EESTI STANDARD EVS-ISO/IEC 27033-1:2024

Avaldatud eesti keeles: märts 2024
Jõustunud Eesti standardina: märts 2024

INFOTEHNOLOOGIA
Turbemeetodid
Võrguturve
Osa 1: Ülevaade ja mõisted

Information technology
Security techniques
Network security
Part 1: Overview and concepts
(ISO/IEC 27033-1:2015, identical)

EVS • EESTI STANDARDIMIS- JA AKREDITEERIMISKESKUS
ESTONIAN CENTRE FOR STANDARDISATION AND ACCREDITATION

EESTI STANDARDI EESSÕNA

See Eesti standard on

— rahvusvahelise standardi ISO/IEC 27033-1:2015 ingliskeelse teksti sisu poolest identne tõlge eesti keelde ja sellel on sama staatus mis ümbertrüki meetodil vastu võetud originaalversioonil. Tõlgenduserimeelsuste korral tuleb lähtuda ametlikes keeltes avaldatud tekstidest;

— jõustunud Eesti standardina inglise keeles märtsis 2024;

— eesti keeles avaldatud sellekohase teate ilmumisega EVS Teataja 2024. aasta märtsikuu numbris.

Standardi tõlke koostamise ettepaneku on esitanud tehniline komitee EVS/TK 04 „Infotehnoloogia“, standardi tõlkimist on korraldanud Eesti Standardimis- ja Akrediteerimiskeskus ning rahastanud Majandus- ja Kommunikatsiooniministeerium.

Standardi on tõlkinud TepInfo OÜ, standardi on heaks kiitnud EVS/TK 04.

See standard on rahvusvahelise standardi ISO/IEC 27033-1:2015 eestikeelne [et] versioon. Teksti tõlke on avaldanud Eesti Standardimis- ja Akrediteerimiskeskus ning sellel on sama staatus ametlike keelte versioonidega.

This standard is the Estonian [et] version of the International Standard ISO/IEC 27033-1:2015. It was translated by the Estonian Centre for Standardisation and Accreditation. 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 35.040

SISUKORD

EESSÕNA V
SISSEJUHATUS VI
1 KÄSITLUSALA 1
2 NORMIVIITED 1
3 TERMINID JA MÄÄRATLUSED 1
4 SÜMBOLID JA LÜHENDID 6
5 STRUKTUUR 9
6 ÜLEVAADE 11
6.1 Taust 11
6.2 Võrguturbe plaanimine ja haldus 13
7 RISKIDE TUVASTAMINE JA ETTEVALMISTUSED TURVAMEETMETE PIIRITLEMISEKS 15
7.1 Sissejuhatus 15
7.2 Teave praeguste ja/või plaanitavate võrkude kohta 16
7.2.1 Turvanõuded üleorganisatsioonilises infoturvapoliitikas 16
7.2.2 Teave praeguste ja/või plaanitavate võrkude kohta 16
7.3 Infoturvariskid ja võimalikud reguleerimisalad 20
8 TUGIMEETMED 23
8.1 Sissejuhatus 23
8.2 Võrguturbe haldus 24
8.2.1 Taust 24
8.2.2 Võrguturbe halduse tegevused 24
8.2.3 Võrguturbe rollid ja kohustused 26
8.2.4 Võrgu seire 27
8.2.5 Võrguturbe hindamine 27
8.3 Tehniliste nõrkuste haldus 27
8.4 Identifitseerimine ja autentimine 28
8.5 Võrgu revisjonlogimine ja seire 29
8.6 Sissetungituvastus ja -tõrje 30
8.7 Kaitse kahjurkoodi eest 31
8.8 Krüptograafiapõhised teenused 31
8.9 Jätkuvuse haldus 32
9 VÕRGUTURBE KAVANDAMISE JA TEOSTAMISE JUHISED 33
9.1 Taust 33
9.2 Võrgu tehnilise turbe arhitektuur/kavand 33
10 TÜÜPSED VÕRGUSTSENAARIUMID – RISKID, KAVANDAMISMEETODID JA REGULEERIMISKÜSIMUSED 36
10.1 Sissejuhatus 36
10.2 Internetti pääsu teenused töötajaile 36
10.3 Tõhustatud koostöö teenused 36
10.4 Partnerteenused 37
10.5 Tarbeteenused 37
10.6 Ostuteenused 37
10.7 Võrgu segmentimine 37
10.8 Mobiilside 38
10.9 Reisivate kasutajate võrgutugi 38
10.10 Kodu- ja väikekontorite võrgutugi 38

