

Tallinna Pedagoogikaülikool
Informaatika osakond

IT riskianalüüs Elektroskandia AS näitel.

Magistritöö

**Anne Parts
Juhendaja Monika Oit**

Tallinn 2003

1	Sissejuhatus.....	6
1.1	Teema valiku põhjendus	6
1.2	Töö eesmärk.....	6
1.3	Teema aktuaalsus	7
1.4	Kasutatud metoodika	7
1.5	Magistritöö ülesehitus	8
2	Infoturbe põhimõisted.....	9
2.1	Infoturbe aspektid	9
2.1.1	Terviklus	10
2.1.2	Käideldavus.....	10
2.1.3	Konfidentsiaalsus	12
2.1.4	Autentsus.....	12
2.1.5	Jälitatavus.....	13
2.1.6	Toimivus	13
2.1.7	Usaldatavus	13
2.1.8	Töökindlus	13
2.2	Turvapoliitika.....	13
2.3	Infovarad	13
2.4	Ohud.....	14
2.4.1	Jaotus ohu iseloomu järgi.....	14
2.4.1.1	Juhuslikud ohud	15
2.4.1.2	Tahtlikud ohud	15
2.4.2	Jaotus ohu toime järgi	15
2.4.2.1	Passiivsed ohud.....	15
2.4.2.2	Aktiivsed ohud	15
2.4.3	Jaotus ohuallika päritolu järgi	15
2.5	Nõrkused	16
2.5.1	Infrastruktuuri nõrkused.....	16
2.5.2	Infotehnilised nõrkused.....	16
2.5.3	Personali nõrkused	17
2.5.4	Organisatsiooni nõrkused.....	17
2.6	Toime	17

2.7	Risk	17
2.8	Riskianalüüs	18
2.9	Turvameetmed	19
2.9.1	Turvameetmed valdkonna järgi	19
2.9.1.1	Organisatsioonilised turvameetmed	19
2.9.1.2	Füüsilised turvameetmed	20
2.9.1.3	Infotehnilised turvameetmed	20
2.9.2	Turvameetmed toimemehhanismide järgi:	20
2.9.2.1	Ennetavad turvameetmed	20
2.9.2.2	Avastavad turvameetmed	23
2.9.2.3	Taastavad turvameetmed	24
2.10	Turvateenused	25
2.10.1	Autentimine	25
2.10.2	Pääsu reguleerimine	26
2.10.3	Salgamise vääramine	26
2.11	Turvamehhanismid	26
2.11.1	Tuvastusmehhanismid	26
2.11.2	Tõkestamismehhanismid	26
2.11.2.1	Pääsu reguleerimise mehhanismid	27
2.11.2.2	Krüptotehnika	27
2.11.3	Taastemehhanismid	27
2.12	Jääkrisk	27
2.13	Kitsendused turvaülesande lahendamisel	28
3	Turvariski analüüs	30
3.1	Metoodilised allikad	30
3.1.1	Riiklikud institutsioonid	30
3.1.1.1	NIST - National Institute of Standards and Technology.	31
3.1.1.2	NSA – National Security Agency	32
3.1.1.3	BSI - Bundesamt für Sicherheit in der Informationstechnik	32
3.1.1.4	OGC - The Office of Government Commerce	33
3.1.2	Rahvusvahelised eriala- ja standardimisorganisatsioonid	35
3.1.2.1	ISACA	35
3.1.2.2	ISO - International Organization for Standardization	36

3.1.3	Infoturbealaseid standardeid	36
3.1.3.1	ISO 13335 “Infotehnoloogia. Infoturbe halduse suunised”	36
3.1.3.2	ISO/IEC TR 13569 “Pangandus ja sellega seotud teenuste infoturbe suunised”	37
3.1.3.3	ISO / IEC 17799 ja BS7799 "Infotehnoloogia. Infoturbe halduse praktilised juhised"	38
3.1.3.4	CC- Common Criteria.....	39
3.1.4	Turbehalduse metoodilisest korraldusest Eestis	41
3.1.4.1	Eesti Andmekaitse Inspektsioon	41
3.1.4.2	Cybernetica AS	41
3.1.4.3	AS Stallion	41
3.1.4.4	Domina Privacy & Security	42
3.2	Riskianalüüsi meetodid	42
3.2.1	Kvantitatiivne riskianalüüs	42
3.2.2	Kvalitatiivne riskianalüüs	43
3.2.3	Jäme riskianalüüs	44
3.2.4	Detailne riskianalüüs.....	44
3.2.5	Etalonturve	45
3.2.6	Segametoodika	46
3.2.7	Mitteformaalne metoodika.....	47
3.2.8	Formaalsed meetodid	47
3.3	Riskianalüüsi vahendid	48
3.3.1	Risk Management Guide for Information Technology Systems.	48
3.3.2	IT Baseline protection manual ja selle tugitarkvara GSTOOLS	49
3.3.3	COBRA.....	53
3.3.3.1	Küsimuste koostamine	53
3.3.3.2	Riski hindamine	54
3.3.3.3	Aruannete generaator	54
3.3.3.4	Eksperthinnangute andmebaas.....	54
3.3.4	OCTAVE	55
3.3.4.1	Ettevõtte varadest lähtuva võimalike ohtude profiili koostamine....	55
3.3.4.2	Infrastruktuuri nõrkuste määratlemine.....	57
3.3.4.3	Turvastrateegia ja turvaplaanide koostamine.....	58

3.3.4.4	Riskianalüüsi maatriks: (konkreetse näite puhul)	59
3.3.5	CobiT	61
4	Infoturbe riskid firmas Elektroskandia näitel	65
5	Kokkuvõte.....	66
6	Kasutatud kirjandus:	68
7	Summary	71
8	LISAD.....	72
8.1	Lisa 1 Elektroskandia AS varadele mõjuda võivad ohud.	72
8.2	Lisa 2 Elektroskandia AS varadele mõjuda võivad nõrkused.	72
8.3	Lisa 3 Elektroskandia AS IT riskihindamise maatriks.	72

1 Sissejuhatus

1.1 Teema valiku põhjendus

Infotehnoloogia tungimine pea kõigisse eluvaldkondadesse on meie igapäevane reaalsus. Infotehnoloogia areng on toonud palju uusi rakendusi: E-post, e-äri, internetiportaali, majandustarkvara, kliendihaldustarkvara, dokumendihaldus, finants-tarkvara jne., mis võimaldab paljudes valdkondades saavutada eesmärke tunduvalt kiiremini ja väiksemate kuludega. Samas uudsete lahendustega kaasnevad ka uued riskid. Kui vanasti kaitsti põhiliselt materiaalseid väärtusi, siis tänapäeval on lisaks sellele vaja kaitsta ka teavet, sealhulgas eraldi veel ka intellektuaalselt omandit. Arvestades, et infotehnoloogia on muutunud üheks kiiremini arenevaks ja teiste valdkondadega enim seotud inimtegevuse valdkonnaks, on äärmiselt oluline selle kiire ja läbimõeldud areng igas ettevõttes. Samas suureneb ka ettevõtete sõltuvus infosüsteemidest ja nende töökindlusest. Tänapäeval on mõeldamatu hakkama saada ilma automatiseeritud infotöötluseta, mis toob kaasa vajaduse arvestada järjest enam infost ja infosüsteemidest tuleneva riskiga.

Arendades infosüsteemi, tuleks paralleelselt analüüsida ka infosüsteemi rakendamise tulenevaid ohte. Kuid IT riskianalüüs on siiani suhteliselt vähe arenenud valdkond. Lähteandmeid riskianalüüsiks on vähe, nende kogumine on töömahukas, puuduvad ka laiemale kasutajaskonnale suunatud selgepiirilised tegevusjuhised riskianalüüsiga tegelemiseks ja arvestades, et see on tundlik teema, siis näiteid teostatud riskianalüüsides on raske kätte saada. Riskianalüüsi meetodid on seetõttu kaudsed ja sobiva leidmine raske. Formaliseeritud meetodid on üldse alles arenemisjärgus.

Seetõttu on ülevaate saamine riskianalüüsi meetoditest, neid toetavatest vahenditest ja tegelikest probleemidest selliste meetodite praktikas kasutamisel väga aktuaalne teema.

1.2 Töö eesmärk

Magistritöö eesmärk on anda ülevaade olemasolevatest infosüsteemide turvariski halduse ja -analüüsi metoodikatest ning analüüsida nende kasutatavust praktiliste turvaülesannete lahendamisel.

Töö teine eesmärk on saada teoreetiliselt põhjendatud juhendmaterjal turvariskide hindamiseks ning turbeprobleemidega tegelemiseks ettevõttes või asutustes, kus infotehnoloogilised süsteemid on vaid põhitegevust abistava iseloomuga.

1.3 Teema aktuaalsus

Tänapäeval on ettevõtte jaoks järjest olulisem vajaliku informatsiooni õigsus ja õigeaegne kättesaamine. Äriprotsesside järjest suurem sõltuvus infotehnoloogilistest süsteemidest aga tekitab uusi riske, mida igakord ei osata näha ega ka end nende eest kaitsta. Info parema kättesaadavuse tagamiseks arendatavad arvutivõrgud on tekitanud olukorra, kus ohud ähvardavad infosüsteeme nii väljast kui ka seest.

Infotehnoloogiast tulenevad riskid ei ole vaid tehnoloogiline probleem - mida keerulisemaks ja avatumaks lähevad infosüsteemid, seda rohkem tuleb pöörata tähelepanu töötajate sellealase teadlikkuse tõstmisele. Töötajad peavad mõistma, et infotehnoloogilisi süsteeme ähvardavad arvestatavad riskid ning et informatsiooni hävimisel, volitamatul muutmisel või volitamatul avalikustamisel võivad olla rasked tagajärjed organisatsioonile ja ta töötajatele. Olles teadlik võimalikest ohtudest, oskab töötaja realiseerunud ohu ära tunda. Mida kiiremini intsident avastatakse, seda kiiremini suudetakse see likvideerida ja seda väiksemat kahju suudab oht tekitada. Ideaalsel juhul oleks infoturbereeglid ettevõtte turvapoliitika dokumendi või sisekorraeeskirjade lahutamatu osa. Ent kogu selle tegevuse aluseks on turvariskide analüüs, mille tulemusena tuvastatakse tegelikud ohud infosüsteemis ning nende võimalikud realiseerumise teed.

1.4 Kasutatud metoodika

Infoturberiski hindamise metoodikate ülevaate koostamisel ning ettevõtte äriprotsesside profiiliga sobiliku riskianalüüsi meetodi valikul on kasutatud võrdlevat analüüsi. Ettevõtte äriprotsesse on analüüsitud struktuurse analüüsi meetodil, turvaprobleemide analüüsi ja turvariski halduse aluseks on vastavad rahvusvahelised standardid ning erinevate riikide metoodilised materjalid.

1.5 Magistritöö ülesehitus

Käesolev magistritöö koosneb 8 peatükist 132 lehel, sisaldab 17 joonist ja 3 tabelit.

Esimene peatükk on sissejuhatus, kus autor põhjendab teema aktuaalsust ja tähtsust tänapäeval. Töö põhiosa algab 2 peatükist, kus autor annab ülevaate infoturbe seonduvatest ja magistritöös käsitletud põhimõistetest. Peatükis 3 antakse ülevaade infoturbe riskianalüüsi meetoditest. Metoodilistest allikatest vaadeldakse nii riikide vastava ala metoodikat väljatöötavate asutuste kui ka rahvusvaheliste organisatsioonide materjale ning sellealaseid standardeid. Peatükis 4 on teostatud Elektroskandia AS riskianalüüs, tuginedes eelnevalt vaadeldud põhimõistetele ja meetoditele.

Järgneb kokkuvõte, kasutatud kirjanduse loetelu, inglisekeelne resümee ja lisad.

2 Infoturbe põhimõisted.

Sageli mõistetakse infoturvalisuse all vaid konfidentsiaalsuse tagamist ning teised tänapäeval informatsiooni turvalise töötlemisega seonduvad aspektid jäävad tähelepanuta. Tagamaks üheselt arusaadavat mõistete süsteemi, on käesolevas peatükis antud ülevaade infoturbe põhimõistetest, mida on magistritöös käsitletud.

2.1 Infoturbe aspektid

Omaniku ja legaalse kasutaja seisukohalt taanduvad kõik arvutisüsteemi varadele esitatavad nõuded järgmisele kolmele omadusele: (Riigi Infosüsteemide Arenduskeskus 2003)

- terviklus – andmete kaitstus võltsimise ja volitamata muutmise eest,
- käideldavus – andmete kiire ja mugav kättesaadavus volitatud isikutele,
- konfidentsiaalsus – andmete loetavus üksnes volitatud isikutele.

Mõnedes käsitlustes (EVS-ISO/IEC TR 13335-1:1999, IT Governance Institute 2000), vaadeldakse infoturbe aspektidena ka autentsust, jälitatavust, usaldatavust ja töökindlust, ent sisuliselt taandub vastava turvaülesande lahendamine samuti ülaltoodud kolme omaduse tagamisele.

Süsteemide turvalisuse omadusi saab tagada vaid suuremal või väiksemal määral: ei ole olemas sajaprotsendilist konfidentsiaalsust, käideldavust ega terviklust. See eeldab omakorda aga teatud mõõdupuu(de) olemasolu ning kasutamist andmete nõutava turvalisuse taseme praktilisel määratlemisel.

Et turvanõuete püstitamine oleks üheselt mõistetav, võib kasutada nõuete kirjeldamiseks mingeid kokkuleppelisi tähistusi või keelt. Eestis on kasutusele võetud kokkuleppelised turvaklassid, mille abil on turvanõudeid võimalik esitada lihtsalt ja konkreetselt. (Riigi Infosüsteemide Arenduskeskus 2003)

Vanemad turvalisuse tasemete määratlused (TCSEC, ITSEC) käsitlesid turvalahenduste funktsionaalseid omadusi ning vastavad turvaklassid (vastavalt A, B, C, D või E1, E2, E3 jne.) on tegelikult üheselt määratud komplektid funktsionaalsetest nõuetest. Klasse on vähe, mis seab aga olulised kitsendused turvanõuete kirjeldamise täpsusele ja muudab klassifikatsiooni kasutamise väheefektiivseks. Uusimates (algust tehti juba ITSEC klassides) klassifikaatorites on turvalisus kui eesmärk jagatud

erinevateks aspektideks, millele vastavad spetsiifilised turvanõuded ja ka spetsiifilised turvameetmed. (**Common Criteria, 2003**)

2.1.1 Terviklus

Andmeterviklus on omadus, mis näitab, et andmeid ei ole volitamatul viisil muudetud ega hävitatud. (EVS-ISO/IEC TR 13335-1, 1999)

Süsteemi terviklus on süsteemi omadus täita oma ettenähtud otstarvet kahjustamatul viisil, vabana sihilikust või juhuslikust volitamatust manipuleerimisest. (EVS-ISO/IEC TR 13335-1, 1999)

Eestis juurutatud turvaklasside süsteemis väljendab tervikluse omadus andmete volitamata muutmise võimatust ja andmete allika tuvastatavust ja tõestatavust. (Riigi Infosüsteemide Arenduskeskus, 2003) Terviklusnõude kvantitatiivne skaala on määratletud järgmiste nõuete tasemetega ranguse järjekorras arvestades:

1. andmeallika tõestatavus
2. andmeallika tuvastatavus
3. volitamatu muutmise tuvastatavus

Eesti turvaklasside süsteemi klassifikatsioon tervikluse põhjal: (Riigi Infosüsteemide Arenduskeskus 2003)

- Klass T3. Andmed, mille allikat peab saama tõestada kolmandale osapoolle. (Siia kuuluvad andmed on sedavõrd kaaluka tähtsusega, et nende sisestajat või viimaste muudatuste tegijat võib olla vaja kohtus tõestada.)
- Klass T2. Andmed, mille allikas peab olema tuvastatav. (Siia kuuluvad andmed on piisava tähtsusega, mistõttu peab vastutav töötaja saama tuvastada, kes on andmed sisestanud või neis viimati muutusi teinud.)
- Klass T1. Andmed, mille volitamatud muutmised peavad olema tuvastatavad (seda ka juhul, kui need on tehtud süsteemiülevaate poolt tema töö käigus).
- Klass T0. Andmete terviklusomadused pole olulised.

2.1.2 Käideldavus

Käideldavus on omadus olla volitatud olemi nõudmisel kättesaadav ja kasutuskõlblik ehk omadus väljendub nende andmete õigeaegses ja hõlpsas kättesaadavuses volitatud isikutele. (EVS-ISO/IEC TR 13335-1, 1999) Käideldavus on infosüsteemi põhiline

nõue, ilma milleta pole kogu infosüsteemil mõtet. Töökindluse nõue tähendab ka sisuliselt teatud tasemel käideldavust.

Eesti turvaklasside süsteem (Buldas, Oit, Praust 2003) iseloomustab käideldavuse vajadust kahe kvantitatiivse suurusega :

- teabe aegkriitilisus – aeg, mille jooksul peavad andmed peale vajaduse tekkimist olema kättesaadavad, st. nende hilisemal kättesaadavusel pole mõtet.
- teabe hilinemise tagajärgede kaalukus – potentsiaalne hinnatud kahju, mis tekitab andmete hilinemisel.

Neid kahte parameetrit tuleb vaadelda sõltumatutena. Teave võib olla aegkriitiline, kuid samas tema mittesaamise tagajärjed ei pruugi olla eriti tõsised.

Eesti turvaklasside süsteemi klassifikatsioon aegkriitilisuse põhjal:

- Klass K3. Andmed, mis tuleb saada sekundite jooksul.
- Klass K2. Andmed, mis peavad olema kättesaadavad mõne või mõnekümne minuti jooksul.
- Klass K1 Andmed, mis peavad olema kättesaadavad mõne päevaga.
- Klass K0. Andmed, mille hilinemine mitme päeva jooksul ei põhjusta komplikatsioone.

