26.04.2022

Ettevõtlus- ja infotehnoloogiaministri määruse „Eesti infoturbestandard“ eelnõu seletuskiri

1. Sissejuhatus

Eelnõu eesmärk on kehtestada Eesti infoturbestandard.

Eesti infoturbestandardi (edaspidi *E-ITS*) siht on arendada ning edendada Eesti avaliku sektori asutuste ja erafirmade infoturbe taset. E-ITS-i eesmärk on esitada eestikeelne ja Eesti õigusruumile vastav alus infoturbe käsitlemiseks, mis ühtlasi vastaks rahvusvahelisele standardile ISO/IEC 27001:2017 (Infotehnoloogia. Turbemeetodid. Infoturbe halduse süsteemid. Nõuded).[1] E-ITS esitab etalonturbe rakendamise süsteemi, mis aitab organisatsioonil saavutada tema vajadustega sobivat infoturbe taset.

Organisatsiooni juhtkond ise otsustab, milliseid objekte ja protsesse on tarvis kaitsta. Etalonturve seab kaitstavad objektid ja protsessid vastavusse etalonturbe kataloogi tüüpmoodulitega. Etalonturbe kataloogis leiduvad tüüpmoodulid kirjeldavad tüüpilisi ohte ja neile vastavaid, riskianalüüsi põhjal valitud turvameetmeid. Turvameetmete rakendamine vähendab infoturbeohtude realiseerumise tõenäosust. Etalonturve võimaldab organisatsioonil taaskasutada infoturbe parimaid praktikaid ning seeläbi kokku hoida infoturbe rakendamisele kuluvaid vahendeid.

Standard põhineb Saksa etalonturbe süsteemil BSI IT-Grundschutz (BSIG) ja standardil EVS-ISO/IEC 27001:2014 "INFOTEHNOLOOGIA. Turbemeetodid. Infoturbe halduse süsteemid. Nõuded".[2]

Määruse eelnõu ja seletuskirja koostasid Majandus- ja Kommunikatsiooniministeeriumi riikliku küberturvalisuse osakonna küberturvalisuse õigusnõunikud Raavo Palu (e-post: raavo.palu@mkm.ee) ja Oliver Grauberg (oliver.grauberg@mkm.ee).

Eelnõu ja seletuskirja osas tegi õiguslikke ettepanekuid Majandus- ja Kommunikatsiooniministeeriumi õigusosakonna õigusnõunik Ave Henberg (e-post: ave.henberg@mkm.ee; telefon: 6256360).Eelnõu ja seletuskirja toimetas keeleliselt Majandus- ja Kommunikatsiooniministeeriumi riikliku küberturvalisuse osakonna küberturvalisuse õigusnõunik Raavo Palu (e-post: raavo.palu@mkm.ee).

2. Eelnõu sisu ja võrdlev analüüs

Eelnõu koosneb kahest paragrahvist, millest esimene on EITS-i kehtestamine ja järgimine ning teine on määruse jõustumine.

Määruse volitusnormideks on küberturvalisuse seadusesse (edaspidi *KüTS*) lisanduv KüTS § 7 lg 5 ning sama lõike alusel antava Vabariigi Valitsuse määruse „Võrgu- ja infosüsteemide küberturvalisuse nõuded“ (edaspidi *VV määrus*) § 3 lõige 1. KüTS-i täiendamine toimub

[1] Standard leitav ning võimalik osta siit: https://www.evs.ee/et/evs-en-iso-iec-27001-2017.
[2] E-ITS-i lühijuhend, punkt 1 – kättesaadav: https://eits.ria.ee/et/versioon/2020vers1/juhendid/luehijuhend/.

küberturvalisuse seaduse, avaliku teabe seaduse ja Eesti Rahvusringhäälingu seaduse muutmise seaduse 531 SE (edaspidi *531 SE*)[3] tulemusena.

KüTS § 7 lõige 5 võimaldab Vabariigi Valitsusel või tema volitatud ministril kehtestada määrusega samas paragrahvis sätestatud kohustuste täitmise ning võrgu- ja infosüsteemide (edaspidi *süsteem*) küberturvalisuse tagamiseks:
1) infoturbe halduse nõuded, üldnimetusega Eesti infoturbestandard;
2) turvameetmete üldnõuded;
3) süsteemide turvameetmete erinõuded ning nende kohaldamise ulatuse.

