

INFOTEHNOLOOGIA

Turbemeetodid

Võrguturve

Osa 2: Võrguturbe kavandamise ja teostamise juhised

Information technology

Security techniques

Network security

**Part 2: Guidelines for the design and implementation of
network security
(ISO/IEC 27033-2:2012)**

EESTI STANDARDI EESSÕNA

See Eesti standard on

- rahvusvahelise standardi ISO/IEC 27033-2:2012 ingliskeelse teksti sisu poolest identne tõlge eesti keelde. Tõlgenduserimeelsuste korral tuleb lähtuda ametlikes keeltes avaldatud tekstidest;
- jõustunud Eesti standardina sellekohase teate avaldamisega EVS Teataja 2013. aasta augustikuu numbris.

Standardi on tõlkinud Cybernetica AS, standardi tõlke on heaks kiitnud EVS/TK 4 „Infotehnoloogia“.

Standardi tõlkimise koostamise ettepaneku on esitanud EVS/TK 4, standardi tõlkimist on korraldanud Eesti Standardikeskus ning rahastanud Majandus- ja Kommunikatsiooniministeerium.

See standard on rahvusvahelise standardi ISO/IEC 27033-2:2012 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 International Standard ISO/IEC 27033-2:2012. It has been 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 35.040 Märgistikud ja informatsiooni kodeerimine

Võtmesõnad: arvutivõrk, infotehnoloogia, infoturve, meetodid

Hinnagrupp N

Standardite reprodutseerimise ja levitamise õigus kuulub Eesti Standardikeskusele

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

Kui Teil on küsimusi standardite autorikaitse kohta, võtke palun ühendust Eesti Standardikeskusega:

Aru 10, 10317 Tallinn, Eesti; www.evs.ee; telefon 605 5050; e-post info@evs.ee

SISUKORD

EESSÕNA	IV
1 KÄSITLUSALA	1
2 NORMIVIITED	1
3 TERMINID JA MÄÄRATLUSED	1
4 LÜHENDID	1
5 DOKUMENDI STRUKTUUR	2
6 VALMISTUMINE VÕRGUTURBE KAVANDAMISEKS	2
6.1 Sissejuhatus	2
6.2 Varade piiritlemine	2
6.3 Nõuete kogumine	3
6.3.1 Õiguslikud ja regulatiivsed nõuded	3
6.3.2 Ärinõuded	3
6.3.3 Sooritusnõuded	3
6.4 Nõuete läbivaatus	3
6.5 Olemasolevate kavandite ja teostuste läbivaatus	4
7 VÕRGUTURBE KAVANDAMINE	4
7.1 Sissejuhatus	4
7.2 Kavandamisprintsüübid	5
7.2.1 Sissejuhatus	5
7.2.2 Sügavuti kaitse	5
7.2.3 Võrgutsoonid	6
7.2.4 Kavandi elastsus	6
7.2.5 Stsenariumid	7
7.2.6 Mudelid ja karkassid	7
7.3 Kavandi kinnitamine	7
8 TEOSTAMINE	7
8.1 Sissejuhatus	7
8.2 Võrgukomponentide valimise kriteeriumid	8
8.3 Toote või tarnija valimise kriteeriumid	8
8.4 Võrguhaldus	9
8.5 Logimine, seire ja intsidentidele reageerimine	10
8.6 Dokumentatsioon	10
8.7 Testimisplaanid ja testimise läbiviimine	10
8.8 Kinnitamine	11
Lisa A (teatmelisa) ISO/IEC 27001:2005/ISO/IEC 27002:2005 võrguturbe meetmete ja ISO/IEC 27033-2:2012 jaotiste vahelised viited	12
Lisa B (teatmelisa) Näitelised dokumendimallid	13
Lisa C (teatmelisa) ITU-T X.805 karkassi ja ISO/IEC 27001:2005 meetmete vastendus	21
Kirjandus	25

EESSÕNA

ISO (Rahvusvaheline Standardimisorganisatsioon) ja IEC (Rahvusvaheline Elektrotehnikakomisjon) moodustavad ülemaailmse standardimise spetsialiseeritud süsteemi. ISO või IEC rahvuslikud liikmeskogud osalevad rahvusvaheliste standardite väljatöötamises tehniliste komiteede kaudu, mis on nendes organisatsioonides rajatud käsitlema tehnilise tegevuse eri valdkondi. ISO ja IEC tehnilised komiteed teevad koostööd mõlemale huvipakkuvatel aladel. Selles töös osalevad käsikäes ISO ja IEC-ga ka muud rahvusvahelised riiklikud ja mitteriiklikud organisatsioonid. Infotehnoloogia alal on ISO ja IEC loonud ühise tehnilise komitee ISO/IEC JTC 1.

