ASUTUSESISESEKS KASUTAMISEKS

Rektori otsus……
Teabevaldaja nimi: Sisekaitseakadeemia
Juurdepääsupiirangu alus: AvTS § 35 lg 1 p 9
Lõpptähtaeg: …….
Märke vormistamise kuupäev: …….

Sisekaitseakadeemia

Sisejulgeoleku Instituut

Steven Kirs

PÄÄSTETEENISTUJATE SUHTUMINE HEIDUTAVATESSE MEETMETESSE INFOTURBE VALDKONNAS HÄIREKESKUSE NÄITEL

Magistritöö

Juhendaja:

Tuuli Pärnsalu, MA

Tallinn 2014

SISEKAITSEAKADEEMIA

Sisejulgeoleku Instituut	Kuu ja aasta: mai 2014
Töö pealkiri eesti keeles: Päästeteenistujate suhtumine heidutavatesse meetmetesse infoturbe valdkonnas Häirekeskuse näitel Töö pealkiri võõrkeeles: Rescue servant´s attitude toward deterrent measures in the field of information security using the example of Estonian Emergency Response Centre	
Töö autor: Steven Kirs	Ei ole nõus oma magistritöö kättesaadavaks tegemisega elektroonilises keskkonnas. Allkiri:
Lühikokkuvõte: Magistritöös on 89 lehekülge, 26 joonist, 4 tabelit ja 76 kasutatud kirjanduse allikat. Magistritöö eesmärgiks oli selgitada välja päästeteenistujate hinnangud heidutavatele meetmetele, mis võiksid kujundada nende infoturbe alast käitumist ja saadud tulemuste põhjal töötada välja soovitusettepanekud Häirekeskusele töötajate infoturbe alase käitumise parendamiseks. Magistritöö uurimisstrateegiaks oli kaardistav uuring (ingl k *survey*), mille andmete kogumine toimus kvantitatiivset andmekogumisemeetodit kasutades. Valimi moodustasid Häirekeskuse päästeteenistujad. Magistritöö empiirilise uuringu tulemused näitasid, et heidutavate meetmete rakendamine on üks võimalus kujundada töötajate suhtumist infoturbe alasesse käitumisse soovitud suunas, kuna töötajate õiguskuulekus turvameetmete järgimisse suurenes heidutavate meetmete rakendamise tulemusena. Teooria ja empiirilise uuringu tulemuste analüüsi ja sünteesi tulemusena esitas autor soovitusettepanekud Häirekeskusele. Käesolev töö pakub uut lisateadmist sisejulgeoleku organisatsioonide infoturbespetsialistidele töötajate infoturbe alasest käitumisest ja heidutavate meetmete rakendamise võimalustest selle kujundamisel.	
Võtmesõnad: infoturve, infoturbe alane käitumine, heidutuse teooria, heidutuse kasutamine infoturbes	
Võõrkeelsed võtmesõnad: information security, information security behavior, deterrence theory, using deterrence in information security	
Säilitamise koht:	
Kaitsmisele lubatud Sisejulgeoleku Instituudi juhataja: Harry Lahtein	Allkiri:
Vastab lõputöö nõuetele Juhendaja: Tuuli Pärnsalu	Allkiri:

SISUKORD:

MÕISTETE JA LÜHENDITE LOETELU

Asutusesiseseks kasutamiseks mõeldud teave – teave, millele asutuse juht on kehtestanud juurdepääsupiirangu asutusesiseseks kasutamiseks[1];

Infoturbe halduse süsteem – tegevusriski kaalutlemisel põhinev organisatsiooni üldise haldussüsteemi osa, mis tegeleb infoturbe rajamise, evitamise, rakendamise, seire, hoolduse ja täiustamisega, suunates ja juhtides infoturvet poliitikate, protseduuride jm vahendite kaudu[2];

Infoturve – riskihalduslik tegevus teabe turvalisuse säilitamiseks vastavalt organisatsiooni tegevuse eesmärkidele, sealhulgas andmekaitse realiseerimise vahend[3];

Kasutaja – infosüsteemi kasutama volitatud isik[4];

Teave – mõtestatud informatsioon, andmed[5];

Turvaintsident – soovimatu või ootamatu turvasündmus(tik), mis võib väga tõenäoliselt kahjustada organisatsiooni tegevust ja ähvardada teabe turvalisust[6].

[1]Avaliku teabe seadus § 41 lg 1, 15.11.2000, jõustunud 01.01.2001 – RT I 2000, 92, 597 ... RT I, 19.12.2012, 5.
[2]Andmekaitse ja infoturbe seletussõnastik AKIT, Cybernetica AS, 2011-2012 <http://akit.cyber.ee/> (04.02.2014).
[3]*Ibid.*
[4]*Ibid.*
[5]*Ibid.*
[6]*Ibid.*

SISSEJUHATUS

Avaliku sektori organisatsioonide valduses on hulgaliselt informatsiooni riigi kodanike, seal elavate välismaalaste, tegutsevate ettevõtete ning isegi diplomaatiliste esinduste kohta. Kõiki neid andmeid töödeldakse ja säilitatakse infotehnoloogilisi vahendeid kasutades mahukates andmebaasides. Kuna väga suurele osale teabest on seatud juurdepääsupiirangud (riigisaladus, asutusesiseseks kasutamiseks mõeldud teave, sensitiivsed isikuandmed vms), siis on avaliku sektori asutuste kohustus kaitsta sellise teabe kontrollimatut levikut ja andmebaaside autoriseerimata kasutamist. Infosüsteemide turvalisuse tagamine on avaliku sektori organisatsioonide üheks suurimaks väljakutseks, sest andmete konfidentsiaalsuse kadu võib põhjustada probleeme isikutele ja ettevõtetele, kahjustada avaliku sektori asutuste ja Eesti riigi mainet (sh rahvusvahelisel tasandil). Selle vältimiseks töötavad asutused välja ning rakendavad infoturbepoliitikat.

Kuigi väljastpoolt tulenevate infosüsteemi rünnete tõrjumine andmete kaitsmise eesmärgil on ülioluline, on teaduslikud uuringud tõestanud, et infoturbeahela nõrgimaks lüliks on organisatsiooni enda töötajad, kes on paljude turvaintsidentide põhjustajaks[7]. Infoturbepoliitikas tuleb seega ette näha turvameetmed töötajate käitumise mõjutamiseks. Nimetatud turvameetmete hulka kuulub näiteks infoturbe alase teadlikkuse tõstmine, turvasüsteemide täiustamine, sanktsioonide rakendamine jne. Teadlased on vaadelnud töötajate infoturbe alast käitumist, võttes aluseks kriminoloogiast teadaolevaid teooriaid ja leidnud, et kõige paremini selgitavad seda ratsionaalse valiku ja heidutuse teooriad[8]. Heidutuse teooria väidab, et turvanõuete järgimist on võimalik tõhustada erinevate heidutavate meetmete (nt karistused, ümberkaudsete hukkamõist) rakendamise kaudu.[9] Käesolev magistritöö uurib heidutuse mõju sisejulgeolekuasutuse töötajate infoturbe alasele käitumisele.

[7]Straub, D. W. and Nance, W. D., Discovering and Disciplining Computer Abuse in Organizations: A Field Study, *MIS Quarterly*, 3, 1990, 45-62.
[8]D'Arcy, J. and Hovav, A. Deterring internal information systems misuse: An end user perspective, *Communications of the ACM*, 50, 10, 2007, 113-117.; Bulgurcu, B., Cavusoglu, H., & Benbasat, I. Information Security Policy Compliance: An Empirical Study of Rationality-Based Beliefs and Information Security Awareness, *MIS Quarterly*, 34, 3, 2010, 523-548.
[9]D'Arcy, J. and Hovav, A. Deterring internal information systems misuse: An end user perspective, *Communications of the ACM*, 50, 10, 2007, 113-117.

Magistritöö on aktuaalne, sest avaliku sektori töö tõhususe ja maine säilitamise huvides on ära kasutada kõik võimalikud viisid infoturbepoliitika järgimise tagamiseks infosüsteemide kasutajate seas. Selleks, et maksimeerida ja samas optimeerida heidutavate meetmete kasutamist töötajate mõjutamiseks, on oluline teada saada, millistel konkreetsetel meetmetel oleks suurim efekt õiguskuuleka käitumise esilekutsumisel. Magistritöö autor on seisukohal, et töötajate uurimine läbi heidutuse teooria rikastab sisejulgeoleku infoturbespetsialistide senist teadmist töötajate infoturbe alasest käitumisest.

Jürgen Esinurm uuris oma magistritöös töötajate teadlikkuse hetkeolukorda Eesti sisejulgeoleku organisatsioonides ning jõudis järeldusele, et käesoleval hetkel on Eesti sisejulgeoleku organisatsioonides töötajate infoturbe alane teadlikkus küll ebaühtlane, kuid ekspertide hinnangul keskmisel tasemel[10]. Vaatamata sellele, et töötajate teadlikkus ohtudest on keskmisel tasemel olemas, esineb siiski sisejulgeoleku organisatsioonides piiratud juurdepääsuga teabe soovimatu avalikuks saamise juhtumeid. Magistritöö probleem seisneb selles, et ei ole uuritud töötajate hoiakuid ja suhtumisi infoturbesse töökeskkonnas ega käsitletud kõiki võimalusi töötajate käitumise kujundamiseks. Käesolev uurimus täidab selle lünga just heidutavate meetmete osas, sest uurib, kuidas suhtuvad sisejulgeoleku töötajad heidutavate meetmete rakendamisse infoturbe alase käitumise kujundamisel.

Magistritöö valimiks on Häirekeskuse päästeteenistujad. Häirekeskus sobib esindama uuritavat sihtgruppi, sest tegu on sisejulgeoleku tagamisega tegeleva asutusega, kus töödeldakse igapäevaselt suurel hulgal tundliku iseloomuga isikuandmeid, teateid õigusrikkumistest ja õnnetustest. Häirekeskuse infosüsteemist andmete ebasoovitav avalikuks tulek võib seada ohtu isikute turvalisuse, raskendada õigusrikkumiste ja õnnetuste lahendamist ning vähendada pikemas perspektiivis Häirekeskuse usaldusväärsust ühiskonnas. Vastavalt Päästeinfosüsteemi pidamise põhimääruse[11] § 3 lg-le 2 käsitletakse Häirekeskuses töödeldavat ja hoitavat teavet asutusesiseseks kasutamiseks mõeldud teabena.

Magistritöö eesmärk on selgitada välja päästeteenistujate hinnangud heidutavatele meetmetele, mis võiksid kujundada nende infoturbe alast käitumist ja saadud tulemuste põhjal töötada välja soovitusettepanekud Häirekeskusele töötajate infoturbe alase käitumise parendamiseks. Eesmärgi saavutamiseks püstitab autor järgnevad uurimisülesanded:

1. anda ülevaade infoturbe, infoturbe alase käitumise ja heidutuse teoreetilisest käsitlusest;

[10]Esinurm, J., "Infoturbe alane teadlikkus sisejulgeolekuorganisatsioonis", magistritöö, Sisekaitseakadeemia, (2013), lk 53.
[11]Päästeinfosüsteemi pidamise põhimäärus, vastu võetud siseministri määrusega 31.01.2012 nr 2, jõustunud 05.02.2012 – RT I, 02.02.2012, 6... RT I, 05.04.2013, 17.

2. uurida empiiriliselt ning analüüsida päästeteenistujate hinnanguid infoturbega seotud käitumisele ja heidutavatele meetmetele käitumise mõjutajana;
3. töötada teoreetilise käsitluse ja empiirilise uuringu tulemuste analüüsil ja sünteesil välja soovitusettepanekud Häirekeskusele töötajate infoturbe alase käitumise parendamiseks.

Magistritöö uurimisstrateegiaks on kaardistav uuring. Andmete kogumine toimub kvantitatiivset andmekogumise meetodit kasutades. Autor võtab vaatluse alla Häirekeskuse, kus viib päästeteenistujate seas läbi anonüümse küsitluse, millele vastamine toimub veebikeskkonnas etteantud küsimustele tuginedes. Saadud uuringu tulemused põhinevad päästeteenistujate individuaalsetel väärtushinnangutel ja käitumisel. Magistritöö uuringu tulemusena esitab autor Häirekeskusele soovitusi töötajate infoturbe alase käitumise parendamiseks. Empiirilise uuringu tulemuste ja soovituste iseloomust tulenevalt (informatsioon Häirekeskuse töötajate infoturbe alase käitumise kohta) on magistritööl vastavalt avaliku teabe seaduse[12] § 35 lg 1 p-le 9 juurdepääsupiirang asutusesiseseks kasutamiseks.

Magistritöö koosneb kahest peatükist. Magistritöö esimene peatükk moodustab töö teoreetilise osa, milles autor käsitleb infoturbe teoreetilisi aluseid, töötajate infoturbe alast käitumist, heidutuse teooriat ja selle rakendamise võimalusi infoturbe alase käitumise mõjutamiseks. Töö teoreetilise osa koostamisel on autor lähtunud erialakirjandusest, rahvusvahelistest ja siseriiklikest standarditest, seadustest ja teadusartiklitest. Töö teine peatükk käsitleb empiirilist uuringut, mis sisaldab ankeetküsitluse analüüsi ja soovitusettepanekuid päästeteenistujate infoturbe alase käitumise parendamiseks.

Töö tulemus annab aluse uurida heidutuse mõju töötajate infoturbe alasele käitumisele ka teistes sisejulgeoleku organisatsioonides, kus töökeskkond on Häirekeskusega võrreldes teistsugune. Autor tänab oma juhendajat Tuuli Pärnsalut ja kõiki teisi, kes aitasid kaasa töö valmimisele.

[12]Avaliku teabe seadus, 15.11.2000, jõustunud 01.01.2001 – RT I 2000, 92, 597 ... RT I, 19.12.2012, 5.

1. UURINGU TEOREETLINE TAUST

1.1 Infoturbe teoreetilised alused

Käesolev magistritöö keskendub töötajate infoturbe alase käitumise uurimisele. Kuna infoturbe valdkond on väga lai, kätkedes erinevaid turvalisuse tegureid, peab autor esmalt vajalikuks selgitada infoturbe olemust, tutvustada infoturberiske ning turbe korraldamise protsesse infot töötlevas asutuses. Peatükk jaguneb sisult kaheks. Peatüki esimeses pooles käsitleb autor infoturbe kujunemist ja selle definitsioone. Peatüki teises pooles tutvustab infoturbe riske ja turbe korraldamise protsesse.

Infoturbe kujunemise võib jagada kolme etappi. Esimene etapp algas 1960-datel aastatel, kui infoturbe peamiseks eesmärgiks oli tagada hoonete füüsiline kontroll ja turvalisus. Teise etapi alguseks peetakse 1970-date keskpaika, kui infoturvet hakati rakendama konkreetsemalt organisatsiooni spetsiifilistele vajadustele tuginedes. Kolmanda etapi alguseks peetakse nn infotehnoloogiaajastu algust 1980-datel aastatel, kui kasutusse tuli uus tehnoloogia ning organisatsioonidel tekkis vajadus ühendada oma info- ja kommunikatsiooni teenused üheks tervikuks, liikudes kinnisest keskkonnast rohkem kompleksemasse, mis ühendas omavahel erinevaid süsteeme ja võrke.[13]

Traditsiooniliselt on teabe turvalisuseks ehk infoturbeks nimetatud infovarade kolme esmavajaliku omaduse tagamist teatavas (konkreetsetest tingimustest sõltuvas) ulatuses. Need omadused on käideldavus (ingl k *availability*), terviklus (ingl k *integrity*) ja konfidentsiaalsus (ingl k *confidentiality*). Teabe käideldavus on infovarade takistusteta kättesaadavus volitatud kasutajaile ja nende teovõime. Samuti tähendab käideldavus seda, et turvasüsteemid ise ei tohi tekitada volitatud kasutajatele takistusi infovarade kasutamisel ning nende süsteemide tekitatud ajutised kitsendused peavad olema võimalikult väikesed. Teabe terviklus on teabe pärinemine autentsetest allikatest ning kindlus, et teave pole hiljem muutunud või seda pole hiljem volitamatult muudetud. Teabe konfidentsiaalsus tähendab, et arvutisüsteemi infovarad on kättesaadavad ainult volitatud asjaosalistele.[14]

[13]Von Solms, R., Information Security Management: The Second Generation, *Computer & Security*, 15, 1996, 281-288.
[14]Hanson, V., Laur, M., Oit, M., Alliksoo, *Infosüsteemide turve 1. Turvarisk* (Cybernetica AS, 2009), lk 16.

Seega teabe turvalisuse oluliste komponentidena tuleb käsitleda selle käideldavust, terviklust ja konfidentsiaalsust, mis tähendab, et töödeldavad andmed peavad olema ajakohased, kättesaadavad täielikult vajalikus mahus ning töödeldavad ainult volitatud asjaosalistele kindlaks määratud juurdepääsuõiguste alusel. Kuigi käideldavust, terviklust ja konfidentsiaalsust käsitletakse enamasti koos, tuleb käideldavust vaadelda teabe turvalisuse komponentidest tähtsaimana. Kui volitatud kasutaja ei saa teavet või infosüsteemide teenuseid kasutada, muutub infovarade väärtus sisuliselt võrdseks nulliga ja selle tulemusena kaotavad muud turbemeetmed (terviklus ja konfidentsiaalsus) oma mõtte.

Infoturbel (ingl k *information security*) on väga palju erinevaid definitsioone. Andmekaitse ja infoturbe seletussõnastiku kohaselt on infoturve kõige klassikalisemas mõttes riskihalduslik tegevus teabe turvalisuse säilitamiseks vastavalt organisatsiooni tegevuse eesmärkidele[15]. Vabariigi Valitsuse määrus „Infoturbe juhtimise süsteem" § 2 lg 1 defineerib infoturbe asutuse turvameetmete loomise, valimise ja rakendamise protsesside kogumina[16]. Eesti standard EVS-ISO/IEC 27001: 2006 (edaspidi ISO 27001: 2006) määratleb infoturvet teabe käideldavuse, tervikluse ja konfidentsiaalsuse säilitamisena[17]. Eeltoodud definitsoone üldistades on infoturve riskide hindamisel põhinev protsess, mille eesmärk on luua ja hallata turvameetmeid, et tagada organisatsioonile kuuluva teabe käideldavus, terviklus ja konfidentsiaalsus.