VV määruse § 3 lõike 1 kohaselt kehtestab E-ITS-i üleriigilise küberturvalisuse tagamise korraldamise eest vastutav minister määrusega. Eelnõu koostamise ajal E-ITS-i kehtestajaks ettevõtlus- ja infotehnoloogiaminister. Lisaks Riigi Teatajale avaldatakse E-ITS-i sisu ka Riigi Infosüsteemi Ameti poolt portaalis.[4]

531 SE seletuskirjas (seaduseelnõu § 1 punkti 10 selgitused lk-del 14-15) on siinse eelnõuga kehtestatava määruse kohta selgitatud:
„Eelnõu lisaks olev kavandatav Vabariigi Valituse määrus annab üleriigilise küberturvalisuse tagamise korraldamise eest vastutavale ministrile (kelleks eelnõu koostamise hetkel on ettevõtlus- ja infotehnoloogiaminister) volituse kehtestada E-ITS (kui dokument ise) määrusega. Selleks sätestatakse eelnõu punktiga ka edasivolituse võimalus. E-ITS-i kehtestamine on otstarbekam läbi viia edasivolituse alusel ministri määrusega, sest praktikas võimaldab ministri määruse kehtestamine vastavalt vajadusele dokumenti ajakohastada tulenevalt pidevalt muutuvast IKT raamistikust. See siiski ei tähenda, et teised osapooled (sh ministeeriumid jt asutused) ei saaks osaleda ning kaasa rääkida E-ITS-i sisu uuendamisel ja sisustamisel. Seaduseelnõus ei kasutata sõnastust „valdkonna eest vastutav minister“, sest tulevikus võib tekkida vajadus kavandatavas Vabariigi Valitsuse määruses sätestada edasivolitust võimaldav norm erinevate valitsusalade ministritele, ning sellises olukorras valdkonna täpsustamata jätmine seaduseelnõus võib tekitada õigusselgusetust, et milline minister millise valdkonna eest vastutab. E-ITS kehtestamine käskkirjaga ei ole võimalik, kuivõrd E-ITS-i kehtestamine ei ole käsitletav üksikjuhtumi reguleerimisena. [….]

Vabariigi Valitsusele on ette nähtud võimalus määruse andmist edasi volitada kogu volitusnormi ulatuses. Jääb Vabariigi Valitsuse otsustada kas volitatakse, ning kui jah, siis mis ulatuses käesolevas volitusnormis sätestatud nõuete kehtestamist ministrile edasi volitatakse.

Edasivolituse eesmärk on ministeeriumi valitsemisalade valdkondade korraldamise võimaldamine. Volitusnormi esimeses kahes lõikes tähendab see avaliku sektori digiarengu ja üleriigilise küberturvalisuse tagamise juhtimise, korraldamise ja järelevalve võimaldamist ning kolmandas lõikes ka iga valitsusala korraldamise võimaldamist, kui reguleerimisobjektiks on konkreetsele valitsusalale iseloomulike süsteemide pidamine.

Edasivolituse ulatuse samastamine volitusnormiga on vajalik seetõttu, et iga volitus võib hõlmata eriliigilisi regulatsioone, mis lähtuvalt oma eripärast peaksid olema reguleeritud Vabariigi Valituse tasandil või ministri määrusega. Näiteks, kui Vabariigi Valitsus kehtestaks

[3] Küberturvalisuse seaduse, avaliku teabe seaduse ja Eesti Rahvusringhäälingu seaduse muutmise seadus 531 SE – kättesaadav: https://www.riigikogu.ee/tegevus/eelnoud/eelnou/cd3107f9-b19c-4ed4-b6a7-7379fa3bf6b9/K%C3%BCberturvalisuse%20seaduse,%20avaliku%20teabe%20seaduse%20ja%20Eesti%20Rahvusringh%C3%A4%C3%A4lingu%20seaduse%20muutmise%20seadus.
[4] E-ITS-i portaal on kättesaadav siit: https://eits.ria.ee/.

määrusega turvameetmete üldnõude, siis tehnilisemad nõuded selle sisustamisel tuleks välja töötada ning koostada küberturvalisuse tagamise korraldamise valitsemisalas. Täiendavalt tuleneb selline edasivolituse ulatuse vajadus ka tehnoloogilise arenguga järjepidamise vajadusest. Täpsem edasivolituse defineerimine näiteks konkreetsete süsteemide või tehnoloogiate osas võib kiiresti infotehnilisel maastikul aeguda.“

Eelnõu § 1 kehtestab E-ITS-i ning selgitab selle järgimist. Paragrahv koosneb neljast lõikest.

Lõike 1 kohaselt on E-ITS lisatud eelnõule ning see on ka kättesaadav E-ITS-i portaalist.

Sarnaselt hetkel kehtiva ISKE-ga on ka E-ITS pidevat kaasajastamist ning täiendamist nõudev dokument. Majandus- ja Kommunikatsiooniministeeriumi valitsemisala asutus Riigi Infosüsteemi Amet korraldab E-ITS-i täiendamise ning uuendamisega seotud teenuseid, võttes selle aluseks varasemase rakendamise praktikat ning muutusi infotehnoloogilises maailmapildis ja õigusraamistikes. Tulenevalt eeldatavast vajadusest E-ITS-i korduvalt muuta ja ajakohastada ei ole Vabariigi Valitsuse määruse vorm sobilik E-ITS-i kehtestamiseks. Sellegipoolest omab E-ITS-i kehtestamine regulatiivset mõju ning ei ole käsitletav üksikjuhtumi reguleerimisena oma rakendusala tõttu, mistõttu on välistatud E-ITS-i kehtestamine käskkirjaga. Eesmärgipärane vorm E-ITS-i kehtestamiseks ongi eeltoodust lähtuvalt ministri määrus.