Rahvusvahelised standardid kavandatakse vastavalt ISO/IEC direktiivide 2. osas esitatud reeglitele. Ühise tehnilise komitee peamine ülesanne on koostada rahvusvahelisi standardeid. Ühises tehnilises komitees vastu võetud rahvusvahelised standardikavandid saadetakse rahvuslikele kogudele hääletamiseks. Rahvusvahelise standardina avaldamine nõuab heakskiitu vähemalt 75 % hääletanud rahvuslikelt kogudelt.

Tuleb pöörata tähelepanu võimalusele, et standardi mõni osa võib olla patendiõiguse subjekt. ISO-t ega IEC-d ei saa pidada vastutavaks sellis(t)e patendiõigus(t)e väljaselgitamise eest.

Standardi ISO/IEC 27033-2 koostas ISO/IEC ühendatud tehnilise komitee JTC 1 „Infotehnoloogia“ alamkomitee SC 27 „Turbemeetodid“.

See ISO/IEC 27033-2 esimene redaktsioon tühistab ja asendab standardi ISO/IEC 18028-2:2006, olles selle tehniline uustöötlus.

ISO/IEC 27033 üldpealkirjaga „Infotehnoloogia. Turbemeetodid. Võrguturve“ koosneb järgmistest osadest:

- Osa 1. Ülevaade ja mõisted;
- Osa 2. Võrguturbe kavandamise ja teostamise juhised;
- Osa 3. Tüüpsed võrgustenaariumid. Riskid, kavandamismeetodid ja reguleerimisküsimused.

Koostamisel on järgmised osad:

- Osa 4. Võrkudevahelise side turve turvalüüside abil;
- Osa 5. Võrkudevahelise side turve virtuaalsete privaatvõrkude (VPN) abil.

Tulevase 6. osa teema moodustab traadita IP-võrkupääsu turve.

Võib järgneda veel muid osi, sest võrguturbe valdkonnas muutub ja areneb tehnoloogia lakkamatult.

ISO/IEC 27033-2:2012 selles korrigeeritud versioonis on korrigeeritud pealkirja tiitellehel ja leheküljel 1.

1 KÄSITLUSALA

See ISO/IEC 27033 osa annab organisatsioonidele juhiseid võrguturbe plaanimiseks, kavandamiseks, teostamiseks ja dokumenteerimiseks.

2 NORMIVIITED

Alljärgnevalt nimetatud dokumendid on vajalikud selle standardi rakendamiseks. 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

ISO/IEC 27000:2009. Information technology — Security techniques — Information security management systems — Overview and vocabulary

ISO/IEC 27001:2005. Information technology — Security techniques — Information security management systems — Requirements

ISO/IEC 27002:2005. Information technology — Security techniques — Code of practice for information security management

ISO/IEC 27005:2011. Information technology — Security techniques — Information security risk management

ISO/IEC 27033-1. Information technology — Security techniques — Network security — Part 1: Overview and concepts

3 TERMINID JA MÄÄRATLUSED

Standardi rakendamisel kasutatakse standardeis ISO/IEC 7498 (kõik osad), ISO/IEC 27000, ISO/IEC 27001, ISO/IEC 27002, ISO/IEC 27005 ja ISO/IEC 27033-1 toodud termineid ja määratlusi.

4 LÜHENDID

Standardi rakendamisel kasutatakse standardis ISO/IEC 27033-1 toodud ja alljärgnevalt esitatud lühendeid.

IPS	<i>Intrusion Prevention System</i> — Sissetungi tõrje süsteem
POC	<i>Proof of Concept</i> — Kontseptsiooni tõendus
RADIUS	<i>Remote Authentication Dial-In User Service</i> — Protokoll RADIUS („kaugautentimise sissehelistusteenus“)
RAS	<i>Remote Access Service</i> — Kaugpöörduse teenus
SMS	<i>Simple Message Service</i> — SMS-teenus („lihtne sõnumiteenus“)
SMTP	<i>Simple Mail Transfer Protocol</i> — protokoll SMTP („lihtne meiliedastuse protokoll“)
TACACS	<i>Terminal Access Controller Access-Control System</i> — Protokoll TACACS („terminalipääsu kontrolleri pääsu reguleerimise süsteem“)
TFTP	<i>Trivial File Transfer Protocol</i> — Protokoll TFTP („triviaalne failiedastusprotokoll“)
TLS	<i>Transport Layer Security</i> — Protokoll TLS („transpordikihi turve“)