TALLINNA ÜLIKOOL
Informaatika Instituut

Riskihaldus riigisaladust töötlevates infosüsteemides

Magistritöö

Autor: Sven Juhkam
Juhendaja: Priit Parmakson

Autor: ..... „ ..... „ 2009
Juhendaja: ..... „ ..... „ 2009
Instituudi direktor: ..... „ ..... „ 2009

TALLINN 2009

Autorideklaratsioon

Deklareerin, et käesolev magistritöö on minu töö tulemus ja seda ei ole kellegi teise poolt varem kaitsmisele esitatud.

.....	.....
(kuupäev)	(magistritöö kaitsja allkiri)

SISUKORD

Annotatsioon 6
Abstract....7
SISSEJUHATUS....8
Aktuaalsus....8
Eesmärk....9
Probleemi kirjeldus....10
PEATÜKK 1. RIIGISALADUST TÖÖTLEVAD INFOSÜSTEEMID....11
1.1 Eesmärk....11
1.2 Mõisted....11
1.3 Riigisaladuse mõiste....13
1.4 Riigisaladust töötlevad infosüsteemid....15
PEATÜKK 2. RISKIHALDUSEST ÜLDISELT 17
2.1 Riiklikud institutsioonid....17
2.1.1 ENISA....17
2.1.2 Saksamaa BSI 18
2.1.3 NIST....19
2.1.4 OGC - The Office of Government Commerce....20
2.1.5 DSD- Austraalia infoturbe organisatsioon....20
2.1.6 Prantsusmaa infoturbeamet 21
2.1.7 Eesti infoturbeasutused....21
2.2 Rahvusvahelised standardid....22
2.2.1 ISO 13335 Infoturbe halduse suunised....22
2.2.2 ISO/IEC 27002 Infotehnoloogia. Infoturbe halduse praktilised juhised....23
2.2.3 EVS-ISO TR 13569 Pangandus ja sellega seotud rahandusteenused....24
2.2.4 ISO/IEC 15 408 Common Criteria....24
2.2.5 Eurostandardid....25
2.3 Riskianalüüsi programmid....26
2.3.1 Valiku kriteeriumid....26
2.3.2 CRAMM....28
2.3.3 RiskWatch....28
2.3.4 EBIOS....29
2.3.5 GSTOOL....29

2.3.6 ISKE....30
2.3.7 Eesti Ühispanga etalonturbesüsteem (EÜE)....30
2.3.8 Sobiv alussüsteem....31
PEATÜKK 3. RISKIHALDUSE PROTSESS....33
3.1 Eesmärk....33
3.2 Mõisted....33
3.3.1 Riskianalüüs ja riskihaldus infosüsteemi elutsükli jooksul....37
3.3.2 Riskianalüüsi meeskond....38
3.3.3 Riskianalüüsi protsess....39
3.3.5 Materiaalsete ja infovarade väärtuse hindamine....40
3.3.6 Ohud ja haavatavused....41
3.3.7 Olemasolevad vastumeetmed....41
3.3.8 Soovitatavad uued vastumeetmed....41
3.3.9 Riskianalüüsi protsessi kokkuvõte....42
3.4 Riskianalüüsi meetodid....43
3.4.1 Kvantitatiivne riskianalüüs....43
3.4.2 Kvalitatiivne riskianalüüs....44
3.4.3 Jäme riskianalüüs....45
3.4.4 Detailne riskianalüüs....46
3.4.5 Eeskujul baseeruv riskianalüüs – Etalonturve....47
3.4.6 Segametoodika....49
3.4.7 Kogemustel baseeruv riskianalüüs....49
3.4.8 Kokkuvõte erinevatest riskianalüüsi meetoditest....50
PEATÜKK 4. ETALONTURBEMEETODI ISKE ANALÜÜS....52
4.1 Eesmärk....52
4.2 Etalonturbe olemus....53
4.3 Astmeline etalonturve....53
4.4 Turvameetmete liigitus ISKEs....54
4.5 Etalonmeetmestiku halduse korraldamine....55
4.6 Turvameetmete analüüs....55
4.6.1 Paroolile esitatavad nõuded....55
4.6.2 Teabe kustutamine....57
4.6.3 Riistvara terviklikus....57
4.6.4 Logid....58

4.6.5 Teabele juurdepääs....60
4.7 Peatüki kokkuvõte....62
KOKKUVÕTE....63
KASUTATUD KIRJANDUS....65
LISA 1. ISKE RS TURVAMEETMED....69
LISA 2. ELEKTROONILISE TEABETURBE VÄLJAVÕTE....74
LISA 3. RIIGISALADUSE KAITSE JUHEND....78

Annotatsioon

Käesoleva magistritöö "Riskihaldus riigisaladust töötlevates infosüsteemides" üldeesmärgiks on anda ülevaade riskihaldusest ja selle läbiviimise etappidest ning tutvustada infoturbega seotud mõisteid, standardeid ja asutusi, samuti teha ülevaade olemasolevatest infosüsteemides rakendatavatest riskianalüüsi meetoditest, võrrelda erinevaid riskianalüüsi meetodeid ja riskianalüüsi programme. Analüüsida erinevaid riskianalüüsi meetodeid, standardeid ja valida välja sobiv riskianalüüsi meetod ja programm, mis sobiks riigisaladust töötlevatele infosüsteemidele. Lõpptulemuseks annab magistritöö riigisaladuse infosüsteemi valdajatele ülevaate riskihaldusest. Magistritöö on kokku pandud seadusandlust, erinevaid standardeid, infoturbe käsiraamatuid ja rahvusvaheliste organisatsioonide juhendeid järgides.

Abstract

The general objectives of the Master's Thesis "Risk Management in Classified Information Systems" are to present an overview on the risk management and on the stages for its realisation and to present definitions, standards and agencies related to information security. In this thesis paper also an overview is given on existing methods that are implemented in different information systems, comparing the methods of risk assessment and automatic risk assessment programs.

The final goal of this Master's Thesis is to analyse different risk assessment methods and standards with the purpose to find the best suitable risk assessment method and the automatic program for information systems processing the classified information. The output of this paper is risk management overview for professionals who manage the information systems processing the classified information. The Master's Thesis follows Estonian legislation, existing standards and different manuals on security and other similar manuals of international organisations.

SISSEJUHATUS

Infosüsteem on tänapäeval hädavajalik enamikus organisatsioonides. Organisatsioonid, kes kasutavad üha enam uusi infosüsteeme, jäävad nendest üha rohkem sõltuvusse s.t. kui mõne infosüsteemi rakendus ei toimi pikemat aega, võib peatuda kogu organisatsiooni tegevus. Sellepärast tuleb juba organisatsiooni infosüsteemi projekteerimise ajal arvestada infosüsteemile ja tema rakendustele mõjuda võivate ohtudega ja turvapoliitika väljatöötamisel peab kaasnevaid ohte ja riske arvestama. Organisatsiooni põhjalikult välja töötatud turvapoliitika ja turvameetmete rakendamisega saab vähendada enamikku riske ning ära hoida kahjusid organisatsiooni varadele ja informatsioonile. Infosüsteemideta ei saa läbi ka riigiasutused, kes töötlevad riigisaladust.

Infosüsteemi mõjutavaid ohte ja riske saab kindlaks teha süsteemse riskihalduse meetodiga. Hetkel kasutatakse rohkem kogemustel baseeruvaid, isekujunenud meetodeid, mida on siis erinevatesse standarditesse-juhenditesse kirjutatud ja seeläbi korrastatud. Ühtne ja selgepiiriline metoodika tihti puudub, on palju erinevaid lähenemisi, millede seast sobiva valimine on raske. Samuti on vähegi suuremate infosüsteemide riskianalüüs väga töömahukas, ohud muutuvad ja täienevad, avastatakse uusi nõrkusi ja turvameetmeid lisandub pidevalt – kõigi nendega arengutega on vaja kaasas käia.

Infoturbele spetsialiseerunud töötajaid on ainult väga vähestes asutustes, eeskätt erasektoris. Infoturbega tegelevad enamasti süsteemiadministraatorid, kellest suur osa on erihariduseta praktikud. Mõningat edu on saavutatud tehniliste turvameetmete alal, näiteks tulemüüride ja VPNvõrkude suhteliselt ulatusliku kasutamise näol. Halvasti tuntakse ja rakendatakse aga organisatsioonilisi meetmeid, sealhulgas kas või nendesamade tehniliste meetmete turvapoliitikate ja haldusprotseduuride osas. Seda võimendab tehniliste spetsialistide negatiivne hoiak organisatsiooniliste meetmete suhtes.

Aktuaalsus

Ametnikel, kes vastutavad oma asutuses riigisaladust töötlevat infosüsteemide turvalisuse eest, puudub ühtne meetod, kuidas viia läbi riskianalüüsi oma infosüsteemile. Tihti peale puudub neil

ülevaade infoturbe korraldusest ja nad ei ole varem kokkupuutunud riskihalduse ja -analüüsiga.

Kuna riigisaladust töötlevate infosüsteemide riskide haldus ja riskide analüüs on küllaltki tundlik teema, siis on ka raske leida konkreetseid näiteid tehtud riskianalüüsidest. Seepärast on ülevaate saamine erinevate riikite infoturbeasutustest, standarditest, riskianalüüsi meetoditest, neist toetavatest programmidest ja tegelikult üleskerkivatest probleemidest vajalik, samuti nagu nende meetodite rakendamine praktikas.

Eesmärk

Käesoleva magistritöö üldeesmärgiks on anda ülevaade riskihaldusest ja selle läbiviimise etappidest ning tutvustada infoturbega seotud mõisteid, standardeid ja asutusi, samuti teha ülevaade olemasolevatest infosüsteemides rakendatavatest riskianalüüsi meetoditest, võrrelda erinevaid riskianalüüsi meetodeid ja riskianalüüsi programme. Analüüsida erinevaid riskianalüüsi meetodeid, standardeid ja valida välja sobiv riskianalüüsi meetod ja programm, mis sobiks riigisaladust töötlevatele infosüsteemidele.

Magistritöö annab ülevaate infosüsteemide turvalisusega tegelevatele ametnikele riskihaldusest üldiselt. See vajadus on tekkinud sellest, et riigisaladust töötleva infosüsteemi turvalisuse eest vastutavatel ametnikel ei ole kogemusi riskihalduse korraldamiseks ja samas ei ole võimalik või on raskendatud sellise teenuse sisseostmine erafirmadelt.

Töös käsitletakse püstitatud küsimust ratsionaalse otsustusprotsessi mudelile (ingl. k. *Rational Decision-Making Model*) tuginedes. Ratsionaalse otsustusprotsessi mudel on organisatsiooniteoorias hästituntud samm-sammuline meetod probleemi süstemaatiliseks uurimiseks ja lahendamiseks.
Mudelist on mitmeid versioone, tavaliselt on sammude hulgas:

1. probleemi määratlemine;
2. kõigi võimalike lahendusvariantide genereerimine;
3. lahendusvariantide objektiivsete hindamiskriteeriumite genereerimine;
4. parima lahenduse väljaselgitamine hindamiskriteeriumite abil.

Probleemi kirjeldus

Riigisaladust töötlevatele infosüsteemidele on vastavalt „Riigisaladuse ja salastatud välisteabe seadusele“ kohustuslik, et enne selle kasutusele võtmist saadakse akrediteering st et riigisaladust töötlevat infosüsteemi hinnatakse elektroonilise teabeturbe nõuetele vastavuse seisukohast.

Töötlussüsteemi omanik peab selleks esitama akrediteerimisasutusele turvanõuete loetelu, mille üheks osaks on ülevaade riskianalüüsi tulemustest. Samas puuduvad konkreetsed juhendid ja sobiv meetod, kuidas organisatsioonis riigisaladust töötlevatele infosüsteemidele riskihaldust korraldada ühtse meetodi järgi, mis oleks arusaadav riigisaladus töötleva infosüsteemi valdajale. Samuti peaks riskianalüüsi käigus pöörama tähelepanu nõuetele, mis tulenevad seadusest ja selle põhjal väljaantud määrustest. Siiani on riskianalüüsiks kasutatud erinevaid meetodeid ja nende analüüside hindamine on raske ning tihtipeale ei ole analüüsis tähelepanu pööratud kõigile nõuetele, mis tulenevad seadusest ja määrustest. Organisatsioonides puudub professionaalne personal, kes suudab läbi viia riskianalüüsi kasutades keerulisi ja töömahukaid meetodeid.

Antud magistritöö peaks huvi pakkuma kõikidele IT turvalisuse valdkonnas tegutsevatele spetsialistidele, kelle peamiseks tööülesandeks on infoturbe korraldamine asutuses.

PEATÜKK 1. RIIGISALADUST TÖÖTLEVAD INFOSÜSTEEMID

1.1 Eesmärk

Peatüki eesmärgiks on anda ülevaade riigisaladuse seaduses ja selle alusel väljaantud määrustes kasutatavatest mõistetest, selgitada, mis on riigisaladus ja mis on salastatud välisteave. Siin käsitletakse riigisaladuse tasemeid ja seda millise info on riik kuulutanud riigisaladuseks, samuti seda mille poolest erineb riigisaladus töötlev infosüsteem teistest infosüsteemidest.

1.2 Mõisted

1. salastatud teabekandja – mis tahes objekt, millele on jäädvustatud riigisaladus või salastatud välisteave;
2. teabevaldaja – asutus, põhiseaduslik institutsioon või juriidiline või füüsiline isik, kelle valduses on riigisaladus või salastatud välisteave;
3. juurdepääsuvajadus – töö- või teenistusülesandest, samuti õppe- või uurimistööst, riigihankest või rahvusvahelisest hankest tulenev riigisaladuse või salastatud välisteabe töötlemise vajadus, samuti õigus tutvuda riigisaladuse või salastatud välisteabega muul käesolevas seaduses sätestatud alusel;
4. teadmisvajadus – juurdepääsuvajadus teatavale riigisaladusele või salastatud välisteabele;
5. juurdepääsuõigus – isiku õigus töödelda riigisaladust või salastatud välisteavet ametikohajärgselt või asutuse juhi otsuse, juurdepääsuloa või -sertifikaadi, tunnistajakaitse kaitseabinõude kohaldamise või uurimisasutuse, prokuratuuri või kohtu määruse alusel;
6. töötlemine – teabe või teabekandja koostamine, märgistamine, kogumine, hoidmine, säilitamine, vedamine, reprodutseerimine, edastamine, hävitamine, nendest väljavõtete tegemine, nendega tutvumine või muu teabe või teabekandjaga tehtav toiming, sõltumata toimingu teostamise viisist või kasutatavatest vahenditest;
7. riigi julgeoleku volitatud esindaja – Kaitseministeeriumi põhimääruses määratud Kaitseministeeriumi struktuuriüksus, mille ülesandeks on salastatud välisteabe kaitse korraldamine ja kontroll;
8. turvaala – konfidentsiaalse, salajase või täiesti salajase taseme riigisaladuse või salastatud välisteabe ja seda sisaldava salastatud teabekandja töötlemiseks kasutatav ala.
9. administratiivala – töötleva üksuse kasutuses olev selge välispiiriga ala, millele

sisenenud kõik isikud ja sõidukid tuvastatakse;

10. infosüsteem – infosüsteem, sealhulgas tehnilised vahendid, mida kasutatakse teabe elektrooniliseks töötlemiseks;

11. elektrooniline teabeturve – riigisaladuse või salastatud välisteabe käideldavuse, salajasuse ja terviklikkuse tagamine töötlussüsteemis;

12. infosüsteemi akrediteerimine – töötlussüsteemi elektroonilise teabeturbe nõuetele vastavuse hindamine;

13. käideldavus – teabe kasutamise ja teabele juurdepääsu võimalus volitatud isiku nõudel;

14. salajasus – teabe volitamata isikutele mittekättesaadavus või mittearusaadavus;

15. terviklikkus – teabe omadus olla volitamata isikute poolt muutmata, täiendamata või hävitamata;

16. oht – teabe käideldavuse, salajasuse või terviklikkuse potentsiaalne kahjustumine;

17. turvarike – olukord, kus teave või selle kaitsmist toetavad süsteemitoimingud ja vahendid kaotasid või võisid kaotada varguse, sabotaaži, terrorismiaktide, muu lubamatu tegevuse või turvaaukude tõttu salajasuse, terviklikkuse või käideldavuse (sealhulgas teabe kadumine, volitamata isikutele teatavakssaamine, volitamata isikute poolt muutmine või hävitamine või rünne süsteemi suhtes);

18. turvarisk – turvarikke esinemise tõenäosus;

19. riskihaldus – vara, teabe, ohu, turvarikke ja turvariski analüüs, mille põhjal määratakse kindlaks teabe ja selle kaitsmist toetavate süsteemitoimingute ja -vahendite turvameetmed. Riskihaldus hõlmab süsteemi turvameetmete planeerimist, korraldamist, kasutamist ja kontrollimist, selleks et vältida turvariski väljumist vastuvõetavatest piiridest ja turvarikkeid;

20. haavatavuse analüüs – süsteemi üksikasjalik kontrollimine, et selgitada välja süsteemi turvaaugud, ohud süsteemis töödeldava teabe salajasusele, terviklikkusele ja käideldavusele ning süsteemi vastuvõtlikkus mis tahes ründele või ohule;

21. infosüsteemi turvanõuete loetelu – süsteemi kohustuslike turvanõuete loetelu, mis sätestab, kuidas saavutada süsteemi piisav turvalisus ning kuidas tagada ja kontrollida teabe turvalisust süsteemis;

22. infosüsteemi turvanõuete rakendamise juhend – dokument, mis kirjeldab detailselt süsteemi turvanõuete loetelus ettenähtud turvanõuete täitmise korda ja iga konkreetse töötaja või muu isiku ülesandeid teabe turvalisuse tagamisel;

23. väline turvakeskkond – süsteemi paiknemiskohta ümbritsev keskkond, sealhulgas hoone või ala, milles toimuvad sündmused võivad mõjutada süsteemi turvalisust;

24. sisemine turvakeskkond – välise turvakeskkonnaga piirnev ruum või ala, kus paiknevad

süsteemi komponendid või kus neid kasutatakse;

25. elektrooniline turvakeskkond – piirdub süsteemi komponentidega, mille abil teavet elektrooniliselt töödeldakse ning mille kaitseks süsteemi käitav personal rakendab elektroonilisi turvameetmeid.

26. kiirgusturve – kiirgusturbe meetmed tagavad, et salastatud teave ei leviks kontrollimatult süsteemist väljaspoole elektromagentlainetena. (RT I 2007, 73, 449)

1.3 Riigisaladuse mõiste

Riigisaladus on Eesti Vabariigi julgeoleku või välissuhtlemise tagamise huvides avalikuks tuleku eest kaitset vajav ametlikult salajaseks määratud info, materjal või muu teave.

See teave on üksnes riigisaladust käsitlevas seaduses ja selle seaduse alusel välja antud õigusaktides sätestatud tunnustele vastav teave:

1. riigisaladus – Eesti Vabariigi julgeoleku või välissuhtlemise tagamise huvides avalikuks tuleku eest kaitset vajav üksnes käesolevas seaduses ja selle alusel antud õigusaktides sätestatud tunnustele vastav teave, välja arvatud salastatud välisteave;
2. salastatud välisteave – välisriigi, Euroopa Liidu, NATO või mõne muu rahvusvahelise organisatsiooni või rahvusvahelise kokkuleppega loodud institutsiooni poolt salastatud ja Eestile avaldatud teave ning Eesti Vabariigi poolt välislepingu täitmiseks loodud teave, mis tuleb salastada välislepingu kohaselt.