Lõike 2 järgi sisaldab E-ITS-i versioon 2021:
1) organisatsiooni infoturbe halduse süsteemi nõudeid;[5]
2) rakendusjuhendit;[6]
3) etalonturbe kataloogi;
4) auditeerimise juhendit.[7]

Versiooni nimi vastab dokumentatsiooni koostamise ja kinnitamise aastale. Tulevikus kavandatakse E-ITS-i uuendada igal aastal ning siis toimub ka versiooni uuendamine.

E-ITS-i portaalis on ka täiendavad dokumendid, sh selgitavad juhendid. Üks neist on seletav sõnaraamat, mille abiga saavad selgemaks E-ITS standardis kasutatud terminid. Sõnastik põhineb Saksa päritolu BSI-IT-Grundschutziga kaasneval sõnastikul ja ISO27000 seeria terminite selgitustel.[8] Rollisõnastik määratleb rollid, mida läheb vaja E-ITS rakendamisel, olles abiks etalonturbe kataloogist valitud meetme pealkirjas nimetatud vastutaja määramisel organisatsioonis.[9]

Samas portaalis on ka riskihaldusjuhend[10], alusohtude kataloog[11], vastavustabelid (alusohtude viitetabel, vastavustabel ISKE meetmetele, vastavustabel ISO 27001 standardi nõuetele)[12] ning etalonturbe sammud[13].

[5] https://eits.ria.ee/et/versioon/2021/juhendid/isms-noouded/.
[6] https://eits.ria.ee/et/versioon/2021/juhendid/rakendusjuhend/.
[7] https://eits.ria.ee/et/versioon/2021/juhendid/auditeerimisjuhend/.
[8] https://eits.ria.ee/et/seletav-sonaraamat.
[9] https://eits.ria.ee/et/rollisonastik.
[10] https://eits.ria.ee/et/versioon/2021/juhendid/riskihaldusjuhend/.
[11] https://eits.ria.ee/et/versioon/2021/juhendid/alusohtude-kataloog/.
[12] https://eits.ria.ee/et/versioon/2021/juhendid/vastavustabelid/.
[13] https://eits.ria.ee/et/versioon/2021/juhendid/etalonturbe-sammud/.

E-ITS-i portaalis on 2020. a versioonis (pole ametlikult kinnitatud) avaldatud E-ITS-i lühijuhend, mille peatükid 1, 3, 3.1 ja 3.2 selgitavad E-ITS-i olemust ning sisu.[14] Järgnevad tekstid on väljavõtted nendest peatükkidest:

„1 Käsitlusala

Lühijuhend annab esmase ülevaate Eesti infoturbestandardist (E ITS). Eesti infoturbe-standardi siht on arendada ning edendada Eesti avaliku sektori asutuste ja erafirmade infoturbe taset. Seni on samal otstarbel kasutusel olnud ISKE (infosüsteemide turvameetmete süsteem = infosüsteemide kolmeastmeline etalonturve).

E-ITS-i eesmärk on esitada eestikeelne ja Eesti õigusruumile vastav alus infoturbe käsitlemiseks, mis ühtlasi vastaks standardile ISO/IEC 27001 (27001). E-ITS esitab etalonturbe rakendamise süsteemi, mis aitab organisatsioonil saavutada tema vajadustega sobivat infoturbe taset.

Organisatsiooni juhtkond ise otsustab, milliseid objekte ja protsesse on tarvis kaitsta. Etalonturve seab kaitstavad objektid ja protsessid vastavusse etalonturbe kataloogi tüüpmoodulitega. Etalonturbe kataloogis leiduvad tüüpmoodulid kirjeldavad tüüpilisi ohte ja neile vastavaid, riskianalüüsi põhjal valitud turvameetmeid. Turvameetmete rakendamine vähendab infoturbeohtude realiseerumise tõenäosust. Etalonturve võimaldab organisatsioonil taaskasutada infoturbe parimaid praktikaid ning seeläbi kokku hoida infoturbe rakendamisele kuluvaid vahendeid.

Standard põhineb Saksa etalonturbe süsteemil BSI IT-Grundschutz (BSIG) ja standardil EVS-ISO/IEC 27001:2014 "INFOTEHNOLOOGIA. Turbemeetodid. Infoturbe halduse süsteemid. Nõuded" (27001).