Klassifikatsioon hilinemise tagajärgede kaalukuse põhjal:

- Klass R3. Andmete õigeaegne mittesaamine põhjustab kas riigi suveräänsuse kadu või ettevõtte pankrotti; kahjusid, mis on võrreldavad riigieelarve või ettevõtte aastakäibega; mitmeid hukkunuid või ulatuslikku keskkonnasaastet.
- Klass R2. Andmed, mille õigeaegne mittesaamine põhjustab kas olulist kahju riigi suveräänsusele või ettevõtte mainele; miljonitesse ulatuvaid kahjusid; ohtu inimelule või keskkonnasaastet.
- Klass R1. Andmete õigeaegne mittesaamine põhjustab kas häireid riigikorralduses või ettevõtte tegevuses; sadadesse tuhandetesse ulatuvaid kahjusid; ohtu inimeste tervisele või keskkonnasaaste ohtu.
- Klass R0. Andmete õigeaegne mittesaamine ei too kaasa mainimisväärseid tagajärgi.

2.1.3 Konfidentsiaalsus

Konfidentsiaalsus on omadus, mis näitab, et informatsioon ei ole tehtud kättesaadavaks volitamata isikuile, olemitele või protsessidele ega neile avalikustatud. (EVS-ISO/IEC TR 13335-1, 1999)

Konfidentsiaalsust kvantitatiivses tähenduses tuleb ühest küljest mõista kui vajalike salastusmeetmete ranguse mõõtu, teisest küljest aga kui avalikustamisest tulenevate kahjude ulatuse määra. (Riigi Infosüsteemide Arenduskeskus 2003)

Üldlevinud konfidentsiaalsusskaala koosneb viiest tasemest:

- Avalik
- Piiratud kasutamisega - asustuse või firmasiseseks kasutamiseks
- Konfidentsiaalne
- Salajane
- Ülisalajane

Eesti turvaklasside süsteem on jaganud konfidentsiaalsuse neljaks tasemeks (Buldas , Oit, Praust, 2003)

S3 — teave on seaduses või seaduse alusel salastatud.

S2 — teabele on juurdepääs lubatud vaid eraldi subjekti või omaniku nõusolekul.

S1 — teabele on juurdepääs lubatud ainult teatud tingimuste täitmisel.

S0 — teabele ei ole seatud mingeid juurdepääsupiiranguid.

Erinevalt teistest infoturbe aspektidest on konfidentsiaalsuse osas enamasti olemas ka riiklikke regulatsioone. Eestis näiteks Avaliku teabe seadus (RT I 2000, 92, 597), milles on määratletud riigiasutuste sisemiseks kasutamiseks mõeldud andmete klassid. Isikuandmete kaitse seadus (RT I 1996, 48, 944), mis sätestab mitteavalikustatava delikaatsete isikuandmete mõiste. Riigisaladuse seadus (RT I 1999, 16, 271), mis sätestab kolm riigisaladuse taset.

2.1.4 Autentsus

Autentsus on omadus, mis tagab, et mingi subjekti või ressursi identsus ühtib väidetavaga. Autentsus puudutab kasutajaid, protsesse, süsteeme, informatsiooni jm. olemeid. (EVS-ISO/IEC TR 13335-1, 1999) Autentsuse tagamise ülesanne taandub tervikluse tagamisele.

2.1.5 Jälitatavus

Jälitatavus on omadus, mis tagab, et mingi olemi toiminguid saab üheselt jälitada selle olemini. (EVS-ISO/IEC TR 13335-1, 1999) Ka jälitatavus ei ole eraldiseisev turvaomadus, jälitatavuse tagamine taandub samuti tervikluse tagamisele.

2.1.6 Toimivus

Informatsioonile ja infosüsteemidele esitatavate nõuete hulgas räägitakse CobiT-is (IT Governance Institute, 2000) ka toimivusest, mis taandub tegelikult terviklus- ja käideldavusnõuetele – toimivus tähendab seda, et informatsioon oleks asjakohane ning tarnitakse õigeaegselt, õigena, kooskõllalisena ja kasutuskõllblikuna. Enamus käsitlusi seda turvalisuse aspekti siiski eraldi ei sisalda.

2.1.7 Usaldatavus

CobiT-i käsitluses (IT Governance Institute, 2000) on toodud sisse ka usaldatavuse mõiste – usaldatavus tähendab informatsiooni õigsust ja asjakohasust, sisuliselt taandub see suures osas tervikluse mõistele. Asjakohasus peaks tulenema äriprotsesside õigest käsitlusest infosüsteemi projekteerimisel.

2.1.8 Töökindlus

Mõnikord räägitakse infoturvalisuse raames ka infosüsteemi töökindlusest. Definitsiooni järgi on töökindlus $R(t)$ tõenäosus, millega süsteem täidab oma funktsioone ajavahemikul $[t_0, t]$ eeldusel, et ta töötas hetkel t_0 , ning iseloomustab teenuse pidevust. Sisuliselt iseloomustab töökindlus süsteemi käideldavust. (Hanson, Buldas, Martens, Lipmaa, Ansper, Tulit, 1997, 14)

2.2 Turvapoliitika

Turvapoliitika on dokument, milles asutuse või ettevõtte juhtkond fikseerib oma suhtumise infoturbesse ning sätestab infoturbealase tegevuse eesmärgid ning juhtimisskeemi. Turvapoliitika peaks olema asutuse või ettevõtte strateegilise arengukava osa ning seda peaks regulaarselt läbi vaatama.

2.3 Infovarad

Infovarad on asutuse või ettevõtte jaoks mingit väärtust omav informatsioon ning selle nõuetekohast töötlemist tagavad seadmed ja infrastruktuurid.

Turbehalduse standardi käsitluses jagunevad ettevõtte infovarad järgmiselt: (EVS-ISO/IEC TR 13335-1, 1999)

- füüsilised varad (nt arvutite riistvara, sideseadmed, hooned)
- informatsioon ja andmed (dokumendid, andmebaasid)
- tarkvara
- mingi toote valmistuse või teenuse andmise võime
- inimesed
- ainetud varad (maineväärtus, imago)

Arvutisüsteemide peamised varad on andmed, IT aparatuur, andmesidekanalid ja tarkvara. Muude kaitstavate varadega (näiteks pangaseifiga) võrreldes on arvutisüsteemide varadel oma spetsiifika, mida tuleb turvameetmete kavandamisel arvestada. (Hanson, Buldas, Martens, Lipmaa, Ansper, Tulit, 1997, 12)

Näiteks :

- Varade väärtus - arvutis salvestatud andmebaasi väärtus võib sageli ületada pangaseifi sisu väärtuse.
- Portatiivsus - riistvara võib portfelli mahutada kümnete tuhandete kroonide väärtuses, andmeid aga oluliselt suuremas väärtuses.
- Võimalus vältida füüsilist kontakti - adekvaatse kaitseta elektronarveldus ning muud võrguteenused võimaldavad vargusi ja muid kahjustusi ilma füüsilise sissetungita kahjukannataja juurde.

2.4 Ohud

Oht on süsteemi või organsatsiooni kahjustada võiva soovimatu intsidendi potentsiaalne põhjus. (EVS-ISO/IEC TR 13335-1, 1999)

Ohud võivad pärineda looduslikust või inimallikast ning olla juhuslikud või sihilikud.

2.4.1 Jaotus ohu iseloomu järgi

Ohuallikate olemuse järgi on turvalisuse seisukohalt otstarbekas eristada juhuslikke sekkumiskatseid tahtlikest teguritest. Sageli püütakse turvameetmete valimisel kaitsta süsteeme ainult teadlike sissetungide eest (eriti pärast mõnda teatavaks saanud õnnestunud sissemurdu), tegelike kahjude statistika aga näitab juhuslike mõjurite märksa kaalukamat rolli. (Hanson, Buldas, Martens, Lipmaa, Ansper, Tulit, 1997, 20)

2.4.1.1 Juhuslikud ohud

Juhuslikud ohud tulenevad vääramatust looduslikust jõust, mis võib olla loomult juhuslik (äike, ujutus) või regulaarne (kulumine, materjalide väsimine, saastumine), aga ka inimvigadest, mida võivad põhjustada ebapiisavad oskused, hooletus, juhtimisvead, keskkonnategurid. Eriti kaalukad on juhtimis- ja otsustusvead infosüsteemi elutsükli kõigis järkudes. Turvaülesande püstituse ja lahendamise tarbeks on kasulik rühmitada niisugused stiihilised ja poolstiihilised ohud nende kandja järgi. (Hanson, Buldas, Martens, Lipmaa, Ansper, Tulit, 1997, 21)

- keskkonnaohud,
- infosüsteemi või infrastruktuuri tehnilised rikked ja defektid,
- inimohud.

2.4.1.2 Tahtlikud ohud

Tahtlikud ohud ehk ründed lähtuvad inimestest, kes on mitmesugustel motiividel ja ajenditel (isiklikud huvid, huligaansus, riiklik või eraluure jne) valmis sihilikult kahju tekitama. Neid ohte on otstarbekas eritleda ründeobjektide ja meetodite järgi.

2.4.2 Jaotus ohu toime järgi

2.4.2.1 Passiivsed ohud

Passiivsed ohud ei põhjusta realiseerumisel süsteemi(de)s sisalduva informatsiooni, süsteemi talitluse ega oleku muutumist. Passiivse ohu realiseerumine on näiteks passiivse harundi kasutamine sideliinis edastatava informatsiooni jälgimiseks (pealtkuulamine).

2.4.2.2 Aktiivsed ohud

Aktiivsed ohud võivad muuta süsteemis sisalduvat informatsiooni, süsteemi olekut või süsteemi talitlust. Aktiivse ohu näide on süsteemi marsruutimistabelite sihilik muutmine, mille võib sooritada volitamata kasutaja.

2.4.3 Jaotus ohuallika päritolu järgi

Sisemised ohud tähendavad seda, et oht mõjub süsteemile seestpoolt, st süsteemi seaduslikud kasutajad võivad käituda ettenähtust erineval või volitamatul viisil. Enamik tuntud raaliroimadest on põhinenud sisemistel rünnetel, mida ei tõkestanud

turvamehhanismid. Sisemiste rünnete osakaaluks hinnatakse koguni 70%; üle poole turvaprobleemidest põhjustavad süsteemi legaalsed kasutajad ja nende eksimused. Välised ohud tulenevad süsteemivälistest teguritest ja volitamatud kasutajatest.

2.5 Nõrkused

Nõrkused on ettevõtte nõrgad kohad, mille kaudu saavad realiseeruda ettevõtte infosüsteemi ähvardavad ohud. (EVS-ISO/IEC TR 13335-1, 1999) Nõrkus iseenesest ei kahjusta; nõrkus on lihtsalt tingimus või tingimustik, mis võib lubada ohul mõjutada mingit vara. Nõrkused jagunevad (Hanson, Buldas, Martens, Lipmaa, Ansper, Tulit, 1997, 44)

- infrastruktuuri nõrkused
- infotehnilised nõrkused
- personali nõrkused
- organisatsioonilised nõrkused

Eestikeelses terminoloogias nimetatakse nõrkusi ka turvaaukudeks. (Hanson, Buldas, Martens, Lipmaa, Ansper, Tulit, 1997, 43)

2.5.1 Infrastruktuuri nõrkused

Infrastruktuuri nõrkused on ettevõtte infrastruktuuri nõrgad kohad, mille kaudu saavad realiseeruda ettevõtte infosüsteemi ähvardavad ohud.

Infrastruktuuri nõrkuseks on näiteks kaitstava objekti ebasoodne asukoht (reeglina suurendab see mitmesuguste ohtude realiseerumistõenäosust.) Samuti on nõrkuseks primitiivne või amortiseerunud infrastruktuur. (Ei võimalda näiteks realiseerida turvameetmeid (füüsilisi ja infotehnilisi))

2.5.2 Infotehnilised nõrkused

Infotehnilised nõrkused on infotehniliselt nõrgad kohad ettevõtte infosüsteemis, mille kaudu saavad realiseeruda ohud. Infotehniliseks nõrkuseks on näiteks piiratud ressursid, aparatuuri või sideliinide väär paigaldus, vead, defektid või dokumenteerimata omadused programmides, protokollide ja sideprotseduuride puudused, andme- halduse puudused, vahendite ja meetmete tülisus.

2.5.3 Personali nõrkused

Personali nõrkus puudutab töötajaid, tarnijaid ja allettevõtjaid. Ta viitab töötaja koolitusele ja teadmistele tööprotseduuride ja turvameetmete alal ning nende järgimisele. (ISO TR 13569 kavand, 2000)

Personali nõrkuste hulka kuuluvad väärad menetlused (tulenevad tihti teadmatusest või mugavusest ja on sageli süstemaatilised), teadmatus ja motivatsioonitus (laieneb reeglina kogu organisatsiooni töötajatele), turvanõuete eiramine (nii hooletusest kui ka sihilik).

2.5.4 Organisatsiooni nõrkused

Organisatsioonilised nõrkused on nõrgad kohad ettevõtte organisatsioonilises korralduses, mille kaudu saavad realiseeruda ettevõtte infosüsteemi ähvardavad ohud.

Organisatsiooni(listeks) nõrkusteks on töökorralduse puudused (reeglid, uue olukorraga kohanemine jms), ressursihalduse puudused (arvutid, side, hooldus, testimine, andmekandjad jms), dokumenteerimise puudused (IT seadmed, sideliinid, andmekandjad jms), turvameetmete valimise puudused (meetmeid rakendatakse valesti või vales kohas/konfiguratsioonis), turvasüsteemide halduse puudused .

2.6 Toime

Toime infoturbe kontekstis on sihiliku või juhusliku soovimatu intsidendi tagajärg, mis mõjutab varasid.(EVS-ISO/IEC TR 13335-1, 1999) Tagajärgedeks võivad olla teatud varade häving, infotehnoloogilise süsteemi kahjustus ning konfidentsiaalsuse, tervikluse, käideldavuse, jälitatavuse, autentsuse või töökindluse kadu. Võimalike kaudsete tagajärgede hulka kuuluvad rahalised kahjud ning turuosa või firma imago kaotus. Kui me oskame hinnata võimalike intsidentide poolt tekitatud kahju suurst, siis on võimalik otstarbekamalt investeerida turvameetmetesse.

Arvestada tuleb soovimatu intsidendi asetleidmise sagedust. See on eriti tähtis siis, kui iga üksikjuhtumi põhjustatud kahju on väike, kuid paljude intsidentide liitmõju pikema aja kestel võib olla kahjulik. Toimete hindamine on riskide hindamise ja turvameetmete valimise oluline element.

2.7 Risk

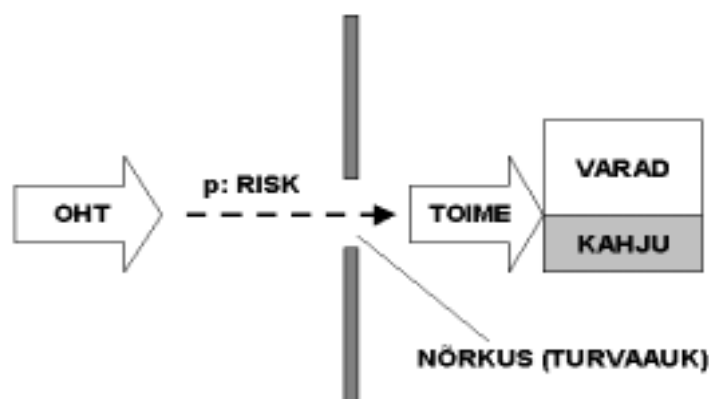
Risk on võimalikkus, millega konkreetne oht kasutab ära nõrkused mingi vara kahjustamiseks ja seega otseselt või kaudselt organisatsiooni kahjustamiseks. (EVS-

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, 58)

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.

2.8 Riskianalüüs

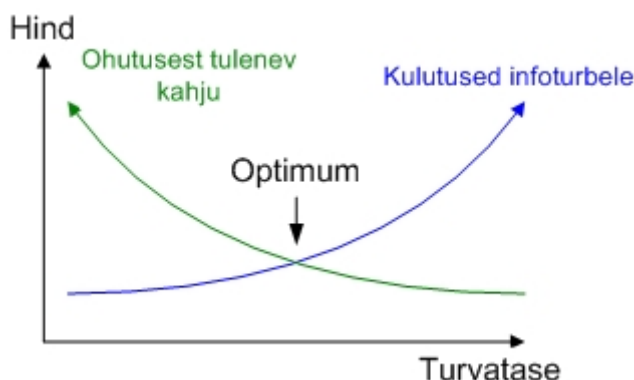
Riskianalüüs on andmetöötlussüsteemi varade, neid ähvardavate ohtude ja süsteemi vastava ohu / nõrkuse identifitseerimise süstemaatiline meetod. (Praust V, 1997) Riskianalüüsi eesmärk on prognoosida objektile tekitatavat kahju mingiks perioodiks, näiteks aastaks. Turvarisk on rahas väljendatav suurus, mis võrdub ohtude realiseerumisel tekkiva kahju ning nende ohtude realiseerumise tõenäosuse korrutisega. Kui see prognoos on teada, taandub turvaküsimus tasuvuse määramise ülesandeks, milles võrreldakse prognoositud kahju võimalikele turvameetmetele tehtavate kulutustega sama perioodi kohta. Riskianalüüs on laiem turbeprotsessi, riskihalduse osa.



Joonis 1 Turbe kahjustumise skeem (Praust V, 2001)

Riski hindamiseks tuleb kõigepealt hinnata varade väärtus ja määrata kindlaks varasid ähvardavad ohud ning nende realiseerumise tõenäosused. Seejärel tuleb määratleda turvaeesmärgid - mida me tahame kaitsta ja kui tugevalt.

Lõpuks on vaja välja selgitada püstitatud eesmärkide saavutamiseks vajalikud turvameetmed, hinnata nende rakendamisega seotud kulutusi ning vajadusel (kui kulutused infoturbele ületavad ohtude realiseerumisest tuleneva tõenäolise kahju) turvaeesmärgi korrigeerida (leida optimum).



Joonis 2 Kahjude ja turbekulude tüüpiline sõltuvus turvatasemest

(Hanson, Buldas, Martens, Lipmaa, Ansper, Tulit, 1997, 82)

2.9 Turvameetmed

Turvameetmed on teoviisid, protseduurid või mehhanismid, mis võivad kaitsta ohu eest, kahandada mingit nõrkust, piirata soovimatu intsidendi toimet, avastada soovimatuid intsidente ja soodustada taastet. (EVS-ISO/IEC TR 13335-1, 1999)

Turvameetmed võimaldavad vähendada nõrkusi ehk turvaauke.