Anderson väidab, et infoturbe definitsioon peab olema kindel, terviklik ja täpne[18]. Tema sõnul on ülaltoodud terminid (käideldavus, terviklus ja konfidentsiaalsus) liiga laiatähenduslikud, et hõlmata kindlat, terviklikku ja täpset määratlus infoturbest, mistõttu on see sageli tekitanud segadust infoturbespetsialistidele. Anderson on erinevate infoturbe käsitluste analüüsi tulemusena töötanud välja järgneva definitsiooni: infoturve hõlmab endas head informeeritud kindlustunnet, et infovarasid ohustavad riskid ja kontroll on viidud tasakaalu. Magistritöö autori arvates on Andersoni määratlus infoturbest üks paremaid, sest on konkreetne ja täpne, sisaldades seejuures kõiki infoturbe aspekte. Definitsiooni igat komponenti on ta iseloomustanud järgnevalt. Hea informeeritus – tähendab, et infoturvet tuleb vaadelda läbi teadmiste ja kogemuste vaatenurga, arvestades seejuures konkreetse

[15]Andmekaitse ja infoturbe seletussõnastik AKIT, Cybernetica AS, 2011-2012 <http://akit.cyber.ee/> (04.02.2014).
[16]Infoturbe juhtimise süsteem, vastu võetud Vabariigi Valitsuse määrusega 15.03.2012 nr 26, jõustunud 01.01.2013 – RT I, 19.03.2012, 4.
[17]Eesti Standard EVS-ISO/IEC 27001: 2006, Infotehnoloogia. Turbemeetodid. Infoturbe halduse süsteemid. Nõuded <http://www.evs.ee/tooted/evs-iso-iec-27001-2006> lk10 (02.02.2014)
[18]Anderson, J. M.. Why we need a new definition of information security, *Computers & Security*, 22, 4, 2003, 308-313.

organisatsiooni vajadusi. Erineva iseloomuga organisatsioonid vajavad erinevaid infoturbemeetmeid. Oluline on see, et neid teadmisi ja kogemusi viiakse töötajateni, et suurendada nende arusaamist ja vastutusvõimet. Kindlustunne – põhineb veendumusel, et organisatsioonide infovarade kaitsevõimekus on piisavalt hea ning olemas on teave võimalike ohtude kohta. Infovarasid ohustavad riskid – iga organisatsioon peab hindama ja liigitama enda jaoks võimalikke riske järjepidevalt, kuna keskkond meie ümber on pidevalt muutumas ja kätkeb endas uute potentsiaalsete ohtude teket. Ohte tuleb seega käsitleda erinevalt ja vastavalt olukorrale. Kontroll – tähendab, et organisatsiooni teavet tuleb kaitsta ja kontrollida. Muuhulgas tuleb vähendada süsteemi ja protsesside nõrku kohti, mis põhineb riskianalüüside läbiviimisel. Tasakaal – tähendab oskust leida kõige paremini sobiv infoturbe lahendus, võttes arvesse nii huvipoolte nõudeid ja ootusi kui ka organisatsiooni tegelikke vajadusi.[19]

Tänapäeval kasutavad organisatsioonid teabe töötlemiseks, hoiustamiseks ja edastamiseks infotehnoloogia vahendeid, kuna see kiirendab tööprotsesside toimimist ja võimaldab maksimeerida efektiivsust. Teabe töötlemine ja edastamine elektrooniliselt organisatsiooni võrgu või interneti kaudu võib kätkeda aga riski selle volitamatule kasutamisele[20]. Mida suurem on teabe kättesaadavus, seda suuremad on ka potentsiaalsed infoturbe ohud, mille tõrjumiseks tuleb rakendada tugevamaid ja paremaid turvalisuse meetmeid. Sagedased turvaintsidendid viitavad sellele, et organisatsioonid ei juhi infoturbe protsesse piisavalt hästi või ei pööra infoturbe vajalikkusele piisavas ulatuses tähelepanu. Kui organisatsioonid ei juhi infoturbe protsesse piisvalt hästi, võib see põhjustada infovarade käideldavuse, tervikluse ja konfidentsiaalsuse kahjustumist, mis võib omakorda tekitada organisatsioonidele majandusliku kahju või vähendada nende usaldusväärsust.[21]

Infoturbe tähtsus tuleneb andmete tähendusest ja väärtusest[22]. Näiteks sisejulgeoleku organisatsioonidel on ligipääs isikuandmetele, riigisaladustele ja ka muule riigi julgeolekut puudutavale teabele kõige laialdasem. Selliste andmete konfidentsiaalsuse kadu võib põhjustada ohtu isikutele ja vähendada sealhulgas organisatsiooni usaldusväärsust ühiskonnas, millest pikemas perspektiivis võib kujuneda julgeolekuoht riigile. Seega võib

[19]Anderson, J. M.. Why we need a new definition of information security, *Computers & Security*, 22, 4, 2003, 308-313.
[20]P.J., Why is Information Security important? (07.01.2009) <http://mindfulsecurity.com/2009/07/ 01/why-is-information-security-important/> 03.03.2014
[21]Blakley, B., McDermott, E., and Geer, D., Information security is information risk management, *ACM Workshop on New Security Paradigms NSPW*, 2001, 97-104, p97.
[22]Tallinna linna asutuste infoturbe põhimõtted § 3 lg 3, vastu võetud Tallinna Linnavalitsuse määrusega 15.12.2010 nr 104, jõustunud 20.12.2010 – RT IV, 24.05.2013, 38.

sisejulgeoleku organisatsioonide puhul pidada infoturbe rakendamise vajalikkust vägagi tähtsaks.

Infoturvet on sageli peetud tehniliseks probleemiks koos tehnilise lahendusega[23]. Tegelikkuses kätkeb infoturve riskide haldamist. Riskide haldamine põhineb aga riskide määratlemisel ja mõõtmisel ning vastavate meetme rakendamisel selliste riskide ärahoidmiseks.[24] Kuna teavet hoitakse enamasti infosüsteemides, mis on seotud erinevate võrkudega, siis on potentsiaalseid ohuallikaid seetõttu rohkem. Tehnoloogia pakub väga palju erinevaid võimalusi teabe kogumiseks, jagamiseks, müümiseks, vahetamiseks ja levitamiseks ilma selle omaniku teadmata[25]. Turvalisuse lahendused võivad olla väga head, kuid ometi näitavad kogemused, et ka neist on võimalik mööda pääseda eelnevalt nimetatud põhjustel. Infoturbe reeglid ja juhendid võivad töötada väga hästi, kuid alati peab seejuures arvestama võimalike riskidega, kuna tehnoloogiat võidakse kasutada nii headel kui halbadel eesmärkidel. Näiteks tundlikku teavet on väga lihtne talletada mälupulgale, mille kadumist ei märka tavaliselt hiljem keegi.[26]

Infoturberiskide tundmine ja haldamine on teabe turvalisuse tagamise üheks oluliseks eelduseks. Hea riskihalduslik tegevus tagab selle, et suudetakse õigeaegselt reageerida potentsiaalsetele infoturbe ohtudele ning ennetada nende poolt tekitatavat kahju. Infotehnoloogia vahendite kasutajateks on enamasti inimesed, kelle käitumist mõjutab suhtumine[27]. Suhtumine on infoturbe tagamisel ülioluline, kuna inimesed on infosüsteemide vahetud kasutajad. Kui inimesed ei pea infoturbe protseduure vajalikuks või neil puudub infoturbe alane teadlikkus, mõjutab see infoturbe efektiivsust. Sageli on infoturbe toimimist käsitletud seetõttu ka inimeste probleemina.[28]

Selleks, et organisatsioonide info- ja kommunikatsioonivahendite kasutamine toimuks turvaliselt, sealhulgas käituksid turvaliselt nende kasutajad, rakendavad organisatsioonid

[23]Ruighaver, A. B., Maynard, S. B., & Chang, S., Organisational Security Culture: Extending the End User Perspective, *Computers & Security, 26*, 2007, 56-62, p56.
[24]Blakley, B., McDermott, E., and Geer, D., Information security is information risk management, *ACM Workshop on New Security Paradigms NSPW*, 2001, 97-104, p98.
[25]Varney, C. A., „Consumer Privacy in the Information Age: A View from the United States, The Privacy & American Business National Conference, Omni Shoreham Hotel, Washington, D.C." (1996) <http://www.ftc.gov/public-statements/1996/10/consumer-privacy-information-age-view-united-states> (12.11.2013).
[26]Lampson, B. W, Computer Security in the Real World, *Principles of Computer Systems*, 37, 6, 2002, 37-46.
[27]Leelo, E., "Efektiivne andmekaitse algab suhtumisest" (2005) <http://www.hlp.ee/media/ITee_0905_Leego.pdfZ> (10.12.2013).
[28]Schneier, B., Managed Security Monitoring: Network Security for the 21st Century, *Computers & Security*, 20, 2001, 491-503, p491.

infoturbepoliitikat[29]. Infoturbepoliitikat on peetud organisatsiooni infoturbe korraldamise nurgakiviks[30]. Andmekaitse ja infoturbe seletussõnastiku kohaselt on infoturbepoliitika organisatsiooni turvapoliitika osa, mis määratleb üldeesmärgid teabe turvalisuse ja infoturbe alal ning infoturbe halduse süsteemi struktuuri, olles infoturbe esmane alusdokument[31].

Infoturbe kirjanduses on infoturbepoliitikal mitmeid definitsioone. Infoturbepoliitikat on defineeritud kui plaani, mille eesmärk on anda töötajatele käitumisnormid, et tagada seeläbi organisatsiooni infovarade turvalisus[32]. Infoturbepoliitikat on käsitletud ka kooslusena, mis sisaldab endas erinevaid turvalisuse põhimõtteid, korraldusi, meetodeid, tehnilisi lahendusi ja võtteid[33]. Samas on infoturbepoliitikat määratletud tegevusena, mille laiem eesmärk on aidata selgitada välja kaitsmist vajavad infovarad ning kujundada organisatsiooni liikmete suhtumist nimetatud varade kaitsmisesse[34]. Üldistades eeltoodud määratlusi, on infoturbepoliitika organisatsiooni infoturbe esmane alusdokument, mis sisaldab organisatsiooni infovarade turvalisuse tagamise strateegiat. Sõna strateegia viitab siinkohal infoturbe põhiidee ja eesmärkide saavutamiseks tehtavatele jõupingutustele.

Infoturbepoliitika koostamisel lähtutakse üleüldisest organisatsiooni turvapoliitikast, mis omakorda tuleneb arengustrateegiast ja muudest poliitikatest. Infoturbe dokumentatsiooni kujundamisel lähtutakse tavaliselt valikust, kas töötada välja pikem kõikehõlmav või lühem infoturbepoliitika dokument. Lühema infoturbepoliitika dokumendi kasutamine eeldab eraldi spetsiifiliste lisadokumentide väljatöötamist (näiteks erinevad turvalisust puudutavad reeglid ja korraldused). Mõlemal variandil on omad eelised ja puudused. Mahukama poliitikadokumendi puhul on kogu turvalisust puutuv materjal koos, kuid arvestama peab, et selle haldamine ja lugemine võib osutuda töötajatele tülikaks. Samuti võib tekkida risk, et töötajad ei saa sellest piisavalt hästi aru või ei leia sealt üles neile vajalikke osi. Lühem alusdokument on üksnes kompaktne raamdokument, sisaldades viiteid erinevatele muudele

[29]Whitman, M. E., In Defense of the Realm: Understanding the Threats to Information Security, *International Journal of Information Management*, 24, 2004, 43-57, p52.
[30]Fung, P., Kwok, L.-F., Longley, D., Electronic Information Security Documentation (2003) < http://crpit.com/confpapers/CRPITV21AFung.pdf> p1 (04.03.2014).
[31]Andmekaitse ja infoturbe seletussõnastik AKIT, Cybernetica AS, 2011-2012 <http://akit.cyber.ee/> (04.02.2014).
[32]Hone, K., & Eloff, J. H., What Makes an Effective Information Security Policy?, *Network Security*, 20,6, 2002, 14-16, p14.
[33]Tryfonas, T., Kiountouzis, E., & Poulymenakou, A., Embedding Security Practicies in Contemporary Information Systems Development Approaches, *Information Management & Computer Security*, 9, 4, 2001, 183-197, p187.
[34]Canavan, S., Diver, S. „An Information Security Policy Development Guide for Large Companies" (2003) <http://www.sans.org/reading-room/whitepapers/policyissues/information-security-policy-a development-guide-for-large-and-small-companies-1331?show=information-security-policy-a-development-guide-for-large-and-small-companies-1331&cat=policyissues> p2 (09.02.2014).

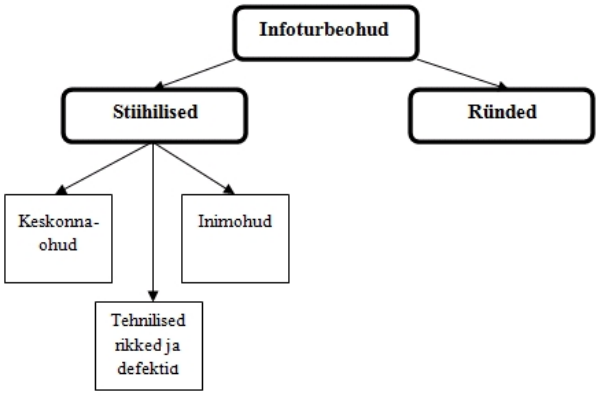
turvalisust puudutavatele lisadokumentidele. Nende leidmine dokumentide süsteemist võib tekitada raskusi, kuid nende lugemist peetakse kergemaks, kuna dokumendid on lühemad ja konkreetsemad.[35]

Infoturbepoliitikat on nimetatud organisatsiooni infoturbe korraldamise vundamendiks, sest see on organisatsiooni infoturbe korraldamise alusdokument. On leitud, et infoturbepoliitika on efektiivne, kui see on põhjendatud, lihtsasti loetav ja praktiline.[36] Kui organisatsioon rakendab vastavalt oma vajadustele infoturbepoliitikat võib pidada seda põhjendatuks. Kui organisatsiooni töötajad saavad aru ja järgivad infoturbepoliitikast tulenevaid turvameetmeid, on see piisavalt lihtsasti loetav ja arusaadav ning kui turvameetmed on tasakaalus infoturberiskidega, on see kokkuvõttes praktiline. Selleks, et infoturve saaks toimida, on vaja inimesi, protsesse ja tehnoloogiat. Kui organisatsiooni töötajatel on olemas vajalikud teadmised ja oskused, turvaline tehnoloogia ning turvameetmed, suudab enamik organisatsioone osutada vastupanu erinevatele infoturbeohtudele ning neid ennetada.[37] Infoturbe teoreetilistest alustest järeldub, et infoturberiskide tundmine ja haldamine on teabe turvalisuse tagamise üheks oluliseks eelduseks. Järgnevalt analüüsitakse lähemalt infoturbe riske ja nende haldamist.

Infoturbe praktika kohaselt on parim strateegia keskenduda riskidele, mille avaldumise tõenäosus on kõige suurem. Kui proovida maandada kõiki võimalikke riske, sealhulgas riske, mis kunagi ei avaldu, kulutatakse ära ressursid, mille tulemusena võib tekkida puudujääk seal, kus neid enim vajatakse.[38] Infovarade turvalisus ei tähenda üksnes nende kaitsust või puutumatust, vaid ka infovara omaduste püsimist ohtude kiuste. Infoturbe eesmärgiks on kaitsta infovarasid võimalike riskide eest, mis võivad tekkida infovarade nõrkuste ärakasutamisel ohuolukorras ja rünnakute käigus. Infoturbe ohud on potentsiaalsed turvakahjude algallikad, mis adekvaatsete kaitsemeetmete puudumisel võivad põhjustada turvarikkeid. Neid ohte võib toimelt liigitada nelja põhitüüpi. Halvang – ilmneb selles, et mingi vara hävib, muutub kättesaamatuks või kasutuskõlbmatuks. Teisisõnu on rikutud selle vara käideldavus. Infopüük – tähendab mingi volitamata subjekti (kasutaja, programm, arvutisüsteem) rünnet konfidentsiaalsusele ehk andmeleket. Modifitseering – on volitamatu

[35]Riigi Infosüsteemid, "Asutuse Infoturbepoliitika" <http://www.riso.ee/sites/default/files/soovitused/tinfoturbpol.htm> (05.03.2014)
[36]Verdon, D., Security Policies and the Software Developer, *IEEE Security&Privacy*, 2006, 42-49, p43.
[37]Oslan, G., "People, processes and technology: A winning combination in the fight against cyber crime",*GSN Government Security News*, 14.08.2011 <http://www.gsnmagazine.com/node/ 24210?c=cyber_security> (08.01.2014).
[38]Andress, J., *The Basics of Information Security. Understanding the Fundamentals of InfoSec in Theory and Practice* (Elsevier, 2011), p10.

muudatuste tegemine. Võltsing – tähendab võltsitud objektide lisamist infosüsteemi, sõnumite reprodutseerimist vääras kontekstis, sõnumi saatmise või saamise salgamist jne.[39]



Joonis 1. Infoturbe ohud[40] (autori kohandatud)

Turvalisuse seisukohalt liigitatakse ohuallikaid olemuselt kahte põhitüüpi, milleks on sihilikud sekkumiskatsed ehk ründeohud ja stiihilised ohud (vt Joonis 1). Ründeohud lähtuvad inimestest, kes on mitmesugustel motiividel ja ajenditel (isiklikud huvid, huligaansus, riiklik või eraluure vms) valmis sihilikult kahju tekitama. Neid ohte eristatakse ründeobjektide ja meetodite järgi. Stiihilised ohud tulenevad vääramatust looduslikust jõust, mis võib olla loomult juhuslik (nt äike, üleujutus jne) või regulaarne (nt kulumine, materjalide väsimine, saastumine jne), aga samuti inimvigadest, mida võivad põhjustada ebapiisavad oskused, hooletus, juhtimisvead, keskkonnategurid jne. Turvaülesande püstituse ja lahendamise tarbeks rühmitatakse stiihilised ohud nende kandja järgi keskkonnaohtudeks, infosüsteemi tehnilisteks riketeks ja inimohtudeks.[41]

Infoturbes kasutatakse riski definitsiooni selleks, et hinnata ohtude realiseerumise võimalust ning valida selle vältimiseks sobiv turvameede. Infoturberiski mõõdetakse sündmuse realiseerumise tõenäosuse ja tagajärgede kombinatsiooniga. Infoturbes hinnatakse ohtude realiseerumise sagedust põhiliselt statistiliste väärtuste alusel. Riskide hindamiseks ja analüüsimiseks kasutatakse enamasti kvantitatiivseid meetodeid. Kvantitatiivse meetodi kasutamine on kasulik, kuna see võimaldab esitada selgeid tulemusi arvudes, mida on hea esitleda organisatsiooni juhtkonnale ja samuti tagab see parema arusaadavuse riskide esinemise tõenäosusest.[42]

[39]Hanson, V., Laur, M., Oit, M., Alliksoo, *Infosüsteemide turve 1. Turvarisk* (Cybernetica AS, 2009), lk22.
[40]*Ibid*, lk22.
[41]*Ibid*, lk22.
[42]Henry, K., "Risk Management and Analysis", *Information Security Management Handbook 5th Edition*, Ed. Tipton, H. & Krause, M. (CRC Press, Boca Raton,2004), p1182.

