RIIGI INFOSÜSTEEMI AMET

INFOSÜSTEEMIDE KOLMEASTMELISE ETALONTURBE SÜSTEEMI ISKE

Rakendusjuhend

Versioon 8.00
Jaanuar 2017

Sisukord

1 Lühiülevaade....3
1.1 Rakendusala....3
1.2 Etalonturbe olemus....3
1.3 Astmeline etalonturve....4
1.4 Rakendusjuhendi struktuur....4
1.5 ISKE rakendamine....4
1.5.1 ISKE rakendamise 11 sammu....5
1.5.2 ISKE rakendamine pilveteenuste kasutamisel ja teenuste väljasttellimisel....6
1.6 Etalonturbe täiendamine....6
2. Infovarade vajaliku turvataseme määramine....7
2.1 Infosüsteemide analüüs....7
2.1.1 Infosüsteemide inventuur....7
2.1.2 Infovarade spetsifitseerimine ja liigitus....7
2.1.3 Infovarade grupeerimine....8
2.2 Turvalisuse näitajad....8
2.2.1 Informatsiooni turvalisus ja turvaeesmärgid....8
2.3 Andmete turvaklassi määramine....9
2.4 Muude infovarade turvaklassi määramine....12
3. Nõutava turbeastme ja turvameetmestiku määramine....13
3.1 Turbeastme määramine turvaklassi järgi....13
3.2 Turvaklassita infovarade turbeastme määramine....16
3.3 Turvameetmete määramine....16
4 Kasutatud mõisted ja lühendid....17
5 Lisateabe viited....20
LISA 1 – Muudatused ISKE rakendusjuhendi versioonis 8.00....21

1 Lühiülevaade

ISKE põhineb turvet vajavate infovarade kirjeldamisel tüüpmoodulite abil ning sisaldab vahendeid iga tüüpmooduli turvaklassi määramiseks ja mooduli nõutava turbeastme määramiseks selle turvaklassi järgi. Sõltuvalt tüüpmooduli nõutavast turbeastmest määratakse mooduli turvaspetsifikatsiooni kaudu kataloogidest turvameetmed ja kontrollitakse mooduli turvalisust ohtude kataloogi abil.

ISKE kataloogid asuvad ISKE Portaalis, aadressil https://iske.ria.ee, samas portaalis on kajastatud ka kataloogide versioonide muutelugu.

1.1 Rakendusala

ISKE on mõeldud andmekogude pidamisel kasutatavate infosüsteemide ja nendega seotud infovarade turvalisuse saavutamiseks ja säilitamiseks.

ISKE on rakendatav ka muudes riigi- ja omavalitsusasutustes, äriettevõtetes ning mittetulunduslikes organisatsioonides.

ISKE ei ole mõeldud riigisaladust käitlevate infosüsteemide turbeks.

1.2 Etalonturbe olemus

ISKE rakendamine tähendab seda, et nõutava turvataseme saavutamiseks tuleb rakendada kõik konkreetse infovara tüübi ja konkreetse nõutava turvataseme kohta spetsifitseeritud kohustuslikud meetmed. Turvameedet ei pea rakendama juhul kui konkreetse turvameetme rakendamine ei vähenda riske ja/või turvameetme rakendamine on kulukas võrreldes turvameetme rakendamisest tulenevate riskide vähendamisega. Samuti ei pea igat turvameedet rakendama, kui riskid on kaetud teiste meetmete rakendamisega.

Riigiasutustes tuleb konkreetsete turvameetme mitte rakendamine aktsepteerida infoturbe juhi või infoturbe eest vastutava isiku poolt. Seejuures tuleb asutuse juhti teavitada turvameetmete mitterakendamisest tulenevatest riskidest.

Lisaks on igal turvatasemel soovituslikud meetmed, mida soovitatakse rakendada, kuid mis ei ole kohustuslikud:

- "Z" tähistab soovituslikke meetmeid, mis võivad osutuda vajalikeks eelkõige kõrgema turvanõudluse puhul.
- "W" tähistab meetmeid, mille eesmärgiks on aidata mõista ja rakendada teisi turvameetmeid

NB! Kasvõi ühest kohustuslikust meetmest loobumine võib tähendada seda, et nõutavat turvataset ei saavutata.

ISKE rakendamisele vaatamata tuleb asutuste infoturbe eest vastutajail hoolikalt jälgida teavet uute ohtude kohta ja vajaduse korral rakendada lisaks etalonmeetmetele muid abinõusid nende ohtude tõrjeks. Lisaks jäävad alati ohud, mida ei käsitle käesolev juhend, selle tulevased versioonid ega ka enamik teisi turvastandardeid, kuid millega tuleb igapäevaselt arvestada.

1.3 Astmeline etalonturve

Asutustes on reeglina kasutusel turvanõuete taseme poolest üksteisest erinevad süsteemid ja teenuseid. Neile on otstarbekas rakendada vastavalt erineva tugevusega turvameetmestikke.

ISKE pakub kolme turbeastet: madalat (L), keskmist (M) ja kõrget (H).

Meetmestik on ehitatud kihilisena, nii et keskmine aste saadakse teatud meetmete lisamise teel madala astme omadele ja kõrge aste saadakse teatud meetmete lisamisel keskmise astme omadele.

1.4 Rakendusjuhendi struktuur

ISKE rakendusjuhendi põhikomponendid on infovarade spetsifitseerimise ja turvaanalüüsi juhised ning järgmised etaloninstrumendid:

1) turvaklasside määramise 4-tasemeline skaala (vt jaotis 2.3),
2) tabel nõutava turbeastme (L/M/H) määramiseks turvaklassi järgi, vt jaotis 3.1
3) infovarade tüüpmoodulite turvaspetsifikatsioonide kataloog B, vt. viimast kehtivat versiooni: https://iske.ria.ee
4) ohtude kataloog G, vt. viimast kehtivat versiooni: https://iske.ria.ee
5) turbeastmete L ja M turvameetmete kataloog M, vt. viimast kehtivat versiooni: https://iske.ria.ee,
6) turbeastme H turvameetmete kataloog H, vt. viimast kehtivat versiooni: https://iske.ria.ee

Jaotises 5 viidatud võõrkeelsetest (alus)materjalidest võib leida muid abivahendeid: metoodilisi juhiseid, turvameetmete rakendamise põhjalikke juhendeid, dokumenteerimisvorme jm.

1.5 ISKE rakendamine

ISKE rakendamine on pidev protsess, kuna muutuvad nii IT keskkond, turvaohud ja meetmed kui ka ISKE ise.

Perioodiliselt ja asutuse IT keskkonna või süsteemide muudatuste puhul tuleb üle kontrollida, millised moodulid, ohud ja turvameetmed lisandusid ning vajadusel rakendada vajalikke turvameetmeid. Sama tuleks teha pärast ISKE rakendusjuhendi uuendamist ja ISKE Portaalis uue täisversiooni publitseerimist.

ISKE nõudmisi peab arvesse võtma enne uute infosüsteemide arendusega alustamist või olemasolevatesse muudatuste tegemist, sest infosüsteemide tagantjärele kohendamine kehtivatele nõuetele vastavaks võib osutuda väga keeruliseks.

ISKE rakendamise paremaks korraldamiseks asutuses tuleb määrata ISKE rakendamise eest vastutav isik – ISKE koordinaator/infoturbe eest vastutav isik/infoturbejuht vms. ISKE rakendamine asutuses ei saa olla IT-osakonna sisene „projekt“, vaid pigem kogu asutust läbiv programm või tegevuste kogum mistõttu on vajalik, et ISKE rakendamise eest vastutaval isikul oleks hea side asutuse juhtkonna ning erinevate osakondadega. Täiendavalt tuleb arvestada infoturbe juhtimise süsteemi määruse nõuetega, vt.https://www.riigiteataja.ee/akt/119032012004.