Eeltoodud definitsiooninormis sisaldub seega kaks olulist tunnust:

1. teave peab olema “Riigisaladuse ja salastatud välisteabe seaduses” sätestatud kui riigisaladus ning;
2. see peab vajama Eesti Vabariigi julgeoleku ja välissuhtlemise tagamise huvides avalikuks tuleku eest kaitset.

“Riigisaladuse ja salastatud välisteabe kaitse korra” paragrahvides 4 - 8 sisaldub valdkondade kaupa kirjeldus julgeoleku ja välissuhtlemise huvides kaitset vajavatest teabeliikidest. Nendele kirjeldustele vastav teave on riigisaladus, sõltumata sellest, mil viisil seda parasjagu kasutatakse või millisel kujul ta esineb. (RT I 2007, 73, 449)

Teabe kaitsevajaduse suurenemise järjekorras kaitstakse riigisaladust järgmistel tasemetel, alates madalamast tasemest:

1. piiratud tase;
2. konfidentsiaalne tase;
3. salajane tase;
4. täiesti salajane tase.

Vajadus nelja taseme järele tuleneb asjaolust, et sama süsteem on kasutusel paljudes teistes riikides, samuti NATOs ja Euroopa Liidus.

Riigisaladuse liikide loetelu esitamisel on lähtutud kontseptsioonist, et teave peab olema seotud riigi julgeoleku või välissuhtlemise tagamisega.
Riigisaladuse liigid:

- välissuhete riigisaladus;
- riigikaitse riigisaladus;
- korrakaitse riigisaladus;
- julgeolekuasutuste riigisaladus;
- infrastruktuuri ja teabe kaitse riigisaladus.

(RT I 2007, 16, 77)

Juriidiliselt on riigisaladus teave, mille omandiõigus kuulub ainult riigile. Eesti Vabariigis kontrollib ligipääsu ja vastutab riigisaladuste eest Kaitsepolitseiamet, kaitseväes ja Kaitseliidus Kaitsejõudude Peastaap. Elektroonilist teabeturvet riigisaladust töötlevates infosüsteemides korraldab ja kontrollib Teabeamet. Mõistagi vastutab riigisaladuse eest ka isik, kellele on riigisaladus usaldatud.

Teiste riikide ja rahvusvaheliste organisatsioonidega (sh NATO ja EL) on sõlmitud salastatud välisteabe kaitseks vastastikused kokkulepped, millega Eesti Vabariik on võtnud endale kohustuse kehtestada riigisiseselt kehtivad nõuded tagamaks talle usaldatud teabe kaitse. See on oluline Eesti Vabariik rahvusvahelise usaldusväärsuse suurendamiseks, mis omakorda võimaldab Eesti Vabariigi julgeolekut paremini kaitsta, saades koostööpartneritelt rohkem teavet ning tagades koostööpartneritele Eesti Vabariigi poolt edastatud teabe kindlama kaitse.

Eesti Vabariigi seadusandlikud aktid, mis pudutavad riigisaladust, on paljus osas koostatud NATO poolt väljatöötatud direktiivide põhjal. Elektroonilises teabeturbes on samuti palju protseduure ülevõetud. NATOs ei ole hetkel veel samuti välja valitud seda ühte ja head metoodikat riskihalduse läbiviimiseks.

1.4 Riigisaladust töötlevad infosüsteemid

Riigisaladust töötlevaid infosüsteeme võib salastatud teabe töötlemiseks kasutada üksnes vastavussertifikaadi olemasolu korral. Töötlussüsteemile vastavussertifikaadi väljastamise eelduseks on akrediteerimisprotsessi läbiviimine. Töötlussüsteemi akrediteerimise eesmärk on tagada piisav veendumus, et süsteem vastab elektroonilise teabeturbe tagamiseks kehtestatud nõuetele ning on piisavalt turvaline.

Olulisemad seadusandlikud aktid akrediteerimisprotsessis on:

1. Riigisaladuse ja salastatud välisteabe seadus
2. Riigisaladuse ja salastatud välisteabe kaitse kord. Vabariigi Valitsuse määrus nr.262
3. Arvutite ja kohtvõrkude kaitse nõuded. Kaitseministri määrus nr.34

Riigisaladust töötlevate infosüsteemide akrediteerimise üle otsustamisel lähtutakse:

1. süsteemi füüsilistest turvameetmetest;
2. süsteemiga seotud turvariskidest ja nende analüüsist;
3. süsteemi turvanõuete loetelust;
4. süsteemi turvanõuete rakendamise juhendist;
5. süsteemi asukoha kiirgusturbe tsoneerimise tulemustest;
6. teabest elektroonilise teabeturbe nõuete täitmise kohta töötleva üksuse poolt.

(RT I 2007, 73, 449)

Infosüsteemi akrediteerimiseks peavad olema koostatud vähemalt järgmised dokumendid:

1. süsteemi tehniline kirjeldus;
2. süsteemi riskide analüüs;
3. süsteemi turvanõuete loetelu;
4. süsteemi turvanõuete rakendamise juhis.

Süsteemi tehnilise kirjelduse alusel koostatakse süsteemi esialgne riskianalüüs. Riskianalüüs on aluseks süsteemi turvanõuete loetelu koostamisel. Uue süsteemi ehitamisel teostatakse riskianalüüs pärast süsteemi valmimist uuesti ning turvanõuete loetelu täiendatakse vastavalt.

Turvanõuete loetelu on turvanõuete rakendamise juhendi koostamise aluseks. Riigisaladuse

töötlevatel infosüsteemidele on seadusega määratud kindlad meetmed, mille rakendamiseta ei tohi töödelda töötlussüsteemis salastatud teavet. Tuleb arvestada selliste ohtudega, millele tavalist teavet töötlevates infosüsteemides ei ole tarvis suurt tähelepanu pöörata. Näiteks kiirgusturbe ranged nõuded ja krüptoseadmete kasutamise ranged reeglid. Nii kiirgusturbe nõuete kui ka krüptoseadmete kasutamise nõuete kohta on olemas eraldi määrused, mis aga on salastatud piiratud tasemega teabena ja käesolevas magistritöös neid nõudeid ei käsitleta. Kuna riigisaladust töötlevad infosüsteemid on enamalt jaolt kinnised, see tähendab nad ei ole ühenduses internetiga, siis ei ole tarvidust arvestada internetist tulenevaid ohte.

Riigisaladust võib edastada üldiseid kommunikatsiooniliine kasutades ainult krüpteeritult ja krüpteerimisprogrammid ning krüpteerimisseadmed peavad olema heakskiidetud vastavate asutuste poolt.

PEATÜKK 2. RISKIHALDUSEST ÜLDISELT

2.1 Riiklikud institutsioonid

Suuremad riigid omavad reeglina eraldi institutsioone infoturbealase tegevuse suunamiseks ja koordineerimiseks. Juhtivamateks riikideks infoturvalisust puudutavate regulatsioonide ja organiseerimise küsimustes on Ameerika Ühendriigid ja Kanada, Euroopas Saksamaa, Inglismaa ja Prantsusmaa.

Peatüki eesmärk on tutvustada lühidalt erinevate riikide ja organisatsioonide infoturbeasutusi, kus tegeldakse suuremal või vähemal määral riskianalüüsi meetodite koostamisega. Vajadusel saab riigisaladuse valdaja nende asutuste kodulehtedelt lisa informatsiooni infoturbe ja riskihalduse kohta.

2.1.1 ENISA

On Euroopa Komisjoni poolt 2004 aastal loodud infoturbe agentuur. Agentuuri eesmärgiks on tõsta Euroopa Liidu liikmesriikide võimet, vältida infoturbe probleeme ning olla suutelised tegelema ja reageerima võrgu ja infoturbe probleemidele nende tekkimisel.

Agentuuri põhiüleanneteks on:

- Euroopa Komisjoni ja liikmesriikide infoturbe alane nõustamine ja abistamine;
- infoturbeintsidentide ja riskide kohta andmete kogumine ja andmete analüüsimine;
- riskide hindamise ja riskide haldamise metoodikate edendamine, et suurendada võimekust tegeleda infoturbe ohtudega;
- turvateadlikkuse kasvatamine ja koostöö edendamine infoturbe valdkonna erinevate osapoolte vahel (eriti arendada avaliku – erasektori infoturbealast koostööd). (ENISA, 2008)

2.1.2 Saksamaa BSI

1991 a. asutatud Saksamaa Infoturbeamet (*Bundesamt für Sicherheit in der Informationstechnik*, *BSI*) on kahtlemata Euroopa võimsaim ning suurima uurimis- ja arendussuutvusega infoturbekeskus. Ta töötab välja turvamehhanisme, -metoodikaid ja -juhendeid Saksamaa riigi- ja omavalitsusasutustele, annab välja turvatoodete ja -süsteemide sertifikaate, korraldab kursusi ja konverentse jne.

BSI - on välja töötanud IT etalonturbe teatmiku – *IT Baseline Protection Manual*, mille eesmärk on saavutada organisatsiooniliste, personalikesksete, infrastruktuuriliste ja tehniliste tüüpsete turvameetmete asjakohase rakendamisega tegelev IT-süsteemide turve, mis oleks adekvaatne ja piisav kesktaseme turvanõuete mõttes ning võiks olla aluseks kõrgemat kaitseastet nõudvate IT rakenduste puhul.

Sel eesmärgil soovitab IT etalonturbe teatmik vastumeetmete komplekte tüüpiliste IT konfiguratsioonide, keskkondade ja organisatsiooniolude tarbeks. Selle teatmiku koostamisel eeldas Saksa Infoturbe Riigiamet riiklike institutsioonide riskianalüüsil saadud hinnanguid teadaolevate ohtude ja nõrkuste põhjal ning töötas välja selleks otstarbeks sobivad mõõdustikud. Seetõttu ei tarvitse IT etalonturbe teatmiku kasutajad uuesti läbi teha neid IT etalonturbega seotud analüüse. Neil tuleb ainult hoolitseda selle eest, et soovitatud turvameetmed järjekindlalt ja täielikult evitataks. Ühtlasi aitab see tagada, et kesktaseme kaitse nõuetele vastava infoturbe võib saavutada vaeva säästes, eriti seetõttu, et üksiksüsteemide turvapoliitikad võivad viidata IT etalonturbe teatmikule. (BSI, 2008)

BSI poolt on välja töötatud järgmised infoturbe materjalid:

- BSI - Standart 100-1 „Turvaline informatsiooni haldamise süsteem“ ;
- BSI - Standart 100-2 „ IT - etalonturbe meetod“;
- BSI – Standart 100-3 „Etalonturbel põhinev riskianalüüs“;
- Infoturbe käsiraamat;
- Etalonturbe profiilid;
- Etalonmeetmete kataloog 2005 (saksa keelne 2007).

2.1.3 NIST

Üks vanimaid organisatsioone Ameerikas on 1901. aastal asutatud USA Riiklik Standardite ja Tehnoloogia Instituut - *National Institute of Standards and Technology.* NIST-i ülesanneteks on ka tagada informatsiooni turvalisus ja säilitada kriitiliste teenuste käideldavus majanduslikult mõistlike turvameetmetega. NIST-il on põhikirjajärgne vastutus anda välja turvastandardeid ja ettekirjutusi riskitundlikele kriitilistele riiklikele süsteemidele nagu näiteks elekter, vesi, gaas ja ka infosüsteemid – neid standardid kasutatakse tihti ka erasektoris.

Standardeid infosüsteemidele teeb NIST-i Infotehnoloogia Laboratoorium – ITL - *Information Technology Laboratory.* Lisaks juhendab infotehnoloogia alaseid uurimusi ning arendab testmeetmeid. Põhilisteks suundadeks on ka krüptograafiatehnoloogia ja rakendused, autentimine, avaliku võtme infrastruktuur, internetiturvalisus ja turvalisuse haldamine. Vastavad publikatsioonid on NIST-i uuringute ja avastuste resultaadiks turvalisuse vallas. Publikatsioonid on avaldatud kui *Special Publications. Special Publications* 500-seeriad käsitlevad infotehnoloogia ja 800-seeriat käsitlevad arvutiturvalisus. 800-seeria hulgas on ITL näiteks koostanud detailse riskihalduse juhise – *Risk Management Guide for Information Technology Systems, NIST Special Publication 800-39.*

Selle juhise järgi tuleb läbiviia järgmised tegevused:

- süsteemi iseloomustus;
- ohtude tuvastamine;
- nõrkuste tuvastamine;
- juhttoimete analüüs;
- ohtude realiseerumise tõenäosuse tuvastamine;
- mõjude analüüs;
- riski hindamine;
- soovitused meetmeteks;
- tulemite dokumenteerimine. (NIST ITL, 2008)

2.1.4 OGC - The Office of Government Commerce

Inglismaal põhiliselt riigihangete korraldusega tegeleva ametiasutuse OGC– *Office of Governmental Commerce* poolt on koostatud ka IT hangete alaseid juhendmaterjale, mis on koondatud *IT Infrastructure Library-sse* (ITIL). ITIL on OGC poolt registreeritud kaubamärk ITIL on juhis praktikutele, kuidas korraldada IT teenuste haldust ettevõttes. ITIL koostati 80-ndatel aastatel Inglismaal *Central Computing and Telecommunications Agency poolt*. Praegu arendatakse edasi OGC nime all. ITSMF (*IT Service Management Forum*) tunnistab ja soovitab ITIL dokumentide kasutamist, need on kujunenud standardiks Inglismaal.

OGC poolt on väljatöötatud riiklikele organisatsioonidele mõeldud riskianalüüsi meetod CRAMM. Samas on ka väljatöötatud automatiseeritud tööriist CRAMM. Ilma selle tööriistata on raske läbiviia GRAMM meetodil riski analüüsi. CRAMM (meetod ja tööriist) on esimesi väljalaskeid, mis baseerub inglise valitsusorganisatsioonide parimatel praktikatel. Praegusel hetkel on CRAMM briti valitsuse riskianalüüsi meetod, kuid teda kasutatakse ka mujal paljudes riikides, organisatsioonides ja tööstuses. CRAMMi kasutab ka NATO, kelle jaoks on eraldi väljatöötatud moodul, mis on salastatud ning ei ole kättesaadav.
(OGC, 2008)

2.1.5 DSD- Austraalia infoturbe organisatsioon

Organisatsiooni ülesandeks on toetada Austraalia valitsust ja militaarstruktuure kõrgetasemelise infoturbealase informatsiooni, juhendite ja soovitustega. Samuti tegeleb DSD krüptoseadmete hindamise ja turvalise kommunikatsiooni lahenduste väljatöötamisega. DSD on kehtestanud – Austraalia infoturvalise hindamise programmi -AISEP. Samuti on DCD väljatöötanud IT turvalisuse käsiraamatu *Australian Government Information and Communications Technology Security Manual ACSI 33*. Käsiraamatus olevad nõuded on kohustuslikud kõigile Austraalia riigiasutustele. Käsiraamatut on kaks versiooni. Üks versioon, mis on avalik, on mõeldud kuni piiratud tasemega riigisaladust töötlevate infosüsteemide jaoks ja teine versioon, mis ei ole avalik, on mõeldud kõrgema kui piiratud tasemega riigisaladust töötlevate infosüsteemide jaoks. Turvameetmeid täiendatakse regulaarselt üks kord aastas.
(DSD, 2008)

2.1.6 Prantsusmaa infoturbeamet

DCSSI *(Central Information Systems Security Division)* on Prantsusmaa infoturbe asutus kelle põhiülesandeks on väljatöötada regulatsioonid ja turvaprotseduurid riigiinfosüsteemide jaoks, krüptoseadmete sertifitseerimine ja uute toodete väljatöötamine ning infosüsteemide sertifitseerimine ja auditeerimine. Veel tegeleb DCSSI infoturbealase koolitusega.

DCSSI poolt on väljatöötatud riskihaldusmeetod ja programm EBIOS. See oli algul mõeldud ainult riigiasutuste jaoks, kuid nüüd on see vabalt kättesaadav kõigile ja on populaarne paljudes organisatsioonides. Teda on lihtne kasutada, ta on varustatud põhjalike juhenditega ning on kooskõlas enamiku infoturbe standarditega. Positiivne on veel see, et riskianalüüsi programm on tasuta saadaval kõigile huvilistele.
(DCSSI, 2008)

2.1.7 Eesti infoturbeasutused

Eestis oli varem infoturbe alane tegevus küllaltki nõrk ja vajalikku eesti keelset informatsiooni ja nõuannet saada oli küllaltki raske. Kuid viimasel ajal on märgata infoturbe alase tegevuse aktiviseerumist. Selle üheks tõukejõuks olid kindlasti 2007. aasta mais toimunud Eesti Vabariigi vastased küberrünnakud. Allpool on ära toodud mõned aktiivselt tegutsevad infoturbeasutused:

1. Andmekaitse Inspektsiooni – põhiülesandeks on isikuandmete töötlemisega tegelevate asutuste järelevalve ja andmekaitsealase tegevuse korraldamine;

2. Finantsinspektsioon – kes annab nõu ja kontrollib rahandusega seotud organisatsioonide (pangad, kindlustused) infoturbealast tegevust;

3. Teabeamet – korraldab ja kontrollib riigisaladust töötlevate infosüsteemide kaitset;

4. Riigi Infosüsteemide Arenduskeskus – Keskuse põhiülesanded on riigi infosüsteemide arengukavade elluviimise korraldamine, koordineerimine, juhendamine ja riigi infosüsteemide haldamine. Samuti tegeleb see asutus standardimisega ja on käsile võtnud etalonturbe meetodi kohaldamise riigiasutuste infosüsteemidele. Eesti riigi tasemel

täidab CERT (Computer Emergency Response Team) ülesandeid ning tegeleb Eesti arvutivõrkudes toimuvate turvaintsidentide käsitlemisega, ennetavate tegevustega turvaintsidentide ärahoidmiseks ja kasutajate turvateadlikkuse tõstmisega;

5. SIVAK- Kaitseväe Side- ja Infosüsteemide Väljaõppe- ja Arenduskeskuse koosseisu kuulub küberkaitsekeskus, mille baasil on arendatud välja NATO Kooperatiivse Küberkaitse Kompetentsikeskus. Kompetentsikeskus on NATO programmi raames loodud rahvusvaheline sõjaline organisatsioon, mille eesmärgiks on arendada NATO ja liikmesriikide küberkaitsealast koostööd ning töötada välja põhimõtted ja meetodid küberkaitse teostamiseks. Kompetentsikeskuse eesmärgiks on uute küberkaitsemeetodite, kontseptsioonide ja tehniliste lahenduste väljatöötamine. Samuti on NATO kompetentsikeskuse funktsiooniks küberkaitsealaste analüüside koostamine, õppe- ja teavitusmateriaaljde loomine ning väljaõppe korraldamine.

2.2 Rahvusvahelised standardid

Alljärgnevalt antakse ülevaade infoturbe korralduses kasutatavatest standarditest üldiselt ja kirjeldatakse, kas ja kuidas saab neid kohandada ka riskihalduse jaoks.

2.2.1 ISO 13335 Infoturbe halduse suunised

See on viieosaline infoturbe haldust käsitlev dokument, mis on üle võetud ka Eesti standardiks. ISO/IEC TR 13335 on jaotatud mitmeks osaks.

