TARTU ÜLIKOOL
Arvutiteaduse instituut
Informaatika õppekava

Ivan Strikkojev

Eesti infoturbestandardi võrgud ja side mooduligrupi rakendamine haridusasutusele

Bakalaureusetöö (9 EAP)

Juhendaja: Alo Peets, MSc

Tartu 2025

Eesti infoturbestandardi võrgud ja side mooduligrupi rakendamine haridusasutusele

Lühikokkuvõte:

Eesti infoturbestandard (E-ITS) on riiklik raamistik, mis määratleb nõuded infoturbe tagamiseks rakendatavas organisatsioonis. Käesoleva bakalaureusetöö eesmärk on hinnata ühe haridusasutuse võrgutaristu vastavust E-ITSi NET mooduligrupi nõuetele, tuvastada puudujäägid ning koostada lahendused nende kõrvaldamiseks. Töö käigus kirjeldatakse olemasolevat võrgu arhitektuuri ja seadistusi, analüüsitakse tulemüüri konfiguratsiooni, logimist, monitooringut, varundust ning raadiovõrgu turvalisust. Esitatud soovitused ja tehnilised juhised on rakendatavad nii uuritud haridusasutuses kui ka teistes koolides, sealhulgas uue võrgu loomisel või võrgulahenduse tellimisel teenusepakkujalt, aidates tagada E-ITSi nõuetele vastavus ja võrgu turvalisus.

Võtmesõnad: E-ITS, NET-kategooria, võrgu monitooring, infoturve, tulemüür, haridusasutus, võrguturve, rünnakutuvastus

CERCS: P175 Informaatika, süsteemiteooria

Implementation of the Network and Communication Module Group of the Estonian Information Security Standard for an Educational Institution

Abstract:

The Estonian Information Security Standard (E-ITS) is a national framework that defines the requirements for ensuring information security within an organisation. The aim of this bachelor's thesis is to assess the compliance of an educational institution's network infrastructure with the requirements of the E-ITS NET module group, identify deficiencies, and develop solutions for their elimination. The thesis describes the existing network architecture and configurations, analyses firewall configuration, logging, monitoring, backups, and wireless network security. The presented recommendations and technical guidelines can be applied not only in the analysed educational institution but also in other schools, including in new network deployments or when procuring network solutions from a service provider, helping to ensure compliance with E-ITS requirements and network security.

Keywords: E-ITS, NET category, network monitoring, information security, firewall, educational institution, network security, intrusion detection

CERCS: P175 Informatics, systems theory

Sisukord

Sissejuhatus

Infoturbe tagamine haridusasutustes on viimastel aastatel muutunud üha olulisemaks seoses kasvavate küberohtude ja rangemate õiguslike nõuetega. Vastavalt ettevõtlus- ja infotehnoloogiaministri 16.12.2022 määrusele nr 101 „Eesti infoturbestandard“ (RT I, 06.08.2022, 18) ning selle Lisa 1 kinnitamise määrusele nr 34 (RT I, 12.12.2022, 34) [1] on E-ITS rakendamine kohustuslik kõigile haridusasutustele, sõltumata nende omandivormist. Haridusasutused on seaduse kohaselt koolieelsed lasteasutused, põhikoolid ja gümnaasiumid, kutseõppeasutused, rakenduskõrgkoolid, ülikoolid, huvialakoolid, täiendusõppeasutused jms, samuti neid teenindavad teadus- ja metoodikaasutused. Põhikool ja gümnaasium võivad olla nii munitsipaalkoolid kui ka riigikoolid Vabariigi valitsuse otsusel. See tähendab, et kõigil nendel asutustel on kohustus tagada oma infosüsteemide vastavus E-ITSi nõuetele.

E-ITS on riiklik infoturbe raamistik, mis põhineb Saksa BSI IT-Grundschutz metoodikal ja on kooskõlas rahvusvahelise standardiga ISO/IEC 27001[2]. Standard määratleb infoturbe halduse süsteemi (ISMS) ülesehituse ning esitab konkreetsed tehnilised ja organisatsioonilised meetmed, mis aitavad tagada andmete konfidentsiaalsuse, tervikluse ja käideldavuse [3]. Haridusasutuste jaoks on E-ITSi rakendamine eriti oluline, kuna nende IT-taristu koosneb erinevatest võrkudest, seadmetest ja teenustest, mille turvalisus sõltub nende õigest kavandamisest, haldamisest ja monitoorimisest.

Käesoleva bakalaureusetöö eesmärk on analüüsida ühe haridusasutuse võrgutaristu vastavust E-ITSi NET-kategooria (NET.1–NET.3) [3] nõuetele, tuvastada puudujäägid ja pakkuda välja lahendused nende kõrvaldamiseks. Töö keskendub võrgu arhitektuurile, seadistustele ja haldusprotsessidele, sh tulemüüri, kommutaatorite ja raadiovõrkude turvalisusele. Analüüsi aluseks on asutuse osalemine Haridus- ja Teadusministeeriumi koordineeritud E-ITSi rakendamise projektis, mille käigus viidi läbi esmane riskianalüüs ja varade kaardistus.

Uuritav probleem seisneb selles, et kuigi võrgutaristu on rajatud kaasaegsete tehniliste standardite kohaselt, ei ole mitmed E-ITSi nõutud turvameetmed täielikult rakendatud või dokumenteeritud. See võib suurendada võrgu haavatavust, vähendada intsidentide avastamise võimekust ning raskendada taastamist tõrgete korral.

Bakalaureusetöö koosneb neljast põhilisest peatükist. Esimeses peatükis antakse ülevaade EITSist ja selle NET-kategooria struktuurist, rõhutades selle olulisust haridusasutuste

kontekstis. Teises peatükis kirjeldatakse olemasolevat võrgutaristut ning hinnatakse selle vastavust E-ITS NET-meetmetele. Kolmandas peatükis analüüsitakse tuvastatud puudujääke ja nende mõju võrgu turvalisusele. Neljandas peatükis esitatakse ettepanekud ja lahendused, mis viivad võrgutaristu vastavusse E-ITSi nõuetega, arvestades asutuse eripära ja ressursse.

Lisades on esitatud riskianalüüsi tulemused (Lisa 1), meetmete hindamistabel (Lisa 2), näidisdokumendid võrgu ja seadmete halduse ning turvameetmete kohta (Lisa 3–Lisa 5). Need materjalid täiendavad töö põhisisu ja pakuvad praktilisi näiteid E-ITSi nõuete rakendamise kohta.

1. Mõisted ja terminid

Konfidentsiaalsus (ingl *confidentiality*) on teabe kättesaamatus või paljastamatus volitamata isikutele, olemitele või protsessidele. Üks kolmest infoturbe põhikomponendist, märgitakse tähega C lühendis C-I-A. [2]

Terviklus (ingl *integrity*) on teabe õigsus ja täielikkus, lubamatute muudatuste puudumine, hõlmab ka autentsust ja salgamatust. Üks kolmest infoturbe põhikomponendist, märgitakse tähega I lühendis C-I-A. [2]

Käideldavus (ingl *availability*) on teabe omadus olla volitatud olemi nõudel õigel ajal kättesaadav ja kasutuskõlblik. Üks kolmest infoturbe põhikomponendist, märgitakse tähega A lühendis C-I-A. [2]

Eesti infoturbestandard (lühend E-ITS) eestikeelne ja Eesti õigusruumile vastav alus infoturbe käsitlemiseks. [2]

Infoturbe halduse süsteem (ingl *Information Security Management System*, lühend ISMS) on süsteem, mis koosneb poliitikatest, protseduuridest, juhistest ning nendega seotud ressurssidest ja tegevustest, mida organisatsioon kollektiivselt haldab, et kaitsta oma infovarasid. ISMS on suunatud ärieesmärkide saavutamisele ning kujutab endast süstemaatilist lähenemist infoturbe rajamisele, käigushoiule, seirele, hooldamisele ja täiustamisele. See põhineb riski kaalutlemisel ja selle aktsepteerimisel tasemetele, mis tagavad riskide toimiva käsitluse ja halduse. [2]

Infoturvapoliitika (ingl *Information Security Policy*) on organisatsiooni keskne infoturbealane dokument, mis sätestab arengusuunad ja taotletavad sihid ning määrab lubatu ja lubamatu. [2]

Kaitseala (saksa *Informations-verbund*) on turbekontseptsiooni koostamise ja rakendamise käsitlusala. Organisatsioon liigitab kaitsealasse kogumi sihtobjekte, mida turbeprotsess hakkab edaspidi kaitsma. [2]

Sihtobjekt (saksa *Zielobjekt*) on kaitseala allosa – igasugune infosüsteemi kuuluv kaitsetarbega vara, nagu äriprotsess, rakendus, IT-lahenduse komponent, komponendirühm, hoone, kinnistu või allüksus. Sihtobjektile vastendatakse etalonmoodul(id). [2]

Kaitsetarve (ingl *protection requirement*) on vara väärtusest tulenev vajadus seda kaitsta. Kaitsetarve on andmete ja teabe vajadus kaitsta neid kahju eest, mille võib tekitada konfidentsiaalsuse, tervikluse või käideldavuse või kõigi kolme rikkumine. E-ITSi kontekstis laieneb kaitsetarve ka äriprotsessile, mille korral hinnatakse kaitsetarvet, lähtudes kahjustsenaariumitest. Kaitsetarvet väljendatakse kolmeastmelises skaalas: „normaalne“, „suur“ või „väga suur“. [2]

Infoturbe meetmete rakendusplaan (lühend IMR) on dokument, milles loetletakse ja kirjeldatakse infoturbe halduse süsteemile kohaldatavaid turvameetmeid, põhjendatakse meetmete teostamise valikuid ning määratakse vastutajad ja tähtajad. [2]

Turvaline kest (ingl *Secure Shell*) ehk SSH on protokollisari, mis võimaldab turvalist ja krüpteeritud kaugpöördumist kaugarvutisse. [5]

Port (ingl *port*) on liides kahe võrgu vahel suhtluseks. [5]

HTTP (ingl *HyperText Transfer Protocol*) on rakenduskihi protokoll, mis määrab ära sõnumite vormingu ja edastusviisi serveri ja veebilehitseja vahel.[5]

HTTPS (ingl *HyperText Transfer Protocol Secure*) on rakenduskihi protokolli HTTP turvalisem variant, mis loob transpordikihi protokolli SSL / TLS abil krüpteeritud kanali serveri ja veebilehitseja vahel.[5]

VLAN (ingl *Virtual Local Area Network*) on loogiliselt kokkukuuluv võrgustatud olemite (tööarvutite, serverite, võrguseadmete) kogum, mis konfigureeritakse peamiselt tarkvaras, nii et olemid näivad kuuluvat ühte kohtvõrku, sõltumatult oma asukohast. [5]

DMZ (ingl *demilitarized zone*) on üüsiline ja/või loogiline alamvõrk, mis eraldab usaldatava võrgu ebausaldatavast, eriti organisatsiooni sisemise võrgu välisest võrgust, ning on "neutraalne tsoon", milles asuvad proksid serverite mõlemapoolse kättesaadavuse võimaldamiseks ja tulemüürid. [5]

Valgefiltreerimine (ingl *whitelisting*) on lubatavuse reguleerimine valge nimekirjaga. [5]

Killurünne (ingl *fragmentation attack*) on ründepakettide killustaminetulemüüride vm turvamehhanismide läbimiseks, kui need mehhanismid ei kontrolli kõiki kilde. [5]

Syslog on arvutisüsteemi sündmuste logimise protokoll. [5]

SNMP (ingl *simple network management protocol*) on võrgustatud seadmete seire ja halduse protokollistik TCP/IP-mudeli rakenduskihis. [5]

WPA2-PSK (ingl *Wi-Fi Protected Access 2 with pre-shared key*) traadita võrgu turvaprotokoll, mis krüpteerib paketipõhiste võtmetega ja senisest tugevama, AES-põhise algoritmiga. WPA2 tööviise, kasutamiseks kodus või väikekontoris; ei nõua autentimisserverit, iga seade krüpteerib võrguliikluse 256-bitise võtmega. [5]

NTP (ingl *Network Time Protocol*) on protokoll arvutikellade sünkroniseerimiseks pakettkommutatsioonvõrkudes, muutuva latentsuse tingimustes. [5]

2. Eesti Infoturbestandardi ülevaade

2.1 Mis on E-ITS?

Eesti infoturbestandard (E-ITS) on riiklik infoturbe raamistik, mis sätestab nõuded infoturbe halduse süsteemile (ISMS – *Information Security Management System*) [2]. E-ITS kehtestati ettevõtlus- ja infotehnoloogiaministri määrusega nr 101 16.12.2022. a (RT I, 06.08.2022, 18) ning selle Lisa 1 määrati määrusega nr 34 (RT I, 12.12.2022, 34)2024-01-03_EN [1]. Tegemist on kehtiva õigusaktiga, mille täitmine on kohustuslik kõigile avaliku sektori asutustele, sealhulgas üldhariduskoolidele.