Infoturbe riskianalüüsi eesmärk on hinnata reaalseid ohte ja kulutusi ning selgitada välja aktsepteeritavad riskid, mille turbekulud on ligikaudu võrdsed tõenäoliste kahjudega.[43] Infoturbe riskianalüüs koosneb järgnevatest etappidest: kaitstava info ja tööprotsesside tuvastamine; kaitstava info ja tööprotsessidega seotud peamiste ohtude tuvastamine; võimalike riskikohtade tuvastamine; konfidentsiaalsuse, tervikluse ja käideldavuse kadumisel tekkivate kahjude tuvastamine ja võimalike tagajärgede hindamine; tööprotsesside võimalike turvaintsidentide mõju analüüs; turvaintsidentide kahjuriski kohta hinnangu andmine.[44]

Riskide haldamise strateegia on põhililselt juhtkonna vastutada, see tähendab, et juhkonna kõrgeim tasand kehtestab suunised, kuidas riskidega ümber käia. Asjakohased suunised juhtkonnale töötavad välja aga organisatsiooni infoturbehalduse eest vastutavad isikud. Võimalikud variandid suunistest on järgnevad: riske püütakse vältida adekvaatsete turbemeetmete võtmisega; riske püütakse vältida tööprotsesside ümberstruktureerimise või nendest loobumisega; riske võidakse delegeerida, nt väljasttellimise või kindlustuslepingute sõlmimisega; riskidega võidakse leppida.[45]

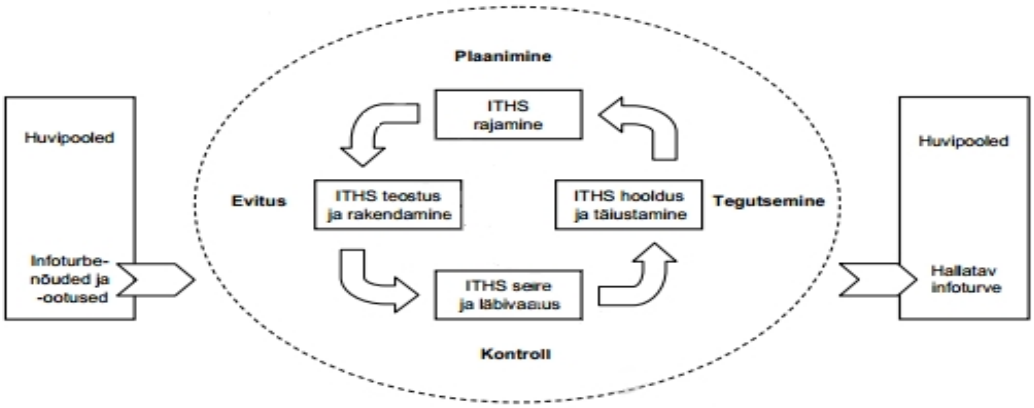
Käesoleva peatüki eesmärgist tulenevalt käsitletakse viimase punktina infoturbe korraldamist. Infoturbe protsesside korraldamine toimub läbi infoturbe halduse süsteemi (edaspidi ITHS). Eestis on organisatsioonide ja ametkondade ITHS kujundamise aluseks Eesti standard ISO 27001: 2006, mille koostamisel on lähtutud rahvusvahelistest ISO standarditest. Eesti standard ISO 27001: 2006 on koostatud eesmärgiga anda mudel ITHS rajamiseks, evituseks, rakendamiseks, seireks, läbivaatuseks, hoolduseks ja täiustamiseks. Vastavalt ISO standardile 27001: 2006 peab ITHS kasutuselevõtt kuuluma organisatsiooni strateegiliste otsuste hulka. Organisatsiooni ITHS kavandamist ja teostamist mõjutavad organisatsiooni vajadused, eesmärgid, turvanõuded, kasutatavad protsessid ning organisatsiooni suurus ja struktuur. Samas peab arvestama sellega, et need tegurid ja neid toetavad süsteemid võivad ajas muutuda ning seetõttu tuleb hinnata ITHS mastaapsust vastavalt organisatsiooni hetke vajadustele.[46]

Rahvusvahelistes standardites on infoturbe haldamist käsitletud läbi kvaliteedi- ja projektijuhtimise meetodi PDCA (ingl k *Plan, Do, Check, Act*), mis rühmitab vajalikud toimingud nelja etappi: alustades planeerimisest kuni tulemuste hindamise ja järgimise korra

[43] *Ibid*. p1188.
[44] BSI., „Standard BSI 100-1 Infoturbehalduse süsteemid (ISMS)" (2008) <https://www.ria.ee/public/ISKE/Standard_BSI_100-1.pdf> lk 8 (04.03.2014).
[45] *Ibid*, lk8.
[46] Eesti Standard EVS-ISO/IEC 27001: 2006, Infotehnoloogia. Turbemeetodid. Infoturbe halduse süsteemid. Nõuded <http://www.evs.ee/tooted/evs-iso-iec-27001-2006> lk 6 (02.02.2014).

jaoks parandusettepanekute tegemiseni[47]. Eesti standardis ISO 27001: 2006 käsitletakse infoturbe haldamist läbi PEKT (plaanimine, evitus, kontroll, tegutsemine) mudeli, mis toetub rahvusvahelisele PDCA meetodile.

Plaanimine (ITHS rajamine) – riskihaldusesse ja ja infoturbe täiustamisse puutuvate ITHS poliitikate, eesmärkide, protsesside ja protseduuride kehtestamine organisatsiooni üldistele poliitikatele ja eesmärkidele vastavate tulemuste saamiseks. Evitus (ITHS teostus ja rakendamine) – ITHS poliitikate, meetmete, protsesside ja protseduuride teostamine ja rakendamine. Kontroll (ITHS seire ja läbivaatus) – protsesside soorituse hindamine ja (kohaldatavail juhtudel) mõõtmine ITHS poliitika, eesmärkide ja praktilise kogemuse põhjal ning tulemuste teatamine juhtkonnale ITHS läbivaatuseks. Tegutsemine (ITHS hooldus ja täiustamine) – ITHS siseauditi ja juhtkondliku läbivaatuse tulemuste põhjal või muu asjassepuutuva teabe põhjal rakendada parandus- ja vältimismeetmeid ITHS pideva täiustuse saavutamiseks.[48]



Joonis 2. Infoturbe halduse süsteemi mudel "PEKT"[49]

Joonisel 2 nähtub, kuidas ITHS saab sisendandmetena huvipoolte infoturbenõuded ja –ootused ning loob vajalike toimingute ja protsessidega infoturbe tulemid, mis rahuldavad neid nõudeid ja ootusi. Eeltoodud mudel annab vaid hea lähtekoha, mida iga ettevõte või ametiasutus kohandab vastavalt enda raamtingimustele, turbenõuetele ja eelarvele[50].

[47]BSI., „Standard BSI 100-1 Infoturbehalduse süsteemid (ISMS)" (2008) <https://www.ria.ee/public/ISKE/Standard_BSI_100-1.pdf> lk 3 (04.03.2014).
[48]Eesti Standard EVS-ISO/IEC 27001: 2006, Infotehnoloogia. Turbemeetodid. Infoturbe halduse süsteemid. Nõuded <http://www.evs.ee/tooted/evs-iso-iec-27001-2006> lk 7 (02.02.2014).
[49]*Ibid,* lk7.
[50]BSI., „Standard BSI 100-1 Infoturbehalduse süsteemid (ISMS)" (2008) <https://www.ria.ee/public/ISKE/Standard_BSI_100-1.pdf> lk 3 (04.03.2014).

Infoturbe tagamine ei ole mitte ajaliselt piiratud, vaid pidev projekt. Infoturbe halduse süsteemi komponente tuleb seega pidevalt kontrollida, et välja selgitada, kas need on jätkuvalt sobivad ja piisavalt tõhusad. Infoturve puudutab eranditult kõiki töötajaid, mis tähendab, et igaüks saab vastutustundliku ja tagajärgedele mõtleva käitumisega anda panuse kahjude vältimisse ja turbeprotsessi edu tagamisse. Seega infoturbeaspektide teadvustamine ning töötajate koolitamine on infoturbe tagamise põhieelduseks. Infoturbe tagamist mõjutavad oluliselt ka töökliima, ühised väärtused ja töötajate käitumine. Töötajatele tuleb selgitada, et neil on kohustus järgida nende tööd puudutavaid seadusi, ettekirjutusi ja reegleid. Selleks tuleb töötajaid eelnevalt asjakohaste infoturvet puudutavate reeglitega kurssi viia ning samal ajal hoolitseda selle eest, et nad oleksid piisavalt motiveeritud neid reegleid järgima. Seda mitte tehes võib töötajate käitumine mõjutada infoturbe efektiivsust.[51]

Kokkuvõtlikult võib alapeatükist välja tuua, et infoturbe definitsioone on väga palju, kuid neist tuntuim, milleks on teabe käideldavuse, tervikluse ja konfidentsiaalsuse säilitamine, on tekitanud arusaamatuse tõttu infoturbespetsialistides segadust, millest lähtuvalt on teadlased pakkunud välja paremaid ja arusaadavamaid infoturbe määratlusi. Teadlaste arvates on infoturve hea informeeritud kindlustunne, et infovarasid ohustavad riskid ja kontroll on viidud tasakaalu. Infoturbe põhieesmärk on säilitada teabe käideldavust, konfidentsiaalsust ja terviklust, mis väljendub teabe ja infosüsteemide kaitsmises loata juurdepääsu, kasutamise, avaldamise, muutmise või hävitamise eest.[52] Infoturbe tähtsus tuleneb andmete tähendusest ja väärtusest[53]. On oluline teada, et infovarade turvalisus ei tähenda üksnes nende kaitstust või puutumatust, vaid ka infovarade omaduste püsimist ohtude kiuste. Eeltoodust tulenevalt moodustab infoturbe protsessidest olulise osa riskide haldamine, mille eesmärk on selgitada välja konkreetsed ohud, mis võiksid põhjustada kahju organisatsiooni infovaradele ning rakendada abinõusid hoidmaks ära nimetatud ohtude avaldumist.[54] Töötajate hoolimatu käitumine võib olla üks nimetatud ohtudest, mis võib organisatsioonile tekitada suuri majanduslikke kahjusid. Infoturbe paremaks korraldamiseks rakendavad organisatsioonid infoturbe halduse süsteemi. Infoturbe halduse süsteemi mudel tuleneb rahvusvahelistest standarditest, mille eemärk on anda lähtekoht infoturbe korralduse välja töötamiseks, mida

[51] *Ibid*, lk 6.
[52]Anderson, J. M.. Why we need a new definition of information security, *Computers & Security*, 22, 4, 2003, 308-313.
[53]Tallinna linna asutuste infoturbe põhimõtted § 3 lg 3, vastu võetud Tallinna Linnavalitsuse määrusega 15.12.2010 nr 104, jõustunud 20.12.2010 – RT IV, 24.05.2013, 38.
[54] Henry, K., "Risk Management and Analysis", *Information Security Management Handbook 5th Edition*, Ed. Tipton, H. & Krause, M. (CRC Press, Boca Raton,2004), p1182.

iga organisatsioon kohandab vastavalt enda vajadustele.[55] Selleks, et organisatsioonide info- ja kommunikatsioonivahendite kasutamine toimuks turvaliselt, sealhulgas käituksid turvaliselt nende kasutajad, rakendavad organisatsioonid infoturbepoliitikat. Infoturbepoliitika on organisatsiooni infoturbe esmane alusdokument, mis sisaldab organisatsiooni infovarade turvalisuse tagamise strateegiat.[56] Infoturbe efektiivus sõltub sellest, kui hästi viivad seda ellu organisatsiooni töötajad, sest üksnes tehnilistest lahendustes ei piisa, et saavutada soovitud turvalisuse tase[57]. Käesolev töö uurib töötajate infoturbe alast käitumist ja heidutavaid meetmeid selle kujundamisel. Magistritöö järgnev peatükk keskendub täpsemalt töötajate infoturbe alase käitumise uurimisele ning annab sissejuhatuse heidutuse teoreetilistele alustele.

1.2 Töötajate infoturbe alane käitumine

Eelmine peatükk oli magistritööle sissejuhatava iseloomuga, tutvustades infoturbe olemust, selle riske ja korraldamist organisatsioonis. Esimeses peatükis selgus, et infoturbe toimimist mõjutavad ka töötajad, kelle ülesandeks on järgida infoturbe reegleid ja korraldusi. Töötajate koostöö valmidusest ja suhtumisest infoturbesse saab alguse infoturbe toimimine. Kuna magistritöö eesmärk on selgitada välja töötajate hinnangud heidutavatele meetmetele infoturbe alase käitumise kujundamisel, peab autor vajalikuks enne heidutuse teoreetiliste alusteni minemist lähemalt selgitada töötajate infoturbe alast käitumist.

Infoturbe alast käitumist ei ole infoturbe valdkonda käsitlevas kirjanduses ühetaoliselt defineeritud. Siiski on mitmetes allikates seostatud infoturbe alast käitumist turvakäitumisega (ingl k *security behavior*)[58]. Andmekaitse ja infoturbe seletussõnastiku kohaselt on turvakäitumine töötajate (mõnes kontekstis ka mingi süsteemi) käitumine turvapoliitika seisukohalt[59]. Infoturbepoliitika moodustab organisatsiooni turvapoliitikast ühe

[55] BSI., „Standard BSI 100-1 Infoturbehalduse süsteemid (ISMS)" (2008) <https://www.ria.ee/public/ISKE/Standard_BSI_100-1.pdf> lk 3 (04.03.2014).
[56] Whitman, M. E., In Defense of the Realm: Understanding the Threats to Information Security, *International Journal of Information Management*, 24, 2004, 43-57, p52.
[57] Henry, K., "Risk Management and Analysis", *Information Security Management Handbook 5th Edition*, Ed. Tipton, H. & Krause, M. (CRC Press, Boca Raton,2004), p751.
[58] Herath, T., Rao, H. R., Encouraging information security behaviors in organizations: Role of penalties, pressures and perceiced effectiveness, *Decision Suppoert Systems*, 47, 2009, 154-165, p154.; Leach, J, Improving User Security Behaviour, *Computer & Security*, 22, 8, 2003, 685-692, p685.
[59] Andmekaitse ja infoturbe seletussõnastik AKIT, Cybernetica AS, 2011-2012 <http://akit.cyber.ee/> (04.02.2014).

osa, olles aluseks infoturbe korraldusele[60]. Sellest tulenevalt on autor seisukohal, et infoturbe alast käitumist võib tuletatult turvakäitumisest, defineerida kui töötajate käitumist infoturbepoliitika seisukohalt.

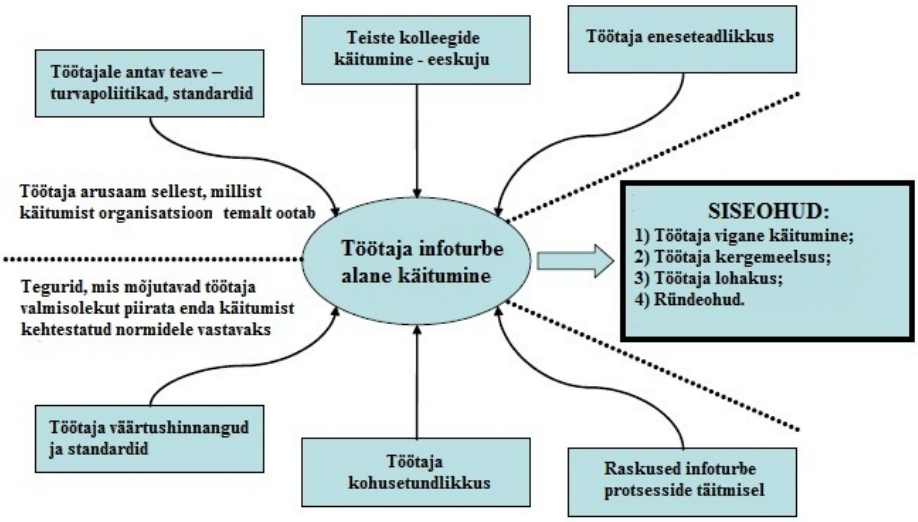
Töötajaid, täpsemalt nende infoturbe alast käitumist, on peetud infoturbe protsesside toimimise aluseks[61]. Täites organisatsioonis oma ülesandeid puutuvad töötajad kokku infovarade ja -süsteemidega. Suurem osa organisatsioone usaldab oma töötajaid andes neile volitusi töödelda organisatsioonile kuuluvaid infovarasid. On oluline teada, et töötajate käitumine võib organisatsiooni infovaradele tähendada nii kaitset kui ohtu.[62] Infoturbe teadlaste arvates võib töötajate käitumine tekitada väga suuri infoturberiske, kuna töötajad on usaldusväärsed organisatsiooni liikmed, kelle suhtes ei kehti suurem osa väliseid turvameetmeid (tulemüürid, antiviirused jne), mida organisatsioon rakendab selleks, et tagada teabe käideldavust, terviklust ja konfidentsiaalsust[63].

