

INFOTEHNOLOOGIA

Turbemeetodid

Infoturbe halduse süsteemid

Ülevaade ja sõnavara

Information technology

Security techniques

Information security management systems

Overview and vocabulary

(ISO/IEC 27000:2009)

EESTI STANDARDI EESSÕNA

Käesolev Eesti standard:

- on rahvusvahelise standardi ISO/IEC 27000:2009 "Information technology - Security techniques - Information security management systems - Overview and vocabulary" ingliskeelse teksti identne tõlge eesti keelde ning tõlgendamise erimeelsuste korral tuleb lähtuda ametlikes keeltes avaldatud tekstidest,
- on kinnitatud Eesti Standardikeskuse 05.08.2010 käskkirjaga nr 140,
- jõustub sellekohase teate avaldamisel EVS Teataja 2010. aasta septembrikuu numbris.

Standardi tõlkis Cybernetica AS, standardi tõlke on heaks kiitnud EVS/TK 4 "Infotehnoloogia".

Standardi tõlke koostamisetööpaneku esitas EVS/TK 4, standardi tõlkimist korraldas Eesti Standardikeskus ning rahastas Majandus- ja Kommunikatsiooniministeerium.

Standardi eestikeelses väljaandes on terminid ja määratlused, mis toetuvad ISO/IEC juhendile 73, viidud vastavusse selle juhendi uustõlkega aastast 2009 ja vastavates kohtades on esitatud nurksulgudes viide sellele juhendile [ISO juhend 73:2009]. Nimetatud juhendi eestikeelne väljaanne on tähisega ISO juhend 73:2009.

See dokument on EVS-i poolt loodud eelvaade

01.040.35 Infotehnoloogia. Kontoriseadmed (sõnavara); 35.040 Märgistikud ja informatsiooni kodeerimine
Võtmesõnad: infotehnoloogia, arvutivõrk, infoturve, infoturbe haldus, sõnastik
Hinnagrupp K

Standardite reprodutseerimis- ja levitamiseõigus kuulub Eesti Standardikeskusele

Andmete paljundamine, taastekitamine, kopeerimine, salvestamine elektroonilisse süsteemi või edastamine ükskõik millises vormis või millisel teel on keelatud ilma Eesti Standardikeskuse poolt antud kirjaliku loata.

Kui Teil on küsimusi standardite autorikaitse kohta, palun võtke ühendust Eesti Standardikeskusega:
Aru 10 Tallinn 10317 Eesti; www.evs.ee; Telefon: 605 5050; E-post: info@evs.ee

SISUKORD

EESSÕNA	II
0 SISSEJUHATUS	II
0.1 Ülevaade	II
0.2 ISMS-i standardipere	II
0.3 Selle standardi eesmärk	III
1 KÄSITLUSALA	1
2 TERMINID JA MÄÄRATLUSED	1
3 INFOTURBE HALDUSE SÜSTEEMID (ISMS)	6
3.1 Sissejuhatus	6
3.2 Mis on ISMS	6
3.3 Protsessimeetod	8
3.4 ISMS-i tähtsus	8
3.5 ISMS-i rajamine, seire, käigushoid ja täiustamine	9
3.6 ISMS-i kriitilised edutegurid	10
3.7 ISMS-i standardite pere kasulikkus	11
4 ISMS-I STANDARDIPERE	11
4.1 Üldteavet	11
4.2 Ülevaadet ja terminoloogiat kirjeldavad standardid	13
4.3 Nõudeid spetsifitseerivad standardid	13
4.4 Üldjuhiseid kirjeldavad standardid	13
4.5 Sektorispetsiifilisi juhiseid kirjeldavad standardid	14
Lisa A (teatmelisa) Tingimuste väljendamise verbivormid	16
Lisa B (teatmelisa) Terminid liigendatult	17
Kasutatud kirjandus	19

EESSÕNA

ISO (Rahvusvaheline Standardiorganisatsioon) ja IEC (Rahvusvaheline Elektrotehnikakomisjon) moodustavad ülemaailmse standardimise spetsialiseeritud süsteemi. ISO või IEC rahvuslikud liikmeskogud osalevad rahvusvaheliste standardite väljatöötamises tehniliste komiteede kaudu, mis on nendesse organisatsioonidesse loodud käsitlemaks tehnilise tegevuse eri valdkondi. ISO ja IEC tehnilised komiteed teevad koostööd mõlemale huvi pakkuvatel aladel. Selles töös osalevad käsikäes ISO ja IEC-ga ka muud rahvusvahelised riiklikud ja mitteriiklikud organisatsioonid. Infotehnoloogia valdkonnas on ISO ja IEC rajanud ühise tehnilise komitee ISO/IEC JTC 1.