E-ITSi peamine eesmärk on tagada, et organisatsioonide infosüsteemid ja äriprotsessid oleksid kaitstud kogu oma elutsükli vältel, pöörates tähelepanu andmete konfidentsiaalsusele (C), terviklusele (I) ja käideldavusele (A) [3]. Standardi rakendamine aitab ennetada andmeleket, teenusetõkestusründeid ja muid küberturbeintsidente, tagades samal ajal süsteemide usaldusväärsuse ja seadusandlusele vastavuse.

E-ITS põhineb Saksa BSI IT-Grundschutz metoodikal ning on kooskõlas rahvusvahelise standardiga ISO/IEC 27001, võimaldades sobival juhul ka sertifitseerimist [6]. Eestis haldab E-ITSi Riigi Infosüsteemi Amet (RIA), kes vastutab standardi ajakohastamise ning rakendamise toetamise eest. RIA ametlikus portaalis eits.ria.ee on kättesaadavad abimaterjalid, kontrollnimekirjad ning rakendamise juhendid asutustele.

Koolide jaoks on E-ITS eriti oluline, kuna haridusasutused töötlevad tundlikke isikuandmeid (õpilased, õpetajad, vanemad) ning kasutavad mitmekesist IT-infrastruktuuri (WiFi-võrgud, infosüsteemid, õppeplatvormid). Standardi kohaselt peab kool:

- määratlema infoturbe kaitseala (nt WiFi, Stuudium, arvutid, printerid jne);
- tuvastama sihtobjektid;
- hindama nende kaitsetarbe taset (normaalne, suur, väga suur);
- valima sobiva turbeviisi (põhi-, standard- või tuumikuturve);
- koostama infoturbe meetmete rakendusplaani (IMR);
- korraldama regulaarset auditeerimist.

Seega ei ole E-ITS pelgalt tehniline juhend, vaid osa haridusasutuste juriidilistest kohustustest, mille rakendamine tugevdab organisatsiooni vastupanuvõimet küberohtudele ning toetab jätkusuutlikku ja vastutustundlikku IT-halduse praktikat.

2.2 E-ITS-i struktuur ja loogika

Eesti infoturbestandard (E-ITS) on üles ehitatud süstemaatilise ja tsüklilise loogika alusel, mis lähtub juhtimissüsteemi põhimõtetest ning riskijuhtimisest. Standard jaguneb mitmeks temaatiliseks jaotiseks, milles kirjeldatakse infoturbe protsessi kõiki etappe alates kavandamisest ja riskihaldusest kuni käigushoiu ja täiustamiseni.

E-ITSi struktuur sisaldab järgmisi põhikomponente:

- **Infoturbe halduse süsteem (ISMS)** – organisatsiooni juhtimise osa, mis hõlmab infoturbe eesmärkide seadmist, poliitikate ja protsesside loomist, vastutuse määratlemist ning ressursside planeerimist.
- **Infoturbe protsessi tsükkel** – plaanimine, rakendamine, hindamine ja täiustamine.
- **Riskihaldus** – iga kaitstava sihtobjekti kaitsetarve määramine ja riskide hindamine. Vajadusel viiakse läbi täiendav etalonturbe väline riskianalüüs.
- **Etalonturbe meetmed** – tüüpolukordade jaoks koostatud meetmekataloog, mis võimaldab kiiresti rakendada tõendatud parimaid praktikaid.
- **Kaitseala ja sihtobjektide mõiste** – kooli kontekstis tähendab see näiteks infosüsteeme, servereid, tööjaamu, võrguühendusi, dokumente ja protsesse, mis vajavad infoturbe kaitset.
- **Turbeviisid** – vastavalt sihtobjekti kaitsetarbele ja asutuse küpsusastmele valitakse sobiv turbeviis (põhi-, standard- või tuumikuturve).
- **Rakendatavus ja auditeerimine** – E-ITSi rakendamist saab tõendada välisaudiitori hinnanguga, mida saab kasutada ka kooli sisehindamise või riikliku järelevalve käigus.

Loogiliselt on E-ITS üles ehitatud nõnda, et see ei nõua igas olukorras maksimaalseid meetmeid, vaid võimaldab organisatsioonil lähtuvalt tegelikust riskitasemest ja vajadusest

rakendada paindlikke lahendusi. See tähendab, et kool saab E-ITSi rakendada oma konteksti ja ressursside põhjal, määratledes ise, millised sihtobjektid ja riskid on prioriteetsed.

Standardi rakendamine eeldab asutuse sisese dokumentatsiooni loomist ja ajakohastamist, sh infoturvapoliitika, riskianalüüsid, protsessikirjeldused ja meetmete rakendusplaan. Eelnev aitab tagada süsteemne, jälgitav ja ajas uuenev infoturbe korraldus, mis sobitub ka haridusasutuse igapäevategevusega.

2.3 Miks see on koolide jaoks oluline

Üldhariduskoolid töötlevad ja haldavad suures mahus tundlikku teavet – sealhulgas õpilaste isikuandmeid, hinneteavet, õpilaspilte, terviseandmeid, samuti töötajate andmeid ja õppematerjale. Tundliku info turvaline käitlemine ei ole ainult eetiline kohustus, vaid õiguslik nõue, mis tuleneb isikuandmete kaitse üldmäärusest (GDPR ja IKS) [5, 6], küberturvalisuse seadusest (KüTS) [9] ning Eesti infoturbestandardist (E-ITS).

Rahvusvahelised uuringud kinnitavad, et koolid on küberkurjategijate järjest sagedasem sihtmärk, kuna nad haldavad mahukaid isikuandmete kogumeid ja kasutavad mitmekesist IKT-taristut. [10]

E-ITSi rakendamine koolis aitab:

- tagada andmete konfidentsiaalsust, terviklust ja kättesaadavust (CIA),
- ennetada küberturbeintsidente (nt lunavararünnakud, andmelekked, paroolide vargus),
- kaitsta haridusasutuse mainet ja usaldusväärsust,
- täita seadusest tulenevaid kohustusi koolijuhi tasandil,
- süsteemselt hallata riske ja planeerida kaitsemeetmeid,
- valmistuda järelevalvemenetluseks

Lisaks annab E-ITS praktilise raamistiku, mille alusel kool saab hinnata, millised süsteemid ja andmed vajavad kõrgemat kaitset ning kuidas vastavad meetmed rakendada olemasoleva taristu ja eelarve raames. Näiteks võrgu seadistamise või uuendamise puhul saab rakendada NET-kategooria meetmeid, mis võimaldavad eristada õpilaste, õpetajate ja külaliste võrke ning

jälgida võrguliiklust. Samuti on oluline, et internetiühendus saabuks korrektselt ja turvaliselt läbi tulemüüri, mis täidab kontrolli- ja kaitsefunktsiooni. Lisaks tuleb tagada korrektne haldusvõrgu eraldamine ning sobiv *trunk*- ja *access*-portide seadistamine kommutaatoritele, mis toetavad VLAN-liiklust. Kõik see tagab, et erinevad võrgusegmendid (nt serverid, teenused, töökohad, avalik WiFi) toimivad isoleeritult ja kooskõlas infoturbe põhimõtetega.

E-ITS toetab ka astmelist ja kontekstitundlikku lähenemist, mis sobib hästi koolikeskkonda. Kool saab alustada näiteks varade kaardistamisest, VLAN-segmenteerimisest või töötajate teadlikkuse tõstmisest, liikudes seejärel samm-sammult kõrgema turbetasemeni.

Tabel 1. E-ITSi rakendamise praktilised sammud koolis.

Samm	**Kirjeldus**	**Seos E-ITS-iga**
1.	Kooli IKT-taristu ja sihtobjektide kaardistamine	Kaitseala ja sihtobjektide määramine
2.	Riskide hindamine – millised süsteemid on kriitilised ja millised ohud neid ohustavad	Riskihalduse protsess
3.	Kaitsetarbe määramine (normaalne, suur, väga suur)	Kaitsetaseme määramine ja turbeviisi valik
4.	Turvameetmete valik ja rakendamine (nt WiFi paroolid, tulemüür, kontode piirangud)	Etalonturbe meetmed
5.	Dokumentatsioon (infoturvapoliitika, kasutustingimused, koolituskava)	ISMS meetod
6.	Töötajate ja õpilaste koolitamine infoturbe teemadel	Infoturbealane teadlikkus ja koolitus
7.	Regulaarne kontroll ja vajadusel auditeerimine	Käigushoid ja täiustamine

Juhtum: Koolivõrgu arhitektuuri ja tulemüüri puudulik turvamine põhjustab turvaintsidendi

Koolis kasutatakse ühte ühtset sisevõrku, kuhu on ühendatud kõik seadmed: õpetajate ja õpilaste arvutid, serverid, printerid ning WiFi tugijaamad. Klientide ja serverite võrgusegmenteerimine puudub ning kogu võrk töötab ühes loogilises segmendis ilma tsoonide eralduseta. Samuti puudub demilitariseeritud tsoon (DMZ) ning välisühendused ei ole eristatud ega kontrollitud.

Tulemüür on konfigureeritud minimaalsete reeglitega: lubatud on kõik standardsed teenused (nt HTTP, SMB, DNS, ICMP), puudub dünaamiline paketifiltreerimine (*stateful inspection*), ning tulemüür ei logi ühendusi ega tõrjub fragmenteeritud pakette (killurünnete kaitse puudub).

Ründaja kasutab ära ühe võrku ühendatud haavatava seadme (nt printeri või IoT-seadme) turvaprobleemi ning pääseb sisemisse võrku. Kuna võrk ei ole segmenteeritud ning tulemüüri reeglid ei piira sisemist liiklust, saab ründaja skaneerida võrgu ulatuses avatud teenuseid ja tuvastada sisemise kooliserveri. Serveri haldusliides on ligipääsetav ilma täiendava autentimiseta, mistõttu saab ründaja ligipääsu tundlikele dokumentidele ja paigaldab tagaukse, et säilitada püsiv ligipääs süsteemile.

Kogu selle aja jooksul ei toimu ühtegi hoiatussignaali, kuna tulemüür ei logi ebatavalist liiklust ega ühendusi. Samuti ei logita konfiguratsioonimuudatusi ega volitamata ligipääsu katsed. IT-personal ei märka intsidenti enne, kui andmed lekivad ning kooli töövood katkestatakse.

Tagajärjed:

- Kool kaotab ligipääsu oma sisemistele serveritele ja süsteemidele.
- Isikuandmed (sh hinnetelehed, õpilaste kontaktandmed jm) satuvad lekitamise ohtu.

Tabel 2. Kaitsemeetmed, mis oleksid intsidenti ennetanud.

Meetme kood	**Turvameede**	**Ennetav mõju**
NET.1.1.M4	Võrgu tsoneerimine	Eraldab sisevõrgu ja välisvõrgu tsoonideks, piirates ründaja liikumist võrgu sees.
NET.1.1.M5	Klientide ja serverite segmenteerimine	Takistab otseühendusi kriitilistele serveritele.
NET.1.2.M1	Võrguhalduse kavandamine	Võimaldab planeerida ligipääsu, logimist ja haldusvõrgu kaitset.
NET.3.2.M2	Tulemüürireeglid	Liiklus toimub ainult lubatud teenustele valge nimekirja põhimõttel.
NET.3.2.M3	Paketifiltri reeglid	Filtreerib ebatavalised TCP/UDP/ICMP paketid ja väldib staatilisi ühendusi.
NET.3.2.M4	Tulemüüri turvaline konfigureerimine	Desaktiveerib tarbetud teenused ja tagab konfiguratsiooni tervikluse.
NET.3.2.M9	Tulemüüri logimine	Võimaldab tuvastada ebatavalist või volitamata tegevust võrgu tasemel.
NET.3.2.M10	Killuründe tõrje	Väldib fragmenteeritud pakettide kaudu tehtavaid varjatud ründeid.
NET.1.2.M7	Võrgusündmuste logimine	Annab nähtavuse võrgu tegevuse ja võimalike intsidentide osas.

