Avaldatud eesti keeles: mai 2020
Jõustunud Eesti standardina: mai 2020

INFOTEHNOLOOGIA
Turbemeetodid
Infoturbe hindamise kriteeriumid
Osa 1: Sissejuhatus ja üldmudel

Information technology
Security techniques
Evaluation criteria for IT security
Part 1: Introduction and general model
(ISO/IEC 15408-1:2009)

EESTI STANDARDIKESKUS
ESTONIAN CENTRE FOR STANDARDISATION

EESTI STANDARDI EESSÕNA

See Eesti standard on

— Euroopa standardi EN ISO/IEC 15408-1:2020 ingliskeelse teksti sisu poolest identne tõlge eesti keelde ja sellel on sama staatus mis jõustumisteate meetodil vastu võetud originaalversioonil. Tõlgenduserimeelsuste korral tuleb lähtuda ametlikes keeltes avaldatud tekstidest;

— jõustunud Eesti standardina inglise keeles mais 2020;

— eesti keeles avaldatud sellekohase teate ilmumisega EVS Teataja 2020. aasta maikuu numbris.

Standardi tõlke koostamise ettepaneku on esitanud EVS/TK 4 „Infotehnoloogia“, standardi tõlkimist on korraldanud Eesti Standardikeskus.

Standardi on tõlkinud Cybernetica AS, standardi on heaks kiitnud EVS/TK 4.

See standard EVS-EN ISO/IEC 15408-1:2020, mille alusdokument on muutmata kujul Euroopa standardina üle võetud rahvusvaheline standard ISO/IEC 15408-1:2009, on sisult identne 2011. a märtsis jõustunud Eesti standardiga EVS-ISO/IEC 15408-1:2011.

Euroopa standardimisorganisatsioonid on teinud Euroopa standardi EN ISO/IEC 15408-1:2020 rahvuslikele liikmetele kättesaadavaks 18.03.2020.

Date of Availability of the European Standard EN ISO/IEC 15408-1:2020 is 18.03.2020.

See standard on Euroopa standardi EN ISO/IEC 15408-1:2020 eestikeelne [et] versioon. Teksti tõlke on avaldanud Eesti Standardikeskus ja sellel on sama staatus ametlike keelte versioonidega.

This standard is the Estonian [et] version of the European Standard EN ISO/IEC 15408-1:2020. It was translated by the Estonian Centre for Standardisation. It has the same status as the official versions.

Tagasisidet standardi sisu kohta on võimalik edastada, kasutades EVS-i veebilehel asuvat tagasiside vormi või saates e-kirja meiliaadressile standardiosakond@evs.ee.

ICS 35.030

EUROOPA STANDARD
EUROPEAN STANDARD
NORME EUROPÉENNE
EUROPÄISCHE NORM

EN ISO/IEC 15408-1

March 2020

ICS 35.030

English Version

Information technology - Security techniques - Evaluation criteria for IT security - Part 1: Introduction and general model (ISO/IEC 15408-1:2009)

Technologies de l'information - Techniques de sécurité - Critères d'évaluation pour la sécurité TI - Partie 1: Introduction et modèle général (ISO/IEC 15408-1:2009)

Informationstechnik - IT-Sicherheitsverfahren - Evaluationskriterien für IT-Sicherheit - Teil 1: Einführung und allgemeines Modell (ISO/IEC 15408-1:2009)

This European Standard was approved by CEN on 2 March 2020.

CEN and CENELEC members are bound to comply with the CEN/CENELEC Internal Regulations which stipulate the conditions for giving this European Standard the status of a national standard without any alteration. Up-to-date lists and bibliographical references concerning such national standards may be obtained on application to the CEN-CENELEC Management Centre or to any CEN and CENELEC member.

This European Standard exists in three official versions (English, French, German). A version in any other language made by translation under the responsibility of a CEN and CENELEC member into its own language and notified to the CEN-CENELEC Management Centre has the same status as the official versions.

CEN and CENELEC members are the national standards bodies and national electrotechnical committees of Austria, Belgium, Bulgaria, Croatia, Cyprus, Czech Republic, Denmark, Estonia, Finland, France, Germany, Greece, Hungary, Iceland, Ireland, Italy, Latvia, Lithuania, Luxembourg, Malta, Netherlands, Norway, Poland, Portugal, Republic of North Macedonia, Romania, Serbia, Slovakia, Slovenia, Spain, Sweden, Switzerland, Turkey and United Kingdom.

