Majandus- ja Kommunikatsiooniministeerium

Riigi infosüsteemi koosvõime

Kinnitatud majandus- ja kommunikatsiooniministri käskkirjaga 11-0377, 22.12.2011

Infoturbe koosvõime raamistik

Versioon 2

2011

Riigi infosüsteemi koosvõime
Infoturbe koosvõime raamistik

Versioon 2
2011

Käesolev dokument on osa riigi infosüsteemi koosvõime raamistikust. Dokument on avatud ettepanekuteks avaliku, era ja kolmanda sektori asutustele ning kõigile asjasthuvitatud isikutele. Ettepanekud palume saata e-kirjana aadressile koosvoime@riso.ee.

Raamistiku dokumente uuendatakse pidevalt ning dokumendi hetkeseis avaldatakse riigi infosüsteemide osakonna wikis[1]. Muudatuste sisseviimise järel kinnitatakse dokumendi ametlik versioon, mis kooskõlastatakse avaliku sektori asutustega ja avaldatakse koosvõime raamistiku veebisaidil[2].

Infoturbe koosvõime raamistiku eelmised ametlikud versioonid on järgmised.

•Versioon 1.2 (22.07.2011) esitati ettepanekute tegemiseks ning konsultatsiooniperioodil tehtud ettepanekud on arvesse võetud versioonis 2.

•Versioon 1.1 (24.09.2010) kinnitati majandus- ja kommunikatsiooniministri käskkirjaga 10-0270.

•Versioon 1.0 (31.01.2007) arutati läbi ja kiideti heaks infoturbe koosvõime töögrupis.

[1] http://www.riso.ee/wiki/

[2] http://www.riso.ee/et/koosvoime/raamistik

[3] http://www.creativecommons.ee

Sisukord

1. Sissejuhatus....4
2. Eesti infoturbe koosvõime raamistiku poliitiline kontekst ja aluspõhimõtted....6
2.1. Raamistiku eesmärgid, rakendamisala ja sihtgrupid....6
2.3. Raamistiku õiguslik staatus, toimimine ja läbivaatused....7
3. Infoturbe valdkonnad....9
3.1. Koostöö ja koordineerimine....9
3.2. Teadvustamine ja koolitus....9
3.3. Infoturbe õigusaktide väljatöötamine ja uuendamine....9
3.4. Informatsiooni infrastruktuuri kaitse....10
3.5. Inimeste ja varade kaitse rakendustegevused....10
4. Õiguslik koosvõime....11
4.1. Seadused ja määrused....11
4.2. Strateegiad, raamistikud ja tegevuskavad....11
4.3. Juhendid, head tavad, standardid, materjalid....12
5. Organisatsiooniline koosvõime infoturbe valdkonnas....13
5.1. Info- ja sideturbe korraldamine....13
5.2. Organisatsioonid ja koostöö....13
6. Semantiline koosvõime infoturbe valdkonnas....15
7. Tehniline koosvõime infoturbe valdkonnas....16
7.1. e-identiteet, Eesti avaliku võtme infrastruktuur ja ID-kaart....16
7.2. Infosüsteemide turvameetmed....18
7.2.1. Infosüsteemide turvameetmete süsteemi rakendamine....18
7.2.2. Muud andmekasutajad ja teenustasemete lepped....19
7.2.3. Kriitilise informatsiooni infrastruktuuri kaitse....20
7.3. Soovitatavad standardid, juhised ja tehnoloogiad....21
7.3.1. Standardid....21
7.3.2. Protokollid ja tehnoloogiad ning muud soovitused....22
8. Raamistiku rakendamine....23
8.1. Soovitused infoturbe saavutamiseks....23
8.2. Infoturbe lühiküsimustik valdkonna infoturbepoliitika eest vastutajale, asutuse IT-juhile ja infoturbe eest vastutajale....23
8.3. Mõõdikud....24

1. Sissejuhatus

Infoturbe koosvõime raamistiku esimene versioon valmis avaliku ja erasektori ning akadeemiliste asutuste koostöös 2007. aasta alguses. Selle eesmärk – turvaline, turvateadlik ja arengule kaasa aitav infoühiskond Eestis – on jäänud samaks, kuid aastate jooksul on infoturve muutunud veelgi olulisemaks nii Eestis, Euroopa Liidus kui ka kogu maailmas.

Eestis on lisandunud küberrünnete kogemus, valminud küberjulgeoleku strateegia ja selle rakendusplaan ning rajatud NATO küberkaitsekeskus. Vabariigi Valitsus on kinnitanud mitu uut arengu- ja tegevuskava, sealhulgas „Eesti infoühiskonna arengukava 2013“[4]. Riigi Infosüsteemide Arenduskeskusest on saanud Riigi Infosüsteemi Amet. Aktiivselt tegeletakse kriitilise informatsiooni infrastruktuuri kaitse teemadega. Töötatakse välja uusi koosvõimeraamistiku versioone. Infosüsteemide kolmeastmelise etalonturbe süsteemi (ISKE) esmase auditi tähtajad on möödunud, mitu asutust on ISKE auditi läbinud ja enamik asutusi on ISKE nõuete rakendamist alustanud. Jätkuvalt ei saa infoturvet tagada üks ametkond, asutus, ettevõte, töögrupp või riik – vaja on kõigi osaliste koostööd nii Eestis kui ka väljaspool. Eriti oluline on seejuures avaliku ja erasektori koostöö. Tagasiside huvipooltelt näitab, et koosvõimeraamistik toimib, kuid selle mõju levib aeglaselt.

Euroopa Liidus (EL) on valminud majanduskasvu strateegia „Euroopa 2020“ ja selle põhieesmärkidest lähtuv suurprojekt „Euroopa digitaalne tegevuskava“, mille teemad on ka usaldus ja turvalisus. Digitaalsel tegevuskaval põhineb Euroopa „eValitsuse tegevuskava 2011–2015“, mis sätestab muu hulgas nõuded elektrooniliste toimingute ja lahenduste turvalisusele ning e-autentimisteenuste arendamisele. Euroopa Komisjoni teatises „Euroopa avalike teenuste koosvõime alused“ esitletakse digitaalse tegevuskava kahte olulist osa: Euroopa koosvõimestrateegiat (EIS)[5] ja Euroopa koosvõimeraamistikku (EIF)[6]. EIS pakub välja koosvõime põhivaldkonnad, sealhulgas turvalise infovahetuse. EIF nimetab Euroopa avalike teenuste ühe aluspõhimõttena turvalisust ja privaatsust ning soovitab avalike teenuste kontseptuaalmudeli ühe põhiosana kasutada infosüsteemide turvalist andmevahetuskihti. Euroopa Võrgu- ja Infoturbeamet (ENISA) mandaati pikendav ettepanek on heakskiitmisel. Mitmes ELi riigis on vastu võetud KII kaitse strateegia.

Kogu maailmas on teadvustatud kriitilise informatsiooni infrastruktuuri kaitse olulisust. Näiteks võttis Rahvusvaheline Telekommunikatsiooni Liit (ITU) vastu globaalse küberturbe tegevuskava. 2008. aasta maailma majandusfoorumil leiti, et järgmise kümne aasta jooksul esineb 10–20% oht elutähtsate sideinfrastruktuuride kokkuvarisemiseks, mis tooks kaasa ligikaudu 250 miljardi USA dollari suuruse ülemaailmse majanduskulu. Kasvavad uute tehnoloogiate (nt mobiilsete sidevahendite ja intelligentsete seadmete võrgud) kasutuselevõtuga seotud turvariskid. Areneb ISO 27000 infoturbe standardite seeria, mis toob kaasa uusi ja hõlmab seni kehtinud infoturbestandardeid.

Ülaltoodud ja paljud muud tegurid tingivad vajaduse infoturbe koosvõime raamistikku regulaarselt uuendada.

Käesolevas raamistikus kirjeldatakse olulisemaid infoturbe aspekte, mida tuleb arvestada koosvõimelise infosüsteemi loomisel nii riigi kui ka asutuse tasandil. Võrreldes esimese infoturbe koosvõime raamistikuga on lisatud ja täiendatud kriitilise informatsiooni infrastruktuuri kaitse teemat ning kogu tekst on kaasajastatud. Dokumendi esimesed jaotised käsitlevad eelkõige infoturbe koosvõime põhimõtteid ja organisatsioonilisi küsimusi ning on

[4] http://www.riso.ee/et/files/Infoyhiskonna_arengukava_2013.pdf

[5] European Interoperability Strategy (EIS), http://ec.europa.eu/isa/documents/isa_annex_i_eis_en.pdf

[6] European Interoperability Framework (EIF), http://ec.europa.eu/isa/documents/isa_annex_ii_eif_en.pdf

suunatud peaasjalikult infoturbe eest vastutajatele. Tehnilise koosvõime jaotis on orienteeritud eelkõige IT-juhile ja spetsialistile.

Raamistiku olulisemad järeldused ja nõuded on välja toodud rohelise taustaga raamitud kastides.