Rahvusvahelised standardid kavandatakse vastavalt ISO/IEC direktiivide teises osas esitatud reeglitele.

Ühise tehnilise komitee peavõõrand on rahvusvaheliste standardite koostamine. Ühises tehnilises komitees vastuvõetud rahvusvahelised standardikavandid saadetakse liikmeskogudele hääletamiseks. Avaldamine rahvusvahelise standardina nõuab heakskiitu vähemalt 75% hääletanud rahvuslikelt liikmesorganisatsioonidelt.

Tuleb pöörata tähelepanu võimalusele, et mõned selle dokumendi elemendid võivad olla patendiõiguse objektiks. ISO ega IEC ei ole kohustatud mingeid või kõiki selliseid patendiõigusi välja selgitama.

ISO/IEC 27000 valmistas ette ühise tehnilise komitee ISO/IEC JTC 1 "Infotehnoloogia" alamkomitee SC 27 "Infoturbe meetodid".

0 SISSEJUHATUS

0.1 Ülevaade

Haldussüsteemide standardid annavad mudeli, mida järgida haldussüsteemi rajamisel ja käitamisel. See mudel sisaldab neid aspekte, mida ala asjatundjad peavad üksmeelselt ala praeguseks rahvusvaheliseks arengutasemeks. ISO/IEC JTC 1 SC 27 juures tegutses ekspertkomisjon, mis on spetsialiseerunud haldussüsteemide rahvusvaheliste standardite väljatöötamisele infoturbe alal; need standardid moodustavad infoturbe halduse süsteemide (ISMS) standardipere.

ISMS-i standardipere abil saavad organisatsioonid välja töötada ja realiseerida raamstruktuuri oma infovarade halduseks ning valmistada oma ISMS-ile, mida rakendatakse rahandusteabe, intellektuaalse omandi, töötajate isikuandmete, klientidelt või kolmandatelt pooltelt organisatsioonile usaldatud teabe ja muu sellise teabe kaitseks, sõltumatu hinnangu saamiseks.

0.2 ISMS-i standardipere

ISMS-i standardipere¹ on mõeldud abistama igat liiki ja igas suuruses organisatsioone ISMS-i teostamisel ja käigushoiul. ISMS-i standardipere koosneb järgmistest standarditest üldpealkirjaga "Infotehnoloogia. Turbemeetodid".

- ISO/IEC 27000:2009, *Infoturbe halduse süsteemid. Ülevaade ja sõnavara*
- ISO/IEC 27001:2005, *Infoturbe halduse süsteemid. Nõuded*
- ISO/IEC 27002:2005, *Infotehnoloogia. Turbemeetodid. Infoturbe halduse tegevusjuhised*
- ISO/IEC 27003, *Infoturbe halduse süsteemi teostusjuhised*
- ISO/IEC 27004, *Infoturbe haldus. Mõõtmine*

¹ Selles jaotises ilma väljaandmise ajata viidatud standardid on alles väljatöötamisel.

- ISO/IEC 27005:2008, *Infoturvariski haldus*
- ISO/IEC 27006:2007, *Nõuded infoturbe halduse süsteeme auditeerivatele ja sertifitseerivatele asutustele*
- ISO/IEC 27007, *Infoturbe halduse süsteemide auditeerimise juhised*
- ISO/IEC 27011, *Standardil ISO/IEC 27002 põhinevad infoturbe halduse juhised sideala organisatsioonidele*

MÄRKUS Üldpealkiri "Infotehnoloogia. Turbemeetodid" näitab, et need standardid koostas ühise tehnilise komitee ISO/IEC JTC 1, "Infotehnoloogia", alamkomitee SC 27, "Infoturbe meetodid".