11 'TEHNILISED' TEEMAD – RISKID, KAVANDAMISMEETODID JA REGULEERIMISKÜSIMUSED 38
12 TURBELAHENDUSE VÄLJATÖÖTAMINE JA TESTIMINE 39
13 TURBELAHENDUSE KÄITUS 40
14 LAHENDUSE TEOSTUSE SEIRE JA LÄBIVAATUS 40
Lisa A (teatmelisa) ISO/IEC 27001/27002 võrguturbealaste meetmete ning ISO/IEC 27033-1 peatükkide/jaotiste vahelised ristviited 41
Lisa B (teatmelisa) Turbeprotseduuride dokumendi näidismall 46
Kirjandus 50

EESSÕNA

ISO (International Organization for Standardization) on ülemaailmne rahvuslike standardimisorganisatsioonide (ISO rahvuslike liikmesorganisatsioonide) föderatsioon. Tavaliselt tegelevad rahvusvahelise standardi koostamisega ISO tehnilised komiteed. Kõigil rahvuslikel liikmesorganisatsioonidel, kes on mingi tehnilise komitee pädevusse kuuluvast valdkonnast huvitatud, on õigus selle komitee tegevusest osa võtta. Selles töös osalevad ka ISO-ga seotud rahvusvahelised riiklikud organisatsioonid ning vabaühendused. Kõigis elektrotehnika standardimist puudutavates küsimustes teeb ISO tihedat koostööd Rahvusvahelise Elektrotehnikakomisjoniga (IEC).

Selle dokumendi väljatöötamiseks kasutatud ja edasiseks haldamiseks mõeldud protseduurid on kirjeldatud ISO/IEC direktiivide 1. osas. Eriti tuleb silmas pidada eri heakskiidukriteeriumeid, mis on eri liiki ISO dokumentide puhul vajalikud. See dokument on kavandatud ISO/IEC direktiivide 2. osas esitatud toimetamisreeglite kohaselt (vt www.iso.org/directives).

Tuleb pöörata tähelepanu võimalusele, et dokumendi mõni osa võib olla patendiõiguse objekt. ISO ei vastuta sellis(t)e patendiõigus(t)e väljaselgitamise ega selgumise eest. Dokumendi väljatöötamise jooksul väljaselgitatud või selgunud patendiõiguste üksikasjad on esitatud peatükis „Sissejuhatus“ ja/või ISO-le saadetud patentide deklaratsioonide loetelus (vt www.iso.org/patents).

Mis tahes selles dokumendis kasutatud äriline käibenimi on kasutajate abistamise eesmärgil esitatud teave ja ei kujuta endast toetusavaldust.

Selgitused vastavushindamisega seotud ISO eriomaste terminite ja väljendite kohta ning teave selle kohta, kuidas ISO järgib WTO tehniliste kaubandustõkete lepingus sätestatud põhimõtteid, on esitatud järgmisel aadressil: Foreword - Supplementary information.

Selle dokumendi eest vastutab tehnilise komitee ISO/IEC JTC 1 „Information technology“ alamkomitee SC 27 „Security techniques“.

Teine väljaanne tühistab ja asendab esimest väljaannet (ISO/IEC 27033-1:2009), mis on tehniliselt üle vaadatud.

ISO/IEC 27033 koosneb üldpealkirja „Information technology — Security techniques — Network security“ all järgmistest osadest:

— Part 1: Overview and concepts;

— Part 2: Guidelines for the design and implementation of network security;

— Part 3: Reference networking scenarios — Threats, design techniques and control issues;

— Part 4: Securing communications between networks using security gateways;

— Part 5: Securing communications across networks using Virtual Private Networks (VPNs);

— Part 6: Securing wireless IP network access.