Dokumendi võtmesõnu „PEAB“, „EI TOHI“, „NÕUTAV“, „TULEB“, „EI TULE“, „PEAKS“, „EI PEAKS“, „SOOVITATAV“, „VÕIB“ ja „VALIKULINE“ tuleb tõlgendada nii, nagu on kirjeldanud internetiehituse töörühm (IETF)[7]. Nimetatud sõnade olulise rõhutamiseks on need esitatud läbiva suurtähega ning nende tähendus on järgmine.

Tähendus:	**Tähendust väljendavad sõnad:**
Nõutav/kohustuslik (absoluutne nõue või keeld)	PEAB, NÕUTAV, TULEB ingl *MUST, REQUIRED, SHALL*
Soovitus (kõrvalekaldumine on lubatud ainult kaalutud põhjenduse olemasolul)	PEAKS, TULEKS, SOOVITATAV ingl *SHOULD, RECOMMENDED*
Aktsepteeritav/lubatud	VÕIB, VALIKULINE ingl *MAY, OPTIONAL*
Mittesoovitatav (lubatud ainult kaalutud põhjenduse olemasolul)	EI TOHIKS, EI PEAKS, MITTESOOVITATAV ingl *SHOULD NOT, NOT RECOMMENDED*
Keelatud (absoluutne keeld)	EI TOHI, EI TULE ingl *MUST NOT, SHALL NOT*

Riigi infosüsteemi koosvõime raamistiku dokumentides kasutatud mõisted ja lühendid on toodud koosvõimeraamistiku sõnastikus[8], samas on ka ülaltoodud võtmesõnade pikemad eestikeelsed selgitused.

[7] Internet Engineering Task Force (IETF) RFC 2119: „Key words for use in RFCs to indicate requirement levels“

[8] http://www.riso.ee/wiki/Sõnastik

2. Eesti infoturbe koosvõime raamistiku poliitiline kontekst ja aluspõhimõtted

Kuna infoturve ja sellega seonduv muutub üha olulisemaks, on tekkinud erinevaid valdkondlikke dokumente ja algatusi. Allpool täpsustatakse infoturbe koosvõime raamistiku eesmärke, sihtgruppi, seoseid teiste infoturbealgatustega ning arengupõhimõtteid.

2.1. Raamistiku eesmärgid, rakendamisala ja sihtgrupid

Infoturbe raamistik loob eeldused majanduse ning info- ja kommunikatsioonitehnoloogia keskkonna kaitseks ning arendamiseks. Raamistik katab põhilised infoturbega seotud valdkonnad nii Eesti avalikus kui erasektoris. Infoturberaamistiku eesmärk on turvaline, turvateadlik ja arengule kaasa aitav infoühiskond Eestis. Selle eesmärgi saavutamisel on tähtsad järgmised aspektid.

- **Koostöö ja koordineerimine**: toimiv infoturbealane avaliku ja erasektori koostöö nii Eestis kui ka rahvusvahelisel tasemel.
- **Teadvustamine ja koolitus**: infoturbeprobleemide teadvustamine, väga hea infoturbealane kompetentsus ja teadlikkus.
- **Infoturvet reguleeriva seadusandluse väljatöötamine ja uuendamine**: sellise õigusraamistiku kehtestamine, mis toetab infosüsteemide turvalist ja laialdast kasutamist, tagades samal ajal inimeste põhiõiguste kaitse.
- **Informatsiooni infrastruktuuri kaitse**: infoturbega seotud riskide maandamine Eestis, eriti kriitilise infrastruktuuri ettevõtetes, elektroonilise side võrkudes ning info- ja sidesüsteemides; kriitilise informatsiooni infrastruktuuri kaitse põhimõtete rakendamine, soodustamaks küberjulgeolekut.
- **Inimeste ja varade kaitse rakendustegevused**: Eesti majanduse konkurentsivõime suurendamine turvalise infoühiskonna loomise teel; turvaliste ID-kaardi põhiste süsteemide ja teenuste arendamine; kohustusliku kolme-astmelise turvameetmete süsteemi ja infoturbe standardite laiaulatuslik rakendamine riigi ja kohaliku omavalitsuse infosüsteemide ja teenuste hankimisel, tarnimisel ja haldamisel nii avlaikus kui (vastavalt vajadusele) erasektoris.

Raamistik ei käsitle riigisaladust sisaldavaid või sõjaliseks otstarbeks mõeldud andmeid ja süsteeme.

Tehnoloogiliselt hõlmab infoturberaamistik nii infotehnoloogiliste süsteemide kui ka elektroonilise side turvet.

Käesoleva dokumendi sihtgrupp on riigi ja kohaliku omavalitsuse asutused ning ettevõtted, sealhulgas:

- asutuste ja ettevõtete juhtkond, IT-juhid ning infoturbe eest vastutajad;
- infosüsteemide ja IT-teenuste hankijad, arendajad, tarnijad ja haldajad riigiasutustes ja erasektoris;
- küberjulgeoleku ja kriitilise informatsiooni infrastruktuuri kaitse korraldamise eest vastutajad.

Raamistiku järgimine on kohustuslik riigi ja kohaliku omavalitsuse asutuste infosüsteemide suhtluse korraldamisel. Kuigi raamistiku sihtgrupis on ka erasektori asutused (eeldatakse, et neilgi on otstarbekas arvestada raamistiku soovitustega, näiteks teenuste väljatöötamisel, süsteemide kavandamisel või riigihangetes osalemisel), on raamistik nende jaoks soovituslik.

2.2. Infoturbe koosvõime raamistik ja seotud algatused

Infoturbe koosvõime raamistiku alus on Majandus- ja Kommunikatsiooniministeeriumi koostatud „Eesti infoühiskonna arengukava 2013“. Selle üks tegevussuund on avaliku sektori infosüsteemide kujundamine ühtseks koosvõimeliseks tervikuks ning see näeb ette avaliku sektori poolt ettevõtetele ja kodanikele pakutavate teenuste turvalisuse ja kodanike turvateadlikkuse kasvu. Nende eesmärkide saavutamiseks vajalikke tegevusi täpsustavad riigi koosvõime ülddokument „Riigi infosüsteemi koosvõime raamistik“ ja käesolev infoturberaamistik.

Eesti küberruumi haavatavuse vähendamiseks ja infosüsteemide tõhusamaks kaitseks riigis koostas Kaitseministeerium Vabariigi Valitsuse korraldusel koostöös Haridus- ja Teadusministeeriumi, Justiitsministeeriumi, Majandus- ja Kommunikatsiooniministeeriumi, Siseministeeriumi ja Välisministeeriumiga arengukava „Küberjulgeoleku strateegia 2008–2013“[9]. Riigi küberjulgeolek hõlmab selle dokumendi kontekstis kõiki elektroonilise teabe, teabekandjate ning -teenustega seotud toiminguid, mis mõjutavad riigi julgeolekut.

Küberjulgeoleku strateegia ja infoturberaamistik on omavahel kooskõlas ja seotud, kuid neil on erinevad sihtgrupid, orientatsioon ja sisu.

Küberjulgeoleku mõiste hõlmab kõiki elektroonilise teabe, teabekandjate ja -teenustega seotud toiminguid, mis mõjutavad riigi julgeolekut. Küberjulgeoleku strateegia on suunatud eelkõige (kuigi mitte ainult) riigikaitse ja kriitilise informatsiooni infrastruktuuri kaitsega seotud asutustele. Strateegia tugineb eeskätt riigi kui terviku küberruumi haavatavuse vähendamisele, keskendub riigi julgeolekule ning hõlmab erinevaid riigisaladusega seotud valdkondi.

Infoturberaamistik määrab kindlaks Eesti infoturbe toimimise üldpõhimõtted. See on mõeldud riigiasutuste ja erasektori ühtsete standardite kehtestamiseks riigisisese infoturbe tagamisel, sealhulgas avalike teenuste pakkumiseks kasutatavate infotehnoloogiliste lahenduste arendamisel ja haldamisel. Raamistik ei käsitle riigisaladusega seonduvat.

Käesolev infoturberaamistiku versioon käsitleb eelmistest põhjalikumalt kriitilise informatsiooni infrastruktuuri kaitset. Sealjuures on lähtutud e-ühiskonna ja avaliku sektori seisukohast, täpsemalt sellest, mida asutused ja ettevõtted peavad arvestama seoses kriitilise informatsiooni infrastruktuuri kaitsega ning millised on infosüsteemi koosvõime küberjulgeoleku aspektid.

Peale eespool nimetatud dokumentide toetub infoturbe koosvõime raamistik mitmetele muudele õigusaktidele, dokumentidele ja algatustele, millele on viidatud järgnevas tekstis.

2.3. Raamistiku õiguslik staatus, toimimine ja läbivaatused

Raamistik ei loo uut eraldiseisvat tegevusvaldkonda, vaid on mõeldud infoturbe eesmärkide saavutamiseks infoturbe tervikliku ja paljusid osapooli hõlmava käsitluse ning osapoolte tõhusama koostöö kaudu.