Osa 1 annab ülevaate infoturbe halduse kirjeldamiseks kasutatavatest põhimõistetest ja mudelitest. See materjal sobib infoturbe eest vastutavatele juhtidele ning organisatsiooni üldise turvaprogrammi eest vastutajaile. **(**EVS-ISO/IEC TR 13335-1, 1999)

Osa 2 kirjeldab haldus- ja plaanimisaspekte. Ta puudutab juhte, kelle kohustused on seotud organisatsiooni infotehnoloogiasüsteemidega. (EVS-ISO/IEC TR 13335-2, 1999)

Osa 3 kirjeldab turbemeetodeid, mis puutuvad neisse, kes osalevad haldustegevustes projekti elutsükli kestel, näiteks plaanimisel, projekteerimisel, teostamisel, testimisel, hankimisel või

ekspluateerimisel. (EVS-ISO/IEC TR 13335-3, 1999)

Osa 4 juhatab, kuidas valida turvameetmeid ning kuidas seejuures toetuda etalonmudelitele ja -meetmetele. Ta kirjeldab ka, kuidas see täiendab 3. osas kirjeldatud turbemeetodeid ja kuidas turvameetmete valimiseks saab kasutada täiendavaid hindamismeetodeid. Väikesemahuline 8. peatükk, mis jaotab meetmed kaheteistkümneks üsna üldiselt määratletud tüübiks. Meetmeid on püütud seada vastavusse mudeli kuue turvaeesmärgiga, kuid seda on õnnestunud teha ainult osaliselt, üldtunnustatud traditsiooniliste eesmärkide puhul, osa eesmärke on sisuliselt katmata. Selle osa lisades on abimaterjalina viidatud kaheksale muule turvajuhendile, millest enamik ei sobi etalonturbeks ja millest osa on moraalselt vananenud. (EVS-ISO/IEC TR 13335-4, 2000)

Võrguturbe meetmeid sisaldab 5. osa, mis jaotab need umbes kahekümneks väga üldiselt käsitletud tüübiks. (EVS - ISO/IEC 13335-5, 2003)

2.2.2 ISO/IEC 27002 Infotehnoloogia. Infoturbe halduse praktilised juhised

ISO/IEC 27002 sai oma praeguse nime juulis 2007, mil see nimetati ümber standardist ISO/IEC 17799. Standard on alguse saanud Briti standardina BS 7799 *British Standards Institute* poolt. Ka see standard on nime all EVS-ISO/IEC 17799:2003 tõlkemeetodil üle võetud Eesti standardiks. Standardis käsitletavad teemad on turvapoliitika, turvaorganisatsioon, varade klassifitseerimine ja juhtimine, personali turvalisus, füüsiline ja keskkonna turvalisus, arvutite ja võrgu ohjamine, süsteemi ligipääsu ohjamine, süsteemiarendus ja hooldus, organisatsiooni tegevuskavad (sealhulgas häire- ja kriisiolukorra puhul), vastavus seadusandluse ja lepingulistele nõuetele. Erinevus võrreldes standardiga ISO/IEC 13335 on suunatud juhtkonnale – tehniliste küsimuste asemel keskendutakse juhtimisalastele küsimustele.

Standard sisaldab ka riskide hindamise metoodikat. Standard ning selles sisalduv metoodika oli ka kaalumisel Eesti valitsusasutuste kohustusliku turbemetoodika väljatöötamisel aluseks võtta, kuid parema granulaarsuse ning lihtsamini rakendatava metoodika tõttu eelistati Saksa Infoturbeameti (BSI) metoodikat. (Koppelmaa, 2004)

ISO/IEC 27000 standardite perekond on suunatud infoturbe juhtimisele ning hetkel aktiivselt arendatav. Suhteliselt hästi ajakohastatud standard. Teda on läbi vaadatud iga paari aasta järel ning tänu sellele juhitakse seal tähelepanu ka moodsatele tehnoloogiatele nagu süle- ja

pihuarvutid, mobiiltelefonid või traadita Interneti levialad. Samas ei ole vähemalt viimastes versioonides enam liigselt rõhku asetatud juba vananevatele tehnoloogiatele.

2.2.3 EVS-ISO TR 13569 Pangandus ja sellega seotud rahandusteenused

On üle võetud ka Eesti standardiks. Praegu on ISO-s menetlemisel standardi uustöötlus. ISO infoturbestandarditest on 13569 turvameetmete ja nende rakendamise kirjelduse poolest kahtlemata kõige detailsem, konkreetsem ja elulähedasem. Turve põhineb levinuimal, kolme eesmärgiga turvamudelil.

EVS-ISO TR 13569 annab ülevaate alljärgnevatel teemadel:

- määratleb infoturbe programmi;
- esitab infoturbepoliitika ja organisatsiooni tegevused;
- pakub äripraktikas tunnustatud ja finantsrakendustele sobiliku komplekti turvameetmeid;
- on kooskõlas olemasolevate turbehalduse standarditega;
- sisaldab hulga dokumendi- ja protseduuride näidiseid.

Turvameetmete täpset arvu on tülikas kindlaks teha, kuid muude allikatega võrreldavatel alustel võib nende koguarvuks hinnata umbes 200-250. Tuleb arvestada, et umbes 20% meetmetest on pangandusspetsiifilised, võib granulaarsust hinnata pigem väikeseks kui suureks. Infovarade granulaarsus on suhteliselt suur, kuid infovarade puhul ilmneb panganduse spetsiifika veelgi tugevamalt.

Ajakohastamise periood on liiga pikk (nagu muudelgi ISO standarditel) ning standardi sisu pole veel piisavalt stabiliseerunud. (EVS-ISO TR 13569, 2006)

2.2.4 ISO/IEC 15 408 Common Criteria

Common Criteria (CC) on rahvusvaheline ISO standard tehnoloogilise infrastruktuuri toodete turvalisuse hindamiseks. Hindamise objektiks võivad olla nii infotehnoloogia seadmed kui ka programmid.

ISO/IEC 15 408 koosneb kolmest osast:
Osa 1: Sissejuhatus ja üldine mudel. Määratleb CC üldised põhimõtted infotehnoloogiliste toodetele ja süsteemidele;
Osa 2: Andmeturvalisuse funktsionaalsed vajadused. Esitleb kogumi funktsionaalseid komponente, millede abil antakse hinnatava toote funktsionaalsed nõudmised;
Osa 3: Andmeturbe turvanõuded. Esitleb andmeturbe turvanõudeid, mille abil hinnatakse hinnatava toote turvanõuded.

Riskianalüüsiga seondub kaudselt – võimaldab hinnata juba rakendatud turvameetmete taset ja seega ei määratleda jääkriske.
(Common Criteria, 2008)

2.2.5 Eurostandardid

Terviklikud infoturbesüsteeme ja rakendusvaldkonnast sõltumatud eurostandardid puuduvad. Muude normdokumentide hulgast võib leida üksikuid, mis puudutavad seda valdkonda väga üldiste nõuete tasemel. Paar tüüpilist näidet on järgmised.

- Eurodirektiiv 2002/58/EC

(Directive 2002/58/EC of the European Parliament and of the Council, of 12 July 2002, concerning the processing of personal data and the protection of privacy in the electronic communications sector)
See on isikuandmete ja privaatsuse kaitsele suunatud deklaratiivne ja turvapoliitiline dokument, mis käsitleb elektroonilise side valdkonda. Ta sätted võivad küll olla aluseks ja abivahendiks konkreetsete infoturbe poliitikate koostamisel, mitte aga turbe praktilisel korraldamisel ja rakendamisel.

- *VI/661/97 Rev. 2 Paying Agencies' I.T. Systems. Computer Security Guidelines*

on Euroopa Komisjoni Põllumajandusdirektoraadis 1998. a. koostatud dokument, mille kümmekond lehekülge sisaldavad suuniseid infoturbe korralduseks ja loetlevad paarkümmend turvameetmetüüpi.

- *ENV 12924 (1997) Medical Informatics: Security Categorisation and Protection*

for Healthcare Information Systems
määratleb rea turvaprofiile tervishoiuandmetele ja vastavad etalonmeetmed. Standard on tugevalt rakendusspetsiifiline ja teda täiendab rida muid, turbe kitsamate aladega seotud standardeid.

- *ETSI Baseline Security Standard Features and Mechanisms*

kirjeldab detailidesse laskumata mõningaid infoturbe alal kasutatavaid turvamehhanisme, mitte aga nende rakendamist.
(Hanson,V. Praust,V. 2003)

2.3 Riskianalüüsi programmid

Peatüki eesmärk on analüüsida erinevaid riskihalduse ja riskianalüüsi programme ning teha kindlaks, millised on sobivamad töövahendid riigisaladust töötlevate infosüsteemide jaoks.

Enamasti kujutavad sellised tooted endast riskihalduseks või turbe standardsuse (enamasti ISO/IEC 17799 järgi) auditeerimiseks määratud tarkvara, mille üheks koostisosaks on turvameetmete kataloog.

Nende eelisteks on:

1. kogutud riskianalüüsi informatsiooni lihtne salvestamine, töötlemine ja kättesaadavus;
2. võimalus vaadelda vastumeetmete kombinatsiooni mõju materiaalse ja infovara kaotusele;
3. võimalus kiiresti sisestada riskikeskkonna muutusi ja identifitseerida riski muutusi;
4. võimalus rakendada “katse ja eksituse” meetodit otsides vastuvõetavaid tulemusi;
5. võimalus võrdlemiseks: st luuakse olukord, kuis kaks eksperti kasutavad sama töövahendit samade nõuete korral ja tulemus peaks olema samasugune.

2.3.1 Valiku kriteeriumid

All järgnevas osas antakse ülevaade olemasolevatest ja levinumatest riskihaldus ja – analüüsi programmidest. Tänapäeval on juba igal riskianalüüsi meetodil olemas ka oma programm. Programmi valiku protsess on sarnane teiste programmide valiku protsessiga ja selle käigus

tuleb tähelepanu pöörata samadele funktsioonidele, mida on vaja programmide lihtsaks kasutamiseks. Põhiliselt on vaadeldud järgmiste funktsionaalsuste olemasolu:

- riistvara ja tarkvara nõuded - peab sobima enamkasutavate operatsioonisüsteemidega. Ei tohiks olla liigseid nõudeid riistvarale. Peab töötama keskpärase lauarvuti või kaasaskantava arvutiga;
- kasutatav meetod - enamus riskianalüüsi programme kasutab kvalitatiivset või kvantitatiivset hindamist ja mõnel on nad kombineeritud. Tulemused esitatakse kas matemaatilisel või keelelisel kujul. Kasutatav meetod peab olema lihtne ja kasutajale peab olema arusaadav, kuidas tulemused saadakse;
- kasutatavad infotehnoloogia turvastandardid – tähtis on, et oleks kasutatud vähemalt ühte üldtuntud infotehnoloogia turvastandardit;
- raporti esitamise nõuded – raport peab kokkuarvutama riskid ja esitama ka vastumeetmed. Tulemusi peab saama esitada ka graafilisel kujul;
- dokumentatsiooni olemasolu - kasutusjuhendi olemasolu;
- turvalisus ja ajaloo nõuded- kuna riskianalüüs on küllaltki tundliku informatsiooni töötlemine siis peavad olema kasutusel teatud turvafunktsioonid nagu krüpteerimine kasutajate haldus, ajaloo ja logimise funktsioonid;
- kasutamismugavus – programm peab olema lihtsalt kasutatav ja kiiresti õpitav. Programmi disain peab olema sarnane enamlevinud programmide disainile;
- kasutatavad keeled – soovitavalt peab olema kindlasti inglise keeles ja parimal juhul eesti keeles;
- koolitus ja tehnilisele toele – programmile peab olema kasutaja koolitus ja soovitav on kasutajatoe olemasolu juhuks kui programmiga esineb probleeme;
- maksumus – maksumus ei tohi olla liiga kõrge ja soovitav on kasutada tasuta rakendusi.

Lisaks tuleb tähelepanu pöörata järgmistele võimalustele:

- kogutud riski hindamise informatsiooni lihtne salvestamine, töötlemine ja kättesaadavus;
- võimalus vaadelda vastumeetmete kombinatsiooni mõju materiaalse ja infovara kaotusele;
- võimalus kiiresti sisestada riskikeskkonna muutusi ja identifitseerida riski muutusi;
- võimalus rakendada “katse ja eksituse” meetodit otsides vastuvõetavaid tulemusi;
- võimalus võrdlemiseks: st olukord, kui kaks eksperti kasutavad sama töövahendit samade nõuete korral, peaks tulemus olema samasugune.

Allpool vaadeldakse järgmisi programme:

- CRAMM (Insight Consulting Limited, UK)
- RiskWatch (firmalt RiskWatch, USA)
- EBIOS (DCSSI, Prantsusmaa)
- GSTOOL (BSI, Saksamaa)
- ISKE (RIA, Eesti)
- Eesti Ühispanga etalonturbesüsteem (EÜP, Eesti)

2.3.2 CRAMM

Programm on loodud Cramm meetodi kasutamise lihtsustamiseks. Programmi on loonud firma *Insight Consulding*. Kõik meetodi etapid on korrapäraselt toetatud. Programme on kaks versiooni: *Cramm expert ja Cramm express*. Prooviversioon on saadaval programmi proovimiseks. *Cramm expert* vajab teadmisi Cramm meetodist ja *Cramm expressi*ga saavad hakkama ka need, kellel pole põhjalike teadmisi Cramm meetodist.
Cramm -is on väga suur vastumeetmete andmebaas. Ligi 3000 vastumeedet, mis on jaotatud 70 -sse loogilise gruppi.
Keeled: inglise, hollandi, tsehhi.
Maksumus:cramm expert : £2950 cd ja £875 aastane litsentsi maksumus.
Kasutajad: Inglismaa valitsusasutused, NATO ja paljud tesite riikide valitsusasutused ning organisatsioonid.
Standardid: BS 7799 (ISO27002)
(CRAMM, 2008)

2.3.3 RiskWatch

Riskihalduse toodete hulgas on viimased kümme aastat olnud liidripositsioonil tootesari *RiskWatch*. Programmi kasutavad paljud suurfirmad ja valitsusasutused. Nagu näiteks NSA, Ameerika kaitseministeerium, IBM ja teised suurfirmad. Sellesse tootesarja kuuluv *RiskWatch for Information Systems* põhineb ISO 17799 ja US-NIST 800-26 standarditel.
Keeled: inglise keel.
Maksumus: $14500.
Standardid: ISO 17799, ISO 27001, COBIT 4.0

Kasutajate treening 2 päeva mille maksumus 1000$
(Parts, A. 2003, RiskWatch, 2008)

2.3.4 EBIOS

Prantsuse infoturbeasutuse DCSSI poolt on väljatöötatud riskihaldus meetod ja programm EBIOS. See oli algul mõeldud ainult riigiasutuste jaoks, kuid nüüd on see vabalt kättesaadav kõigile ja on populaarne paljudes organisatsioonides. Teda on lihtne kasutada, ta on põhjalike juhenditega ja kooskõlas enamiku infoturbe standarditega.
Keeled: inglise, prantsuse, hispaania, taani
Maksumus: tasuta.
Standardid: ISO 13335, ISO 15408, ISO 17799.
(EBIOS, 2008)

2.3.5 GSTOOL

BSI on oma metoodika toeks arendanud ka automatiseeritud turbehaldusvahendi – *IT Baseline Protection Tool* - GSTOOL. GSTOOL on tarkvara, mille abil on kasutajatel võimalik luua, administreerida, täiendada *"IT Baseline Protection Manual"*-il põhinevat turvalisuse kontseptsiooni. GSTOOL võimaldab:

- koguda infot IT süsteemist ja IT struktuurianalüüsist;
- koguda infot tarkvara rakendustest;
- määratleda turvanõudeid;
- määratleda turvameetmetest;
- hinnata investeeringuid;
- genereerida aruandeid;

Keeled: saksa, inglise
Maksumus: 900 eurot.
Standardid: ISO/IEC 17799, ISO/IEC 27001.
(BSI GSTOOL, 2008)

2.3.6 ISKE

ISKE on infosüsteemide kolmeastmeline etalonturbesüsteem. ISKE väljatöötamisel ja arendamisel on aluseks võetud Saksamaa BSI poolt avaldatav infoturbe standard – IT *Baseline Protection Manual.*

ISKE rakendamise eesmärgiks on tagada infosüsteemides töödeldavatele andmetele piisava tasemega turvalisus. Süsteem on loodud eelkõige riigi ja kohaliku omavalitsuse andmekogude pidamisel kasutatavatele infosüsteemidele ning nendega seotud infovaradele turvalisuse tagamiseks. ISKEt saavad kasutada ka äriettevõtted oma IT varadele turvalisuse tagamiseks. ISKE ei ole mõeldud riigisaladust käitlevate infosüsteemide turbeks. ISKE rakendusjuhendi esimene versioon valmis 2003. aasta oktoobrikuus.

ISKEs on kirjeldatud kolme turbe taset – madal (L), keskmine (M) ja kõrge (H). Vastav turbetase määratakse andmetele turvaklasside (turvaosaklasside) määramise kaudu. Turvaklasside määramisel lähtutakse teabe konfidentsiaalsusest, teabe terviklikkusest, aegkriitilise teabe käideldavusest, teabe hilinemise tagajärgede lubatavast kaalukusest. 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 etalonkataloogidest turvameetmed ja kontrollitakse mooduli turvalisust ohtude etalonkataloogi abil.
Maksumus: tasuta
Keeled: eesti
Treening: 1päev - 1800 EEKi.
(ISKE, 2008)

2.3.7 Eesti Ühispanga etalonturbesüsteem (EÜE)

Eesti Ühispanga süsteemi kirjeldus on asutusesisene turvadokument, mida on (pärast teatavat töötlust ja mõnede osade väljajätmist) avaliku versioonina viimasel ajal tutvustatud ka avaliku halduse ringkondades ja mujal. Informaatikakeskuse tellimusel koostatud avalik versioon

pärineb 31. juulist 2003.

Eesti Ühispanga süsteem lähtub USA energeetikaministeeriumi standardist , millele on püütud lisada erinevaid turvatasemeid ning nendest lähtuvaid turvanõudeid, millest on sõltuvaks tehtud turvameetmed ning nende omadused.

Alussüsteemi kohandamise aluseks on võetud Andmekaitse Inspektsiooni etalonturbesüsteemi astmelise turbe metoodika ning sealt tulenevad 4x4 turvaosaklassi, mille puhul turvaeesmärk on jagatud teabe hilinemise tagajärgede lubatavaks kaalukuseks, aegkriitilise teabe käideldavuseks, teabe tervikluseks ja teabe konfidentsiaalsuseks. Ühispanga sisestandardis on sellele 4x4-mudelile turvameetmete eri gruppides peale ehitatud kolme- kuni neljatasemeline turvameetmete jaotus, mis on viidud vastavusse sellise 4x4-skeemiga ehk Andmekaitse Inspektsiooni turvastandardi turvaklassidega.

Selles turbesüsteemis jagatakse infovarad ja neile rakendatavad turvameetmed järgmisse nelja rühma:

- turbe organisatsioon,
- infrastruktuur,
- IT vahendid,
- talitluse pidevus,

Nendes neljas rühmas eristatakse kokku 24 väiksemat allrühma, mille kohta määratletaksegi kolme- kuni neljatasemelised turvanõuded. Liigitus ja tasemeteks jaotus vastab seejuures suures osas USA energeetikaministeeriumi standardile.
(Hanson, V. Praust, V. 2003.)