Töötajaid on sageli peetud infosüsteemide nõrgimaks lüliks, kuna neil on paljudel juhtudel täielik ligipääs infosüsteemides olevale teabele, mis annab neile võimalused tekitada organisatsioonile olulist majanduslikku kahju[64]. Ernst & Young´i rahvusvahelises uuringus uuriti 1400 ettevõtet kokku 50-st erinevast riigist ja leiti, et töötajate põhjustatud turvaintsidendid tulenesid kõige sagedamini madalast infoturbe alasest teadlikkusest. Paul van Kessel´i sõnul võib organisatsioonidel kuluda aastaid oma maine ja usaldusväärsuse väljatöötamiseks, kuid piisab vaid ühest töötaja põhjustatud turvaintsidendist, et rikkuda varasemad jõupingutused.[65] Seega on organisatsioonidel soovitatav suhtuda töötajate käitumisse äärmise tähelepanelikkusega.

Juba keskajal usuti, et inimmõistus koosneb kolmest osast – ratsionaalsus, emotsionaalsus ja tahtevõimelisus. Teisisõnu inimene mõtleb, tunneb ja tegutseb.[66] Kabay sõnul tugineb inimeste turvalisusega seonduv käitumine suhtumisel ja uskumusel, mida mõjutavad

[60]Riigi Infosüsteemid, "Asutuse Infoturbepoliitika" <http://www.riso.ee/sites/default/files/soovitused/tinfoturbpol.htm> (05.03.2014).
[61]Wood, M. B., „*Introducing Computer Security",* (NCC Publications, 1982), p46.
[62]Whitman, M. E., Enemy at the Gate: Threats to Information Security, *Communications of the ACM*, 46, 8, 2003, 91-95.
[63]Stanton, J. M., Stam, K. R., Mastrangelo, P. and Jolton, J., Analysis of end user security behaviors, *Computers & Security*, 24, 2, 2005, 124–133, p125.
[64]Warkentin, M., and Willison, R., Behavioral and policy issues in information systems security: the insider threat, *European Journal of Information Systems*, 18, 2, 2009, 101-105, p102.
[65]Ernst & Young, „Global information security survey 2008" <http://www.continuitycentral.com/news04217.html > (01.02.2014).
[66]Lotz, D. "Pärast valgustusajastut ja postmodernismi. Karistuse kutse, mis juhatab õiget mõistust, õigeid südameid ja õigeid käsi!" (2000) <ekklesia.ee/vana/elu/d5.pdf> lk3 (20.02.2014)

põhiliselt isiklikud väärtushinnangud[67]. Sellele lisaks on arvatud, et inimeste käitumist mõjutavad ka kehtivad sotsiaalsed normid[68]. Organisatsioonidesse kuuluvad erineva taustaga inimesed, kes omavad seejuures erinevaid väärtushinnanguid ja tõekspidamisi, mistõttu võidakse suhtuda erinevalt ka organisatsioonis kehtivatesse normidesse. Infoturbe efektiivsuse huvides on oluline, et organisatsiooni töötajad mõistaksid üheselt infoturbe vajalikkust, see tähendab, et infoturve peab kuuluma töötajate väärtushinnangute hulka[69]. Leach´i sõnul on siseohu peamiseks põhjuseks töötajate vale käitumine ning selle ennetamiseks on oluline mõista käitumist mõjutavaid tegureid. Leach´i arvates jagunevad töötajate infoturbe alast käitumist mõjutavad tegurid kaheks – esiteks töötajate teadlikkus sellest, millist käitumist organisatsioon neilt ootab; teiseks tegurid, mis mõjutavad töötajate valmisolekut piirata enda käitumist kehtestatud normidele vastavaks (vt Joonis 3).[70]



Joonis 3. Töötaja infoturbe alane käitumine[71] (autori kohandatud)

Leach on kirjeldanud joonisel 3 toodud tegureid järgnevalt. Antav teave – antud tegur kätkeb turvapoliitikaid ja standardeid, mille laiem eesmärk on aidata omandada turvalised käitumisnormid. Infoturbe alane käitumine sõltub infoturbepoliitikatest ja standarditest arusaamisest. Seega rõhuasetus on kergesti loetavusel ja mõistetavusel. Kolleegide käitumine – teiste kolleegide ja juhtkonna eeskuju on väga oluline tegur töötaja käitumise kujundamisel. Eneseteadlikkus – turvaeeskirjad ei määratle kõikide sündmuste jaoks tegevusi, millega

[67]Kabay, M. E., "Using Social Psychology to Implement Security Policies", (2009) <www.mekabay.com/infosecmgmt/Soc_Psych_INFOSEC.pdf> p12-13 (20.02.2014).
[68]Jolibert, A., & Baumgartner, G., Values, Motivation and Personal Goals: Revisited, *Psychology & Marketing*, 14, 17, 1997, 675-688, p678.
[69]Thomson, K., von Solms, R., Louw, L., „Toward Corporate Information Security Obedience" <http://dl.ifip.org/index.php/AICT/article/viewFile/32363/1084> p27 (10.02.2014).
[70]Leach, J, Improving User Security Behaviour, *Computer & Security*, 22, 8, 2003, 685-692.
[71]*Ibid.*

töötaja võib reaalselt kokku puutuda. Seega tegutsetakse enamasti eneseteadlikkusele ja varasematele kogemustele tuginedes. Infoturbepoliitika annab üksnes suunised õigeks käitumiseks, mida seostatakse isiklike teadmiste ja varasemalt läbikogetuga. Väärtushinnangud ja standardid – enamik töötajaid üritab järgida organisatsiooni väärtusi ja standardeid tingimusel, et need on kooskõlas isiklike väärtustega. Vastuolu korral hindab enamik töötajaid isiklikud väärtused ümber, lõpetab töösuhte või neist saavad potentsiaalsed turvanõete rikkujad. Kohusetundlikkus – üldiselt võib turvanõuete järgimine tekitada töötajate seas vastumeelsust. Kui töötajad tajuvad näiteks seda, et organisatsioonid on käitunud nende suhtes valesti (teinud ülekohut), võib nende suhtumine infoturbesse muutuda. Töötajad võivad olla ühel hetkel väga õiguskuulekad ja teisel hetkel tahtlikud turvanõete rikkujad. Raskused infoturbe protsesside täitmisel – kui turvanõuded on liiga raskesti täidetavad, nõuavad seejuures liiga suurt pingutust ning tunduvad samas ebaotstarbekad, on suur tõenäosus, et neid ei täideta.[72]

Silowash´i jt sõnul on siseohtu võimalik ennetada, kuid see nõuab terviklikku strateegiat, mis sisaldab turvaeeskirju, korraldusi, organisatsiooni kultuuri, ja tehnilisi vahendeid[73]. West´i sõnul on turvalisus sageli abstraktne ja raskesti hoomatav kontseptsioon. Olukorras, kus töötajad langetavad valikuid turvalisema ja vähem turvalise otsuse vahel, on turvalisema otsuse tegemise tulemuseks sageli vaid see, et midagi nähtavat ei muutu ja oht ei avaldu.[74] Herley sõnul on turvanõuete eiramine töötajate poolt täiesti ratsionaalne tegu, kuna turvaeeskirjade täitmine nõuab sageli lisapingutusi[75]. Kuigi turvanõuete eesmärk on infovarade ja töötajate kaitsmine väliste rünnakute eest, suhtutakse sageli nende kasutamisse negatiivselt, sest töötajate hinnangul pikendab turvanõuete järgimine tööprotsesse ja vähendab töö tegemise efektiivsust[76].

Leach´i sõnul on väga oluline tegur töötajate käitumise kujunemisel kolleegide eeskuju. Kui organisatsiooni tuleb uus töötaja, võtab ta enamasti omaks organisatsioonis kehtivad normid ja väärtused. Kui uus töötaja näeb, et kolleegide suhtumine infoturbesse on tõrjuv ning seda ei

[72]Leach, J, Improving User Security Behaviour, *Computer & Security*, 22, 8, 2003, 685-692.
[73]Silowash, G. J., Cappelli, D. M., Moore, A. P., Trzeciak., R. F., Shimeall. T., Common Sense Guide to Mitigating Insider Threats, 4th Edition, *Software Engineering Institutem Paper 677* (2012) < http://repository.cmu.edu/cgi/viewcontent.cgi?article=1669&context=sei> p4 (06.02.2014)
[74]West, R. The Psychology of Security – Why do good users make bad decisions?, *Communication of the ACM* , 51, 5, 2008, 34-40, p36.
[75]Herley, C., So Long, And No Thanks fo the Externalities: The Rational Rejection Security Advice Users (2009) <http://research.microsoft.com/en-us/um/people/cormac/papers/2009/SoLongAndNoThanks.pdf> p2 (05.03.2014).
[76] West, R. The Psychology of Security – Why do good users make bad decisions?, *Communication of the ACM* , 51, 5, 2008, 34-40, p39.

peeta vajalikuks, on suur tõenäosus, et ka tema eirab peagi turvanõudeid.[77] Ruighaver´i jt sõnul on töötajate infoturbe alase käitumise kujunemisel väga oluline roll organisatsioonikultuuril[78]. Organisatsioonikultuur on kooslus organisatsioonis kehtivatest normidest ja väärtustest, mis kujundavad liikmete käitumist, hoiakuid ja ootusi[79]. Ruighaver´i jt sõnul on juhtkonna toetus väga oluline tegur infoturbe sobitamisel organisatsioonikultuuriga. Infoturbe toimimise efektiivsus sõltubki paljudel juhtudel juhtkonna toetusest. Kui organisatsiooni töötajad tajuvad, et juhtkond suhtub turvalisuse probleemidesse ükskõikselt või hoolimatult, siis muutub ka nende suhtumine peagi sarnaseks.[80] Infoturbe korraldamine on edukas vaid siis, kui juhtkond seda piisavas ulatuses jõustab ja on seejuures ise alluvatele turvanõute järgimisel eeskujuks.

Warketing ja Willison toovad töötajate tekitatud turvaintsidentide tekkepõhjustena välja tahtliku käitumise ja ettevaatamatuse. Tahtlik käitumine väljendub selles, et infoturbepoliitikast tulenevaid korraldusi eiratakse teadlikult, lähtudes isiklikest huvidest (näiteks rahulolematus organisatsiooniga, huligaansus, luure jne). Ettevaatamatus on ajendatud põhjustest, mis on seotud madala infoturbe alase teadlikkusega, puuduliku motivatsiooniga jne.[81] Mõlemad käitumisviisid viitavad töötajate ratsionaalsusele, valikute tegemisele selliselt, nagu neile kasulikum tundub. Tahtliku rikkumise korral võib töötaja olla teadlik organisatsiooni turvanõuetest, kuid eirab neid isikliku kasusaamise eesmärgil. Ettevaatamatus ei pea olema seotud tahtlusega, kuid töötaja võib sellegipoolest lähtuda valikute tegemisel ratsionaalsusest. Ta ei pruugi teada, kuidas on õige käituda teatud olukorras ja sellest lähtuvalt käitub nii, nagu talle hetkel kasulikum tundub. Paraku võib selline käitumine kätkeda potentsiaalset turvaohtu.

Leach´i sõnul on väga oluline, et turvaeeskirjad ja standardid oleksid selgesti loetavad ja arusaadavad. Kui töötajad ei saa aru organisatsiooni turvaeeskirjadest, võib see tekitada raskusi turvanõuete järgimisel. Niisamuti võib turvaeeskirjade lugemine tekitada vastumeelsust, kui need on väga pikad ja mahukad.[82] Turvaeeskirjade lugemine võib tunduda ka aeganõudva ja ebavajalikuna, kuna paljudel juhtudel arvatakse, et ollakse teadlikud

[77]Leach, J, Improving User Security Behaviour, *Computer & Security*, 22, 8, 2003, 685-692.
[78] Ruighaver, A. B., Maynard, S. B., & Chang, S., Organisational Security Culture: Extending the End User Perspective, *Computers & Security, 26*, 2007, 56-62, p56.
[79]Schein, E. H., *Organizational Culture & Leadership Third Edition* (San Francisco, CA:Jossey-Bass, 2004), p17.
[80]Ruighaver, A. B., Maynard, S. B., & Chang, S., Organisational Security Culture: Extending the End User Perspective, *Computers & Security, 26*, 2007, 56-62, p59.
[81]Warkentin, M., and Willison, R., Behavioral and policy issues in information systems security: the insider threat, *European Journal of Information Systems*, 18, 2, 2009, 101-105, p101.
[82]Leach, J, Improving User Security Behaviour, *Computer & Security*, 22, 8, 2003, 685-692.

võimalikest ohtudest ja osatakse neid vältida[83]. Paraku näitavad uuringud vastupidist[84]. Organisatsioon peab tegelema infoturbe juurutamisega süstemaatiliselt, sest vastasel korral langeb peagi töötajate huvi turvanõudeid järgida ning see võib kaasa tuua infoturbeohte.

Kui eelkirjeldatud tegurite toimel turvanõuete järgimist ei tagata, siis üldjuhul on organisatsiooni huvides kohaldada lisaabinõusid tõhustamaks töötajatepoolset turvanõuete järgimist. Töötajate käitumise mõjutamiseks võidakse kasutusele võtta turvameetmed, mis koos rakendudes peaksid tugevdama organisatsioonikultuuri.[85] Nimetatud meetmete hulka kuulub näiteks infoturbe alase teadlikkuse tõstmine. Kuna töötajad kujundavad paljudel juhtudel oma suhtumise infoturbesse lähtuvalt teadlikkusest ja organisatsioonis kehtivatest normidest, on teadlaste hinnangul üks efektiivsemaid viise töötajate infoturbe alase käitumise parendamiseks infoturbe alase teadlikkuse tõstmine, mida on kinnitanud samuti teaduslikud uuringud.[86]

Infoturbe alase teadlikkuse tõstmise laiem eesmärk on informeerida töötajaid infoturberiskidest ja tutvustada õigeid käitumisviise. Sageli ei teata, mida tähendab turvalisuse tagamine ning milliseid tagajärgi võib infoturbe korralduste mittejärgimine kaasa tuua.[87] Kurjategijate (näiteks häkkerid) edukus tuleneb paljudel juhtudel töötajate naiivsusest ja teadmatusest. Näiteks infopüük on üks levinumaid viise, kuidas organisatisoonile kuuluvat teavet kergesti kätte saada. Infopüügi kaudu meelitatakse organisatsiooni töötajatel välja teavet, mille abil on võimalik organisatsioonile kahju tekitada[88]. Seega on organisatsiooni infovarade kaitsmise huvides oluline koolitada töötajaid ja tõsta nende teadlikkust, et ennetada infoturbeohtude avaldumisel tekkivat kahju. Teadlaste arvates on infoturve üksnes nii hea, kui hästi viivad seda ellu organisatsiooni töötajad, sest tehnilistest lahendustest üksi ei piisa, et kaitsta organisatsiooni ja sellele kuuluvaid varasid[89].

Eeltoodule lisaks on infoturbe praktikas kasutatud töötajate kontrollimist. Töötajate kontrollimist on peetud sageli tehnoloogiliseks turvameetmeks, kuna see põhineb enamasti

[83]West, R. The Psychology of Security – Why do good users make bad decisions?, *Communication of the ACM* , 51, 5, 2008, 34-40, p36.
[84]Ernst & Young, „Global information security survey 2008" <http://www.continuitycentral.com/news04217.html > (01.02.2014).
[85]*Ibid*, p685.
[86]Siponen, M. T., A Conceptual Foundation for Organizational Information Security Awareness, *Information Management & Computer Security, 8,* 1, 2000, 31-41, p31.
[87]Sandhu, R., Good-Enough Security: Toward a Pragmatic Business-Driven Discipline, *IEEE Internet Computing*, 3, 2003, 66-68, p67.
[88]Workman, M., Gaining Access with Social Engineering: An Empirical Study of the Threat, *Information Systems Security Journal*, 16, 6, 2007, 315-331, p315.
[89]Henry, K., "Risk Management and Analysis", *Information Security Management Handbook 5th Edition*, Ed. Tipton, H. & Krause, M. (CRC Press, Boca Raton,2004), p751.

tehnilistel järelevalvelistel tegevustel[90]. American Medical Association´i uuringute kohaselt on populaarsemateks järelevalvelisteks tegevusteks interneti tegevuse jälgimine (66%), telefonide järelevalve (45%) ja e-kirjade (43%) kontrollimine. Eeltoodud tegevusi on nimetatud koos elektrooniliseks järelevalveks.[91] Infoturbespetsialistide ja juhtkonna arvates on töötajate kontrollimine tehniliste vahendite abil üks efektiivseimaid viise ennetamaks siseohu teket[92]. Kuid leidub ka uuringuid, mis on kinnitanud vastupidist[93]. Kuigi elektroonilise järelevalve kasutamist on peetud vägagi populaarseks, ei välista see kõigil juhtudel ebasoovitavat käitumist (näiteks paroolide üleskirjutamist ja nende jagamist). Elektroonilist järelevalvet kasutatakse ka selleks, et tõhustada tööprotsesside toimimist. Kui töötajad tajuvad, et neid võidakse jälgida, tegelevad nad vähem kõrvaliste asjadega (internetis uudiste lugemine, sotsiaalmeedia kasutamine jms) ning keskenduvad rohkem tööprotsessidele. Joinson ja Whitty sõnul tuleb elektroonilise järelevalve kasutamisega olla ettevaatlik. Nimetatud meetme liigne kasutamine võib tekitada töötajates tunde, et organisatsioon ei usalda neid ning sellest tulenevalt tekitada töötajates rahulolematust ja stressi, mis võib omakorda mõjutada tööprotsesside efektiivsust. Usalduse küsimus on sageli tekitanud probleeme elektroonilise järelevalve kasutamisel. Selleks, et mõjutada töötajate suhtumist, peavad organisatsioonid töötajaid teavitama, et nimetatud meetmete kasutamine on üksnes turvalisuse tagamise eesmärgil ja nende kohta kogutud andmeid hallatakse turvaliselt. Joinson ja Whitty on siiski seisukohal, et järelevalveliste meetmete kasutamine vähendab töötajate usaldust organisatsiooni suhtes.[94]

Omaette grupi moodustavad infoturbe tagamisel mitmesugused heidutavad meetmed. Teadlaste hinnangul võimaldab heidutavate meetmete rakendamine suurendada töötajate huvi järgida organisatsiooni turvanõudeid[95]. Töötajate infoturbe alast käitumist mõjutavaid turvameetmeid on veel (näiteks läbipääsu reguleerimine, audentimine jne), kuid autor ei pea nimetatud meetmete käsitlemist oluliseks, kuna magistritöö keskendub üksnes heidutavate meetmete rakendamise uurimisele.