Infoturberaamistiku õiguslik staatus ja toimimine on sama, mis kõigil teistel riigi infosüsteemi koosvõime raamistiku dokumentidel. Koosvõimeraamistik on strateegiline dokument, millest Majandus- ja Kommunikatsiooniministeerium (MKM) kui riigi infosüsteeme koordineeriv asutus lähtub infopoliitiliste otsuste tegemisel, struktuurifondidest rahastavate projektide hindamisel, riigi infosüsteemi õigusaktide väljatöötamisel, ministeeriumide IKT-alaste õigusaktide kooskõlastamisel ja infosüsteemide kooskõlastamisel riigi infosüsteemi haldussüsteemis (RIHA). Koosvõimeraamistiku dokumendid kehtestatakse

[9] https://valitsus.ee/UserFiles/valitsus/et/valitsus/arengukavad/kaitseministeerium/kuberjulgeolek.pdf

riigi infosüsteemi koordineeriva ministri käskkirjaga ning nende järgimine on riigi ja kohalike omavalitsuste infosüsteemide suhtlust korraldades kohustuslik. Kuigi raamistiku sihtgrupis on ka erasektori asutused (eeldatakse, et neilgi on otstarbekas arvestada raamistiku soovitustega, nt teenuste väljatöötamisel, süsteemide kavandamisel või riigihangetes osalemisel), on raamistik nende jaoks soovituslik.

Lisaks on raamistik kohustuslik kui eri osapoolte kokkulepe. Raamistik ja sellega seotud dokumendid läbivad konsultatsiooniperioodi, mille vältel riigi ja kohaliku omavalitsuse asutused, erasektor, kolmanda sektori asutused ja eraisikud saavad esitada muudatus- ja täiendusettepanekuid. Ettepanekud ja kommentaarid arutatakse koosvõimeraamistiku juhtgrupi poolt läbi ning selle lõppversiooni käsitletakse kui osalevate poolte kokkulepet.

Mitmeid koosvõime raamistiku nõudeid ei ole võimalik täita kõigil asutustel kohe, see võib võtta mitu aastat. Igal asutusel peaks aga olema tegevuskava tulemusteni jõudmiseks.

Raamistik vaadatakse läbi kord aastas või oluliste muutuste korral rahvusvahelises keskkonnas, tegutsemisasjaoludes, õiguslikes tingimustes või tehnilises keskkonnas. Sellega tagatakse raamistiku pidev sobivus, asjakohasus ja toimivus. Infoturberaamistiku arendamise, läbivaatuse ja hindamise eest vastutab Majandus- ja Kommunikatsiooniministeerium. Läbivaatuse käigus hinnatakse raamistiku täiustamise võimalusi.

Läbivaatuse lähteandmed sisaldavad järgmist teavet:

- infoturberaamistikku puudutavad muudatused Eestis, Euroopa Liidus ja mujal maailmas;
- huvipoolte tagasiside, raamistiku eelmise versiooni läbivaatuste tulemused;
- muutused, mis võivad mõjutada organisatsioonide infoturbe halduse metoodikat, sealhulgas organisatsioonilise keskkonna, ressursside, eeskirjade ja õiguslike tingimuste või tehnilise keskkonna muutused;
- ohtude ja kitsaskohtadega seotud suundumused;
- informatsioon infoturbeintsidentide kohta;
- asjakohaste ametiasutuste soovitused.

Läbivaatuse tulemite hulka peaksid kuuluma kõik otsused ja meetmed, mis käsitlevad järgnevat:

- metoodika täiustamine infoturbe ja selle protsesside haldamisel;
- juhtimiseesmärkide ja meetmete täiustamine;
- ressursside ja/või kohustuste jaotuse täiustamine;
- muude muudatuste tegemine.

3. Infoturbe valdkonnad

Infoturbe koosvõime raamistiku väljatöötamine ja elluviimine hõlmab paljusid osapooli. Teave infoturbe probleemide ja lahenduste kohta tuleb viia võimalikult paljude asjaosalisteni. Infoturberaamistik on jaotatud viieks põhiliseks valdkonnaks: koostöö ja koordineerimine, teadvustamine ja koolitus, õigusaktide väljatöötamine, informatsiooni infrastruktuuri kaitse ning inimeste ja varade kaitse rakendustegevused.

3.1. Koostöö ja koordineerimine

Infoturbega tegelevad erinevad asjaosalised, seega on selle töö planeerimine ja koordineerimine väga oluline. See hõlmab infoturbetegevuste koordineerimist ning Eesti-sisese ja rahvusvahelise koostöö korraldamist koostöös era- ja kolmanda sektoriga. Muu hulgas kuuluvad siia järgmised tegevused:

- Eesti IT-keskkonna riskianalüüsi teostamise koordineerimine
- turvaintsidentide käsitlemise võimekuse arendamine Eestis
- infoturbealase kontaktvõrgustiku haldamine Eestis ja rahvusvahelise koostöö korraldamine ENISAga (European Network and Information Security Agency)
- küberjulgeoleku tagamisega seotud rahvusvahelise koostöö arendamine
- piiriüleste e-teenuste infoturbealase arenduse koordineerimine.

3.2. Teadvustamine ja koolitus

Infoturbe tagamiseks peavad kõik osapooled olema teadlikud ohtudest, riskidest, rünnetest, meetmetest ja teistest infoturbe asjaoludest.

Avaliku sektori asutused peavad kaitsma oma süsteeme, kuid olema ka eeskujuks teistele pooltele. Erasektori asutused peaksid teadvustama infoturvet kui strateegilist edufaktorit, mitte vaid kui kuluartiklit. Inimesed peaksid aru saama, et nende koduarvutite asjakohane turvamine on ülitähtis üldises infoturbeahelas.

Selleks tuleb läbi viia pidevat turvaalast teadvustamist ja koolitust, sealhulgas järgmisi tegevusi:

- infoturberaamistiku tutvustamine ja avalikkusega suhtlemine
- infoturbe koolitus asutuste juhtkondade esindajatele ja IT-juhtidele
- infoturbe koolitus ja väljaõpe haridusasutustes
- inimeste turvaalane harimine, trükised ja teabepäevad
- infoturbeks vajalike uuringute, arendustööde ja rahvusvahelise teaduskoostöö läbiviimine
- tegevusvalmiduse arendamine kriisisituatsioonidega toimetulekuks avalikus ja erasektoris
- avalikkuse turvateadlikkuse ja rahulolu uuringute läbiviimine.

3.3. Infoturbe õigusaktide väljatöötamine ja uuendamine

Infoturvet reguleerivad vastavad õigusaktid. Vaja on välja töötada, evitada ja uuendada IKT ning elektroonilise side infoturbe tagamiseks vajalik kord, dokumentatsioon ja vahendid. Muu hulgas tuleb välja töötada või uuendada järgmiste valdkondade õigusaktid:

- infoturve ja elektrooniline side
- küberjulgeoleku tagamine ja kriitilise informatsiooni infrastruktuuri kaitse
- turvastandardid, infosüsteemide kolmeastmeline etalonturbe süsteem (ISKE) ja turvanõuete klassifitseerimise metoodika
- andmekogude pidamise korraldamine turvameetmete süsteemi nõuete kohaselt
- turvalised e-teenused
- riigihangetes rakendatavad infoturbenõuded.

3.4. Informatsiooni infrastruktuuri kaitse

Informatsiooni infrastruktuur on kaasaegse riigi ja majanduse üks alus, samas ohud sellele üha suurenevad. Vaja on kaitsta informatsiooni infrastruktuuri, arvestada infoturbe aspekte muudes infrastruktuuri kaitse valdkondades, korraldada küberkuritegevuse vastaseid toiminguid ja koordineerida neid tegevusi ka rahvusvaheliselt. Käesolevasse valdkonda kuuluvad muu hulgas järgmised tegevused:

- informatsiooni infrastruktuuri kaitse tagamine
- kriitilise informatsiooni infrastruktuuri turvaeesmärkide ja turbeastmete täpsustamine, vajaduse korral täiendavate turvameetmete rakendamine
- interneti füüsilise ja loogilise infrastruktuuri tugevdamine
- infoturbe aspektide arvestamine muudes infrastruktuuri kaitse valdkondades
- küberkuritegevuse vastaste toimingute korraldamine ja koordineerimine
- küberrünnakute, sealhulgas välismaalt tulevate rünnete vastase tegevuse korraldamine ja koordineerimine
- rämpsposti levitamise vastaste õiguslike, organisatsiooniliste ja tehniliste meetmete edasiarendamine ning osalemine riikide sellealases koostöös
- internetis oleva illegaalse või ebasoovitava sisu vastaste meetmete rakendamine (eriti seoses lastekaitsega)
- infoturbeintsidentidega tegeleva üksuse CERT (*Computer Emergency Response Team*) edasiarendamine
- küberjulgeolekut tagavate metoodikate ja meetmete täiendamine ning osalemine sellealases rahvusvahelises koostöös.

3.5. Inimeste ja varade kaitse rakendustegevused

Infoturbe õigusaktid ja meetmed on vaja ellu viia. Eriti oluline on inimeste kaitse vastavalt põhiõigustele ning asutuste ja ettevõtete kaitse meetmete rakendamine. Sellesse valdkonda kuuluvad muu hulgas järgmised tegevused:

- turvaliste (ID-kaardi põhiste) tüüplahenduste väljatöötamine ja rakendamine
- piiriüleste avaliku võtme infrastruktuuril (sh ID-kaardil) põhinevate teenuste käivitamine
- ISKE ja infoturbe standardite rakendamine
- isikuandmete kaitse meetmete rakendamine.