1.5.1 ISKE rakendamise 11 sammu

ISKE rakendamise eest vastutav isik korraldab järgnevat:

1. viib läbi koostöös asutuse IT eest vastutava töötajaga ja asutuse juhtkonnaga infovarade inventuuri ja spetsifitseerimise vastavalt juhistele jaotises 2.1
2. viib läbi koostöös põhitegevuse poole esindajatega andmekogude kaardistamise. Iga andmekogu omanik (ehk peakasutaja) määrab koostöös ISKE rakendamise eest vastutava isikuga andmekogule turvaklassi vastavalt jaotises 2.3 antud juhistele ning märgib turvaklassid infovarade spetsifikatsioonidesse. Lisaks tuleb edastada andmekogu turvaklass RIHAsse https://riha.eesti.ee kaudu.
3. määrab koos infoturbe spetsialistiga muude infovarade turvaklassi vastavalt juhistele jaotises 2.4 ning märgib turvaklassid infovarade spetsifikatsioonidesse.
4. määrab jaotises 3.1 oleva tabeli abil kõikide turvaklassiga infovarade vajaliku turbeastme ja märgib turbeastmed infovarade spetsifikatsioonidesse.
5. kui kõrgeimaks vajalikuks turbeastmeks osutus M või H, otsustab juhtkonna esindaja koos ISKE rakendamise eest vastutava isikuga, kas rakendada kogu asutuses ühte turbeastet või jaotada asutus eri turbeastmetega tsoonideks. Viimasel juhul kavandavad nad tsoonid ja selliste tsoonide loomiseks vajalikud muudatused. Kui turvaastmete määramisel ei ilmnenud vajadust turbeastet L ületavaks turbeks, rakendatakse aste L kogu asutuse ulatuses.
6. vaatab ISKE Portaalist läbi kataloogi B, võrdleb seda infovarade spetsifikatsioonidega ja märgib spetsifikatsioonidesse tüüpmoodulite tähised vastavalt juhistele jaotistes 2.1. Kui tüüpmoodulite kataloogi läbivaatusel ilmneb veel spetsifitseerimata varasid, spetsifitseerib ta need töö selles järgus. Tüüpmoodulid, millele vastavaid varasid asutuses ei ole, jäetakse arvestamata; see nõue ei puuduta organisatsioonilisi varasid, mis kuuluvad moodulirühma B1.
7. koostab kõrgeimast määratud turbeastmest lähtudes turbehalduse meetmete loetelu, leides need meetmed ISKE Portaalist kataloogi B põhjal turvameetmete kataloogist "M: turvameetmed turbeastmele L, M" ja turbeastme H korral ka kataloogist "H: turvameetmed turbeastmele H".
8. koostab koos juhtkonna esindaja ja asutuse IT eest vastutava töötajaga plaani ISKE Portaalist infoturbe halduse moodul B 1.0 meetmete rakendamiseks, seejärel määrab muude infovarade turbe rakendamise prioriteedid ja turbe rakendamise plaani, arvestades ka meetmete rakendamise maksumuse ning ajalise kestvuse prognoose. Plaani koostades on eelnevalt vajalik omada ülevaadet, missugused turvameetmed on juba rakendatud ja millised ei ole rakendatud.
9. korraldab plaani täitmise, koostades turvameetmete loetelud tüüpmoodulite turvaspetsifikatsioonide ja turvameetmete kataloogide põhjal, juhindudes turbehalduse meetmetest ja kaasates töösse asjakohaseid töötajaid ja informeerides regulaarselt juhtkonda.
10. kontrollib pärast iga infovara turvameetmete evitamist ISKE Portaalist ohtude kataloogi G alusel tegelikku turvaolukorda, arvestades tegelikke ohte konkreetse infosüsteemi lõikes. Kui ilmneb mingeid ohte, mida tüüpmooduli turvaspetsifikatsioon ei arvesta, kontrollib ta rakendatud turvameetmete piisavust tegelikes tingimustes ning rakendab vajaduse korral täiendavaid turvameetmeid.
11. hoiab konfiguratsiooni ja muudatuste haldust käigus, st kõik muudatused infovarade, tüüpmoodulite, turvaklasside ja meetmete osas tuleb asutuses kasutusel olevasse töövahendisse sisestada, et oleks tagatud ajakohane ülevaade asutuse infovaradega toimuvast.

NB! Kui asutuses tehakse olulisi muudatusi andmekogude osas (luuakse uus andmekogu, andmekogu andmete koosseis muutub vmt) ja/või nendega seotud infovarade lõikes, siis alustatakse kogu rakendamise protsessiga algusest peale või sellest etapist alates, mida muudatus mõjutas.

1.5.2 ISKE rakendamine pilveteenuste kasutamisel ja teenuste väljasttellimisel

Pilveteenuste kasutamisel ning IT teenuste väljasttellimisel tuleb arvestada, et teenusepakkuja infrastruktuur ja protsessid ei ole reeglina vahetult auditeeritavad. Seetõttu võib ISKE rakendamisel osaliselt tugineda asutuse ja teenuseosutaja vahelise lepingu tingimustele, teenuse osutamise üldtingimustele ning teenuseosutaja turvasertifikaatidele kajastades eelmainitut asjakohases riskianalüüsis.

Samuti peab arvestama võimalike riskidega, näiteks kolmanda osapoole pikaajaline võrgukatkestus, teenusepakkuja pankrot jmt. Täpsem loetelu on moodulis B1.11 Väljasttellimine (*Outsourcing*). Väljaspool Euroopa Liitu paiknevate teenusepakkujate puhul tuleb täiendavalt arvestada ka juriidiliste ja julgeoleku aspektidega. Kuivõrd hallatud tarkvara või teenust kasutav asutus vastutab andmete turvalisuse eest siiski igal juhul ise, tuleb asutusel teenusepakkuja valikul teenuslepingus osapoolte vastutus selgelt määratleda.

Olulisemad tingimused, mida peaks asutuse ja pilveteenuse osutaja vahelises lepingus võimalusel reguleerima, on loetletud "Riigipilve kontseptsiooni rakendamise õigusanalüüsis“ (lk 57, p 4.7 "Lepingutingimused avaliku pilveteenuse osutajaga", kättesaadav: *https://www.mkm.ee/sites/default/files/report-state-cloud-concept.ria_2016-05-11.final_.sorainen.pdf).*

1.6 Etalonturbe täiendamine

ISKE kataloogide publitseeritakse ISKE Portaalis (https://iske.ria.ee).

Ametlik majandus- ja kommunikatsiooniministri poolt kinnitatud ISKE kataloogide täisversioon ilmub perioodiliselt ja kannab järgmist markeeringut (X.00), täisversioon .

Täisversioonide vahel väljastatakse RIA poolt täiendavaid vaheversioone (markeeringuga X.01, X.02, …). Vaheversioonid sisaldavad olulisi turbevajaduste täienemisest tingitud muudatusi ja täiendusi mis kajastuvad ka järgmises ametlikus versioonis. Vaheversioonid võimaldavad rakendajatel jooksvalt teha algust turbemeetmete rakendamise tegevustega.

Iga järgmine versioon võib sisaldada uusi tüüpmooduleid koos vastavate turvameetmetega ja/või uusi turvameetmeid senistele tüüpmoodulitele.

ISKE rakendusjuhendi ja/või uue versiooni ilmumisel vaatab infoturbe spetsialist läbi täiendused moodulite loetelus ja moodulite turvaspetsifikatsioonides ning korraldab uutele moodulitele vastavate infovarade turbe ja võimalikud senistele moodulitele vastavate varade turvameetmete täiendused **ühe aasta jooksul peale uue juhendi ametlikku kinnitamist** majandus- ja kommunikatsiooniministri poolt. Aasta peale uue ametliku rakendusjuhendi avalikustamist lisatakse täiendused/muudatused auditeerimisele kuuluvate objektide nimekirja.

2. Infovarade vajaliku turvataseme määramine

2.1 Infosüsteemide analüüs

See on ettevalmistav töö, mis loob lähteandmed infosüsteemide turvaanalüüsiks ja selle dokumenteerimiseks. Töö sooritatakse kolmes etapis. Kõik koostatavad spetsifikatsioonid peavad sisaldama turvaklassi, turbeastme ja tüüpmooduli tähise lahtreid, mis täidetakse hiljem.