Tõhus turve nõuab tavaliselt eri turvameetmete kombinatsiooni, luues varadele mitu turbekihti. Näiteks tuleks arvutitele kohaldatavat pääsu reguleerimist toetada personaliprotseduuride, koolituse ja füüsilise turbega. (EVS-ISO/IEC TR 13335-1, 1999)

2.9.1 Turvameetmed valdkonna järgi

Turvameetmeid saab luua organisatsiooniliste, füüsiliste või infotehniliste vahenditega või nende kombinatsiooniga. (Hanson, Buldas, Martens, Lipmaa, Ansper, Tulit, 1998, 24)

2.9.1.1 Organisatsioonilised turvameetmed

Organisatsioonilised turvameetmed on personalile suunatud meetmed, mis sisaldavad töökorralduse, turbesüsteemide kavandamise, halduse ja turvaintsidentide käsitlemise tegevusi ning toiminguid.

Organisatsioonilisi meetmeid tuleb rakendada esmajärjekorras, alates turvapoliitika sõnastamisest, riskianalüüsist ja turbeplaani koostamisest. Enamasti on nad muude võimalustega võrreldes ökonoomsemad ja paljudel juhtudel ka tõhusamad (nt. tulemusliku viirusetõrje sisseseadmisel)

2.9.1.2 Füüsilised turvameetmed

Füüsilised turvameetmed on põhiliselt nii üldisele töökeskkonnale kui IT-infrastruktuurile suunatud meetmed, mis hõlmavad nii objekti infrastruktuuri (ehituslikud piirid, kommunikatsioonid, kütte- ja kliimaseadmed, turvauksed ja –aknad, seifid, barjäärid, tõkkepuud, väravad) kui ka mehaanilisi komponente (lukud, sildid, viidad, pakendid, märgised).

Sageli liigitatakse füüsiliste turvameetmete alla ka pääslatöötajad, turvamehed jmt. töötajad.

2.9.1.3 Infotehnilised turvameetmed

Infotehnilised turvameetmed on infotehnoloogiliste vahendite toel ja –keskkonnas realiseeritavad meetmed turvateenuste osutamiseks.

Infotehnilised turvameetmed on kasutusel peamiselt loogilise eraldamise ja turvarikete tuvastuse funktsioonide teostamiseks. Kaks peamist praktilist vahendit on tarkvarapõhine pääsu reguleerimine (andmetele ja infosüsteemidesse + autentimistehnika) ja krüptograafia võtted (teabe teisendamine loetamatule kujule).

2.9.2 Turvameetmed toimemehhanismide järgi:

Lähtudes turbeabinõude otstarbest, võib turvameetmed jagada. (Hanson, Buldas, Martens, Lipmaa, Ansper, Tulit, 1998, 16)

- Ennetavad turvameetmed
- Avastavad turvameetmed
- Taastavad turvameetmed

2.9.2.1 Ennetavad turvameetmed

Ennetavad turvameetmed võimaldavad ennetada turvarikkeid: sulgeda turvaauke, ära hoida ründeid, vähendada ohtude realiseerumise tõenäosust, kahandada turvarikete toimet infovaradele, hõlbustada objekti taastet.

Ennetavad turvameetmed jagunevad omakorda tugevdusmeetmeteks, peletusmeetmeteks ja eraldusmeetmeteks.

Tugevdusmeetmed on abinõud kaitstava objekti kõige levinumate, peamiselt stiihilistel ohtudel toimimist võimaldavate turvaaukude sulgemiseks või kahandamiseks.

Tugevdusmeetmeteks on näiteks:

- kord (süsteemaatilisus)
- turvateadlikkus
- töötingimused
- ennetav kontroll

Kindel kord, süsteemaatilisus, kindlaksmääratud protseduurid igapäevases tööelus on peamine vahend stiihiliste ohtude tõrjeks. Kõik asutuse töö, sealhulgas infotehnoloogia sujuvat kulgu soodustavad abinõud tõstavad ka turvalisust. Näiteks sisekorra eeskirjad, täpsed ametijuhendid, standardite järgimine, infrastruktuuri ja töövahendite regulaarne hooldus, kindlaksmääratud hankeprotseduurid, töövahendite dokumenteerimine, andmekandjate ja kaabelduse märgistus, versioonihaldus, ressursivarude käigushoid, üldine turvapoliitika, turvaplaan, turvajuhendid.

Kõigi töötajate turvateadlikkus ja motivatsioon on tähtis tugevdav tegur. Infoturbe aluste tundmine on tänapäeval niisama vajalik kui infotehnoloogia enda tundmine. See saavutatakse näiteks töötajate sobiva valimise, regulaarse koolituse, teavitusürituste ja auditeerimistega.

Normaalsed töötingimused tõstavad eelkõige süsteemide käideldavust ja terviklust. Sobiv mikrokliima (temperatuur, õhuniiskus, õhu puhtus) kahandab nii tehniliste komponentide tõrkeid kui ka personali vigu ja tõstab tööviljakust. Inimeste puhul on niisama tõhus ka töökoha ergonoomiline ehitus ja kujundus. Veelgi olulisem on asutuse sotsiaalne kliima. Positiivsed inimsuhted ja objektiivne edutamise- ja ergutuspoliitika loovad aluse töötajate turvamotivatsioonile ning vähendavad siserünnete tõenäosust.

Süsteemaatiline kontroll võimaldab õigel ajal avastada seni märkamatuks jäänud või uusi turvaauke. Süsteemaatilise kontrolli hulka kuuluvad:

- infotehniliste toodete ja turvamehhanismide verifitseerimine ja testimine
- regulaarne turbealase operatiivteabe jälgimine (eriti Internetis)
- turvamehhanismide testründed
- süsteemide auditeerimine standardmetoodikate alusel

Peletusmeetmed kahandavad rünnete üritamise tõenäosust. Peletav toime on reeglina turvameetmete kasulik lisaomadus – ainuüksi teadmine turvameetmete käigushoiust või nende tajumine vähendab ründeindu, eriti kui oodatav saak ei korva ründaja riski. Kui on teada, et asutuse infoturbepoliitika on formuleeritud, et ta on range ja et seda järgitakse rangelt, ei paku konkreetsed turvamehhanismid mõnelegi potentsiaalsele ründajale enam huvi.

Peletusmeetmeteks on näiteks kehtestatud sanktsioonid, hoiatav märgistus dokumentidel, andmekandjatel, kuvadel, ruumide ustel jne. Ka nähtavad turvavahendid – valvur, telekaamera, territooriumi valgustatus, turvauksed, kaartlukud.

Eraldusmeetmed ehk siis põhiliselt tõkestusmeetmed tõrjuvad peamiselt ründeid, kaitstes turvalisuse kõiki põhiaspekte (käideldavus, terviklus, konfidentsiaalsus)

Jaguneb:

- ruumiline isoleerimine
- ajaline isoleerimine
- loogiline isoleerimine

Ruumiline isoleerimine on lihtsaim ja levinuim eraldamisprintsip. Erineva salastusastmega andmeid võib töödelda mitmel eraldi arvutil. Ühel andmekandjal saab hoida ainult võrdse salastusastmega või samadele kasutajatele määratud andmeid. Salastuselt erinevaid andmekandjaid võib säilitada eri kohtades ja erinevatel tingimustel. Erineva salastusega teabe edastuseks võib kasutada eraldi füüsilisi sideline jms.

Ajaline isoleerimine on rakendusvõimalustelt piiratum, kuid kasulik, kui ressursse napib. Näiteks arvuti kasutamine eri aegadel eri tundlikkusega andmete töötamiseks või erineva tarkvara kasutamine eri aegadel samas arvutis. Ka ruumi kasutamine eri aegadel erineva tundlikkusastmega üritusteks.

Loogiline isoleerimine on varade jaotamine (näiteks andmete tükeldamine) piisavalt väikesteks elementideks, mida saab eraldi või rühmitatult töödelda.

Alamliigid:

- pääsu reguleerimine (nt paroolkaitse, kaartlukk)
- teenusevahendus (nt tule müür, andmebaasi päringuprotsessor)
- salastamine (krüpteerimine, peitmine, hävitamine)

2.9.2.2 Avastavad turvameetmed

Absoluutselt turvalisi süsteeme ei ole olemas. Selleks puuduvad sobilikud turvamehhanismid ning maksimaalne turve ei ole enamasti ka majanduslikult õigustatud. Optimaalse turbe korral jääb aktsepteeritud jääkriski tõttu alati turvarikete võimalus, kuid need rikked ei tohi jääda märkamatuks. Seetõttu on oluline roll avastavatel turvameetmetel. Turvarikkest tekkiva kahju minimiseerimise seisukohalt on turvameetmete pingerida järgmine (Hanson, Buldas, Martens, Lipmaa, Ansper, Tulit, 1998, 21):

- operatiivtuvastus
- järeltuvastus
- tõendtuvastus

Operatiivtuvastus hõlmab meetmeid, mis võimaldavad turvaintsidente kohe nende tekkimisel tuvastada ja neile kohe reageerida. Selliste vahendite hulka kuuluvad valvur, sisetelevisioon, tuletõrje- ja valvesignalisatsioon, keskkonnaseire jms. infrastruktuurimeetmed. Infotehnikas on operatiivtuvastus enamasti kombineeritud pääsu reguleerimisega ja muude blokeerimismehhanismidega. Näiteks keelatud operatsiooni blokeerimisele kaasnev vea- või hoiatustead.

Järeltuvastus toimub otseselt või kaudselt turvariketega seotud sündmuste registreerimise alusel.

Näited:

- arvutite ja lukusüsteemide logifailid
- logifailide automaatanalüüsi vahendid
- mitmesugused diagnostika- ja testimisvahendid
- läbivaatuse, verifitseerimise ja auditeerimise meetodid

Tõendtuvastus põhineb mitmesugustel andmekogumitele lisatavatel turvaelementidel, mis võimaldavad kontrollida terviklust ja/või konfidentsiaalsust

Näited:

- paarsusbitt, kontrollsumma, tsükelkood, krüptograafiline sõnumilühend
- digitaalallkiri ja ajatempel
- steganograafiline vesimärk (lisatakse originaali loomisel)
- steganograafiline sõrmejälj (tekib kopeerimisel)

- füüsilised (nähtavad või vähemärgatavad turvakiled, -niidid, -pitserid, värvust muutvad märgised jms)

2.9.2.3 Taastavad turvameetmed

Objekti (infovara) turvalisust kahjustanud turvaintsidendi järel tuleb taastada objekti normaalne talitus seda kiiremini ja seda suuremas ulatuses, mida olulisem on objekt. (Hanson, Buldas, Martens, Lipmaa, Ansper, Tulit, 1998, 16)

Peamised liigid:

- varundamine
- ennistamine
- asendamine

Varundamine on taaste peamine ja tähtsaim eeldus

Näiteid:

- andmete regulaarne (tavaliselt mitte harvemini kui kord nädalas) varukopeerimine
- paralleelselt töös hoitav arvutisüsteem
- RAID-kettasüsteem

Ennistamine hõlmab rikete, tõrgete ja defektide kõrvaldamist

Näited:

- aparatuuri remont
- tarkvara parandamine ja modifitseerimine, sh. versioonihalduse meetmeid rakendades
- operatsioonide tagasivõtt rakendusprogrammides
- infrastruktuuri remont
- viiruse kõrvaldamine viirusetõrjeprogrammiga
- andmeedastuse bitivigade automaatne kõrvaldamine veaparanduskoodiga

Asendamine peab olema ette valmistatud parandamatute kahjustuste puhuks.

Näiteid:

- aegsasti sõlmitud kiirtarne- või üürilepingud
- asendusplaanid töötajate võimalike ootamatute ajutiste väljalangemiste või alalise lahkumise puhuks

2.10 Turvateenused

Turvateenused on turvameetmete abil realiseeritavad teenused, mis võimaldavad ettevõttel realiseerida turbealaseid eesmärgi.

Näiteks autentimise abil tehakse kindlaks kliendi autentsus st. kas klient on see, kelleks ta esineb; pääsu reguleerimine kontrollib, kas tal on õigus seda süsteemi kasutada ja kui ta on kasutanud, siis salgamise väärastamine tõestab, et klient on tõesti sooritanud antud teo.

2.10.1 Autentimine

Autentimine on protsess, millega kinnitatakse ja tõestatakse kliendi identsus. See võib salasõna või biomeetria vahenditega sisaldada kinnitust, et klient on nende volituste tõeline omanik. (Pulman 2003)

Biomeetriline autentimine sisaldab sõrmejälgede, näojoonte, hääle ja võrkkesta mustri identifitseerimist. Registreerimisprotsess võib sisaldada mõnes reaalse maailma identifitseerimisprotsessis nagu autojuhiload, pass, sünnitunnistus jne.

Autentimine on üks süsteemi turvalisuse nurgakive.

Autentimisel on erinevad tasandid, mis on järjestatud pakutava turvalisuse astme alusel:

- Varjatud autentimine põhineb eeldusel, et ainult autoriseeritud kasutajad teavad faili või andmebaasi nime ja andmebaasid on vaid sellega edukalt kaitstud.
- Lihtne autentimine kasutab jagatud saladusi (salasõnu), mida vahetatakse lihttekstina ja mis pakub väga vähe kindlust teate saatja isiku kohta. Näiteks võivad salasõnad kaduda või on need liialt lihtsad, mistõttu on oht, et sama salasõna võivad juhuslikult kasutada mitu inimest. Sellised salasõnad ei ole piisavad identsuse tagajaina. Lihtne salasõna võib olla ka inimestegrupile ühiskasutuseks. Olemas on tarkvaraliike, mis on loodud kasutamise "prooviks", jälgimiseks või salasõnade vahetuseks ja katkestamiseks.
- Kaitstud autentimine on sarnane, aga salasõnad on krüpteeritud.
- Tugevdatud autentimine kasutab krüpteeritud saladust, mida teab vaid teate saatja ja vaid tema saab garanteerida oma identsuse. Seda tüüpi autentimist võib vaja minna näiteks selleks, et teate autenditud saatja ei saa hiljem saatmist eitada kui ta näiteks on tellinud mingeid tooteid või teenuseid.

2.10.2 Pääsu reguleerimine

ISO 7498-2 järgi on pääsu reguleerimine ressurssidele volitamatu juurdepääsu vältimine, kaasa arvatud ressursside volitamatul viisil kasutamise vältimine.

Lisaks infotehnoloogilistele vahenditele tuleb pääsu reguleerimiseks rakendada ka füüsilisi ja organisatsioonilisi vahendeid.

2.10.3 Salgamise vääramine

Salgamise vääramine - lahti seletatuna tähendab seda, et teo sooritanu ei saa hiljem eitada oma tegu. (Tavast A. 2001)

Allika tõestusega: andmete saajale antakse tõestus andmete lähtekoha kohta. See kaitseb saatja katsete eest tõele vastukäivalt eitada andmete või nende sisu saatmist.

Saabumise tõestusega: andmete saatjale antakse tõestus andmete kättesaamise kohta. See kaitseb saaja katsete eest tõele vastukäivalt eitada andmete või nende sisu kättesaamist.

2.11 Turvamehhanismid

Turvateenused takistavad ohtude realiseerumist ja/või aitavad vähendada ohtude realiseerumisel saadavat kahju. Turvamehhanismid realiseerivad turvateenuseid.

Turvameetmed paigutavad mehhanismid organisatsiooni või süsteemi konteksti.

Mehhanismide funktsioonid jagunevad kolme põhitüüpi – tuvastamine, tõkestamine ja taaste ehk realiseerunud ohu tagajärgede kõrvaldamine.

2.11.1 Tuvastusmehhanismid

Ohtude tuvastamine on primaarse tähtsusega infoturbesüsteemi rajamise ja täiustamise juures. Kui ettevõttel puudub info konkreetset süsteemi ähvardavatest ohtudest ning selle vastu suunatud rünnetest, siis ei teata ka, mida kaitsta, kuidas kaitsta ja kui palju ressursse enesekaitsele kulutada.

Tuvastamiseks kasutatakse operatiivtuvastust, järeltuvastust, tõendtuvastust. (Hanson, Buldas, Martens, Lipmaa, Ansper, Tulit, 1998, 21)

(vt. Ka peatükk 2.9.2.2 Avastavad turvameetmed)

2.11.2 Tõkestamismehhanismid

Ohtude tõkestamise peamised mehhanismid on pääsu reguleerimine ja krüptotehnika.

2.11.2.1 Pääsu reguleerimise mehhanismid

Pääsu reguleerimise ülesanne on reguleerida ja kontrollida juurdepääsu infosüsteemis sisalduvale informatsioonile. Pääsu reguleerimine hõlmab süsteemi kasutajate määramist ja tema vastutuse fikseerimist, samuti tema juurdepääsu võrgule, arvutile, rakendusele ja süsteemile. Pääsu reguleerimine hõlmab ka kasutuse järelevalvet.

2.11.2.2 Krüptotehnika

Krüptotehnikat kasutatakse ennekõike infovarade peamiste turvatahkude kaitsmiseks. Krüpteerimine on andmete teisendamine volitamata kasutaja jaoks loetamatusse vormi, mille lugemine on võimalik vaid salajase võtme abil. Krüpteerimine kui vahend on esile kerkinud seoses vajadusega anda informatsiooni digitaalsetele esitusvormidele samasugused omadused, nagu seda on allkirjastatud ja salastatud paberdokumentidel. Viimaseid on raske kopeerida ja võltsida, mida aga ei saa öelda näiteks andmefailide kohta. Tänapäevaseid vahendeid õigesti kasutades on võimalik digitaalseid dokumente muuta palju kindlamateks kui seda on paberdokumendid.

2.11.3 Taastemehhanismid.

Taastemehhanisme kasutatakse realiseerunud ohtude tagajärgede kõrvaldamiseks. Objekti turvalisust kahjustanud intsidendi järel tuleb taastada objekti normaalne talitus seda kiiremini ja seda suuremas ulatuses, mida olulisem ja tundlikum on objekt.

Taaste eelduseks on **varundamine** – varusüsteemide, komponentide, andmete, protseduuride, ruumide jne loomine/soetamine ning nende kasutuselevõtu tagamine nõutava ajaga. Näiteks andmete regulaarne varukopeerimine, infotöötlussüsteemi kriitiliste sõlmede dubleerimine ja operatsioonide päeviku pidamine.