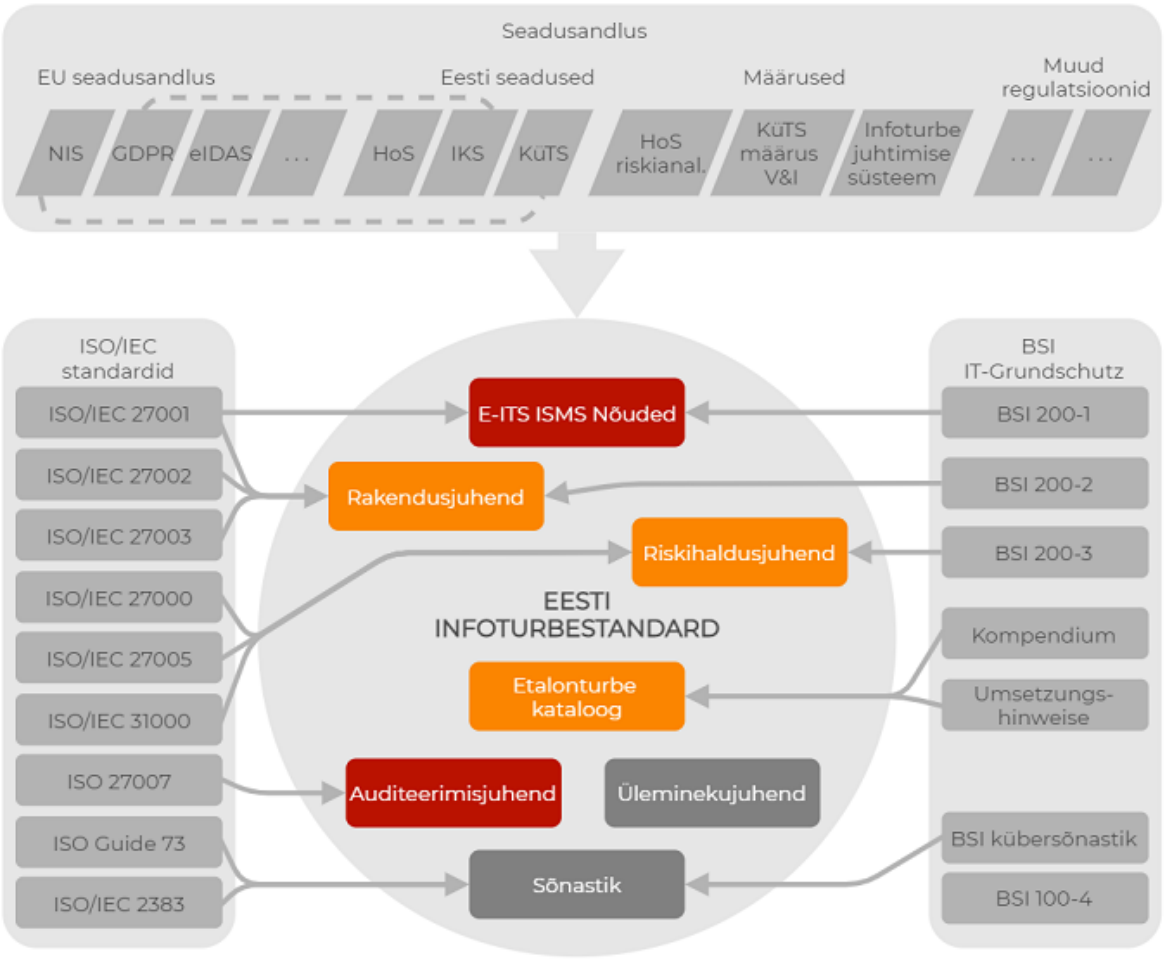
Lühijuhend on mõeldud infoturbe rakendamisega kokkupuutuvatele inimestele nii avalikus kui ka erasektoris, eelkõige juhtidele ja otsustajatele, aga ka IT töötajatele, äriprotsesside juhtidele, infoturbejuhtidele, infoturbetöötajatele ja IT-töötajatele.

3 Infoturbe korraldamine E-ITS alusel

E-ITS esitab infoturbe korraldamise parimad teadaolevad viisid. Standardi omanik on Riigi Infosüsteemi Amet. Standard tugineb seadusandlusele. E-ITS ökosüsteemi oluliseks osaks on audiitorite kogukond, kes hakkab tuvastama organisatsioonide infoturbehalduse süsteemide vastavust standardi nõuetega.

Joonis [1] selgitab E-ITS olulisimate dokumentide suhtestumist Eestis kehtivate seaduste ja üldtuntud infoturbestandarditega.[15]

[14] https://eits.ria.ee/et/versioon/2020vers1/juhendid/luehijuhend/.
[15] Eelnõu koostajate märkus: E-ITS-i lühijuhendis on vastava joonise numbriks 2, kuid siinses eelnõus on tegemist esimese joonisega, mistõttu on seletuskirjas märgitud joonise numbriks 1.