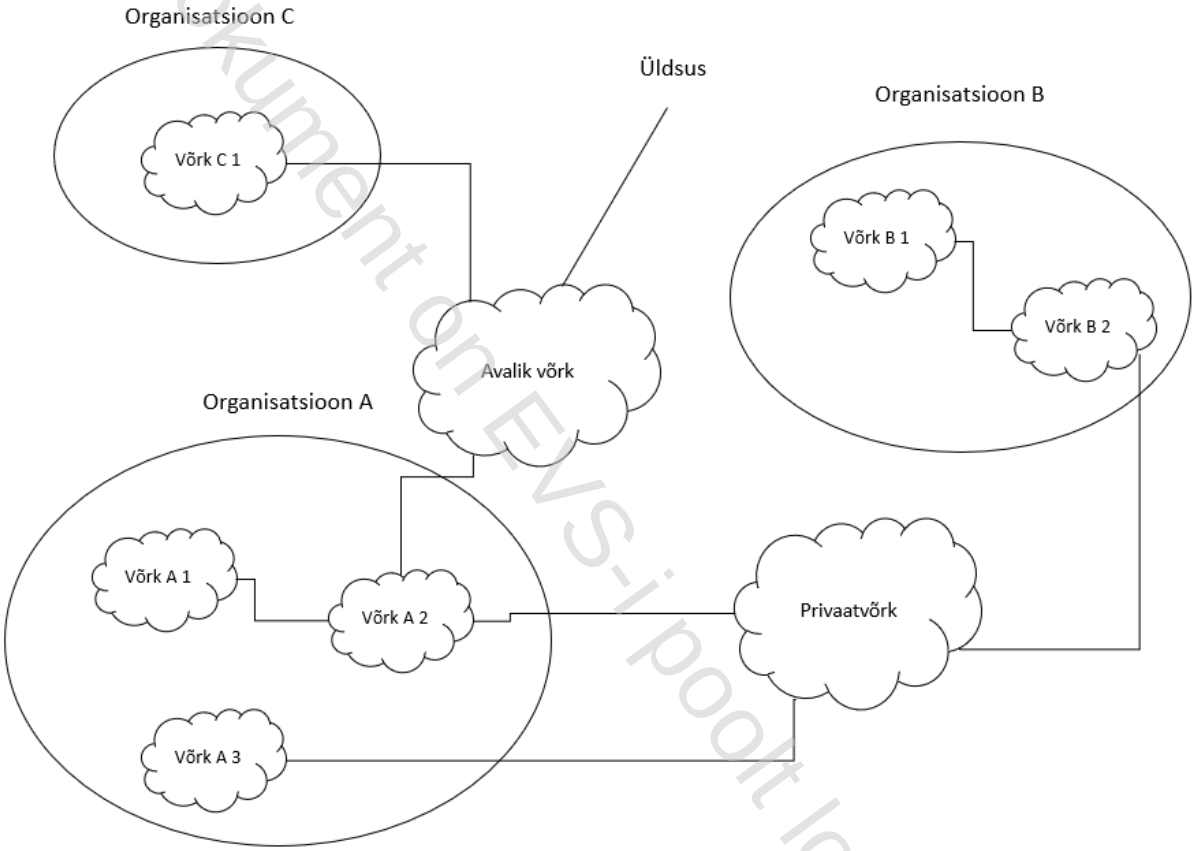
SISSEJUHATUS

Tänapäeva maailmas on enamiku ettevõtete ja riigiasutuste infosüsteemid ühendatud võrkudega (vt joonis 1), kusjuures võrguühendused on tüübilt vähemalt üks järgnevaist:

— organisatsioonisisesed;

— organisatsioonide vahelised;

— organisatsiooni ja üldsuse vahelised.



Joonis 1 — Üldised võrguühenduste tüübid

Lisaks võimaldab avalike võrkude (eriti Interneti) tehnoloogia kiire areng palju mitmekülgsemaid äritegevuse võimalusi. Organisatsioonid rakendavad elektroonilist äritegevust üha globaalsemalt ja pakuvad avalikke võrguteenuseid. Mainitud võimalused hõlmavad nii odavama andmeside tarnimist, Interneti kasutamist lihtsalt ülemaailmse ühendusmeediumina, kui ka Interneti tarnijate (ISP-de) antavate keerukamate teenusteni. See võib tähendada suhteliselt odavate kohalike ühenduspunktide kasutamist ahela mõlemas otsas, aga ka täieulatuslikke võrgustatud elektroonilise kaubanduse ja teeninduse süsteeme, mis kasutavad veebipõhiseid rakendusi ja teenuseid. Peale selle suurendab uus tehnoloogia (sh andmete, kõne ja video integratsioon) kaugtöö võimalusi, nii et töötajad saavad küllaltki pikkadel perioodidel tegutseda oma tavalistest töökohtadest eemal. Nad saavad olla ühenduses kaugvahendite abil, millega pääsevad organisatsiooni ja kogukonna võrkudesse ning tööalast tegevust toetava teabe ja teenuste juurde.