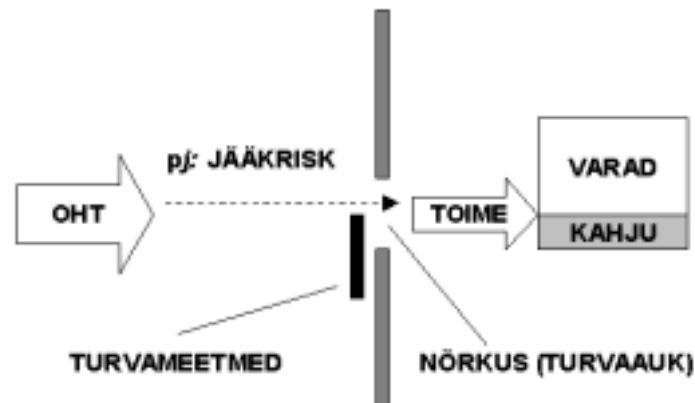
Komponendi funktsionaalsuse **ennistamine** hõlmab rikete, tõrgete ja defektide kõrvaldamist. Näiteks aparatuuri remont, kuid ka automaatse ennistuse vahenditest viirusetõrjeprogrammid.

Parandamatute kahjustuste puhuks peab olema ette valmistatud komponendi **asendamine**. Asendusplaanid peavad hõlmama ka töötajate võimalikke ootamatuid ajutisi väljalangemisi või alaliseks lahkumist.

2.12 Jääkrisk

Reeglina kahandavad turvameetmed riske ainult osaliselt. **Jääkrisk** on riski tase pärast juhtkonna poolt kehtestatud turvameetmete juurutamist ja käivitamist, s.o. ettevõtte

juhtide poolt aktsepteeritav riskitase, mis peab olema kulude kokkuhoiu seisukohalt optimaalne.(EVS-ISO/IEC TR 13335-1:1999)



Joonis 3 Turvameetmete mõju (Praust V, 2001)

Organisatsiooni vajaduste ja turbe vastavuse otsustamise üks osa on jääkriski aktsepteerimine, see peab olema juhtkonna teadlik otsus.

2.13 Kitsendused turvaülesande lahendamisel

Kitsendusi turvaülesande lahendamisele seab või tunnustab tavaliselt organisatsiooni juhtkond ning neid mõjutavad keskkonnad, mille tingimustes organisatsioon tegutseb. Mõned arvestamisele kuuluvad kitsendused on järgnevad:

- Rahalised – juhtkond võib ette anda turvaülesande lahendamise maksimaalse eelarve, aga ka üldjuhul ei tohiks turvameetmed olla kulukamad, kui varad, mida meetmed kaitsevad. Erandi sellest moodustavad turvanõuded, mis on tingitud mitterahalisest teguritest (seaduste nõuded, kokkulepped koostööpartneriga jms).
- Keskkondlikud – valikuid võivad mõjutada kohalik kliima, lähiümbruse geograafilised iseärasused, kasutada olev ruum jne.
- Ajalised – näiteks võib ettevõtte juhtkond nõuda, et turvameetmed peavad olema rakendatud teatud tähtajaks või vastupidi, ei saa juurutada enne kindlat hetke. Juurutusaega võib edasi lükata ka uue turvatoote ilmunisaeg.
- Juriidilised – turvameetmete valikut võivad mõjutada seadused ja eeskirjad, mis puudutavad infotöötlust otseselt (isikuandmete seadus, andmekogude seadus, riigisaladuse seadus jt) või kaudsemalt (töökaitse seadused, tuletõrje-eeskirjad jms).

- Tehnilised – eeskätt riistvara ja tarkvara ühilduvusega seotud piirangud.
- Kultuurilised ja sotsiaalsed – turvameetmed vajavad personali aktiivset tuge. Et personal turvameetmed omaks võtaks ja ei hakkaks neid ignoreerima, ei tohi turvameetmed oma otstarbalt ega olemuselt olla vastuolus kohalike, sh organisatsioonis valitsevate kultuuritavadega.

Kõiki neid tegureid tuleb arvestada turvameetmete valimisel ja teostamisel. Senised ja uued kitsendused tuleb perioodiliselt läbi vaadata ja tuvastada kõik muutused. Tuleks ka silmas pidada, et kitsendused võivad muutuda koos aja, geograafia, sotsiaalse arengu ja organisatsiooni kultuuriga.

3 Turvariski analüüs

Infoturbe haldus algab turvariski analüüsist ja eelkõige analüüsi metoodika valikust. Riskide hindamise ja analüüsimise meetodeid on arvukalt ning meetodi valik on organisatsiooni enda otsustada. Kuna lähteinfo on enamasti ebapiisav, siis vaatamata meetodite rohkusele, on ohtudest tulenevate riskide analüüsimine suuresti subjektiivne, toetudes hindaja(te) varasemale praktilisele kogemusele, omandatud teadmistele, analüütilisele mõtlemisele, töötajate küsitlusele ning hindaja isiksusest tulenevale võimele teha teemakohaseid üldistusi. Siiski on võimalik analüüsi meetodi sobiliku valikuga seda ülesannet lihtsustada.

Käesolevas peatükis on antud ülevaade nii riskianalüüsi meetodite väljatöötajatest kui ka meetoditest endist ning riskianalüüsi läbiviimiseks olemasolevatest tugisüsteemidest.

3.1 Metoodilised allikad

3.1.1 Riiklikud institutsioonid

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

Arvestades viimase aja suundumusi, suhtub USA endisest tõsisemalt nii arvutikuri-tegevusse üldiselt kui ka eriti nn. küberterrorismi, kuna rahvusliku julgeoleku aspektist kriitilised infrastruktuuri osad on endisest kesksesmas asendis ja seetõttu on ründed nende vastu ka palju tõenäolisemad. Seetõttu on küberrünnakuteks valmisolek üks USA julgeolekupoliitika peamisi alasid.

Tegutsemise hoogustumine paistab välja ka uute organisatsiooniüksuste loomisest. Tähtis koordineeriv organ on *Critical Infrastructure Assurance Office* - CIAO - (vt. <http://www.ciao.gov/publicaffairs/about.html>) ja põhiline tegutsev ametiasutus sellel alal on *the National Infrastructure Protection Center* -NIPC (vt. <http://www.nipc.gov/>), kelle ülesanne on aktiivselt paljastada, ennetada, hoiatada ja uurida arvutikuritegevust. NIPC-il on otsesidemed valitsuse ja majanduse ning muud elutähtsat infrastruktuuri ühendava keskusega *Information Sharing Analysis Center* – iga (ISAC). (vt. <http://www.nipc.gov/about/pdd63.htm>)

Saksamaal on korralikult väljatöötatud andmeturvalisust puudutav reeglite süsteem. Saksamaa siseministeeriumi haldusalas töötav Infoturbe Riigiamet (*Bundesamt für Sicherheit in der Informationstechnik* (BSI)) (vt. <http://www.bsi.de>) vastutusel on põhimõtteliselt kõik andmeturbesse puutuv alates testimisest kuni toodete sertifitseerimiseni.

Ka Inglismaal on infoturbe hästi organiseeritud - infoturbealase tegevuse koordineerijaks on standardimisorganisatsioon - *British Standards Institute* (samuti BSI) – (vt. <http://www.bsi-global.com/index.xalter>). BSI on olnud üks juhtivamaid andmeturbe standardite ja kvaliteedisertifitseerimissüsteemide väljatöötajaid. BSI poolt välja töötatud ettevõtete ja organisatsioonide juhtkonnale mõeldud andmeturbe standard BS 7799 (*British Standards Institute* 2003) oli üks esimesi süsteemse turbehalduse korraldust reguleerida üritavaks standardiks, olles praeguse rahvusvahelise standardi ISO TR 17799 (EVS - ISO/IEC 17799, 2003) eelkäijaks.

3.1.1.1 NIST - National Institute of Standards and Technology.

USA Riiklik Standardite ja Tehnoloogia Instituut - *National Institute of Standards and Technology* (vt. <http://csrc.nist.gov>) – on asutatud aastal 1901 Ameerikas. NIST-i missiooniks on arendada ja edendada standardeid ja tehnoloogiaid, parendamaks tootlikkust, hõlbustamaks kaubandussuhteid ning parandada üldist elukvaliteeti. NIST-is töötab umbes 3000 teadlast, inseneri ja tehnikut. NIST-i ülesanneteks on ka tagada informatsiooni turvalisus ja säilitada kriitiliste teenuste käideldavus majanduslikult mõistlike turvalisusmeetmetega. NIST-il on põhikirjajärgne vastutus anda välja turvalisusstandardeid ja ettekirjutusi riskitundlikele riiklikele süsteemidele - neid standardid võetakse vabatahtlikkuse alusel tihti kasutusele ka erasektoris.

NIST-i Infotehnoloogia Laboratoorium – ITL - *Information Technology Laboratory* (vt. <http://www.itl.nist.gov>) juhendab infotehnoloogia alaseid uurimusi ning arendab testmeetmeid ja standardeid infotehnoloogiatele. ITL-i juures asuv *Computer Security Division* töötab välja ja avaldab arvutiturvalisuse prototüüpe, standardeid ja protseduure kaitsmaks sensitiivset informatsiooni autoriseerimata ligipääsu ja muutmise eest. Põhilisteks suundadeks on ka krüptograafiatehnoloogia ja rakendused, autentimine, avaliku võtme infrastruktuur, internetiturvalisus ja turvalisuse juhtimine. Vastavad publikatsioonid on NIST-i uuringute ja avastuste resultaadiks turvalisuse vallas. Publikatsioonid on avaldatud kui *Special Publications*, *NIST Internal Reports*

ja ITL (tegelikult siis CSD) bülletäänid. *Special Publications* sisaldab 500-seeriat (Infotehnoloogia) ja 800-seeriat (Arvutiturvalisus).

800-seeria hulgas on ITL näiteks koostanud detailse riskihalduse juhise - *Risk Management Guide for Information Technology Systems* (Stoneburner, Goguen, Feringa, 2003), mis püüab aidata ettevõtteid IT riskide efektiivsemal haldamisel. (vt. ka peatükk 3.3. "Riskianalüüsi vahendid")

3.1.1.2 NSA – National Security Agency

The *National Security Agency* – NSA (vt. <http://www.nsa.gov/>) - koordineerib, juhendab ja viib läbi spetsialiseeritud toiminguid kaitsmaks USA infosüsteeme, samuti vahendab ta sellealast välismaist informatsiooni

Rainbow Series on kogumik 37-st dokumendist (The *National Security Agency* 2003), mis on adresseeritud erinevatele arvutiturbealasele valdkonnale (Iga dokument on erinevat värvi, sellest on tulnud ka nimetus "Vikerkaare seeria"). Peamine dokument selles seerias on "Trusted Computer System Evaluation Criteria – TCSEC (5200.28-STD, Orange Book)" usaldatava infotehnoloogiasüsteemi arendamise kriteeriumid, aastast 1985. See dokument defineerib seitse erinevat usaldatavuse taset, mida on võimalik saavutada järgides "Trusted Product Evaluation Program (TPEP)" antud juhiseid:

- Functionally Tested
- Structurally Tested
- Methodically Tested and Checked
- Methodically Designed, Tested, and Reviewed
- Semiformally Designed and Tested
- Semiformally Verified Design and Tested
- Formally Verified Design and Tested

3.1.1.3 BSI - Bundesamt für Sicherheit in der Informationstechnik

BSI - *Bundesamt für Sicherheit in der Informationstechnik* (vt. <http://www.bsi.de>) - Saksamaa Infoturbe Riigiamet - on välja töötanud IT etalonturbe teatmiku – *IT Baseline Protection Manual* (IT Baseline Protection Manual, 2001), mille eesmärk on saavutada organisatsiooniliste, personalikesksete, infrastruktuuriliste ja tehniliste tüüpsete turvameetmete asjakohase rakendamisega teatav IT-süsteemide turva-

standard, mis oleks adekvaatne ja piisav kesktaseme turvanõuete mõttes ning võiks olla aluseks kõrgemat kaitseastet nõudvate IT rakenduste puhul.

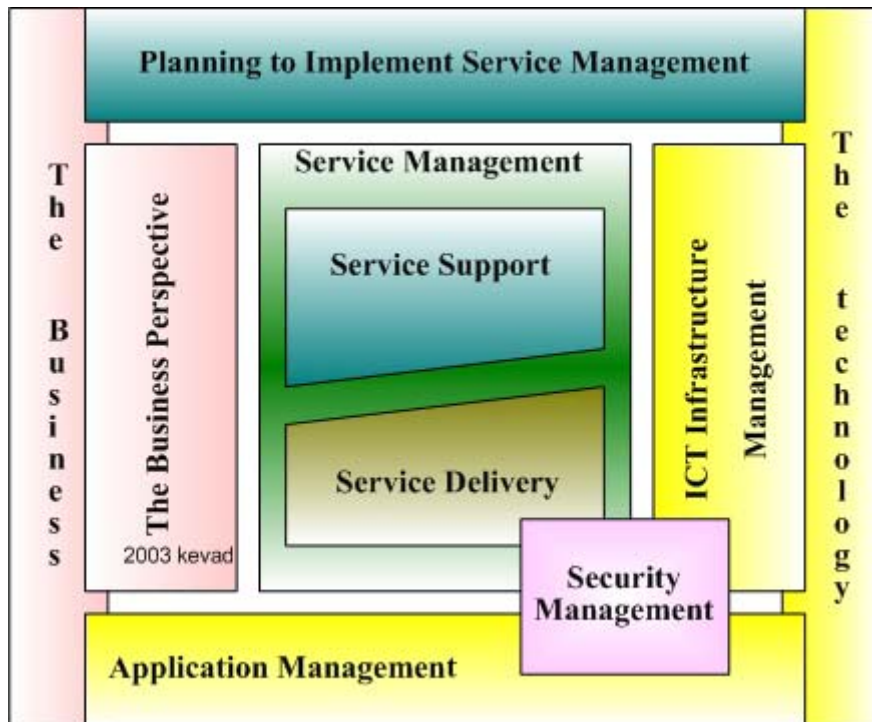
Sel eesmärgil soovitab IT etalonturbe teatmik vastumeetmete komplekte tüüpiliste IT konfiguratsioonide, keskkondade ja organisatsiooniolude tarbeks. Selle teatmiku koostamisel eeldas Saksa Infoturbe Riigiamet riiklike institutsioonide riskianalüüsil saadud hinnanguid teadaolevate ohtude ja nõrkuste põhjal 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. Seega muutub IT etalonturbe üldise kokkuleppe aluseks turvameetmete kohta, mis on vajalikud kesktaseme kaitse nõuete täitmiseks.

IT Baseline Protection Manual-i on detailsemalt vaadeldud peatükis 3.3 “Riski-analüüsi vahendid”

3.1.1.4 OGC - The Office of Government Commerce

Inglismaal põhiliselt riigihangete korraldusega tegeleva ametiasutuse OGC– *Office of Governmental Commerce* (vt. <http://www.ogc.gov.uk/>) poolt on koostatud ka IT hangete alaseid juhendmaterjale, mis on koondatud IT Infrastructure Library-sse (ITIL). ® ITIL on OGC poolt registreeritud kaubamärk (vt. <http://www.itil.co.uk/>) ITIL on juhised praktikutele, kuidas korraldada IT teenuste haldust ettevõttes. ITIL koostati 80-ndatel aastatel Inglismaal *Central Computing and Telecommunications Agency* poolt. Praegu arendatakse edasi OGC egiidi all. ITSMF (*IT Service Management Forum*) tunnistas ja soovitas ITIL dokumentide kasutamist, need on kujunenud de facto standardiks Inglismaal.

Järgnev joonis kirjeldab ITIL publikatsioonide perekonda.



Joonis 4 ITIL publikatsioonide perekond.

Iga raamat käsitleb oma valdkonda. Raamatus antakse juhtnöörid, mida on vaja teha kindlustamiseks vaadeldava valdkonna toimimine. Raamatuid on seitse.

1. *Service Support* – Teenuste tugi

- Help Desk
- intsidentide haldus
- probleemide haldus
- konfiguratsiooni haldus
- muudatuste haldus
- versioonihaldus

2. *Service Delivery* - Teenuste tarnimine:

- teenustasemete haldamine
- IT teenuste finantsjuhtimine
- mahtude haldamine
- käideldavuse haldamine

3. *ICT Infrastructure Management* - IKT infrastruktuuri haldus

- disain ja planeerimine
- ellurakendamine
- opereerimine
- tehniline tugi

4. *Security Management* - Turbehaldus
5. *Application Management* – Rakenduste haldus
6. *Planning to Implement Service Management* - Teenuste halduse juurutamise plaanimine
7. *The Business Perspective* - Äri plaanimine

Igas valdkonnas toodud:

- eesmärk
- skoop
- protsessi põhiolamus
- kasu tema juurutamisest
- planeerimine ja juurutamine
- põhitegevused
- rollid ja vastutus
- põhilised mõõdikud

Detailsem ülevaade ITIL vahenditest on toodud peatükis 3.3 “Riskianalüüsi vahendid”.

3.1.2 Rahvusvahelised eriala- ja standardimisorganisatsioonid

3.1.2.1 ISACA

Information Systems Audit and Control Association (ISACA) (vt. <http://www.isaca.org>) on infosüsteemide audiitorite tugiorganisatsioon, kes sertifitseerib infosüsteemide audiitoreid, avaldab auditialast kirjandust, töötab välja auditi metoodikaid, korraldab koolitust, algatab uurimis- ja arendustöid, avaldab ajakirja *IS Audit & Control Journal* ning korraldab viiel mandril rahvusvahelisi konverentse. Infosüsteemide haldamiseks, juhtimiseks ja auditiks on koostatud 1996 aastal CobiT (*Control Objectives for Information and Related Technology*) (IT Governance Institute 2000)

CobiTi kolmas trükk tuli välja 2000 aastal kui ”avatud standard” S.t ISACA loodab, et sellest kujuneb laialt aktsepteeritud IT-juhtimise metoodika. CobiT-i eesmärgiks on pakkuda IT turbe ja juhtimise selge poliitika ja üldtunnustatud head toimimisviisid eelkõige ärieesmärkide vajaduste seisukohalt vaadates. CobiT-it arendatakse pidevalt edasi, uurimistöö ja avaldamine tehakse võimalusel Pricewaterhouse Coopersi

heakskiidul ja ISACA liikmete toetusel. Uurimismaterjal saadakse Euroopa turvalisuse Foorumi (*European Security Forum* (ESF)) ja Gartner Groupi abil. CobiT-it kui töövahendit on detailsemalt analüüsitud peatükis 3.3.5. "Riskianalüüsi vahendid".