2.3.8 Sobiv alussüsteem

Kõigist läbivaadatud programmidest kõige lihtsamini kasutatav programm oli Infosüsteemide kolmeastmeline etalonturbesüsteem ISKE, mis on väljatöötatud Eestis ja mille arendamisel on aluseks võetud Saksamaa BSI poolt avaldatav infoturbe standard – IT *Baseline Protection Manual.*
Põhjused on järgmised:

1. Võrreldes teiste vaadeldud programmidega on ta lihtsalt kasutatav;

2. Turvameetmed on määratletud väga detailselt. Hästi struktureeritud ja üheselt identifitseeritud turvameetmed hõlbustavad tunduvalt turbe tüpiseerimist, eri süsteemide turbe täpset võrdlust ja turbe objektiivset auditeerimist;
3. ISKE põhineb levinuimal, kolme-eesmärgilisel turvamudelil, mida on kerge sobitada neljaeesmärgilise mudeliga;
4. ISKE on loodud riigiasutustele ning lähtudes ohusituatsioonist, mis on Eesti oludele sarnasem kui näiteks USA riigiasutuste, militaarstruktuuride või tuumaelektrijaamade oma;
5. Turbe tugevuse tagab pädev infoturbeasutus, kes on sooritanud vajalikud riskianalüüsid ja analüüsinud ka väga ulatuslikku rakenduskogemust;
6. ISKE-t täiendatakse regulaarselt ja piisavalt tihti;
7. ISKE-l on olemas väga põhjalik ohtude ja vastumeetmete kataloog;
8. Koolitus ja kasutusjuhend on eesti keeles.

PEATÜKK 3. RISKIHALDUSE PROTSESS

3.1 Eesmärk

Eesmärk on anda ülevaade riskihalduse protsessist üldiselt. Millised on tegevused mida vaja teha, et organisatsioonis toimiks süstemaatiline riskihaldus. Antakse veel ülevaade erinevatest riskianalüüsi meetoditest. Tuuakse välja nende eelised ja puudused.

3.2 Mõisted

Risk on võimalikkus, millega konkreetne oht kasutab ära nõrkused mingi vara kahjustamiseks ja seega otseselt või kaudselt organisatsiooni kahjustamiseks. (EVS ISO/ IEC TR 13335-1, 1999). Risk on ohtudest tulenevate kahjude statistiline mõõt, mida on kasulik teada objekti turvatarbe otsustamiseks ja turvameetmete valimiseks. (Hanson, Buldas, Martens, Lipmaa, Ansper, Tulit, 1997, 44).

Riski iseloomustab kaks tegurit – soovimatu intsidendi asetleidmise tõenäosus ja selle intsidendi toime. Igasugune varade, ohtude, nõrkuste ja turvameetmete muudatus võib tunduvalt mõjutada riske. Keskkonna või süsteemi muutuste varajane avastamine või teadmine suurendab võimalust rakendada riski kahandamiseks sobivaid meetmeid.

Jääkrisk Harilikult kahandavad turvameetmed riske ainult osaliselt. Tavaliselt ei ole võimalik enamat saavutadagi ja mida enam riske kahandatakse, seda suuremad on kulutused. Siit järeldub, et tavaliselt jäävad mingid jääkriskid. Organisatsiooni vajaduste ja turbe vastavuse otsustamise üks osa on jääkriski aktsepteerimine. Seda protsessi nimetatakse riski aktsepteerimiseks. (EVS-ISO/IEC TR 13335-1, 1999).

Riskihaldus on infotehnoloogilise süsteemi ressursse mõjutada võivate määramatute sündmuste tuvastuse, ohje ja välistamise või minimeerimise protsess tervikuna. Riskihalduse tegevused on kõige tõhusamad, kui nad leiavad aset süsteemi kogu elutsükli kestel. Riskihalduse protsess ise on suur tegevuste tsükkel. Uute süsteemide puhul saab hõlmata kogu tsükli, olemasolevate

süsteemide korral võib aga riskihalduse algatada süsteemi elutsükli suvalises punktis. Strateegia võib ette kirjutada läbivaatuste sooritamist süsteemi elutsükli teatud punktides või ettemääratud aegadel. Eelmisele läbivaatusele võivad järgneda järeltoimingud turvameetmete rakendamise edenemise kontrolliks. Võib ilmneda vajadus sooritada riskihaldust süsteemide projekteerimise ja väljatöötamise ajal, et tagada turbe projekteerimine ja teostamine ökonoomia seisukohalt kõige õigemal ajal. Kui plaanitakse süsteemi olulisi muudatusi, tuleks algatada ka riskihaldus.

Millist riskihalduse metoodikat ka ei kasutataks, on oluline saavutada tasakaal turvameetmete piiritlemisele ja teostamisele kulutatud aja ja ressursside minimeerimise vahel, tagades ühtlasi kõigi süsteemide asjakohase kaitse. (EVS- ISO/IEC TR 13335-1, 1999)

Riskianalüüs tuvastab riskid, mis nõuavad reguleerimist või aktsepteerimist. Infoturbe kontekstis hõlmab infotehnoloogiliste süsteemide riskianalüüs varade väärtuste, ohtude ja nõrkuste analüüsi. Riskid hinnatakse potentsiaalse toimena, mida põhjustaks konfidentsiaalsuse, tervikluse, käideldavuse, jälitatavuse, autentsuse või töökindluse rikkumine. Riskianalüütilise läbivaatuse tulemus on varade tõenäoliste riskide tuvastamine.

Riskianalüüs on riskihalduse osa – see on protsess, kus hinnatakse ja kirjeldatakse süsteemis varitsevaid ohte, süsteemi nõrkusi, varasid, millest süsteem koosneb, mida süsteem töötleb ja millele süsteem ligipääsu võimaldab, süsteemis rakendatud turvameetmeid, ning kõige selle läbi tuuakse välja süsteemiga seotud olulisemad riskid. Riskianalüüsi väljundit kasutatakse selleks, et olulisemaid riske vähendatakse sobivaid turvameetmeid rakendades nii, et nad jääksid etteantud piiridesse. Tihti seatakse tehtavate kulutuste piir nii, et see oleks enam-vähem võrdne võimaliku maksimaalse kahjuga pärast nende turbekulutuste tegemist.

Riskide vähendamine võib tähendada süsteemi muutmist, kasutajate teavitamist, teatud varade eraldamist süsteemist jne. Riskianalüüsi hinnangud peavad olema võimalikult täpsed ja soovitatavalt rahasummades väljendatud, vastasel juhul ei ole sellele järgnevad sammud kuigi efektiivsed. (EVS- ISO/IEC TR 13335-1, 1999).

Edukat riskihaldust iseloomustab:

1. reaalsed, stabiilsed ja arusaadavad nõudmised kasutajale, mis on toetatud juhtkonna poolt;

2. hea koostöö erinevate üksuste vahel;
3. korralikult planeeritud riskihaldusprotsess, mis on seotud teiste protsesside ja programmidega;
4. selgeks tehtud riskid ja läbiviidud riskianalüüs;
5. koostatud ja rakendatud riskivähendamis plaan;
6. jätkuv riskihaldus plaan;
7. korralikult dokumenteeritud riskihaldus protsess.

3.3 Riskihaldusest üldiselt

Käesolev osa puudutab riskianalüüsi ja -haldamist üldiselt ning riskianalüüsi protsessi. Eduka riskianalüüsi ja -halduse tagamiseks peab organisatsiooni üldine teabeturbe poliitika määratlema vähemalt järgneva:

1. milline on isikute ring, kes on kaasatud riskianalüüsi ja riskihaldamise protsessi – näiteks juhtkonna esindaja, projektiga töötavad isikud, süsteemi vastutavad käitajad, julgeolekupersonal ja riigisaladuse kaitset korraldav isik;
2. milline on riskianalüüsi ja riskihaldamise struktureeritud protsess (läbi viidavad kas käsitsi või automatiseeritud töövahendit kasutades), ning millised on protsessi staadiumid.

Näiteks kuuluvad siia alla järgnevad tegevused:

- riskianalüüsi ulatuse ja eesmärgi kindlaksmääramine;
- süsteemi olulise riist- ja tarkvara (ehk materiaalsete varade) väärtuse hindamine;
- infovarade väärtuse hindamine avaldamise ja avalikustamise, lubamatu muutmise, käideldamatuks muutmise ja hävimise suhtes;
- asjassepuutuvate ohtude ja nendega seotud haavatavuste väljavalimine;
- kindlakstehtud ohtude ja haavatavuste mõju süsteemile;
- olemasolevate vastumeetmete kindlaksmääramine;
- vajalike vastumeetmete kindlaksmääramine ja võrdlus olemasolevate vastumeetmetega;
- riskide ja soovitatavate vastumeetmete ülevaade;
- riskianalüüsi aruande koostamine, mis sisaldab rakendatavate vastumeetmete kirjeldust ning jääkriski kirjeldust.

Esmase riskianalüüsi protsessi tulemusena saadav teadmistebaas tuleb säilitada ja seda peab kasutama hilisemate täienduste alusena.

Riskianalüüsi on protsess, mille käigus tuvastatakse julgeolekuriske, st. ohte ja haavatavusi, nende mõju süsteemile ja määratakse kindlaks valdkonnad, mis nõuavad tehnilisi ja mittetehnilisi vastumeetmeid. Riskianalüüs aitab määratleda olemasolevaid riske, identifitseerida süsteemi olemasoleva turvalisuse tase ning koguda teavet, mis on vajalikud efektiivsete ning piisavate turvameetmete valimiseks.

Riskianalüüs aitab otsustada, milliseid ja millisel määral tehnilisi ja mitte-tehnilisi turvameetmeid kasutada. Riskianalüüsil antakse hinnang ka lubatavale jääkriskile. Riskianalüüsi protsessi läbiviimise lisakasuks on ka organisatsiooni töötajaskonna (tippjuhist kuni abipersonalini) suurenenud turvateadlikkus.

Kuna süsteemi loomise ajal on turvameetme rakendamine lihtsam ja efektiivsem kui hilisem meetmete kasutuselevõtmine, tuleks esmane riskianalüüs läbi viia projekti planeerimisstaadiumis ning seda hiljem täpsustada ja täiendada.

Riskianalüüsi protsess ei ole ühekordne ja lõplik tegevus. Seda tuleb läbi viia regulaarselt, eriti juhtudel kui muutuvad süsteem või süsteemile avalduvad ohud või süsteemi haavatavus, samuti siis kui muutub organisatsiooni ise.

Riskianalüüsi läbiviimiseks planeeritava aja hulk peab oleva vastavuses soovitava eesmärgiga. Väga lihtsate süsteemide hindamiseks ei peaks kasutama keerulisi meetodeid või riskide hindamise automatiseeritud vahendeid. Keerukas süsteem, suure hulga informatsiooni ja suure hulga erinevate kasutajate arvu ning paljude ühendustega teistesse süsteemidesse vajab aga kindlasti formaalset struktureeritud lähenemist ning seetõttu vajab rohkem ressursse (aeg, inimesed, raha).

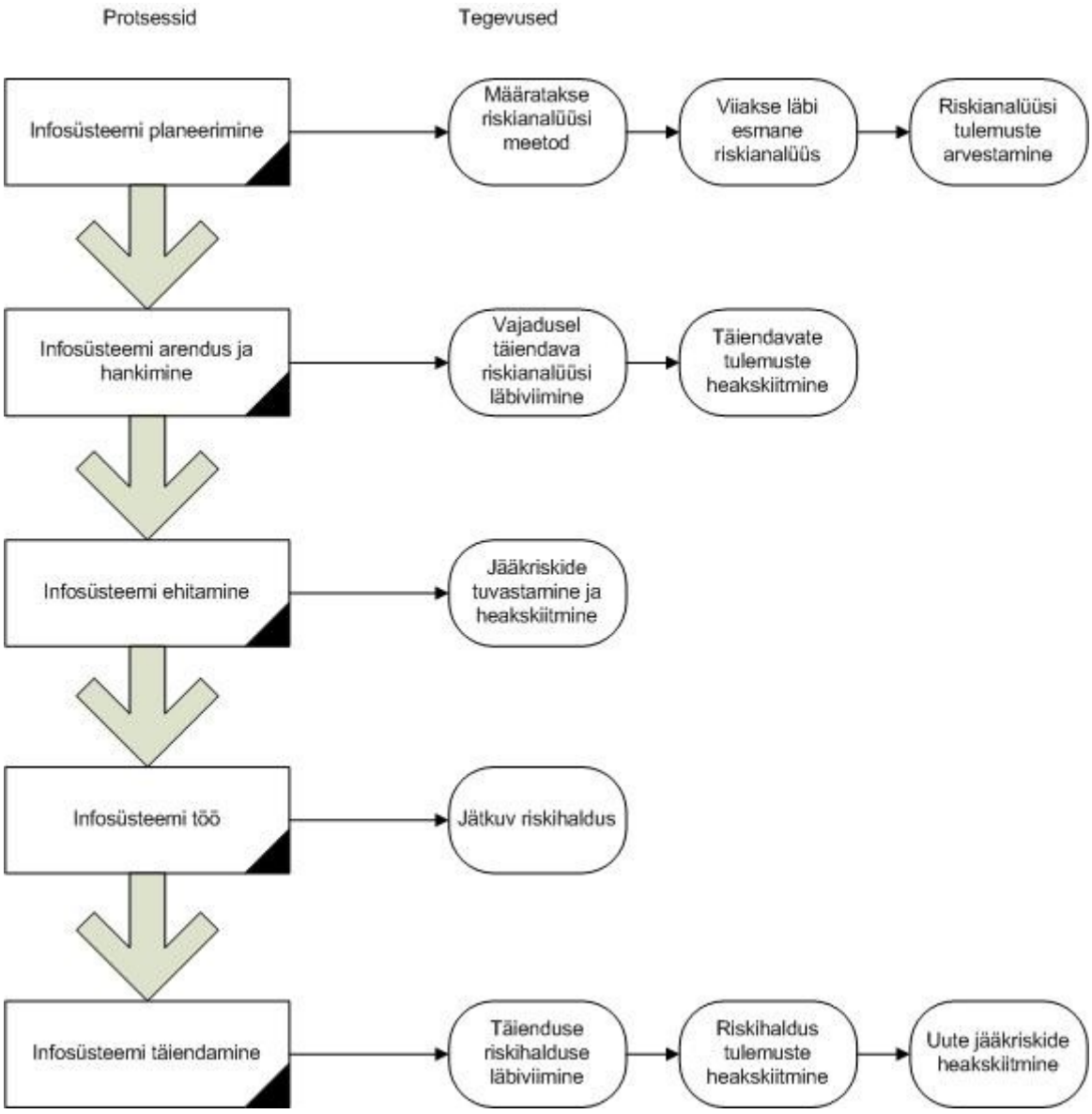
Riskianalüüsi läbiviimine sõltub juhtkonna osast selles protsessis. Juhtkond peab olema teadlik riskianalüüsi vajadusest, eesmärkidest ja ulatusest, seejärel peab olema protsessile toetus erinevatel organisatsiooni tasemetel ning riskianalüüsi tulemused peab juhtkond üle vaatama ja heaks kiitma.

3.3.1 Riskianalüüs ja riskihaldus infosüsteemi elutsükli jooksul

Süsteemi elutsükli (sh kasutusaja) jooksul sooritatakse reeglina järgnevad tegevused:

1. süsteemi planeerimine:
   - määratakse riskianalüüsi vajadus ning riskianalüüsi ja riskihalduse metodoloogia;
   - viiakse läbi esmane riskianalüüs;
   - kiidetakse heaks esmase riskianalüüsi tulemused ning arvestatakse neid süsteemi lõplikul planeerimisel.
2. süsteemi arendus ja hankimine:
   - vajadusel viiakse läbi täiendav riskianalüüs;
   - vajadusel kiidetakse heaks täiendava riskianalüüsi tulemused.
3. süsteemi ehitamine / töölerakendamine ja akrediteerimine:
   - tuvastatakse ja kooskõlastatakse vastuvõetavad jääkriskid;
   - identifitseeritakse edasine riskihalduse protsess.
4. süsteemi töö:
   - sooritada jätkuvalt riskihaldamist.
5. süsteemi täiendamine:
   - läbi viia täienduse ja kogu süsteemi riskianalüüs;
   - heaks kiita täienduse ja kogu süsteemi riskianalüüsi tulemused;
   - üle vaadata ja nõustuda vastuvõetava jääkriskidega;
   - üle vaadata ja nõustuda edasise jätkuva riskihalduse protsessiga.

(Stoneburner G, Goguen A, and Feringa A. 2001)



Joonis 1: Riskihaldus infosüsteemi elutsükli jooksul. Autor

3.3.2 Riskianalüüsi meeskond

Riskianalüüsi meeskonna koosseis on projekti eduka tulemuse seisukohast äärmiselt oluline. Oluline on, et esindatud oleksid juhtkond, projektiga töötavad isikud, süsteemi vastutavad käitajad, julgeolekupersonal ja riigisaladuse kaitset korraldav isik.

Riskianalüüsi meeskonna juht peab olema teadlik organisatsiooni tegevuse eesmärkidest, ideaalis võiks see olla süsteemi töö eest vastutav isik. Oluline on, et meeskonna juhil või vähemalt mõnel meeskonna liikmel oleks olemas varasem kogemus riski haldamise protsessist.

Riskianalüüsi meeskonna liikmed tuleb kohale määrata juhtkonna poolt.

Alternatiivina võib kasutada riskianalüüsiks erafirmasid. Seda võimalust ei tohi kasutada riskianalüüsi eesmärgi või tehnika mõistmise asemel, vaid pigem ressursside efektiivsemaks ärakasutamiseks. Valitud tööettevõtjal peavad olema vastavad kogemused, ta peab olema läbinud vajadusel vastava julgeolekukontrolli ja tööettevõtja töötajad peavad olema läbinud vajadusel vastava personaalse julgeolekukontrolli. (ISP205, 2005)

3.3.3 Riskianalüüsi protsess

Riskianalüüsi protsess on andmete kogumise ja hindamise protsess, mis puudutab kahte põhilist küsimust:

- mis on hinnatava objekti väärtus (nii infotehnoloogiline, materiaalne kui julgeolekulik);
- milline on mõju või tulemus varadele, kui identifitseeritud ohud ka tegelikult aset leiavad (st. riski tase).

Riskianalüüsi protsessi eesmärgiks on määrata süsteemile riskile vastav turvaprofiil. Riskianalüüsi tulemuseks on turvastrateegia, mis annab piisava kaitse süsteemi varadele.

Riskianalüüsi protsessi saab jagada järgmisteks etappideks:

1. riskikeskkonna ulatuse ja eesmärgi määramine;
2. materiaalsete ja andmevarade kindlaksmääramine, mis aitavad kaasa süsteemi eemärgi või organisatsiooni missiooni täitmisele;
3. materiaalsete varade väärtuse või tähtsuse kindlaksmääramine. Materiaalsete varade hulka kuuluvad riistvara, tarkvara, erivarustus ja nendega seotud dokumentatsioon;
4. infovarade väärtuse ja tähtsuse määramine järgnevate mõjutuste suhtes: loata avaldamine, muutmine, kättesaadamatus ja hävitamine (käideldavus, konfidentsiaalsus, terviklikkus);
5. ohtude ja võimalusel nende suuruse identifitseerimine;
6. haavatavuste ning tõenäosuse, et seda haavatavust ära kasutatakse, identifitseerimine;
7. nõuete määratlemine turvamehhanismidele;
8. olemasolevate vastumeetmete identifitseerimine;
9. vajalike uute vastumeetmete määratlemine ja võrdlus olemasolevate vastumeetmetega, sh juba rakendatud vastumeetmete identifitseerimine ja soovitatavate vastumeetmete

identifitseerimine;

10. riskide ja planeeritavate vastumeetmete ülevaatamine arvestades järgnevat:

- materiaalsete ja infovarade kaotuse vältimine – eesmärgiks on rakendada vastumeetmeid, et vältida kaotusi nii palju kui võimalik, arvestades, et teatud riske ei saa tehnoloogilistel või protseduurilistel põhjustel kõrvaldada;
- materiaalsete ja infovarade kaotuse piiramine – eesmärgiks on rakendada vastumeetmeid sel määral, et kaotused oleks piiratud aktsepteeritava tasemega;
- materiaalsete ja infovarade kaotuse riski aktsepteerimine – kus võetakse vastu otsus aktsepteerida riski ja tulemusi, näiteks juhul kui kaotuste maksumus / mõju on
- tähtsusetu või peetakse kaotuse tõenäosust piisavalt väikeseks või on vastumeetmete maksumus palju suurem või mittetasakaalus hinnatavate kaotuste maksumuse /tähtsusega.