ISMS-i standardiperesse kuulub ilma selle üldpealkirjata järgmine standard:

- ISO 27799:2008, *ISO 27799:2008. Tervishoiuinformaatika. Infoturbe haldus standardiga ISO/IEC 27002 tervishoiualal*

0.3 Selle standardi eesmärk

See standard annab ülevaate ISMS-i standardipere teemaks olevatest infoturbe halduse süsteemidest ja määratleb nendega seotud terminid.

MÄRKUS Lisa A selgitab, kuidas ISMS-i standardiperes kasutatakse verbivorme nõuete ja/või juhiste väljendamiseks.

ISMS-i standardiperesse kuuluvad standardid, mis

- a) määratlevad nõuded ISMS-ile ja selliste süsteemide sertifitseerijaile;
- b) annavad otsest tuge, detailseid juhiseid ja/või tõlgendusi kogu PCDA-protsessistiku (PCDA: plaanida, teha, kontrollida, tegutseda) ja nõudestiku tarbeks;
- c) arvestavad ISMS-i puhul sektorispetsiifilisi juhiseid;
- d) käsitlevad ISMS-i vastavuse hindamist.

Selles standardis kasutatud terminid ja määratlused:

- hõlmavad ISMS-i standardiperes üldkasutatavaid termineid ja määratlusi;
- ei hõlma kõiki ISMS-i standardiperes kasutatavaid termineid ja määratlusi;
- ei kitsenda ISMS-i standardiperes terminite määratlemist sinna kuuluva standardi otstarbeks.

ISMS-i standardiperest on jäetud välja standardid, mis käsitlevad ainult turvameetmete teostamist, erinevalt kõigi ISO/IEC 27002 meetmete käsitlesest.

ISMS-i standardipere muutuva seisu kajastamiseks kavatakse käesolevat standardit pidevalt uuendada sagedamini kui muid ISO/IEC standardeid.

1 KÄSITLUSALA

Käesolev standard annab

- a) ülevaate ISMS-i standardiperest;
- b) sissejuhatuse infoturbe halduse süsteemidesse (ISMS);
- c) PDCA-protsessi ("plaanida, teha, kontrollida, tegutseda") lühikirjelduse;
- d) terminid ja määratlused ISMS-i standardiperes kasutamiseks.

See standard on rakendatav igat liiki organisatsioonides (näiteks äriettevõtetes, riigiasutustes, mitte-tulunduslikes organisatsioonides).

2 TERMINID JA MÄÄRATLUSED

Standardi rakendamisel kasutatakse järgmisi termineid ja määratlusi.

MÄRKUS Määratluses või märkuses on paksu kirjaga ja sellele järgneva kirjenumbriga sulgudes tähistatud termin, mis on määratletud mujal selles jaotises. Täieliku määratluse saamiseks saab sellise paksus kirjas termini asendada tema määratlusega.

Näide:

rünne (2.4) on määratletud kui "katse hävitada, paljastada, muuta, blokeerida või varastada mingit **vara** (2.3) või saada talle volitamatu juurdepääs või kasutada teda volitamatult";

vara on määratletud kui "miski, millel on organisatsiooni jaoks väärtus".

Termini "**vara**" asendamisel ta määratlusega

on **rünne** nüüd "katse hävitada, paljastada, muuta, blokeerida või varastada midagi, millel on organisatsiooni jaoks väärtus, või saada talle volitamatu juurdepääs või kasutada teda volitamatult".

2.1

pääsu reguleerimine

vahendid, millega tagada, et juurdepääs **varadele** (2.3) on volitatud ja kutsendatud äri- ja turvanõuete põhjal

2.2

jälitatavus

olemi vastutus oma toimingute ja otsuste eest

2.3

vara

miski, millel on organisatsiooni jaoks väärtus

MÄRKUS Varade tüüpe on palju, sealhulgas järgmised:

- a) **infovara** (2.18);
- b) tarkvara, näiteks arvutiprogramm;
- c) füüsiline vara, näiteks arvuti;
- d) teenused;
- e) inimesed ning nende kvalifikatsioon, oskused ja kogemused;