2.4 NET. Võrgud ja Side

E-ITS süsteemis moodustab NET-kategooria ühe tehniliselt olulisema valdkonna, mille eesmärk on tagada organisatsiooni võrgutaristu, sidekanalite ja ühenduste turvalisus. Võrk on infosüsteemide aluskiht, mille turvaline arhitektuur, haldus ja seire on võtmetähtsusega kogu süsteemi töökindluse ja kaitstuse seisukohalt.

NET-kategooria on jaotatud nelja suuremasse moodulisse [4]:

- **NET.1 – Võrgutaristu ja seadmed**,
- **NET.2 – Traadita ühendused**,
- **NET.3 – Võrguühenduste turvamine**,
- **NET.4 – Side**.

Iga moodul koosneb mitmetest meetmetest (nt NET.1.1.M1, NET.2.1.M4 jne), mis kirjeldavad konkreetseid nõudeid, protsesse ja kontrollimeetmeid, mida organisatsioon peab rakendama. Alljärgnevalt on toodud iga mooduli peamine fookus:

NET.1 – Võrgud ja side

Moodul NET.1 keskendub võrkude turvalisele arhitektuurile, dokumenteerimisele ja haldusele. See sisaldab meetmeid nagu:

- **NET.1.1 – Võrgu arhitektuur ja lahendus**, mis määratleb nõuded võrgupoliitika olemasolule, tsoneerimisele, segmenteerimisele, tundlike andmete kaitsele ja võrgu teostuskavale.
- **NET.1.2 – Võrguhaldus**, mis käsitleb võrgu monitooringut, logimist, varundust, SNMP kasutamist, sünkroniseerimist ning haldusvõrgu turvet ja dokumentatsiooni.

NET.2 – Raadiovõrgud

NET.2 moodul hõlmab kõiki traadita võrkudega seotud turvanõudeid. See sisaldab kahte alamoodulit:

- **NET.2.1 – Raadiokohtvõrgu käitamine**, kus on sätestatud nõuded traadita taristu kavandamisele, turvalisele seadistusele ja tugijaamade füüsilisele kaitsele.
- **NET.2.2 – Raadiokohtvõrgu kasutamine**, mis määrab reeglid kasutajate autentimiseks, teadlikkuse tõstmiseks ja avalikes WiFi-võrkudes tegutsemiseks.

NET.3 – Võrgukomponendid

Moodul NET.3 keskendub sideprotokollide, tulemüüride ja VPN-lahenduste turvalisusele. See sisaldab järgmisi alamooduleid:

- **NET.3.1 – Ruuter ja kommutaator**, kus sätestatakse nõuded nende seadmete konfiguratsioonile, logimisele, haldusele ja varundamisele.
- **NET.3.2 – Tulemüür**, mis määratleb tulemüüri turvajuhised, reeglid, konfiguratsiooni ja logimise nõuded.
- **NET.3.3 – Virtuaalne privaatvõrk (VPN)**, kus kirjeldatakse VPN-i rakendamise plaani, seadmete turvalisust, teenusepakkuja valikut ning konfiguratsiooni kontrolli.

NET.4 – Side

Moodul NET.4 käsitleb telefonikeskjaamade (NET.4.1) ja IP-telefoni (NET.4.2) turvalisust. Siiski ei kuulu see moodul käesoleva lõputöö analüüsi fookusesse, kuna uuritavas koolis ei ole tänasel päeval rakendatud eraldiseisvat telefonikeskjaama ega VoIP-lahendusi.

Käesoleva lõputöö fookus on seatud võrkudele, kuna koolide võrgutaristu kujundamine ja haldamine on praktikas sageli seotud riskidega. Tihti paigaldatakse võrk riigihanke korras kooli ehituse või renoveerimise käigus, kus keskendutakse esmalt funktsionaalsusele ja ühenduse kättesaadavusele, kuid infoturbe nõuded ei pruugi olla esmatähtsad.

2024. aastal valminud uue kooli puhul teostas võrgutaristu (tulemüür, kommutaatorid, WiFi tugijaamad) paigalduse ja algse konfigureerimise lepingupartner, kellelt süsteem võeti pärast seadistust üle kooli haldamiseks ja edasiseks vastutuseks.

E-ITS standardid, eelkõige NET-kategooria moodulid (NET.1–NET.3), esitavad võrgule, seadmetele ja sideprotokollidele selged turvanõuded. Osad neist on rakendatavad juba võrgu

planeerimise ja ehitamise faasis, samas kui teised nõuavad jätkutegevusi, haldust, jälgimist ja dokumenteerimist kooli igapäevase töö käigus.

Kuna osa vastutusest jääb võrgu tarnijale ja teine osa langeb kooli enda IT-spetsialistile, on oluline mõista, kus lõpeb projekti garantii ning kus algab kooli enda vastutus võrgu turvalisuse tagamisel.

Lõputöö raames analüüsitakse, millised E-ITS meetmed olid juba rakendatud seadmete üleandmisel ning milliseid täiendavaid turvameetmeid oleks olnud vajalik rakendada kooli poolt pärast süsteemi kasutuselevõttu.

3. Olemasoleva olukorra analüüs koolis

3.1 Võrgutaristu olukord kooli kasutusse andmisel

Haridusasutus liitus Haridus- ja Teadusministeeriumi (HTM) koordineeritud „E-ITS pilootprojektiga“, mille eesmärk oli alustada infoturbestandardi (E-ITS) praktilist rakendamist valitud haridusasutustes. Projekti viis ellu rahvusvaheline nõustamisettevõte EY**,** kelle toel toimus koolivõrgu esmane riskianalüüs (Lisa 1)**,** sihtobjektide määramine ja varade kaardistus. Nimetatud tegevused lõid aluse võrgu seisundi hindamiseks ning vastavuse analüüsiks E-ITS standardi NET-kategooriate lõikes.

Kooli kaitsetarve on määratud tasemele „Normaalne“, mistõttu on enamik sihtobjekte ja IT-vahendeid võimalik kaitsta etalonturbe põhimeetmete abil. Hinnatavas keskkonnas ei tuvastatud spetsiifilisi seadmeid ega lahendusi, mis oleksid tekitanud vajaduse täiendava riskihalduse või kõrgemate turvameetmete rakendamise järele. Selline olukord võimaldas keskenduda meetmete rakendamisele, mis on proportsionaalsed kooli tegelike riskidega ning tagavad jääkriski püsimise aktsepteeritaval tasemel.

Koolile anti kasutusse ehituse käigus välja ehitatud võrgulahendus, mille arhitektuur vastab Hariduse Infotehnoloogia Sihtasutuse (HITSA) standardaadressplaanile. Võrk on eelhäälestatud ja loogiliselt segmenteeritud, sisaldades olulisi turvakihte ning eraldatud teenusetsone.

3.1.1 Võrgu arhitektuur ja segmentatsioon

Võrgutaristu koosneb kolmest põhikomponendist:

1. **Juhtmega ühendus (LAN)** — CAT6 kaabeldus õpetajate töökohtadele, serveritele ja teenustele.
2. **Traadita ühendus (WiFi)** — eraldatud SSID-d töötajatele, õpilastele ja külalistele.
3. **WAN** — väline ühendus RIA võrkuga (kasutusel VLAN-untrust tsoonis).

Võrk on jagatud funktsionaalseteks VLAN-segmentideks, millest igaühele on määratud IP-alamvõrk ja turvameetmed:

Tabel 3. VLAN-segmentid.

VLAN	Kirjeldus	Märkused
8	Management	Tulemüüri ja kommutaatori haldus, lokaalne ligipääs
16	LAN – töötajad	Traadiga ühendus, õpetajate ja töötajate töökohad
24	WiFi – töötajad	Isoleerimine puudub
32	Serverid	Serverid, ilma DHCP-ta
34/36	Arvutiklassid	Iga klass oma VLAN-is
40	WiFi – külalised	Isoleeritud
42	WiFi – õpilased	Isoleeritud
50	Teenused 1	Raamatukogu, kaardiluugeja süsteem
52	Teenused 2	Valvekaamerad, IP-telefonid

3.1.2 Võrgukomponendid

Võrgu tuumik põhineb Huawei võrguseadmetel, mille konfiguratsioon oli eelhäälestatud:

- **Tulemüür**: Huawei USG6525E-AC (versioon V600R007C20SPC600), kasutusel aktiivselt kõikide ühenduste haldamiseks. Sisaldab eraldi liideseid WAN-, LAN- ja *trunk*-ühendusteks (XGE0/0/0, XGE0/0/1), mis kannavad kõiki VLAN-segmente. Seadme haldus toimub veebipõhise GUI-liidese kaudu, millele pääseb ligi ainult haldusvõrgust (VLAN8). GUI-s konfigureeritakse turvapoliitikad, NAT-reeglid, logihaldus ja süsteemiseaded. Võimalik on kasutada ka CLI lokaalse või SSH-ühenduse kaudu.
- **Kommutaatorid ja pääsupunktid (AP)**: erinevad mudelid (S5736-S24UM4XC, S5731-S24P4X, AirEngine 5761-seeria tugijaamad), mille haldus on tsentraliseeritud Huawei iMaster NCE platvormi kaudu. iMaster võimaldab seadmete konfigureerimist, VLAN-ide ja portide seadistamist, SSID-de loomist, seadmete tarkvarauuenduste haldamist, võrgu monitooringut ning sündmuselogide vaatamist. Ligipääs iMasterile on lubatud ainult haldusvõrgust ning autentimine toimub administraatori kontoga.
- **WiFi pääsupunktid**: Huawei AirEngine 5761-seeria tugijaamad, paigaldatud kõigisse klassidesse, sööklatesse, koridoridesse ja auditooriumisse. Traadita võrgud on jagatud SSID-deks ja seotud vastava VLAN-iga.

3.1.3 Turvameetmed ja haldusvõimalus

- **Tulemüüril** on konfigureeritud eraldus tsoonide vahel. WAN-liides on seotud *untrust*-tsooniga ja LAN-liidesed *trust*-tsoonidega.

- **WiFi-võrkudes** on rakendatud kasutajate isolatsioon ainult õpilaste ja külaliste võrkudes.
- **VPN-teenus** on olemas, kuid lubatud ainult haldusvõrgus kaugjuurdepääsuks. Kasutajaliides MGMT on ligipääsetav ainult lokaalselt.
- **Logimine ja monitooring** toimub piiratud mahus; olemasolev konfiguratsioon ei sisalda tsentraalset logihaldust ega IDS/IPS süsteeme.
- **DNS ja DHCP** on määratud tulemüüri tasemel igale VLAN-ile eraldi. Serverivõrkus puudub DHCP.

3.2 E-ITS NET põhimeetmete vastavuse hindamine

Alljärgnevas tabelis on toodud määratud sihtobjektid ja neile vastavad E-ITS NET-meetmed:

Tabel 4. Sihtobjektid ja neile vastavad E-ITS NET-meetmed.

Sihtobjekt	**Kirjeldus**	**Vastavad NET-meetmed**
V001 Võrk	LAN, WAN, WiFi, VPN	NET.1.1, NET.1.2, NET.2.1, NET.2.2, NET.3.3
V002 Võrguseadmed	Eulemüür, kommutaatorid, pääsupunktid ja pääspunktid	NET.1.1, NET.1.2, NET.3.1, NET.3.2, NET.3.3

Käesoleva töö raames hinnati vastavust ainult põhimeetmetele NET-moodulites (NET.1.1, NET.1.2, NET.2.1, NET.2.2, NET.3.1, NET.3.2, NET.3.3). Standardmeetmete eesmärke on võimalik osaliselt katta ka teiste E-ITS moodulite (nt SYS, APP, CON) kaudu, tuginedes alusohtude viitetabelile. Kõrgmeetmeid ei hinnatud ega rakendatud, kuna riskianalüüsi (Lisa 1) tulemused ei näidanud riske üle taseme „Keskmine“ ja jääkrisk jäi aktsepteeritavale tasemele. Meetmete vastavuse hindamisel kasutati viiepunktilist hindamissüsteemi koos täiendava kommentaariga iga meetme kohta:

Tabel 5. E-ITSi meetmete hindamissüsteem[11].

Teostatusmärge	**Märke sisu**	**Kommentaar**
R	Rakendatud	Turvameede on teostatud täielikult, tõhusalt ja otstarbekalt.
O	Osaliselt rakendatud	Meede on teostatud vaid osaliselt; vajab täiendavat juurutamist või dokumenteerimist.
E	Ei ole rakendatud	Meede on teostamata või teostatud ebaolulisel määral, kuid vajab rakendamist.