4. Õiguslik koosvõime

Allpool esitatakse olulisemad infoturbe koosvõime raamistikku reguleerivad õigusaktid ning muud asjassepuudutavad seadused ja määrused, strateegiad, visioonid ja head tavad.

4.1. Seadused ja määrused

Eestis reguleerivad infoturvet otseselt või kaudselt järgmised seadused ja määrused:

- avaliku teabe seadus
- isikuandmete kaitse seadus
- infosüsteemide turvameetmete süsteemi määrus
- infosüsteemide andmevahetuskihi määrus
- infoühiskonna teenuse seadus
- isikut tõendavate dokumentide seadus
- digitaalallkirja seadus
- autoriõiguse seadus
- elektroonilise side seadus
- hädaolukorra seadus
- karistusseadustik
- kriminaalmenetluse seadustik
- elutähtsate teenuste toimepidevuse riskianalüüsi koostamise juhend
- elutähtsate teenuste toimepidevuse plaani koostamise juhend.

4.2. Strateegiad, raamistikud ja tegevuskavad

Eestis käsitlevad infoturbevaldkonda otseselt või kaudselt järgmised strateegiad, raamistikud ja tegevuskavad:

- „Eesti infoühiskonna arengukava 2013" ja selle rakendusplaan
- „Küberjulgeoleku strateegia 2008–2013" ja selle rakendusplaan
- „Riigi infosüsteemi koosvõime raamistik"
- Riigi IT arhitektuur
- „Semantilise koosvõime raamistik"
- Euroopa digitaalne tegevuskava[10]
- „Euroopa e-valitsuse tegevuskava 2011–2015 IKT-lahendused aruka, jätkusuutliku ja innovaatilise valitsemise edendamiseks"[11]
- „Euroopa avalike teenuste koosvõime alused"[12], „Euroopa koosvõimestrateegia Euroopa avalike teenuste osutamiseks"[13] ja „Euroopa koosvõimeraamistik Euroopa avalike teenuste osutamiseks"[14]
- „Euroopa kaitsmine laiaulatuslike küberrünnakute ja häirete eest: valmisoleku, turvalisuse ja vastupidavuse suurendamine"[15]

[10] KOM(2010) 245

[11] KOM(2010) 743

[12] KOM(2010) 744

[13] KOM(2010) 744 (1. lisa)

[14] KOM(2010) 744 (2. lisa)

- „Saavutused ja edasised sammud: üleilmse küberjulgeoleku suunas”[16]
- „Turvalise infoühiskonna strateegia – dialoog, partnerlus ja aktiivne osalemine”[17]
- ITU globaalse küberturbe tegevuskava[18].

4.3. Juhendid, head tavad, standardid, materjalid

Eestis käsitlevad infoturvet otseselt või kaudselt järgmised juhendid, head tavad ja standardid:

- infosüsteemide kolmeastmelise etalonturbe süsteemi (ISKE) rakendusjuhend[19]
- Andmekaitse Inspektsiooni juhendmaterjalid[20]
- infosüsteemide kolmeastmelise etalonturbe süsteemi (ISKE) rakendusjuhendi lisa 1: kataloogid (meede M 2.192: infoturbepoliitika koostamine)[21]
- asutuse infosüsteemi talitluspidevuse- ja taasteplaanid[22]
- Eesti infosüsteemide audiitorühingu infosüsteemide audiitorkontrolli eeskirjad[23]
- tehnilist koosvõimet tagavad soovituslikud standardid ja tehnoloogiad (vt allpool tehnilise koosvõime jaotises)
- Sihtasutuse Vaata Maailma hallatav arvutikaitse.ee veebisait[24]
- ISO 27000 standardite seeria[25]
- ENISA soovitused[26]
- maailma majandusfoorumi aruanne globaalsete riskide kohta[27].

[15] KOM(2009) 149

[16] KOM(2011) 163

[17] KOM(2006)251

[18] http://www.itu.int/osg/csd/cybersecurity/gca/

[19] http://www.ria.ee/ISKE

[20] http://www.aki.ee/est/?part=html&id=86

[21] http://www.ria.ee/public/ISKE/iske_kataloogid_5_01.pdf

[22] http://www.riso.ee/et/infopoliitika/soovitused

[23] http://www.eisay.ee/633

[24] http://www.arvutikaitse.ee/

[25] http://www.27000.org/

[26] http://www.enisa.europa.eu/

[27] http://www.weforum.org/pdf/globalrisk/report2008.pdf

5. Organisatsiooniline koosvõime infoturbe valdkonnas

5.1. Info- ja sideturbe korraldamine

Infoturbe koosvõime raamistiku eesmärkide saavutamiseks arvestavad kõik raamistiku koostamise ja elluviimisega seotud pooled oma valdkondlike tegevuste korraldamisel infoturbe vajadustega. Valitsusasutused võtavad infoturbe raamistiku kasutusele kooskõlas kehtivate õigusaktide ja oma põhimäärustega.

Infoturbe valdkondade vahelisi tegevusi koordineerib Majandus- ja Kommunikatsiooniministeerium, kaasates selleks avaliku sektori (sh Siseministeerium, Kaitseministeerium, Justiitsministeerium, Haridus- ja Teadusministeerium, Välisministeerium ja Riigikantselei) ning kolmanda ja erasektori esindajad. Lähtudes infoturberaamistiku eesmärkide saavutamiseks tehtud ettepanekutest ja soovitustest, vaatab Majandus- ja Kommunikatsiooniministeerium Eesti infoturbe olukorra ja arengu igal aastal üle ning täiendab raamistikku vajaduse korral.

Majandus- ja Kommunikatsiooniministeerium koordineerib Eesti infoturbe tegevuste käsitlemist Eesti infoühiskonna arengukavas ja selle rakendusplaanis.

Küberjulgeoleku strateegia koostas Vabariigi Valitsuse korralduse kohaselt Kaitseministeerium koostöös Haridus- ja Teadusministeeriumi, Justiitsministeeriumi, Majandus- ja Kommunikatsiooniministeeriumi, Siseministeeriumi ja Välisministeeriumiga. Alates 1. jaanuarist 2011 on küberjulgeoleku üldine koordineerimine, strateegia koostamise edasine koordineerimine ja Vabariigi Valitsuse julgeolekukomisjoni alakomisjoni (küberjulgeoleku nõukogu) töö koordineerimine Majandus- ja Kommunikatsiooniministeeriumi ülesanne.

Avaliku sektori infoturbe alaseid tegevusi finantseeritakse ametkondlikest eelarvetest, Euroopa Liidu fondidest ja teistest allikatest.

5.2. Organisatsioonid ja koostöö

Infoturve on oluline teema enamikus IT-alastes ettevõtmistes ja seepärast avaldavad selle kujunemisele mõju paljud avaliku ja erasektori asutused. Rahvusvaheliselt on tähtsamad küberjulgeolekut ja infoturvet mõjutavad organisatsioonid Euroopa Liit, Euroopa Nõukogu, NATO, ÜRO ja OECD. Eesti avalikust sektorist mõjutavad infoturbe valdkonda enam järgmised asutused.

- Majandus- ja Kommunikatsiooniministeeriumi riigi infosüsteemide osakond (RISO) koordineerib infoturbe koosvõime raamistiku väljatöötamist, rakendamist ja arendamist.
- Kaitseministeeriumi juhitud komisjon on koos teiste ministeeriumidega välja töötanud küberjulgeoleku strateegia ja koostanud selle rakendusplaani aastateks 2009–2011.
- Riigi Infosüsteemi Amet (RIA) korraldab X-tee, ISKE, CERT Eesti, kriitilise informatsiooni infrastruktuuri kaitse, RIA andmesideosakonna (ASO) võrgu ja avaliku võtme infrastruktuuriga seotud tegevusi.
- RISO korraldab infotehnoloogia, sealhulgas infoturbe valdkonna standardimist ning koordineerib riigi infosüsteemi keskse infrastruktuuri arendamist.
- Justiitsministeerium vastutab küberjulgeoleku karistusõiguse küsimuste lahendamise eest.