Inventuuri ja spetsifitseerimise detailsus sõltub asutuse vajadustest ja süsteemi arhitektuurist. Üldine põhimõte on, et detailsuse aste peab võimaldama ISKE rakendamist ning ei tohiks tekitada rakendajale asjatut aja- ja töökulu. Võimalusi detailsuse astme määramiseks on mitmeid:

- Spetsifitseerida sellise detailsusega, nagu seda on vaja ISKE rakendamiseks – moodulite määramiseks, ISKE rakendamise tööde planeerimiseks ja täitjate kaasamiseks jne.
  Näiteks, kui asutuses on kasutusel Windows Server 2008, peab see olema spetsifikatsioonis kirjas, et rakendada moodulit B 3.108, planeerida selle meetmed, määrata täitjad ning kontrollida täitmist.
- Spetsifitseerida sellise detailsusega, nagu on vaja IT keskkonna haldamiseks ja/või süsteemide konfiguratsioonihalduseks.
  Näiteks, asutustes tuleb niikuinii omada ülevaadet IT keskkonnast (seadmed, litsentsid, süsteemid jne). Selline ülevaade, mida on vajadusel täiendatud, võib olla ISKE rakendamiseks piisav.

Igal juhul tuleb eristada asutuse enda kontrolli olevaid infosüsteemi komponente ja väljast tellitavaid teenuseid, samuti pilveteenused.

2.1.1 Infosüsteemide inventuur

Infosüsteemide inventuuri vastavaust tuleb kontrollida vähemalt korra aastas. Soovituslik on kõik infosüsteemides toimunud muudatused, mis omavad tähtsust ISKE rakendamise osas, koheselt oma inventuuri haldamise töövahendisse sisse märkida.

2.1.2 Infovarade spetsifitseerimine ja liigitus

Iga kajastatud komponendi kohta peaks olema saadaval minimaalne informatsioon, mida võib säilitada eraldi tabelis, kataloogis või tööriistas/haldusvahendis. Komponendi jaoks valitud detailsusaste sõltub asutuse enda vajadustest kuid peab olema piisav, et sellele tuginedes saaks ISKE-t rakendada ja auditeerida.

Informatsiooni detailsusaste näide:

- Unikaalne nimetus (nt seadme täielik nimi või id number);
- Tüüp (nt x rakenduse andmebaasi server, tööjaam, sidesüsteem vmt) ja funktsioon;
- Kasutatav platvorm (st riistvara ja operatsiooni süsteem);
- Tööviis (st käitav, toetav või autonoomne);
- Kasutatav rakendus ja andmebaas;
- Asukoht (nt hoone ja ruumi number);
- Vastutav administraator ja kasutajad (üksus/ametikoht/roll/...);
- Olek (kasutuses, testimisel, plaanitud)

- Kasutatavad kommunikatsiooni liidesed (internet, Bluetooth, WLAN adapter);
- Võrguühenduse tüüp ja võrguaadress.

Lisaks seadmetele tuleb spetsifitseerida üldkasutatavad infrastruktuuri osad (nt arhiivi- ja laoruumid, koosolekuruumid, serveriruumid, seadmekapid, toitekilbid, toiteliinid jne).

Võrkude topoloogiat, infosüsteemi komponentide vahelisi seoseid jms. on mõistlik esitada/hallata skeemidena.

Infovarad liigitatakse käitavateks, toetavateks ja autonoomseteks varadeks.

Käitavad infovarad - varad, mis otseselt on vajalikud andmekogu töö tagamiseks (nt rakendus, andmebaas, server jmt);

Toetavad infovarad - varad, mis on vajalikud andmekogude ja/või nendega seotud käitavate varade toimimise tagamiseks, kuid mis ise ei ole otseselt vajalikud andmete töötlemiseks ega ka andmekogust andmete kättesaadavaks tegemisega.

Autonoomsed infovarad - varad, mille esmane funktsioon ei ole seotud andmete ega andmekogudega (nt tööruumid, majad).

Eelneval viisil eri tüüpi varadeks jagamine võib eri asutustes erineda ja siinkohal ei saa ette anda ka ainuõigeid lahendusi. Olulisem on siinkohal hinnata varade toetusastet. Selleks antakse vajalikud juhised käesoleva rakendusjuhendi jaotises 2.4.

2.1.3 Infovarade grupeerimine

Sarnased infovarad on soovitatav grupeerida mis lihtsustab ISKE haldust ja turvameetmete rakendamise protsessi.
Sarnaste infovarade grupeerimisel ühte gruppi võib arvestada järgmiste tunnustega:

- Infovarad on sama tüüpi;
- Infovarad on konfigureeritud ja konfigureeritakse ühetaoliselt;
- Infovarad on ühendatud võrku ühetaoliselt (IT süsteemid samasse kommutaatorisse);
- Infovaradel on samad administratiivsed ja infrastruktuursed nõuded;
- Infovaradel on samad kaitse nõuded;

Infovarade grupeerimisel tuleks arvestada, et turvameetmete rakendamise protsessis oleks jätkuvalt võimalik pidada arvestust turvameetmete rakendatuse üle.

Näide infovarade grupeerimisel on asutuse tööjaamad. Ühte gruppi võib paigutada asutuse tööjaamad, mille operatsioonisüsteemiks on Windows 7 ning mis on keskselt ja ühetaoliselt hallatud.

2.2 Turvalisuse näitajad

2.2.1 Informatsiooni turvalisus ja turvaeesmärgid

ISKE kasutab turvamudelit, mis toetub kolmel osaeesmärgi (käideldavuse, tervikluse ja konfidentsiaalsuse) tagamisele.

Andmete käideldavus on eelnevalt kokkulepitud vajalikul/nõutaval tööajal kasutamiskõlblike andmete õigeaegne ja hõlbus kättesaadavus (st vajalikul/nõutaval ajahetkel ja vajaliku/nõutava aja jooksul) selleks volitatud tarbijaile (isikutele või tehnilistele vahenditele**).** Käideldavus on esmane nõue iga infosüsteemi kõigile andmetele ja muudele infovaradele; käideldavuse kadumisel on kogu infosüsteem tarbetu.

Andmete terviklus on andmete õigsuse/täielikkuse/ajakohasuse tagatus ning päritolu autentsus ja volitamatute muutuste puudumine.

Andmete konfidentsiaalsus on andmete kättesaadavus ainult selleks volitatud tarbijaile (isikutele või tehnilistele süsteemidele) ning kättesaamatus kõigile ülejäänutele.

Üheski infosüsteemis ei ole olemas täielikku turvet**,** st täielikku käideldavust, täielikku terviklust ja täielikku konfidentsiaalsust. Millistele infoturbe aspektidele tuleb konkreetsete andmete korral tähelepanu pöörata, oleneb konkreetsest infosüsteemist ja selle otstarbest, st käideldavate andmete väärtusest. Enamasti tuleb arvesse võtta turvalisuse kõiki kolme komponenti, kuid erinevate kaaludega. Organisatsioonis nõutav infoturbe tase sõltub organisatsiooni ülesannetest, õigusaktidest ja eeskirjadest, organisatsiooni tegevuse sisemisest korraldusest, infosüsteemide ja ka teenuseandjate ja koostöö- või lepingupartnerite tagatud või nõutud turvatasemest jms.

Andmete turvalisus tähendab, et on saavutatud kolm eesmärki**: teabe käideldavus (K), teabe terviklus (T), teabe konfidentsiaalsus (S)**.

2.3 Andmete turvaklassi määramine

Andmete vajaliku turbetaseme peab määrama andmete omanik. Infoturbe spetsialist ei saa määrata andmete vajalikku turbetaset, kuna ta ei tarvitse teada andmete turbevajaduse tausta ja põhitegevuse poolelt andmetele esitatavaid nõudeid. IT- või infoturbespetsialist võib olla nõuandja rollis. Pärast andmete turbetaseme ja turvaosaklasside määramist omaniku poolt tuleb turvaklassid **asutuse juhtkonnal kinnitada**.