P	Pole asjakohane	Meetme teostamine pole vajalik ega konkreetsete sihtobjektide puhul asjakohane (näiteks teenuste aktiveerimatuse tõttu). Meetme mitterakendamine ei avalda mõju asutuse infoturbele.
A	Aksepteeritud risk	Meede on rakendamata, kuid seotud risk on saanud juhtkonna tasemel aksepteeringu ning selle kohta on olemas kirjalik kinnitus.

Tabel 6. E-ITSi meetmete hindamise kokkuvõte.

Teostatus	**Meetmete arv**	**Osakaal**
R – Rakendatud	20	35 %
O – Osaliselt rakendatud	16	28 %
E – Ei ole rakendatud	14	25 %
P – Pole asjakohane	7	12 %
A – Aksepteeritud risk	0	0 %
Kokku: 57 meetmest		

Tabel 7. E-ITSi meetmete hindamistulemuste näited.

Meede	**Teostatus**	**Kommentaar**
NET.3.2.M2 – Tulemüürireeglid	O – Osaliselt rakendatud	Reeglid on kehtestatud ja sisene/väljuv liiklus toimub läbi tulemüüri, kuid puudub reeglite täielik dokumentatsioon, erandite haldus ja vastutajate määramine.
NET.3.2.M3 – Sobivad filtreerimisreeglid paketifiltris	E – Ei ole rakendatud	Tulemüüri konfiguratsioon ei sisalda dünaamilise paketifiltri (*stateful inspection*) reegleid TCP/UDP/ICMP liikluse, ega vigaste TCP lippude kombinatsioonide blokeerimist.
NET.3.2.M10 – Killuründe tõrje paketifiltris	E – Ei ole rakendatud	Killuründe vastased mehhanismid (nt IPv4/IPv6 fragmentatsiooni blokeerimine) ei ole aktiveeritud tulemüüris.
NET.3.2.M22 – Tulemüüri kellaaja sünkroniseerimine	R – Rakendatud	Tulemüür sünkroniseerib kellaaega usaldusväärse NTP-serveriga ning muud sünkroniseerimisallikad on blokeeritud.

3.2.1 Näiteid rakendatud meetmetest

Alljärgnevalt on esitatud neli põhimeedet, mis kooli võrgukeskkonnas on täielikult rakendatud ning mille teostatus kinnitati tehnilise analüüsi ja seadistuste kontrolli kaudu.

NET.1.1.M5 – Klientide ja serverite võrgusegmentide eraldamine

Kooli võrgu dokumentatsioonis, mis edastati kasutuselevõtu käigus, on selgelt määratletud

VLAN-struktuur, kus serverid paiknevad eraldatud VLAN-is (VLAN32) ning kliendiseadmed teistes segmentides (nt VLAN16, VLAN24). Võrgu turvapoliitika määrangud tulemüüris (*Security Policy*) näitavad, et tsoonidevaheline suhtlus on vaikimisi keelatud (*all deny*), välja arvatud lubatud ühendus VLAN16 ja VLAN32 vahel, mis toimub *any-any* põhimõttel. Sellest hoolimata on serverivõrgus täiendav tulemüür, mis piirab lubatud liiklust. Logide analüüs kinnitas, et kõik lubamata ühendused blokeeriti ning logikirjed sisaldasid ka vastavaid lähte- ja sihtporte.

NET.1.2.M9 – Võrguhalduse side turve

Võrguhalduseks kasutatakse eraldatud haldusvõrku (VLAN8), millele on ligipääs ainult määratud haldussüsteemidest. Ligipääs toimub turvaliste protokollide (HTTPS, SSH, SNMPv3) kaudu ning tulemüüri seadistused piiravad ühendusi kindlate IP-aadresside põhjal. Dokumentatsioon ja tulemüüri turvapoliitika kinnitavad, et haldusvõrgul puudub otsene internetiühendus. Haldusliikluse marsruut on lahendatud VPN-ühenduse kaudu haldusserverisse, kust edasi toimub IPsec-tunnel USG6525E tulemüüri.

NET.1.2.M10 – SNMP-side piiramine

Huawei USG6525E tulemüüri seadistustes (*System* → *Setup* → SNMP) on määratud SNMP kasutamiseks ainult turvaline versioon v3. Ligipääs SNMP-le on piiratud haldusvõrgu kindlate IP-aadressidega, mis välistab volitamata päringud teistest võrkudest. Ebavajalikud ja ebaturvalised SNMP versioonid (v1, v2c) on keelatud, tagades, et võrgu seire- ja haldusside toimub ainult krüpteeritult ja autentitult.

NET.3.2.M9 – Tulemüüri logimine

Tulemüüri logifunktsioonid on seadistatud vastavalt E-ITS nõuetele, logides kõik olulised turvasündmused, sealhulgas sisselogimiskatsed, konfiguratsioonimuudatused, blokeeritud ühendustaotlused ning süsteemiteated. Logide toimimist kontrolliti praktilise testimise teel – viidi läbi ebaõnnestunud sisselogimiskatsed ja tehti konfiguratsioonimuudatusi, mille järel kontrolliti logikirjeid *Monitor*-vaates. Kõik sündmused registreeriti korrektselt. Logid kogutakse automaatselt tulemüüris, kuid neid ei edastata tsentraalsesse logihaldussüsteemi.

3.3 Riskide ja haavatavuste hinnang

Läbiviidud võrgustruktuuri analüüs ja infoturbemeetmete hindamine näitasid, et kooli võrk on kaasaegselt üles ehitatud ning sisaldab mitmekesiseid tehnilisi võimalusi. Samas ilmnesid mitmed olulised kitsaskohad, mis võivad mõjutada võrgu usaldusväärsust ja infoturvalisust.

Peamised tuvastatud probleemivaldkonnad võib koondada nelja laiemasse kategooriasse:

1. **Dokumentide vähesus**

Võrguga seotud tehniline ja halduslik dokumentatsioon eksisteerib osaliselt, kuid see ei ole süsteemselt koondatud ega ühtlustatud. Puuduvad koondülevaated võrgu arhitektuurist, seadistustest ning haldusprotseduuridest, mis raskendab võrgu haldamist ja tõrgete analüüsi.

2. **Logimise ja jälgimise piiratus**

Kuigi võrgu põhikomponentidel on logifunktsioonid olemas, ei toimu süstemaatilist sündmuste logimist ega tsentraalset logide kogumist. Logide kategooriline katvus on piiratud ning intsidentide tuvastamine ja analüüs on seetõttu ebatõhus.

3. **Turvamehhanismide puudulik rakendamine**

Mitmed üldtuntud tehnilised kaitsemehhanismid, nagu dünaamiline paketifiltreerimine, killurünnete tuvastus ja eriliikide (nt ICMP, UDP) kontroll, ei ole konfigureeritud või on konfigureeritud vaid osaliselt. See jätab võrgu avatuks spetsiifilistele ründetüüpidele.

4. **Varundus- ja taastamispoliitika ebaselgus**

Puudub süsteemne lähenemine konfiguratsioonide, seadistuste ja kriitiliste teenuste andmete varundamisele. Samuti ei ole määratletud taastamiskorraldus võimalike rikete või intsidentide puhuks.

Kuigi tuvastatud probleemid ei pruugi avalduda koheselt igapäevases töös, loovad need akumuleeruva riski, mis võib kriitilises olukorras takistada reageerimist, põhjustada andmekadu või võimaldada loata juurdepääsu süsteemidele.

Arvestades, et praegune riskianalüüs ei tuvastanud riske üle taseme „Keskmine“ ning need on kaetud põhimeetmete või teiste moodulite kaudu, tuleb organisatsioonil edaspidistes riskihindamise tsüklites arvestada võimalusega rakendada ka standardmeetmeid. See on eriti oluline juhul, kui riskitase tõuseb või kui selgub, et praegused meetmed ei kata kõiki tuvastatud ohte piisaval määral.

4. Puudujääkide analüüs

E-ITS nõuete rakendamine koolikeskkonnas on võrdlemisi uus protsess, mille praktika kujuneb alles välja. Haridusasutuse puhul on käesolev hinnang esimene põhjalikum võrgutaristu vastavuse kontroll E-ITS NET-meetmete lõikes. Kuigi võrgu arhitektuur ja seadistused vastavad üldjoontes kaasaegsetele standarditele ning on rajatud kogenud teenusepakkuja Dateli poolt, näitas analüüs, et mitmed meetmed on rakendatud vaid osaliselt või üldse mitte.

Käesoleva analüüsi käigus ei hinnatud meedet **NET.3.3 Virtuaalne privaatvõrk (VPN)**, kuna see on hinnangus märgitud kui *pole asjakohane*. VPN-lahendust kasutatakse koolis üksnes administraatori kaugühenduseks haldusserverisse, mistõttu ei kuulu see töö fookusesse.

Esimene ja kõige ilmsem puudujääk puudutab dokumentatsiooni. Olemasolev dokumentatsioon on pigem tehnilise inventuuri tasemel ning ei sisalda kõiki E-ITS-is nõutavaid üksikasju, näiteks tsoonide vaheliste ühenduste täielikku kirjeldust, tulemüürireeglite dokumenteeritud erandeid või vastutajate määramist. Seadmete ja võrgu esmane seadistus on tehtud vastavalt teenusepakkuja praktikatele, kuid teatud konfiguratsioonielementide (näiteks tsentraalse logihalduse seadistamine, varukoopiate säilitamine ja kontroll) täiendamine on jäetud kooli IT-spetsialisti hooleks. See on loonud olukorra, kus osa turvameetmeid ei ole juurutatud või on juurutatud osaliselt, mis vähendab võrgu vastupanuvõimet võimalike rünnete või intsidentide korral.

Käesolevas peatükis kirjeldatakse üksikasjalikult neid meetmeid, mille teostatus hindamistabelis (Lisa 2) on märgitud kui *Ei ole rakendatud* (E) või *Osaliselt rakendatud* (O). Iga puudujäägi puhul on esitatud ülevaade tehtust ja tingimustest, mis vajavad rakendamist.

4.1 Dokumentide puudulikkus

E-ITS standard nõuab, et võrguarhitektuur, tsoonide vahelised ühendused ja tulemüürireeglid oleksid dokumenteeritud piisava detailsusega, et võimaldada nende regulaarset ülevaatust ja ajakohastamist. Kuna kooli võrk rajati enne nende nõuete jõustumist, piirdub dokumentatsioon peamiselt seadmete inventuuri tasemega.

Puudujäägid ilmnesid tulemüüri konfiguratsiooni ja seadmete seadistuse analüüsi käigus. Huawei USG6525E tulemüüri *WEB GUI* liideses (*Policy → Security Policy*) teostati

turvapoliitikate täiseksport, mille põhjal hinnati reeglite lähte- ja sihttsoone, IP-aadresse ja lubatud teenuseid. Analüüs näitas, et kogu VLAN-idest väljuv liiklus välisvõrku (*untrust*) oli lubatud üldise reegliga *any–any*, ilma teenuse- või aadressipiiranguteta. Lisaks puudusid E-ITS nõutud mehhanismid, nagu liiklus- ja sessioonilogide salvestamine ning IPS-profiilide rakendamine. Selline seadistus vähendab oluliselt võimalust kontrollida, milline liiklus on lubatud, ja raskendab lubamatu tegevuse tuvastamist.

4.2 Tulemüüri konfiguratsiooni puudused

Tulemüüri seadistust võrreldi E-ITS NET.3.2 ja NET.1.1 meetmete nõuetega, keskendudes rakendamata või osaliselt rakendatud punktidele. Kontroll viidi läbi logides sisse tulemüüri *WEB GUI* kaudu ning vajadusel kasutati käsurida käske detailsema konfiguratsiooni ülevaatamiseks.

Analüüs näitas, et kuigi vaikimisi keelav reegel oli olemas, oli enamik tsoonidevahelisest ja väljuvast liiklusest lubatud any–any põhimõttel (NET.3.2.M3). Puudusid TCP-, UDP- ja ICMP-liikluse filtreerimisreeglid *whitelisting*-põhimõttel. Samuti olid jaotises *Policy → Security Protection → Attack Defense → Single-Packet Attack* kõik kaitsemehhanismid välja lüllitatud (NET.3.2.M10), sealhulgas *IP Fragment, Teardrop, Ping of Death* ja *TCP Flag* kaitse. Vastavate seadete puudumine jätab tulemüüri haavatavaks teatud tüüpi ühepaketiliste rünnete suhtes.