11. riskihalduse aruande koostamine, mis sisaldab rakendatavate vastumeetmete kirjeldust ja jääkriski kirjeldust. (Stoneburner G, Goguen A, and Feringa A. 2001)

3.3.4 Riskikeskkond

Esimene ülesanne riskikeskkonna identifitseerimisel on informatsiooni hankimine süsteemi ümbritseva keskkonna kohta, millel võib olla mõju riskianalüüsile. Siia kuuluvad näiteks organisatsiooni rajatiste joonised või skeemid, süsteemiga seotud rajatised, andmekandjate hoiustamise/säilitamise rajatised, andmete sisestamise / väljastamise piirkonnad, terminalide / tööjaamade piirkonnad, tavakasutajate ligipääsu piirkonnad, süsteemi seadmete piirkonnad, kommunikatsioonirajatised ja üldised administratiivsed / kontorite piirkonnad jne. Lisaks tuleb hankida ka näiteks elektrivarustuse, kütte, ventilatsiooni ja õhukonditsioneerimise skeemid. Paljud ülalnimetatud joonised ja skeemid on vajalikud ainult esialgse riskianalüüsi käigus. (ISP205, 2005)

3.3.5 Materiaalsete ja infovarade väärtuse hindamine

Järgmiseks sammuks on materiaalsete ja infovarade väärtuse hindamine.

Materiaalsete varade puhul, mille hulka kuuluvad riistvara, tarkvara, erivarustus ja nendega seotud dokumentatsioon, on väärtuseks nende asendamise või ehitamise väärtus, millele

lisatakse nende mittemateriaalne väärtus (nt. algoritm krüptograafilises vahendis või kiipkaardile salvestatud võti).

Infovarade korral saab väärtust kindlaks teha küsitledes teabe omanikke või teisi isikuid, kes on võimelised hindama infovarasid. Väärtuse, mis võib olla kvalitatiivne faktor (näiteks madal, keskmine või kõrge), võib saada „informatsiooni omanikelt“ või nende esindajatelt saadavast informatsioonist ja see tuleneb kõige halvemast stsenaariumist järgnevates olukordades:

1. hävimine;
2. kättesaadamatus;
3. avaldamine autoriseerimata isikutele;
4. muutmine autoriseerimata isikute poolt.

3.3.6 Ohud ja haavatavused

Üldiselt on küllalt lihtsalt võimalik luua süsteemile tavaohtude nimekiri. Selle koostamiseks võib korraldada riskihaldusmeeskonna ajurünnakuid või leida selline ohtude nimekiri Internetist. Kõik kaasaegsed riskianalüüsi automaatsed töövahendid sisaldavad ohtude nimekirja.

Teiselt poolt pole haavatavused kunagi püsivad ja sõltuvad näiteks tehnoloogia arengust ja süsteemi kasutajatest. Seetõttu tuleb iga punkti potentsiaalsete haavatavuste nimekirjas vaadelda tegeliku riskikeskkonna seisukohast ja hinnata nende potentsiaalsete haavatavuste avastamise tõenäosust. Seda saab teha näiteks rajatise tegeliku inspektsiooni abil või intervjueerides vastavat personali.

3.3.7 Olemasolevad vastumeetmed

Järgmiseks sammuks on määrata ja dokumenteerida kõik süsteemis juba olemasolevad vastumeetmed riskikeskkondade kaupa.

3.3.8 Soovitatavad uued vastumeetmed

Pärast seda, kui on identifitseeritud kõik infovarad ja (võimalusel) materiaalsed varad koos nende väärtusega riskikeskkondade kaupa koos ohtude ja haavatavustega, on järgmiseks

sammuks määrata kindlaks soovitatavad turvavastumeetmed.

See saavutatakse tegeldes iga materiaalse või infovaraga või varade rühmaga, uurides ohte ja haavatavusi ning identifitseerides turvavastumeetmed. Teistpidi saab seda teha võttes iga identifitseeritud ohu ja haavatavuse ning vaadelda iga materiaalset või infovara, mida saab mõjutada ning määrata seejärel kindlaks vastumeetmed. Tuleb meeles pidada, et ohul on tähtsus ainult siis, kui esineb haavatavus, mida saab ära kasutada. Teistpidi muutub haavatavus ainult siis oluliseks, kui esineb oht, mis seda võib ära kasutada.
Vastumeetmeid identifitseerides tuleb lisaks arvestada seadusandluses esitatud riigisaladuse kaitsemeetmetega.

3.3.9 Riskianalüüsi protsessi kokkuvõte

Riskianalüüsi protsessi lõpus peab tulemuseks olema turvameetmete nimekiri. Seda nimekirja peab võrdlema olemasolevate meetmetega ja koostama soovitatavate vastumeetmete nimekirja. Protsessi viimaseks staadiumiks on soovitatavate vastumeetmete ülevaatamine juhtkonna poolt ning kokkuleppimine kontrolliva asutusega.

Kui riskianalüüsi protsess on lõpetatud ja on saavutatud kokkulepe vastumeetmete lõpliku nimekirja osas, tuleb turvalisusega seotud dokumentatsioonis välja tuua hindamise tulemused ning riskianalüüsi protsessi käigus saadud oluline informatsioon. See informatsioon tuleb lisada süsteemi turvanõuete loetellu.

Turvalisusega seotud dokumentatsioonis peab käsitlema järgnevat riskide hindamise käigus saadud infot:

- riskianalüüsi eesmärk ja ulatus;
- riskianalüüsi metodoloogia;
- varade, mõjude, ohtude ja haavatavuste identifitseerimine;
- soovitused vastumeetmete gruppide osas;
- aktsepteeritavad jääkriskid. (ISP205, 2005)

3.4 Riskianalüüsi meetodid

Järgnevalt on kirjeldatud erinevaid lähenemisi infosüsteemide riskianalüüsile.
Riskihalduse üks alamülesandeid ongi sobiva meetodi valik ja meetodi kohandamine oma vajadustele. Liiga suurt täpsust taotledes kulub palju ressursse ja töö ei pruugigi valmis saada, samas aegub täpne riskianalüüs kiiresti. Liiga üldine analüüs aga ei oma märkimisväärset rakendusväärtust. Seega on meetodi valik oluline. Järgnevad meetodid ei ole alati üksteist välistavad, neid saab tihtipeale edukalt kombineerida.

Ülevaade hõlmab nii standardites kui muudes juhendmaterjalides käsitletud riskianalüüsi meetodeid, tuues välja nende kasutatavuse tingimused ja probleemid vastava metoodika rakendamisel.

Turbehalduse standardites käsitletavad riskihalduse metoodikad koosnevad sisuliselt kahest osast – riskianalüüsist ning selle tulemite alusel turvameetmete plaanimisest.
Tegelikult seisneb ka riskihalduse meetodite põhierinevus ikkagi riskianalüüsi osas, st selles, kuidas tuvastatakse turvarisk.

Riskianalüüsi tüüpidena võiks veel eraldi rääkida kvalitatiivsest ja kvantitatiivsest analüüsist. Kuna kahjud ei ole alati materiaalsed, siis ei ole nad ka alati võrreldavates ühikutes väljatoodavad. Kvalitatiivse analüüsi puhul üritatakse leida kõigile turvaaspektidele ligikaudsed tasemehinnangud ning nende abil tuvastada riskantsemaid kohti süsteemis. Kvantitatiivse analüüsi puhul üritatakse kõiki aspekte kirjeldada samades ühikutes. (Parts, A. 2003)

3.4.1 Kvantitatiivne riskianalüüs

Kvantitatiivse riskianalüüsi korral taandatakse kõik rahale: hinnatakse ohtude suhtelisi sagedusi ja raha suurust, mis on tarvilik, et need ohud saaksid kasutada ära teatud nõrkusi. Nii varade väärtust kui ka kahju suurust hinnatakse rahaliselt, ka ainetute varade väärtusele püütakse anda rahaline hinnang. Kõik arvutused sooritatakse tõenäosustena rahalisel skaalal.

Selle meetodi kasutamine eeldab:

- kõikide varade detailset spetsifitseerimist;
- kõikide ohtude ja nende esinemissageduste spetsifitseerimist;
- kõikide varade kõikide nõrkuste hindamist ründeks vajaminevate rahaliste kulutustega;
- ohtude ja ohustatud varade kokkuviimist kõikide varade korral;
- põhjalikke matemaatilisi arvutusi (reeglina on abivahendina kasutusel spetsiaalne küsimustik või tarkvara).

Meetodi eelis:

- kui arvandmed nii ohtude realiseerimise sageduse kui ka nõrkuste ründe summade kohta on olemas, annab kvantitatiivne riskianalüüs küllalt täpse tulemuse.

Meetodi puudused:

- suur töömahukus ja ressursikulu (ohte ja nõrkusi on sadu);
- tõenäosuste leidmiseks vajalik ohtude statistika võib puududa või olla ebatäpne, mis teeb selle meetodi pruukimise raskeks. (Parts, A. 2003)

Riigisaladust töötlevate infosüsteemide puhul on raske sellist meetodit kasutada, kuna raske on anda sellisele infole rahalist väärtust. Ei saa kasutada ka teiste riikide kogemust, kuna selline info on kinnine ja avalikult selliseid andmeid ei esitata.

3.4.2 Kvalitatiivne riskianalüüs

Kvalitatiivne riskianalüüs on ohtude toime hindamine, kus hinnatakse väärtuste asemel väärtuste tinglikke ja jämedaid astmikke. Tavaliselt on kasutusel 3-4 astet (nt suur- keskmine- väike). Ka teadaolevad täpsed rahalised väärtused viiakse sellisele kujule. Kvantitatiivselt raskesti mõõdetavate väärtuste puhul kasutatakse ka empiirilisi ja subjektiivseid eksperthinnanguid. (Parts, A. 2003)

Reeglina võetakse jämeda skaala põhjal arvesse järgmised tegurid:

- vara ahvatlevus (ründe puhul);
- hõlpsus, millega vara on muundatav hüvituseks (ründe puhul);
- ründaja tehnilised võimalused;
- nõrkuste ärakasutatavuse määr;

- ohu tegeliku realiseerumise sagedus;

Meetodi eelised:

- lihtsam on kajastada mitterahalisi väärtuseid;
- protsess on väiksema mahuga ja seega kiirem;

Meetodi puudused:

- realiseerumissageduste kohta on kasutuskõlblikke andmeid raske saada, eriti rünnete hindamisel;
- ka füüsiliste varade väärtusi hinnatakse suhtelisel skaalal;
- erinevad inimesed võivad suhtelist skaalat erinevalt lahti mõtestada.

Kvantitatiivne ja kvalitatiivne uurimus täiendavad teineteist, ei võistle, tihti ei saagi neid täpselt teineteisest eristada. Kvantitatiivseid ja kvalitatiivseid meetodeid võib kasutada paralleelselt, kui arvandmed on olemas, kasutatakse neid, kui ei ole siis kasutatakse kvalitatiivset mõõtu.
(Parts, A. 2003)

Riigisaladust töötlevate infosüsteemide puhul on selle meetodi rakendamine lihtsam kui kvantitatiivse meetodi puhul sest mitterahalist väärtust on lihtsam anda riigisaladusele.

3.4.3 Jäme riskianalüüs

Jäme riskianalüüs on infosüsteemi olulisuse ja infosüsteemi ohtude hindamine väga jämedal hinnangute skaalal. Jämedat riskianalüüsi on otstarbekas kasutada eelanalüüsiks ehk konkreetsetele oludele sobivaima riskihaldusmetoodika valimiseks.

Jämeda riskianalüüsi puhul hinnatakse:

- infotehnoloogilise süsteemi abil saavutamisele kuuluvaid tegevuseesmärke;
- organisatsiooni tegevuse sellest infotehnoloogilisest süsteemist sõltuvuse määra, st. kas funktsioonid, mida organisatsioon peab kriitiliseks oma püsima-jäämisele või tegevuse tõhusale sooritamisele, sõltuvad sellest süsteemist või selles süsteemis töödeldava informatsiooni konfidentsiaalsusest, terviklusest, käideldavusest, jälitatavusest, autentsusest ja töökindlusest;

- sellesse infotehnoloogilisse süsteemi investeerimise taset süsteemi väljatöötamise, hoolduse või asendamise terminites selle infotehnoloogilise süsteemi varade osas, millele organisatsioon otseselt omistab väärtuse.

Kui need elemendid on hinnatud, on otsuse tegemine üldiselt hõlbus. Kui mingi süsteemi eesmärgid on organisatsiooni tegevuseks tähtsad, kui süsteemi asenduskulud on suured või kui varade väärtusi ähvardab suur risk, vajab see süsteem detailset riskianalüüsi. Iga loetletud tingimus eraldi on piisav detailse riskianalüüsi sooritamise õigustuseks.
(Parts, A. 2003)

Jämeda riskianalüüsiga selgitatakse välja süsteemid, mille risk on suur või mis on eluliselt tähtsad organisatsiooni talitlusele. Jäme riskianalüüs on vajalik, et välja selgitada, milline metoodika on iga töötlussüsteemi puhul asjakohane.

Meetodi eelis:

- saab kiiresti hinnata millist riskianalüüsi meetodit kasutada infosüsteemile ja kui põhjalik see peaks olema.

Meetodi puudus:

- ainult selle meetodi kasutamisel ei suudeta hinnata kõiki riske ja infosüsteemis ei tagata piisavat turvalisust.

Riigisaladust töötlevatele infosüsteemile puhul võiks kasutada seda meetodit süsteemi projekteerimise ajal, kuid ainult seda meetodit kasutades ei saavutata piisavat turvalisust infosüsteemis.

3.4.4 Detailne riskianalüüs

Detailne riskianalüüs sisaldab varade põhjalikku väljaselgitamist ja hindamist, neid varasid ähvardavate ohtude hindamist, nõrkuste hindamist. Nende hindamiste tulemusi kasutatakse seejärel lähteandmetena riskide hindamiseks ja sellest tulenevalt põhjendatud turvameetmete väljaselgitamiseks.

Detailse riskianalüüsi puhul toimitakse alljärgnevalt:

- Hinnatakse jääkrisk - selleks kasutatakse kas kvalitatiivset või kvantitatiivset riskianalüüsi metoodikat;
- Leitakse valdkonnad, kus on jääkriski vaja vähendada;
- Rakendatakse nendes valdkondades vajalikke turvameetmeid;
- Leitakse uus jääkrisk ja hinnatakse, kas see on piisaval tasemel (võrrelduna varade väärtuse ja turvameetmete maksumusega);
- Kogu protseduuri korratakse, kuni saavutatakse aktsepteeritav jääkrisk.

Meetodi eelised:

- annab olukorrast üsna tõepärase pildi;
- arvutatud jääkrisk on suure tõenäosusega tegelik jääkrisk;
- korraliku metoodika kasutamisel ei jää "turvaauke kahe silma vahele";
- tõenäoliselt leitakse kõigi süsteemide jaoks kohased turvameetmed. (Parts, A. 2003)

Meetodi puudus:

- tulemuste saamine nõuab üsna palju aega, vaeva ja oskusi.

Riigisaladust töötlevates infosüsteemides viiakse detailne riskianalüüs läbi kui süsteemid on piisavalt suured. Nende infosüsteemide korral, kus arenduseks kulutatavad rahalised vahendid on piiratud või arendustööle on seatud lühikesed tähtajad, detailne riskianalüüs ei sobi. Sel juhul tuleb kasutada alternatiivseid meetodeid. Kahjuks on detailse riskianalüüsi teostamine suhteliselt keerukas ja kulukas. Näiteks automatiseeritud programmiga CRAMM detailse riskianalüüsi läbiviimine keskmise suurusega infosüsteemis võtab aega spetsialistide sõnul umbes 3 kuud.

3.4.5 Eeskujul baseeruv riskianalüüs – Etalonturve

Etalonturbe meetod on peamiseks alternatiiviks detailsele riskianalüüsile juhul, kui viimast ei võimalda realiseerida rahalised või ajalised ressursid. Sisuliselt tähendab see riskianalüüsi taandamist analüüsile, kas etaloniks olnud süsteemi riskitase on sama suur või kõrgem, kui vaadeldaval süsteemil. Etalonturvet rakendataksegi reeglina samatüübiliste äriprotsessidega asutuste korral (näiteks riigiasutused, finantsinstitutsioonid jms.).

Astmeliste turvameetmete metoodika on etalonturbe metoodika edasiarendus, kus

infosüsteemide turvanõuded (konfidentsiaalsusele, käideldavusele, terviklusele) jagatakse astmeteks (tasemeteks 0 kuni 3) ning kus on loetletud vajalikud turvameetmed turvanõuete kõigi astmete täitmiseks – st astmeliste turvameetmete metoodikaga määratakse turvanõuete vajalikele astmetele vastavad vajalikud turvameetmed ja nende astmed. Turvanõuded esitavad süsteemile info valdajad ning määravad sellega infosüsteemi turvaklassi, mis omakorda määrab vastava infosüsteemi infoturbeks vajalike turvameetmete kompleksi. Saadud vajalike turvameetmete kompleks tagab, et asutuse jaoks on turvariskid majanduslikult optimaalselt maandatud. (Kivimaa, J. 2004)

Etalonturbe metoodika on metoodika,- kus teatud loetletud turvameetmete rakendamise korral on keskmise (riigi)asutuse jaoks turvariskid maandatud. Meetod põhineb mõnegi tunnustatud organisatsiooni, näiteks *Bundesamt für Sicherheit in der Informationstechnik(BSI)* – Saksamaa Infoturbe Liiduamet, eelnevatel kogemustel ja/või teostatud riskianalüüsil.
Etalonturbe metoodika korral on ette antud komplekt kohustuslikke turvameetmeid, millest kõikide realiseerimine peaks tagama teatud etalontaseme turbe (jääkriski) kõikide süsteemide kaitseks mingil etteantud (etalon)tasemel. Nõutava kaitsetaseme saavutamiseks tuleb selline etalonmeetmestik rakendada täielikult, midagi välja jätmata. (Parts, A. 2003)

Meetodi eelised:

- mistahes muu riskianalüüsi meetodiga võrreldes kulub vähem ressursse - aeg, raha, töö, spetsialistid;
- samu meetmeid saab rakendada paljudele erinevatele süsteemidele.

Meetodi puudused:

- kui etalontase on liiga kõrge, võib mõnede süsteemide turve olla liialdatud;
- kui tase liiga madal, võib mõnede süsteemide turve jääda ebapiisavaks - jäävad liiga suured jääkriskid;
- võib tekkida raskusi turvalisust puudutavate muutuste halduses. (Näiteks süsteemi moderniseerimisel võib olla raske otsustada, kas algsed etalonturvameetmed on endiselt piisavad);
- unikaalse arhitektuuriga infosüsteemide korral võib mõni valdkond jääda katmata ja tekitada ülisuure turvariski.

Arvestades magistritöö tõstatatud probleemi, leiab autor, et etalonturbemeetod sobib kõige

paremini üheks kasutatavaks riskianalüüsi meetodiks riigisaladust töötlevates infosüsteemides.

3.4.6 Segametoodika

Segametoodika võtab nii detailsest riskianalüüsist kui ka etalonturbe metoodikast üle mitmeid häid omadusi, leides nende vahel mõistliku kompromissi.