ISKE kasutab turbetasemete määramiseks neljapallilist skaalat ja põhineb eelnevalt nimetatud jaotise 2.2.1 kolmel turvaeesmärgil.
Rakendades kolmele turvaeesmärgile neljapallilist skaalat määratletakse alljärgnevad **turvaosaklassid**, mille tähised koosnevad turvaeesmärgi tähisest ja turvataseme väärtusest.

Käideldavus:

K0 – Käideldavus – väiksem kui 90% aastas ja maksimaalne lubatud ühekordse katkestuse pikkus teenuse töö ajal üle 24 tunni (st ühekordse katkestuse pikkus tohib olla suurem kui 24 tundi)*;
K1 – Käideldavus – suurem või võrdne 90% ja väiksem kui 99% aastas ning maksimaalne lubatud ühekordse katkestuse pikkus teenuse töö ajal kuni 24 tundi (st ühekordse katkestuse pikkus võib olla vahemikus väiksem või võrdne 24 tunniga ja suurem kui 4 tundi)*;
K2 – Käideldavus – suurem või võrdne kui 99% ja väiksem kui 99,9% aastas ning maksimaalne lubatud ühekordse katkestuse pikkus teenuse töö ajal kuni 4 tundi (st ühekordse katkestuse pikkus võib olla vahemikus väiksem või võrdne 4 tunniga ja suurem kui 1 tund)*;
K3 – Käideldavus – suurem ja võrdne kui 99,9 % aastas ja maksimaalne lubatud ühekordse katkestuse pikkus teenuse töö ajal kuni 1 tund (st ühekordse katkestuse pikkus võib olla väiksem või võrdne 1 tunniga) *;

Terviklus:

T0 – info allikas, muutmise ega hävitamise tuvastatavus ei ole olulised; info õigsuse, täielikkuse ja ajakohasuse kontrollid pole vajalikud;
T1 – info allikas, selle muutmise ja hävitamise fakt peavad olema tuvastatavad; info õigsuse, täielikkuse, ajakohasuse kontrollid erijuhtudel ja vastavalt vajadusele;
T2 – info allikas, selle muutmise ja hävitamise fakt peavad olema tuvastatavad; vajalikud on perioodilised info õigsuse, täielikkuse ja ajakohasuse kontrollid;
T3 – infol allikal, selle muutmise ja hävitamise faktil peab olema tõestusväärtus; vajalik on info õigsuse, täielikkuse ja ajakohasuse kontroll reaalajas.

Konfidentsiaalsus:

S0 – avalik info: juurdepääsu teabele ei piirata (st lugemisõigus kõigil huvitatutel, muutmise õigus määratletud tervikluse nõuetega);
S1 – info asutusesiseseks kasutamiseks: juurdepääs teabele on lubatav juurdepääsu taotleva isiku õigustatud huvi korral;
S2 – salajane info: info kasutamine lubatud ainult teatud kindlatele kasutajate gruppidele, juurdepääs teabele on lubatav juurdepääsu taotleva isiku õigustatud huvi korral,
S3 – ülisalajane info: info kasutamine lubatud ainult teatud kindlatele kasutajatele, juurdepääs teabele on lubatav juurdepääsu taotleva isiku õigustatud huvi korral.

* Maksimaalne lubatud katkestuste arv, maksimaalne lubatud summaarne katkestuste aeg ja muud detailsemad teenustaseme mõõdikud kirjeldatakse ja lepitakse kokku asutuse teenustaseme lepetes (SLA-des). Teenustaseme lepingus tuleb detailsemal tasemel määrata teenuse osutamise tingimused (nt päringutele vastamise aeg, planeeritud hooldustööde tegemise aeg, nõutav rikete kõrvaldamise aeg, riketest teavitamise kontaktid, varundamise tingimused jmt).

Andmete turvaklass on kolme turvaosaklassi konkreetne kombinatsioon. Nende kõikvõimalike kombinatsioonide arv on 4x4x4, seega on erinevaid turvaklasse 64.

Andmete turvaklassi tähis moodustatakse osaklasside tähistest nende järjestuses K-T-S.

Üks konkreetne andmete turvaklass on näiteks **K2T3S1**. Selline tähis on aluseks andmetele ja muudele infovaradele kohustuslike etalonturvameetmete määramisel. Andmeturbe eesmärkide tagamiseks peavad olema rakendatud turvameetmed, mis vastavad infovara turvaklassile. Turvameetmed valitakse turvaklassile vastavast etalonmeetmete kataloogist konkreetse infovara etalonturbe spetsifikatsioonide alusel.

Andmete turvaklassi määramiseks teostab andmekogu vastutav töötleja infosüsteemides käideldavate andmete turvaanalüüsi määrates turvaosaklassid ülaltoodud kriteeriumide alusel. Ühe andmekogu eri andmetel võib olla erinev turvaklass. Turvaanalüüsis tuleb käsitleda erilise tähelepanuga andmeid, mida käitatakse kas pilveteenuseid kasutades või näiteks täisteenusena mõne teenusepakkuja juures.

Andmete turvaklass ei ole piisav asendamaks andmekogust pakutavate teenuste teenustaseme lepinguid või kokkuleppeid.

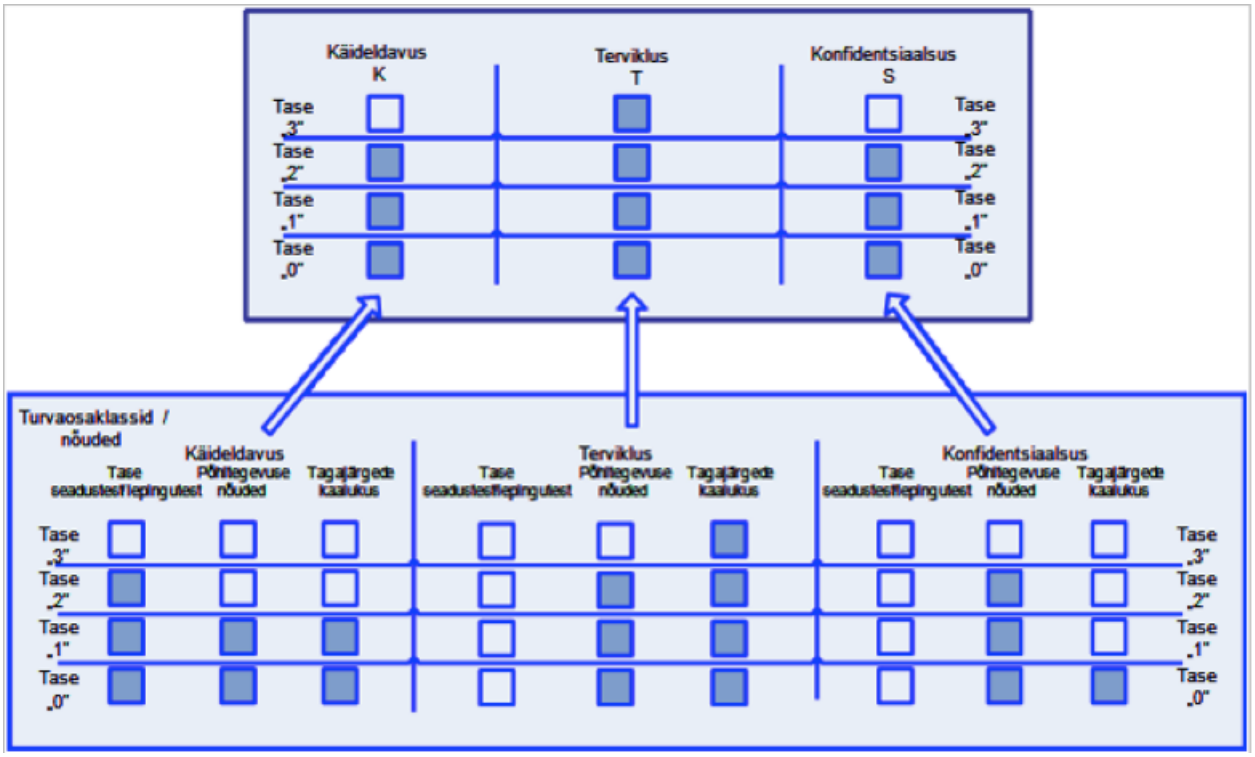
Turvaosaklasside määramisel tuleb arvestada järgmist tüüpi nõuetega (vt. joonis 1 lk 12):