Need puudused viitavad, et kuigi tulemüür täidab oma põhiülesande tsoonide eraldamisel, ei ole rakendatud olulisi kaitsekihte ja monitooringumeetmeid, mis on E-ITS nõuete kohaselt vajalikud.

4.3 Logimise, monitooringu ja varunduse puudused

E-ITS nõuete kohaselt tuleb kõigi võrgu põhikomponentide – tulemüüride, kommutaatorite ja tugijaamade – logisid koguda tsentraalselt, säilitada turvaliselt ning analüüsida regulaarselt. Kooli seadmetel selline lähenemine hetkel puudub.

Huawei iMaster halduskeskkonna kontroll näitas, et kommutaatorite sündmuselogid salvestatakse ainult lokaalselt. *Syslog* serveri aadressi ei olnud määratud, mistõttu seadmetelt pärit logid ei liigu tsentraalsesse logihaldussüsteemi. Täiendava kontrolli käigus avati

USG6525E tulemüüri menüüd *Policy → Security Policy ja Content Security*, kus tuvastati, et üheski turvapoliitikas ei olnud seotud sissetungituvastuse ega -tõrje profiile (IDS/IPS). See tähendab, et ründe- ja anomaaliatuvastus puudub nii tulemüüri kui ka teiste võrgukomponentide tasandil.

Varunduse osas selgus, et USG6525E tulemüüris (*System → Configuration File Management*) on salvestatud ainult seadme esmakonfiguratsioon, automaatne varundamine ja väline salvestuskoht puuduvad. Huawei iMasteris (*Monitoring and O&M → Maintain → Device Maintenance → Configuration File Managemen*t) olid saadaval vaid vaikimisi stardifailid, automaatseid varundustöid ei olnud määratud ja konfiguratsioonide ajalugu puudus. Selline lähenemine tähendab, et rikke või konfiguratsioonivea korral sõltub kogu taastamine käsitsi toimingutest, mis võib põhjustada pikemaid töökatkestusi ja andmekadu.

4.4 Raadiokohtvõrk

Kooli raadiokohtvõrgu turvameetmeid hinnati vastavuses E-ITS NET.2.1 ja NET.2.2 nõuetega. Kontroll viidi läbi Huawei iMaster halduskeskkonnas, kasutades menüüd *Plan → Provision → Device Configuration → Site Configuration → AP → WiFi*, kus iga SSID puhul vaadati üle *Basic Settings, Security Authentication* ja *Policy Control* seadistused.

Selgus, et kõik SSID-d kasutavad WPA2-PSK autentimist ning RADIUS-serverit või WPA2-Enterprise lahendust ei ole rakendatud. Paroolide regulaarset vahetust ei toimu, mis suurendab riski, et kompromiteeritud parooliga pääseb võrku volitamata isik. Lisaks ei olnud aktiveeritud volitamata tugijaamade tuvastus (*Rogue AP detection*) ning püsivara uuendusi ei teostatud automaatselt. Puudus ka tegevusplaan juhuks, kui pääsupunkt varastatakse või kaob. Kuigi õpilaste ja külaliste võrkudes oli aktiveeritud kliendieraldus (*Client Isolation*), jäid mitmed teised kriitilised turvameetmed rakendamata.

5. Parandusettepanekud ja lahendused

Käesolev peatükk sisaldab soovitusi ja lahendusi, mis on otseselt seotud eelmises peatükis kirjeldatud puudustega. Eesmärk on viia kooli võrgutaristu ja seotud protsessid vastavusse Eesti Infoturbestandardi (E-ITS) NET.1–NET.3 kategooria nõuetega, arvestades asutuse eripära ja olemasolevaid ressursse. Ettepanekud on esitatud soovituslikus vormis, kuid tuginevad tuvastatud mittevastavustele ja parimatele praktikale IT-turbe valdkonnas.

5.1 Dokumenteerimise täiustamine

Analüüsi käigus selgus, et dokumentatsioon, mis on seotud meetmetega NET.1.1.M1, NET.1.1.M2, NET.1.1.M13, NET.1.2.M1, NET.1.2.M2, NET.1.2.M11, NET.2.1.M1, NET.2.2.M1, NET.3.1.M9, NET.3.2.M1, NET.3.2.M14 on osaliselt puudulik või ei sisalda kõiki E-ITS-i nõutud elemente. Praegune dokumentatsioon on peamiselt inventuurilaadne ning ei paku täielikku ülevaadet võrgu arhitektuurist, tsoonidevahelistest ühendustest ega tulemüürireeglite eranditest.

Nagu rõhutavad Chaudhuri ja Shoemaker [10], tuleb infoturvet käsitleda kõigil tasanditel. Alates töökohtade ja serverite kaitsmisest kuni kogu võrgu turvalisuse tagamiseni. E-ITS põhimeetmete rakendamine, sealhulgas dokumentatsiooni täiustamine, aitab vähendada süsteemi haavatavust ja tõsta vastupanuvõimet küberohtudele.

Vastavuse saavutamiseks tuleb koostada eraldiseisvad ja selgelt piiritletud dokumendid, mis hõlmavad võrgu haldust ja turvalisust (NET.1.1.M1, NET.1.1.M2, NET.1.1.M13, NET.1.2.M1, NET.1.2.M2, NET.1.2.M11), raadiokohtvõrgu haldamise korda (NET.2.1.M1, NET.2.2.M1) ning võrgu- ja turvaseadmete käidudokumentatsiooni ja turvajuhendit (NET.3.1.M9, NET.3.2.M1, NET.3.2.M14). Kõik dokumendid tuleb hoida turvalises keskkonnas, näiteks *Microsoft SharePoint'i* piiratud ligipääsuga alas, dokumentide registris või NAS-serveris, kus on rakendatud kasutusõiguste kontroll ja logimine. Dokumentide ajakohastamine peab toimuma regulaarselt, vähemalt kord aastas või kohe pärast olulisi muudatusi võrgus. Iga dokumendi eest tuleb määrata vastutav isik, et tagada pidev vastavus E-ITS-i nõuetele.

Lisaks on töö Lisa 3, Lisa 4 ja Lisa 5 osas esitatud näidisdokumendid koos väljamõeldud andmetega, mis illustreerivad, kuidas nõutud dokumente saab vormistada ja milliseid

struktuurielemente neis kasutada. Need näited on mõeldud mallidena, mida saab kohandada vastavalt kooli tegelikele andmetele ja vajadustele.

Oluline tõsta kooli töötajate teadlikkust ja pädevust küberohtude ennetamisel ning reageerimisel. Uuringud näitavad, et inimfaktor on üks peamisi küberrünnakute õnnestumise põhjuseid haridusasutustes [10]. Regulaarne infoturbealane koolitus ja juhendmaterjalide tutvustamine aitavad vähendada inimtegevusest tulenevaid riske, õpetades töötajaid ära tundma potentsiaalseid ohte (nt andmepüügi e-kirjad, pahavara) ja käituma intsidentide korral vastavalt turvaprotokollidele. Teadlik ja koolitatud personal on võrdselt tähtis osa tehniliste turvameetmete kõrval, suurendades märkimisväärselt kooli vastupanuvõimet küberohtudele.

5.2 Tulemüüri konfiguratsiooni täiustamine

Kuigi vaikimisi *deny all* poliitika oli seadistatud, olid tsoonidevahelised reeglid loodud põhimõttel *any–any*, mis ei vasta *whitelisting*-põhimõttele (NET.3.2.M2). Selleks tuleb lubada ainult tööks vajalikud teenused ja protokollid, mille nimekiri täpsustatakse pärast dokumentatsiooni korrastamist ja logimise täiustamist. Vaikimisi lubatud teenuste hulka võiks kuuluda näiteks HTTPS (TCP/443), DNS (UDP/53 ja TCP/53) ning ICMP võrgu tõrkeotsingu eesmärgil. Vajaduse korral võib lisada ka NTP (UDP/123) ajasünkroonimiseks. Külaliste WiFi-võrgus tuleks lubada vaid HTTPS ja DNS, välistades muu liikluse. Oluline on enne piirangute kehtestamist põhjalikult analüüsida olemasolevat võrguühenduste kasutust, et vältida oluliste teenuste (nt operatsioonisüsteemide värskendused või andmebaasiühendused) tahtmatut blokeerimist. Sobivate filtreerimisreeglite rakendamiseks (NET.3.2.M3) tuleb lisada täiendav kaitse vigaste TCP-lippude kombinatsioonide vastu. Huawei tulemüüri seadetes aktiveeritakse see funktsioon järgmiselt [9]:

```
system-view

firewall defend tcp-flag enable

quit
```

Tulemüüri haldusliideste turvalisuse tõstmiseks (NET.3.2.M6) on soovitatav piirata haldusjuurdepääs kindlate IP-aadressidega ja kasutada turvalisi protokolle, lisades ka ajapiirangud, näiteks tööpäeviti kell 07:00–18:00.

Killurünnete tõrjeks (NET.3.2.M10) tuleb aktiveerida mehhanismid IPv4 ja IPv6 killurünnete vastu [12]:

```
system-view

firewall defend ip-fragment enable

quit
```

Kõik tehtud muudatused tuleb lisada käidudokumentatsiooni, et tagada nende jälgitavus ja vastavuse tõendatavus.

5.3 Logimise, monitooringu ja varunduse rakendamine

Logimise ja monitooringu puhul on oluline, et kõik võrgu põhikomponentide sündmused, veateated ja alarmid koonduksid tsentraalsesse logihaldusesse (NET.1.2.M1). Selle saavutamiseks tuleb seadistada logide edastus nii Huawei iMasteri kui ka USG tulemüüri tasemel Syslog-serverisse, kasutades selleks eraldi turvapoliitikat, mis tagab logiedastuse turvalisuse.

Varundamise puhul (NET.1.2.M6 ja NET.3.1.M8) tuleb aktiveerida automaatsed varundustööd. Huawei iMasteris tuleb seada igakuised varundused, mis salvestatakse turvalisse NAS-serverisse SFTP-protokolli kaudu. Varundamise alla kuuluvad keskse võrguhalduslahenduse seadistused. USG6525E tulemüüri puhul tuleb seadistada konfiguratsioonifailide regulaarne varundamine NAS-serverisse FTP-protokolli kaudu (kuna SFTP tuge seadmel ei ole). Varukoopiad hoitakse eraldatud turvalises võrgualas, et tagada kättesaadavus avariiolukorras.

Lisaks tuleb seadistada turvapoliitikad, mis lubavad varundus- ja logiedastuse puhul ainult vajalikud protokollid ja IP-aadressid, vähendades seeläbi võimalikke turvariske.

5.4 Raadiovõrgu turvameetmete rakendamine

Raadiovõrgu turvalisuse tõstmiseks on soovitatav jätkata WPA2-PSK autentimismehhanismi kasutamist (NET.2.1.M3), kuna see on kasutajamugavuse seisukohalt sobivaim lahendus

olukorras, kus raadiovõrku kasutavad kõik õpilased alates 1. kuni 12. klassini. Parooli keerukus peab vastama nõuetele (vähemalt 20 märki) ning see tuleb vahetada regulaarselt kord aastas.

Lisaks tuleb aktiveerida volitamata pääsupunktide tuvastus (*Rogue AP detection*) (NET.2.1.M5), et ennetada kõrvaliste seadmete ühendamist kooli võrku. Püsivara uuendused viiakse läbi käsitsi tootjapoolse uuendusteate saamisel, kuid vähemalt kord kuue kuu jooksul tuleb teostada manuaalne kontroll värskenduste olemasolu kohta ja paigaldada need viivitamata. Samuti tuleb dokumenteerida tegevusplaan juhuks, kui pääsupunkt varastatakse või kaob, et tagada kiire ja koordineeritud reageerimine.

Kokkuvõte

Käesoleva bakalaureusetöö eesmärk oli analüüsida ühe haridusasutuse võrgutaristu vastavust Eesti infoturbestandardi (E-ITS) NET-kategooria nõuetele, tuvastada puudujäägid ning pakkuda välja lahendused nende kõrvaldamiseks. Analüüs viidi läbi osana Haridus- ja Teadusministeeriumi koordineeritud E-ITSi rakendamise projektist, mille käigus teostati riskianalüüs, varade kaardistus ja võrgu seadistuste ülevaatus.

Töö käigus kirjeldati olemasolevat võrgutaristut, hinnati selle vastavust E-ITSi meetmetele ning toodi välja rakendamata või osaliselt rakendatud turvameetmed. Täpsemalt käsitleti dokumenteerimise, tulemüüri konfiguratsiooni, logimise, monitooringu, varundamise ja raadiovõrgu turvalisuse puudusi. Puudujääkide analüüs põhines nii seadmete konfiguratsiooni tehnilisel kontrollil kui ka E-ITSi nõuete võrdlusel tegeliku olukorraga.