3.1.2.2 ISO - International Organization for Standardization

Rahvusvaheline Standardimisorganisatsioon ISO (<http://www.iso.ch/>), mille liikmeteks on rahvuslikud standardiorganisatsioonid, arendab infoturvet käsitlevaid standardeid infotehnoloogia standardimise ühendkomitee JTC1 all, kus töö toimub üheaegselt nii ISO kui ka IEC (*International Electrotechnical Commission*, <http://www.iec.ch>) egiidi all. Infoturbealased standardeid töötatakse välja allkomitee SC27 raames, aga mõned kasulikud dokumendid tekivad ka teistes komiteedes, nagu näiteks panganduse IT lahendustega tegelev TC68.

ISO poolt ongi olulisemateks panusteks infoturbealasessse tegevusse valdkonna käsitlelust ühtlustavad turbehalduse standardid ning paljud turvamehhanismide standardid. Riskianalüüsi metoodilisi aluseid käsitletakse põhiliselt standardites ISO/IEC 13335 ja ISO 13569 juhiseid sisaldab ka BS 7799 (*British Standards Institute* 2003), baasil välja töötatud uuem standard ISO/IEC 17799 (EVS - ISO/IEC 17799:2003).

3.1.3 Infoturbealaseid standardeid

3.1.3.1 ISO 13335 "Infotehnoloogia. Infoturbe halduse suunised"

Standardi eesmärk on anda suuniseid infoturbe halduse aspektide kohta, alustades mõistete struktuuri selgitamisest ja lõpetades konkreetsete rakendusjuhiste ning dokumendi näidisstruktuuridega. See standard on tõlkemeetodil üle võetud ka Eesti standardiks.

Standard koosneb järgmistest osadest :

- ISO/IEC TR 13335-1 "Infoturbe mõisted ja mudelid"(EVS-ISO/IEC TR 13335-1, 1999)
- ISO/IEC TR 13335-2 "Infoturbe haldus ja plaanimine" (EVS-ISO/IEC TR 13335-2, 1999)
- ISO/IEC TR 13335-3 "Infoturbe halduse meetodid" (EVS-ISO/IEC TR 13335-3, 1999)

- ISO/IEC TR 13335-4 “Turvameetmete valimine” (EVS-ISO/IEC TR 13335-4, 2000)
- ISO/IEC TR 13335-5 “Välisühenduste turvameetmed” (EVS-ISO/IEC TR 13335-5, 2003)

Standardi esimene osa annab ülevaate infoturbe halduse kirjeldamiseks kasutatavatest põhimõistetest ja mudelitest, järgmised osad kirjeldavad detailsemalt, kuidas neid mõisteid ja mudeleid saab asutuses tõhusalt kasutada.

Teine osa käsitleb tõhusa infoturbe programmiga seotud haldusprotsessi ja kohustusi. Kolmanda osa eesmärk on kirjeldada ja soovitada meetodeid infoturbe edukaks halduseks. Neid meetodeid võib kasutada turvanõuete ja riskide hindamiseks ning abivahendina asjakohaste turvameetmete, st. infoturbe õige taseme väljaselgitamisel ja säilitamisel. Standardi kolmanda osa lisad sisaldavad mõningaid kasulikke näiteid:

- Lisa A Üleüldise infoturbepoliitika sisukorra näide
- Lisa B Varade väärtustamine
- Lisa C Võimalike ohutüüpide loetelu
- Lisa D Tavaliste nõrkuste näiteid
- Lisa E Riskianalüüsi meetodite tüübid

Neljas osa annab suuniseid turvameetmete valimise kohta. On antud suunised olukordadeks, kus tuleb teha otsus IT-süsteemile turvameetmete valimiseks vastavalt IT-süsteemi tüübile ja tunnusomadustele, vastavalt turvaprobbleemide ja ohtude jämedatele hinnangutele, vastavalt detailse riskianalüütilise läbivaatuse tulemustele.

Lisaks neile suunistele on antud ristviited, mis näitavad, kus võivad turvameetmete valimisel abistada üldkättesaadavad teatmikud, mis sisaldavad turvameetmeid. Vaadeldav standard näitab ka, kuidas saab koostada ettevõtte kohast etaloniturbeteatmikku.

Standardi viies ja viimane osa annab infoturbe halduse eest vastutajale suuniseid võrkude ja side kohta. Need suunised aitavad piiritleda ja analüüsida sidega seotud tegureid, mida tuleks arvestada võrguturbe nõuete kehtestamisel.

3.1.3.2 ISO/IEC TR 13569 “Pangandus ja sellega seotud teenuste infoturbe suunised”

Kuna pankadel on nõutav riskitase kõrgem, siis on pankade jaoks välja töötatud täiendav turbehalduse standard ISO 13569 (ISO TR 13569 2000), kus käsitletud

meetmed on põhjalikumad, pöörates mõnele momentidele suuremat tähelepanu (rahandustehingute kaardid, rahaautomaadid, elektronarveldus). Ka see standard on tõlkemeetodil üle võetud Eesti standardiks.

ISO 13569 standardi kasulikke aspekte:

- Selge ja arusaadav nõrkuste, ohtude, riski liikide definitsioon ja loetelu.
- Riski hindamise maatriksi kirjeldus ja selle kasutamise juhised.
- Õpetused riski hindamise maatriksi täitmisel tuvastatud ohtude (nt. osakonna töötaja avaldab osakonnas oleva väärtvahendeid või konfidentsiaalset teavet sisaldava seifi lukukombinatsiooni) koos põhjendustega dokumenteerimise vajadusest.
- Suunised, et kui mõne äriefunktsiooni puhul on võib-olla mingi nõrkuse või terve nõrkuseliigi kaudu toimiva ohu kohta sobiv vastata "pole kohaldatav", tuleks dokumenteerida selle otsuse aluseks olev põhjendus.

Kindlasti on kasulikud ka lisa ära toodud turvaalaste dokumentide näidised. Nende hulka kuuluvad:

- Nõukogu otsus
- Üldpoliitika
- Töötaja teadlikkuse lisaleping
- Sisselogimise ja faksi hoiatused
- Infoturbe teate näidis
- Riski aktsepteerimise vorm
- Kaugtöötaja leping

Kuigi standardi nimetus viitab pangandusasutustele, on standard kasutatav igas suuruses ja igat liiki ettevõtetes, kes tahavad rakendada ettenägelikku, äriselt mõistlikku ja põhjalikku infoturbe programmi.

3.1.3.3 ISO / IEC 17799 ja BS7799 "Infotehnoloogia. Infoturbe halduse praktilised juhised"

Rahvusvahelise standardi ISO/IEC 17799 "Infotehnoloogia. Infoturbe halduse praktilised juhised" (EVS - ISO/IEC 17799:2003) algvariandi koostas Briti Standardiamet standardina BS 7799 (*British Standards Institute* - BSI 2003). Standardis käsitletavad teemad on turvapoliitika, turvaorganisatsioon, varade klassifitseerimine ja juhtimine, personaali turvalisus, füüsiline ja keskkonna

turvalisus, arvutite ja võrgu ohjamine, süsteemi ligipääsu ohje, süsteemiarendus ja hooldus, ettevõtte/äri tegevuskavad (sh häire- ja kriisiolukorra puhul), vastavus seadusandluse ja lepingulistele nõuetele. Selle standardi Eesti standardiks ülevõtmise protsess on lõppjärgus.

ISO/IEC 17799 juures rõhutatakse, et see ei ole lihtsalt IT turvalisuse standard, vaid informatsiooni turvalisuse standard. Informatsioon võib eksisteerida paljudes vormides. Ta võib olla välja trükitud või kirjutatud paberile, säilitatud elektrooniliselt, üle kantud kasutades postiteenuseid või elektroonilisi kanaleid pidi, näidatud filmina või edastatud vestluses telefonitsi. Ükskõik, mis vormis informatsioon on või liigub, ta peab alati olema vastavalt kaitstud.

Standardis pööratakse tähelepanu ka õiguslikust vaatepunktist olulisteks peetavatele turvameetmetele - intellektuaalse omandi õigused, andmekaitse ja isikuteabe privaatus. Turbevajaduse probleemi käsitleb standard vaid põgusalt (võrreldes eelnevalt vaadeldud standarditega) ja ei kirjelda ohtusid, ega nõrkusi. Riskianalüüsi asemel on vaadeldud turvariskide hindamist, mis iseenesest on ärilise kahju hindamine, mis võib tekkida tõenäolise turvarikke esinemisel, arvestades ohtusid, nõrkusi ning hetkel rakendatud turvameetmeid.

Turvameetmeid on kirjeldatud küllalt põhjalikult. Standard pöörab näiteks tähelepanu ka konfidentsiaalsuslepingutele - ajutistelt töötajatelt ja kolmandatest osalistest kasutajailt, kui neid juba ei seo kehtiv leping (mis sisaldab konfidentsiaalsuslepet), tuleks enne neile juurdepääsu andmist infotöötlusvahenditele nõuda konfidentsiaalsusleppe allakirjutamist.

Kokkuvõtlikult võiks öelda, et standardis on pearõhk meetmete loetlemisel. Standard võimaldab igat tüüpi ja suurusel organisatsioonides, kes on juba mõistnud infoturbevajadust, luua nende vajadusele vastav infoturbe süsteem standardis kirjeldatud meetmete abil.

3.1.3.4 CC- Common Criteria

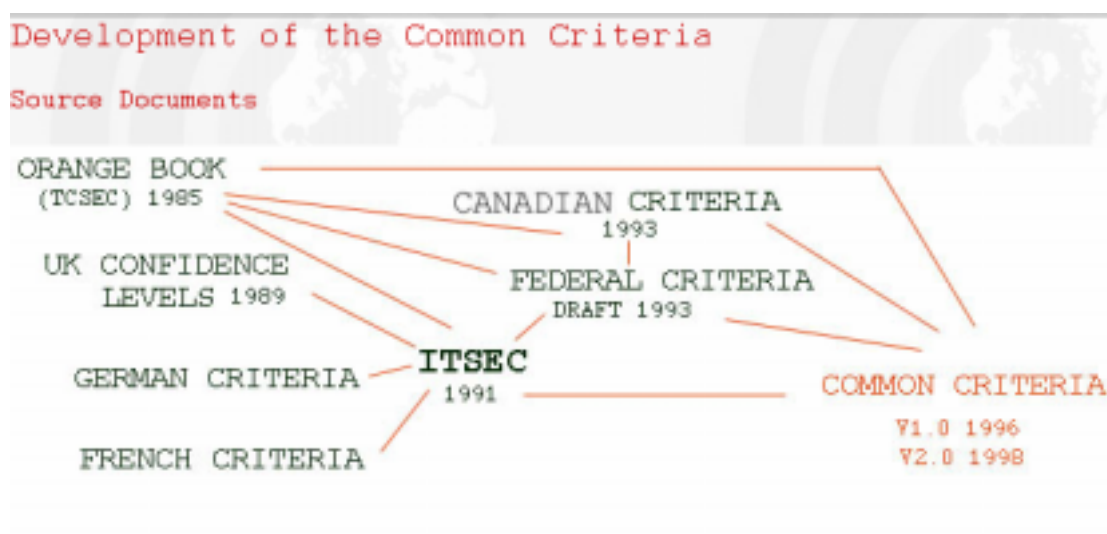
Common Criteria (CC) on rahvusvaheline ISO standard (ISO/IEC 15 408) tehnoloogilise infrastruktuuri toodete turvalisuse hindamiseks. Riskianalüüsiga seondub kaudselt – võimaldab hinnata juba rakendatud turvameetmete taset ja seega määratleda jääkriske.

Common Criteria uusim versioon 2.1 on pärit aastast 1999 ja see 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.

Hinnatav toode või süsteem CC terminoloogias on Target of Evaluation (TOE). TOE võib olla näiteks operatsioonisüsteem, andmevõrk, hajussüsteem või arvutiprogramm. CC vaatleb toodete käideldavust, terviklust ja töökindlust ja võtab arvesse ka inimtegevusest põhjustatud tahtlikud või ka tahtmatud ohud.

Uus toodete juurutamiseks välja arendatud rahvusvaheline süsteemide ja toodete juurutamise kriteerium - International Common Criteria –ICC (on harmoniseeritud kokkuvõtte Põhja- Ameerika (*Trusted Computer System Evaluation Criteria*, TCSEC) Kanada (*Canadian Trusted Computer Product Evaluation Criteria*, CTCPEC) ja Euroopa (*Information Technology Security Evaluation Criteria*, ITSEC) materjalidest, teostamaks IT andmeturbesüsteemide hindamist ja sertifitseerimist. (The IT security.com 2003)



Joonis 5 Common Criteria areng. (Common Criteria 2003)

3.1.4 Turbehalduse metoodilisest korraldusest Eestis

Eestis on süsteemne ja riigi poolt toetatud infoturbealane tugitegevus suhteliselt nõrk ja algusjärgus. Infoturbealase töö metoodika arendamisega Eestis otseselt ei tegeleta, mingil määral toimub metoodiliste materjalide kohandamine ja levitamine. On olemas asutusi ja ettevõtteid, kelle põhitegevusalade hulka kuulub ka infoturbe valdkond.

3.1.4.1 Eesti Andmekaitse Inspektsioon

Andmekaitse Inspektsiooni (<http://www.dp.gov.ee/?js=1>) põhiülesanneteks on

- sõltumatu järelevalve teostamine isikuandmete töötlemise ja andmekogude pidamise seaduslikkuse üle
- andmekaitsealase tegevuse korraldamine.

Andmekaitse Inspektsioon (AKI) alustas tegevust 1999. aasta jaanuaris ja tegelikult ongi AKI ainus riiklik institutsioon, kes on üritanud lisaks oma järelevalvetegevusele astuda ka konstruktiivseid samme, määratledes turvanõuete püstitamiseks vajaliku turvaklasside süsteemi (Riigi Infosüsteemide Arenduskeskus, 2003), mis kaudselt järgib Common Criteria nõuete püstitamise põhimõtteid ning millele on loodetud pakkuda ka vastavat etalonmeetmete struktuuri. Hetkel on need tegevused seoses suure järelevalvekoormusega ja hiljutiste umberkorraldustega IT-alastes juhtimisstruktuurides soikunud.

3.1.4.2 Cybernetica AS

Cybernetica AS (<http://www.cyber.ee/>) tegeleb mitmesuguste turvalahenduste väljatöötamisega, ent oma põhitegevuse kõrvalt on üritanud korrastada ka eestikeelset turvaterminoloogiat ja tagada eestikeelse õppekirjanduse kättesaadavus – Cybernetica poolt on koostatud esimesed eestikeelsed ülevaateraamatud “Infosüsteemide turve: Turvarisk” ja “Infosüsteemide turve: turbetehnoloogia”. Cybernetica metoodiline tegevus avaldub põhiliselt läbi Tallinna Tehnikaülikooli ja Tartu Ülikooli mitmete õppetoolide, mida toetatakse nii õppeprogrammide plaanimise kui õppejõududega.

3.1.4.3 AS Stallion

AS Stallion (vt. <http://www.stallion.ee/>) põhilisteks tegevusaladeks on

- andmeturvalisuse toodete ja teenuste pakkumine
- veebitehnoloogia alased teenused

Andmeturvalisuse valdkonnas on AS Stallion eesmärgiks hetkel kõrgekvaliteediliste ja maailmas tunnustatud turvatehnoloogiatoodete pakkumine Eesti ettevõtetele ja organisatsioonidele, samuti mitmesugused vastavad andmekaitse alased konsultatsioonid.

3.1.4.4 Domina Privacy & Security

Domina Security (vt. <http://www.dominasecurity.com/est/index.asp>) pakub uusi info-tehnoloogilisi lahendusi (Internet, VPN, UMTS, kodu automatiseerimine) ning tagab neile maksimaalse kaitse võimalike digitaalsete sissetungide eest. Pakutakse rida praktilisi ja teostatavaid turbelahendusi, alustades riskide kindlakstegemisest kuni nende hajutamiseni, riskianalüüs jääb tehnoloogia tasemele.

3.2 Riskianalüüsi meetodid

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

Turbehalduse standardites käsitletavat riskihalduse metoodikad koosnevad sisuliselt kahest osast – riskianalüüsist ning selle tulemite alusel turvameetmete plaanimisest. Tegelikult on ka riskihalduse meetodite põhierinevus ikkagi riskianalüüsi osas, st 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 turvaspektidele ligikaudsed tasemehinnangud ning nende abil tuvastada riskantsemaid kohti süsteemis. Kvantitatiivse analüüsi puhul üritatakse kõiki aspekte kirjeldada samades ühikutes.

3.2.1 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 väärtus kui ka kahju suurus hinnatakse rahaliselt, ka ainetute varade väärtusele (nt andmete terviklus) püütakse anda rahaline hinnang. St. kõik arvutused sooritatakse tõenäosustena rahalisel (vm. sellele analoogilisel) 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 summase kohta on olemas, annab kvantitatiivne riskianalüüs küllalt täpse tulemuse

Puudused:

- suur töömahukus ja ressursikulu (ohte ja nõrkusi on sadu)
- tõenäosuste leidmiseks vajalik ohtude statistika võib puududa või olla ebatäpne (nt. Eesti oludes), mis teeb selle meetodi pruukimise võimatuks

3.2.2 Kvalitatiivne riskianalüüs

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

Reeglina võetakse jämeda skaala põhjal arvesse järgmised tegurid:

- vara ahvatlevus (ründe puhul)
- hõlpsus, millega vara on muundatav hüvituseks (ründe puhul)
- ründaja tehnilised võimalused
- nõrkuste ära kasutatavuse määr
- ohu tegeliku realiseerumise sagedus

Puudused:

Realiseerumissageduste kohta on kasutuskõlblikke andmeid mõnevõrra raskem 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.

3.2.3 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 kuuluvad tegevuseesmärgid.
- organisatsiooni tegevuse sellest infotehnoloogilisest süsteemist sõltuvuse määra, st. kas funktsioonid, mida organisatsioon peab kriitiliseks oma püsijäämisele või tegevuse tõhusale sooritamisele, sõltuvad sellest süsteemist või selles süsteemis töödeldava informatsiooni konfidentsiaalsusest, terviklusest, käideldavusest, jälitatavusest, autentsusest ja töökindlusest.
- Sellesse infotehnoloogilisse süsteemi investeerimise tase süsteemi väljatöötamise, hoolduse või asendamise terminites, selle infotehnoloogilise süsteemi varad, 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.