- Andmekaitse Inspektsioon täidab isikuandmete kaitse järelevalve ülesandeid ning tegeleb rämpsposti probleemidega.
- Majandus- ja Kommunikatsiooniministeeriumi sideosakond töötab välja riigi arengukavu elektroonilise ja postiside valdkonnas ning valmistab ette valdkonda reguleerivate õigusaktide eelnõusid.
- Tehnilise Järelevalve Amet on tehniliselt piiratud ressursside (raadiosagedused ja telefoninumbrid) kasutuse korraldaja ja elektroonilise side turu reguleerija Eestis ning tegeleb ka rämpsposti probleemidega.
- Siseministeerium koos teiste ministeeriumidega korraldab kriisireguleerimist.
- Kaitseliidu küberkaitse üksused annavad kriisiolukorras kriitilise infoinfrastruktuuri ettevõtetele abi.
- Keskkriminaalpolitsei infotehnoloogiakuritegude talitus ning Kohtuekspertiisi ja Kriminalistika Keskuse IT-labor tegelevad küberkuritegevuse probleemidega.
- Kaitseväe Side- ja Infosüsteemide Väljaõppe- ja Arenduskeskus viib ellu kaitseotstarbelisi side, infotehnoloogia ja infooperatsioonide arendusprojekte ning korraldab erialast koolitust.
- NATO Küberkaitsekeskus[28] arendab NATO, selle liikmesriikide ja partnerite küberkaitsealast võimekust, koostööd ja infovahetust.
- Küberjulgeoleku nõukogu, Vabariigi Valitsuse julgeolekukomisjoni juurde moodustatud ja erinevaid ametkondi hõlmav ekspertrühm, mille tööd korraldab Majandus- ja Kommunikatsiooniministeerium, hindab küberjulgeoleku strateegia elluviimist ja tulemuslikkust.
- Eesti Hariduse ja Teaduse Andmesidevõrk EENet sätestab EENeti võrgu turvareeglid ja haldab turvalisuseteemalist postiloendit.
- Tarbijakaitseameti roll on inimesi internetis levivate pettuste eest hoiatada ja tõsta tarbijate teadlikkust, et osataks internetipettuseid ära tunda ja neid vältida.

Erasektorist mõjutavad infoturbe valdkonda enim pangad, telekommunikatsiooniettevõtted, Eesti Energia, AS Sertifitseerimiskeskus (SK), IT-teenuste pakkujad ja infoturbega tegelevad firmad.

Riigi infoturbealase töö korraldamisel on eriti tähtis erinevate seotud organisatsioonide omavaheline koostöö. Infoturberaamistiku valdkondi koordineerivad järgmised asutused:

- koostöö ja koordineerimine – Majandus- ja Kommunikatsiooniministeerium
- teadvustamine ja koolitus – Haridus- ja Teadusministeerium koostöös Riigikantselei, Kaitseministeeriumi ning Majandus- ja Kommunikatsiooniministeeriumiga
- infoturbe õigusaktide väljatöötamine ja uuendamine – Majandus- ja Kommunikatsiooniministeerium koostöös Siseministeeriumiga
- informatsiooni infrastruktuuri kaitse – Majandus- ja Kommunikatsiooniministeerium ja Siseministeerium koostöös Kaitseministeeriumiga
- inimeste ja varade kaitse rakendustegevused – Majandus- ja Kommunikatsiooniministeerium ja Siseministeerium koostöös Kaitseministeeriumiga.

[28] http://www.ccdcoe.org/

6. Semantiline koosvõime infoturbe valdkonnas

Semantilise koosvõime üks eesmärk infoturbe valdkonnas on see, et organisatsioonid, infosüsteemid, teenused ja arendajad saaksid infoturbe tasemetest ja nõuetest ühtemoodi ja üheselt aru. Näiteks kui ühe süsteemi turvanõuded ja -meetmed on nõrgad ning see süsteem soovib kasutada kõrge turbeastmega süsteemi andmeid, siis peavad kõrge turbeastmega süsteem või selle arendajad üheselt aru saama esimese süsteemi turbeastet kajastavast infost (ja vastupidi).

Semantilist koosvõimet riigi ja kohaliku omavalitsuse andmekogude vahel hõlbustab ISKE, kus esitatakse olulisemad infoturbe mõisted.

Semantilise koosvõime parandamiseks infoturbe valdkonnas kasutatakse vastavalt võimalustele infoturbe valdkonna sõnastikku, ontoloogiat ja muid semantikavarasid, mis vajadusel registreeritakse RIHAs.

Piiriüleste teenuste korral aitavad semantilist koosvõimet muu hulgas parandada muuhulgas tugevatel sertifikaatidel põhinevad autentimis- ja autoriseerimislahendused, mis Euroopa Liidu kodanikele luuakse.

6.1. Riigi infosüsteemi süntaksi- ja semantikavarasid TULEB kaitsta semantilise koosvõime raamistiku nõuete kohaselt.

7. Tehniline koosvõime infoturbe valdkonnas

Subsidiaarsuse põhimõtte kohaselt vastutab iga asutus infoturbe eest oma haldusalas. Käesolevas peatükis käsitletakse kõige tähtsamaid infoturbega seotud üleriigilisi tegevussuundi.

7.1. e-identiteet, Eesti avaliku võtme infrastruktuur ja ID-kaart

Et muuta Eesti infoühiskonda turvalisemaks, on vaja toimivat seadusandlust, infrastruktuuri, vahendeid ja inimeste teadlikkust. Oluline roll on seejuures Eesti avaliku võtme infrastruktuuril, sealhulgas ID-kaardil, mobiil-ID-l, digitaalsel templil ja digi-ID-l.

Eestis reguleerivad avaliku võtme infrastruktuuri ja ID-kaardi alast tegevust kaks seadust. Isikut tõendavate dokumentide seaduse § 2 nimetab digitaalset isikutunnistust kui ühte isikut tõendavatest dokumentidest. Seaduse § 3 järgi on digitaalseks isiku tõendamiseks ettenähtud dokument (digitaalne dokument) elektroonilises keskkonnas isiku tõendamiseks ja isikusamasuse kontrollimiseks ettenähtud dokument. Seadus kehtestab Eesti elanikule dokumendikohustuse ja kirjeldab ID-kaardi kui esmase siseriikliku isikuttõendava dokumendi funktsioone. Paragrahvi § 20[4] järgi on mobiil-ID vormis digitaalne isikutunnistus digitaalne isikutunnistus, mille digitaalset tuvastamist võimaldav sertifikaat ja digitaalset allkirjastamist võimaldav sertifikaat on seotud mobiiltelefoni SIM-kaardiga.

Digitaalallkirja seadus sisaldab Eestis kehtivat digitaalallkirja mõistet ning sellega seotud korda ja teenuseid, sealhulgas sertifikaatide väljaandmist. Seadus hõlmab nii ID-kaardi digitaalallkirja sertifikaate kui ka muid sertifitseerimisteenuseid, milleks antakse välja sertifikaate digitaalallkirja seaduse mõistes (sh mobiil-ID).

Kuna ID-kaarte väljastab kodanikele riik ja samas on riik teinud ID-kaardi elanikele kohustuslikuks, siis on selge, et just eelkõige avaliku sektori e-teenused peavad toetama ID-kaardi kasutust. Seega tuleb võimalusel üle minna ID-kaardi põhisele autentimisele ning koolitada kasutajaid ID-kaarti kasutama.

ID-kaarti võib kasutada mitmel viisil.

- **ID-kaardi isikuandmete faili kasutamine.** ID-kaardi isikuandmete fail sisaldab sama informatsiooni, mis on kaardile kantud visuaalselt: kaardiomaniku nime, kaardi kehtivusaega ja muud sarnast. Oluline on, et see sisaldab ka kaardiomaniku isikukoodi. Kui omanik sisestab kaardi kiipkaardilugejasse, on süsteemil võimalik sealt kiirelt välja lugeda isikukood ja kasutada seda edasistes toimingutes.
- **ID-kaardi elektroonilise isikutuvastuse omaduse kasutamine.** ID-kaardi autentimissertifikaat ehk elektroonilise isikutuvastuse sertifikaat võimaldab eeskätt veebiteenustel tuvastada kasutajaid turvaliselt ja eelneva registreerimiseta. Kliendi autentimine veebiseansiks on HTTPS-protokolli komponent ning veebiserverit saab hõlpsasti panna ID-kaardiga autentimist toetama. Pärast autentimist tuleb kontrollida kasutaja sertifikaadi kehtivust sertifitseerimisteenuse osutaja kehtivusinfo teenuste abil. Värskeima info annab kehtivuskinnituse teenus, mis kasutab OCSP-protokolli.
- **ID-kaardi @eesti.ee meiliaadressi kasutamine.** ID-kaardi autentimissertifikaat sisaldab ka riigi poolt kaardiomanikule antavat eluaegset meiliaadressi kujul Eesnimi.Perenimi_XXXX@eesti.ee, kus XXXX on juhuslikult genereeritud neljakohaline arv. Alates 2005. aastast väljastatakse sertifikaatide uuendamisel ja uute

ID-kaartide väljastamisel e-posti aadress kujul Eesnimi.Perenimi@eesti.ee. Kui sama ees- ja perenimega isikuid on mitu, saavad järgmised isikud aadressi kujul Eesnimi.Perenimi.N@eesti.ee, kus N on järjenumber. Eelmised aadresskujud jäävad samuti kehtima.

- **Digitaalallkiri.** Ametnik (nii nagu iga teinegi) saab kasutada ID-kaarti tööalaselt digitaalseks allkirjastamiseks. ID-kaardi digitaalallkirja sertifikaadi sertifitseerimispoliitika ei sea mingeid piiranguid sertifikaadi kasutusalale. Seega võib seda kasutada digitaalseks allkirjastamiseks mis tahes rollis. Siin on kohane võrdlus omakäelise allkirjaga – see on samasugune, olenemata selle andmise otstarbest.