Segametoodika kaks peamist võtet:

1. Etalonturbe metoodikad (etalonmeetmete komplektid) on välja töötatud mitme erineva turvataseme (käideldavus- terviklus- ja konfidentsiaalsus taseme) jaoks;
2. Infosüsteemi kriitilistes valdkondades ja unikaalse arhitektuuriga osades kasutatakse detailset riskianalüüsi, mujal aga odavamat etalonturbe metoodikat.

Meetodi eelised:

- riskianalüüsiga võrreldes on ta vähem ressursimahukam;
- etalonmetoodikaga võrreldes võimaldab ta samas infosüsteemide (infovarade) ja nende komponentide lõikes individualiseeritumat lähenemist.

Meetodi puudused:

- võrreldes detailse riskianalüüsiga annab ta siiski vähem tõepärasema pildi;
- võrreldes etalonmetoodikaga on ta kallim. (Parts, A. 2003)

Riigisaladust töötlevatele infosüsteemidele sobib see riskianalüüsi metoodika kõige paremini, sest enamus riigisaladust töötlevaid infosüsteeme on standardse ehitusega ja vähesed süsteemid erinevad oma suuruse ja ülesehituse poolest.

3.4.7 Kogemustel baseeruv riskianalüüs

Kogemustel baseeruv riskianalüüs on kiire ja vähese vaevaga läbi viidav. Sedasorti analüüs ei baseeru mitte niivõrd ressursside ja riskide objektiivsel hindamisel, vaid administraatorite ja analüütikute kogemusel. Seega on kogemustel baseeruva riskianalüüsi õnnestumiseks vaja kogemustega läbiviijaid. Paraku on sellisel lähenemisel palju varjukülgi. Kergesti tekib piiratud maailmavaate või silmaklappide efekt: nähakse vaid seda tüüpi riske, millega ollakse seni tuttav.

Saavutamata võib jääda üks riskianalüüsi põhieesmärke: selgitada välja ka administraatorile seni tundmata ohud/riskid. Samuti ei ole selline analüüs väga paindlik muutuvates oludes, kus ressursside väärtus ja riskid kiiresti muutuvad.

Kasutatakse juhul, kui:

- riskianalüüs on vaja läbi viia väga kiiresti;
- etalonturbemetoodikaid ei ole või neid ei saa mingil põhjusel kasutada;
- on olemas arvestavate kogemustega spetsialistid.

Meetodi eelised:

- pole vaja õppida uusi oskusi ja tehnikaid;
- saab läbi viia väiksemate ressurssidega (odavamalt) kui detailset riskianalüüsi.

Meetodi puudused:

- struktuursuse eiramisega kaasneb alati risk jätta midagi olulist kahe silma vahele;
- kogemused võivad olla subjektiivsed või sageli hoopis puududa;
- kulutused turvameetmetele ei ole (juhtkonna ees) piisavalt põhjendatud;
- suured probleemid analüüsi läbiviija töölt lahkumisel või töösuhte lõpetamisel.

3.4.8 Kokkuvõte erinevatest riskianalüüsi meetoditest

Riskianalüüsi meetodi valimisel on kolm põhivõimalust:

- kasutada riskianalüüsi sooritamiseks kogemustel baseeruv metoodikat ning keskenduda neile infosüsteemidele, mis tunduvad olevat suurte riskide ees kaitsetud;
- kasutada kõigi infosüsteemide jaoks üht ja sama etalonmetoodikat sõltumata süsteeme ähvardavatest riskidest ning aktsepteerida asjaolu, et turvatase ei tarvitse kõikjal olla piisav;
- segametoodika – sooritada esialgne jäme riskianalüüs suurte riskide eest kaitsmata infosüsteemide ja tegevuse seisukohalt kriitiliste süsteemide väljaselgitamiseks, seejärel aga teostada niisuguste süsteemide detailne riskianalüüs, rakendades kõigile teistele süsteemidele etalonturbe meetmed.

Autori arvates sobivad vaadeldud meetoditest kõige paremini riigisaladust töötlevate

infosüsteemide jaoks etalonturbemeetod ja segameetod. Kõige parema tulemuse saab detailse riskianalüüsi meetodi puhul, aga tema suureks puuduseks on see, et ta on liiga töömahukas ja kallis. Detailset riskianalüüsi meetodit on soovitav kasutada riigisaladuse taseme täiesti salajast infot töötleva infosüsteemi puhul.

Tabelis on autor võrrelnud erinevaid riskianalüüsi meetodeid. On võrreldud aega, maksumust keerukust ja tulemust. Hindamise aluseks on eelnevate meetodite puuduste ja eeliste võrdlemine. Hindamine ajale, maksumusele ja keerukusele toimus madalast, kuni väga kõrgeni. Meetodi kasutamisel saadud tulemuse hindamine toimus rahuldavast, kuni väga hea. Tabeli koostamise eesmärk oli saada ülevaade erinevate meetoditele kuluvale ajale, maksumusele, keerukusele ja saadud tulemusele.

Tabel. Riskianalüüsi meetodite hindamine

Kriteerium: / Meetod:	Aeg	Maksumus	Keerukus	Tulemus
Jäme	madal	madal	madal	rahuldav
Detailne	väga kõrge	väga kõrge	väga kõrge	suurepärane
Etalonturbe	kõrge	keskmine	keskmine	hea
Segametoodika	kõrge	kõrge	kõrge	hea
Mitteformaalne	madal	keskmine	madal	rahuldav

Allikas: Autor

PEATÜKK 4. ETALONTURBEMEETODI ISKE ANALÜÜS

4.1 Eesmärk

Eelpool peatükkides vaadeldud riskianalüüsi programmidest ja meetoditest on kõige parem autori arvates etalonturbemeetod ISKE ja selle alusel koostatud ISKE rakendusjuhend. Vaja on metoodikat, mis tagaks riigisaladust töötlevale infosüsteemile turvameetmete määramise just selle süsteemi turvanõuete kohaselt ja poleks nii töömahukas kui detailne riskianalüüs, aga võimaldaks saavutada piisava turbetaseme. Selleks analüüsitakse allolevas peatükis Eesti Vabariigis riigi ja kohaliku omavalitsuse andmekogudes sisalduvate andmekoosseisude töötlemiseks kasutatavate infosüsteemide ning nendega seotud infovarade kaitseks hästi tuntud etalonturbemeetodi ISKE turvameetmeid.

Peatüki eesmärk on vaadelda, kas etalonturbemeetodi ISKE on täielikult rakendatav riigisaladust töötlevates infosüsteemides, või tuleb seda modifitseerida vastavalt riigisaladuse ja salastatud välisteabe seadusele ja selle alusel antud määrustes esitatud nõuetele. Selle selgitamiseks kasutab autor võrdlevat meetodit. Autor võrdleb mõningaid ISKE turvameetmeid ja Kaitseministri määruses nr. 34 esitatud põhilisi nõueteid. Meetmed on võetud ISKE lisast nr.1 ja Kaitseministri määrusest nr. 34. Iga võrreldud turvameetme lõpus teeb autor kokkuvõte selle turvameetme sobivusest.

ISKE rakendamise eesmärk on tagada järgmist:

- riigisaladus on kaitstud volitamata juurdepääsu eest;
- riigisaladuse konfidentsiaalsus on tagatud;
- riigisaladuse ja teenuse terviklus on tagatud;
- riigisaladuse ja teenuste käideldavus on tagatud;
- autentimine tagab üksnes volitatud kasutajate pääsu;
- õigusaktides ja eeskirjades/kordades esitatud nõuded on täidetud;
- asutuse infoturbe poliitika on kinnitatud ja seda rakendatakse;
- jätkusuutlikkuse ja talitluspidevuse plaanid on koostatud, rakendatud ja testitud;
- infoturbe intsidente käsitletakse asjakohaselt;

- muutused infosüsteemis on kooskõlastatud ja hallatud;

4.2 Etalonturbe olemus

Infosüsteemi turbe eest vastutavad ametnikud vajavad pidevalt kaasajastatud infoturbe metoodikat. Eestile käib sellise metoodika ülalpidamine üle jõu ning see ei ole ka otstarbekas. ISKE puhul tehtud valik on kasutada alusena Saksa infoturbeasutuse BSI poolt väljatöötatud *IT-Grundschutzhandbuch* metoodikat. Samas on Eesti asutustel oma eripära, mis on tinginud kolmeastmelise etalonturbe sisseviimise.

Etalonturve on tüpiseeritud minimaalne turvameetmestik, mida tuleb rakendada infovaradele ettenähtud turvataseme saavutamiseks ja säilitamiseks. ISKE turvameetmestik on koostatud tüüpiliste infovarade turvaanalüüsi ja nende turbe pikaajalise praktika põhjal.

"Minimaalne" tähendab seda, et nõutava turvataseme saavutamiseks tuleb rakendada kõik konkreetse infovara tüübi ja konkreetse nõutava turvataseme kohta spetsifitseeritud kohustuslikud meetmed. Lisaks on igal turvatasemel soovituslikud meetmed, mida soovitatakse rakendada, kuid mis ei ole kohustuslikud. Ühtlasi tähendab selline minimaalsus optimaalsust, sest kasvõi ühest kohustuslikust meetmest loobumine tähendab, et nõutavat turvataset ei saavutata. Muude turvameetmete põhjendamatu lisamine toob kaasa lisakulud, infovarade käideldavuse languse ja tööprotsesside aeglustumise.

Infosüsteemid töötavad pidevalt muutuvas keskkonnas, kus tekib üha uusi ohte. Seetõttu ei saa etalonmeetmestik püsida muutumatuna, vaid vajab regulaarset värskendamist. Selliste värskenduste sooritamine sagedamini kui kord aastas ei ole reaalne. Asutuste infoturbe eest vastutajail tuleb hoolikalt jälgida teavet uute ohtude kohta ja vajaduse korral rakendada lisaks etalonmeetmetele muid abinõusid nende ohtude tõrjeks. Lisaks jäävad alati ohud mida ei käsitleta ei etaloonturbes, teistes turvastandartites ega ka seadusandluses. (ISKE, 2007)

4.3 Astmeline etalonturve

Infosüsteemide turvameetmete analüüsimisel ilmneb tavaliselt, et asutuses on kasutusel

turvameetmete taseme poolest üksteisest erinevaid süsteeme. On selge, et 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 turvameetmete lisamise teel madala astme omadele ja kõrge aste saadakse teatud meetmete lisamisel keskmise astme omadele. (ISKE, 2007)

4.4 Turvameetmete liigitus ISKEs

Turvameetmed on ISKEs liigitatud teostusviisi järgi:

- Organisatsioonilised turvameetmed on ISKEs mooduli all üldkomponendid;
- Füüsilised turvameetmed on ISKEs mooduli all infrastruktuur;
- Infotehnoloogilised turvameetmed on ISKEs mooduli all IT-süsteemid.

Olulisemad on organisatsioonilised turvameetmed ilma nendeta ei toimi ka teised meetmed. Organisatsioonilised turvameetmed sisaldavad peamiselt töökorralduse ja haldusega seotud tegevusi ning toimingud.

Füüsilised turvameetmed hõlmavad objekti infrastruktuuri.

Infotehnoloogilised turvameetmed sisaldavad kõike seda, mida saab teha IT vahendite (tarkvara ja riistvara) abil. (ISKE, 2007)

ISKE jagab turvameetmed viite moodulisse:

- B1 üldkomponendid;
- B2 infrastruktuur;
- B3 IT süsteemid;
- B4 võrgud;
- B5 IT rakendused

4.5 Etalonmeetmestiku halduse korraldamine

Etalonmeetmestiku pideva turbetoime hoidmiseks nõutaval tasemel tuleb luua organisatsioonilised protseduurid, struktuuriüksused ja teavituskanalid järgmiste tegevuste sooritamiseks:

- etalonturbesüsteemi juhendi regulaarne täiendamine alussüsteemi uute versioonide ilmumisel;
- täienduste levitamine;
- kõiki või paljusid asutusi puudutavate turvasituatsiooni muutuste jälgimine ja sellest teavitamine;
- ajutiste lisameetmete koordineerimine turvasituatsiooni muutumisel.

4.6 Turvameetmete analüüs

Allpool võrreldakse ISKE turvameetmeid ja Kaitseministri määruses nr. 34 esitatud põhilisi turvameetmeid, et selgitada, kas ISKEs olevad turvameetmed on piisavad riigisaladust töötlevatele infosüsteemidele seadusandluses esitatud turvameetmetele ja kas on kaetud kõik vajalikud nõuded.

4.6.1 Paroolile esitatavad nõuded

Kõik süsteemi kasutavad isikud tuleb identifitseerida usaldusväärselt ja teha kindlaks nende õigus pääseda juurde salastatud teabele. Kõik automatiseeritud protsessid, mis töötavad konkreetse isiku heaks, peab seostama üheselt selle isikuga. Selle kindlaks tegemiseks kasutatakse paroole. Parooli kasutamise turvameetmed peavad vähendama järgnevat riski:
isikud võivad teeselda teisi isikuid, et saada juurdepääsu informatsioonile, mille jaoks nad pole läbinud julgeolekukontrolli või mida nad ei pea teadma, või sooritavad operatsioone, millest tuleb aru anda, ilma seda tegemata.

Allpool vaatleme millised turvameetmed on esitatud ISKE-s paroolidele ja kas turvameetmed on piisavad võrreldes Kaitseministri määruses nr. 34 esitatud nõuetele.

ISKE turvameede M2.11

Paroolide kasutamise reeglid turbeastme (L) meetme M2.11 puhul:

- mitte kergesti mõistatatav (auto number, sünnikuupäev, lapse nimi);
- vähemalt üks märk olgu number või erimärk;
- pikkus vähemalt 6 märki; jälgida, mitut märki kontrollib turvamehhanism;
- tehases seatud jms paroolid asendada individuaalsetega;
- salastada, teada tohib ainult kasutaja;
- eriolukordade jaoks hoida kinnises ümbrikus, kaitsta võrdselt ID-kaardiga;
- vahetada regulaarselt, nt iga 90 päeva järel;
- kui on saanud teatavaks, asendada kohe;
- pärast asendamist mitte enam kasutada vanu;
- sisestada tuleb märkamatult.

Lisareeglid, kui võimalik:

- triviaalsete (BBBBBB, 123456) valimine tõkestada;
- iga kasutaja peab saama oma parooli igal ajal muuta;
- ühekordsed: uue kasutaja alglogimisel, võrgus avatekstina edastamisel;
- kolme edutu sisestuse järel blokeering, mille saab kõrvaldada ainult süsteemiülem;
- võrgus ei tohiks autentimisel edastada avatekstina;
- sisestus varjatult, kuvamiseta;
- süsteemis salvestada kaitstult, nt krüpteeritult;
- asendamise peab perioodiliselt algatama süsteem;
- süsteem peab välistama vanade sisestuse (säilitades paroolide ajaloo).

ISKEs on näiteks parooli nõuded turbeastme (HG)puhul:

- olema vähemalt 9 märki pikk;
- sisaldama vähemalt kaks suur- ja kaks väiketähte;
- sisaldama vähemalt kaks numbrit või muud erimärki;
- olema kontrollitud parooliskanneriga nõrkade paroolide otsinguks. (ISKE, 2007)

Kaitseministri määrusest nr. 34 on paroolile nõutud:

- salasõna pikkuseks piiratud tasemega teavet töötlevas infosüsteemis 6 tähemärki ja

konfidentsiaalse ja kõrgema tasemega infot töötlevas infosüstemis 8 tähemärki;

- salasõnas peab sisalduma suur ja väike täht, erimärk või number;
- viie varasema kasutuses olnud salasõna kasutamine on keelatud;
- salasõnadel on maksimaalne kehtivusaeg (180 päeva);
- salasõnadel on minimaalne kehtivusaeg (1 päev). (RTL, 2007, 102, 1702)

Siit näeme, et ISKE kõrgema taseme (HG) turvameetmed on tugevamad, kui määruse turvameetmed. Kohe tekib kasutajal probleem, millist turvameedet rakendada. Tuleb arvestada, et määruses on kirjas minimaalsed nõuded. Riigisaladust töötlevate infosüsteemide hinnangu andmisel lähtutakse määruses esitatud turvameetmedest, ehk siis selles näites nõrgematest turvameetmetest. Samas ei ole väga hea, kui esitatakse kasutajatele liiga tugevad salasõna turvameetmed. Siis tekib oht, et kasutajad hakkavad neid üles kirjutama ja sellisel juhul võib kasutaja salasõna lihtsalt saada teatavaks teistele isikutele.

4.6.2 Teabe kustutamine

On teada, et teabe kustutamisel tavaliste operatsioonisüsteemi vahenditega ei kustuta teavet andmekandjalt täielikult ja hiljem on võimalik teatud tark- või riistvara kasutades teave andmekandjal taastada.

Kaitseministri määrusest nr. 34 tuleb nõue teabe kustutamise kohta:

- Süsteemis salastatud teabe kustutamiseks kasutatakse tarkvara, mis kirjutab kustutatava salastatud teabe üle vähemalt seitse korda. (RTL, 2007, 102, 1702)

ISKEs sellisele ohule pole tähelepanu pööratud ja sellekohane turbemeede üldse puudub.

4.6.3 Riistvara terviklikus

Kaitseministri määrusest nr. 34 tuleb nõue seadmete volitamata avamise tuvastamise kohta:

- Salastatud teavet sisaldavale töötlussüsteemi komponendile paigaldatakse selle volitamata avamise tuvastamist võimaldav vahend (nt turvakleebis, -plomm või -tross). (RTL, 2007, 102, 1702)

Võimalik on seadmetesse paigaldada pealtkuulamise või teabe lekket võimaldavaid seadmeid. Selle vältimiseks või rikkumise tuvastamiseks tuleb seadmetele paigaldada turvakleebis. ISKE-s ei ole sellist turvameedet, mis nõuaks seadmetele turvakleebise paigaldamist.

4.6.4 Logid

Logid on vajalikud infosüsteemis toimuvate tegevuste jälgimiseks. Logide abil saab tuvastada kasutajate pahatahtlike turvarikkumisi ja peavad võimaldama saada ülevaade salastatud teabega teostatavatest toimingutest (loomine, edastamine, muutmine või kustutamine jms).
Isikud, kellel on luba pääseda juurde süsteemile, võivad seda luba kuritarvitada, et:

- pääseda ligi informatsioonile, mis ei vasta nende põhjendatud teadmisvajadusele;
- sooritada muid turvalisusega seotud operatsioone (näiteks teha loata koopiaid);
- rikkuda või üritada rikkuda süsteemi turvanõudeid ilma selle eest vastustust kandmata;
- isikud, kellel ei ole luba pääseda juurde süsteemile, võivad soovida pääseda ligi süsteemile;
- muuta süsteem täielikult või osaliselt töökõlbmatuks.

Logide korrapärane ja regulaarne jälgimine peab vähendama selliseid riske.

Võrdleme ISKE logimise turvameetmete piisavust Kaitseministri määruses nr. 34 kehtestatud logimise nõuetele.

ISKE turvameetmed:
Meede M2.133
Andmebaasisüsteemi logifailide kontroll. Turbeaste (L) puhul:

- kasutajate seansside ajad ja kestused;
- andmebaasiühenduste arv;
- nurjunud ühenduskatsed;
- tupikud andmebaasisüsteemis;
- iga kasutaja S/V statistika;
- pöördused süsteemitabelite poole;
- uute baasiobjektide genereerimine;
- andmete muutmised (vajadusel + kuupäev, kellaaeg, kasutaja). (ISKE, 2007)

Meede M4.15

Turvaline sisselogimine turbeaste (L) korral.