- **Seadustest ja lepingutest tulenevad nõuded**
  Seadustest tulenevad nõuded nt teabe konfidentsiaalsusele. Kui teave on seadusandluses tunnistatud avalikustamisele kuuluvaks teabeks (nt lähtuvalt avaliku teabe seadusest), siis tuleks määrata konfidentsiaalsuse turvaosaklassiks S0. Kui teave on seaduse alusel tunnistatud vastava tasemega juurdepääsupiiranguga teabeks, siis tuleks sellele vastavalt nõuetele määrata konfidentsiaalsuse turvaosaklass S1, S2 või S3. Delikaatsete isikuandmete töötlemisel tuleks määrata teabe konfidentsiaalsuse turvaosaklassiks vähemalt S2.
  Lepingutest tuleb lähtuda juhul kui nendest tulenevad kohustused andmete käideldavusele, terviklusele ja/või konfidentsiaalsusele. Kui näiteks riigiasutus tarbib teise riigiasutuse poolt pakutavaid teenuseid ja nende vahel on sõlmitud leping, mis määrab eraldi nõuded andmete käideldavusele, terviklusele ja konfidentsiaValsusele, siis tuleb turvaosaklasside määramisel arvestada nimetatud nõuete ja kohustustega.

- **Põhitegevuse (või äritegevuse) protsessidest tulenevad nõuded**
  Põhitegevusest võivad tuleneda konkreetsed nõuded pakutavatele IT-teenustele ning need määravad ka nõuded andmete käideldavuse, terviklusele ja konfidentsiaalsusele. Kui asutuse teenindusbürood peavad teenindama kodanikke nt vahemikus E–R 09.00–18.00, siis nendel aegadel peavad toimima IT-süsteemid ja peab olema tagatud andmete käideldavus.

- **Tagajärgede kaalukuse hindamine**
  Tagajärgede kaalukus tähendab turvaintsidendist tekkivate kahjude hindamist. Kahjusid võib hinnata neljatasemelisel skaalal:

  R0 – turvaintsidendiga (st info käideldavuse ja/või konfidentsiaalsuse ja/või tervikluse nõuete mittetäitmisega) ei kaasne märkimisväärseid kahjusid;
  R1 – kaasnevad vähe olulised kahjud, turvaintsident (st info käideldavuse ja/või konfidentsiaalsuse ja/või tervikluse nõuete mittetäitmine) põhjustab tõenäoliselt märkimisväärseid takistusi asutuse funktsiooni täitmisele või märkimisväärseid rahalisi kaotusi;
  R2 – kaasnevad olulised kahjud, turvaintsident (st info käideldavuse ja/või konfidentsiaalsuse ja/või tervikluse nõuete mittetäitmine) põhjustab tõenäoliselt olulise takistuse asutuse funktsiooni täitmisele või ohtu inimeste tervisele või keskkonnasaaste ohtu või olulisi rahalisi kaotusi;
  R3 – kaasnevad väga olulised (missioonikriitilised) kahjud, turvaintsident (st info käideldavuse ja/või konfidentsiaalsuse ja/või tervikluse nõuete mittetäitmine) põhjustab tõenäoliselt asutuse funktsiooni täitmatajätmise või märkimisväärseid häireid riigikorralduses või ohtu inimelule või keskkonnasaastet või väga olulisi rahalisi kaotusi.



Joonis 1. *Turvaosaklassid ja turvaosaklasside määramise nõuded*

Kui eelnevalt nimetatud nõuded määravad erinevad tasemed, siis tuleb turvaosaklassi määramisel lähtuda kõrgeimast tasemest.

Näiteks, tervikluse turvaosaklassi korral seadustes/lepingutest ei tulene nõudeid, põhitegevuse nõuded määravad taseme „2" ja tagajärgede kaalukus määrab taseme „3", siis lähtudes eelnevast määratakse turvaosaklassiks T3.

Turvaanalüüsi süstemaatiliseks teostamiseks ja dokumenteerimiseks kasutatakse infosüsteemide spetsifikatsioone, mis koostati infosüsteemide analüüsi tulemusena (jaotis 2.1) ning, millesse märgitakse andmete turvaklassid. Turvaanalüüsi käigus vaadatakse läbi kõik spetsifitseeritud infosüsteemid. Andmete turvaanalüüsi teostab andmekogu vastutav töötleja. .

2.4 Muude infovarade turvaklassi määramine

Kui andmete turvaklassid on määratud, määratakse muude infovarade turvaklassid, alustades kõige kõrgemate turvaklassidega andmeid käitlevatest infosüsteemidest.

Järgmisena vaadatakse kõiki süsteemiga seotud infovarasid (sh. toetavad ja autonoomsed varad) ja hinnates nende tähtsust kõrgeima turvaklassiga andmekogude seisukohalt, alljärgnevas tabelis oleval skaalal.

Vara roll	**Kriteerium**
Tähtis	Ilma nimetatud varata ei saa andmekogu toimida ja see vara on otseselt vajalik andmekogu toimimiseks ja/või muude vahenditega saab andmekogu toimida suhteliselt lühikest aega.

Vähetähtis	Andmekogu saab toimida ja/või töid/teenuseid/funktsioone saab ka täita muul viisil.

Kui vara osutub kõrge turvaklassiga andmekogu jaoks tähtsaks, tuleb talle määrata samasugune turvaklass, muul juhul võib klass olla ühe taseme võrra madalam. Turvaosaklassi võib alandada ainult juhul, kui see ei ohusta kogu süsteemi turvalisust ega ole seatud turvalisuse klassiga vastuolus.

Infovarade turvaklassid määrab asutuse infotehnoloogia eest vastutav spetsialist koos infoturbespetsialistiga.

Töö käigus tuleb hoolikalt jälgida süsteemidevahelisi seoseid, hoolitsedes selle eest, et oluliste infosüsteemidega seotud muude süsteemide liiga nõrk turve ei ohustaks oluliste süsteemide turvalisust. Kui asutuse struktuur, ruumid, tehniline taristu ja tingimused võimaldavad kulude kokkuhoiuks kasutada tsoneerimist erinevate ISKE klasside osas, siis võib seda kasutada. Infovarade toetusastme määramisel tuleb arvestada ohte ja riske, mis võivad tuleneda vara turbeastme alandamisest ning kas asutus on valmis neid riske aktsepteerima.

Näiteid vara turvaklassi määramistest

Kui andmekogu turbeaste on H ja H turbeaste tuleneb käideldavusest, siis on enamikel juhtudel mõistlik määrata kõrged käideldavuse nõuded ka kõigile andmekogu käideldavust tagavatele varadele, st rakendus, andmebaas, operatsioonisüsteem, server, võrguseadmed, tulemüür, serveriruum, kaablid ja töökohad, mis vajavad kõrget käideldavust andmete käitlemise mõttes. Turbeastet on mõistlik alandada näiteks järgmiste toetavate varade jaoks: kontoriruumid, koosoleku saalid ja need tööjaamad, mille kasutajad ei pea pääsema andmekogule ligi H käideldavuse tasemel. Jälgima peab ka seda, et kui andmekogu konfidentsiaalsust on vaja tagada S2 tasemel, siis tööjaama turvaklass, kus andmeid töödeldakse, peab olema sama. Lisaks, kui süsteemi arhitektuur seda lubab, võib andmekogu teenustele määrata ka eraldi turvaklassid.

Kui aga H turbeaste tuleneb andmete konfidentsiaalsuses, siis ei pea tingimata H turbeastet määrama nt kaabeldusele ja seda juhul kui kaablis on andmed krüpteeritud kujul.

Muudest infosüsteemidest sõltumatute infosüsteemide puhul vaadeldakse kõigepealt andmete turvaklassi. Kui see on suhteliselt madal, hinnatakse kogu süsteemi tähtsust; selleks võib samuti kasutada ülaltoodud tabelit. Kui süsteem tervikuna osutub hetkel käideldavatest andmetest olulisemaks (näiteks maksumust arvestades), antakse talle vastavalt kõrgem turvaklass. Infosüsteemile määratud turvaklass määratakse ka temaga otseselt seotud infovaradele.

