61

Predhovor

ISO (Medzinárodná organizácia pre normalizáciu) a IEC (Medzinárodná elektrotechnická komisia) tvoria špecializovaný systém celosvetovej normalizácie. Národné orgány, ktoré sú členmi ISO alebo IEC, zúčastňujú sa 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.

Postupy použité pri tvorbe tohto dokumentu ako aj tie, ktoré sú určené na jeho ďalšie udržiavanie sú opísané v časti 1 smerníc ISO/IEC. Mali by sa uviesť najmä rôzne kritériá schvaľovania, ktoré sú potrebné pre rôzne typy dokumentov. Tento dokument bol vypracovaný podľa edičných pravidiel smernice ISO/IEC, Časť 2 (pozri www.iso.org/directives alebo www.iec.ch/members_experts/refdocs).

ISO a IEC upozorňujú na možnosť, že vykonávanie tohto dokumentu môže zahŕňať používanie patentu (patentov). ISO a IEC nezastávajú žiadne stanovisko, pokiaľ ide o dôkazy, platnosť alebo uplatniteľnosť akýchkoľvek nárokovaných patentových práv v súvislosti s nimi. K dátumu uverejnenia tohto dokumentu ISO a IEC nedostali oznámenie o patente(-och), od ktorého(-ých) sa môže vyžadovať vykonanie tohto dokumentu. Upozorňujeme však, že to nemusí predstavovať najnovšie informácie, ktoré možno získať z patentovej databázy dostupnej na www.iso.org/patents a https://patents.iec.ch. ISO a IEC nezodpovedajú za identifikáciu ktorýchkoľvek, alebo všetkých takýchto patentových práv.

Akýkoľvek obchodný názov použitý v tomto dokumente slúži len na informáciu pre používateľa a neznamená jeho schválenie.

Vysvetlenie dobrovoľnej povahy noriem, významu špecifických pojmov a výrazov ISO týkajúcich sa posudzovania zhody, ako aj informácií o väzbe ISO na princípy Svetovej obchodnej organizácie (WTO) uplatňované pri odstraňovaní technických prekážok obchodu (TBT), pozri na www.iso.org/ iso/foreword.html. V IEC pozri www.iec.ch/ understanding-standards.

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.

The procedures used to develop this document and those intended for its further maintenance are described in the ISO/IEC Directives, Part 1. In particular, the different approval criteria needed for the different types of document should be noted. This document was drafted in accordance with the editorial rules of the ISO/IEC Directives, Part 2 (see www.iso.org/directives or www.iec.ch/members_experts/refdocs).

ISO and IEC draw attention to the possibility that the implementation of this document may involve the use of (a) patent(s). ISO and IEC take no position concerning the evidence, validity or applicability of any claimed patent rights in respect thereof. As of the date of publication of this document, ISO and IEC had not received notice of (a) patent(s) which may be required to implement this document. However, implementers are cautioned that this may not represent the latest information, which may be obtained from the patent database available at www.iso.org/patents and https://patents.iec.ch. ISO and IEC shall not be held responsible for identifying any or all such patent rights.

Any trade name used in this document is information given for the convenience of users and does not constitute an endorsement.

For an explanation of the voluntary nature of standards, the meaning of ISO specific terms and expressions related to conformity assessment, as well as information about ISO's adherence to the World Trade Organization (WTO) principles in the Technical Barriers to Trade (TBT) see www.iso.org/iso/foreword.html. In the IEC, see www.iec.ch/understanding-standards.

Tento dokument vypracovala spoločná technická komisia ISO/IEC JTC 1, Informačné technológie, subkomisia SC 27, Informačná bezpečnosť, kyberbezpečnosť a ochrana súkromia.

Toto druhé vydanie ruší a nahrádza prvé vydanie (ISO/IEC 27032: 2012), ktoré bolo technicky revidované.

Hlavné zmeny sú tieto:

- upravený bol názov;
- zmenila sa štruktúra dokumentu;
- zmenil sa prístup k posudzovaniu a ošetreniu rizika, pridaním obsahu o hrozbách, zraniteľnostiach a vektoroch útokov s cieľom identifikovať a riadiť riziká internetovej bezpečnosti;
- do prílohy A sa doplnilo mapovanie medzi opatreniami internetovej bezpečnosti uvedenými v bode 9.2 a opatreniami uvedenými v norme ISO/IEC 27002.

Akákoľvek spätná väzba alebo otázky k tomuto dokumentu sa majú adresovať národnému normalizačnému orgánu používateľa. Kompletný zoznam týchto orgánov nájdete na:

www.iso.org/members.html

a www.iec.ch/national-committees.

This document was prepared by Joint Technical Committee ISO/IEC JTC 1, Information technology, Subcommittee SC 27, Information security, cybersecurity and privacy protection.

This second edition cancels and replaces the first edition (ISO/IEC 27032:2012) which has been technically revised.

The main changes are as follows:

- the title has been modified;
- the structure of the document has been changed;
- the risk assessment and treatment approach has been changed, with the addition of content on threats, vulnerabilities and attack vectors to identify and manage the Internet security risks;
- a mapping between the controls for Internet security cited in 9.2 and the controls contained in ISO/IEC 27002 has been added to Annex A.

Any feedback or questions on this document should be directed to the user's national standards body. A complete listing of these bodies can be found at

www.iso.org/members.html

and www.iec.ch/national-committees.

Úvod

Cieľom tohto dokumentu je riešiť otázky internetovej bezpečnosti a poskytnúť návody na riešenie spoločných hrozieb pre internetovú bezpečnosť, ako sú:

- útoky v oblasti sociálneho inžinierstva;
- útoky nulového dňa;
- útoky na ochranu súkromia;
- hekerské útoky; a
- šírenie škodlivého softvéru (malvéru), špionážneho softvéru a iného potenciálne nežiaduceho softvéru.