---

[90]Joinson, A. & Whitty, M., Watched in workplace, *Infosecurity*, 5, 1, 2008, p38-40.
[91]AMA/ePolicy Institute Research, „2007 Electronic Monitoring & Surveillance Survey" (2007) <http://www.plattgroupllc.com/jun08/2007ElectronicMonitoringSurveillanceSurvey.pdf> p1-3 (06.03.2014).; Wakefield, R. L., Employee Monitoring and Surveillance – The Growing Trend, *Information Systems Control Journal*, 1, 2004, 1-3, p1.
[92]Joinson, A. & Whitty, M., Watched in workplace, *Infosecurity*, 5, 1, 2008, p38-40.
[93]GFI, Security Survey in the United States (2007) <http://www.gfi.com/documents/rv/smbsurvey.pdf> p12 (06.03.2014).
[94]Joinson, A. & Whitty, M., Watched in workplace, *Infosecurity*, 5, 1, 2008, p38-40.
[95]D'Arcy, J. and Hovav, A. Deterring internal information systems misuse: An end user perspective, *Communications of the ACM*, 50, 10, 2007, 113-117.; Straub, D. W., Welke, R. J., Coping with systems risk: Security planning models for management decisions making, *MIS Quart*, 22, 4, 1998, 441-469.

Kokkuvõtlikult võib alapeatükist välja tuua, et töötajate infoturbe alane käitumine, mida võib defineerida kui töötajate käitumist infoturbepoliitika seisukohalt, võib organisatsioonis tekitada suuri infoturberiske. Seepärast on organisatsioonidel soovitatav pöörata töötajate käitumisele tähelepanu ja püüda mõista infoturbe käitumist mõjutavaid tegureid. Erinevad teadlased on toonud välja mitmeid töötajate infoturbe alast käitumist mõjutavaid tegureid nagu organisatsioonikultuur, teadlikkus, ratsionaalsus jne[96]. Kui turvalisust üksnes nende tegurite toimel ei saavutata, on organisatsiooni huvides kohaldada lisaabinõusid töötajate turvanõuete järgimise tõhustamaks. Üks efektiivsemaid viise töötajate infoturbe alase käitumise parendamiseks on infoturbe alase teadlikkuse tõstmine. Peale selle kasutatakse töötajate kontrollimist jne. Omaette abinõude grupi moodustavad ka heidutavad meetmed. Järgnev alapeatükk käsitlebki lähemalt heidutuse teoreetilisi aluseid ning selle seoseid infoturbe alase käitumisega andes sissejuhatuse magistritöö empiirilisele uuringule.

1.3 Heidutuse teoreetilised alused ja rakendamise võimalused infoturbes

Eelmine peatükk tutvustas infoturbe alast käitumist, seda mõjutavaid tegureid ning turvameetmeid, mida organisatsioonid rakendavad turvalisuse saavutamiseks. Magistritöö eesmärgist tulenevalt keskendub käesolev peatükk lähemalt heidutavatele meetmetele ning nende rollile töötajate infoturbe alase käitumise kujundamisel. Peatükk jaguneb sisult kaheks. Selle esimeses pooles tutvustab autor heidutuse teooria kujunemist ja olemust. Peatüki teises pooles uurib autor konkreetsemalt heidutavate meetmete rakendamise võimalusi infoturbe alase käitumise kujundamiseks.

Kuna töötajate soovimatu käitumine võib põhineda nii tahtlusel kui ettevaatamatusel, on teadlased samastanud seda kriminoloogias uuritava hälbiva käitumisega. Hälbiv käitumine on ühiskonnas aktsepteeritud tegevusviisidele ja käitumismallidele mittevastav käitumine[97]. Võttes aluseks kriminoloogiast tuntud teooriad (heidutuse teooria, ratsionaalse valiku teooria, neutraliseerimistehnikate teooria, sotsiaalse kontrolli teooria), on infoturbe valdkonnas läbi

[96]Leach, J, Improving User Security Behaviour, *Computer & Security*, 22, 8, 2003, 685-692; West, R. The Psychology of Security – Why do good users make bad decisions?, *Communication of the ACM* , 51, 5, 2008, 34-40, p36.; Ruighaver, A. B., Maynard, S. B., & Chang, S., Organisational Security Culture: Extending the End User Perspective, *Computers & Security, 26*, 2007, 56-62, p56.

[97]Crossler, R. E., Johnston, A. C. Lowry, P. B., Hu, Q., Warketin, M. Baskerville, M., Future directions for behavioral information security research, *Computer & Security*, 32, 2013, 90-101.

viidud erinevaid uuringuid[98]. Enim on töötajate infoturbe alast käitumist uuritud heidutuse teooriale toetudes, mis on valitud ka käesoleva uurimuse teoreetiliseks aluseks.

Heidutuse teooria väidab, et inimeste käitumist on võimalik muuta karistusi kohaldades[99]. Heidutuse mõiste (ingl k *deterrence*) pärineb kriminoloogiast ja sellega tähistatakse karistamise kasutamist hirmutamaks ühiskonnaliikmeid hoiduma õigusrikkumiste toimepanemisest. Kriminoloogias on heidutuse teooria välja kujunenud Thomas Hobbes´i (1588-1678), Cesare Beccaria (1738-1794) ja Jeremy Bentham´i (1748-1832) töödest. Nad uskusid, et inimese kuritegelik käitumine leiab aset siis, kui see toob kaasa naudingu (loob tasu saamise võimaluse) ja samaaegselt on risk karistada saada väike. Sellest tulenevalt leiti, et süüdlase karistamine peaks kaasa tooma kuritegevuse vähenemise.

Heidutusel on teooria kohaselt kaks eesmärki. Karistamise laiem eesmärk on tekitada õiguskuulestust, andes rahvale teada, et seadustele mitteallumine toob kaasa karistuse, mistõttu nad hoiduvad sarnaste õigusrikkumiste toimepanemisest tulevikus (üldpreventsioon). Üldpreventsioon jaguneb omakorda kaheks – negatiivseks ja positiivseks preventsiooniks. Negatiivset preventsiooni tuntakse hirmutamispreventsioonina, mis seisneb konkreetse isiku karistamisega teistele isikutele hirmutava toime avaldamises. Positiivse preventsiooni eesmärk on avaldada õiglase karistusega mõju, mis kinnitab inimeste usku normikehtivusse ja usaldust õiguskorra vastu. Eripreventsioon keskendub konkreetsete üksikkurjategijate mõjutamisele, nähes karistuse eesmärki selle isiku veenmises edaspidi hoiduma süütegude toimepanemisest.[100] Esiteks peab heidutus vähendama kuritegevuse levikut ühiskonnas ja hirmutama kodanikke kuritegudest loobuma läbi kartuse saada karistada. Teiseks peab heidutus mõjutama kurjategijat tulevikus hoiduma uusi kuritegusid sooritamast.

Heidutuse teooria (ingl k *deterrence theory*) kohaselt on kuritegevust võimalik vähendada läbi karistuse rakendamise, sest suureneb kuritegevuse hind ja arusaam, et kuritegevus ei tasu ennast ära. Heidutus vähendab kuritegevuse meeldivust ja tulusust. Becker on käsitlenud karistust olulise mõjutegurina kuritegude sooritamise vähenemisel. Becker leidis, et saadav

[98]D'Arcy, J. and Hovav, A. Deterring internal information systems misuse: An end user perspective, *Communications of the ACM*, 50, 10, 2007, 113-117.; Bulgurcu, B., Cavusoglu, H., & Benbasat, I. Information Security Policy Compliance: An Empirical Study of Rationality-Based Beliefs and Information Security Awareness. *MIS Quarterly*, 34, 3, 2010, 523-548.; Siponen, M., Vance, A., Neutralization: New Insights Into the Problem of Employee Information Systems Security Policy Violation, *MIS Quarterly*, 34, 3, 2010, 487-502.; Lee, S. M., Lee, S. and Yoo, S. An Integrative Model of Computer Abuse Based on Social Control and Deterrence theories, *Information & Management*, 41, 2004, 707-718.

[99]Vito, G. F., Maahs, J. R., *Criminology Theory, Research and Policy, Third Edition* (Jones & Bartlett Learning Publication, 2011), p51.

[100]Kivi, L. Sootak, J., Karistuse kohaldamise alused karistusseadustikus, *Juridica*, 2001, 7, 475-484.

karistus suurendab kuriteo sooritamise hinda, mis toob kaasa kuritegude arvu vähenemise. Muuhulgas uskus ta, et seadusekuulelikku käitumist on võimalik suurendada läbi inimeste harimise ja karistusmäärade tõstmise.[101]

Heidutuse teooria väidab, et kui karistus on piisavalt „kiire (rakendub vahetult peale kuriteo toimepanemist), kindel (järgneb teole igal juhul) ja karm", siis on inimese huvides kuuletuda seadusele. Karistus peab olema piisavalt karm, et mõjuda heidutavalt. Seejuures peab see olema proportsioonis tehtava teoga vältimaks ebaõiglust. Karistuse kindlus seisneb teadmises, et toime pandud kuritegu saab kindlasti karistatud. Klassikalised teoreetikud, muuhulgas Beccaria uskusid, et kui inimene teab, et tema sooritatavale teole järgneb karistus, hoidub ta selle toimepanemisest tulevikus. Veelgi enam, leiti, et karistus peab olema võimalikult kiire, st järgnema kuriteole koheselt, et mõjutada inimest kuriteost loobuma. Mida kiiremini kohaldub karistus, seda suurem on tõenäosus, et potentsiaalne kurjategija saab aru, et kuritegu ei tasu ennast ära.[102] Eeltoodust järeldub, et parim viis ennetada või vähenda kuritegevust, on suurendada karistuse kõiki kolme tegurit - kiirust, kindlust ja karmust. Kui potentsiaalse kurjategija hirm tabamise suhtes suureneb, võib ta otsustada loobuda hälbivast käitumisest, sest karistada saamise risk kaalub üles saadava kasu.

Siegel toob välja, et karistuste rakendamise kõrval omab heidutavat mõju kuritegelikule käitumisele ka ümberkaudsete hukkamõist, mis väljendub eelkõige kurjategija stigmatiseerimises, vihkamises ja eemaletõukamises lähedaste (vanemad, partnerid, sõbrad, naabrid, kolleegid, õpetajad jne) poolt. See võib kaasa tuua häbitunde, piinlikkuse ja lugupidamise vähenemise iseenda suhtes. Mitmed uuringud on tõestanud, et ümberkaudsete hukkamõist omab võrreldes karistamisega isegi suuremat mõju karistuse vähenemisele. Selle põhjusena näeb Siegel sotsiaalset kontrolli, mis mõjutab inimest tajutava negatiivse reaktsiooni kaudu suhetes lähedastega.[103]

Heidutuse teooria näeb piinlikkuse ja häbitunde kartust tugeva mõjutegurina kuritegeliku käitumise suhtes. Indiviidid, kes kardavad ümberkaudsete hukkamõistu, suhtuvad vastumeelselt ka hälbivasse käitumisse, mis avaldub peamiselt kahel viisil. Esiteks seostub neile seaduserikkumine isikliku häbitundega. Teiseks on kartus avaliku häbitunde ees. Seega isikud, kes teadvustavad endale, et hälbiv käitumine võib põhjustada häbitunnet, on vähem

[101]Becker, G. S., Crime and Punishment: An Economic Approach, *The Journal of Political Economy*, 76, 2, 1968, 169-217, p 176-178.
[102]Onwudiwe, I. D., Odo, J and Onyeozili, C., „Deterrence Theory", *Encyclopedia of Prison & Correctional Facilities*, Ed. Bosworth, M. (Thousand Oaks, CA, SAGE Publications, 2005), p 235.
[103]Siegel, L. J., *Criminology, Ninth Edition* (Thomson Wadsworth, 2008), p 115.

altid rikkuma seadusi, võrreldes nendega, kes seda ei teadvusta. Kuigi heidutuse teooria näeb piinlikkuse ja häbitunde kartust tugeva mõjutegurina, sõltub selle mõju lisaks ka kogukonna iseärasustest ja kuriteoliigist. Näiteks võib selline karistus olla väga efektiivne kogukonnas, kus inimesed on omavahel tuttavad, kuna kuriteo varjamine avalikkuse eest oleks raskendatud.[104]

Kokkuvõtlikult järeldub eeltoodust, et heidutuse teooria kohaselt on inimeste käitumist võimalik mõjutada karistustega ja sotsiaalset survet (ümberkaudsete hukkamõistu) kohaldades. Esiteks peab heidutus vähendama kuritegevuse levikut ühiskonnas hirmutades kodanikke kuritegudest loobuma läbi kartuse saada karistada (üldpreventsioon). Teiseks peab heidutus mõjutama kurjategijat tulevikus hoiduma uusi kuritegusid sooritamast (eripreventsioon). Efektiivseim on heidutus juhul, kui karistus on kiire, kindel ja piisavalt karm.

Heidutuse teooria põhiseisukohti on autor kasutanud selgitamaks eelmises alapeatükis käsitletud töötajate infoturbe alast käitumist. Mitmed teadlased (eelkõige Straub) on heidutuse teooriale tuginedes läbi viinud empiirilisi uuringuid[105]. Nende põhjal on jõutud seisukohale, et heidutavad meetmed aitavad parandada töötajate õiguskuulekust turvameetmete järgimisel, kuna töötajad tajuvad enam turvameetmete eiramisega kaasnevat vastutust.[106] Nagu selgus eelmises alapeatükis, on töötajate infoturbe alast käitumist mõjutavaid tegureid mitmeid (organisatsioonikultuur, eeskujud jne). Antud töö eesmärgi seisukohast on oluline märkida, et avaliku sektori töö tõhususe ja maine säilitamise huvides on ära kasutada kõik võimalikud viisid infoturbepoliitika järgimise tagamiseks infosüsteemide kasutajate seas. Seetõttu on käesoleva töö autor võtnud vaatluse alla heidutuse rakendamise kui ühe abinõu töötajate infoturbe alase käitumise mõjutamiseks. Järgnevalt uuribki autor heidutavate meetmete, eelkõige sanktsioonide ja ümberkaudsete hukkamõistmise rakendamist töötajate infoturbe alasele käitumisele.

---

[104] *Ibid*, p115.

[105] Straub, D.W. Computer abuse and computer security: Update on an empirical study, *Security, Audit and Control Review*, 4, 2, 1986, 21-31.; Hoffer, J. A., & Straub, D. W., The 9 to 5 underground: Are you policing computer crimes? *Sloan Management Review*, 30, 4, 1989, 35.; Straub, D. W., & Nance, W. D. Discovering and disciplining computer abuse in organizations: A field study. *Managemet Information Systems Quarterly*, 14, 1, 1990, 46-62.; Straub, D. W., Welke, R. J., Coping with systems risk: Security planning models for management decisions making, *MIS Quart*, 22, 4, 1998, 441-469.

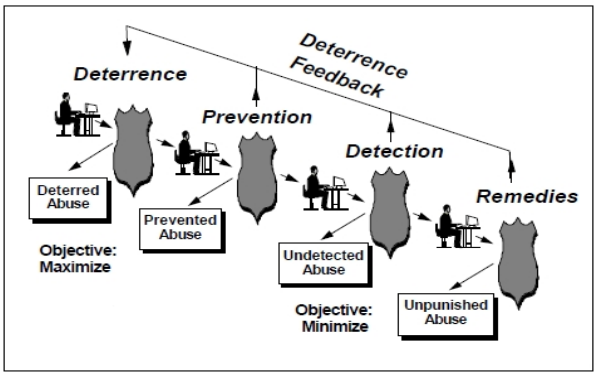
[106] Straub, D. W., Welke, R. J., Coping with systems risk: Security planning models for management decisions making, *MIS Quart*, 22, 4, 1998, 441-469.; D'Arcy, J. and Hovav, A. Deterring internal information systems misuse: An end user perspective, *Communications of the ACM*, 50, 10, 2007, 113-117.; Hu, Q., Xu, Z., Dinev, T. and Ling, H., Does Deterrence Work in Reducing Information Security Policy Abuse by Employees?, *Communication of the ACM*, 54, 6, 2011, 54-60.