Hetkel mitte kasutusel olevate infovarade puhul (veel käiku andmata toite- või sideliinid, testimisel olev tarkvara jms) tuleb hindamisel arvestada nende tulevast otstarvet.

3. Nõutava turbeastme ja turvameetmestiku määramine

3.1 Turbeastme määramine turvaklassi järgi

Turvaklassi järgi määratakse kõigi eelnevalt spetsifitseeritud (jaotis 2.1.2) ja turvaanalüüsi tulemusena turvaklassi saanud infovarade nõutav turbeaste.

Turvaklasse ehk kolme turvaosaklassi erinevaid kombinatsioone on kokku 64.

Alljärgnev tabel seab nende 64 kombinatsiooniga vastavusse kolm etalonturbe astet:

- **madal turbeaste (L),**
- **keskmine turbeaste (M),**
- **kõrge turbeaste (H).**

		K0	K1	K2	K3
T0	S0	L	L	M	H
	S1	L	L	M	H
	S2	M	M	M	H
	S3	H	H	H	H
T1	S0	L	L	M	H
	S1	L	L	M	H
	S2	M	M	M	H
	S3	H	H	H	H
T2	S0	M	M	M	H
	S1	M	M	M	H
	S2	M	M	M	H
	S3	H	H	H	H
T3	S0	H	H	H	H
	S1	H	H	H	H
	S2	H	H	H	H
	S3	H	H	H	H

Iga infovara turvaklassi osaklasside järgi leitakse sellest tabelist vastava vara jaoks nõutav etalonturbeaste ja märgitakse see infovarade spetsifikatsiooni (jaotis 2.1.2).

Seejärel leitakse tüüpmoodulite kataloogist M sellele infovarale vastava tüüpmooduli tähis ja märgitakse see infovarade spetsifikatsiooni (jaotis 2.1.2).

Kui kõikide spetsifitseeritud varade turbeastmed on määratud, sõltub edasine tegevus saadud turbeastmete arvust:

- kui kõikidel varadel on ühesugune turbeaste, võib määrata turvameetmed tüüpmoodulite turvaspetsifikatsioonide ja turvameetmete kataloogi abil;
- kui turbeastmeid on kaks või kolm, tuleb analüüsida võimalust asutuse infoturbe otstarbekaks tsoneerimiseks.

Tsoneerimise otstarbekas korraldamine võib nõuda muudatusi süsteemide funktsioonides ja paigutuses, ruumide funktsioonides jne. Enne lõplikke turvaotsustusi tuleb muudatused kavandada, kinnitada ja plaanida. Optimaalse tsoneerimise huvides võib olla vajalik tõsta mõnede infovarade eelnevalt leitud turbeastet, mõnedel varadel võib seda aga funktsioonide ümberpaigutamise tulemusena langetada.

3.2 Turvaklassita infovarade turbeastme määramine

Jaotises 3.1 on juhised turvaklassiga infovarade, st spetsifitseeritud infovarade nõutava turbeastme määramiseks. Spetsifitseerimisele kuulusid aga ainult andmed, materiaalsed infovarad ja tarkvara. Kaitset vajavad aga ka töökorraldusprotsessid ja muud organisatsioonilised ressursid, ka infoturbe haldus ise sõltub nõutavast turbetasemest.

Kõik sellised spetsifitseerimata varad on kirjeldatud vastavate tüüpmoodulitena kataloogis B, mis kuuluvad peamiselt tüüpmoodulite rühma B1.

Kogu tüüpmoodulite rühmale B1 tuleb määrata kõrgeim jaotises 3.1 määratud turbeaste.

Kui tüüpmoodulite läbivaatusel ilmneb, et spetsifitseerimata on jäänud veel mingeid infovarasid, tuleb uurida nende seoseid juba liigitatud infovaradega ja määrata selle põhjal turbeaste.

3.3 Turvameetmete määramine

Kui kõigi infovarade nõutav turbeaste on määratud, tuleb leida igale infovarale vastavad tüüpmoodulid kataloogist B. Tüüpmoodulite spetsifikatsioonides on ka loetelu rakendamisele kuuluvatest turvameetmetest.

Seejuures tuleb silmas pidada etalonturbe kihilisust. See tähendab, et astme M rakendamiseks tuleb rakendada astme L ja astme M turvameetmed ning astme H rakendamiseks tuleb rakendada astme L, astme M ja astme H turvameetmed.

Kõrgeima kihi meetmed jagunevad

- kohustuslikeks (kataloogi H alamkataloogi HG meetmed) ja
- tingimuslikeks (kataloogi H alamkataloogide HK, HT, HS meetmed).

Tingimuslike meetmete rakendamine sõltub moodulirühma kõrgeima tasemega turvaosaklassi(de)st:

- K3 korral tuleb rakendada kõik alumises tabelis loetletud HK-meetmed

- T3 korral tuleb rakendada kõik alumises tabelis loetletud HT-meetmed
- S3 korral tuleb rakendada kõik alumises tabelis loetletud HS-meetmed

Turvameetmete määramist tuleb alustada moodulirühmaga B1 ja mooduliga B1.0, mis määrab infoturbe halduse meetmed.

Seejärel tuleb määrata turvameetmed kõrgeima turbeastmega infovaradele ning saavutada nende kiire kihthaaval rakendamine.

Edasine varade käsitlemise järjestus pole eriti oluline ja võib sõltuda konkreetsetest tingimustest.

Kui kõik turvameetmed on määratud, tuleb kontrollida kõigi moodulispetsifikatsiooni ohtude veeru ja ISKE ohtude kataloogi G andmetega võrreldes tegelikku ohusituatsiooni võimalike kataloogis puuduvate ohtude avastamiseks. Kui selliseid uusi ohte ilmneb, tuleb uurida, kas määratud etalonmeetmed on nende tõrjeks piisavad või tuleb rakendada veel mingeid lisameetmeid.

4 Kasutatud mõisted ja lühendid

Käesolevas seletussõnastikus selgitatakse neid mõisteid ja termineid, mida ei leia http://akit.cyber.ee sõnastikust ega standardist ISO/IEC 27000 „Turbemeetodid, infoturbe halduse süsteemid, ülevaade ja sõnavara“.

Informatsioon ehk **teave** on igasugune teadmine, mis puudutab objekte – näiteks fakte, sündmusi, asju, protsesse või ideid ja millel on teatavas kontekstis eritähendus.

Andmed on informatsiooni taastõlgendatav esitus, mis sobib edastuseks, tõlgenduseks või töötluseks. Informatsioonil iseenesest puudub vorm, see tekib alles esituse ehk andmete kaudu. Andmed on informatsiooni esitus mingil eelnevalt kokkulepitud kujul ja kandjal, näiteks paberdokumendina, digitaalsalvestisena magnetkettal, mikrofilmina, fotona jne.

Andmekogu on riigi, kohaliku omavalitsuse või muu avalik-õigusliku isiku või avalikke ülesandeid täitva eraõigusliku isiku infosüsteemis töödeldavate korrastatud andmete kogum, mis asutatakse ja mida kasutatakse seaduses, selle alusel antud õigusaktis või rahvusvahelises lepingus sätestatud ülesannete täitmiseks.

Andmete turvaanalüüs – Turvaklassi määramiseks sooritatav andmete tähtsuse hindamine ning andmete turvalisuse puudumisest tulenev kahjude hindamine.

Audit on süstemaatiline kontroll etteantud turvaeeskirja sobivuse ja selle järgimise üle. Audit peab olema sõltumatu ja neutraalne.

BSI (Bundesamt für **Sicherheit** in der **Informationstechnik**, Saksamaa Infoturbeamet**)** – Asutus, mis arendab ja haldab ISKE aluseks olevat etalonturbe käsiraamatut *IT-Grundschutzhandbuch*, vt http://www.bsi.bund.de/index.htm.

