ICS 35.030 SLOVENSKÁ TECHNICKÁ NORMA September 2026

STN	**Informačná bezpečnosť, kybernetická bezpečnosť a ochrana súkromia Model a metóda operacionalizácie inžinierstva ochrany súkromia (POMME)**	**STN ISO/IEC 27561** 97 4238

Information security, cybersecurity and privacy protection
Privacy operationalisation model and method for engineering
(POMME)

Sécurité de l'information, cybersécurité et protection de la vie privée
Méthode et modèle d'opérationnalisation de la confidentialité pour l'ingénierie
(POMME)

Táto slovenská technická norma je slovenskou verziou medzinárodnej normy ISO/IEC 27561: 2024.
Preklad zabezpečil Úrad pre normalizáciu, metrológiu a skúšobníctvo Slovenskej republiky.
STN ISO/IEC 27561 má rovnaké postavenie, ako majú oficiálne verzie.

This standard is the Slovak version of the International Standard ISO/IEC 27561: 2024.
It was translated by Slovak Office of Standards, Metrology and Testing.
STN ISO/IEC 27561 has the same status as the official versions.

142996

Národný predhovor

Obrázky a matematické výrazy v tejto STN sú prevzaté z elektronických podkladov dodaných z ISO/IEC, © 2024 ISO/IEC, ref. č. ISO/IEC 27561: 2024 E.

Táto STN obsahuje jednu národnú poznámku.

Normatívne referenčné dokumenty

Táto slovenská technická norma neobsahuje normatívne referenčné dokumenty.

Vypracovanie

Spracovateľ: Ing. Lenka Gondová, SynCo s.r.o., Bratislava

Technická komisia: TK 37 Informačné technológie

Informačná bezpečnosť, kybernetická bezpečnosť a ochrana súkromia
Model a metóda operacionalizácie inžinierstva ochrany súkromia (POMME)

ISO/IEC 27561
Prvé vydanie
2024-03

ICS 35.030

Obsah

strana

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 alebo mimovládne organizácie.

Postupy použité pri tvorbe tohto dokumentu, ako aj tie, ktoré sú určené na jeho ďalšie udržiavanie sú opísané v smernici ISO/IEC, Časť 1. Do úvahy sa majú zobrať najmä rozdielne kritériá schvaľovania pri rôznych typoch dokumentov ISO. 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 uplatňovanie tohto dokumentu môže zahŕňať použitie patentu/patentov. V súvislosti s tým ISO a IEC nezaujíma žiadne stanovisko týkajúce sa dôkazu, platnosti alebo použiteľnosti akýchkoľvek nárokovaných patentových práv. Ku dňu zverejnenia tohto dokumentu ISO a IEC nedostali oznámenie o patente/patentoch, ktoré môžu byť potrebné na používanie tohto dokumentu. Používatelia sú však upozornení na skutočnosť, že toto nemusia byť najnovšie informácie, ktoré možno získať z patentovej databázy dostupnej na www.iso.org/patents a https://patents.iec.ch. ISO a IEC nenesú zodpovednosť za identifikáciu ktoréhokoľvek alebo všetkých takýchto patentových práv.

Akákoľvek obchodná značka použitá v tomto dokumente slúži len na informáciu pre používateľa a neznamená jeho schválenie.

Vysvetlenie dobrovoľného charakteru noriem, významu špecifických termínov a výrazov 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. Pre IEC pozri na www.iec.ch/understanding-standards.

Tento dokument vypracovala spoločná technická komisia ISO/IEC JTC 1 *Informačné technológie*.

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.