CEN-CENELEC Management Centre:
Rue de la Science 23, B-1040 Brussels

SISUKORD

EUROOPA EESSÕNA

Standardi ISO/IEC 15408-1:2009 teksti on koostanud Rahvusvahelise Standardimisorganisatsiooni (ISO) tehniline komitee ISO/IEC JTC 1 „Information technology“ ja selle on standardina EN ISO/IEC 15408-1:2020 üle võtnud tehniline komitee CEN/CLC/JTC 13 „Cybersecurity and Data Protection“, mille sekretariaati haldab DIN.

Euroopa standardile tuleb anda rahvusliku standardi staatus kas identse tõlke avaldamisega või jõustumisteatega hiljemalt 2020. a septembriks ja sellega vastuolus olevad rahvuslikud standardid peavad olema kehtetuks tunnistatud hiljemalt 2020. a septembriks.

Tuleb pöörata tähelepanu võimalusele, et standardi mõni osa võib olla patendiõiguse objekt. CEN ei vastuta sellis(t)e patendiõigus(t)e väljaselgitamise ega selgumise eest.

CEN-CENELEC-i sisereeglite järgi peavad Euroopa standardi kasutusele võtma järgmiste riikide rahvuslikud standardimisorganisatsioonid: Austria, Belgia, Bulgaaria, Eesti, Hispaania, Holland, Horvaatia, Iirimaa, Island, Itaalia, Kreeka, Küpros, Leedu, Luksemburg, Läti, Malta, Norra, Poola, Portugal, Prantsusmaa, Põhja-Makedoonia Vabariik, Rootsi, Rumeenia, Saksamaa, Serbia, Slovakkia, Sloveenia, Soome, Šveits, Taani, Tšehhi Vabariik, Türgi, Ungari ja Ühendkuningriik.

Jõustumisteade

CEN on standardi ISO/IEC 15408-1:2009 teksti muutmata kujul üle võtnud standardina EN ISO/IEC 15408-1:2020.

EESSÕNA

ISO (Rahvusvaheline Standardimisorganisatsioon) ja IEC (Rahvusvaheline Elektrotehnikakomisjon) moodustavad spetsialiseeritud ülemaailmse standardimise süsteemi. ISO või IEC eri maade liikmeskogud osalevad rahvusvaheliste standardite väljatöötamises tehniliste komiteede kaudu, mis on nendes organisatsioonides rajatud, et käsitleda tehnilise tegevuse eri valdkondi. ISO ja IEC tehnilised komiteed teevad koostööd mõlemale huvi pakkuvatel aladel. Selles töös osalevad käsikäes ISO-ga ka teised rahvusvahelised, riiklikud ja valitsusvälised organisatsioonid. Infotehnoloogia valdkonnas on ISO ja IEC rajanud ühise tehnilise komitee ISO/IEC JTC 1.

Rahvusvahelised standardid kavandatakse ISO/IEC direktiivide 2. osas esitatud reeglite kohaselt.

Tehniliste komiteede põhiülesanne on rahvusvaheliste standardite koostamine. Ühistes tehnilistes komiteedes vastuvõetud rahvusvahelised standardikavandid saadetakse hääletamiseks rahvuslikele liikmesorganisatsioonidele. Avaldamine rahvusvahelise standardina nõuab, et hääletusel osalenud rahvuslikest liikmesorganisatsioonidest kiidaks selle heaks vähemalt 75 %.

Tuleb pöörata tähelepanu võimalusele, et standardi mõni osa võib olla patendiõiguse objekt. ISO ega IEC ei vastuta sellis(t)e patendiõigus(t)e väljaselgitamise ega selgumise eest.

Standardi ISO/IEC 15408-1 on koostanud ühise tehnilise komitee ISO/IEC JTC 1 „Information technology“ alamkomitee SC 27 „IT Security techniques“. ISO/IEC 15408 omaga identse teksti on ühiskriteeriumide projekti sponsororganisatsioonid avaldanud pealkirjaga „Infoturbe hindamise ühiskriteeriumid“. Mõlema publikatsiooni ühine XML-kuju asub aadressil http://www.oc.ccn.cni.es/xml.

See kolmas väljaanne tühistab ja asendab teist väljaanne (ISO/IEC 15408-1:2005), mis on tehniliselt üle väljaanne.

ISO/IEC 15408 üldpealkirjaga „Information technology — Security techniques — Evaluation criteria for IT security“ („Infotehnoloogia. Turbemeetodid. Infoturbe hindamise kriteeriumid“ koosneb järgmistest osadest):

— Part 1: Introduction and general model (Osa 1: Sissejuhatus ja üldmudel);

— Part 2: Security functional components;

— Part 3: Security assurance components.