Joonis [1]. E-ITS võtmedokumentide suhtestumine oluliste mõjutajatega

E-ITS seob ühtsesse tervikusse järgmised turbeprintsiibid, -tehnoloogiad ja kontrollimehhanismid:

- *riskihaldus, lähtumine võimalikust kahjust, kahju vältimine. Kui tuvastati ohud, mida etalonturve hallata ei suuda, suunab E-ITS kasutaja vahetu riskihalduse protseduuri juurde;*
- *infoturbe haldussüsteem (i.k. ISMS – **I**nformation **S**ecurity **M**anagement **S**ystem) muutuste avastamiseks ja infoturbe jätkusuutlikkuse tagamiseks;*
- *etalonturve – alusohtude tõrjumiseks riskianalüüsi tulemusel leitud tüüpsed meetmed, mis on mugavalt pakendatud ja rakendajale kasutusvalmis;*
- *auditeerimine ja sertifitseerimine – infoturbekohuslasele on väline vastavusaudit kohustuslik, sertifitseerimine standardi ISO/IEC 27001 suhtes on vabatahtlik ning asendab vastavusauditit.*

3.1 Eesti infoturbestandardi põhimõtted

E-ITS eeldab, et organisatsioon käsitleb infoturvet läbi äriprotsesside prisma. Toimiva infoturbe eeldusena peab organisatsioon olema teadlik oma eesmärkidest, põhikirjalistest ülesannetest jms ning suutma kirjeldada oma toimimise valdkondi läbi äriprotsesside. Infoturbe ülesanne organisatsioonis on säilitada äriprotsesside käigus töödeldava teabe turvalisus.

Infoturbe konkreetsed eesmärgid on seejuures vastavuses organisatsiooni tegevuse eesmärkidega.

Infoturve on pidevalt toimiv protsess, mitte ühekordne tegevus. Infoturve lähtub organisatsiooni eesmärkidest ja selle olulistest äriprotsessidest. Infoturbe tehnilised elemendid saab vajadusel sisse osta, kuid täpne arusaam organisatsiooni äriprotsessidest, nende tähtsusest ning kogu tegevuse eesmärkidest on ainult organisatsiooni juhtkonnal. See paneb juhtkonnale erilised ootused teadlikkuse, otsuste ja vastutuse osas.

Infoturve on tippjuhi vastutusalas, sest tippjuht näeb organisatsiooni tervikuna ning mõistab, mis võib äriprotsesse ohustada. Tippjuht teeb infoturbeprotsesse otseselt mõjutavad otsused turbeks vajalike ressursside jaotamise ning riskide aktsepteerimise kohta.

Infoturbe protsessi käivitamisele eelneb juhtkonna poolne kohustumus – avaldus, millega juhtkond võtab vastutuse infoturbe elluviimise eest organisatsioonis ning mille toel näitab ta edaspidi eeskuju kõigile töötajatele. Infoturve kaitseb organisatsiooni ohtude eest üksnes juhul, kui ta on loomuliku osana integreeritud äriprotsessidesse. Infoturbe nõuetega peavad kursis olema ning neid oma töös arvestama kõik töötajad.

Infoturve vajab pidevat uuendamist, sest ohud muutuvad ja teisenevad ajas. Infoturbe jätkusuutlikkuse tagamiseks näeb E-ITS ette, et organisatsioonis rakendatakse infoturbe halduse süsteem. Infoturbe seis organisatsioonis vajab pidevat parandamist, kavakindlat juhtimist ja jätkusuutlikku haldust selleks, et

- *mõista organisatsiooni tööprotseduure ja avastada neis ebaturvalisi kohti;*
- *täita seaduste ja standardite nõuded;*
- *seista vastu pidevalt teisenevatele küberohtudele.*

E-ITS aluspõhimõtteks on riskihaldus. Et vältida kahju, mida ohud realiseerudes äriprotsessile võivad tekitada, peab organisatsioon oma riskid arvele võtma ja neid haldama. Standard on riskihalduse teinud kättesaadavaks ja mugavaks ka väikesele organisatsioonile.

E-ITS turbemeetodiks on etalonturve. See tähendab, et tüüpjuhtude riskianalüüs on juba ette keskselt ära tehtud standardi koostaja poolt. Riskide vähendamiseks pakutakse standardi rakendajale valmis tüüpmeetmed, mis paiknevad etalonturbe kataloogis.

3.2 Kasu E-ITS rakendamisest

E-ITS rakendamine organisatsioonis toob kaasa infoturbekulutuste optimeerimise ning mitmed kaasnevad eelised.

- *Eesti avaliku sektori kõigi asutuste infoturve on ühtlaselt kõrgel tasemel (üks kõigi, kõik ühe eest), mis omakorda toetab e-riigi turvalist toimimist.*
- *Organisatsioon suudab kiiresti arenevas infoühiskonnas omi ülesandeid täita ja end globaalsete välisohtude eest kaitsta.*
- *Organisatsioon on halvimaks valmistunud. On tagatud organisatsiooni tegevuse jätkuvus. Läbi on mõeldud organisatsiooni ja selle töötajate kaitse küberohtude eest.*
- *Kui infoturve on hästi korraldatud, siis saab organisatsioon keskenduda oma põhitegevusele ning pole karta ootamatuid ründeid, sanktsioone ega trahve.*
- *Organisatsioon saavutab eelise ning parema maine omalaadsete organisatsioonide seas (olen naabrist parem).*

- *Organisatsioon saab oma turvalisust ning jätkusuutlikkust tõendada ka klientidele ja partneritele.*

Läbimõeldud ja jätkusuutlik infoturbeprotsess tagab seega organisatsiooni teenuste jätkuvuse ning hea maine. Infoturbe kõrge tase võib olla omakorda eelduseks rahastuse hankimisel projektidele (näiteks struktuurifondidest või hangetes).