Töö tulemusena koostati soovitused ja tehnilised juhised, mis võimaldavad viia võrgu arhitektuuri, seadistused ja haldusprotsessid vastavusse E-ITSi NET-kategooria nõuetega. Pakutud lahendused hõlmavad muu hulgas võrgu- ja tsoonidokumentatsiooni täiendamist, tulemüüri reeglite ja kaitsemehhanismide täiustamist, tsentraalse logihalduse ja automaatse varunduse rakendamist ning raadiovõrgu turvameetmete parendamist.

Positiivse tulemusena leiti, et võrgu arhitektuuris on juba rakendatud VLAN-segmentatsioon serverite ja kliendivõrkude vahel ning tulemüür logib edukalt kõiki blokeeritud ühendusi, võimaldades intsidente tuvastada reaalajas.
Samas tuvastati puudusena, et tulemüüris puuduvad dünaamilise paketifiltri (stateful inspection) reeglid ja killurünnete tõrje mehhanismid ning olemasolevad Security Policy reeglid vajavad ümberseadistamist whitelisting-põhimõttel. Nende meetmete rakendamine eeldab süvendatud teadmisi Huawei USG6525E konfiguratsioonist ja võrgu turvapoliitika detailset haldust.

Lõputöö käigus analüüsiti põhjalikult konkreetse haridusasutuse näitel võrgu vastavust E-ITS nõuetele ja soovitustele. Dokumentatsiooni ja seadistuse uurimise tulemusena tuvastati asjakohased puudujäägid ning pakuti välja rakendatavad lahendused, mis tõstavad võrgu turvalisuse taset ja vastavust E-ITSile. Valminud analüüsi ja ettepanekute põhjal on võimalik edaspidi lahendusi rakendada mitte ainult uuritud haridusasutuses, vaid ka teistes koolides, sealhulgas uue võrgu loomisel või teenusepakkujalt võrgulahenduse tellimisel. See tagab, et

võrgutaristu kavandamine ja haldamine toimub alates algusest E-ITSi nõuetele vastavalt, vähendades tulevasi turvariske ja tagades töökindluse pikemas perspektiivis.

Viidatud kirjandus

[1] Riigi Teataja, „Eesti infoturbestandardi määrus“. Vaadatud: 11. august 2025. [Online]. Available at: https://www.riigiteataja.ee/akt/130012024007?leiaKehtiv

[2] „E-ITS nõuded infoturbe halduse süsteemile“. Vaadatud: 11. august 2025. [Online]. Available at: https://eits.ria.ee/et/versioon/2023/eits-poohidokumendid/eits-noouded-infoturbe-halduse-suesteemile

[3] „E-ITS Kaitsetarbe määramine“. Vaadatud: 11. august 2025. [Online]. Available at: https://eits.ria.ee/et/abimaterjalid/rakendusjuhend/samm-4

[4] Riigi Infosüsteemi Amet, „Eesti Infoturbestandard“. 2023.

[5] „ANDMEKAITSE JA INFOTURBE PORTAAL“. Vaadatud: 12. august 2025. [Online]. Available at: https://akit.cyber.ee/

[6] M. Seeba, R. Matulevičius, ja I. Toom, „Development of the Information Security Management System Standard for Public Sector Organisations in Estonia“, *Bus. Inf. Syst.*, lk 355–366, juuli 2021, doi: 10.52825/bis.v1i.43.

[7] Euroopa Parlamendi ja nõukogu määrus (EL) 2016/679). 2016. Vaadatud: 11. august 2025. [Online]. Available at: http://data.europa.eu/eli/reg/2016/679/2016-05-04/est

[8] Riigi Teataja, „Isikuandmete kaitse seadus“. Vaadatud: 11. august 2025. [Online]. Available at: https://www.riigiteataja.ee/akt/104012019011?leiaKehtiv

[9] Riigi Teataja, „Küberturvalisuse seadus Riigi Teataja“. Vaadatud: 11. august 2025. [Online]. Available at: https://www.riigiteataja.ee/akt/106082022018?leiaKehtiv

[10] A. Chaudhuri ja D. Shoemaker, „Cyber-attack on schools – steps toward resilience“, *EDPACS*, kd 0, nr 0, lk 1–9, doi: 10.1080/07366981.2025.2503627.

[11] „E-ITS Infoturbe meetmete rakendusplaani koostamine“. Vaadatud: 11. august 2025. [Online]. Available at: https://eits.ria.ee/et/abimaterjalid/rakendusjuhend/samm-7

[12] „Single-Packet Attack Defense Configuration Commands“. Vaadatud: 11. august 2025. [Online]. Available at: https://info.support.huawei.com/hedex/api/pages/EDOC1100149308/AEJ0713J/18/resources/cli/single_picket_con.html

Lisad

Lisa 1. Riskianalüüs

Ohu tähis	Ohu nimetus	Kahju	Sagedus	Riskiaste	Peamiselt mõjutatud sihtobjektid
G 0.1	Tuli	Tõsine	Harv	Keskmine	IT-süsteemid ja riistvarakomponendid Taristu
G 0.2	Halvad keskkonnatingimused	Piiratud	Harv	Madal	IT-süsteemid ja riistvarakomponendid Taristu
G 0.3	Vesi	Piiratud	Harv	Madal	IT-süsteemid ja riistvarakomponendid Taristu
G 0.4	Määrdumine, tolm, korrosioon	Piiratud	Harv	Madal	IT-süsteemid ja riistvarakomponendid Taristu
G 0.5	Loodusõnnetused	Tõsine	Harv	Keskmine	IT-süsteemid ja riistvarakomponendid Taristu
G 0.6	Keskkonnaõnnetused	Tõsine	Harv	Keskmine	IT-süsteemid ja riistvarakomponendid Taristu
G 0.7	Suurüritused	Piiratud	Harv	Madal	IT-süsteemid ja riistvarakomponendid Taristu
G 0.8	Toitekatkestus või toitehäire	Piiratud	Harv	Madal	Kogu kaitseala
G 0.9	Sidevõrkude tõrge või häire	Piiratud	Harv	Madal	Võrgukomponendid
G 0.10	Tehnovõrkude tõrge või häire	Tõsine	Harv	Keskmine	
G 0.11	Teenusetarnete tõrge või häire	Piiratud	Harva	Madal	Rakendused ja tarkvarakomponendid

G 0.12	Elektromagnethäired	Tõsine	Harv	Keskmine	Võrgukomponendid IT-süsteemid ja riistvarakomponendid
G 0.13	Paljastava parasiitkiirguse püük	Piiratud	Harv	Madal	IT-süsteemid ja riistvarakomponendid
G 0.14	Spionaaž	Tühine	Harv	Madal	Kogu kaitseala
G 0.15	Pealtkuulamine	Piiratud	Harv	Madal	Võrgukomponendid
G 0.16	Seadmete, andmekandjate ja dokumentide vargus	Piiratud	Harv	Madal	IT-süsteemid ja riistvarakomponendid
G 0.17	Seadmete, andmekandjate ja dokumentide kaotamine	Piiratud	Harv	Madal	IT-süsteemid ja riistvarakomponendid
G 0.18	Halb kavandamine või sobitamata jätmine	Tõsine	Harv	Keskmine	Kogu kaitseala
G 0.19	Kaitset vajava teabe avalikustamine	Tõsine	Keskmine	Keskmine	Rakendused ja tarkvarakomponendid
G 0.20	Ebausaldatavast allikast pärit teave või tooted	Tõsine	Keskmine	Keskmine	Rakendused ja tarkvarakomponendid IT-süsteemid ja riistvarakomponendid
G 0.21	Riistvara või tarkvara manipuleerimine	Tõsine	Harv	Keskmine	IT-süsteemid ja riistvarakomponendid
G 0.22	Informatsiooni manipuleerimine	Tõsine	Harv	Keskmine	Rakendused ja tarkvarakomponendid
G 0.23	Lubamatu sisenemine IT-süsteemidesse	Tõsine	Keskmine	Keskmine	IT-süsteemid ja riistvarakomponendid
G 0.24	Seadmete või andmekandjate hävitus	Piiratud	Harv	Madal	IT-süsteemid ja riistvarakomponendid
G 0.25	Seadmete või süsteemide tõrge	Piiratud	Keskmine	Keskmine	Kogu kaitseala
G 0.26	Seadmete või süsteemide väärtalitlus	Piiratud	Sage	Keskmine	Kogu kaitseala
G 0.27	Ressursside puudumine	Tõsine	Keskmine	Keskmine	Kogu kaitseala

G 0.28	Tarkvara nõrkused või vead	Piiratud	Sage	Keskmine	Rakendused ja tarkvarakomponendid
G 0.29	Õigusnormi või eeskirjade rikkumine	Tõsine	Keskmine	Keskmine	Rakendused ja tarkvarakomponendid
G 0.30	Seadmete ja süsteemide lubamatu kasutus	Tõsine	Harv	Keskmine	Kogu kaitseala
G 0.31	Seadmete ja süsteemide väärkasutus	Tõsine	Keskmine	Keskmine	Kogu kaitseala
G 0.32	Volituste kuritarvitus	Piiratud	Keskmine	Keskmine	Kogu kaitseala
G 0.33	Personali puudumine	Tõsine	Keskmine	Keskmine	Kogu kaitseala
G 0.34	Rünne	Tõsine	Harv	Keskmine	Kogu kaitseala
G 0.38	Isikuandmete väärkasutus	Piiratud	Keskmine	Keskmine	Rakendused ja tarkvarakomponendid
G 0.35	Sundus, väljapressimine ja korruptsioon	Piiratud	Harv	Madal	Rakendused ja tarkvarakomponendid
G 0.36	Identiteedivargus	Piiratud	Harv	Madal	Kogu kaitseala
G 0.37	Toimingute salgamine	Piiratud	Harv	Madal	Rakendused ja tarkvarakomponendid
G 0.39	Kahjurprogrammid	Piiratud	Sage	Keskmine	Rakendused ja tarkvarakomponendid
G 0.44	Lubamatu sisenemine ruumidesse	Piiratud	Keskmine	Keskmine	Taristu
G 0.40	Teenusetõkestus	Piiratud	Harv	Madal	Kogu kaitseala
G 0.41	Sabotaaž	Piiratud	Harv	Madal	Kogu kaitseala
G 0.42	Psühholoogiline manipuleerimine	Piiratud	Harv	Madal	Kogu kaitseala
G 0.43	Sõnumite süstimine	Piiratud	Harv	Madal	Rakendused ja tarkvarakomponendid
G 0.45	Andmekaotus	Tõsine	Keskmine	Keskmine	Rakendused ja tarkvarakomponendid

G 0.46	Kaitsetarbega informatsiooni tervikluse kadu	Tõsine	Harv	Keskmine	Rakendused ja tarkvarakomponendid
L 0.2	Piisavat kaitset mitte tagavad lepingud partneritega	Tõsine	Keskmine	Keskmine	Kogu kaitseala
G 0.47	IT-põhiste rünnete kahjulikud kõrvaltoimed	Piiratud	Harv	Madal	Kogu kaitseala
L 0.1	Personali vähene infoturbeteadlikkus	Tõsine	Keskmine	Keskmine	Kogu kaitseala