SISSEJUHATUS

ISO/IEC 15408 teeb võimalikuks sõltumatute turbe hindamiste tulemite võrreldavuse. Selleks annab see ühe üldise nõudestiku IT-toodete turvafunktsioonistiku kohta ning turbe tagamise meetmed, mida neile IT-toodetele rakendatakse turbe hindamise käigus. Need IT-tooted võivad olla rakendatud riistvaras, püsivaras või tarkvaras.

Hindamisprotsess selgitab välja teatava usaldusmäära selle kohta, kas niisuguste IT-toodete turvafunktsioonistik ja neile rakendatavad kindlusmeetmed vastavad neile nõuetele. Hindamistulemused võivad aidata tarbijail otsustada, kas hinnatavad IT-tooted rahuldavad nende turvavajadusi.

ISO/IEC 15408 on kasulik juhend turvafunktsioonidega IT-toodete väljatöötamiseks, hindamiseks ja/või soetamiseks.

ISO/IEC 15408 on kavandatud paindlikuna ning võimaldab rakendada tervet rida hindamismeetodeid terve rea IT-toodete tervele reale turvaomadustele. Standardi kasutajad peaksid olema ettevaatlikud, et standardi paindlikkust mitte kuritarvitada. Näiteks võib ISO/IEC 15408 kasutamine ebasobivate hindamismeetodite, asjakohatute turvaomaduste või ebasobivate IT-toodete puhul viia tarbetute hindamistulemusteni.

Sellel, et mingit IT-toodet on hinnatud, on tähendus ainult hinnatud turvaomaduste ja kasutatud hindamismeetodite kontekstis. Otsustamiseks, kas hindamine annab mõttekaid tulemusi, on hindamisorganeil soovitatav hoolikalt kontrollida tooteid, omadusi ja meetodeid. Seda konteksti on soovitatav arvestada ka hinnatud toodete soetajail, et otsustada, kas toode on kasulik ja rakendatav konkreetsele olukorrale ja vajadustele.

ISO/IEC 15408 käsitleb varade kaitset lubamatu avalikustamise, muutmise või kasutuskõlbmatuse eest. Üldiselt nimetatakse turvalisuse rikkumise nende kolme tüübiga seotud kaitse kategooriaid vastavalt konfidentsiaalsuseks, terviklikkuseks ja käideldavuseks. ISO/IEC 15408 võib peale nende kolme olla rakendatav ka infoturbe muudele aspektidele. ISO/IEC 15408 on rakendatav riskidele, mida tekitavad nii (pahatahtlikud või muud) inimtegevused kui ka muud tegevused. Standard ISO/IEC 15408 ei taotle rakendatavust teistel IT aladel peale infoturbe, kuid seda võidakse nendes rakendada.

Teatud teemad loetakse väljaspool ISO/IEC 15408 käsitlusala olevaiks nendega kaasnevate erimeetodite või mõningase perifeersuse tõttu infoturbe suhtes. Mõned neist on loetletud järgnevalt.

a) ISO/IEC 15408 ei sisalda turbe hindamise kriteeriume, mis puudutavad IT turvafunktsioonidega otseselt mitteseotud halduslikke turvameetmeid. On aga arvestatud sellega, et sageli võidakse olulist turvet saavutada või toetada halduslike, näiteks korralduslike, personalialaste, füüsiliste ja protseduuriliste meetmetega.

b) Infoturbe mõningate füüsiliste tehniliste aspektide (näiteks elektromagnetilise kiirguse ohje) hindamist ei ole konkreetselt hõlmatud, kuid selles valdkonnas saab rakendada paljusid käsitletud mõisteid.

c) ISO/IEC 15408 ei käsitle hindamismetoodikat, millega tuleks nimetatud kriteeriume rakendada. Selle metoodika annab ISO/IEC 18045.

d) ISO/IEC 15408 ei käsitle halduslikku ega õiguslikku raamstruktuuri, mille tingimustes võivad hindamisorganid rakendada nimetatud kriteeriume. Eeldatakse aga, et standardit ISO/IEC 15408 kasutatakse hindamise eesmärkidel mingi sellise raamstruktuuri kontekstis.

e) Protseduurid hindamistulemite kasutamiseks akrediteerimisel jäävad ISO/IEC 15408 käsitlusalast välja. Akrediteerimine on halduslik protsess, millega antakse õigus käitada IT-toodet (või toodete kogumit) selle täielikus käituskeskkonnas, sisaldades ka kõiki IT-väliseid osi. Hindamisprotsessi tulemid sisestatakse akrediteerimise protsessi. Et aga IT-väliste omaduste ning nende ja IT turvaosade vahelise seose hindamiseks on sobivamaid meetodeid, peaksid akrediteerijad seadma neile aspektidele eraldi tingimusi.

f) ISO/IEC 15408 ei hõlma krüptograafiliste algoritmide olemuslike omaduste hindamise kriteeriume. Kui peaks olema vajadus krüptograafia matemaatilisi omadusi sõltumatult hinnata, peaks sellise hindamise tingimused seadma see hindamisskeem, mille raames rakendatakse standardit ISO/IEC 15408.