Logimisfunktsioon peab võimaldama järgmisi meetmeid:

- nurjunud logimiskatsete arv on piiratud, seejärel blokeering;
- iga edutu logimiskatse järel pikeneb vaheaeg enne järgmist logimisviipa;
- sisselogimisel teatatakse kasutajale eelmise eduka sisselogimise aeg ja väljalogimise aeg;
- kasutaja peab saama edutu logimise korral vastava teate. (ISKE, 2007)

Meede M2.64
Logi kontroll.
Kuna logifailid on seotud isikutega, jälgida kasutamist ainult turvaotstarbel.
Kontrollida:

- kas sisse- ja väljalogimisajad on tööaja piires;
- kas ebaõnnestunud logimiste arv kasvab;
- kas volitamata pääsu katsete arv kasvab;
- kas mingi pika perioodi kohta pole logiandmeid puudu;
- kas logiandmeid pole juba liiga palju (nii et on raske jälgida);
- kas mingi kasutaja pole liiga pikalt sees. (ISKE, 2007)

Meede M2.110
Andmeprivaatsuse suunised logimisprotseduuridele .

Logimise miinimum:

- süsteemi genereerimine, süsteemiparameetrite muutmine;
- kasutajate konfigureerimine;
- õiguseprofiilide koostamine;
- rakendustarkvara installeerimine ja muutmine;
- failikorralduse muudatused;
- varundusmeetmete teostamine;
- haldusinstrumentide kasutamine;
- volitamatu sisselogimise katsed ja õiguste rikkumine.

Isikuga seotud logitavad kasutajatoimingud:

- andmesisestus;
- andmeteisaldus;
- automaatotsingud;
- andmete kustutus;
- teatavate programmide käivitus. (ISKE, 2007)

Kaitseministri määrusest nr. 34 tulenevad nõuded:

- süsteemi logiinformatsiooni säilitatakse 5 aastat;
- süsteem salvestab süsteemi kasutamise analüüsiks vajaliku informatsiooni (sh käivitamine ja sulgemine, kasutajapoolne sisenemine ja väljumine, muudatused kasutajate või kasutajagruppide kasutajaõigustes, muudatused logiinformatsiooni seadistustes, kellaaja ja kuupäeva muutmine ja ebaõnnestunud katsed süsteemi siseneda);
- süsteemis logitakse juurdepääs salastatud teabele;
- logiinformatsiooni kirje sisaldab sündmuse toimumise kuupäeva, kellaaega, liiki ja märget sündmuse õnnestumise või ebaõnnestumise kohta ning seob kasutajanime selle olemasolul logitava sündmusega;
- juurdepääs logiinformatsioonile on vastava eriõigusega kasutajal. (RTL, 2007, 102, 1702)

Selgub, et logimisele on ISKE turvameetmetes palju tähelepanu pööratud ja need turvameetmed on piisavad rakendamiseks riigisaladust töötlevates infosüsteemides.

4.6.5 Teabele juurdepääs.

Juurdepääs salastatud informatsioonile peab olema piiratud julgeolekukontrolli läbinud isikutega, kellel on põhjendatud teadmisvajadus vastava informatsiooni suhtes. Riskiks on et julgeolekukontrolli mitteläbinud isikud või isikud, kellel puudub põhjendatud teadmisvajadus informatsioonile juurdepääsuks, saavad tahtlikult või juhuslikult juurdepääsu salastatud informatsioonile või süsteemi riist- või tarkvarale, mis kaitseb salastatud informatsiooni.

ISKE-st tulenevad järgmised turvameetmed:

Meede M5.10

Piiratud õiguste andmine (juurdepääsuks serveris asuvatele failidele):

- igale ainult tööks vajalike failide juurde, vastav pääsutüüp;
- eriti piirata pääsu kataloogide ülatasemele;
- uute tarkvaratoodete installeerimisel vaadata õigused uuesti läbi;
- õiguste piiramine eriti oluline PCdel, millel on flopidraiv;
- kui serveri kettal on ruumi vähe, piirata seal kasutajale antavat ruumi. (ISKE, 2007)

Kaitseministri määrusest nr. 34 tulenevad turvameetmed:

- süsteem võimaldab juurdepääsu vaid sellisele salastatud teabele, mille suhtes töötlussüsteemi kasutajal on põhjendatud teadmisvajadus;
- süsteem võimaldab juurdepääsu vaid sellise salastatuse tasemega teabele, mille suhtes on kasutajal juurdepääsuõigus;
- seansi alustamisel ilmub kuvarile teade töötlussüsteemis töödeldava teabe salastatuse taseme ning juurdepääsu piirangute kohta;
- süsteemi mittekasutamisel 15 minutit või vähem katkeb juurdepääs teabele automaatselt ning kuvaseadmetel esitatu muutub loetamatuks;
- süsteem võimaldab kasutajal katkestada teabele juurdepääs, sh muuta kuvaseadmetel esitatu loetamatuks;
- süsteemis salastatud teabe kustutamiseks kasutatakse tarkvara, mis kirjutab kustutatava salastatud teabe üle vähemalt seitse korda;
- salastatud teavet sisaldavale töötlussüsteemi komponendile paigaldatakse selle volitamata avamise tuvastamist võimaldav vahend (nt turvakleebis, -plomm või -tross). (RTL, 2007, 102, 1702)

Võrdlusest selgub, et ISKEs antud turvameetmed ei taga kuidagi Kaitseministri määrusest tulevaid turvameetmeid. Selleks tuleb rakendada Kaitseministri määrusest nr. 34 tulevaid turvameetmeid.

4.7 Peatüki kokkuvõte

Peatükis anti ülevaade etalonturbemeetodist ISKE. Samuti vaadeldi kuidas jagunevad turvameetmed.

Eelpool analüüsiti, kas etalonturbemeetod ISKE on täielikult rakendatav riigisaladust töötlevates infosüsteemides, või tuleb seda modifitseerida vastavalt riigisaladuse ja salastatud välisteabe seadusele ja selle alusel antud määrustes esitatud nõuetele. Selleks analüüsiti ISKE turvameetmeid ja Kaitseministri määruses nr. 34 esitatud põhilisi nõueteid. Selgus, et ISKE turvameetmed on üldiselt piisavad kaitsmaks riigisaladust töötlevaid infosüsteeme, kuid mõned turvameetmed ei ole piisavad riigisaladust töötlevate infosüsteemide jaoks, võrreldes Kaitseministri määruses nr. 34 esitatavate turvameetmetega.

Riigisaladust töötlevad infosüsteemidel on kõik nõuded, mis tulenevad seadusandlusest, kohustuslikud rakendada. Ehk siis selleks tuleb ISKE madal (L) tasemele, keskmise (M) tasemele lisada juurde uus tase, mille autor on nimetanud riigisaladus (RS) tasemeks. Riigisaladus tasemele (RS) on lisatud riigisaladuse ja salastatud välisteabe seadusest ja selle põhjal välja antud määrustest tulenevad turvameetmed. Riigisaladus turbeastme (RS) on autor lisanud ISKE rakendusjuhendi andmete MS Exeli baasil tehtud rakendusele. Autor lisas veel mooduli B3.100 Identimine ja autentimine ja B3.100.1 Teabele juurdepääs. Moodulite lisamine vajadus tekis sellest, need moodulis olevad turvameetmeid ei sobinud lisada teistele meetmetele ja neid mooduli meetmeid tuleb rakendada kõigil mooduli B3 IT-süsteemid puhul.

KOKKUVÕTE

Käesoleva magistritöö üldeesmärgiks on anda ülevaade riskihaldusest ja selle läbiviimise etappidest ning tutvustada infoturbega seotud mõisteid, standardeid ja asutusi, samuti teha ülevaade olemasolevatest infosüsteemides rakendatavatest riskianalüüsi meetoditest, võrrelda erinevaid riskianalüüsi meetodeid ja riskianalüüsi programme. Analüüsida erinevaid riskianalüüsi meetodeid, standardeid ja valida välja sobiv riskianalüüsi meetod ja programm, mis sobiks riigisaladust töötlevale infosüsteemile.

Esimeses peatükis anti ülevaade riigisaladuse seaduses ja selle alusel väljaantud määrustes kasutatavatest mõistetest, selgitada, mis on riigisaladus ja mis on salastatud välisteave. Käsitletakse riigisaladuse tasemeid ja seda millise info on riik kuulutanud riigisaladuseks, samuti seda mille poolest erineb riigisaladus töötlev infosüsteem teistest infosüsteemidest.

Teises peatüki eesmärk oli tutvustada lühidalt mõnede riikide ja organisatsioonide infoturbeasutusi, kus tegeldakse suuremal või vähemal määral riskianalüüsi meetodite koostamisega. Veel anti ülevaade infoturbe korralduses kasutatavatest standarditest üldiselt ja kirjeldatati, kas ja kuidas saab neid kohandada riskihalduse jaoks. Analüüsiti erinevaid riskihalduse ja -analüüsi programme ning tehti kindlaks, millised on sobivamad programmid riigisaladust töötlevate infosüsteemide jaoks.

Kolmandas peatükis anti ülevaade riskihaldamise protsessist üldiselt. Millised on tegevused mida vaja teha, et organisatsioonis toimiks süstemaatiline riskihaldus. Anti veel ülevaade erinevatest riskianalüüsi meetoditest. Toodi välja nende eelised ja puudused. Leiti sobivamad riskianalüüsi meetodi, mis sobivad riigisaladust töötlevatele infosüsteemidele.

Neljandas peatükis vaadeldi, kas Eesti Vabariigis üldtuntud etalonturbemeetod ISKE on täielikult rakendatav riigisaladust töötlevates infosüsteemides, või tuleb seda modifitseerida vastavalt riigisaladuse ja salastatud välisteabe seadusele ning selle alusel antud määrustes esitatud nõuetele. Selle selgitamiseks kasutas autor võrdlevat meetodit. Autor võrdles ISKE turvameetmete ja Kaitseministri määruses nr. 34 esitatud põhilisi turvameetmeid. Selgus, et

ISKE mõned turvameetmed ei ole piisavad, võrreldes Kaitseministri määruses nr. 34 esitatavate turvameetmetega.

Riigisaladust töötlevad infosüsteemidel on kõik turvameetmed, mis tulenevad seadusandlusest, kohustuslikud rakendada. Ehk siis selleks tuleb ISKE madal (L) tasemele, keskmise (M) tasemele lisada juurde uus tase, mille autor on nimetanud riigisaladus (RS) tasemeks.

Lisas 1 toob autor välja seadusandlusest tulenevate nõuetest ISKE uue turvataseme RS meetmed, mis tuleb kindlasti rakendada riigisaladust töötlevas infosüsteemis.

Lisas 2 väljavõte elektroonilisest teabeturbest „Riigisaladuse ja salastatud välisteabe kaitse kord“ Vabariigi Valitsuse määrus nr. 262 jagu 9-st.

Lisas 3 iga asutus, kes omab ja töötleb riigisaladust, peab olemas olema riigisaladuse kaitse juhend ja selles lisas on ära toodud riigisaladuse kaitse juhendis kajastuvad teemad.

KASUTATUD KIRJANDUS

1. HansonVello, Buldas Ahto, Martens Tarvi, Lipmaa Helger, Ansper Arne, Tulit Viljar (1997). Infosüsteemide turve 1. Küberneetika AS.
2. EVS-ISO/IEC TR 13335-1:1999. Infotehnoloogia. Infoturbe halduse suunised. Osa 1: Infoturbe mõisted ja mudelid.
3. EVS-ISO/IEC TR 13335-2:1999. Infotehnoloogia. Infoturbe halduse suunised. Osa 2: Infoturbe haldus ja plaanimine.
4. EVS-ISO/IEC TR 13335-3:1999. Infotehnoloogia. Infoturbe halduse suunised. Osa 3: Infoturbe halduse meetodid.
5. EVS-ISO/IEC TR 13335-4:2000. Infotehnoloogia. Infoturbe halduse suunised. Osa 4: Turvameetmete valimine.
6. EVS - ISO/IEC 13335-5:2003. Infotehnoloogia. Infoturbe halduse suunised. Osa 5: Võrguturbe halduse suunised.
7. EVS - ISO/IEC 17799:2005. Infotehnoloogia. Infoturbe halduse menetluskoodeks.
8. EVS-ISO TR 13569:2006. Rahandusteenused. Infoturbe suunised**.**
9. RT I 2007, 16, 77. Riigisaladuse ja salastatud välisteabe seadus. URL https://www.riigiteataja.ee/ert/act.jsp?id=12850160 [2008, detsember].
10. RT I 2007, 73, 449. Riigisaladuse ja salastatud välisteabe kaitse kord. URL https://www.riigiteataja.ee/ert/act.jsp?id=12903659 [2008, detsember].
11. RTL, 2007, 102, 1702. Arvutite ja kohtvõrkude kaitse nõuded. URL https://www.riigiteataja.ee/ert/act.jsp?id=12905091 [2008, detsember].
12. Parts, A. (2003). IT riskianalüüs Elektroskandia AS näitel. [Magistritöö]. Tallinn 2003 Tallinna Pedagoogikaülikool informaatika osakond.
13. Kivimaa, J. (2004). Turvaanalüüsi metoodikate hindamine ja astmelise etalonturbe juhendmaterjal. URL http://www.riso.ee/et/files/Astm_etalonturve_vers2_JK.pdf. [2008, detsember].
14. Koppelmaa, I. (2004). Kehtestati infosüsteemide turvameetmete süsteem. URL http://www.riso.ee/et/pub/2004it/docs/2.2.html. [2008, detsember].
15. ISKE, (2007). Riigi Infosüsteemide Arenduskeskus. Infosüsteemide kolmeastmelise etalonturbe süsteem. (versioon 3. 2007) URLhttp://www.ria.ee/public/ISKE_rakendusjuhend_3_00_07092007.pdf. [2008, detsember].

16. Stoneburner G, Goguen A, and Feringa A. (2001). *Risk Management Guide for Information Technology Systems* .
URL.http://csrc.nist.gov/publications/nistpubs/800-30/sp800-30.pdf. [2008, detsember].
17. Praust, V. (2007). Infovarade nõrkused ja rakendatavad turvameetmed.
URL http://www.itcollege.ee/~valdo/turve/turve03.ppt. [2008, detsember].
18. Praust, V. (2006). Riskihaldus. Praktilised lahendused – BSI ja ISKE
URL www.mois.ee/sk/sisemine3.ppt. [2008, detsember].
19. BSI, GSTOOL. (2008). *IT Baseline Protection Tool*,
URL http://www.bsi.bund.de/gstool. [2008, detsember].
20. ENISA, (2008). *European Network and Information Security Agency.*
URL http://www.enisa.europa.eu/pages/01_02.htm. [2008, detsember].
21. BSI, (2008). *Bundesamt für Sicherheit in der Informationstechnik.*
URL http://www.bsi.bund.de/. [2008, detsember].
22. NIST ITL, (2008). *National Institute of Standards and Technology, Information Technology Laboratory.*
URL http://www.itl.nist.gov. [2008, detsember].
23. OGC, (2008). *Office of Governmental Commerce.*
URL http://www.ogc.gov.uk. [2008, detsember].
24. DSD, (2008). *Defence Signals Directorate*.
URL http://www.dsd.gov.au. [2008, detsember].
25. DCSSI, (2008). *Central Information Systems Security Division.*
URL http://www.ssi.gouv.fr/en/dcssi/index.html. [2008, detsember].
26. Common Criteria, (2008). *Common Criteria for Information Technology Security Evaluation.*
URL http://www.commoncriteriaportal.org/thecc.html. [2008, detsember].
27. DoE (2008). *Department of Energy.*
URL http://www.fas.org/irp/doddir/doe/o5639_6a.htm. [2008, detsember].
28. CRAMM, 2008. *Insight Consulding, SIEMENS.*
URL http://www.cramm.com/overview/howitworks.htm. [2008, detsember].
29. RiskWatch*,* 2008.
URL http://www.riskwatch.com. [2008, detsember].
30. EBIOS, 2008.
URL http://www.ssi.gouv.fr/en/confidence/ebiospresentation.html. [2008, detsember].
31. Hanson,V. Praust,V. 2003. Tallinn. Infosüsteemide turbe etalonmeetmete süsteemi

koostamine.

32. ISP205, 2005. *COUNCIL OF THE EUROPEAN UNION. Security risk assessment and risk management of secure systems.*

LISAD

LISA 1. ISKE RS TURVAMEETMED

Turbeastmes RS kokku 74 turvameedet ja need on kohustuslikud rakendada kui infosüsteemis töödeldakse riigisaladust.

RS.1 Olemas on turvanõuete rakendamise juhend.

RS.2 Olemas on organisatsiooni riigisaladuse kaitse kord.

RS.3 Olemas on turvanõueteloetelu.

RS.4 On määratud infosüsteemis töödeldava kõrgeim riigisaladuse tase.

RS.5 On määratud riigisaladuse kaitset korraldav isik.

RS.6 On määratud süsteemi haldav turbeadministraator.

RS.7 Kõigil isikutel on vastava tasemega juurdepääsuload, kellel ligipääs infosüsteemile.

RS.8 On olemas juurdepääsuloa ja juurdepääsusertifikaadi käitlemise kord.

RS.9 Süsteemi kasutajaid teavitatakse enne süsteemi kasutamist nende kohustustest süsteemi turvalisuse tagamisel.

RS.10 On olemas salastatud teabe kaitseplaan ohuolukorras.

RS.11 Süsteemis salvestatud salastatud teabest säilitatakse ajakohast varukoopiat.

RS.12 Süsteemis sisalduva salastatud teabe varundamise sagedus, varukoopiate säilitusnõuded ning -tähtajad ja juurdepääsuõigused varukoopiatele sätestatakse süsteemi turvanõuete loetelus.

RS.13 Varukoopiad on vastavalt märgisatud.

RS.14 Väljastpoolt saabuvate ja väljapoole saadetavate salastatud teabekandjate vastuvõtmise ja edastamise kord.

RS.15 Salastatud teabekandjate registreerimise kord.

RS.16 Salastatud koosolekute pidamise kord.

RS.17 Salastatud teabekandjate arvestus.

RS.18 Salastatud teabekandja märgistamine.

RS.19 Salastatud teabekandja hävitamise meetod ja kord.

RS.20 Süsteemi logiinformatsiooni säilitatakse 5.aastat.

RS.21 Süsteem salvestab süsteemi kasutamise analüüsiks vajaliku informatsiooni (sh käivitamine ja sulgemine, kasutajapoolne sisenemine ja väljumine,muudatused kasutajate või kasutajagruppide kasutajaõigustes, muudatused logiinformatsiooni seadistustes, kellaaja ja kuupäeva muutmine ja ebaõnnestunud katsed süsteemi siseneda).

RS.22 Süsteemis logitakse juurdepääs salastatud teabele.

RS.23 Logiinformatsiooni kirje sisaldab sündmuse toimumise kuupäeva, kellaaega, liiki ja märget sündmuse õnnestumise või ebaõnnestumise kohta ning seob kasutajanime selle olemasolul logitava sündmusega.

RS.24 Juurdepääs logiinformatsioonile on vastava eriõigusega kasutajal.

RS.25 Süsteemis salastatud teabe kustutamiseks kasutatakse tarkvara, mis kirjutab kustutatava salastatud teabe üle vähemalt seitse korda.

RS.26 Viiruse või muu kurivara avastamiseks ette nähtud tarkvara on installeeritud kõikidesse serveritesse ja kõvakettaga tööjaamadesse ja konfigureeritud viisil, et kontrollimine toimub automaatselt.

RS.27 Viiruse või muu kurivara avastamiseks ja tõrjeks ette nähtud tarkvara uuendatakse regulaarselt arvestades süsteemi kasutamisintensiivsust.