Jämeda riskianalüüsi meetodi kohaldamine ühendatult etalonturbe meetodiga ja vastavalt vajadusele sooritatava detailse riskianalüüsiga pakub enamikule organisatsioonidele tõhusaimat edenemisteed.

3.2.4 Detailne riskianalüüs

Detailne riskianalüüs sisaldab varade põhjalikku väljaselgitamist ja hindamist, neid varasid ähvardavate ohtude hindamist, nõrkuste hindamist. Nende hindamiste tule-

musi kasutatakse seejärel lähteandmetena riskide hindamiseks ja sellest tulenevalt põhjendatud turvameetmete väljaselgitamiseks.

Detailse riskianalüüsi puhul:

- 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

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.

Tõsine puudus: tulemuste saamine nõuab üsna palju aega, vaeva ja oskusi.

Järeldus: detailne riskianalüüs tasub ära vaid kallite ülioluliste infosüsteemide korral, kus arendustööle on jäetud piisavalt aega ja raha. 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.

3.2.5 Etalonturbe

Etalonturbe meetod on peamiseks alternatiiviks detailsele riskianalüüsile juhul, kui viimast ei võimalda realiseerida rahalised või ajalised ressursid. Sisuliselt tähendaks 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, finants-institutsioonid jms.).

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.

Eelised:

- mistahes muu riskianalüüsi meetodiga võrreldes kulub (mõni suurusjärg) vähem ressursse — aeg, raha, töö, spetsialistid.
- samu meetmeid saab rakendada paljudele erinevatele süsteemidele.

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 üha piisavad).
- unikaalse arhitektuuriga infosüsteemide korral võib mõni valdkond jääda katmata ja tekitada ülisuure turvariski.

3.2.6 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 konfidentsiaalsustaseme) jaoks.
2. Infosüsteemi kriitilistes valdkondades ja unikaalse arhitektuuriga osades kasutatakse detailset riskianalüüsi, mujal aga odavamat etalonturbe metoodikat.

Eelised:

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

Puudused:

- võrreldes detailse riskianalüüsiga annab ta siiski vähem tõepärasema pildi.
- võrreldes etalonmetoodikaga on ta kallim.

3.2.7 Mitteformaalne metoodika

Mitteformaalne metoodika on alternatiiv eeltoodud süsteemsetele lähenemistele, kuigi ka need ei kuulu tegelikult formaalsete meetodite hulka.

Mitteformaalse riskihalduse metoodika korral ei põhine riskide hindamine mitte abstraktsetel meetoditel, vaid spetsialistide (oma töötajad, välised konsultandid) kogemusel.

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.

Eelised:

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

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.

3.2.8 Formaalsed meetodid

Formaalsed infosüsteemide riskianalüüsi meetodid on alles arenemisjärgus ja nende tase süsteemide erinevate komponentide lõikes on erinev. On mitmeid andmebaaside turvaaspektide kirjeldamiseks ja siis ka formaalseks riskide analüüsiks kasutatavaid meetodeid (Castano S., Fugini M., Martella G., Samarati P.1995), ent ka need keskenduvad tsentraalsetele lahendustele. On tehtud katsetusi turvaatribuutide lisamiseks süsteemianalüüsiks kasutatavatele SADT-tüüpi meetoditele (Ziya Aktas A. 1987), ent praktiliseks kasutamiseks sobilikke formaalseid meetodeid praegusel hetkel ei eksisteeri. Pigem võib pseudoformaalseks meetodiks nimetada panganduse turvastandardis (ISO TR 13569 kavand, 2000) pakutud riskimaatriksi kasutamist.

3.3 Riskianalüüsi vahendid

Metoodikad leiavad praktikas rakendust enamasti siis kui need on toetatud vastavate tugivahenditega. Riskianalüüsi toekas on väljatöötatud erinevaid vahendeid. On koostatud nii dokumente - juhiseid, mille punktuaalsel järgimisel saab koostada ettevõtte riskianalüüsi kui ka automatiseeritud vahendeid, kus küsimustele vastamise järgselt programm võib genereerida olemasolevate riskide ülevaate ja nende üldise mõju äritegevusele, ettepanekud täiendavate turvameetmete rakendamiseks, pakutavad lahendused turbe tagamiseks.

V.Hansoni andmetel (Hanson, Buldas, Martens, Lipmaa, Ansper, Tulit, 1997, 78)

võrreldes analüüsiküsimustike "käsitsi" töötlemisega annab niisugune tarkvara enamasti 50 kuni 70% ajasäästu. Riskianalüüsi tarkvara paketid, mis esitavad lähteandmete saamiseks sadu küsimusi, võimaldavad tavaliselt sooritada nii kvantitatiivset kui ka kvalitatiivset analüüsi.

3.3.1 Risk Management Guide for Information Technology Systems.

ITL on koostanud detailse riskihalduse juhise - Risk Management Guide for Information Technology Systems. (Stoneburner, Goguen, Feringa , 2001)

Juhis püüab aidata ettevõtteid IT riskide efektiivsemal haldamisel.

1. osa annab ülevaate riskihaldusest – kuidas riskihaldus kuulub IT süsteemi arengutsükklisse, kuidas peab olema jagatud vastutus ja kes peavad osalema riskihalduse protsessis.
2. osa kirjeldab riskianalüüsi metoodikat ja riskihalduse üheksat sammu.
3. osa kirjeldab riskide vähendamise strateegiat, turvameetmeid, tasuvuse analüüsi, kontrollmeetmeid, jääkriski.
4. osas pööratakse tähelepanu sellele, et iga infosüsteem areneb ja on pidevas muutuses, millest johtuvalt tuleb hoida ka riskihaldus pidevas liikumises. Vastavalt IT süsteemide arengule muutuvad ka riskid, ohud ja nõrkused, seetõttu tuleb riskihaldusega pidevalt tegeleda ja hoida see ajakohasena.

Lisas tuuakse ära näited intervjuu küsimustikust andmete kogumisel (interview questions), riskianalüüsi (lõpp)aruandest (risk assessment report outline) ja riskide halduse plaanist (safeguard implementation plan summary table).

Edaspidisel Elektroskandia AS riskianalüüsi teostamisel on tuginetud ka NIST poolt välja töötatud IT süsteemide riskihaldusjuhisele - *Risk Management Guide for*

Information Technology Systems. NIST poolt pakutud riskihalduse 9 sammu kergendavad riskihalduse väljatöötamist ja juurutamist :

1. IT süsteemi kirjeldamine
2. ohtude kirjeldamine
3. nõrkuste kirjeldamine
4. olemaolevate ja plaanitavate turvameetmete analüüs
5. tõenäosuste hindamine
6. toime analüüs
7. riskianalüüs
8. turvameetmete valimine
9. dokumenteerimine

3.3.2 IT Baseline protection manual ja selle tugitarkvara GSTOOLS

BSI (Bundesamt für Sicherheit in der Informationstechnik) Saksamaal on koostanud riigiasutuste turvalisuse tagamiseks juhendmaterjalid- IT Baseline Protection Manual (*IT Baseline Protection Manual, 2001*), mille koosseisu kuuluvad:

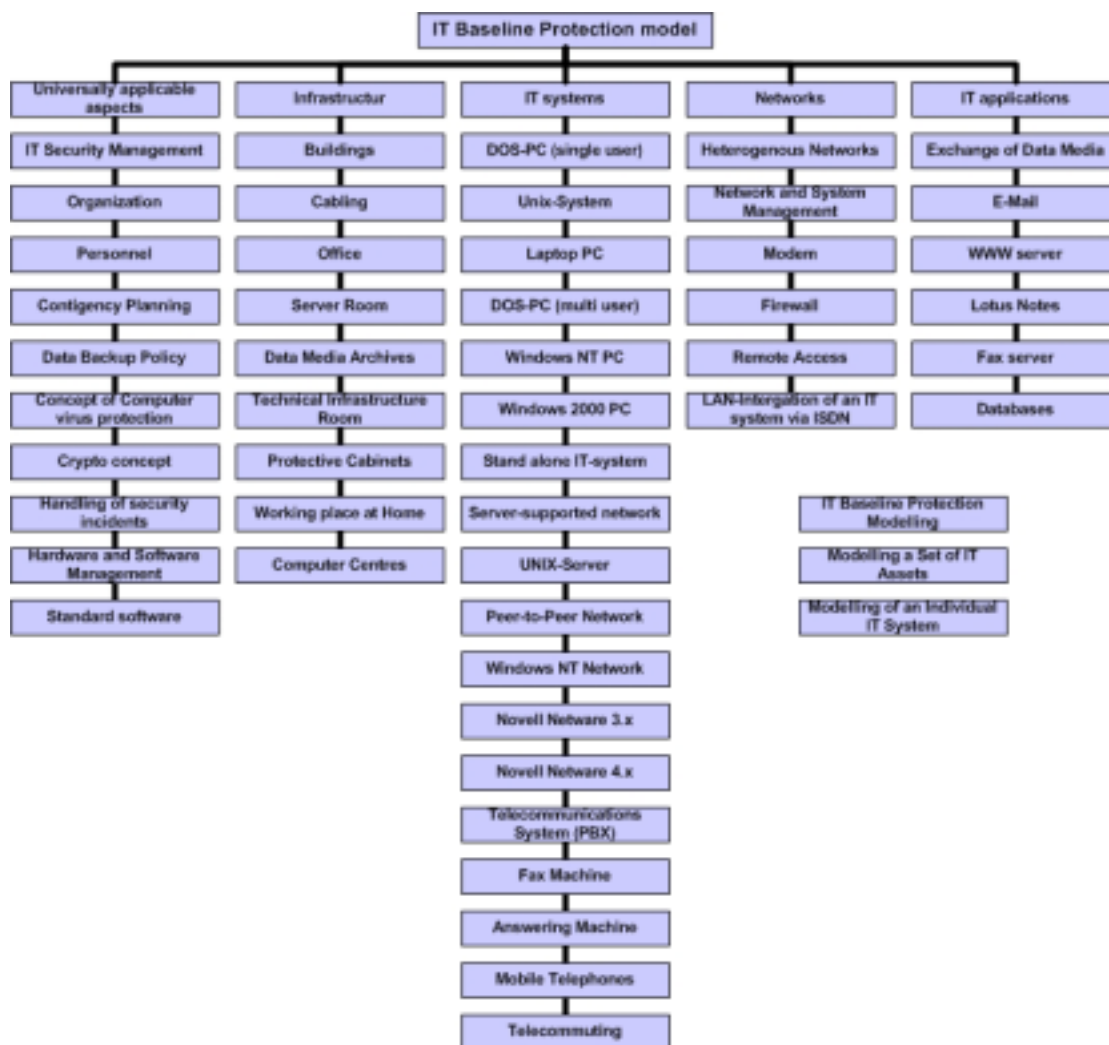
- Tüüpmodulite kataloog
- Modulite turvaspetsifikatsioonid (O / M)
- Ohtude (O) kataloog
- Turvameetmete (M) kataloog

Varade kaardistus toimub tüüpmodulitena, mille kirjeldused on kataloogis ette antud.

On viis moodulite klassi:

1. Organisatsiooni universaalsed aspektid – kohustuslikud alati, kui vastavad moodulid puuduvad, tuleb nad lisada (turbehalduse korraldus, intsidendikäsitus, viirusetõrje jms.)
2. Infrastruktuur – hoone, kaabeldus, torustikud jms.
3. Infotehnoloogiaseadmed – personaalarvuti olenevalt kasutatavast operatsioonisüsteemist, võrku ühendatud arvuti, server, arvutivõrk olenevalt võrgu tüübist jms.
4. Sidevõrgud – võrguhaldus, võrguseadmed: modem, marsruuter, tule müür, kaugpöördus jms.
5. Infotehnoloogilised rakendussüsteemid – e-post, veebiserver, andmebaasid, dokumendihaldussüsteem (Lotus Notes) jms.

Sisuliselt on vaja kirja panna, millised tüüpmodulid vaadeldavas infosüsteemis esinevad (näiteks võrkühendatud arvuti, modem, server). Iga mooduli kohta on koostatud tema turvaspetsifikatsioon, milles on ära näidatud sellisele süsteemile tavaliselt (= tavapärares Saksa riigiasutuse tingimustes) mõjuvad ohud ning vajalikud turvameetmed. Ohtude ja turvameetmete täpsemad kirjeldused on ära toodud vastavalt ohtude ja turvameetmete kataloogides:



Joonis 6 Objekti liigendus tüüpkomponentideks
(IT Baseline Protection Manual , 2003)

Ohtude kataloogis on hetkel ohte kokku 236, alamkataloogideks

- O.1 Vääramatu jõud
- O.2 Organisatsioonilised puudused
- O.3 Inimeksitused
- O.4 Tehnilised rikked
- O.5 Sihilikud ründed

Meetmete kataloogis on hetkel turvameetmeid kokku 477, alamkataloogideks

M.1 Infrastruktuuriga seotud meetmed

M.2 Organisatsioonilised meetmed

M.3 Personaliga seotud meetmed

M.4 Riistvara ja tarkvara turvameetmed

M.5 Sideturbe meetmed

M.6 Tegevuse katkematuse plaanimisega seonduvad meetmed

Kõiki katalooge uuendatakse vajadusel iga 6 kuu järel.

Näide:

Vaatleme näiteks moodulit serveriruum. Mooduli turvaspetsifikatsioonist saame teada, millised on BSI hinnangul serveriruumile mõjuda võivad ohud:

Stiihilised ohud:

T 1.4 Tuli

T 1.5 Vesi

T 1.7 Lubamatu temperatuur ja niiskus

Organisatsioonilised puudused:

T 2.1 Eeskirjade puudumine/puudused

T 2.6 Lubamatu sisenemine

Tehnilised rikked:

T 4.1 Toitekatkestus

T 4.2 Sisemiste tehnovõrkude rike

T 4.6 Pinge kõikumine/ ülepinge/ alapinge

Ründed:

T 5.1 IT-vahendite manipuleerimine/hävitamine

T 5.2 Andmete või tarkvara manipuleerimine

T 5.3 Volitamatu sisenemine hoonesse

T 5.4 Vargus

T 5.5 Vandalism

Turvameetmed

Turvameetmed, mida pakub välja “IT Baseline Protection Manual” serveriruumile

Infrastruktuur:

S 1.3 Jaotussüsteemi asjakohane segmentimine

- S 1.7 Käsikustutid
- S 1.8 Ruumi valik tulekoormust arvestades
- S 1.10 Tulekindlad uksed
- S 1.15 Suletud aknad ja uksed
- S 1.18 Valve- ja tuletõrjesignalisatsioon
- S 1.23 Uste lukustamine
- S 1.24 Veetorustike vältimine
- S 1.25 Ülepingekaitse
- S 1.26 Avariilülid
- S 1.27 Õhu konditsioneerimine
- S 1.28 Kohalik puhvertoiteallikas [UPS]
- S 1.31 Rikete kaugindikatsioon

Organisatsioon:

- S 2.14 Võtmehaldus
- S 2.16 Välispersonali/külastajate järelevalve/saatmine
- S 2.17 Sisenemise eeskirjad ja reguleerimismeetmed
- S 2.18 Kontrollülevaatused
- S 2.21 Suitsetamise keeld

Arvestades seda, et BSI –s iga mooduli kohta on koostatud tema turvaspetsifikatsioon, milles on ära näidatud sellisele süsteemile tavapärastes Saksa riigiasutuse tingimustes mõjuvad ohud ning vajalikud turvameetmed, ei ole kindlust, et need ohud ja meetmed sobivad Eesti tingimustes - Eesti väikeettevõtetele. Samas on meetod suhteliselt vähe töömahukas kui ettevõttele need tavapärased tingimused sobivad.

BSI on oma metoodika toeks arendanud ka automatiseeritud turbehaldusvahend - *IT Baseline Protection Tool* - GSTOOL. (BSI 2003) GSTOOL on tarkvara, mille abil on võimalik kasutajatel 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

- Kasutada auditeerimisvahendeid
- Teostada turvalisuse kontrolltesti.

GSTOOL on saksakeelsena vabalt internetist allalaetav (BSI 2003).

3.3.3 COBRA

COBRA – “*Consultative, Objective and Bi-functional Risk Analysis*” on riskianalüüsi vahend, mis võimaldab määratleda ettevõtte varadele mõjuda võivaid ohte ja ettevõttes esinevaid nõrkusi. Analüüsi tulemusena pakub süsteem lahendusi ja soovitusi nendega toime tulekuks. Samuti näidatakse kasutajale, millist mõju vastava ohu või nõrkuse tegelik toimimine ettevõttele võib tuua. Toote 15 päevane prooviversioon on internetist allalaetav . (C & A Security Risk Analysis Group 2003)

COBRA moodul “Risk Consultant“ pakub kompleksset riskianalüüsi teenust, mis hõlmab nii kvalitatiivse kui ka kvantitatiivse riskianalüüsi metoodikat. See on küsimustikul põhinev infosüsteem, mis kasutab eksperthinnanguid.

Riski hindamine COBRA abil sisaldab 3 etappi: küsimuste koostamine, riski hindamine, aruannete generaator.

3.3.3.1 Küsimuste koostamine

Antud etapis süsteem küsib kasutajalt, milliseid aspekte kasutaja soovib ettevõtte puhul hinnata. Valida on:

- Kõrge tundlikkusega süsteemide riskianalüüs
- IT turvalisuse riskianalüüs
- IT ja äripoolse riskianalüüs
- e-kaubanduse infrastruktuuri riskianalüüs

Järgmisena küsitakse, mida me soovime hinnata, kas

- Käideldavust
- Mõju äriprotsessidele
- Konfidentsiaalsust
- Terviklust.

Vastavalt tehtud valikutele, koostab süsteem automaatselt süsteemi salvestatud ekspertteadmiste põhjal küsimustiku.

3.3.3.2 Riski hindamine

Antud moodulis kasutaja vastab eelnevalt koostatud küsimustiku küsimustele. Vastused on valikuvariantidega. On nii lühivastuseid, ja/ei vastuseid, kui ka valikvastuseid.

3.3.3.3 Aruannete generaator

Aruande generaator seab vastavusse küsimuste vastused ja baasis talletatud ekspertteadmised ning on võimeline koostama iga mooduli osas aruandeid.