Etalonturve võimaldab organisatsioonil taaskasutada infoturbe parimaid praktikaid ning seeläbi kokku hoida infoturbe rakendamisele kuluvaid vahendeid.“

Lõige 3 kehtestab teenuse osutajale E-ITS-i järgimise ja selle järgimisest tulenevate turvameetmete rakendamise kohustuse. Teenuse osutajate loetelu on sätestatud KüTS § 3 lõikes 1. Lisaks rakenduvad sätestatud kohustused muidugi teistele, kellele kohaldatakse teenuse osutaja kohta sätestatud nõuded, eelkõige on selleks KüTS § 3 lõikes 4 sätestatud loetelu.

Kehtestatav E-ITS-i järgimise kohustus on piiritletud VV määrusest tuleneva volitusnormi ulatusega. Täpsemalt kitsendavad ju kujundavad kohustuse kehtestamist nt VV määruse § 3 lõikes 2 sätestatud erand ning §-s 4 sätestatud auditeerimiskord.

Sisuliselt sätestab lõige kaks eraldiseisvat kohustust. Esimese kohustuse ehk Eesti infoturbestandardi järgimise kohustuse sisu on avatud lõikes 4. Teine eraldiseisev kohustus on turvameetmete rakendamise kohustus. Kui esimese kohustuse täitmine suunab E-ITS-i järgiva teenuse osutaja rakendatavate turvameetmeteni (nt etalonturbe kataloogi kaudu), siis on ka eraldiseisev teenuse osutaja kohustus nimetatud turvameetmeid rakendada vähemalt esimese kohustuse täitmisest tulenevast mahus. Teine kohustus võib sisuliselt olla hõlmatud ka esimese kohustusega (nt kui E-ITS-i tingimustest tuleneb nõue turvameetmeid rakendada), kuid ka sellisel juhul selle kohustuse eraldiseisev väljatoomine kannab eesmärki tagada efektiivsem järelevalve. Küberturvalisuse seisukohalt on nende kohustuste täitmise üheks olulisemaks tulemiks reaalselt rakendatud turvameetmed ning kui teenuse osutaja ei ole suutnud rakendada vajalikke turvameetmeid, siis ei tohiks olla eraldi vaidlusküsimus, et kas E-ITS-i järgimise kohustus ikka hõlmab üleüldist kohustust turvameetmeid rakendada või et kas turvameetmete rakendamata jätmine võis tuleneda mõnest muust vaieldava sisuga E-ITS-i nõude tõlgendamisest.

Lõige 4 sisustab E-ITS-i järgimise kohustuse. E-ITS on kogum erinevatest nõuetest ja juhenditest, mida võib üldistatult grupeerida E-ITS-i tingimusteks. Kui tegemist on E-ITS-i nõudega, siis on tingimuse täitmine sellele nõudele vastavuse saavutamine. Kui tegemist on aga juhendiga (nt E-ITS rakendusjuhend), siis on tingimuse täitmiseks läbiviidud tegevus vastavalt juhendile.

Küberturvalisuse tagamine ei ole staatiline verstapost, vaid pidev protsess jätkuvate küberturvalisusega seotud tegevuste elluviimisel. Seepärast ei ole ka sätestatud, et E-ITS-i järgimine seisneb lihtsalt E-ITS-i tingimuste täitmises, vaid on eraldi täpsustatud tingimuste täitmise kohustust infoturbe halduse faaside kaupa vastavalt E-ITS-i loogikale.

Infoturbe haldus on abstraktsioon organisatsiooni juhtimise osast, mis puudutab infoturvet käsitlevaid plaane, tegevusi ning ressursijaotusi. Kui organisatsioonis puuduvad infoturvet käsitlevad plaanid, tegevused ning ressursijaotused, siis see ei tähenda, et organisatsioonil puudub infoturbe haldus, vaid et organisatsioon ei ole oma infoturbe haldust sisustanud.

Selleks et E-ITS-i järgimine võimaldaks seega teenuse osutajal küberturvalisust tagada, rakendatakse E-ITS-i järgimise kohustust ka infoturbe halduse kõikides faasides: käivitamine, rakendamine, käigushoidmine ning täiustamine.[16] Sõltumata teenuse osutaja tehtud või tegemata tegevustest E-ITS-i järgimisel, on infoturbe haldus kui organisatsiooni juhtimise osa alati vähemalt ühes nimetatud faasidest.

Täiendavalt on E-ITS-i järgimise kohustuse osa E-ITS-i tingimuste täitmise auditeerimine. Samas on E-ITS-i tingimuste täitmise auditeerimine kui E-ITS-i järgimise osa sisustatav käesoleva eelnõuga vaid määral, mis ei ole reguleeritud VV määruse §-s 4. Seega peab teenuse osutaja auditi läbi viima E-ITS-i järgimise ühe osana ning E-ITS-i tingimuste täitmise auditeerimise kohustus ei ole käsitletav eraldiseisvana E-ITS-i järgimise kohustusest.