RS.28 Serverites ja kõvakettaga tööjaamades kasutatakse viiruse või muu kurivara avastamiseks ja tõrjeks ette nähtud tarkvara.

RS.29 Süsteemi sisenev teave kontrollitakse (võimalusel süsteemiväliselt) viiruse või muu kurivara avastamiseks ja tõrjeks enne teabega tutvumist (sh enne faili avamist).

RS.30 Uus tarkvara kontrollitakse enne süsteemis kasutusele võtmist süsteemiväliselt viiruste või muu kurivara avastamiseks ja kõrvaldamiseks.

RS.30 Infosüsteemis on arvestatud määrust „Krüptomaterjalide ning nende töötlemise ja kaitse nõuded“ (määrus on «piiratud» tasemel riigisaladus). Hetkel ei kehti.

RS.31 Süsteemi sisemisest turvakeskkonnast väljuv salastatud teave krüpteeritakse või kaitstakse muu Teabeameti lubatud meetoditega.

RS.32 Teabeameti teavitamine turvaintsidentidest.

RS.33 Süsteemis kasutatava riistvara ja tarkvara üle peetakse arvestust.

RS.34 Süsteemi serverite ja tööjaamade riistvaraline ning tarkvaraline konfiguratsioon dokumenteeritakse.

RS.35 Riist- ja tarkvara konfigureerib vastava eriõigusega kasutaja.

RS.36 Süsteemi tark- ja riistvara vaikimisi salasõnad muudetakse esmasel kasutuselevõtul.

RS.37 Serverite ja tööjaamade konfiguratsiooni vastavust dokumentatsioonile kontrollitakse regulaarselt.

RS.38 Süsteemi riistvara hooldust teostatakse vaid süsteemi sise turvakeskonnas.

RS.39 Süsteemi riistvara hooldust võib teha väljaspool sisemist turvakeskkonda kui salastatud teavet sisaldada võivad komponendid on riistvarast eemaldatud.

RS.40 Kasutatakse ainult heakskiidetud programme.

RS.41 Töötajatel on olemas vastavad juurdepääsuload.

RS.42 Asutusel on olemas riigisaladuse töötlemiluba.

RS.43 Arhiveerimis-andmekandjate korrektne märgistus.

RS.44 Arhiveeritud andmekandjate hoidmine turvaalal või seifi.

RS.45 Peab olema määratud administratiivala ulatus.

RS.46 Peab olema määratud turvaala asukoht.

RS.47 Relva ning tehnilise vahendi ja muu eseme, mida saab kasutada tehnilise vahendina pealtkuulamiseks või salvestamiseks, turvaalale viimise kord.

RS.48 Turvaala valve, turvaalale pääsemise, sellel liikumise ja sealt lahkumise kord.

RS.49 Kaabeldus on paigaldatud määrusest tulenevate nõuetega „Kiirgusturbe tagamise nõuded“ (määrus on «piiratud» tasemel riigisaladus).

RS.50 Ruum on määratletud administratiivalana (piiratud tasemega teabe töötlemisel).

RS.51 Ruum on määratletud turvaalana (konfidentsiaalse ja kõrgema tasemega teabe töötlemisel).

RS.52 Koodluku koodi vahetatakse regulaarselt.

RS.53 Kaabeldus on paigaldatud määrusest tulenevate nõuetega „Kiirgusturbe tagamise nõuded“ (määrus on «piiratud» tasemel riigisaladus).

RS.54 Süsteemi ühendamisel teise infotöötlussüsteemiga on tagatud salastatud teabe kontrollitud

liikumine süsteemide vahel.

RS.55 Süsteemile juurdepääsuks kasutatakse kasutajanime ning salasõna või Teabeameti poolt heaks kiidetud avaliku võtme infrastruktuuri meetodeid.

RS.56 Salasõna süsteemile juurdepääsuks on teada vaid kasutajale.

RS.57 Salasõnadel on miinimumpikkus. (8 tähemärki konfidentsiaalne ja kõrgem teave) (6 tähemärki piiratud teave).

RS.58 Salasõnadel on maksimaalne kehtivusaeg. (180 päeva konfidentsiaalne ja kõrgem teave) (1 aasta piiratud teave).

RS.59 Salasõnadel on minimaalne kehtivusaeg (1 päev).

RS.60 Salasõnas peab sisalduma suur ja väike täht, erimärk või number.

RS.61 Viie varasema kasutuses olnud salasõna kasutamine on keelatud.

RS.62 Salasõna muudetakse viivitamatult turvarikke või volitamata isikute valdusse sattumise või sellekohase kahtluse korral.

RS.63 Juhul kui salasõnu säilitatakse, hoitakse neid krüpteeritud kujul või suletud ümbrikus hoiukohas, mis vastab vastava tasemega salastatud teabekandjate hoiukohale seatud tingimustele.

RS.64 Süsteem blokeerib kasutajakonto automaatselt pärast kolme edutut autentimiskatset.

RS.65 Süsteem teavitab kasutajat autentimise ebaõnnestumise põhjustest minimaalses võimalikus ulatuses.

RS.66 Süsteem võimaldab juurdepääsu vaid sellisele salastatud teabele, mille suhtes töötlussüsteemikasutajal on põhjendatud teadmisvajadus.

RS.67 Süsteem võimaldab juurdepääsu vaid sellise salastatuse tasemega teabele, mille suhtes on kasutajal juurdepääsuõigus.

RS.68 Seansi alustamisel ilmub kuvarile teade töötlussüsteemis töödeldava teabe salastatuse taseme ning juurdepääsu piirangute kohta.

RS.69 Süsteemi mittekasutamisel 15 minutit või vähem katkeb juurdepääs teabele automaatselt ning kuvaseadmetel esitatu muutub loetamatuks.

RS.70 Süsteem võimaldab kasutajal katkestada teabele juurdepääs, sh muuta kuvaseadmetel esitatu loetamatuks.

RS.71 Süsteemis salastatud teabe kustutamiseks kasutatakse tarkvara, mis kirjutab kustutatava salastatud teabe üle vähemalt seitse korda.

RS.72 Salastatud teavet sisaldavale töötlussüsteemi komponendile paigaldatakse selle volitamata avamise tuvastamist võimaldav vahend (nt turvakleebis, -plomm või -tross).

RS.73 Süsteem on eraldatud Internetist.

RS.74 Koht- või laivõrku ühendatud seadmete üle peetakse ajakohast võrguskeemi.

LISA 2. ELEKTROONILISE TEABETURBE VÄLJAVÕTE

„Riigisaladuse ja salastatud välisteabe kaitse kord“ Vabariigi Valitsuse määrus nr. 262 jagu 9. Elektrooniline teabeturbe väljavõte.

§ 105. Elektroonilise teabeturbe põhimõtted

(1) Käesolevas osas sätestatakse elektroonilise teabeturbe nõuded salastatud teabe kaitseks selle elektroonilisel töötlemisel.

(2) Salastatud teavet võib elektrooniliselt töödelda salastatud teabe töötlussüsteemis, mis vastab elektroonilise teabeturbe nõuetele ning millel on Teabeameti antud kehtiv vastavussertifikaat või ajutine kasutusluba.

(3) Salastatud teavet on lubatud töödelda ainult sisemises turvakeskkonnas paiknevate arvutite ja kohtvõrkude abil**.**

(4) Arvuti, milles töötlemiseks lubatud kõrgeim salastatud teabe tase on piiratud, võib viia väljapoole sisemist turvakeskkonda, kui:

1) salastatud teave on krüpteeritud nõuetele vastavate krüptovahenditega;

2) arvutil ei ole märgistust, mis viitaks töödeldava salastatud teabe salastatuse tasemele.

(5) Elektroonilise teabeturbe tagamisel salastatud välisteabe kaitseks võetakse täiendavalt arvesse salastatud välisteabe avaldaja poolt ettenähtud nõudeid.

(6) Elektroonilise teabeturbe tagamisel arvestatakse eelkõige järgmisi turvapõhimõtteid:

1) kasutada võib üksnes funktsioone, protokolle või teenuseid, mis on vajalikud teabe töötlemiseks või selle turvalisuse tagamiseks – minimaalsuse põhimõte;

2) katkematult peab toimuma süsteemi turvariskide ohjamine, sealhulgas vältimine, vähendamine, kõrvalejuhtimine ja lubatav aktsepteerimine – turvariskide pideva haldamise põhimõte – ja süsteemi turvalisuse regulaarne kontrollimine;

3) süsteemi kasutajatel ja administraatoritel on ainult tööülesannete täitmiseks vajalikud kasutajaõigused – privileegide piiratuse põhimõte;

4) eeldatakse kõigi süsteemiga ühendatud teiste süsteemide ebausaldusväärsust ning nendega teabe vahetamisel peab rakendama piisavaid turvameetmeid – isekaitsvate sõlmede kasutamise põhimõte;

5) ühe kasutatava turvameetme rikke korral ei tohi süsteem muutuda ebaturvaliseks – sügavuti kaitse põhimõte.

§ 106. Töötlussüsteemile esitatavad nõuded

(1) Salastatud teabe töötlussüsteemis peab olema tagatud salastatud teabe käideldavus, salajasus ja terviklikkus.

(2) Salastatud teabe töötlussüsteem peab võimaldama:

1) tuvastada ja registreerida isikud, kes omasid või võisid omada juurdepääsu salastatud teabele ja selle kaitsmist toetavatele süsteemitoimingutele ja -vahenditele;

2) eristada süsteemi kasutajaid salastatud teabele juurdepääsu õiguse põhjal;

3) juurdepääsu teabele ja selle kaitsmist toetavatele süsteemitoimingutele ja -vahenditele üksnes juurdepääsuõiguse ja põhjendatud teadmisvajaduse olemasolul;

4) kontrollida teabe ning selle kaitsmist toetavate süsteemitoimingute ja -vahendite salajasust, terviklikkust, käideldavust, samuti nende päritolu, usaldatavust ja ühendusi;

5) saavutada olukorra, kus elektroonilise teabeturbe kaitsemehhanismid toimivad nõuetekohaselt süsteemi kogu kasutusaja jooksul;

6) ära hoida ja kõrvaldada turvarikkeid ning vältida või vähendada nende tekkimisega kaasnevat kahju;

7) käsitleda turvarikkeid, mille käigus määratakse kindlaks ja registreeritakse süsteemile või selle osale avaldunud oht ja selle tagajärjel teabele tekkinud kahju ning selle kõrvaldamiseks võetud meetmed.

(3) Süsteemi kohta käiv teave dokumenteeritakse süsteemi turvanõuete loetelus ja süsteemi turvanõuete rakendamise juhendis.

(4) Töötlev üksus teostab süsteemi suhtes pidevat riskihaldust.

§ 107. Süsteemi turvanõuete loetelu

(1) Süsteemi turvanõuete loetelus esitatakse:

1) süsteemi tehniline kirjeldus;

2) ülevaade süsteemi riskianalüüsi tulemustest;

3) süsteemile esitatavate turvanõuete kirjeldus;

4) süsteemis rakendatavate turvameetmete loetelu;

5) süsteemi turvalisuse korraldamise kirjeldus.

(2) Süsteemi turvanõuete loetelu töötab välja töötlev üksus. Enne salastatud teabe töötlemiseks uue süsteemi ehitamist või kasutusele võtmist kooskõlastab töötlev üksus loetelu Teabeametiga.

(3) Süsteemi turvanõuete loetelu täpsustatakse süsteemi ehitamise ja kasutamise käigus, juhul kui toimuvad muudatused, näiteks kui muutub süsteemi kasutusotstarve, struktuur, ilmnevad uued olulised ohud või muutub süsteemis töödeldava salastatud teabe tase.

Süsteemi turvanõuete loetelu muudatused kooskõlastab töötlev üksus Teabeametiga.

§ 108. Süsteemi turvanõuete rakendamise juhend

(1) Süsteemi turvanõuete rakendamise juhendis esitatakse:

1) süsteemi turvalisuse eest vastutavate isikute ülesanded, õigused ja kohustused;

2) süsteemi kasutajad ning nende ülesanded, õigused ja kohustused;

3) süsteemi riist- ja tarkvara konfiguratsioonihalduse kirjeldus;

4) juhised salastatud teabe elektrooniliseks töötlemiseks;

5) süsteemis kasutatavate teabekandjate töötlemise kirjeldus;

6) süsteemi logifailide ülevaatamise ja intsidentide halduse kirjeldus.

(2) Süsteemi turvanõuete rakendamise juhendi töötab välja töötlev üksus, lähtudes süsteemi turvanõuete loetelust, ning kooskõlastab loetelu Teabeametiga, enne kui süsteemis alustatakse salastatud teabe töötlemist.

(3) Süsteemi turvanõuete rakendamise juhendit täpsustatakse süsteemi ekspluateerimise käigus, juhul kui toimuvad muudatused, näiteks kui muutub süsteemi kasutusotstarve, struktuur, ilmnevad uued olulised ohud või muutub süsteemis töödeldava salastatud teabe tase. Süsteemi turvanõuete rakendamise juhendi muudatused kooskõlastatakse Teabeametiga.

§ 109. Süsteemi akrediteerimine

(1) Süsteemi akrediteerimise eesmärk on saada piisav veendumus, et süsteem vastab elektroonilise teabeturbe tagamiseks kehtestatud nõuetele.

(2) Süsteemi akrediteerimisel lähtub Teabeamet:

1) süsteemi füüsilistest turvameetmetest;

2) süsteemiga seotud turvariskidest;

3) süsteemi turvanõuete loetelust;

4) süsteemi turvanõuete rakendamise juhendist;

5) süsteemi asukoha kiirgusturbe tsoneerimise tulemustest;

6) teabest elektroonilise teabeturbe nõuete täitmise kohta töötleva üksuse poolt.

(3) Teabeamet algatab süsteemi akrediteerimise töötleva üksuse taotlusel või omal algatusel. Töötlev üksus lisab süsteemi akrediteerimise taotlusele süsteemi turvanõuete loetelu ja turvanõuete rakendamise juhendi. Ülejäänud lõikes 2 nimetatud teabe esitab töötlev üksus Teabeameti nõudmisel.

(4) Akrediteerimise tulemusena antakse töötlevale üksusele vastavussertifikaat Teabeameti peadirektori käskkirjaga.

(5) Süsteemile akrediteerimise tulemusena antav ajutine kasutusluba antakse Teabeameti peadirektori käskkirjaga.

(6) Teabeamet keeldub süsteemile vastavussertifikaati või ajutist kasutusluba väljastamast ja

keelab selle kasutamise salastatud teabe töötlemiseks, kui süsteem ei vasta elektroonilise teabeturbe nõuetele. Vastav otsus tehakse Teabeameti peadirektori käskkirjaga.

§ 110. Teabe andmise kohustus

Teabeameti nõudel on töötlev üksus kohustatud viivitamata andma, sealhulgas kirjalikus vormis, teavet tema valduses oleva süsteemi ja elektroonilise teabeturbega seotud asjaolude kohta ning tagama Teabeametile tööajal pideva ning puhkepäevadel ja riiklikel pühadel eelnevalt kokkulepitud ajal juurdepääsu süsteemi osadele, sõltumata nende paiknemiskohast.

§ 111. Vastavussertifikaadi ja ajutise kasutusloa kehtivuse pikendamise kord

(1) Vastavussertifikaadi pikendamiseks esitab töötlev üksus Teabeametile taotluse vähemalt kaks kuud enne vastavussertifikaadi kehtivuse lõppemist.

(2) Ajutise kasutusloa kehtivust võib Teabeamet pikendada omal algatusel ja töötleva üksuse taotluse alusel.

(3) Vastavussertifikaadi ja ajutise kasutusloa pikendamisele kohaldatakse süsteemi akrediteerimise sätteid.

§ 112. Vastavussertifikaadi ja ajutise kasutusloa kehtetuks tunnistamine

(1) Teabeamet tunnistab vastavussertifikaadi või ajutise kasutusloa kehtetuks:

1) töötleva üksuse taotluse alusel;

2) kui töötlev üksus ei ole täitnud Teabeameti ettekirjutust elektroonilise teabeturbe nõude rikkumise või rikkumise ohu kõrvaldamiseks;

3) ilmneb vastavussertifikaadi või ajutise kasutusloa andmisest keeldumise aluseks olev asjaolu.

(2) Vastavussertifikaat või ajutine kasutusluba tunnistatakse kehtetuks Teabeameti peadirektori käskkirjaga.

(3) Vastavussertifikaadi või ajutise kasutusloa kehtetuks tunnistamine tehakse töötlevale üksusele teatavaks kirjalikult.

§ 113. Riigi julgeoleku volitatud esindaja teavitamine

Teabeamet teavitab süsteemile vastavussertifikaadi või ajutise kasutusloa andmisest, vastavussertifikaadi kehtivuse pikendamisest või kehtetuks tunnistamisest riigi julgeoleku volitatud esindajat, kui süsteemis töödeldakse salastatud välisteavet. (RT I 2007, 73, 449)

LISA 3. RIIGISALADUSE KAITSE JUHEND

Lisa annab ülevaate millised teemad peavad olema kajastatud riigisaladuse kaitse juhendis asutuses, mis töötlevad riigisaladust.

1) väljastpoolt saabuvate ja väljapoole saadetavate salastatud teabekandjate vastuvõtmise ja edastamise kord;
2) salastatud teabekandjate registreerimise kord;
3) seifi võtme ja ligipääsukoodi hoiustamise kord;
4) juurdepääsuloa ja juurdepääsusertifikaadi käitlemise kord;
5) salastamisandmete parandamise kord;
6) salastatud koosolekute pidamise kord;
8) turvaala valve, turvaalale pääsemise, sellel liikumise ja sealt lahkumise kord;
9) salastatud teabe kaitse plaan ohuolukorras;
10) teavitamine isikust, kes püüab mis tahes viisil saavutada ebaseaduslikku juurdepääsu salastatud teabele, ning «Riigisaladuse ja salastatud välisteabe seaduse» või selle alusel antud õigusakti nõuete rikkumisest;
11) loend kõikide asutuses, põhiseaduslikus institutsioonis ja juriidilises isikus kehtivate selliste kordade, juhendite ja muude eeskirjade kohta, mis reguleerivad riigisaladuse töötlemist;
12) salastatud teabekandja hävitamise meetod ja kord;
13) administratiivala ulatus;
14) relva ning tehnilise vahendi ja muu eseme, mida saab kasutada tehnilise vahendina pealtkuulamiseks või salvestamiseks, turvaalale viimise kord;
15) sissepääsuloa või sissepääsu tagava vahendi kaotamise, kaotamiskahtluse või muu valduse kaotamisest teavitamise kord;
16) selle isiku määramine, kellele tuleb anda hoiule konfidentsiaalsel ja kõrgemal tasemel salastatud teabekandja säilitamiseks kasutatava seifi luku varuvõti ja luku kood.
Lisaks nimetatutele võib riigisaladuse kaitse juhendis sätestada näiteks:
1) töötleva üksuse piires salastatud teabekandjate vastuvõtmise ja edastamise korra (turvaala piires, administratiivala kaudu);
2) salastatud teabekandjate edastamise täpsema korra;
3) salastatud teabekandjate reprodutseerimise korra;
4) kohapealse mehitatud valve kontrollkäikude korra;

5) turvaalale iseseisva sissepääsuõigusega isikute sissepääsuloa erisused samas töötlevas üksuses töötavate isikute kohta;

6) külalise turvaalale lubamise erisused samas töötlevas üksuses töötavate isikute kohta;

7) riigisaladuse töötlussüsteemi turvanõuete rakendamise juhendi kehtestamine.