Kogu dokumendi ulatuses kasutatud ISO terminoloogia, nagu „saab“, „teatmeline“, „võib“, „normatiivne“, „peab, tuleb“ ja „peaks, tuleks“, on määratletud ISO/IEC direktiivide 2. osas. Tuleb silmas pidada, et terminil „peaks, tuleks“ on lisatähendus, mis on rakendatav selle standardi kasutamisel (vt märkus allpool). Termini „peaks, tuleks“ kasutamiseks standardis ISO/IEC 15408 kehtib järgnev määratlus:

peaks, tuleks (*should*)

normatiivses tekstis näitab „peaks, tuleks“, et „mitme võimaluse hulgast on üks eriti sobiv, nimetamata või välistamata muid, või et teatav teguviis on eelistatud, kuid mitte tingimata nõutav.“ (ISO/IEC direktiivid, 2. osa).

MÄRKUS ISO/IEC 15408 tõlgendab fraasi „mitte tingimata nõutav“ tähendust nii: muu võimaluse valimine nõuab põhjendust selle kohta, miks ei valitud eelistatavat võimalust.

1 KÄSITLUSALA

ISO/IEC 15408 selles osas kehtestatakse infoturbe hindamise üldmõisted ja põhimõtted ning määratakse kindlaks hindamise üldmudel, mis on esitatud standardi eri osades ning mis on tervikuna mõeldud kasutamiseks IT-toodete turvaomaduste hindamise alusena.

Standardi ISO/IEC 15408 esimeses osas kirjeldatakse standardi kõiki osi, määratletakse terminid ja lühendid, mida kasutatakse kõigis osades, kehtestatakse hindamisobjekti (*Target of Evaluation* - TOE) tuummõiste, määratakse hindamise kontekst ja kirjeldatakse lugejaskonda, kellele on hindamise kriteeriumid suunatud. Sissejuhatavalt kirjeldatakse põhilisi turvamõisteid, mis on vajalikud IT-toodete hindamiseks.

Standard määratleb mitmesugused operatsioonid, millega saab lubatavate operatsioonide kasutamise teel kohandada funktsionaalseid ja tagatislikke komponente, mis on esitatud standardi osades ISO/IEC 15408-2 ja ISO/IEC 15408-3.

Esitatud on kaitseprofiilide (PP) tuummõisted, turvanõuete paketid ja vastavuse teema ning kirjeldatud on hindamise tagajärgi ja tulemeid. ISO/IEC 15408 selles, esimeses osas antakse suunised turvasihtide (ST) spetsifitseerimiseks ja kirjeldatakse komponentide korraldust kogu mudeli ulatuses. Hindamismetoodika üldteave ja hindamisskeemide käsitlusala on standardis ISO/IEC 18045.

2 NORMIVIITED

Allpool nimetatud dokumendid, kui need on rakendatavad, on vajalikud ISO/IEC 15408 selle osa rakendamiseks. Dateeritud viidete korral kehtib üksnes viidatud väljaanne. Dateerimata viidete korral kehtib viidatud dokumendi uusim väljaanne koos võimalike muudatustega

ISO/IEC 15408-2. Information technology — Security techniques — Evaluation criteria for IT security — Part 2: Security functional components

ISO/IEC 15408-3. Information technology — Security techniques — Evaluation criteria for IT security — Part 3: Security assurance components

ISO/IEC 18045. Information technology — Security techniques — Methodology for IT security evaluation

3 TERMINID JA MÄÄRATLUSED

Standardi rakendamisel kasutatakse allpool esitatud termineid ja määratlusi.

MÄRKUS See jaotis sisaldab ainult neid termineid, mida kasutatakse eritähenduses kogu standardis ISO/IEC 15408. Mõnesid selles standardis kasutatud üldiseid terminikombinatsioone ei ole selles jaotises määratletud, kuid selguse mõttes on need kasutuskontekstis selgitatud.

3.1 ISO/IEC 15408 üldised terminid ja määratlused

3.1.1
kahjulikud toimingud (*adverse actions*)
toimingud, mida ohuagent sooritab mingi vara suhtes

3.1.2
varad (*assets*)
olemid, mis hindamisobjekti omanikule on eeldatavalt väärtuslikud