Alates 2007. aastast on ID-kaardi kõrval alternatiiviks mobiil-ID. Alates 2010. aasta algusest väljastavad mobiil-ID SIM-kaarte kõik kolm Eesti suuremat mobiiloperaatorit (EMT, Elisa, Tele2). 2011. aastal hakati mobiil-IDd väljastama riikliku dokumendina, mis andis sellele kliendikaardist erineva positsiooni nii teenuste kasutamises (nt võib mobiil-IDd kasutada e-valimistel) kui ka kaitstuses (rakenduvad karistusseadustiku sätted olulise dokumendi kaitseks). Mobiil-ID funktsionaalsus pakub ID-kaardiga samaväärseid võimalusi. Mobiil-ID abil saab autentida e-keskkondades ning anda digitaalset allkirja. Seejuures ei ole kasutajal vaja kiipkaardilugejat ega arvutisse installeeritud eritarkvara.

2009. aasta alguses kehtima hakanud digitaalallkirja seaduse kohaselt on seadustatud digitaalne tempel, mis on digitaalallkirjaga tehniliselt sarnane. Kui digitaalallkirja annab kindel isik ühesuguste põhimõtete kohaselt, siis digitaalse templi võib olla tekitanud kas füüsiline või juriidiline isik väga erinevate põhimõtete järgi. Seetõttu on otstarbekas digitaalse templi sertifikaadiga siduda nn tembelduspõhimõtted, mis kirjeldavad digitaalse templi otstarvet, tekitamise viisi ja muid eripärasusi. Digitaalse templi andmist võib käsitleda kui elektroonilist vastet templile või blanketile.

Digitaalne isikutunnistus ehk digi-ID on ID-kaardiga sarnane kiipkaart, millega saab elektroonilises keskkonnas isikut tuvastada ja anda digitaalset allkirja. Digi-ID ja sellele kantud sertifikaatide kehtivusaeg on kolm aastat. Digi-IDd võib kasutada ID-kaardi kõrval samaaegselt. Digi-ID kasutamiseks elektroonilises keskkonnas ei ole vaja eraldi tarkvara, arvutile kehtivad samad nõuded ja see töötab sama tarkvaraga, mis ID-kaart. Digi-ID valmib ootetööna Politsei- ja Piirivalveameti kontoris (ID-kaart väljastatakse 30 päeva jooksul). Digi-IDd on eriti soovitatav kasutada tööülesannete täitmisel.

Euroopa Liidus on piiriülese e-identiteedi rakendamine kulgenud aeglaselt. Euroopa Parlamendi ja nõukogu direktiivi 2006/123/EÜ 8. artikli 1. punkt ütleb: „Liikmesriigid tagavad, et kõiki teenuste osutamise valdkonnale juurdepääsuga või selles valdkonnas tegutsemisega seotud haldustoiminguid ja -formaalsusi on võimalik hõlpsasti täita asjaomase ühtse kontaktpunkti kaudu ja asjakohastes pädevates asutustes vahemaa tagant ning elektrooniliste vahendite abil”. Teenuste direktiivist ajendatuna viiakse Eestis läbi piiriülese e-identiteedi ja digitaalallkirja tunnustamise projekti. Muu hulgas on DigiDoci portaalis loodud allkirjastamise tugi, mis võimaldab portaali kasutada e-identiteetide koostalitlusvõime platvormi loomise projektis STORK osalevate välisriikide kodanikel. DigiDoci portaali saab kasutada ka USB-lubakaardiga.

ID-kaardiga on seotud järgmised standardid:

- EVS 827:2004. Turvakiibi rakendus ja liides
- EVS 828:2004. Sertifikaadid Eesti Vabariigi isikutunnistusel
- EVS 821:2009. BDOC. Digitaalallkirja vorming
- RFC2650. OCSP: Online Certificate Status Protocol[29]
- W3C: XML-DSIG. XML Signature Syntax and Processing[30]

[29] http://www.faqs.org/rfcs/rfc2560.html

- ETSI TR 101 903. XAdES: XML Advanced Electronic Signatures[31].

Tulevikus tuleb arvestada ka standarditega ISO/IEC 24727 (*Identification cards – Integrated circuit card programming interfaces*) ja CEN/TS 15480 (*Identification card systems. European Citizen Card*).

Järgnevalt on välja toodud põhipunktid, mida silmas pidada e-teenuste arendamisel seoses ID-kaardi ja Eesti avaliku võtme infrastruktuuriga.

7.1. Avalik sektor PEAB riigi väljastatavat ID-kaarti oma infosüsteemides maksimaalselt kasutama.
7.2. Kõik avaliku sektori autentimist nõudvad süsteemid PEAKSID võimaldama ID-kaardiga autentimist ning VÕIVAD aktsepteerida ka mobiil-ID kasutamist.
7.3. Avalik sektor PEAB digitaalallkirja seaduse kohaselt aktsepteerima digitaalallkirju ja digitaalseid templeid.
7.4. Avalik sektor PEAKS avaliku teenuse osutamisel igal võimalikul juhul kasutama digitaalallkirju.
7.5. Avalik sektor PEAKS soodustama ametlikku suhtlust kodanikuga @eesti.ee meiliaadressi kaudu.
7.6. Asutuse dimensiooni näitamiseks ja automaatsete infosüsteemi väljavõtete turvamiseks VÕIB digitaalallkirja seaduse kohaselt kasutada digitaalseid templeid.

Lisainformatsioon on olemas ID-kaardi portaalis[32] ja SK veebisaidil[33] .

7.2. Infosüsteemide turvameetmed

7.2.1. Infosüsteemide turvameetmete süsteemi rakendamine

Kohustus rakendada riigi ja kohaliku omavalitsuse andmekogude pidamisel infosüsteemide turvameetmete süsteemi on sätestatud Vabariigi Valitsuse 20. detsembri 2007. aasta määrusega nr 252 „Infosüsteemide turvameetmete süsteem“ (nn ISKE määrus). Turvameetmete süsteemi koosseisu kuulub rakendusjuhend koos lisadega („Infosüsteemide kolmeastmelise etalonturbe süsteem ISKE. Rakendusjuhend“).

Infosüsteemide turvameetmete süsteemi kehtestamise eesmärk on määratleda üheselt mõistetavalt infosüsteemide turvanõuete spetsifitseerimise kord, turvanõuetest lähtuvalt andmeturbe eesmärkidele vastavate turvaklasside määramise kord ja turvaklassidele vastavate turvameetmete valimise kord.

Infosüsteemi turvaanalüüsi põhjal määratakse töödeldavate andmete koosseisu alusel turvaosaklassid, mille juures arvestatakse enim kaitsmist vajavate andmete andmeturbe eesmärgi taset. Turvaosaklassi tähistamisel kasutatakse vastava andmeturbe eesmärgi nimetusele viitavat tähte ja taseme numbrit. Turbetasemed jaotatakse teabe käideldavuse (K – eelnevalt kokkulepitud vajalikul/nõutaval tööajal kasutamiskõlblike andmete õigeaegne ja hõlbus kättesaadavus selleks volitatud tarbijaile), tervikluse (T – andmete õigsuse/täielikkuse/ajakohasuse tagatus ning päritolu autentsus ja volitamatute muutuste puudumine) ja konfidentsiaalsuse (S – andmete kättesaadavus ainult selleks volitatud tarbijaile ning kättesaamatus kõigile ülejäänutele) alusel. Andmete turvaklassi tähis moodustatakse osaklasside tähistest nende järjestuses K-T-S, näiteks K2T3S1.

[30] http://www.w3.org/TR/2002/REC-xmldsig-core-20020212/

[31] http://uri.etsi.org/01903/v1.3.2/

[32] http://www.id.ee

[33] http://www.sk.ee

Turvaklassidele vastavad turvameetmed valitakse infosüsteemide kolmeastmelise etalonturbe süsteemi (ISKE) rakendamisjuhendi alusel. Riigi Infosüsteemi Ametil on kohustus tagada meetmete ajakohasus.

Igal juhul tuleb tegeleda infoturbe haldusega, mis hõlmab tavaliselt järgmisi tegevusi:

- asutuse infoturbe poliitika väljatöötamine
- infoturbe organisatsioonilise struktuuri loomine, sealhulgas rollide ja kohustuste piiritlemine organisatsioonis
- riskihaldus, sealhulgas järgmiste elementide piiritlemine ja hindamine: kaitstavad varad, ohud, nõrkused, toimed, riskid, turvameetmed, jääkriskid ja kitsendused
- vajaduse korral infoturbe kontseptsiooni koostamine, mis sisaldab vajaliku turbetaseme määramist, praeguse infoturbe olukorra kirjeldust, etalonmeetmete valimist, riskianalüüsi tulemustest sõltuvalt lisameetmete valimist, kõigi meetmete ühendamist ja koostoime hindamist, turbekulude hindamist ja plaanimist, jääkriski hindamist ja kinnitamist
- konfiguratsioonihaldus
- muutuste haldus
- talitluspidevuse plaanimine ja avariijärgse taaste plaanimine
- turvameetmete valimine ja rakendamine
- infoturbealane koolitus, personali teadvustamine infoturbe küsimustes
- järeltegevused, sealhulgas hooldus, turvaaudit, seire, läbivaatus ja intsidentide käsitlus
- infoturbe aruanded juhtkonnale.