Kuigi see keskkond soodustab oluliste ärialaste hüvede saamist, sisaldab see ka uusi turvariske, mida tuleb hallata. Kuna organisatsioonide tegutsemine sõltub tugevalt teabe ja sellega seotud võrkude kasutamisest, võib teabe ja teenuste konfidentsiaalsuse, tervikluse ja käideldavuse kadu avaldada organisatsiooni tegevusele olulist kahjulikku mõju. Seega on üks peamisi nõudeid võrkude ning nendega seotud infosüsteemide ja teabe korralik kaitstus. Teisisõnu: *sobiva võrguturbe teostamine ja säilitamine on iga organisatsiooni tegevuse eduks elutähtis.*

Sellega seoses otsitakse side- ja infotehnoloogia valdkondades kuluefektiivseid terviklikke turbelahendusi, mis on suunatud võrkude kaitsele pahatahtlike rünnete ja tahtmatute väärtoimingute eest ning tegevusalase teabe ja teenuste konfidentsiaalsus-, terviklus- ja käideldavusnõuete täitmisele. Võrgu turve on oluline ka arveldus- või kasutamisteabe täpsuse säilitamiseks vastavalt vajadusele. Kogu võrgu (sh rakenduste ja teenuste) turvalisuse seisukohalt on toodete turvaomadused väga olulised. Kuna aga terviklahenduste pakkumiseks kombineeritakse paljusid tooteid, määrab lahenduse edu nende koostalitlusvõime või selle puudumine. Turve peab olema mitte ainult üks iga toote ja teenuse puhul arvestatav tahk, vaid seda tuleb arendada nii, et see soodustaks turvaomaduste põimimist üldisesse turbelahendusse.

Selle rahvusvahelise standardi eesmärk on anda üksikasjalikke juhiseid infosüsteemide võrkude ja nendevaheliste ühenduste halduse, käituse ja kasutamise turbeaspektide kohta. Need, kes organisatsioonis vastutavad infoturbe, eriti aga võrguturbe eest, peaksid suutma kohandada selles rahvusvahelises standardis olevat materjali vastavalt oma erinõuetele. Selle standardi peamised eesmärgid on järgmised.

— ISO/IEC 27033-1, määratleda ja kirjeldada võrguturbega seotud mõisted ja anda võrguturbe halduse juhiseid. See hõlmab ülevaadet võrguturbest ja sellega seotud määratlustest ning ka juhiseid selle kohta, kuidas tuvastada ja analüüsida võrgu turvariske ja seejärel määratleda võrguturbe nõuded. Sissejuhatavalt käsitletakse ka kvaliteetsete tehnilise turbe arhitektuuride loomist, aga samuti riskide, kavandamise ja ohje aspekte, mis on seotud tüüpiliste võrgustsenaariumite ja võrgutehnoloogia valdkondadega (üksikasjalikumalt käsitletakse neid aspekte ISO/IEC 27033 järgmistes osades);

— ISO/IEC 27033-2, määratleda, kuidas organisatsioonid peaksid jõudma kvaliteetsete tehnilise turbe arhitektuuride, lahenduste ja teostusteni, mis tagavad konkreetsetele ärikeskkondadele sobiva võrguturbe; mille puhul kasutatakse järjekindlat asjakohast lähenemisviisi võrguturbe plaanimisele, kavandamisele ja teostamisele mudelite/karkasside abil (selles kontekstis kirjeldatakse mudeli või karkassi abil üldjoontes esitust või kirjeldust, mis näitab mingit liiki tehnilise turbe arhitektuuri/kavandi struktuuri ja üldist toimimisviisi); ja mis puudutavad kõiki töötajaid, kes osalevad võrguturbe arhitektuuri aspektide plaanimises, kavandamises ja teostamises (nt võrguarhitekte ja -projekteerijaid, võrguhaldureid ja võrguturbeametnikke);

— ISO/IEC 27033-3, määratleda tüüpiliste võrgustsenaariumitega seotud spetsiifilised riskid, kavandamismeetodid ja reguleerimisküsimused. See puudutab kõiki töötajaid, kes osalevad võrguturbe arhitektuuri aspektide plaanimises, kavandamises ja teostamises (nt võrguarhitekte ja -projekteerijaid, võrguhaldureid ja võrguturbeametnikke);

— ISO/IEC 27033-4, määratleda spetsiifilised riskid, kavandamismeetodid ja reguleerimisküsimused võrkudevaheliste teabevoogude turvalüüsidega turvamisel. See puudutab kõiki töötajaid, kes osalevad turvalüüside detailses plaanimises, kavandamises ja teostamises (nt võrguarhitekte ja -projekteerijaid, võrguhaldureid ja võrguturbeametnikke);

— ISO/IEC 27033-5, määratleda spetsiifilised riskid, kavandamismeetodid ja reguleerimisküsimused virtuaalsete privaatvõrkudega (VPN) loodud ühenduste turbe puhul. See puudutab kõiki töötajaid, kes osalevad VPN-i turbe detailses plaanimises, kavandamises ja teostamises (nt võrguarhitekte ja -projekteerijaid, võrguhaldureid ja võrguturbeametnikke);

— ISO/IEC 27033-6, määratleda spetsiifilised riskid, kavandamismeetodid ja reguleerimisküsimused traadita IP-võrkude turbe puhul. See puudutab kõiki töötajaid, kes osalevad traadita võrkude turbe detailses plaanimises, kavandamises ja teostamises (nt võrguarhitekte ja -projekteerijaid, võrguhaldureid ja võrguturbeametnikke).