Úvod

Zásady ochrany súkromia a súvisiace požiadavky na opatrenia na riadenie ochrany súkromia čelia viacerým výzvam vyplývajúcim z potreby dodržiavať očakávania spotrebiteľov a globálne predpisy v oblasti ochrany súkromia, ktoré sa neustále vyvíjajú, ako aj zo zložitého a rýchlo sa meniaceho ekosystému zariadení, sietí a aplikácií, prostredníctvom ktorých prúdia osobné údaje (PII). Aby bolo možné čeliť týmto výzvam, očakáva sa, že zásady ochrany súkromia a súvisiace požiadavky na opatrenia na riadenie ochrany súkromia budú implementované do súborov funkcií a mechanizmov. Model a metóda operacionalizácie ochrany súkromia pre inžinierstvo (POMME) rieši tieto výzvy, najmä v prepojených a vzájomne závislých aplikáciách a rýchlych procesoch vývoja životného cyklu.

Dosiahnutie účinnej implementácie v tomto prostredí je kľúčovou zodpovednosťou inžinierov v oblasti ochrany súkromia a vývojárov a poskytovateľov riešení, ktorí ich podporujú. Pri navrhovaní týchto systémov by mali nielen rozumieť technologickým rozhraniam a vzájomným závislostiam medzi komponentmi, ale aj zabezpečiť, aby boli vybrané a implementované primerané opatrenia ochrany súkromia v celom prostredí toku údajov relevantnom pre ich analýzu.

POMME poskytuje štruktúrovaný a rozširovateľný analytický model a metódu na dosiahnutie týchto cieľov. Je založený na referenčnom modeli a metodike riadenia ochrany súkromia OASIS (PMRM) [1] a odráža zistenia uvedené v norme ISO/IEC TR 27550, ktorá poskytuje rozsiahle informácie o inžinierstve ochrany súkromia, ktoré organizácie môžu využiť na integráciu inžinierstva ochrany súkromia do procesov životného cyklu systému. Opisuje tiež vzťah medzi inžinierstvom ochrany súkromia a inými pohľadmi na inžinierstvo (systémové inžinierstvo, bezpečnostné inžinierstvo a riadenie rizík).

POMME podporuje operacionalizáciu ochrany súkromia, ako je definovaná v norme ISO/IEC 29100, s využitím procesu podľa normy ISO/IEC/IEEE 24774. POMME sa zameriava predovšetkým na funkčnú architektúru a podrobnosti implementácie inžinierstva ochrany súkromia, a nie na „politické“ aspekty ochrany súkromia, ako sú zásady ochrany súkromia, posúdenia vplyvu na ochranu súkromia (PIA) a vyhlásenia o opatreniach na ochranu súkromia. Tieto politické prvky sú nevyhnutnými vstupmi do inžinierskeho procesu a sú už riešené existujúcimi normami, kódexmi postupov a usmerneniami uvedenými v literatúre. POMME využíva tieto prvky na podporu funkčnej úlohy inžiniera ochrany súkromia.

Vďaka použitiu POMME môže inžinier ochrany súkromia definovať doménové hranice cieľa analýzy (TOA) a výskumu, dokumentovať a organizovať informácie (napr. normy, politiky ochrany súkromia a technické údaje). Týmto spôsobom je možné identifikovať schopnosti potrebné na implementáciu požiadaviek opatrení na riadenie ochrany súkromia. To umožňuje inžinierovi ochrany súkromia:

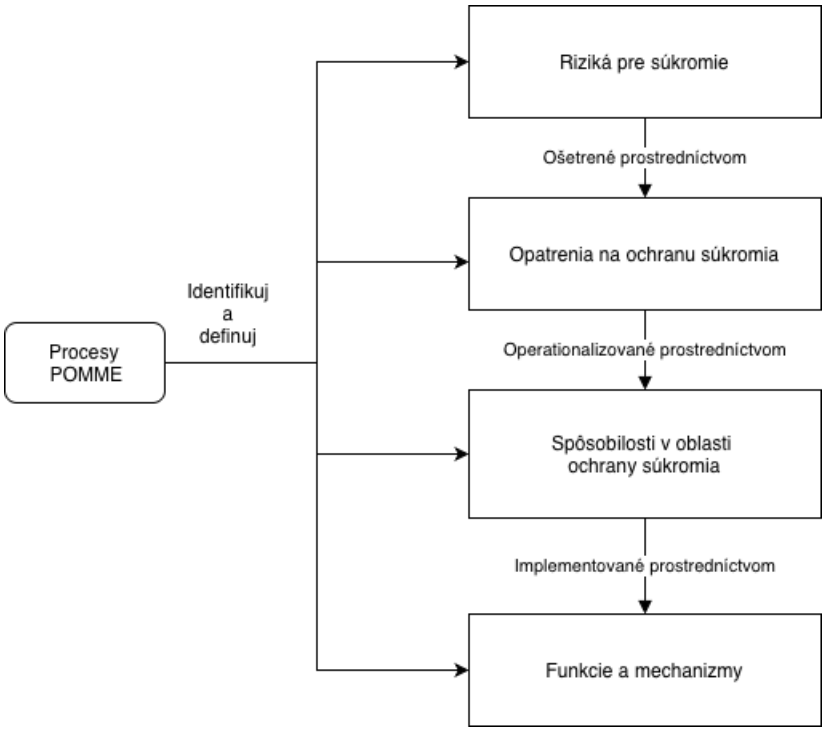
a) určiť funkcie potrebné na implementáciu požiadaviek na opatrenia na riadenie ochrany súkromia;

b) pochopiť vzťahy medzi opatreniami, najmä ak sú opatrenia vzájomne závislé alebo prepojené v sieti alebo založené na cloude;

c) vybrať konkrétne implementačné mechanizmy (napr. konfigurácie kódu alebo produktu), ktoré zabezpečujú požadované opatrenia na ochranu súkromia v prevádzkovom stave.

Ďalšou výhodou POMME je, že jeho štruktúrované procesy podporujú lepšie využívanie a integráciu nástrojov na riadenie ochrany súkromia, ako je napríklad open source softvér špecifický pre ochranu súkromia.

Obrázok 1 a tabuľka 1 ilustrujú model a metódu operacionalizácie POMME.



Obrázok 1 – Model operacionalizácie POMME

Tabuľka 1 obsahuje proces inventarizácie, ktorý pozostáva z ôsmich činností a proces operacionalizácie, ktorý pozostáva z piatich činností.

Tabuľka 1 – Metóda POMME

Proces POMME	Článok	Činnosť
Proces počiatočného inventarizovania informácií	6.3	Definovanie a popis TOA
	6.4	Identifikácia účastníkov a zdrojov informácií
	6.5	Identifikácia systémov a procesov
	6.6	Identifikácia domén a vlastníkov domén
	6.7	Identifikácia rolí a zodpovedností v rámci domény
	6.8	Identifikácia kontaktných bodov
	6.9	Identifikácia tokov údajov
	6.10	Identifikácia osobných identifikačných údajov
Opatrenia ochrany súkromia, požiadavky na riadenie ochrany súkromia, schopnosti, hodnotenie rizík a iterácia	7.3	Špecifikácia opatrení na ochranu súkromia
	7.4	Špecifikácia požiadaviek na opatrenie na ochranu súkromia
	7.5	Špecifikácia schopností
	7.6	Hodnotenie rizík
	7.7	Iterácia

1 Predmet

Tento usmerňovací dokument opisuje model a metódu na zavedenie zásad ochrany súkromia špecifikovaných v norme ISO/IEC 29100 do súboru opatrení a funkčných schopností. Metóda je opísaná ako proces, ktorý vychádza z normy ISO/IEC/IEEE 24774.

Tento dokument je určený na použitie v spojení s príslušnými normami a usmerneniami v oblasti ochrany súkromia a bezpečnosti, ktoré majú vplyv na implementáciu ochrany súkromia. Podporuje sieťové, vzájomne závislé aplikácie a systémy. Tento dokument je určený pre inžinierov a ďalších odborníkov, ktorí vyvíjajú systémy na riadenie alebo spracovanie osobných údajov (PII).

2 Normatívne odkazy

V tomto dokumente nie sú normatívne odkazy.

*) NÁRODNÁ POZNÁMKA 1. – Zaužívaný preklad osobné údaje, skratka „PII“, ďalej len „osobné údaje“.