Vabariigi Valitsuse määruse „Infosüsteemide turvameetmete süsteem" (ISKE määrus) 25.01.2009 jõustunud redaktsioon sätestab ka turvameetmete süsteemi rakendamise auditeerimise põhimõtted riigi infosüsteemi kuuluvate riigi andmekogude pidamisel. Andmekogu vastutav töötleja, kelle andmekogu kuulub turbeastmesse H, oli kohustatud esmakordse turvameetmete süsteemi rakendamise auditeerimise läbi viima hiljemalt 1. märtsiks 2010. Turbeastme M korral oli see tähtaeg 1. detsember 2010 ning turbeastme L korral 1. märts 2011.

7.7. Vabariigi Valitsuse 20. detsembri 2007. aasta määruse nr 252 kohaselt TULEB riigi ja kohaliku omavalitsuse infosüsteemide ning infovarade kaitseks rakendada infosüsteemide kolmeastmelist etalonturbe süsteemi ISKE..
7.8. ISKE rakendamist riigi infosüsteemide ja infovarade kaitseks TULEB auditeerida ülalnimetatud määruse kohaselt. ISKE rakendamist kohaliku omavalitsuse infosüsteemide ja infovarade kaitseks on SOOVITATAV auditeerida.

7.2.2. Muud andmekasutajad ja teenustasemete lepped

ISKE rakendamisel (turvaklasside määramisel, turvameetmete valimisel, turvameetmete rakendamisel) lähtutakse mõnikord vaid oma asutuse seisukohast. Selline lähenemine on ühest küljest loomulik, samas võivad ühe asutuse infosüsteemi andmetest suurel määral sõltuda ka teiste asutuste süsteemid. Seega on asutusepõhisel lähenemisel vähemalt kaks tõsist puudust.

Esiteks ei pruugi ISKE rakendamine ühe asutuse seisukohast lähtudes arvestada seotud andmete väärtuse ja teiste tarbijate vajadustega (turvaklasside määramisel) ning sellest põhjustatud koormusega (turvameetmete valimisel ja rakendamisel). Seepärast tuleks ISKE rakendamisel peale oma asutuse arvese võtta ka seotud andmete väärtust ja teiste andmekasutajate vajadusi.

Teiseks annavad ISKE turvaklassid turvaomadustest väga üldise pildi. Paljude teenuste jaoks on vaja tunduvalt täpsemat spetsifikatsiooni, näiteks ajakriitilise teabe käideldavuse kohta.

Seepärast on soovitatav lisaks ISKE rakendamisele kehtestada teenustasemete lepped andmekogude pakutavate teenuste ja andmete osas.

7.9. ISKE rakendamisel TULEB peale oma asutuse arvesse võtta ka seotud andmete väärtust ja teiste andmekasutajate vajadusi.
7.10. Lisaks ISKE rakendamisele on SOOVITATAV kehtestada teenustasemete lepped andmekogude pakutavate teenuste ja andmete osas.

7.2.3. Kriitilise informatsiooni infrastruktuuri kaitse

Kriitilised infrastruktuurid koosnevad sellistest füüsilistest ja infotehnoloogia rajatistest, võrkudest, teenustest ja ressurssidest, millel häirimisel või hävitamisel on tugev mõju kodanike tervisele, ohutusele, julgeolekule, majanduslikule heaolule või valitsuste tõhusale toimimisele. Kriitilised infrastruktuurid hõlmavad paljusid majandussektoreid, kaasa arvatud pangandus ja rahandus, transport ja turustamine, energia, kommunaalmajandus, tervishoid, toiduga varustamine ja side ning valitsuse võtmeteenistused.[34]

Siseministri määruses „Toimepidevuse riskianalüüsi koostamise juhend"[35] on määratletud elutähtsad teenused. Need on teenused, mis on hädavajalikud eluliselt tähtsate ühiskondlike toimingute, tervishoiu, turvalisuse, julgeoleku ning inimeste majandusliku ja sotsiaalse heaolu korraldamiseks. Hädaolukorra seaduses sätestatakse, et elutähtsa teenuse osutaja on kohustatud tagama elutähtsa teenuse osutamiseks kasutatavate infosüsteemide ning nendega seotud infovarade turvameetmete alalise rakendamise.

Teiste andmekasutajate vajaduste arvestamisel tuleks küberjulgeoleku strateegia lisa 1[36] ja hädaolukorra seaduse[37] kohaselt erilist tähelepanu pöörata võimalikele seostele kriitilise infrastruktuuriga (nt kriitilise infrastruktuuri varade, teenuste või süsteemidega). Kui sellised seosed on olemas, tuleks neid arvestada süsteemide turvaklasside, turbeastmete ja turvameetmete valikul.

Kriitilise informatsiooni infrastruktuuri teenused on tihti sõltuvusahelates. Näiteks mõne elutähtsa teenuse toimimiseks võib olla vaja terve rea komponentsüsteemide ja -teenuste toimimist. Kui asutus või ettevõte on üks komponent sellises ahelas, tuleks seda kindlasti arvestada. Täiendavaid turvanõudeid tuleks kaaluda ka juhul, kui organisatsiooni süsteemid võivad mõjutada interneti infrastruktuuri toimimist või on seotud SCADA juhtimissüsteemidega. Ülalnimetatud juhtudel tuleks muu hulgas analüüsida organisatsiooni süsteemide ja infrastruktuuri vastupanuvõimet võimsa elektromagnetilise impulsi (EMP pommi) mõjule.

Täiendavaid turvanõudeid tuleks arvestada ka allhankelepingutes, sealhulgas teenusepakkujate serveriruumide ja muu infrastruktuuri osas.

Riigi ja kohaliku omavalitsuse andmekogu pidamisel võib ISKE rakendamise käigus (nt infosüsteemidega seotud elutähtsaid teenuseid analüüsides) selguda täiendavate turvanõuete vajadus.

7.11. Elutähtsa teenuse osutaja PEAB tagama elutähtsa teenuse osutamiseks kasutatavate infosüsteemide ning nendega seotud infovarade turvameetmete alalise rakendamise hädaolukorra seaduse kohaselt.

---

[34] KOM(2004) 702 komisjoni teatis nõukogule ja Euroopa Parlamendile kriitilise infrastruktuuri kaitse kohta terrorismivastases võitluses.

[35] https://www.riigiteataja.ee/akt/13326405

[36] https://valitsus.ee/UserFiles/valitsus/et/valitsus/arengukavad/kaitseministeerium/kuberjulgeolek.pdf

[37] Vt § 34, https://www.riigiteataja.ee/akt/108112010021.

7.12. Kui riigi või kohaliku omavalitsuse asutuse andmekogud on seotud kriitilise informatsiooni infrastruktuuriga (nt kriitilise infrastruktuuri varade, teenuste või süsteemidega), TULEB selliseid seoseid arvestada ISKE rakendamisel, sealhulgas süsteemide turvaklasside, turbeastmete ning turvameetmete valikul. Selle nõude järgimine on SOOVITATAV ka ettevõtetel.
7.13. Riigi ja kohaliku omavalitsuse asutuste andmekogude eest vastutajad PEAVAD analüüsima oma asutuse infosüsteemide võimalikku mõju hädaolukorra seaduses toodud elutähtsatele teenustele. Selline analüüs on SOOVITATAV ka ettevõtetel

7.3. Soovitatavad standardid, juhised ja tehnoloogiad

Selles jaotises esitatakse infoturbe seisukohast olulisemad standardid, juhised ja tehnoloogiad. Riigil tuleb raamistikus nimetatud alusdokumendid (sh standardid) vastavalt võimalustele ja kooskõlas autoriõiguse ning muude piirangutega koondada riigi hallatavasse repositooriumisse ja teha avalikule sektorile tasuta kättesaadavaks.