Selleks, et läbiviidav audit oleks aluseks auditeerimise kohustuse täitmisele, peab auditi planeerimine, tegemine jm tegevused (ehk auditeerimine) toimuma vastavalt E-ITS-i auditeerimisjuhendile.

Audit loetakse läbiviiduks, kui audiitor on teenuse osutajale edastanud auditeerimisjuhendi tähenduses lõpparuande. Sellest hetkest alustab kulgemist järgmise auditi läbiviimise tähtaeg ning teenuse osutaja kohustus on tagada vastavaks tähtajaks järgmise auditi läbiviimine. Kuna infoturbe haldus on kestev protsess, siis praktikas tuleb teenuse osutajal hakata tegelema lõpparuandes toodud puuduste likvideerimisega (kui neid tuvastatakse) selleks, et saavutada positiivne tulemus järgmisel auditil.

Ei ole keelatud auditi läbiviimist, ennekõike auditi tellimist, volitada või teha koos teise organisatsiooniga. Ühisauditite läbiviimine või teise organisatsiooni nimel auditi tellimine on ennekõike asjakohane olukordades, kus erinevate organisatsioonide info- ja kommunikatsioonitehnoloogia (edaspidi *IKT*) infrastruktuuri haldamine ja majutamine on üle antud kesksele organisatsioonile. Küll aga peab läbiviidud auditi lõpparuanne käsitlema teavet iga auditi subjekti suhtes. IKT infrastruktuuri haldamine ja majutamine kolmanda organisatsiooni kaudu ei mõjuta auditi subjekti iseseisvat kohustust E-ITS-i järgida, mille täitmist auditeerimine kontrollib.

Eelnõu § 2 sätestab määruse jõustumise. Määrus jõustub 531 SE-ga samal kuupäeval – nimetatud seaduseelnõu jõustub üldises korras.

3. Eelnõu vastavus Euroopa Liidu õigusele

Eelnõu ei oma puutumust Euroopa Liidu õigusega.

Eelnõu ehk E-ITS-i kehtestamise eesmärk ei ole seotud Euroopa Liidu õigusega. Euroopas on standardimine korraldatud vastavalt Euroopa Parlamendi ja nõukogu määrusele (EL) nr 1025/2012. Selle määruse kohaselt on riiklik standard – standard, mille on vastu võtnud riigi standardiorganisatsioon (Eesti puhul Eesti Standardimis- ja Akrediteerimiskeskus). Taoliste standardite puhul kohaldub toote nõuetele vastavuse seaduse[17] § 40. Samas pole E-ITS standard nimetatud Euroopa Liidu ja nõukogu määruse ning toote nõuetele vastavuse seaduse tähenduses. E-ITS on pigem ühtsete nõuete kogum, mitte standardiorganisatsiooni kinnitatud

[16] Vt vastavate tegevusi lähemalt E-ITS-i rakendusjuhendi peatükke 8 (Etalonturbeprotsessi lühikirjeldus), 9 (Etalonturbeprotsessi käivitamine) ning 10 (Etalonturbe protsess).
[17] Toote nõuetele vastavuse seadus, RT I, 22.10.2021, 12.

dokument. Eestis on ka täna juba standardiorganisatsiooni väliseid standardeid, mis on analoogselt kehtestatud määrusega.[18]

Seega on seaduseelnõu kooskõlas Euroopa Liidu õigusega.