Digitaalne allkiri on kontrollinformatsioon, mis lisatakse sõnumile või failile, ja mida iseloomustavad järgmised omadused:

- digitaalne allkiri võimaldab selle looja üheselt kindlaks määrata;

- digitaalne allkiri võimaldab kontrollida, kas fail, millele on lisatud digitaalne allkiri, on identne failiga, mis tõepoolest allkirjastati.

Etalonmeetmed – Tüüpsed katalogiseeritud ja valimismetoodikaga varustatud turvameetmed, mille hulgast tehtav valik sõltub turvaklassist ja andmeid töötleva infosüsteemi koostisest.

Etalonturbe astmelisus – ISKE metoodikas on välja toodud kolm astet: "L" – madal, "M" – keskmine, "H" – kõrge.

- "Z" tähistab soovituslikke meetmeid, mis võivad osutuda vajalikeks eelkõige kõrgema turvanõudluse puhul.
- "W" tähistab meetmeid, mille eesmärgiks on aidata mõista ja rakendada teisi turvameetmeid.

Etalonturve – Turvameetmestik, mille rakendamine on vajalik andmete turvalisuse saavutamiseks ja säilitamiseks.

Infosüsteem – Andmeid töötlev, salvestav või edastav tehniline süsteem koos tema normaalseks talituseks vajalike vahendite, ressursside ja protsessidega.

Infoturbe juht – Ettevõtte või asutuse IT-turvaosakonna pädev isik, kes on vastutav kõigi IT-turvaküsimuste eest, osaledes IT-turvaprotsessis ja IT-turvahaldusmeeskonna töös, aidates kaasa IT-turvaeeskirja, IT-turvakontseptsiooni ja teiste dokumentide (nt hädaolukorraks valmisolek) väljatöötamisele ning planeerides ja kontrollides nende rakendamist.

ISKE – Infosüsteemide kolmeastmelise etalonturbe süsteem.

ISKE koordinaator – Roll, mille täitja ülesanne on kogu ISKE juurutamise koordineerimine ja juhtimine asutuses.

ISKE rakendamise kord – ISKE rakendusjuhendi jaotistes 1–3 esitatud protseduurid ja meetodid ISKE rakendamiseks.

IT-etalonturbe analüüs – IT-etalonturbe analüüsi hulka kuulub modelleerimine koos vajalike turvameetmete väljaselgitamisega ja põhiturvakontroll, mille käigus võrreldakse ettevõttes või asutuses hetkel kasutuses olevat turvameetmete rakendamist sellega, milline see peaks olema.

IT-etalonturve – Mõiste „IT-etalonturve“ tähistab infoturbe haldussüsteemi ülesehitamise metoodikat, samuti IT varade kindlustamist standardturvameetmetega. Lisaks tähistatakse selle mõistega ka seisukorda, mille korral on normaalse kaitsevajadusega IT-süsteemidele vajalik rakendada standardturvameetmeid.

IT-Grundschutzhandbuch – ISKE aluseks olev BSI poolt publitseeritav etalonturbe käsiraamat (https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/itgrundschutzkataloge_node.html).

Käitavad infovarad – Varad, mis otseselt on vajalikud andmekogu töö tagamiseks (nt rakendus, andmebaas, server jmt);

Meetmete kataloog – IT-etalonturbe kataloogides soovitatakse igas moodulis sobivat meedet, mis on kataloogideks kokkuvõetuna liigendatud infrastruktuuriks, organisatsiooniks, personaliks, riistvaraks/tarkvaraks, kommunikatsiooniks ja valmisolekuks hädaolukorras.

Modelleerimine – Vastavalt IT-etalonturbele mõistetakse modelleerimise all ettevõtte või asutuse IT-varade kaardistamist lähtudes IT-etalonturbe kataloogides sisalduvatest moodulitest. Vastavalt IT-etalonturbe kataloogi ptk 2.2 sisaldab iga moodul viidet, millisel puhul seda rakendada ja milliseid eeldusi tuleks seejuures silmas pidada.

Moodul – Mõistet kasutatakse IT-etalonturbe kataloogis sisalduvate soovituste struktureerimiseks. Moodulid on ühe tasandi (nt IT-süsteemid, võrgud) üksused. Neis kirjeldatakse osalt tehnilisi komponente (nt kaabeldus), osalt organisatoorseid meetmeid (nt hädaolukorraks valmisoleku kontseptsioon) ja erilisi rakendusvorme (nt kodune töökoht). Igas moodulis kirjeldatakse kindlat IT-komponenti ja nimetatakse ohud, samuti antakse soovitusi organisatoorsete ja tehniliste turvameetmete rakendamiseks.

Pilveteenus – veebipõhine ühiskasutuses IT haldus- või rakendusteenus. Pilveteenuse puhul jagavad erinevad infosüsteemid samu ressursse või kasutavad erinevad asutused ühte veebipõhist infosüsteemi. Täpsem ning üldkasutavav pilveteenuse definitsioon on toodud NIST-i juhendis 800-145, http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-145.pdf.

RIA – Riigi Infosüsteemi Amet

RIHA – Riigi infosüsteemide haldussüsteem, vt. https://riha.eesti.ee

Toetavad infovarad – Varad, mis on vajalikud andmekogude ja/või nendega seotud käitavate varade toimimise tagamiseks, kuid mis ise ei ole otseselt vajalikud andmete töötlemiseks ega ka andmekogust andmete kättesaadavaks tegemisega (nt varundusserver, võrguseadmed,tulemüür vmt).

Turbeaste – Infoturbe näitaja, mis määratakse turvaklassi põhjal vastavalt ISKE rakendusjuhendis antud juhistele. ISKEs on kolm turbeastet L – madal, M – keskmine ja H – kõrge.

Turvaintsident – Sündmus ja/või sündmused, millega kaasneb andmete ja/või muude infovarade käideldavuse, tervikluse ja/või konfidentsiaalsuse kadu ja/või tekib oluline oht andmete käideldavuse, tervikluse ja/või konfidentsiaalsuse kao tekkeks.

Turvaklass – Andmete tähtsusest tulenev andmete nõutav turvalisuse tase, väljendatuna neljaastmelisel skaalal ning kolmekomponendilisena, st kolme turvaosaklassi ühendina. Andmete turvaklassi tähis moodustatakse turvaosaklasside tähistest nende järjestuses K-T-S, nt K2T3S1.

Turvaosaklass – Andmete tähtsusest tulenev infoturbe eesmärgi saavutamise nõutav tase väljendatuna neljaastmelisel skaalal. Kolmest infoturbe eesmärgist tuleneb kolm turvaosaklassi. Turvaosaklassi tähis koosneb turvaeesmärgi tähisest (nt K, T, S) ja turvataseme väärtusest (nt 0,1,2,3), nt K2.

Turvameede – Organisatsioonilised toimingud ja vahendid, tehnilised protsessid ja tehniliste vahendite rakendamine andmete ja infosüsteemide andmete turvalisuse saavutamiseks ja säilitamiseks Turvameetmeks (lühidalt meetmeks) nimetatakse kõiki tegevusi, mille

eesmärgiks on turvariskide vähendamine ja nende ennetamine. Seda saab teha nii organisatoorsete kui ka inim-, tehniliste- või infrastruktuure puudutavate turvameetmete abil. Sünonüümidena kasutatakse ka mõisteid „turvaabinõu“ või „kaitsemeede“. Kasutatakse ka inglisekeelseid mõisteid *"safeguard"*, *"security measure"* või *"measure"*. Ingliskeelses keeleruumis kasutatakse *"safeguard"* kõrval tihti ka mõistet *"control"*.

5 Lisateabe viited

ISKE põhineb Saksamaa Infoturbeameti (Bundesamt für Sicherheit in der Informationstechnik, BSI) poolt publitseeritaval IT-etalonturbe käsiraamatul (*IT Grundschutzhandbuch'il*). BSI süsteem on väga ulatuslikult ja detailselt dokumenteeritud ning seda täiendatakse regulaarselt kord aastas. Nende moodulite kirjelduste, ohtude ja turvameetmete puhul, kus täpsustavad märksõnad ja lisaseletused puuduvad või osutuvad ebapiisavaks, on soovitatav hankida lisateavet BSI käsiraamatust.