Eespool selgus, et infoturbe peamine eesmärk on tagada organisatsiooni infovarade turvalisus, mille saavutamiseks rakendavad organisatsioonid erinevaid turvameetmeid. Kotulic´i ja Clark´i sõnul on turvameetmete kasutamise eesmärk ära hoida, ennetada ja tuvastada võimalikke turberiske infovaradele[107]. Samuti näitab eelnev teoreetiline käsitlus, et infovarade turvalisus sõltub paljudel juhtudel organisatsiooni enda töötajate käitumisest. Infoturbe toimimine sõltub eranditult kõigist töötajatest ning sellest tulenevalt on organisatsiooni huvides, et töötajad järgiksid kehtivaid turvanõudeid ja eeskirju. Töötajapoolne kehtivate turvameetmete eiramine on käsitletav õigusrikkumisena infoturbepoliitika mõttes. Seetõttu on leitud, et organisatsioonil peab säilima võimalus mõjutada töötajate käitumist, et viia see kooskõlla infoturbepoliitikaga. Teadlaste hinnangul kaotab infoturbepoliitika oma mõtte, kui selle järgimist ei ole võimalik tagada.[108]

Heidutuse teooria rakendamine põhineb sisult samadel eesmärkidel – heidutuse abil ära hoida, ennetada ja tuvastada õigusrikkumisi. Heidutuse teooria peab vajalikuks kohaldada vastutusele võtmist, mis seisneb seaduserikkujate karistamises või ümberkaudsete hukkamõistus, et hirmutada potentsiaalseid rikkujaid hoiduma valest käitumisest tulevikus.[109] Heidutuse rakendamine võib olla kohane ka infoturbepoliitika ellu viimisel avaliku sektori organisatsioonis.

Teoreetilise uurimuse teises osas jõudis autor järeldusele, et töötajate infoturbe alast käitumist mõjutavad mitmed tegurid nagu organisatsioonikultuur, teadlikkus, ratsionaalsus jne. Kui turvalisust üksnes nende tegurite toimel ei saavutata, on organisatsiooni huvides kohaldada lisaabinõusid töötajate turvanõuete järgimise tõhustamaks. Selliste abinõude hulka kuuluvad heidutavad meetmed. Joonisel 4 on kujutatud heidutavate meetmete kohta infoturbe tagamise süsteemis.

[107]Kotulic, A. G., Clark, J. G., Why there aren't more information security research studies, *Information & Management*, 41, 5, 2004, 597-607, p597.
[108]Von Solms, B., & von Solms, R., The 10 Deadly Sins of Information Security Management, *Computer & Security*, 23, 2004, 371-376, p372.
[109]Straub, D. W., Welke, R. J., Coping with systems risk: Security planning models for management decisions making, *MIS Quart*, 22, 4, 1998, 441-469.



Joonis 4. Turvalisuse saavutamise tsükkel (i.k *Security Action Cycle*)[110]

Jooniselt nähtub, et turvariskide vähendamisel on kasutatav neljaastmeline tegevus – heidutamine (ingl k *deterrence*), ennetamine (ingl k *prevention*), tuvastamine (ingl k *detection*) ja korvamine (ingl k *remedies*). Neid tegevusi koos nimetatakse turvalisuse saavutamise tsükliks (ingl k *Security Action Cycle*) (Joonis 4). [111] Joonisel on ka ilmekalt näha heidutuse tähtsus, mis tsükli esimese etapina peab mõjutama töötajaid turvanõudeid järgima. Alles siis, kui heidutus ei toimi ja töötaja siiski otsustab turvanõudeid rikkuda asuvad toimima vale tegevust ennetavad meetmed, rikkumiste tuvastamist võimaldavad mehhanismid ja lõpuks rikkumist korvavad ja heastavad meetmed.

Infoturbes seisneb heidutuse eripära selles, et turvameetmed toimivad heidutava mehhanismina, suurendades infosüsteemide väärkasutamisel tajutavat vastutust, vähendades seejuures turvaintsidentide ilmnemist.[112] Heidutuse teooria kohaselt on inimeste käitumist võimalik muuta karistusi kohaldades. Sellest tulenevalt on töötajate motiveerimist sanktsioonidega peetud üheks võimaluseks turvaintsidentide arvu vähendamisel.[113] Teadlaste väitel aga vähendab juba aktiivne ja nähtav infoturbepoliitika arvutialaseid kuritarvitusi ja veenab potentsiaalseid rikkujaid selles, suure tõenäosusega nende rikkumine avastatakse ja sellele järgneb karm karistus (karistuse kindluse ja karmuse aspekt)[114].

Infoturbe meetmeid iseloomustab omadus heidutada potentsiaalseid turvanõuete eirajaid vältima tegevusi, mis otseselt või kaudselt rikuvad organisatsiooni infoturbenõudeid. On

[110]Straub, D. W., Welke, R. J., Coping with systems risk: Security planning models for management decisions making, *MIS Quart*, 22, 4, 1998, 441-469.
[111]*Ibid.*
[112]D'Arcy, J. and Hovav, A. Deterring internal information systems misuse: An end user perspective, *Communications of the ACM*, 50, 10, 2007, 113-117.
[113]Kabay, M. E., "Using Social Psychology to Implement Security Policies", (2009) <www.mekabay.com/infosecmgmt/Soc_Psych_INFOSEC.pdf > p12 (20.02.2014).
[114]Straub, D. W., Welke, R. J., Coping with systems risk: Security planning models for management decisions making, *MIS Quart*, 22, 4, 1998, 441- 469.

empiiriliselt tõendatud, et turvameetmete rakendamine vähendab infosüsteemi siseriske. Teatav roll selles on ka infoturbespetsialistidel. Üldiselt võttes on selge, et enamus töötajaid, kellele on usaldatud ligipääs organisatsiooni infovaradele, siiski järgib turvanõudeid ka ilma karistustest tuleneva heidutuseta. Selleni viivad neid eelpool vaadetud tegurid, nende veendumised ja väärtushinnangud ning ka teadlikkus riskidest. Infoturbe valdkonnas on aga teadlikkusel lisaaspekt. Infoturbe teadlikkuse tõstmise käigus antakse töötajale ka teadmine, et organisatsioon suhtub infosüsteemide kaitsesse täie tõsidusega ning seejuures ei kohelda tahtlikke rikkujaid kergesti. Seega teadlikkuse tõstmise üks eesmärke on anda arvutikasutajatele teadmine, et infoturbe nõuete eiramine võib kaasa tuua sanktsioone ning veendumus, et neid sanktsioone kavatsetakse töötajate suhtes ka rakendada. Sellest tulenevalt on infoturbe teavitusüritused samuti üks heidutava abinõu vorm. Eelkõige on vastava teooria kohaselt tegu üldpreventsiooniga.[115]

Kui organisatsiooni töötajad eiravad kehtestatud turvanõudeid, seades ohtu organisatsioonile kuuluva tundliku teabe, võidakse nad vastutusele võtta organisatsiooni eeskirjade või kehtivate seaduste alusel. Sanktsioonide rakendamine võib tuleneda nii organisatsiooni enda dokumentidest kui ka kehtivatest seadustest. Näiteks sisejulgeoleku organisatsioonidel on ligipääs suurele hulgale tundlikule teabele, mille kaitset reguleerivad lisaks organisatsiooni eeskirjadele mitmed seadused (näiteks isikuandmete kaitse seadus[116]; riigisaladuse ja salastatud välisteabe seadus[117]; avaliku teabe seadus[118]). Sellisel juhul on heidutuse teooriast tulenevalt tegu kas üld- või eripreventsiooniga. Üldpreventiivne toime on infoturbe rikkumise korral rakendatud sanktsioonidel, mida töötaja kolleegid näevad ja tajuvad hoiatavana. Sel juhul hoiduvad nad sarnastest rikkumistest edaspidi. Eripreventiivne toime avaldub konkreetse töötaja puhul, kes tõenäoliselt püüab edaspidi mitte minna vastuollu organisatsiooni turvaregulatsiooniga.

Heidutav toime võib tuleneda ka turvanõuete eiramisele järgnevast ümberkaudsete hukkamõistust. Nagu eespool selgitatud, näeb heidutuse teooria tugeva mõjutegurina kartust piinlikkuse ja häbitunde ees. Töökollektiivis võib see osutuda oluliseks neil juhtudel, kui organisatsioonikultuur näeb olulise väärtusena turvanõuete järgimist. Heidutuse teooria pakub siinkohal selgituse kaastöötajate hukkamõistmise mõjule ka kõigile ülejäänud töötajatele,

[115]Straub, D. W., Welke, R. J., Coping with systems risk: Security planning models for management decisions making, *MIS Quart*, 22, 4, 1998, 441-469.
[116]Isikuandmete kaitse seadus, 15.02.2007, jõustunud 01.01.2008 – RT I 2007, 24, 127 … RT I, 30.12.2010, 11.
[117]Riigisaladuse ja salastatud välisteabe seadus, 25.01.2007, jõustunud 01.01.2008, RT I 2007, 16, 77 … RT I, 22.12.2011, 24.
[118]Avaliku teabe seadus, 15.11.2000, jõustunud 01.01.2001 – RT I 2000, 92, 597 ... RT I, 19.12.2012, 5.

kuna nad näevad, et valesti käitumine võib kaasa tuua negatiivse suhtumise neisse. Inimesed on üldjuhul erinevad väärtushinnangute ja uskumuste tõttu, mistõttu võivad nad suhtuda erinevalt organisatsiooni turvameetmete järgimise kohustusse[119]. Järelikult võivad töötajad suhtuda erinevalt ka organisatsioonipoolsetesse heidutavatesse meetmetesse. Teadlaste hinnangul on heidutuse efektiivsust võimalik tõsta ennetamise ja tuvastamise kaudu. Nimetatud tegevuste eesmärgiks on raskendada turvanõuete rikkumist ja tuvastada potentsiaalseid rikkujaid. Ennetavate tegevuste hulka kuuluvad peamiselt füüsilised tõkked (näiteks uste lukustamine, paroolide kasutamine).[120] Ennetamist on käsitletud aktiivse tegevusena, sest võimaldab turvanõuete järgimist jõustada ning tõrjuda eemale töötajate ebasoovitavat käitumist.[121] Tuvastamise hulka kuulub näiteks ootamatud auditeerimised või reageerimine turvaintsidentidele. Tuvastamise laiem eesmärk on koguda tõendeid infosüsteemide väärkasutuse kohta ning avastada väärkasutajad.[122]

Eeltoodud nelja tegevuse (heidutamine, ennetamine, tuvastamine, korvamise) koosmõju eesmärgiks on tõrjuda töötajate ebasoovitavat infoturbe alast käitumist, vähendades seeläbi siseohu tekkimise riski. Oluline on mõista, et heidutuse rakendamise eesmärk ei ole süstemaatiline töötajate karistamine. Heidutuse eesmärk on tõhustada töötajate õiguskuulekust turvameetmete järgimisel, st ära hoida siseohu tekkimise riski. Teadlaste hinnangul tasub heidutavate ja ennetavate tegevuste hulka suurendada, kuna see toob kaasa õiguskuulekama käitumise ja vähendab turvanõuete rikkumisi, mis omakorda vähendab tuvastamise ja vastutusele võtmise vajadust. Seega tuleb töötajaid järjepidevalt heidutada, st meelde tuletada, et turvameetmete eiramine toob kindlasti kaasa vastutusele võtmise (sanktsiooni või ümberkaudsete hukkamõistu) ja lisaks paigaldada füüsilisi tõkkeid, et muuta turvanõuete eiramist veelgi keerulisemaks (vt joonis 4). Kui töötaja siiski eirab eelnevalt nimetatud tegevusi, on organisatsiooni huvides võimalikult kiiresti see töötaja tuvastada, eesmärgiga juhtida tähelepanu valele käitumisele ja vajadusel rakendada vastutusele võtmist (korvavaid tegevusi). Kui eeltoodule järgneb edaspidi õiguskuulekam infoturbe alane käitumine, on heidutamine täitnud oma eesmärgi.[123]

[119]Kabay, M. E., "Using Social Psychology to Implement Security Policies", (2009) <www.mekabay.com/infosecmgmt/Soc_Psych_INFOSEC.pdf> p12-13 (20.02.2014).
[120]Straub, D. W., Welke, R. J., Coping with systems risk: Security planning models for management decisions making, *MIS Quart*, 22, 4, 1998, 441-469.
[121]Gopal, R. D., Sanders, G. L., Preventive and Deterrent Controls for Software Piracy, *Journal of Management Information Systems*, 3, 4, 1997, 29-47.
[122]Straub, D. W., Welke, R. J., Coping with systems risk: Security planning models for management decisions making, *MIS Quart*, 22, 4, 1998, 441-469.
[123]*Ibid.*

Empiirilised uuringud on kinnitanud heidutuse teooria kehtivust infoturbe alasele käitumisele. D´ Arcy jt leidsid, et turvameetmed omavad heidutavat efekti, kui rakendada vastutusele võtmist. Nad põhjendasid seda väitega, et töötajad tajusid turvanõuete eiramisega kaasnevat karistada saamise hirmu.[124] Hu jt uurisid töötajate infoturbe alast käitumist läbi heidutuse, ratsionaalse valiku ja enesekontrolli teooria. Nad leidsid, et turvaintsidentide põhjused on seotud töötajate ratsionaalse mõtlemisega – nähakse rohkem saadavat kasu (nt aja kokkuhoid) kui tehtavat kahju, mille tulemusena alahinnatakse turvanõuete rikkumisega kaasnevat riski vastutusele. Hu jt sõnul lähtuvad töötajad valikute tegemisel saadavast kasust rohkem siis, kui nad on madala enesekontrolliga, omakasupüüdlikud või riskialtid. Muuhulgas tegid nad sarnaseid järeldusi D´Arcy jt poolt läbiviidud uuringuga. Hu jt leidsid, et heidutus mõjub positiivselt töötajate käitumisele, kuna tajutakse rohkem rikkumisega kaasnevat vastutust, mis omakorda vähendab siseohu tekkimise riske.[125]

Kokkuvõtlikult võib alapeatükist välja tuua, et heidutavate meetmete rakendamine on teadlaste hinnangul üks võimalus parendada töötajate infoturbe alast käitumist. Heidutavate meetmete kasutamist selgitab heidutuse teooria, mis peab vajalikuks seaduserikkujaid vastutusele võtta neid karistades või hukka mõistes, eesmärgiga mõjutada seaduserikkujat ja hirmutada potentsiaalseid rikkujaid hoiduma valest käitumisest tulevikus. Teadlased on eeltoodut silmas pidades empiiriliselt uurinud heidutavaid meetmeid töötajate soovimatule infoturbe alasele käitumisele ning leidnud, et töötajate õiguskuulekust turvanõuete järgimisel on võimalik suurendada, kui anda neile teadmine neid heidutades, et turvameetmete eiramine toob kindasti kaasa vastutusele võtmise. Empiiriliste uurigute tulemustele toetudes on teadlased jõudnud seisukohale, et heidutavate meetmete rakendamine avaldub preventiivselt soovimatule infoturbe alasele käitumisele, kuna suureneb tajutav vastutus, mis omakorda toob kaasa turvanõuete järgimise tõhustumise.[126]

Eeltoodud teooria põhiseisukohti aluseks võttes on autori eesmärk uurida empiirilise uuringuga heidutavaid meetmeid (sanktsioonid ja ümberkaudsete hukkamõist) sisejulgeoleku asutuse töötajate infoturbe alase käitumise kujundamisel. Infoturbe alase kirjanduse, empiiriliste uuringute ja heidutuse teooria analüüsi tulemusena on autor seisukohal, et

[124]D'Arcy, J. and Hovav, A. Deterring internal information systems misuse: An end user perspective, *Communications of the ACM*, 50, 10, 2007, 113-117.
[125]Hu, Q., Xu, Z., Dinev, T. and Ling, H., Does Deterrence Work in Reducing Information Security Policy Abuse by Employees?, *Communication of the ACM*, 54, 6, 2011, 54-60.
[126]D'Arcy, J. and Hovav, A. Deterring internal information systems misuse: An end user perspective, *Communications of the ACM*, 50, 10, 2007, 113-117.: Hu, Q., Xu, Z., Dinev, T. and Ling, H., Does Deterrence Work in Reducing Information Security Policy Abuse by Employees?, *Communication of the ACM*, 54, 6, 2011, 54-60.; Straub, D. W., Welke, R. J., Coping with systems risk: Security planning models for management decisions making, *MIS Quart*, 22, 4, 1998, 441-469.

heidutuse teooria pakub tugeva teoreetilise aluse töötajate infoturbe alase käitumise selgitamiseks. Järgnev peatükk on magistritöö empiiriline uuring, millega autor soovib selgitada välja, millised heidutavad meetmed kujundavad töötajate hinnangul nende infoturbe alast käitumist kõige paremini.

2. EMPIIRILINE UURING

2.1 Uurimismetoodika ja valim

Infoturbe käsitleva kirjanduse, empiiriliste uuringute ja heidutuse teooria analüüsi tulemusena jõudis autor seisukohale, et heidutuse teooria pakub tugeva aluse töötajate infoturbe alase käitumise selgitamiseks. Infoturbes seisnes heidutuse eripära selles, et turvameetmed toimivad heidutava mehhanismina, suurendades infosüsteemide väärkasutamisel tajutavat vastutust ning vähendades seejuures turvaintsidentide ilmnemist.[127] Eeltoodust lähtuvalt soovib autor empiirilise uuringuga tõestada, kuivõrd mõjutavad töötajate infoturbe alast käitumist organisatsioonipoolsed heidutavad meetmed. Eeltoodu saavutamiseks on oluline teada saada, kuidas suhtuvad sisejulgeoleku töötajad heidutavate meetmete rakendamisse infoturbe alase käitumise kujundamisel.

Magistritöö eesmärgiks on selgitada välja päästeteenistujate hinnangud heidutavatele meetmetele, mis võiksid kujundada nende infoturbe alast käitumist ja saadud tulemuste põhjal töötada välja soovitusettepanekud Häirekeskusele töötajate infoturbe alase käitumise parendamiseks. Uurimistöö eesmärgi saavutamiseks, so seoste uurimiseks ja tõestamiseks[128] viis autor Häirekeskuse päästeteenistujate seas läbi kaardistava uuringu, kuna see võimaldab uurida seoseid ning neid tõestada.

Magistritöö eesmärgi saavutamiseks viis autor ajavahemikul 19.02.2014 – 05.03.2014 läbi empiirilise uuringu. Autor valis uurimisstrateegiaks kaardistava uuringu, kuna see võimaldab kogutud andmete võrdlemise tulemusena hinnata respondentide suhtumist ja käitumist[129]. Kaardistavat uuringut on võimalik kasutada nii kvantitaviise kui kvalitatiivse uuringu puhul[130]. Käesolevas magistritöös kasutab autor kvantitatiivset meetodit, mis hõlmab struktureeritud ankeetküsitluse läbiviimist.