Návody v rámci tohto dokumentu poskytujú technické a netechnické opatrenia na riešenie bezpečnostných rizík na internete vrátane opatrení ohľadom:

- prípravy na útoky;
- predchádzania útokom;
- odhaľovania a monitorovania útokov; a
- reakcie na útoky.

Návod sa zameriava na poskytovanie odvetvovo osvedčených postupov, rozsiahleho vzdelávania spotrebiteľov a zamestnancov s cieľom pomôcť zainteresovaným stranám zohrávať aktívnu rolu pri riešení výziev v oblasti internetovej bezpečnosti. Dokument sa zameriava aj na zachovanie dôvernosti, integrity a dostupnosti informácií cez internet a iných vlastností, ako je pravosť, zodpovednosť, nespochybniteľnosť a spoľahlivosť, ktoré taktiež môžu byť zahrnuté.

To zahŕňa návody týkajúce sa internetovej bezpečnosti pre:

- roly;
- politiky;
- metódy;
- procesy; a
- uplatniteľné technické opatrenia.

Vzhľadom na predmet tohto dokumentu sú navrhované opatrenia nevyhnutne opísané na vysokej úrovni. V dokumente sú ako ďalší návod uvedené normy s podrobnou technickou špecifikáciou a návodmi uplatniteľnými na každú oblasť. Zhoda medzi opatreniami uvedenými v tomto dokumente a opatreniami uvedenými v norme ISO/IEC 27002 je uvedená v prílohe A.

Introduction

The focus of this document is to address Internet security issues and provide guidance for addressing common Internet security threats, such as:

- social engineering attacks;
- zero-day attacks;
- privacy attacks;
- hacking; and
- the proliferation of malicious software (malware), spyware and other potentially unwanted software.

The guidance within this document provides technical and non-technical controls for addressing the Internet security risks, including controls for:

- preparing for attacks;
- preventing attacks;
- detecting and monitoring attacks; and
- responding to attacks.

The guidance focuses on providing industry best practices, broad consumer and employee education to assist interested parties in playing an active role to address the Internet security challenges. The document also focuses on preservation of confidentiality, integrity and availability of information over the Internet and other properties, such as authenticity, accountability, non-repudiation and reliability that can also be involved.

This includes Internet security guidance for:

- roles;
- policies;
- methods;
- processes; and
- applicable technical controls.

Given the scope of this document, the controls provided are necessarily at a high-level. Detailed technical specification standards and guidelines applicable to each area are referenced within the document for further guidance. See Annex A for the correspondence between the controls cited in this document and those in ISO/IEC 27002.

Tento dokument sa osobitne nezaoberá opatreniami, ktoré môžu organizácie požadovať pre systémy podporujúce kritickú infraštruktúru alebo národnú bezpečnosť. Na takéto systémy sa však môže uplatniť väčšina opatrení uvedených v tomto dokumente.

V tomto dokumente sa používajú existujúce koncepty z ISO/IEC 27002, série ISO/IEC 27033, ISO/IEC TS 27100 a ISO/IEC 27701 na ilustráciu:

- vzťahu medzi internetovou bezpečnosťou, webovou bezpečnosťou, sieťovou bezpečnosťou a kyberbezpečnosťou;
- podrobné usmernenia o opatreniach internetovej bezpečnosti uvedené v bode 9.2, ktoré sa zaoberajú kyberbezpečnostnou pripravenosťou systémov orientovaných na internet.

Ako sa uvádza v norme ISO/IEC TS 27100, internet je globálna sieť, ktorú organizácie používajú na všetku komunikáciu, či už digitálnu, alebo hlasovú. Vzhľadom na to, že niektorí používatelia sa zameriavajú na útoky na tieto siete, je kriticky nevyhnutné riešiť príslušné bezpečnostné riziká.

This document does not specifically address controls that organizations can require for systems supporting critical infrastructure or national security. However, most of the controls mentioned in this document can be applied to such systems.

This document uses existing concepts from ISO/IEC 27002, the ISO/IEC 27033 series, ISO/IEC TS 27100 and ISO/IEC 27701, to illustrate:

- the relationship between Internet security, web security, network security and cybersecurity;
- detailed guidance on Internet security controls cited in 9.2, addressing cybersecurity readiness for Internet-facing systems.

As mentioned in ISO/IEC TS 27100, the Internet is a global network, used by organizations for all communications, both digital and voice. Given that some users target attacks towards these networks, it is critical to address the relevant security risks.

1 Predmet

V tomto dokumente sa uvádza:

- vysvetlenie vzťahu medzi internetovou bezpečnosťou, webovou bezpečnosťou, sieťovou bezpečnosťou a kyberbezpečnosťou;
- prehľad internetovej bezpečnosti;
- identifikácia zainteresovaných strán a opis ich rolí v oblasti internetovej bezpečnosti;
- návody na vysokej úrovni na riešenie spoločných otázok internetovej bezpečnosti.

Tento dokument je určený pre organizácie, ktoré používajú internet.

1 Scope

This document provides:

- an explanation of the relationship between Internet security, web security, network security and cybersecurity;
- an overview of Internet security;
- identification of interested parties and a description of their roles in Internet security;
- high-level guidance for addressing common Internet security issues.

This document is intended for organizations that use the Internet.

2 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 odkazoch sa používa najnovšie vydanie citovaného dokumentu (vrátane akýchkoľvek zmien).

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

2 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