Lisa 2. E-ITS NET võrgud ja side meetmed

Turvameetme kood	Turvameetme nimetus	Meetme rakendatus
NET.1.1.M1	Võrgu turvapoliitika	**E**
NET.1.1.M13	Võrgu teostuskava	**E**
NET.1.1.M15	Võrgu vastavuskontroll	**O**
NET.1.1.M2	Võrgulahenduse dokumentatsioon	**O**
NET.1.1.M4	Võrgu tsoneerimine	**O**
NET.1.1.M8	Internetti pääsu alusturve	**O**
NET.1.1.M9	Turvaline andmevahetus ebausaldusväärsete võrkudega	**O**
NET.1.2.M1	Võrguhalduse kavandamine	**O**
NET.1.2.M2	Võrguhalduse nõuete spetsifitseerimine	**E**
NET.1.2.M11	Võrguhalduse juhend	**O**
NET.1.2.M6	Regulaarne andmevarundus	**E**
NET.2.1.M1	Raadiokohtvõrkude kavandamine	**E**
NET.2.1.M2	Sobiv raadiokohtvõrgu standard	**O**
NET.2.1.M3	Turvaline krüptomehhanism	**O**
NET.2.1.M5	Pääsupunkti turvaline seadistus	**O**
NET.2.1.M8	Raadiokohtvõrgu intsidendikäsitluse kord	**O**
NET.2.2.M1	Raadiokohtvõrgu kasutamise eeskiri	**E**
NET.2.2.M2	Raadiokohtvõrgu kasutajate teadlikkuse tõstmine ja koolitus	**O**
NET.2.2.M3	Raadiokohtvõrgu kasutamine avalikes raadiokohtvõrkudes	**E**
NET.3.1.M1	Ruuteri või kommutaatori turvaline baaskonfiguratsioon	**O**
NET.3.1.M4	Ruuteri või kommutaatori haldusliideste turve	**O**
NET.3.1.M9	Ruuteri või kommutaatori käidudokumentatsioon	**E**
NET.3.1.M5	Kaitse IP-pakettide fragmenteerimisrünnete eest	**E**
NET.3.1.M8	Regulaarne andmevarundus	**E**
NET.3.2.M1	Tulemüüride turvajuhend	**E**
NET.3.2.M4	Tulemüüri turvaline konfigureerimine	**O**
NET.3.2.M14	Käidudokumentatsioon	**E**
NET.3.2.M2	Tulemüürireeglid	**O**
NET.3.2.M3	Sobivad filtreerimisreeglid paketifiltris	**E**
NET.3.2.M10	Killuründe tõrje paketifiltris	**E**

Lisa 3. Võrgu halduse ja turvalisuse dokumentatsioon (näidis)

1. Võrgu turvapoliitika

Võrgu turvapoliitika on kehtestatud lähtuvalt organisatsiooni üldisest infoturvapoliitikast. Dokument määratleb nõuded ja juhised võrgu turvaliseks kavandamiseks ja kasutamiseks. Poliitika eesmärk on tagada võrgu konfidentsiaalsus, terviklus ja käideldavus.

Võrgu turvapoliitika sisaldab vähemalt järgmisi põhimõtteid:

(*Punktis toodud andmed täidetakse vastavalt organisatsiooni tegelikule olukorrale ja vajadustele*)

- Võrk segmentitakse vastavalt turvanõuetele.
- Lubatud on ainult määratletud andmesidekanalid ja protokollid.
- Võrguhalduse ja -seire liiklus eraldatakse muust liiklusest.
- Andmeliiklus krüpteeritakse vastavalt vajadusele.
- Andmevahetus teiste organisatsioonidega on reguleeritud.
- Võrgus on vaikimisi **"deny all"** reegel, lubatud liiklus määratakse erandina.

Võrgu turvapoliitika muudatusettepanekud ja lahknevused dokumenteeritakse ning nendest informeeritakse infoturbejuhti. Võrgu turvapoliitika nõuetekohast rakendamist kontrollitakse regulaarselt ning kontrolli tulemused dokumenteeritakse.

2. Võrgulahenduse dokumentatsioon

Võrgulahenduse dokumentatsioon sisaldab ülevaadet võrgu loogilisest ülesehitusest, alamvõrkude ja tsoonide kirjeldust ning tehtud muudatusi. Dokument hoitakse ajakohasena.

2.1 Alamvõrgud

VLAN	**Alamvõrk (IP/mask)**	**Default Gateway**	**DNS server**	**DHCP (jah/ei)**	**Märkused**
10	10.10.10.0/24	10.10.10.1	10.10.10.5	ei	Õpetajate sisevõrk
20	10.10.20.0/24	10.10.20.1	10.10.10.5	jah	Õpilaste sisevõrk
99	10.10.99.0/24	10.10.99.1	10.10.10.5	ei	Haldusvõrk

2.2 Tsoonid

Tsoon	Seotud VLAN / liides	Märkused
LAN-Teachers	VLAN 10	Õpetajate sisevõrk
LAN-Students	VLAN 20	Õpilaste sisevõrk
MGMT	VLAN 99	Haldusvõrk ainult IT-personalile

2.3 Tulemüüri tsoonide reeglid

Lähte tsoon	Siht tsoon	Lähte aadress/piirkond	Siht aadress/piirkond	Lubatud port/protokoll	Märkused
LAN-Teachers	Internet	Any	Any	TCP 80, TCP 443	Veebiliiklus õpetajatele
LAN-Students	Internet	Any	Any	TCP 443	HTTPS ainult
MGMT	LAN-Teachers	10.10.99.10	10.10.10.10	TCP 22	SSH haldusserverisse

3. Võrgu teostuskava

3.1 Internetiühendus

Teenusepakkuja	WAN IP	Varuühendus (jah/ei)	Märkused
Telia	85.253.10.2	jah	Optiline põhiliin
Elisa	194.126.55.18	ei	4G varuühendus puudub
Telia	85.253.10.3	ei	Eraldi IP IPsec-ühenduse jaoks

3.2 IPsec või muud VPN-ühendused

Ühenduse nimetus	Sihtkoht	Märkused
HQ-VPN	194.126.55.50	Peakontoriga püsiv IPsec
Admin-VPN	85.253.10.3	Kaugjuurdepääs halduseks
PartnerVPN	212.47.100.12	Partnerorganisatsiooniga andmevahetus

4. Võrguhalduse kavandamine

Seadme nimetus	Mudel	IP-aadress	Haldusliides (VLAN/tsoon)	Ühendusviis	Lokaalne ligipääs (jah/ei)
CoreSwitch1	Huawei S5736-S24UM4XC	10.10.99.2	VLAN 99	SSH	jah
Firewall1	Huawei USG6525E-AC	10.10.99.1	VLAN 99	HTTPS	jah
AP1	Huawei AirEngine 5761-21	10.10.99.20	VLAN 99	SSH	ei

5. Võrguhalduse nõuete spetsifitseerimine

5.1 Haldusvahendid

Haldusvahend / tarkvara	Eesmärk	Server/host	IP-aadress	Autentimine	Märkused
Unifi Controller	Wi-Fi haldus	Server1	10.10.99.10	LDAP	WLAN seadistamine
Zabbix	Võrgu monitooring	Server2	10.10.99.11	AD	Seire ja häired
SolarWinds	Võrguliikluse analüüs	Server3	10.10.99.12	Local	NetFlow analüüs

5.2 Haldusprotsessi etapid

Etapi nimi	Kirjeldus	Vastutaja	Kord/sagedus	Märkused
Konfiguratsioonimuudatused	Võrguseadmete seadistuste uuendamine	IT-admin	vastavalt vajadusele	Muudatused dokumenteeritakse
Logide ülevaatus	Logide analüüs intsidentide tuvastamiseks	IT-admin	kord kuus	Automaatsed raportid
Pääsuõiguste audit	Võrgupääsuõiguste kontroll	Infoturbejuht	kord kvartalis	

6. Võrguhalduse juhend

6.1 Kasutatavad võrguteenused ja haldusvahendid

Teenus / vahend	Eesmärk	Server/host	IP-aadress	Autentimine	Märkused
RDP	Serverihaldus	Server4	10.10.99.15	AD	Admin serverite haldus
SNMPv3	Võrguseadmete seire	Server2	10.10.99.11	SNMPv3	Krüpteeritud seire
HTTPS	Tulemüüri haldus	Firewall1	10.10.99.1	AD	Ainult IT-võrgust

6.2 Võrguhaldustegevused

Tegevus	Kirjeldus	Keskselt tehtav (jah/ei)	Automatiseeritud (jah/ei)	Vastutaja	Märkused
VLAN loomine	Uue alamvõrgu lisamine	jah	ei	IT-admin	Muudatus dokumenteeritakse

Pääsuloendi uuendamine	Tulemüüri reeglite muutmine	jah	ei	IT-admin	Kooskõlastus infoturbejuhiga
Varukoopia te tegemine	Seadmete konfiguratsiooni de varundamine	jah	jah	IT-admin	Säilitatakse 90 päeva

6.3 Turbemeetmed

Valdkond	**Rakendatud meetmed**	**Märkused**
Autentimine	Kahefaktoriline autentimine VPN-is	Ainult administraatoritele
Logimine	Keskne logiserver (Syslog)	Säilitus 1 aasta
Võrguliikluse kaitse	ACL-id ja tulemüürireeglid	Vaikimisi "deny all" poliitika

Lisa 4. Raadiokohtvõrgu haldamise kord (näidis)

1. Üldsätted

1.1. Käesolev kord kehtestab organisatsiooni raadiokohtvõrgu (WLAN) kavandamise, kasutamise ja haldamise põhimõtted, eesmärgiga tagada võrguteenuste turvaline, tõhus ja otstarbekas toimimine.
1.2. Kord on koostatud vastavalt organisatsiooni infoturbepoliitikale ning lähtub E-ITS nõuetest, sh meetmetest NET.2.1.M1 ja NET.2.2.M1.
1.3. Korda kohaldatakse kõigile töötajatele, lepingupartneritele ja muudele isikutele, kellel on juurdepääs organisatsiooni WLAN-ile.

2. Raadiokohtvõrgu kavandamine

2.1. Enne WLAN-i kasutuselevõttu koostatakse kirjalik kava, milles määratakse: *(Punktis toodud andmed täidetakse vastavalt organisatsiooni tegelikule olukorrale ja vajadustele.)*
a) WLAN-i kasutamise eesmärgid ja selle lisandväärtus organisatsiooni äriprotsessides, sealhulgas interneti kättesaadavuse suurendamine töötajatele, õpilastele ja külalistele, tööprotsesside efektiivsuse parandamine ning juhtmevaba infrastruktuuri kulude vähendamine;
b) geograafilised asukohad ja tsoonid, kus WLAN-i rakendatakse;
c) WLAN-i kaudu toetatavad funktsioonid ja rakendused;
d) andmeliigid, mida ei ole lubatud WLAN-i kaudu edastada;
e) WLAN-i turvanõuded.

2.2. Kava peab sisaldama ka WLAN-taristu haldamise eest vastutavate isikute määramist, teavitusteid ning kehtivaid haldusprotseduure, sealhulgas: *(Haldusprotseduuride täpne sisu määratakse vastavalt organisatsiooni töökorraldusele ja turvanõuetele.)*
• turvaintsidentide lahendamise kord koos reageerimisaja ja eskalatsiooniprotsessiga;
• seadmete hooldus- ja uuenduspoliitika (sh tarkvarauuendused ja turvapaigad);
• konfiguratsioonide varundamise ja taastamise protseduur;
• võrguseadmete ja pääsupunktide regulaarse ülevaatuse sagedus;
• WLAN-kasutuse aruandluse ja järelevalve kord.

2.3. Kava vaadatakse läbi ja ajakohastatakse vähemalt üks kord kahe kalendriaasta jooksul või olulis(t)e muudatus(t)e korral WLAN-taristus.

3. Vastutused ja teavitamine

3.1. WLAN-i haldamise eest vastutab organisatsiooni määratud pädev isik (edaspidi vastutav isik).
3.2. Vastutav isik tagab WLAN-i vastavuse kehtestatud turvanõuetele, dokumentatsiooni ajakohastamise ning kasutajate teavitamise muudatustest.
3.3. Turvaintsidentidest tuleb teavitada vastutavat isikut viivitamata, kasutades organisatsiooni poolt määratud ametlikke teavitusteid (nt e-posti aadress, telefon).

4. Raadiokohtvõrgu kasutamise eeskiri

4.1. WLAN-i kasutamine peab toimuma kooskõlas käesoleva korra ning organisatsiooni infoturbepoliitikaga.
4.2. Lubatud on ühendada ainult organisatsiooni poolt määratud sisemiste ja väliste võrkudega, mille loetelu on toodud käesoleva korra Lisa 1-s ja mida ajakohastatakse vastutava isiku poolt.
4.3. WLAN-i paroolid peavad vastama organisatsiooni paroolipoliitikale (minimaalselt 20 märki, sh suured ja väikesed tähed, numbrid ning erisümbolid).
4.4.Keelatud on:
a)ad-hoc ühenduste loomine;
b) isiklike pääsupunktide (AP) ühendamine organisatsiooni kohtvõrguga;
c) WLAN-seadete muutmine ilma vastutava isiku kirjaliku loata;
d) failikataloogide ja teenuste jagamine ilma eelneva kooskõlastuseta;
e) Käesolevasse punkti kantakse loetelu andmetest ja teabest, mille edastamine WLAN-i kaudu on keelatud vastavalt organisatsiooni turvapoliitikale ja tulemüüri seadistustele (Lisa 2);
f) Kõik WLAN-i kasutavad kliendiseadmed (sh organisatsiooni omandis olevad seadmed, töötajate isiklikud seadmed ja külaliste seadmed) peavad vastama organisatsiooni määratud miinimumnõuetele turvavahendite osas (Lisa 3).
4.5. Pikema kasutuspausi järel tuleb WLAN-liides seadmes välja lülitada, kui see on tehniliselt võimalik.
4.6. Turvaintsidendi korral peab kasutaja:
a) viivitamata katkestama WLAN-ühenduse;
b) teavitama vastutavat isikut;
c) järgima vastutava isiku edasisi juhiseid (sh paroolide vahetamine, ligipääsu piiramine)

5. Järelevalve ja sanktsioonid

5.1. Vastutav isik kontrollib käesoleva korra järgimist regulaarselt, kuid mitte harvem kui üks kord kalendriaastas. Kontrolli tulemused dokumenteeritakse ja säilitatakse vähemalt kolm aastat.
5.2. Kontrollimisel tuvastatud rikkumiste korral võetakse tarvitusele meetmed vastavalt organisatsiooni sisekorraeeskirjale ja infoturbepoliitikale.