[127]D'Arcy, J. and Hovav, A. Deterring internal information systems misuse: An end user perspective, *Communications of the ACM*, 50, 10, 2007, 113-117.
[128]Lavrakas, P., *Encyclopedia of Survey Research Methods Vol 1-2* (Thousand oaks, London, New Delhi, Singapore: Sage Publications, 2008).
[129]Lavrakas, P., *Encyclopedia of Survey Research MethodsVol 1-2* (Thousand oaks, London, New Delhi, Singapore: Sage Publications, 2008).
[130]Andres, L., *Designing & Doing Survey Research* (London Thousand Oaks, New Delhi, Singapore: SAGE Publications, 2012), p3.

Magistritöö valimi moodustas autor eesmärgistatud valimi (ingl k *purposeful sampling*) meetodil, mis põhineb kindla sihtrühma või juhtumi eesmärgipärasel, mitte juhuslikul valikul. Eesmärgistatud valim on valimi tüüp, kus respondendid on valitud olulise informatsiooni saamiseks, mida nemad on kõige sobivamad andma[131]. Töö eesmärgi saavutamiseks oli oluline, et valimi moodustaksid sisejulgeoleku töötajad, kes puutuvad kokku organisatsiooni infosüsteemidega ja neis töödeldavate tundlike isikuandmetega. Eeltoodust tulenevalt valis autor valimiks Häirekeskuse päästeteenistujad. Häirekeskuse päästeteenistujad sobisid esindama uuritavat sihtgruppi, kuna tegemist on tüüpilise sisejulgeoleku tagamisega tegeleva asutusega, kus töödeltakse igapäevaselt suurel hulgal tundliku iseloomuga isikuandmeid, teateid õigusrikkumistest ja õnnetustest. Häirekeskuse päästeteenistujate infoturbe alasest käitumisest sõltub olulisel määral eelnimetatud andmete konfidentsiaalsus ja turvalisus, samuti teiste sisejulgeoleku uurimisasutuste töö efektiivsus (näiteks Politsei- ja Piirivalveamet). Häirekeskuse töökeskkonnast tulenevatele iseärasustele tuginedes on autori hinnangul käesolev valim sobilik magistritöö eesmärgi saavutamiseks.

Kuna valimi moodustasid sisejulgeoleku tagamisega tegeleva asutuse töötajad, pöördus autor uuringu läbiviimiseks nõusoleku saamiseks Häirekeskuse juhtkonna poole. 29.01.2014 esitas autor e-kirja teel Häirekeskuse peadirektori asetäitjatele Ene Hauvmannile ja Eva Rinnele avalduse nõusoleku saamiseks uuringu läbiviimiseks Häirekeskuses. E-kirjas selgitas autor uurimistöö eesmärki, lubas tagada Häirekeskuse päästeteenistujate anonüümsuse ja konfidentsiaalsuse ning selgitas, et andmeid kogutakse statistilise analüüsi koostamiseks ja päästeteenistujate infoturbe alase käitumise parendamiseks. 31.01.2014 e-kirjaga andsid peadirektori asetäitjad nõusoleku uuringus osalemise kohta tingimusel, et ankeetküsitluses sisaldavatele küsimustele on nõusoleku andnud ka Häirekeskuse infoturbeekspert. Lähtudes eeltoodust esitas töö autor 10.02.2014 ankeetküsitluse hindamiseks Häirekeskuse infoturbeeksperdile Triin Eskole. Tuginedes Häirekeskuse töökeskkonna iseloomule, tegi Triin Esko omapoolseid soovitusi ankeetküsitluse tulemuste kasutatavuse suurendamise huvides (vt lk 38). Autor hindas Triin Esko poolt tehtud soovitused asjakohaseks ning täiendas ankeetküsitlust, et see sobituks paremini Häirekeskuse töökeskkonna iseärasustega. Samuti teatas Triin Esko autorile, et uurimistöö, selle tulemuste ja soovituste iseloomust (informatsioon Häirekeskuse töötajate infoturbe alasest käitumises) tulenevalt tuleb vastavalt avaliku teabe seaduse[132] § 35 lg 1 p-le 9 kehtestada magistritööle juurdepääsupiirang.

[131]Teddlie, C., Yu, F., Mixed Methods Sampling A Typology With Examples, *Journal of Mixed Methods Research*, 1, 1, 2007, 77-100.
[132]Avaliku teabe seadus, 15.11.2000, jõustunud 01.01.2001 – RT I 2000, 92, 597 ... RT I, 19.12.2012, 5.

Küsitluse läbiviimisel ei pöördunud autor otse vastajate poole, kuna Häirekeskuse päästeteenistujad jagunevad üle Eesti regionaalselt (Põhja, Ida, Lõuna ja Lääne keskuseks) ning samuti toimub osade päästeteenistujate tööaeg vahetustena, mistõttu oleks see raskendanud autorile päästeteenistujateni jõudmist samaaegselt. Autor koostas kaaskirja, kuhu lisas juurde ankeetküsitluse veebilehe aadressi ning saatis selle Häirekeskuse juhtkonnale palvega see edastada Häirekeskuse päästeteenistujatele. Häirekeskuse juhtkond määras eelnevalt nimetatud ülesande täitmise Häirekekuse arendusosakonna peaspetsialistile Kaili Tamm´ele. Ankeetküsitluse vastajateni jõudmine toimus Kaili Tamm´e kaasabil, kes edastas ankeetküsitluse veebilehe aadressi ja autoripoolse kaaskirja kõigile Häirekeskuse päästeteenistujatele, (kokku 207 isikule), asutusesisese e-posti aadressi kaudu. Ankeetküsitluse vastamise perioodiks oli 15 päeva, mille jooksul saatis autor 25.02.2014 Häirekeskusesse meeldetuletuse küsimustiku täitmise kohta. Meeldetuletuse edastamine päästeteenistujatele toimus Kaili Tamm´e kaasabil, kes saatis autoripoolse meeldetuletuse päästeteenistujatele asutusesisese e-posti aadressi kaudu.

Andmekogumismeetodina kasutas autor struktureeritud ankeetküsitlust. Kvantitatiivne uuring võimaldab võrrelda respondentide erinevusi ja väljendada seda arvudes. Autori hinnangul on ankeetküsitlus antud uuringu puhul sobivaim, kuna see tagab võrreldavuse ning sobib arvamuste ja hoiakute väljaselgitamiseks. Ankeetküsitluse nõrkuseks on asjaolu, et respondendid võivad vastata sellele pealiskaudselt ja nii nagu nende arvates õige on vastata, mitte nii, nagu nad ise tegelikkuses arvavad.[133] Eeltoodud riskide maandamiseks kinnitas töö autor respondentidele küsitlusele eelnenud pöördumiskirjas anonüümsuse ja konfidentsiaalsuse tagamist. Kvantitatiivse meetodi sobilikkust kinnitas lisaks infoturbe valdkonnas läbiviidud varasemate empiiriliste uuringute analüüs. Uuringute analüüsi tulemusena selgus, et kõige enam kasutust leidnud ja paremini infoturbe alast käitumist selgitav uurimismeetod on kvantitatiivne uurimismeetod, mille andmekogumismeetod tugineb situatsioonkaasuste lugemisel ja küsimustele vastamisel[134].

Käesoleva töö küsimustiku on autor ettevalmistanud kirjalike küsimuste kogumina, mille eesmärk on statistilise ülevaate koostamine ja kogutud informatsiooni võrdlemine[135]. Küsimuste koostamisel tugines autor magistritöö eesmärgile. Töö eesmärgist tulenevalt on

[133]Neuman, W. L., *Social Research Methods. Qualitative and Quantitative Approaches* (Boston: Allyn & Bacon, 2011), p 308-309.
[134]D'Arcy, J. and Hovav, A. Deterring internal information systems misuse: An end user perspective, *Communications of the ACM*, 50, 10, 2007, 113-117.
[135]Lavrakas, P., *Encyclopedia of Survey Research MethodsVol 1-2* (Thousand oaks, London, New Delhi, Singapore: Sage Publications, 2008).

autor seisukohal, et situatsioonkaasuste kasutamine arvamuse ja käitumise väljaselgitamiseks on kõige sobilikum. Situatsioonkaasuste kasutamine tagab selle, et esitatud küsimused ei ole respondentidele suunavad ja ei heiduta neid vastamast, mille tulemusena on võimalik teha objektiivseid järeldusi respondentide arvamusest ja käitumisest[136]. Selleks, et suurendada käesoleva uuringu situatsioonkaasuste valiidsust ja usaldusväärsust, lähtus autor kaasuste stsenaariumite koostamisel infoturbe valdkonnas varasemalt läbiviidud heidutuse teooriale tuginenud uuringutest ning mugavdas kaasused Häirekeskuse töökeskonnast tulenevatele iseärasustele kohasemaks[137]. Kokku koostas autor kolm situatsioonkaasust. Kuna autor lähtus kaasuste stsenaariumite koostamisel nii varasemalt läbiviidud uuringutest, kui Häirekeskuse infoturbeeksperdi Triin Esko poolt tehtud soovitustest, otsustas autor loobuda pilootuuringu läbiviimisest.

Häirekeskuse poolt tehtud soovitused olid järgnevad: a) Esialgsetes situatsioonkaasustes oli töö autor kasutanud väljendit „mõnes turvaeeskirjas". Häirekeskuses sellist väljendit kasutuses ei ole. Seetõttu võib see jääda arusaamatuks uuritavale sihtgrupile. Kuna situatsioonkaasused käsitlesid hüpoteetilisi juhtumeid ning välja toodud kaasustes ei olnud silmas peetud konkreetset eeskirja, soovitati kasutada väljendi „mõnes turvaeeskirjas" asemel väljendit „mõnes asutuse eeskirjas või juhendis"; b) Esialgsetes situatsioonkaasustes oli töö autor kasutanud väljendit „infoturbe-eeskiri"; Häirekeskuses sellist väljendit kasutuses ei ole. Turvanõuded töötajatele on Häirekeskuses kirjeldatud Töökorraldusreeglite peatüki „Turvameetmed" all. Sellest lähtuvalt soovitati kasutada väljendi „infoturbe-eeskiri" asemel väljendit „turvameetmeid sisaldav eeskiri või juhend"; c) Esialgsetes situatsioonkaasustes oli töö autor kasutanud demograafilises küsimuses väljendit „tööstaaž". Häirekeskus soovitas väljendit „tööstaaž" täiendada, kuna sellisel kujul jääb selgusetuks, kuidas või mis eesmärgil kasutatakse seda järelduste tegemisel; d) Häirekeskus soovitas viimase ettepanekuna kaaluda olemasolevatele kaasustele erinevate muude kaasuste lisamist, et järelduste ja soovituste tegemine põhineks mitmete erinevate turvanõuete järgimise/hoiakute aspekti analüüsil.

Käesoleva uuringu ankeetküsimustik sisaldas kokku 25 küsimust, millest 21 oli sisulist ja 4 demograafilist küsimust. 21 sisulist küsimust jagunes kolme situatsioonkaasuse vahel võrdselt. Iga situatsioonkaasuse kohta tuli ankeeditäitjal vastata seitsmele küsimusele.

[136]Nagin, D. S., Pogardsky, G., Integrating celerity, impulsivity and extralegal sanction threats into a model of general deterrence and evidence, *Criminology*, 39, 4, 2001, 865-891.; Harrington, S. J., The effect of codes of ethics and personal denial of responsibility on computer abuse judgments and intentions, *MIS Quart*, 20, 3, 1996, 257-258.
[137]Lavrakas, P., *Encyclopedia of Survey Research MethodsVol 1-2* (Thousand oaks, London, New Delhi, Singapore: Sage Publications, 2008).

Küsimused olid koostatud heidutuse teooriale tuginedes ning olid olemuselt sarnased kõigi situatsioonkaasuste puhul. Uuringus kasutatud situatsioonkaasuste stsenaariumid olid järgnevad: a) tööarvuti järelevalveta jätmine (andmelekke riski tekitamine) b) e-kirja manuses oleva ebaturvalise faili avamine (infoturberiski tekitamine) c) kahtlase päritoluga faili allalaadimine ja sellest mitteteavitamine (infoturberiski tekitamine). Häirekeskuse infoturbeeksperdi Triin Esko sõnul on eeltoodud situatsioonkaasuste stsenaariumid sarnased Häirekeskuse infoturberiskidega. Seega muudab see töö autori hinnangul küsimustele vastamise respondentidele kergemaks, kuna sarnaseid olukordi võib tekkida Häirekeskuse töökeskkonnas. Autor on seisukohal, et eeltoodust lähtuvalt oskavad respondendid ennast samastada stsenaariumis olevate tegelaskujudega ning vastavad küsimustele selliselt, nagu nad ise antud olukorras käituksid.

Selleks, et selgitada välja päästeteenistujate hinnangud heidutavatele meetmetele, esitas autor situatsioonkaasuste kohta küsimused, mis on seotud erinevate sanktsioonide ja ümberkaudsete hukkamõist kohaldamisega (vt Lisa 1). Ankeetküsitluse vastamiseks oli respondentidel võimalik anda hinnang 1-5 skaalal. Respondentide hinnangute väljaselgitamiseks kasutas autor järgnevaid vastusvariante - väga suureks; pigem suureks; ei suureks ega väikeseks; pigem väikeseks; väga väikeseks. Käitumist väljaselgitavate küsimuste puhul kasutas autor järgnevaid vastusvariante – jah, käituksin; pigem käituksin; pigem ei käituks; ei käituks; ei oska öelda. Ankeetküsitluse läbiviimiseks valis autor 5-punktiskaala, kuna see on ankeeditäitjatele arusaadavam, aidates parimal moel hiljem tulemusi analüüsida.

Küsitluse läbiviimiseks sisestas autor ankeetküsitluse veebiküsitluskeskkonda *LimeSurvey*. Autori hinnangul tagab veebiküsitlus andmete kogumise kiiruse ja sisestusvigade vältimise, võimaldab paindlikkust ankeedi täitmisel ning tagab respondentide anonüümsuse. Ankeetküsitluse andmete töötlemisel kasutas autor *Microsoft Office Excel* andmetöötlusprogrammi. Ankeetküsitluse tulemuste tõlgendamisel kasutas autor analüüsivat, võrdlevat ja kirjeldavat meetodit. Saadud tulemused on esitatud tabelite ja diagrammidena. Tulemuste analüüsi põhjal tegi autor üldistused ja järeldused, millel põhinesid lõppettepanekud. Empiirilise uuringu etapid on kokkuvõtvalt tooduna tabelis 1.

Tabel 1. Uurimistöö etapid

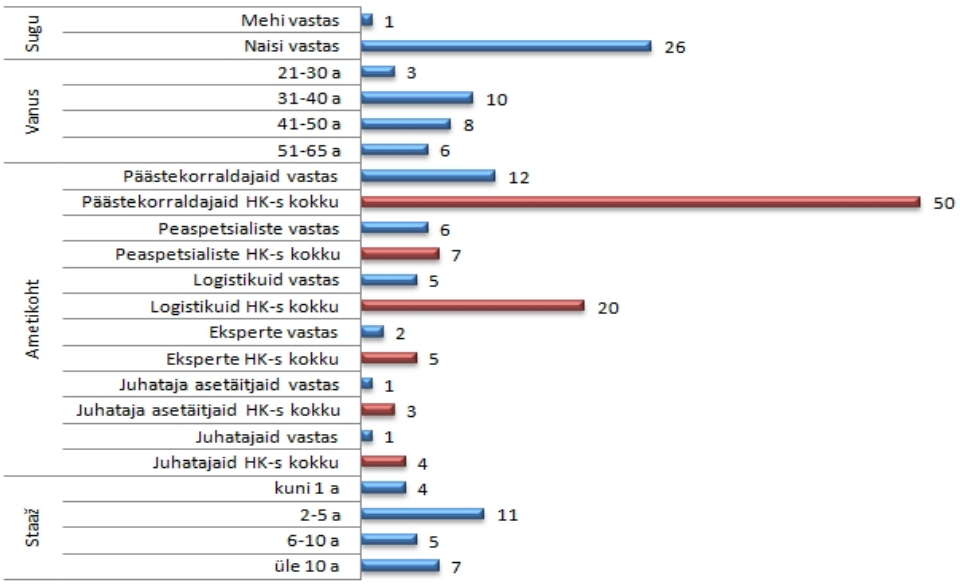
Uurimistöö etapid	**Ajavahemik**
1. Uuringu ettevalmistamine ja teoreetilise kirjanduse analüüs	01.11.2013 – 18.02.2014
2. Valimi väljaselgitamine	jaanuar 2014
3. Ankeetküsitluse koostamine tuginedes kirjanduse analüüsile ja eelnevatele	jaanuar 2014 - veebruar
4. Uuringu läbiviimine	19.02.2014 – 05.03.2014
5. Küsitluse tulemusel saadud andmete statistiline analüüsimine	05.03.2014 – 20.03.2014
6. Tulemuste analüüs ja järelduste esitamine	21.03.2014 – 05.04.2014
7. Tulemuste analüüsile tuginevate ettepanekute esitamine	05.04.2014 – 09.04.2014

2.2 Uurimistulemused ja analüüs

Käesolevas peatükis esitleb autor uuringu tulemused, nende analüüsi ning järeldused seoses põhiseisukohtadega.