Tuleb rõhutada, et see rahvusvaheline standard annab üksikasjalikke teostuse lisajuhiseid nende võrguturbe meetmete kohta, mida standardi põhitasemel kirjeldab ISO/IEC 27002.

Tuleks silmas pidada, et see rahvusvaheline standard ei ole etalon- ega normdokument regulatiivsete või õigusaktidest tulenevate turvanõuete küsimustes. Standard rõhutab küll nende mõjurite tähtsust, kuid ei saa neid konkreetselt esitada, sest need sõltuvad konkreetsest riigist, ettevõtte tüübist jne.

Kui pole öeldud teisiti, on ISO/IEC 27033 kogu selles osas esitatud juhised kohaldatavad praegustele ja/või plaanilistele võrkudele, mida edaspidi nimetatakse lihtsalt võrkudeks või võrguks.

1 KÄSITLUSALA

ISO/IEC 27033 see osa annab ülevaate võrguturbest ja sellega seotud määratlustest. Standard määratleb ja kirjeldab võrguturbega seotud mõisteid ja annab võrguturbe halduse juhiseid. (Lisaks sidelinkide kaudu edastatava teabe turbele puudutab võrguturve seadmete turvet ning seadmete, rakenduste/teenuste ja lõppkasutajatega seotud haldustegevuste turvet.)

See osa puudutab kõiki, kes on seotud mingi võrgu omamise, käituse või kasutamisega. Lisaks juhtidele ja ülematele, kellel on erikohustused infoturbe ja/või võrguturbe ja võrgu käituse alal või kes vastutavad organisatsiooni üldise turbekava ja turvapoliitika väljatöötamise eest, kuuluvad nende hulka kõrgemad juhid ja muud mittetehnilised juhid või kasutajad. See puudutab ka kõiki võrguturbe arhitektuuri aspektide plaanimises, kavandamises ja teostamises osalejaid.

Lisaks annab ISO/IEC 27033 see osa:

— juhiseid selle kohta, kuidas tuvastada ja analüüsida võrgu turvariske ning määrata selle analüüsi põhjal võrgu turvanõuded;

— ülevaate meetmetest, mis toetavad võrgu tehnilise turbe arhitektuure ja nendega seotud tehnilistest meetmetest, ning ka nendest mittetehnilistest ja tehnilistest meetmetest, mis on rakendatavad mitte vaid võrkude puhul;

— sissejuhatava kirjelduse kvaliteetsete võrgu tehnilise turbe arhitektuuride saavutamise ning tüüpiliste võrgustsenaariumite ja võrgu tehnoloogiliste aladega seotud riski-, kavandamis- ja reguleerimisaspektide kohta (üksikasjalikumalt käsitlevad neid ISO/IEC 27033 järgmised osad), ning lühida küsimuste käsitluse, mis on seotud võrguturbe meetmete teostamise ja käitusega ning nende teostuse pideva seire ja läbivaatusega.

Kokkuvõttes annab see osa ülevaate standardist ISO/IEC 27033 ning teekaardi selle standardi teiste osade jaoks.

2 NORMIVIITED

Allpool nimetatud dokumentidele on tekstis viidatud selliselt, et nende sisu kujutab endast kas osaliselt või tervenisti selle dokumendi nõudeid. Dateeritud viidete korral kehtib üksnes viidatud väljaanne. Dateerimata viidete korral kehtib viidatud dokumendi uusim väljaanne koos võimalike muudatustega.

ISO/IEC 7498 (kõik osad). Information technology — Open Systems Interconnection — Basic Reference Model: Naming and addressing

ISO/IEC 27001. Information technology — Security techniques — Information security management systems — Requirements

ISO/IEC 27002. Information technology — Security techniques — Code of practice for information security controls

ISO/IEC 27005. Information technology — Security techniques — Information security risk management

3 TERMINID JA MÄÄRATLUSED

Dokumendi rakendamisel kasutatakse standardites ISO/IEC 7498 (kõik osad), ISO/IEC 27000, ISO/IEC 27001, ISO/IEC 27002, ISO/IEC 27005 ning allpool esitatud termineid ja määratlusi.

MÄRKUS Järgnevad terminid ja määratlused kehtivad ka ISO/IEC 27033 kõigis osades.