Lisa 1 – WLAN SSID ja VLAN määrangud

SSID nimi	VLAN ID	Kasutusala	Eripiirangud / Märkused
Opetajad	10	Õpetajate võrk	Täielik ligipääs sisemistele teenustele
Opilased	20	Õpilaste võrk	Ligipääs piiratud, keelatud pääs serveritele
Kylalised	30	Külaliste võrk	Ainult internetiühendus, sisemised teenused keelatud

Lisa 2 – WLAN-is keelatud andmed ja teave

Andmete tüüp / teabe liik	Keelu põhjus	Märkused
Õpilaste isikuandmed ja õpitulemused	Isikuandmete kaitse ja GDPR nõuete täitmine	Lubatud ainult krüpteeritud kanalite kaudu (nt VPN)
Kooli siseeelarve ja finantsandmed	Ärisaladuse ja finantsinfo kaitse	Ainult sisevõrkude kaudu, mitte avalikus WLAN-is

Lisa 3 – Kliendiseadmete turvavahendite miinimumnõuded

Seadme tüüp	Turvavahendi nõue	Märkused
Organisatsiooni seadmed	Viirusetõrje, tulemüür, krüpteerimine	Nõuded rakendatakse MDM poliitikatega
Töötajate isiklikud seadmed	Viirusetõrje, tulemüür	Kontrollitakse võrguühenduse loomisel
Külaliste seadmed	—	Ligipääs ainult külalisvõrgus, tulemüür piirab

Lisa 5. Võrgu- ja turvaseadmete käidudokumentatsioon ja turvajuhend (näidis)

1. Eesmärk

1.1. Käesoleva dokumendi eesmärk on kehtestada võrgu- ja turvaseadmete (sh ruuterid, kommutaatorid, tulemüürid, VPN-seadmed) käidudokumentatsiooni ja turvalise käituse nõuded vastavalt infoturbe standardi E-ITS meetmetele NET.3.1.M9, NET.3.2.M1 ja NET.3.2.M14.
1.2. Dokument on kohaldatav kõikidele organisatsiooni hallatavatele võrguseadmetele ja nende konfiguratsioonidele.

2. Mõisted

2.1. **Käidudokumentatsioon** – dokumenteeritud andmestik seadmete konfiguratsioonide, muudatuste ja hooldustegevuste kohta.
2.2. **Turvajuhend** – juhendmaterjal, mis kirjeldab turvanõudeid ja -protseduure seadmete turvaliseks käitamiseks.

3. Üldnõuded käidudokumentatsioonile

3.1. Käidudokumentatsioon peab sisaldama vähemalt:
a) seadmete identifitseerimisandmed tabeli kujul:

Seadme nimi	Tüüp	Mudel	Tootja	Seerianumber	Asukoht	IP-aadress(id)	MAC-aadress(id)	VLAN konfiguratsioon
SW1	Kommutaator	S5735-L48T4XE-A-V2	Huawei	GM0CD3TW	Serveriruum 1	10.4.10.2	00:1A:2B:3C:4D:5E	Port 1–12 VLAN 10 (Teachers), Port 13–24 VLAN 20 (Students)
R1	Ruuter	USG6525E-AC	Huawei	GM0CD3VC	Serveriruum 2	172.29.72.1	00:1B:44:11:3A:B7	VLAN10 – Admin, VLAN20 – Õpilased

b) seadmete konfiguratsioonifailid või nende väljavõtted;
c) kõik konfiguratsioonimuudatused koos kuupäeva, muudatuse kirjelduse, põhjenduse ja

teostaja nimega. Kõik konfiguratsioonimuudatused dokumenteeritakse viivitamata pärast muudatuse teostamist;
d) hooldustööd, sealhulgas tarkvara- ja püsivara uuendused;
e) turvameetmete rakendamise kirjeldus.

3.2. Käidudokumentatsioon võib olla paberkandjal ja/või digitaalsel kujul. Digitaalse dokumentatsiooni puhul peavad olema loodud regulaarsed varukoopiad ning tagatud nende turvaline hoiustamine. Dokumentatsioon peab olema kaitstud loata juurdepääsu eest ning kättesaadav ainult volitatud isikutele.

3.3. Käidudokumentatsiooni säilitusaeg on vähemalt kolm aastat.

4. Tulemüüride turvajuhend

4.1. Tulemüüride haldus ja käitamine peab toimuma kooskõlas organisatsiooni infoturvapoliitikaga.

4.2. Tulemüüride konfiguratsioon peab vastama turvalise käituse nõuetele, sealhulgas:
a) lubatud on ainult vajalikud teenused ja protokollid;
b) haldusliidesed on ligipääsetavad üksnes määratud IP-aadressidest või haldusvõrgust;
c) kõik muudatused tulemüüri reeglites dokumenteeritakse koos põhjendustega;
d) tulemüüri konfiguratsiooni terviklus on tagatud krüptograafiliste või muude sobivate meetmetega;
e) tarbetud teenused ja funktsionaalsus on keelatud;
f) tulemüüride logisid analüüsitakse regulaarselt ning neid säilitatakse vähemalt 12 kuud, et võimaldada turvaintsidentide uurimist.

4.3. Turvajuhendi järgimist kontrollitakse vähemalt kord aastas ning alati pärast olulisi muudatusi võrguarhitektuuris või tulemüüri konfiguratsioonis. Kontrollimisel võib kasutada ka konfiguratsiooni testimist ja vajaduse korral turvatestimist (nt lubatud/keelatud teenuste kontroll, võrgu sissetungi simulatsioon), et veenduda turvajuhendi nõuete täitmises.

5. Käidudokumentatsioon tulemüüri kohta

5.1. Käidudokumentatsioon peab sisaldama:

a) kõiki tulemüüri turvalisust mõjutavaid toiminguid (reeglite lisamine, muutmine, kustutamine; konfiguratsiooni ja teenuste muudatused);

b) muudatuste põhjendusi ja kuupäevi;

c) muudatuste teostajate ja kinnitajate andmeid. Kinnitaja peab olema infoturbe eest vastutav isik.

5.2. Dokumentatsioon peab olema hoitud turvalises keskkonnas, milleks on krüpteeritud andmehoidla või server, millele on piiratud ligipääs ja logitud kõik juurdepääsud.

5.3. Muudatuste logi:

Kuupäev	Seade	Muudatuse kirjeldus	Põhjendus	Teostaja	Kinnitaja	Mõju turvalisusele
01.08.2025	Firewall1	Lisatud deny all reegel VLAN20-le	Piirata õpilaste ligipääsu	Admin	Infoturbe juht	Positiivne
15.08.2025	Firewall1	Avatud port 443 VLAN52 teenustele	Teenuste toimimiseks vajalik	Admin	Infoturbe juht	Neutraalne

6. Käidudokumentatsioon ruuteri ja kommutaatori kohta

6.1. Käidudokumentatsioon peab sisaldama:
a) seadme konfiguratsiooni põhiseadeid ja turvameetmeid;
b) konfiguratsioonimuudatusi koos põhjenduste ja kuupäevadega. Kõik konfiguratsioonimuudatused dokumenteeritakse viivitamata pärast muudatuse teostamist;
c) olulisi käidutöid, sealhulgas riist- ja tarkvarauuendusi;
d) muudatusi võrguportide ja teenuste seadistustes.

6.2. Dokumentatsioon peab olema kaitstud volitamata juurdepääsu eest.

7. Hooldustööde logi

Kuupäev	Seade	Hooldustöö kirjeldus	Teostaja	Märkused
20.08.2025	SW1	Tarkvarauuendus versioonile 3.5.1	Admin	Edukalt lõpetatud
21.08.2025	Firewall1	Puhastatud vanad reeglid	Admin	Testitud ja töötav

8. Jõustumine ja ülevaatus

8.1. Käesolev dokument jõustub alates kinnitamise kuupäevast.
8.2. Dokumenti vaadatakse üle vähemalt kord aastas või pärast olulisi muudatusi võrgus või seadmete konfiguratsioonis.

Lisa A – Käidudokumentatsiooni töölehed

Need tabelid on mõeldud võrgu- ja turvaseadmete käidudokumentatsiooni ja muudatuste logide täitmiseks. Dokument täidetakse jooksvalt ning hoitakse turvalises keskkonnas vastavalt käesoleva juhendi nõuetele.

A.1. Seadmete identifitseerimisandmete tabel (ruuterid ja kommutaatorid)

Seadme nimi	Tüüp	Mudel	Tootja	Seerianumber	Asukoht	IP-aadress(id)	MAC-aadress(id)	VLAN konfiguratsioon
SW1	Kommutaator	S5735-L48T4XE-A-V2	Huawei	GM0CD3TW	Serveriruum 1	10.4.10.2	00:1A:2B:3C:4D:5E	Port 1–12 VLAN 10 (Teachers), Port 13–24 VLAN 20 (Students)
R1	Ruuter	USG6525E-AC	Huawei	GM0CD3VC	Serveriruum 2	172.29.72.1	00:1B:44:11:3A:B7	VLAN10 – Admin, VLAN20 – Õpilased

A.2. Tulemüüri muudatuste logi

Kuupäev	Seade	Muudatuse kirjeldus	Põhjendus	Teostaja	Kinnitaja	Mõju turvalisusele
01.08.2025	Firewall1	Lisatud deny all reegel VLAN20-le	Piirata õpilaste ligipääsu	Admin	Infoturbe juht	Positiivne
15.08.2025	Firewall1	Avatud port 443 VLAN52 teenustele	Teenuste toimimiseks vajalik	Admin	Infoturbe juht	Neutraalne

A.3. Hooldustööde logi

Kuupäev	Seade	Hooldustöö kirjeldus	Teostaja	Märkused
20.08.2025	SW1	Tarkvarauuendus versioonile 3.5.1	Admin	Edukalt lõpetatud
21.08.2025	Firewall1	Puhastatud vanad reeglid	Admin	Testitud ja töötav

Lisa 6. Litsents

Lihtlitsents lõputöö reprodutseerimiseks ja üldsusele kättesaadavaks tegemiseks

Mina, Ivan Strikkojev

(autori nimi)

1. annan Tartu Ülikoolile tasuta loa (lihtlitsentsi) minu loodud teose

Eesti infoturbestandardi võrgud ja side mooduligrupi rakendamine haridusasutusele,

(lõputöö pealkiri)

mille juhendaja on Alo Peets,

(juhendaja nimi)

reprodutseerimiseks eesmärgiga seda säilitada, sealhulgas lisada digitaalarhiivi DSpace kuni autoriõiguse kehtivuse lõppemiseni.

2. Annan Tartu Ülikoolile loa teha punktis 1 nimetatud teos üldsusele kättesaadavaks Tartu Ülikooli veebikeskkonna, sealhulgas digitaalarhiivi DSpace kaudu Creative Commonsi litsentsiga CC BY NC ND 4.0, mis lubab autorile viidates teost reprodutseerida, levitada ja üldsusele suunata ning keelab luua tuletatud teost ja kasutada teost ärieesmärgil, kuni autoriõiguse kehtivuse lõppemiseni.

3. Olen teadlik, et punktides 1 ja 2 nimetatud õigused jäävad alles ka autorile.

4. Kinnitan, et lihtlitsentsi andmisega ei riku ma teiste isikute intellektuaalomandi ega isikuandmete kaitse õigusaktidest tulenevaid õigusi.

Ivan Strikkojev

12.08.2025