7.3.1. Standardid

Teema	Standard või juhis	Lühend
Turbekorraldus	EVS-ISO/IEC 27000:2010 Infotehnoloogia. Turbemeetodid. Infoturbe halduse süsteemid. Ülevaade ja sõnavara	ISO/IEC 27000
Turbekorraldus	EVS-ISO/IEC 27001:2006. Infotehnoloogia. Turbemeetodid. Infoturbe halduse süsteemid. Nõuded	ISO/IEC 27001
Turbekorraldus	EVS-ISO/IEC 27002:2008. Infotehnoloogia. Turbemeetodid. Infoturbe halduse tegevusjuhis (endine EVS-ISO/IEC 17799:2003. Infotehnoloogia. Infoturbe halduse menetluskoodeks)	ISO/IEC 27002, ISO/IEC 17799
Turbekorraldus	EVS-ISO/IEC 27003:2011 Infotehnoloogia. Turbemeetodid. Infoturbe halduse süsteemi teostusjuhis	ISO/IEC 27003
Turbekorraldus	EVS-ISO/IEC 27005:2009. Infotehnoloogia. Turbemeetodid. Infoturvariski haldus	ISO/IEC 27005
Turbekorraldus	EVS-ISO/IEC TR 13335. Infotehnoloogia. Infoturbe halduse suunised. Osad 1-5 (osaliselt asendatud standardi ISO/IEC 27005 poolt)	ISO/IEC TR 13335
Turbekorraldus	ISO TR 13569 Pangandus ja sellega seotud rahandusteenused. Infoturbe suunised	ISO TR 13569
Turbekorraldus	Governance, Control and Audit for Information and Related Technology (COBIT). Infosüsteemide auditi ja juhtimise fondi väljaanne	COBIT
Elutsükli protsesside haldus	EVS-ISO/IEC 12207:2009. Süsteemi- ja tarkvaratehnika. Tarkvara elutsükli protsessid EVS-ISO/IEC TR 15271:1999 Infotehnoloogia. ISO/IEC 12207(Tarkvara elutsükli protsessid) juhend.	ISO/IEC 12207, ISO/IEC TR 15271
Sõnastikud	EVS-ISO/IEC 2382. Infotehnoloogia. Sõnastik	EVS-ISO/IEC 2382
Etalonturve	Infosüsteemide kolmeastmelise etalonturbe süsteem (ISKE). ISKE aluseks olev IT-Grundschutzhandbuch	ISKE, IT-Grundschutzhandbuch
Teenuste haldus	ISO/IEC 20000 standardipere standardid ja ITIL	ITIL

7.3.2. Protokollid ja tehnoloogiad ning muud soovitused

Teema	Protokoll/tehnoloogia	Lühend
Ipsec	IPSec koosneb reast protokollidest, mis on ette nähtud IP-kommunikatsiooni krüptimiseks, tervikluse tagamiseks, autentimiseks ja võtmete haldamiseks: http://www.ietf.org/rfc/rfc2411.txt	IPsec
TLS/SSL	TLS IETFi protokoll, mille eelkäija on SSL (*Secure Socket Layer*): http://www.ietf.org/rfc/rfc2246.txt	TLS/SSL
SSH	Secure Shell (SSH) v 2: http://tools.ietf.org/html/rfc4251	SSH-2
S/MIME	Secure/Multipurpose Internet Mail Extensions (S/MIME) v 3: http://www.ietf.org/rfc/rfc2633.txt	S/MIME
XML Signature	XML Signature Syntax and Processing: http://www.w3.org/TR/2002/REC-xmldsig-core-20020212/	XMLSig
XML encryption	XML-Encryption Syntax and Processing (XMLenc): http://www.w3.org/TR/xmlenc-core/	XMLenc
XML Key management	XML-Key Management Specification (XKMS) v 2.0: http://www.w3.org/TR/xkms2/	XKMS
SAML	Security Assertion Markup Language (SAML): http://www.oasis-open.org/committees/security/index.shtml	SAML
PKI	ID-kaardil, digi-ID-l ja mobiil-ID-l olevate sertifikaatide (ESTEID) profiil: http://sk.ee/repositoorium/profiil/	ESTEID
Tulemüürid. Paketifilter	Packet filtering	Packet filtering
NAT	Network Address Translation (NAT)	NAT
Lüüs	Application level gateway, proxy server	Proxy
DMZ	Demilitarised zone (DMZ)	DMZ
Pordid	Avaliku sektori veebides PEAKS kasutama tuntud porte (80, 443)	

7.14. Riigi infosüsteemi arendusel PEAKS lähtuma koosvõimeraamistikus soovitatud standarditest ja tehnoloogiatest.
7.15. Riik PEAKS tegema koosvõimeraamistikus nimetatud standardid avalikule sektorile tasuta kättesaadavaks.

8. Raamistiku rakendamine

8.1. Soovitused infoturbe saavutamiseks

8.1. Riigi või kohaliku omavalitsuse andmekogusid pidava asutuse tippjuht, IT-juht või -spetsialist peab oma süsteemide arenduse ja nende koosvõime tagamisel arvestama järgmist.

- Asutuse infotöö korraldamisel, sealhulgas andmekogude arendamisel, PEAB järgima avaliku teabe seadust, isikuandmete kaitse seadust, Vabariigi Valitsuse määrust „Infosüsteemide turvameetmete süsteem", Vabariigi Valitsuse määrust „Infosüsteemide andmevahetuskiht" ning ISKE metoodikat. Samuti PEAKS arvesse võtma infoturbestandardeid (nt EVS-ISO/IEC 27001 ja EVS-ISO/IEC 27002) ning info- ja sidustehnoloogia juhtimiseesmärkide (COBIT) raamistikku.
- Asutuse infoturbe poliitika ja eelarve kavandamisel PEAB lisaks arvestama „Infoühiskonna arengukava 2013" ja selle rakendusplaani ning riigi infosüsteemi arhitektuuri ja koosvõime raamistikku, küberjulgeoleku strateegiat. SOOVITATAV on arvestada ka RISO soovitusi asutuse infoturbepoliitika ning infosüsteemi talitluspidevus- ja taasteplaanide kohta[38].
- Kui asutus või ettevõte pakub hädaolukorra seaduse tähenduses elutähtsat teenust, siis PEAB ta koostama toimepidevuse riskianalüüsi ja plaani ning rakendama täiendavaid turvameetmeid.

Nende nõuete järgimine on SOOVITATAV ka ettevõtetel.

Infoturbe õigusaktide edasisel täiendamisel on SOOVITATAV täpsemalt kirjeldada teenuspõhiste süsteemide infoturbe aspekte ja eeldusi (nt vastavad suunad ISKE ja infoturbe juhendmaterjalide arendamisel).

8.2. Infoturbe lühiküsimustik valdkonna infoturbepoliitika eest vastutajale, asutuse IT-juhile ja infoturbe eest vastutajale

Riigi ja kohaliku omavalitsuse andmekogude pidamisel on kohustuslik rakendada ISKE-süsteemi. ISKE on väga põhjalik, kattes näiteks selliseid teemasid nagu infoturbe organisatsioon, koolitus, analüüs, turvapoliitika, intsidentide käsitlus, allhanked ja varundus ning infrastruktuuri, süsteemide, rakenduste ja võrkude kaitse.

Kuna ISKE rakendamisalast jäävad välja mitmed asutuseülesed küsimused, on järgnevalt toodud lühiküsimustik asutuse juhile, IT-juhile ja infoturbe eest vastutajale.

8.2. Kas asutuse ülesanded Eesti infoturbe kujundamisel, sealhulgas infoturbe koosvõime raamistikus ja küberjulgeoleku strateegias ning tegevusplaanis nõutud tegevused, on analüüsitud, teadvustatud ja delegeeritud?
8.3. Kas asutusel on olemas infoturbe eest vastutaja?
8.4. Kas asutuse juhtkond arutab pidevalt asutuse ja selle andmekogude infoturbe olukorda?
8.5. Kas vajaduse korral on täpsustatud teistele andmekasutajatele vajalikke teenustasemete reaalseid väärtusi?
8.6. Kas on arvesse võetud elutähtsate teenuste osutamise ja kriitilise infrastruktuuri kaitse nõudeid?

[38] http://www.riso.ee/et/node/52

8.7. Kas asutusel on olemas ulatusliku hädaolukorra lahendamise plaan võimaliku infoturbe intsidendi tarbeks, mis võib hõlmata mitut ametkonda?
8.8. Kas arvesse on võetud isikuandmete töötlemise nõudeid?
8.9. Kas ISKE turvaklasside määratlemisel on võetud arvesse ka teiste andmekasutajate vajadusest tulenevaid nõudmisi, näiteks konfidentsiaalsuse ja käideldavuse osas?
8.10. Kas asutuse IT-infrastruktuuri ja andmekogude olukord on viidud ISKE nõuetega vastavusse?
8.11. Kas turvameetmete süsteemi rakendamist on auditeeritud ning auditi soovitused arvesse võetud?

8.3. Mõõdikud

Majandus- ja Kommunikatsiooniministeerium osaleb interneti turvalisuse mõõdikute väljatöötamises ja edendamises ning viib läbi ID-kaardi ja e-teenuste kasutatavuse uuringuid. Muu hulgas kasutatakse infoturbe hindamisel järgmisi mõõdikuid:

- ID-kaarti ja mobiil-IDd elektrooniliseks isikutuvastuseks ja digiallkirjastamiseks kasutavate Eesti elanike arv
- turvaliste, ID-kaardi ja mobiil-ID võimalusi arvestavate, avaliku sektori e-teenuste pakkumiseks ning avaliku sektori sisemiseks toimimiseks kasutatavate lahenduste arv
- RIHA alusel jälgitavad mõõdikud, sealhulgas RIHAs registreeritud asutuste, infosüsteemide, teenuste, klassifikaatorite ja muude objektide arv
- X-teega liitunud asutuste ja andmekogude arv
- ISKE põhjal auditeeritud asutuste arv
- ligipääsetavuse nõuetele vastavate avaliku sektori veebisaitide osakaal
- Euroopa Liidu pakutud e-teenuste näidisvalikust elluviidud rakenduste arv
- CERT Eesti väljastatavad mõõdikud.

Lisaks on olemas mitmeid muid mõõdikuid, mille otstarbekust tuleb veel analüüsida, näiteks rünnete arv, rämpsposti osakaal, illegaalse sisu osakaal.