BSI koduleheküljelt on saadaval järgmised materjalid:

- **Inglisekeelne juhend *IT Baseline Protection Manual*** (2013. aasta versioon): https://download.gsb.bund.de/BSI/ITGSKEN/IT-GSK-13-EL-en-all_v940.pdf
- **Saksakeelne juhend *IT-Grundschutzhandbuch*** (2016. aasta versioon): https://download.gsb.bund.de/BSI/ITGSK/IT-Grundschutz-Kataloge_2016_EL15_DE.pdf

Turbehalduse korraldamisel võib mõningaid kasulikke juhiseid leida järgmistest standarditest:

- EVS-ISO/IEC 27002. Infotehnoloogia. Turbemeetodid. Infoturbe halduse tegevusjuhis
- EVS-ISO/IEC 27001. Infotehnoloogia. Turbemeetodid. Infoturbe halduse süsteemid. Nõuded.

LISA 1 – Muudatused ISKE rakendusjuhendi versioonis 8.00

1.1 Uuendamine ja ümbertöötamine

ISKE rakendusjuhendi versioonis 8.00 on katalooge, turvaspetsifikatsioone uuendatud ja täiendatud BSI etalonsüsteemi (detsember 2009, september 2011, 2014 ja 2015) saksakeelsete versioonide põhjal vastavalt BSI alussüsteemis tehtud muudatustele ja täiendustele. Uuena on lisandunud pilvetehnoloogiat käsitlev moodul B 1.17.

ISKE kataloogide paremaks töötlemiseks on rakendajatele loodud veebipõhine rakendus ISKE Portaal, aadressil iske.ria.ee. ISKE Portaal sisaldab ametlikku kinnitatud ISKE kataloogide versiooni 8.00 ja kataloogide sisu parema ajakohasuse tagamiseks hakkavad sellele lisanduma täiendavad vaheversioonid (formaadis 8.01, 8.02, …), kuni on avaldatud uus ametlik versioon. Vaheversioonid sisaldavad olulisi turbevajaduste täienemisest tingitud muudatusi ja täiendusi. ISKE Portaal sisaldab avalikku vaadet, mis on kõigile nähtav ja autenditud vaadet, mille kaudu saavad rakendajad kommenteerida kataloogide sisu ning teha muudatus- ja täiendusettepanekuid.

ISKE kataloogide versioonis 8.00 on tõlgitud originaaljuhendist kõigi moodulite kirjeldused ning kõik olulisemad meetmed ja nende selgitused. Lisaks tõlkimisele on meetmeid vastavalt Eesti oludele kohandatud.

Kui peaks leiduma veel meetmeid ISKE turbeastmetes „L" ja „M", millel puudub käesolevas ISKE rakendusjuhendis piisav selgitus, siis neid meetmeid ei ole kohustus rakendada.

Kõik parandusettepanekud ja info ebatäpsuste kohta palume saata iske@ria.ee.

1.2 Muudatused moodulites

1.2.1 Lisandunud moodulid

- B 1.17 – Pilvteenuse kasutamine
- B 5.24 – Veebiteenused
- B 5.25 – Rakendused

1.2.2 Uuendatud moodulid

- B 1.11 – Väljasttellimine (Outsourcing)
- B 1.13 – Infoturbe teadlikkus ja -koolitus
- B 2.1 – Hooned
- B 2.2 – Elektrotehniline kaabeldus
- B 3.101 – Server
- B 3.109 – Windows Server 2008
- B 3.201 – Klient
- B 3.202 – Autonoomne IT-süsteem
- B 3.208 – Interneti-PC
- B 3.210 – Klient Windows Vista all
- B 3.212 Windows 7-ga töötav klientsüsteem

- B 3.303 – Salvestisüsteemid ja salvestivõrgud
- B 3.404 – Mobiiltelefon
- B 3.405 – Nutitelefonid, tahvel- ja pihuarvutid
- B 5.4 – Veebiserver
- B 5.21 – Veebirakendused
- B 5.22 – Logimine

Ülal nimetatud moodulite sisu on ISKEs uuendatud.

1.2.3 Välja jäetud moodulid

- B 3.108 Windows Server 2003
- B 3.209 Klient Windows XP all

1.3 Muudatused meetmetes

1.3.1 Lisandunud meetmed

- M 2.525 – M 2.544
- M 2.546 – M 2.558
- M 2.E22
- M 3.26
- M 3.92 – M 3.96
- M 4.447 – M 4.459
- M 4.462 – M 4.469
- M 5.175 – M 5.177
- M 6.154 – M 6.159
- HG.77 – HG.81
- HK.38

1.3.2 Uuendatud meetmed

- M 1.5
- M 1.33
- M 1.80
- M 2.8
- M 2.13
- M 2.31
- M 2.34 – M 2.35
- M 2.40

- M 2.42
- M 2.64
- M 2.109
- M 2.110
- M 2.165
- M 2.167
- M 2.188 – M 2.190
- M 2.198
- M 2.218
- M 2.273
- M 2.303 – M 2.307
- M 2.312
- M 2.324 – M 2.327
- M 2.330
- M 2.351
- M 2.354 – M 2.355
- M 2.357
- M 2.360 – M 2.362
- M 2.384
- M 2.477
- M 2.486
- M 2.488
- M 3.5
- M 3.46 – M 3.49
- M 3.51
- M 3.72
- M 4.3
- M 4.31
- M 4.56
- M 4.78
- M 4.114 – M 4.115
- M 4.225
- M 4.228

- M 4.230 – M 4.232
- M 4.243 – M 4.249
- M 4.255
- M 4.275
- M 4.310
- M 4.318
- M 4.326
- M 4.344
- M 4.381
- M 4.393 – M 4.395
- M 4.397
- M 4.400
- M 4.405
- M 4.410
- M 4.419
- M 4.422 – M 4.424
- M 4.427
- M 5.14
- M 5.66
- M 5.78 – M 5.81
- M 5.89 – M 5.90
- M 5.121
- M 5.123
- M 5.130
- M 5.150
- M 5.168
- M 5.173
- M 6.72
- M 6.78
- M 6.95
- M 6.98

1.3.3 Välja jäetud meetmed

- M 2.247 – M 2.249

- M 2.328 – M 2.329
- M 3.28
- M 3.31 – M 3.32
- M 4.57
- M 4.148
- M 4.161 – M 4.163
- M 4.165 – M 4.166
- M 4.200z
- M 4.278z
- M 5.132
- M 6.42
- M 6.82
- HS.69

1.4 Muudatused ohtudes

1.4.1 Lisandunud ohud

- G 2.181 – G 2.183
- G 2.185 – G 2.199
- G 2.200 – G 2.201
- G 3.119 – G 2.123
- G 4.94 – G 4.99
- G 5.179 – G 5.194
- G 5.E8
- G 5.E9
- G 5.E10

1.4.2 Uuendatud ohud

- G 1.15
- G 1.19
- G 2.2
- G 2.4
- G 2.7

- G 2.26
- G 2.84 – G 2.86
- G 2.90
- G 2.93
- G 2.105
- G 2.109
- G 2.143
- G 2.158 – G 2.159
- G 3.3
- G 3.9
- G 3.43 – G 3.45
- G 3.76 – G 3.77
- G 4.10
- G 4.22
- G 4.32
- G 4.41 – G 4.43
- G 4.52
- G 4.84 – G 4.85
- G 4. 87
- G 5.1 – G 5.2
- G 5.4
- G 5.7 – G 5.9
- G 5.18
- G 5.20
- G 5.22 – G 5.23
- G 5.27 – G 5.28
- G 5.57
- G 5.87
- G 5.89
- G 5.94 – G 5.99
- G 5.123 – G 5.126
- G 5.130
- G 5.165

- G 5.167 – G 5.169
- G 5.172 – G 5.173

1.4.3 Välja jäetud ohud

- G 2.91
- G 2.92
- G 2.95
- G 3.60
- G 3.61
- G 3.81
- G 4.54
- G 4.55
- G 5.52
- G 5.79