4. Määruse mõjud

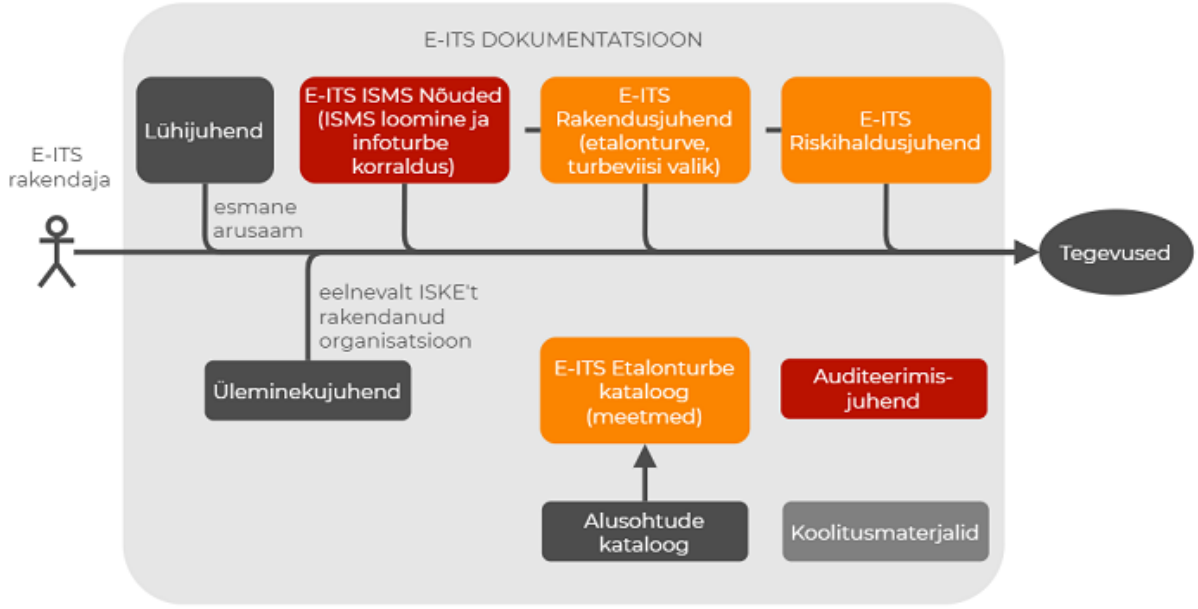
531 SE seletuskirjas (peatükk 6.1. lk-del 33-39) on analüüsitud E-ITS-i kehtestamisega seotud mõjusid. Seaduseelnõu seletuskirjas olev mõjude analüüs lähtub samadest mõjude liikidest, mis on nõutud hea õigusloome ja normitehnika eeskirja[19] § 65 lg 1 punkti 4 kohaselt. VV määruse eelnõu seletuskirjas (peatükk 5.1. lk-del 30–37) on korratud 531 SE mõjude analüüsi sisu. Seetõttu seda analüüsi käesolevas seletuskirjas ei korrata.

Käesoleva eelnõuga eraldiseisvalt seni käsitlemata mõjusid ei kaasne.

5. Määruse rakendamisega seotud tegevused, vajalikud kulud ja määruse rakendamise eeldatavad tulud

531 SE seletuskirjas (peatükk 7.1. lk-del 45-47) on analüüsitud E-ITS-i kehtestamisega seotud riigi ja kohaliku omavalitsuse tegevusi, eeldatavaid kulusid ja tulusid. VV määruse eelnõu seletuskirjas (peatükk 6.1. lk-del 42–44) on korratud sama analüüsi, mis on 531 SE seletuskirjas. Seetõttu ei korrata sama sisu siinses seletuskirjas.

Tegevuste mõttes peab E-ITS-i rakendaja hakkama tegelema E-ITS-i rakendamisega. E-ITS-i lühijuhendi peatükis 4 on toodud joonis, kuidas seda teostada. Joonisel on ette näidatud soovitav liikumistee E-ITS evitamisel ja dokumentidega tutvumisel. Punane värv tähistab kõrgema prioriteediga juhendmaterjale.



[18] Vt nt haridus- ja teadusministri 28.11.2008. a määrust nr 69 „Kutsestandardite koostamise, muutmise ja vormistamise kord“, 19.06.2015. a määrust nr 27 „Täienduskoolituse standard“, 21.03.2007. a määrust nr 27 „Huviharidusstandard“ ning rahandusministri 13.12.2011. a määrust nr 57 „Siseaudiitori kutsetegevuse standardite kehtestamine“.

[19] Hea õigusloome ja normitehnika eeskiri, RT I, 29.12.2011, 228.

Joonis [2]: E-ITS juhendmaterjalidega tutvumise soovitatav järgnevus[20]

6. Määruse jõustumine

Määrus jõustub 531 SE-ga samal kuupäeval – nimetatud seaduseelnõu jõustub üldises korras.

7. Eelnõu kooskõlastamine, huvirühmade kaasamine ja avalik konsultatsioon

Eelnõu esitatakse koos VV määruse eelnõu ja seletuskirjaga kooskõlastamiseks eelnõude infosüsteemi kaudu kõikidele ministeeriumitele ning arvamuse avaldamiseks põhiseaduslikele institutsioonidele, avalik-õiguslikele juriidilistele isikutele, Andmekaitse Inspektsioonile, Riigi Infosüsteemi Ametile, Keskkonnaministeeriumi Infotehnoloogiakeskusele, Registrite ja Infosüsteemide Keskusele, Riigi Info- ja Kommunikatsioonitehnoloogia Keskusele, Rahandusministeeriumi Infotehnoloogiakeskusele, Siseministeeriumi infotehnoloogia- ja arenduskeskusele, Tervise ja Heaolu Infosüsteemide Keskusele, Eesti Linnade ja Valdade Liidule, Eesti Infotehnoloogia ja Telekommunikatsiooni Liidule, Eesti Infosüsteemide Audiitorite Ühingule ning Riigi Infosüsteemi Ameti vahendusel elutähtsate ja oluliste teenuste osutajatele.

[20] Eelnõu koostajate märkus: E-ITS-i lühijuhendis on vastava joonise numbriks 5, kuid siinses eelnõus on tegemist esimese joonisega, mistõttu on seletuskirjas märgitud joonise numbriks 2.