Aruanded koostatakse formaadis, mis peaks olema arusaadav kõikidele töötajatele ja vormistatakse kõiki äridokumendi reegleid jälgides. Pakutavaid aruande aspekte:

- Ettepanekud täiendavate turvameetmete rakendamiseks
- COBRA poolt pakutud lahendused turbe tagamiseks
- Suhteline riski hinnang iga riski kategooria kohta igas vaadeldavas valdkonnas
- Riskide üldine mõju äritegevusele
- Konkreetsete riskantsete valdkondade võimalikud rahalised ja ärilised seosed

Kõikide aruannete nimetusi ja sissejuhatavat teksti saab muuta vastavalt ettevõtte vajadustele ja soovidele.

3.3.3.4 Eksperthinnangute andmebaas.

COBRA sisaldab moodulit “Module Manager”, mille abil saab muuta süsteemis olevat eksperthinnangute andmebaasi või ka luua täiesti uut.

Olemasolevad eksperthinnangute teadmusbaasid:

- IT-Secty: the *IT Security Risk* Knowledge Base
- Op-Risk: the *Operational Risk* Knowledge Base.
- QwickRisk: the *QuickRisk or High Level* Knowledge Base
- E-Struct: the *E-Structure or Network* Knowledge Base

Kaks esimest on vajalikud detailse ja üldlase riskianalüüsi teostamiseks. Kolmandat kasutatakse kui on vaja saada kiiresti IT süsteemile üldlasi hinnangut. Viimane on koostatud spetsiaalselt võrgupõhiste süsteemide hindamiseks.

COBRA puhul ei toimunud ei varade ega ohtude kaardistamist, kasutati ekspertteadmist. 15 päevase prooviversiooni kasutamise käigus selgus, et infovarade ja kahjude hindamise korral pakutud rahalised väärtused Eesti oludesse ei sobi – Eestis on vähe nii suuri firmasid, mis suudaksid neisse mõõdikutesse mahtuda. Seega tuleks

kohe kasutada “Module Manageri”, et muuta eksperthinnangute andmebaasis kahjude hindamise mõõtesuurus.

Arvestades COBRA täisversiooni kohta toodud kirjeldusi, võib oletada et selle süsteemi kasutamine Eesti oludes oleks reaalne, kui eksperthinnangute andmebaasi viia sisse Eesti oludes vajalikke teadmisi (avaliku teabe seadus, isikuandmete kaitse seadus, riigisaladuse seadus) ja infoturbe tagamise alaseid toimingud, kohandades süsteemi kasutamiseks väikeettevõtetes. Sel juhul oleksid COBRA poolt pakutavad lahendused turbe tagamiseks igati vajalikud ja kasulikud. Kasutamisele eelnev eeltöö võiks tellida riiklike vahenditega mõne infoturbeteenuseid pakkuva firma käest, et saavutada täielik ja kasutamiskõlbulik baas, kuna ühe väikeettevõtte jõust ilmselt ei piisa vajaliku universaalsusega produkti loomiseks. Samuti peaks ka hoolitsetama süsteemi pideva arengu ja täiendamise eest.

3.3.4 OCTAVE

OCTAVE - *Operationally Critical Threat, Asset, and Vulnerability Evaluation* (Software Engineering Institute CERT® Coordination Center 2003), on riskianalüüsi teostamise juhend, mida võib iga firma ise oma riskianalüüsi tegemiseks kasutada ja mis:

- näitab, kuidas tegutseda, et saavutada ettevõttes turvalisus.
- aitab kirjeldada kriitilised varad, ärinõuded, ohud ja nõrkused.
- aitab võrrelda ettevõtte turvalisust heade turvatavadega.
- aitab koostab turbeplaani.

Riski hindamine vahendiga OCTAVE koosneb 3 faasist:

Esimeses etapis: kirjeldatakse ettevõtte varad; kirjeldatakse ohud, mis võivad mõjuda varadele; kirjeldatakse turvaabinõud, mida ettevõtte juba kasutab; kirjeldatakse organisatsioonilised nõrkused ja ka turva nõuded. Tööprotsessi peaks olema kaasatud kogu firma: nii juhtkond, keskastme juhid kui ka alluvad.

Teises etapis on põhitähelepanu all infosüsteemi infrastruktuur. Uuritakse nõrkusi, mis võivad võimaldada infosüsteemi autoriseerimata kasutamist.

Kolmandas etapis koostatakse Turvastrateegia ja turvaplaanid

3.3.4.1 Ettevõtte varadest lähtuva võimalike ohtude profiili koostamine

OCTAVE toob ära **varade liigid**, mille alla kõik ettevõtte varad tuleb jaotada:

- Informatsioon
- Infosüsteemid
- Teenused ja programmid
- Inimesed

OCTAVE järgi **mõjud**, mida võib kaasa tuua ohtude realiseerumine on:

- Varad on volitamatu avalikustatud
- Varasid on volitamatu muudetud
- Varad on kaotatud või lõhutud
- Varadele ei pääse ligi

OCTAVE järgi on ohul järgmised iseloomustavad **omadused**:

- Vara, mida ta ohustab
- Tegija – kes või mis ohustab varasid
- Motivatsioon – kas ettekavatsetud või juhuslik
- Ligipääs - kuidas ligipääs varadele saab võimalikuks (andmeside, füüsiline rünne)
- Otsene mõju (andmete: avaldamine, muutmine, hävitamine, eemaldamine, kättesaadavuse kadumine)

OCTAVE jagab ohud järgmistesse **kategooriatesse**:

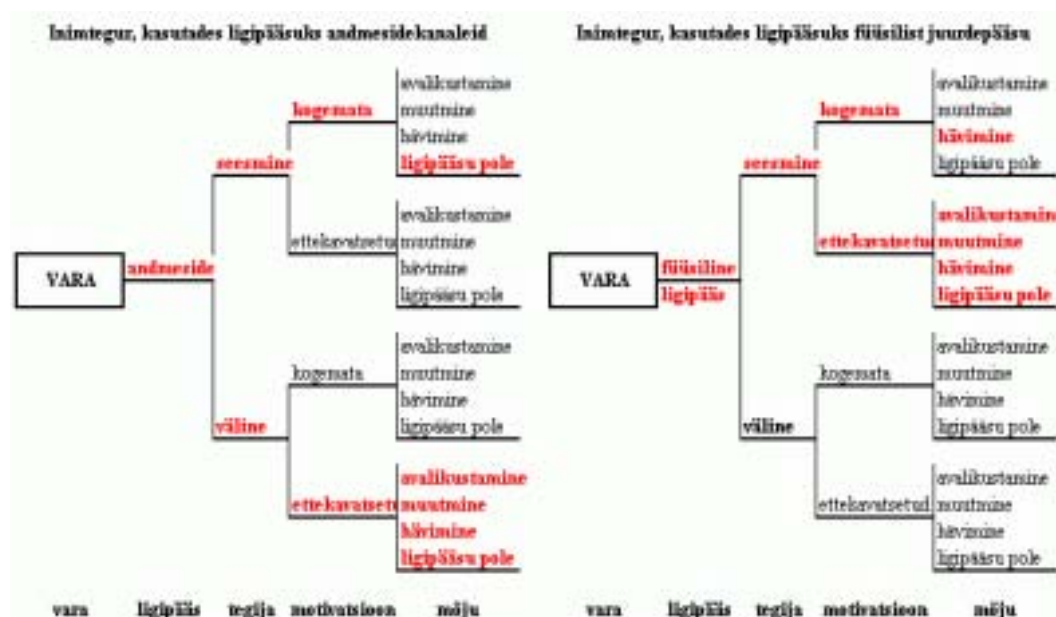
- Nii juhuslikud kui tahtlikud võrgupõhised ohud organisatsiooni kriitilistele varadele. Seotud inimteguriga.
- Nii juhuslikud kui tahtlikud füüsilised ohud organisatsiooni kriitilistele varadele. Seotud inimteguriga.
- Infotehnoloogiliste süsteemide põhjustatud ohud – riistvara defektid, tarkvara tõrked, süsteemide käideldavuskaod, viirused, piraattarkvara jms;
- Ohud, mis ei ole ettevõtte kontrolli all – loodusõnnetused (üleujutused, tormid..), aga ka sidussüsteemidest tulenevad riskid – kriitilise infrastruktuuri, elektri- ja sidevõrkude katkestused jms.

Esimese etapi lõpuks on ettevõttel kirjeldatud varad, varasid ähvardavad ohud ja ohtude realiseerumisel tekkiv kahju.

OCTAVE juhendeid jälgides, saab ettevõtte kõigi varade kohta ohtude profiili.

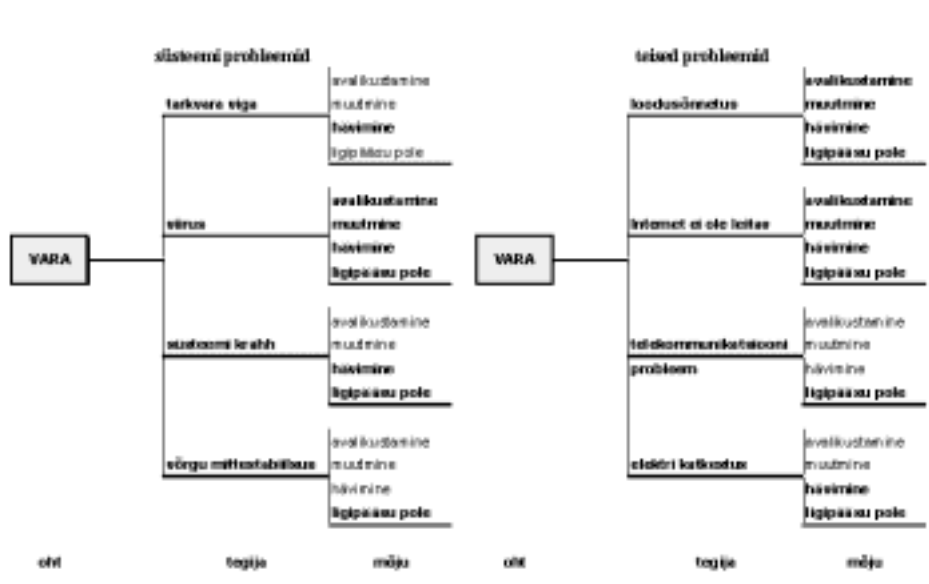
Ohtude profiilid esitatakse puukujulisena. Iga ohtude kategooria kohta saab kirjeldada oma puu.

Näiteks vara – “VARA” ohustatus inimese poolt kasutades andmesidekanalit või füüsilise juurdepääsu võimalust.



Joonis 7 “VARA” ohustatus inimese poolt (Alberts C. Dorofee, A., 2001)

Näiteks vara – “VARA” ohustatus süsteemi vigade poolt või väljastpoolt ettevõtet tulevate vigade poolt.



Joonis 8 “VARA” ohustatus süsteemi vigade poolt (Alberts C. Dorofee, A., 2001)

3.3.4.2 Infrastruktuuri nõrkuste määratlemine

OCTAVE järgi iga tehnoloogiline süsteem omab tehnoloogilisi nõrkusi, millega ettevõttel tuleb arvestada. OCTAVE nõuab, et jälgitaks kasutatava tehnoloogia kohta

registreeritud teadaolevaid nõrkusi . Nõrkuste andmebaas - Common Vulnerabilities and Exposures - CVE (CVE 2003) - on kõigile tasuta ja vabalt kasutatav.

Analoogiliselt ohtude profiilile koostatakse ka nõrkuste profiilid.

3.3.4.3 Turvastrateegia ja turvaplaanide koostamine

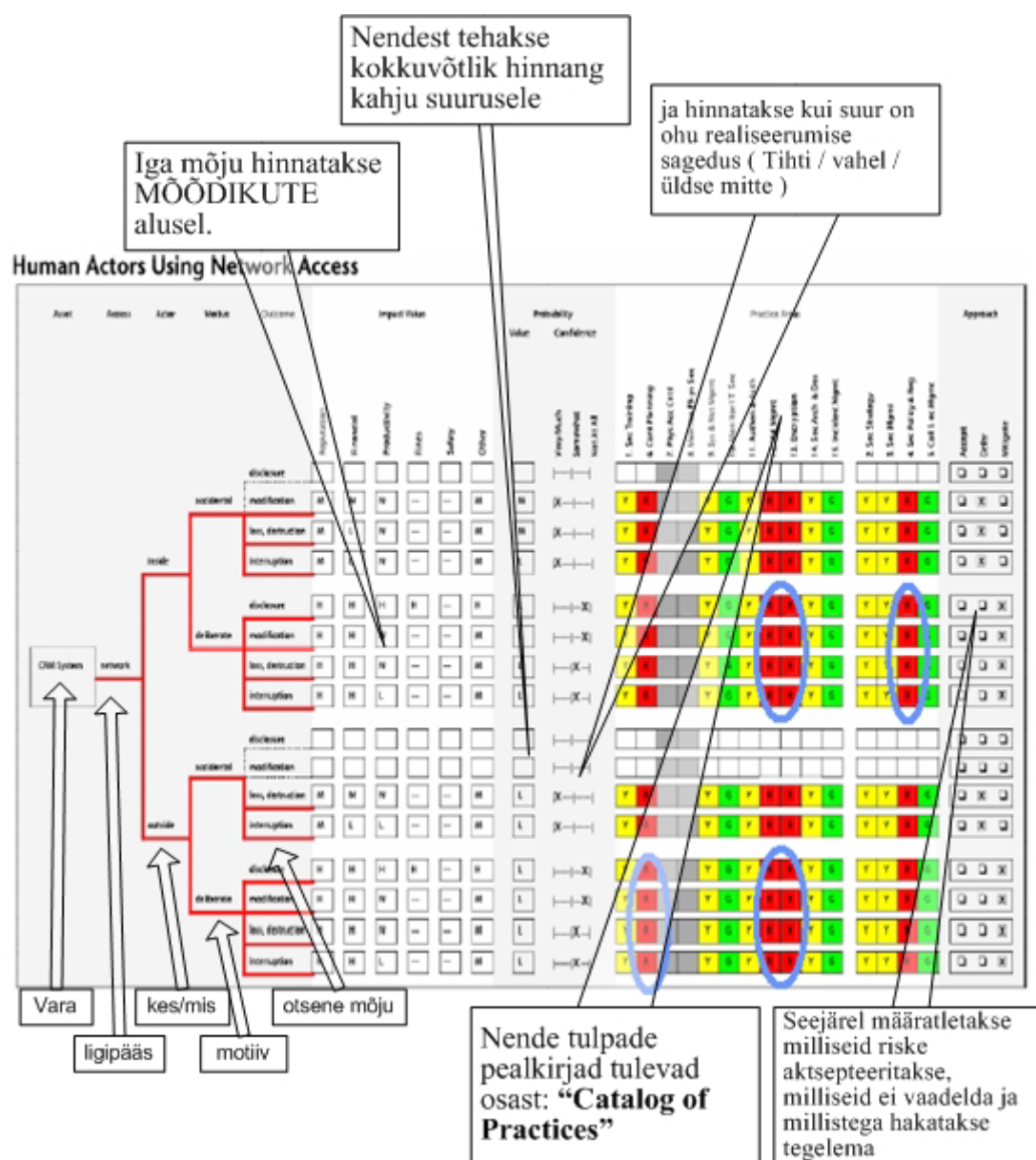
Riskide mõju ettevõtte varadele hinnatakse kvalitatiivselt. Selleks on vaja mõõdikute süsteemi. Mõõdikuteks võivad olla näiteks:

- rahaline kaotus
- tööviljakuse kadu
- konfidentsiaalsus
- maine kadu
- jne.

Mõõdikute väärtusteks võib kokkuleppeliselt olla lihtsalt Suur, Keskmine ja Väike.

Vastavalt esimeses faasis tekkinud puule hinnatakse mõõdikute abil varadele mõjuvate kahjude realiseerumise suurused, tõenäosused ja leitakse “CATALOG OF PRACTISES” alusel, millised tingimused peaksid olema ettevõttes täidetud, et olla turvaline ettevõtte.

3.3.4.4 Riskianalüüsi maatriks: (konkreetse näite puhul)



Joonis 9 Riskianalüüsi maatriks (Dorofee , 2002)

“Catalog of Practices” kirjeldab, millised tingimused peaksid olema ettevõttes täidetud, et olla turvaline ettevõtte.



Joonis 10 Catalog of Practice (Dorofee , 2002)

Kataloog sisaldab ka küsimustikku, mis mõeldud eelkõige järgmistele töötajatele:

- tippjuhid
- osakonnajuhatajad
- spetsialistid
- IT töötajad

Küsimuste vastustest peaks selguma, kuivõrd ettevõtte vastab ettenähtud turvareeglitele.

OCTAVE riski hindamine toimub täielikus vastavuses ISO/IEC 13335 soovitustele.

Kirjeldatakse ettevõtte varad, nõrkused ja turvanõuded. Tööprotsessi kaasatakse kogu firma - juhtkonnast alluvateni. Koostatakse turvastrateegia ja turvaplaanid.

Kui ISO 13335-3 kirjeldab varade väärtustamisel tervelt 11 negatiivset toimet, mida võib hinnata ,

- seaduste ja/või eeskirjade rikkumine,
- tegevusnäitajate halvenemine,
- maineväärtuse kadu või negatiivne mõju mainele,
- isikuteabega seotud turvarike,
- inimeste ohutusega riskimine,
- ebasoodsad mõjud seaduste järgimisele,
- ärilise konfidentsiaalsuse rikkumine,
- avaliku korra rikkumine,
- rahaline kahju,
- äritegevuse katkemine,
- keskkonnaohutusega riskimine

ja ISO 13369 näites oli vaatluse all rahaline kahju, tööviljakuse langus ja asutuse maine kahjustus, siis OCTAVE näide vaatleb neist rahalist kadu, tööviljakuse kadu, konfidentsiaalsuse kadu ja maine kadu.

Octave väärtuseks võiks lugeda, et juhitakse tähelepanu registreeritud teadaolevate nõrkuste andmebaasi - *Common Vulnerabilities and Exposures* (CVE) – olemasolule, mis on pealegi kõigile tasuta ja vabalt kasutatav. (CVE, 2003) Octave väärtuseks võiks lugeda ka kataloogi “*Catalog of Practices*” (Alberts A.J, Dorofee A.J, Allen J.H, 2001) olemasolu.

Nende vahenditega on kasulik tutvuda nii tippjuhil, kes saab võib olla esimest korda teada nõrkuste laiast nomenklatuurist ja turvameetmetest, mis on tulenenud laialt ulatuslikust parimast kogemusest. Samuti on need kasulikud turbspetsialistile, et lihtsalt jälgida, kas oma töös on tulnud ikka meelde kõik vajalik, või on mõni aspekt jäänud tähelepanuta.

Ohtude profiili puukujulisena esitamine on väga illustreeriv, kuid sellel on mõte kui lõpptulemusel on rohkem “oksi” kui üks. Muidu kulub enamus tööst tühjade “okste” välja selgitamisele ja kasulik informatsioon on liialt laiali jagatud erinevate puude vahel.

3.3.5 CobiT

ISACA poolt välja antud info- ja sellega seotud tehnoloogia kontrolli sihid (CobiT- Control Objectives for Information and related Technology), annavad auditi korralduse üldise metoodika. (IT Governance Institute, 2000)

CobiT üritab vastata küsimustele:

- Milles on probleem?
- Mis on lahendus?
- Millest lahendus koosneb?
- Kas see hakkab tööle?
- Kuidas see toimib?



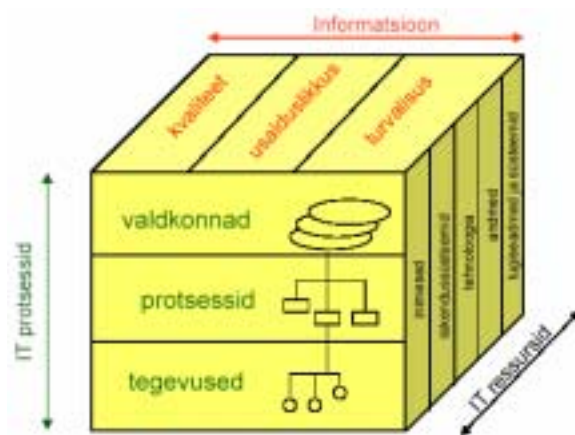
CobiT on mõeldud:

- Juhtkonnale - tasakaalustada riske ja juhtimisinvesteeringuid sageli ennustamatus IT keskkonnas.
- Kasutajale , kes saaksid kinnitust IT turbe rakendamise ja juhtimis-mehhanismide kohta.
- Audiitoritele – et põhjendada oma arvamusi ja anda nõu juhtkonnale sisemiste kontrollimehhanismide üle.

CobiT-i raamstruktuuri aluskontseptsioon on selles, et IT juhtimisele lähenetakse vaadeldes informatsiooni, mida vajatakse ärieesmärkide toetuseks.

Neli põhilist IT valdkonda:

- Planeerimine ja organiseerimine
- Hankimine ja rakendus
- Tarnimine ja tugi
- Seire – kontroll – vastavus juhtimise nõuetele



Joonis 11 CobiT-i raamstruktuur (Leibur G, 2003)

Põhilistes valdkondades on määratletud 34 infotehnoloogia protsessi ja kontrolli üldist sihti.

Iga sihi jaoks on määratud detailsed auditi alad, meetodid, kontrollide hindamine, vastavuse hindamine, riskide hindamine.

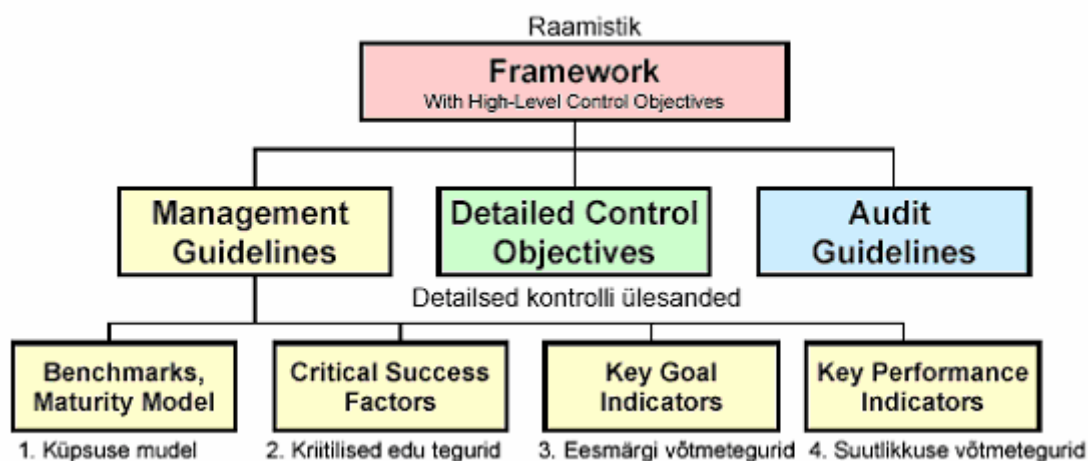
Nendel aladel on määratletud 32 infotehnoloogia protsessi ja kontrolli üldist sihti. Iga sihi jaoks on määratud detailsed auditi alad, meetodid, kontrollide hindamine, vastavuse hindamine, riskide hindamine.

CobiT eristab 3 informatsiooni kohta käivat ärinõuet ja hindab neid 7 kriteeriumi alusel

Ärinõuded: <ul style="list-style-type: none"> • Kvaliteet • Usalduslikkus • Turvalisus 	<ul style="list-style-type: none"> • Toimivus (effectiveness) • Tõhusus (efficiency) • Konfidentsiaalsus (confidentiality) • Terviklus (integrity) • Käideldavus (availability) • Vastavus (compliance) • Informatsiooni usaldatavus (reliability of information)
---	--

IT ressursid jagunevad :

- Andmed
- Rakendussüsteemid
- Tehnoloogia
- Üld-infrastruktuur
- Inimesed



Joonis 12 CobiT' I perekond (Leibur G, 2003)

Alates kolmandast trükist on CobiT vabalt saadaval ka internetist ISACA koduleheküljel.(IT Governance Institute, 2000)

CobiT abil saab:

- hinnata süsteemide ja infotöö vastavust ettevõtte (äri)huvidele

- hinnata ettevõttega seotud kolmandate osapoolte (näiteks avalikkuse) nõuete rahuldatust
- hinnata firma tegevusele eluliselt vajaliku info usaldatavust, kättesaadavust ja kaitstust
- hinnata süsteemide või infotöö korralduse kvaliteeti, turvet ja töökindlust
- kaitsta tellija huve, kui tellitavas projektis on põhiline teadmine täitja poolel
- kontrollida venivaid või muus mõttes ebaedukaid projekte
- pakkuda tuge uute projektide käivitamisel

4 Infoturbe riskid firmas Elektroskandia näitel

5 Kokkuvõte

On analüüsitud kasutuselolevaid riskianalüüsi meetodeid. Enamus neist eeldab teatud statistilise taustainfo olemasolu või vähemalt ajaloolisel kogemusel põhinevaid andmeid ohtude esinemissageduse kohta. Uuemad visioonid ei ole veel piisavalt toetatud metoodikatega. Kuna riiklikul tasemel metoodiline tegevus Eestis puudub, ei ole olemas adekvaatseid lähteandmeid teoreetiliselt põhjendatud üldtunnustatud riskianalüüsi meetodite rakendamiseks. Vaatamata lähteandmete hinnangulisele ja subjektiivsusele on magistritöös riskide analüüsi meetodiks valitud detailne riskianalüüs, kuna see annab kõige põhjalikuma ülevaate turvaolukorrast, kuigi meetod on aeganõudev ja kulukas. Põhjalikult on käsitletud mõõdikute süsteemi määratlemist.

Riskianalüüsi tulemusena võib järeldada, et sobilike etalonmeetmete olemasolul oleks piisanud etalonturbe metoodika kasutamisest. Samas praktiline kogemus üritada kasutada Andmekaitse Inspektsiooni poolt pakutud turvaklasse oma varade hindamisel näitas, et ettevõtte varad kuulusid niivõrd madalasse klassi, et turvameetmed, mis sellise klassi varadele ette nähtud olid, ei rahuldanud ettevõtte tegelikke vajadusi.

Põhjuseks on ilmselt turvaklasside kirjeldamise alused. Suured riigiettevõtted ja väiksed eraettevõtted vajaksid ilmselt erinevaid klassifitseerimise aluseid.

Magistritöö tulemusena on antud ülevaade infoturbe riskianalüüsi metoodilistest allikatest, turvariski halduse ja -analüüsi metoodikatest ning mõnedest analüüsivahenditest. Magistritöö peatükid “Metoodilised allikad” ja “Ülevaade Riskianalüüsi meetoditest” peaksid andma ülevaate riskianalüüsiga põhjalikult tegelema hakkavatele firmade IT spetsialistidele, olemasolevatest kasutatavatest meetoditest ja abivahenditest. Nende alusel peaks IT turvalisuse eest vastutavad töötajad saama ettekujutuse riskihalduse olemusest ja vajalikest sammudest riskihalduse juurutamiseks oma ettevõttes.

Teise osana on magistritöös analüüsitud AS Elektroskandia tegelikke turvariske. On näidatud infotehnoloogiliste süsteemide mõju ettevõtte äriprotsessidele ning neist tulenevaid ohtusid. On selgelt välja toodud infovarade hindamise ning mõõdikute süsteemi kujundamise alused. Lisadena on toodud näiteid erinevate aspektide käsitlest AS Elektroskandia riskianalüüsil ning näitliku materjalina väljavõtteid AS Elektroskandia riskihalduse dokumentidest. Vastavad materjalid peaksid andma

ettekujutuse ühest võimalusest, kuidas läbi viia riskianalüüs ja kuidas dokumenteerida infoturbealduse protsessid .

Magistritöö edasiarendusi võiks ette näha pigem praktilises suunas. Eestis riskianalüüsi alane metoodiline tegevus hetkel puudub, senised soovituslikud materjalid on enamusele Eesti asutustest ja organisatsioonidest ebasobivad, kuna äriprotsessid ja nende juhtimisskeemid ei ole nii liigendatud ega hierarhilised, kui seda eeldatakse.

Perspektiivis oleks vaja koostada väikestele ettevõtetele ja organisatsioonidele sobilik metoodika, mis pigem oleks etalonturve koos vastava etalonmeetmestikuga. Sobivaks lahenduseks oleksid Eesti väikeettevõtetele sobivad turvaklassid ja neile vastav turvameetmete määratlemiseks metoodika, mis annaks infosüsteemi turvaklassile põhineva algversiooni vajalikest turvameetmetest. Hetkel määratletud turvaklasside piirid on väikettevõtte jaoks liiga suured.

6 Kasutatud kirjandus:

- Alberts A.J, Dorofee A.J, Allen J.H. (2001)**, *OCTAVE Catalog of Practices* URL www.cert.org/archive/pdf/01tr020.pdf, (September 1, 2003)
- Alberts C. Dorofee, A. (2001)**, *OCTAVE Threat Profiles*, Software Engineering Inst., Carnegie Mellon Univ, URL <http://www.cert.org/archive/pdf/OCTAVEthreatProfiles.pdf>, (September 1, 2003)
- BSI (2001)**, *IT Baseline Protection Manual* , URL <http://www.bsi.de/gshb/english/menue.htm> (September 1, 2003)
- BSI, (2003)**, *IT Baseline Protection Tool*, URL <http://www.bsi.bund.de/gstool> , (September 1, 2003)
- British Standards Institute - BSI (2003)**, *What is BS 7799?*, URL <http://emea.bsi-global.com/InformationSecurity/Overview/WhatisBS7799.xalter>, (September 1, 2003)
- Buldas Ahto, Oit Monika, Praust Valdo (2003)**, *Turvaklasside kirjeldused (tehniline aruanne)*, Küberneetika AS Infotehnoloogia Osakond URL <http://www.ria.ee/turve/klassid/klassid.htm>, (September 1,2003)
- Castano S., Fugini M., Martella G., Samarati P.,(1995)** *Database Security*, Addison-Wesley, ACM Press ISBN 0-201-59375-0
- Common Criteria (2003)**, *Common Criteria Origin*, URL <http://www.commoncriteria.org/docs/origins.html>, (September 1, 2003)
- CVE (2003)**, *Common Vulnerabilities and Exposures (CVE)* URL <http://www.cve.mitre.org/>, (September 1, 2003)
- C & A Security Risk Analysis Group, (2003)**, *Consultative, Objective and Bi-functional Risk Analysis* URL <http://www.security-risk-analysis.com/index.htm> , (September 1, 2003)
- Dorofee Audrey (2002)**, *Managing Information Security Risks Across the Enterprise*, Software Engineering Inst., Carnegie Mellon Univ., URL <http://www.cert.org/archive/pdf/managing-info-security.pdf>, (September 1, 2003)
- RT I 2000, 92, 597**, Avaliku teabe seadus. URL <https://www.riigiteataja.ee/ert/act.jsp?id=264970> (September 1,2003)
- RT I 1996, 48, 944**, Isikuandmete kaitse seadus. URL <https://www.riigiteataja.ee/ert/act.jsp?id=190382>, (September 1,2003)

RT I 1999, 16, 271), Riigisaladuse seadus.

URL <https://www.riigiteataja.ee/ert/act.jsp?id=264837>, (September 1,2003)

Elektroskandia AS (2003), Kvaliteedikäsiraamat – Ettevõtte üldiseloostus ja struktuur.

Elektroskandia AS (2000),

URL <http://www.elektroskandia.ee/company.php?page=32&branches=.32>,

(September 1, 2003)

EVS-ISO/IEC TR 13335-1:1999, Infotehnoloogia. Infoturbe halduse suunised.

Osa 1: Infoturbe mõisted ja mudelid.

EVS-ISO/IEC TR 13335-2:1999, Infotehnoloogia. Infoturbe halduse suunised.

Osa 2: Infoturbe haldus ja plaanimine.

EVS-ISO/IEC TR 13335-3:1999, Infotehnoloogia. Infoturbe halduse suunised.

Osa 3: Infoturbe halduse meetodid.

EVS-ISO/IEC TR 13335-4:2000, Infotehnoloogia. Infoturbe halduse suunised.

Osa 4: Turvameetmete valimine

EVS - ISO/IEC 13335-5:2003, Infotehnoloogia. Infoturbe halduse suunised.

Osa 5: Võrguturbe halduse suunised

EVS - ISO/IEC 17799:2003, Infotehnoloogia. Infoturbe halduse menetluskoodeks

HansonVello, Buldas Ahto, Martens Tarvi, Lipmaa Helger, Ansper Arne, Tulit Viljar (1997), Infosüsteemide turve 1: turvarisk, Küberneetika AS

HansonVello, Buldas Ahto, Martens Tarvi, Lipmaa Helger, Ansper Arne, Tulit Viljar (1998), Infosüsteemide turve 2: turbetehnoloogia, Küberneetika AS,

ISO TR 13569 kavand, 2000, Pangandus ja sellega seotud rahandusteenused.

Infoturbe suunised

URL <http://www.ria.ee/dirs/standardisation/docs/13569kavand.doc>, (September 1, 2003)

IT Governance Institute (2000), CobiT, URL <http://isaca.org/CobiThorizon.htm>, (September 1, 2003)

Kultuuriministeerium (2003),Riskide hindamise metoodiline juhend,

URL <http://www.kul.ee/print.php?path=729>, (September 1, 2003)

Leibur G. (2003), Auditeerimine. CobiT,

URL http://www.itcollege.ee/~gleibur/loengud/Loeng_16.pdf, (September 1, 2003)

Praust V. (1997), Väike infoturbe seletav sõnastik, Eesti Informaatikakeskus,

URL <http://www.ria.ee/turve/brosyyr/o5.htm>, (September 1, 2003)

Praust V. (2001), Infovarade nõrkused ja rakendatavad turvameetmed,
URL www.itcollege.ee/~valdo/turve/turve03.ppt , (September 1, 2003)

Riigi Infosüsteemide Arenduskeskus (2003), Andmeturbe klasside rakendamise
praktilisi näpunäiteid URL <http://www.ria.ee/turve/klassid/juhend.htm>, (September 1, 2003)

Riigi Infosüsteemide Arenduskeskus (2003), Turvanõuete
klassifitseerimisvajadusest URL <http://www.ria.ee/turve/juhend/juh.htm#8>,
(September 1,2003)

Pulman (2003),Elektrooniline isikutuvastus,
URL http://www.nlib.ee/rkogud/pulman/3_osa/mugand_ter.html#personaltailor,
(September 1, 2003)

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>, (September 1, 2003)

Tavast A. (2001), Eesti standard EVS-ISO/IEC 2382. Infotehnoloogia. Sõnastik,
URL <http://www.imprimaatur.ee/standard/08.htm>, (September 1, 2003)

The ITsecurity.com (2003), Dictionary of Information Security,
URL <http://www.itsecurity.com/dictionary/dictionary.htm>, (September 1, 2003)

The National Security Agency (2003), The Rainbow Series,
URL <http://www.fas.org/irp/nsa/rainbow.htm>, (September 1, 2003)

TCSEC - Trusted Computer System Evaluation Criteria – (5200.28-STD, Orange
Book)” URL <http://www.radium.ncsc.mil/tpep/library/rainbow/> (September 1, 2003)

Software Engineering Institute CERT® Coordination Center (2003), OCTAVE,
URL <http://www.cert.org/octave/>, (September 1, 2003), (September 1, 2003)

Ziya Aktas A. (1987), Structured Analysis and Design of Information Systems,
Prentice-Hall, Englewood Cliffs, New Jersey.

7 Summary

Nowadays the correctness and timely delivery of necessary information are increasingly important for a company. The growing dependance of business processes on information technology systems raises new risks, that cannot always be seen or protected from. Computer networks that have been developed for providing better accessibility to information, have generated the situation, where risks threaten information systems from outside as well as from inside.

The overview of fundamental concepts connected to information security, the methodical sources of risk assessment, the methods of the administration and analysis of security risk, and some means of analyses are given in this postgraduate dissertation.

The second part of the dissertation analyzes the actual security risks of AS Elektroskandia. The influence of infotechnological systems on business processes, and forthcoming dangers arising are introduced. There is thoroughly shown the basis of the assessment of information property, and the formation of the dial system. Some examples of the use of different aspects of risk assessment in AS Elektroskandia, and as visual material some extracts from the documents of risk assessment in AS Elektroskandia, are attached. These materials should give the overview of a possibility how to carry out risk assessment, and to document the process of information security management.

8 LISAD

8.1 Lisa 1 Elektroskandia AS varadele mõjuda võivad ohud.

8.2 Lisa 2 Elektroskandia AS varadele mõjuda võivad nõrkused.

8.3 Lisa 3 Elektroskandia AS IT riskihindamise maatriks.