Vastanute üldiseloomustus

Kogu valimist, milleks oli 207 isikut (Häirekeskuses on Päästeteenistujate ametikohti kokku 238, millest 28.02.2014 seisuga on reaalselt täidetud 207 ametikohta), vastas täielikult küsimustikule 27% ja poolikult 11%. Kuna poolikud vastused olid suures osas täidetud vaid 15%-i ulatuses (vastatud oli enamasti vaid 4-le esimesele küsimusele), otsustas autor jätta poolikult täidetud ankeedid uuringust välja ja lähtub uuringu läbiviimisel vaid täielikult täidetud ankeetidest. Vastanuid oli seega 56, kellest 95% olid naised (53 vastanut) ja 5% mehed (3 vastanut). Vastanutel tuli enda vanuse märkimiseks valida viie kategooria vahel. Vastanute vanused jagunesid järgnevalt: kuni 20a - 0; 21-30a - 7; 31-40a - 20; 41-50a - 17; 51-65a - 12. Kõige enam oli vastanute hulgas päästekorraldajaid (24 vastanut). Vastavalt teenistusstaažile jaguneti järgnevalt: kuni 1a - 8; 2-5a - 23; 6-10a - 11; üle 10a - 14.. Häirekeskuses jagunevad 28.02.2014 seisuga ametikohad vastavalt personaliosakonna väljavõttele järgnevalt: päästekorraldajaid 103, logistikuid 42, valvevahetuse juhte 20, peaspetsialiste 15, eksperte 10, juhatajaid 8, juhataja asetäitjaid 6. (vt Joonis 4)



Joonis 4. Küsimustikule vastanute sotsiaaldemograafiline jaotus esitatud protsentides

Kuna enamik vastajaid oli naissoost (95%), siis andmete analüüsimisel ei erista autor detailselt sugu seostatud vastustega. Eeltoodust tulenevalt võrdleb autor respondentide poolt antud vastuseid kahe kriteeriumi alusel, milleks on teenistusstaaž (edaspidi staaž) ja vanus. Kuna vastanud jagunesid nelja vanusegrupi vahel ebaühtlaselt, otsustas autor analüüsi paremaks läbiviimiseks kitsendada vanusegrupid kaheks - vanus 21 - 40a (27 isikut) ja vanus 41 - 65a (29 isikut). Kuna vastanud jagunesid ka staaži alusel ebaühtlaselt, otsustas autor analüüsi paremaks läbiviimiseks kitsendada nimetatud grupid kaheks - staaž kuni 5 aastat (31 isikut) ja staaž üle 5 aasta (25 isikut). Autor otsustas kitsendada nii vanuse, kui staaži gruppe seetõttu, kuna nimetatud grupid moodustaksid eraldi analüüsides liiga väikese osa üldarvust (56 isikut), et teha objektiivseid järeldusi küsitluses osalenud isikute suhtumisest ja käitumisest.

Respondentide poolt antud vastuseid kajastab autor 100%-lt, kuna kõik 56 ankeeti olid täielikult täidetud. Paraku oli vastanute hulk üldvalimiga võrreldes väike 24%, mistõttu ei võimalda see teha tugevaid üldistusi kõigi Häirekeskuses töötavate päästeteenistujate suhtes. Seega kehtivad järgnevad tulemused ja järeldused ennekõike isikute suhtes, kes osalesid uuringus. Selleks, et lugeja mõistaks paremini analüüsi käiku, esitab autor enne konkreetse kaasuse kohta tehtavat analüüsi kaasuse kirjelduse.

Respondentide poolt antud hinnangud jagunesid kõigi kaasuste küsimuste puhul 5-punktiskaalana. Kuna autorit huvitas üksnes see, kas respondendid hindavad enda käitumist situatsioonkaasuste stsenaariumile tõenäoliseks või mitte, teisendas autor respondentide

vastused analüüsi paremaks läbiviimiseks 5-punktiskaalalt 3-punktiskaalaks. Selle tulemusena on respondentide poolt antud vastused käsitletud joonistes järgnevana: (väga suureks, pigem suureks) – suureks; (pigem väikeseks, väga väikeseks) – väikeseks; ei suureks ega väikeseks; 2) (jah käituksin, pigem käituksin) – käituksin; (pigem ei käituks, ei käituks) – ei käituks; ei oska öelda. Ankeetküstiluste vastuste tulemused 5-punktiskaalana on autor toonud välja lisas 2.

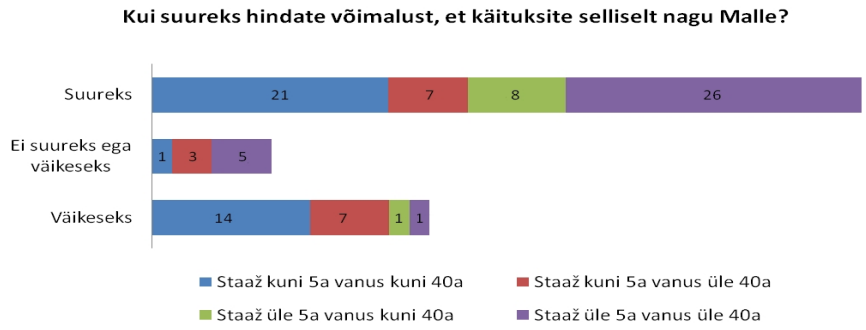
Uuringu analüüs

Kaasuses 1 toodud stsenaarium:

„*Malle teeb kontoris arvutiga tööd kui tema juurde tuleb kolleeg ja kutsub kohvipausile. Kuna Malle on hommikust saadik usinalt töötanud, otsustab ta kutse vastu võtta. Ta lahkub töölaua tagant, kuid ei lukusta arvutit. Malle ei tea täpselt, kas arvuti lukustamine on kohustusena kirjas mõnes turvameetmeid sisaldavas asutuse eeskirjas või juhendis. Samas eeldab ta, et kohvipaus võtab vähe aega ja et selle aja jooksul ei satu kedagi teist tema arvuti juurde*."

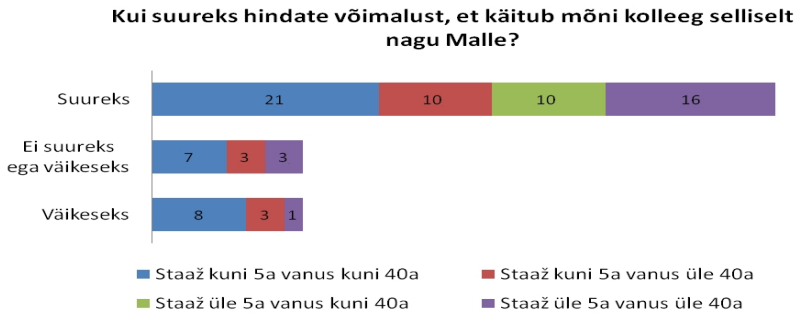
Kaasuse 1 esimese küsimuse eesmärk oli selgitada välja, kui suureks hindavad respondendid võimalust, et nad käituksid selliselt nagu Malle (vt Joonis 5). Antud küsimuse puhul ei ole autor eeldanud, et respondendid oleksid vastamisel teadlikud olnud asutuse turvameetmeid sisaldavatest eeskirjadest või juhenditest. Joonisest 5 nähtub, et 62% kõigist vastanutest hindab tõenäosust käituda sarnaselt Mallega suureks ja 23% väikeseks. 9% hindab seda võimalust ei suureks ega väikeseks. Joonisest 5 nähtub, et respondendid staažiga üle 5a on hinnanud tõenäosust, et nad käituksid Mallega sarnaselt suuremaks kui respondendid staažiga kuni 5a. Eeltoodust tulenevalt peab autor vajalikuks hinnata, kas respondentide staaž mõjutab nende hinnangut Malle käitumisele. Ehk kas respondendid staažiga kuni 5a vastavad erinevalt respondentidest staažiga üle 5a. Selle teadasaamiseks viis autor läbi Hii-ruut olulisuse testi, mille väärtuseks sai 0,029. Saadud tulemust vaatles autor olulisusnivool $p<0,05$. Saadud tulemus on väiksem, kui 0,05 ja seega statistiliselt oluline. Hii-ruut testi tulemusest järeldub, et staaž mõjutab respondentide hinnangut Malle käitumisele. Eeltoodust tulenevalt peab autor vajalikuks hinnata, kas respondentide vanus mõjutab nende hinnangut Malle käitumisele. Ehk kas respondendid vanusega kuni 40a vastavad erinevalt respondenditest vanusega üle 40a. Selle teadasaamiseks viis autor läbi Hii-ruut testi, mille väärtuseks sai 0,145. Saadud tulemust vaatles autor olulisusnivool $p<0,05$. Kuna p väärtus on suurem kui tavapärane olulisusenivoo, siis ei ole see statistiliselt oluline. Hii-ruut testi tulemusest järeldub, et respondentide vanus ei mõjuta respondentide hinnangut Malle käitumisele. Küsimus 1 vastuste põhjal võib öelda, et

respondendid staažiga üle 5a on rohkem altid käituma Mallega sarnaselt kui respondendid staažiga kuni 5a ning seejuures ei ole oluline respondentide vanus.



Joonis 5. Respondentide hinnang enda käitumisele kaasus 1 põhjal protsentides

Kaasuse 1 teise küsimuse eesmärk oli selgitada välja, kui suureks peavad respondendid võimalust, et keegi kolleegidest käitub Mallega sarnaselt. Antud küsimuse puhul ei ole autor samuti eeldanud, et respondendid oleksid vastamisel teadlikud olnud asutuse turvameetmeid sisaldavatest eeskirjadest või juhenditest. Joonisest 6 nähtub, et 56% kõigist vastanutest peab võimalust, et kolleegid käituvad sarnaselt Mallega suureks ja 12% väikeseks. 13% hindab seda võimalust ei suureks ega väikeseks. Joonisest 6 nähtub, et respondendid staažiga üle 5a on hinnanud kolleegide käitumise Mallega sarnaseks suuremaks kui respondendid staažiga kuni 5a. Eeltoodust tulenevalt peab autor vajalikuks hinnata, kas respondentide staaž mõjutab nende hinnangut kolleegide käitumisele. Selle teadasaamiseks viis autor läbi Hii-ruut olulisuse testi, mille väärtuseks sai 0,042. Saadud tulemust vaatles autor olulisusnivool $p<0,05$. Saadud tulemus on väiksem, kui 0,05 ja seega statistiliselt oluline. Hii-ruut testi tulemusest järeldub, et staaž mõjutab respondentide hinnangut kolleegide käitumisele. Eeltoodust tulenevalt peab autor vajalikuks hinnata, kas respondentide vanus mõjutab nende hinnangut kolleegide käitumisele. Ehk kas respondendid vanusega kuni 40a vastavad erinevalt respondenditest vanusega üle 40a. Selle teadasaamiseks viis autor läbi Hii-ruut olulisuse testi, mille väärtuseks sai 0,637. Saadud tulemust vaatles autor olulisusnivool $p<0,05$. Kuna p väärtus on suurem kui tavapärane olulisusenivoo, siis ei ole see statistiliselt oluline. Hii-ruut testi tulemusest järeldub, et respondentide vanus ei mõjuta respondentide hinnangut kolleegide käitumisele. Küsimus 2 vastuste põhjal võib öelda, et respondendid staažiga üle 5a hindavad kolleegide käitumise rohkem Mallega sarnaseks, kui respondendid staažiga kuni 5a ning seejuures ei ole oluline respondentide vanus.

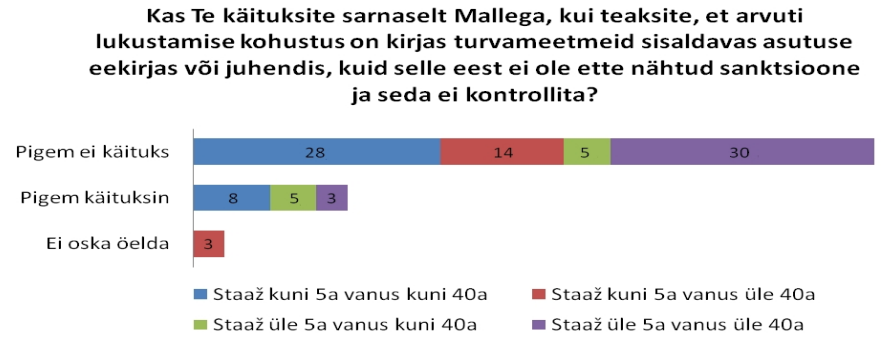


Joonis 6. Respondentide hinnang kolleegide käitumisele kaasuse 1 põhjal protsentides

Eeltoodust tulenevalt soovib autor teada, kas respondentide hinnang kolleegide käitumisele on seoses hinnanguga isiklikule käitumisele. Selle teadasaamiseks viis autor läbi Hii-ruut olulisuse testi, mille väärtuseks sai 0,344. Saadud tulemust vaatles autor olulisusnivool $p<0,05$. Kuna p väärtus on suurem kui tavapärane olulisusenivoo, siis ei ole see statistiliselt oluline. Hii-ruut testi tulemusest selgub, et respondentide hinnang enda ja kolleegide käitumisele kaasus 1 puhul ei erine. Saadud tulemusest järeldub, et respondendid hindavad kolleegide käitumist sarnaseks enda käitumisele.

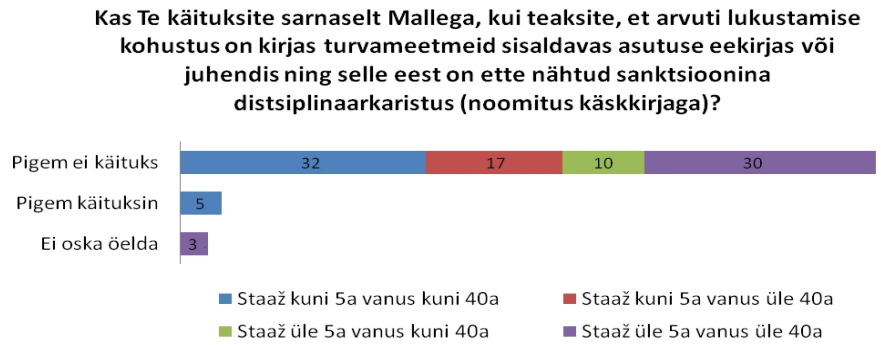
Kaasuse 1 kolmanda küsimuse eesmärk oli selgitada välja, kas respondendid käituksid Mallega sarnaselt, kui nad oleks teadlikud, et arvuti lukustamise kohustus on kirjas turvameetmeid sisaldavas asutuse eeskirjas või juhendis, kuid selle eest ei ole ettenähtud sanktsioone ja seda ei kontrollita. (vt Joonis 7) Jooniselt 7 nähtub, et 77% kõigist vastanutest ei käituks Mallega sarnaselt ja 16% käituks Mallega sarnaselt. 3% respondentidest ei oska öelda, kas nad käituksid Mallega sarnaselt. Joonisest 7 nähtub, et respondendid vanusega üle 40a on hinnanud enda käitumise Mallega vähem sarnaseks kui respondendid vanusega kuni 40a. Eeltoodust tulenevalt peab autor vajalikuks hinnata, kas respondentide vanus mõjutab nende hinnangut Malle käitumisele. Selle teadasaamiseks viis autor läbi Hii-ruut olulisuse testi, mille väärtuseks sai 0,041. Saadud tulemust vaatles autor olulisusnivool $p<0,05$. Saadud tulemus on väiksem, kui 0,05 ja seega statistiliselt oluline. Hii-ruut testi tulemusest järeldub, et respondendid vanusega üle 40a hindavad enda käitumist vastavalt küsimuses kolm esitatule õiguskuulekamaks kui respondendid vanusega kuni 40a. Eeltoodust tulenevalt peab autor vajalikuks hinnata, kas respondentide staaž mõjutab nende hinnangut Malle käitumisele. Ehk kas respondendid staažiga kuni 5a vastavad erinevalt respondenditest staažiga üle 5a. Selle teadasaamiseks viis autor läbi Hii-ruut olulisuse testi, mille väärtuseks sai 0,418. Saadud tulemust vaatles autor olulisusnivool $p<0,05$. Kuna p väärtus on suurem kui tavapärane olulisusenivoo, siis ei ole see statistiliselt oluline. Hii-ruut testi tulemusest järeldub, et

respondentide staaž ei mõjuta respondentide hinnangut Malle käitumisele. Küsimus 3 vastuste põhjal võib öelda, et respondendid vanusega üle 40a hindavad enda käitumist õiguskuulekamaks kui respondendid vanusega kuni 40a ning seejuures ei ole oluline respondentide staaž.



Joonis 7. Respondentide hinnang enda käitumisele kaasuse 1 põhjal protsentides

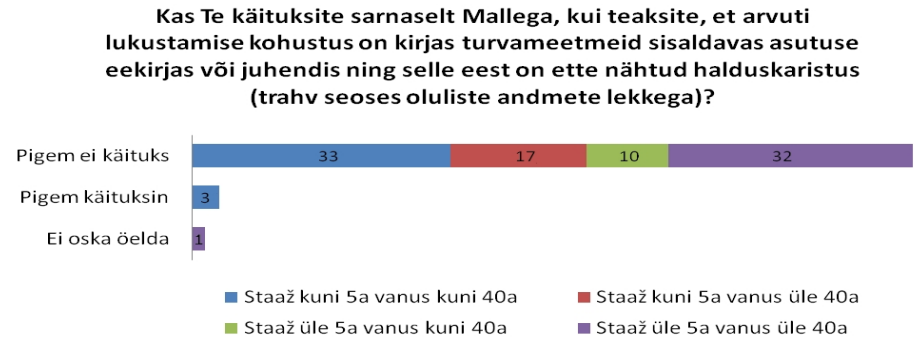
Kaasuse 1 neljanda küsimuse eesmärk oli selgitada välja, kas respondendid käituksid Mallega sarnaselt, kui nad oleks teadlikud, et arvuti lukustamise kohustus on kirjas turvameetmeid sisaldavas asutuse eeskirjas või juhendis ning selle eest on ette nähtud sanktsioonina distsiplinaarkaristus. Jooniselt 8 nähtub, et 89% kõigist vastanutest ei käituks Mallega sarnaselt ja 5% käituks Mallega sarnaselt. 3% respondentidest ei oska öelda, kas käituksid Mallega sarnaselt. Suurem osa (89%) respondentidest ei pea tõenäoliseks käituda Mallega sarnaselt ja seejuures ei ole oluline vanus ega staaž. Küll aga näeb autor joonise 8 põhjal respondentide staažiga kuni 5a ja vanusega kuni 40a seas riski, et olenemata teadlikkusest, et turvanõuete eiramine võib kaasa tuua sanktsioone, võidakse käituda siiski Mallega sarnaselt.



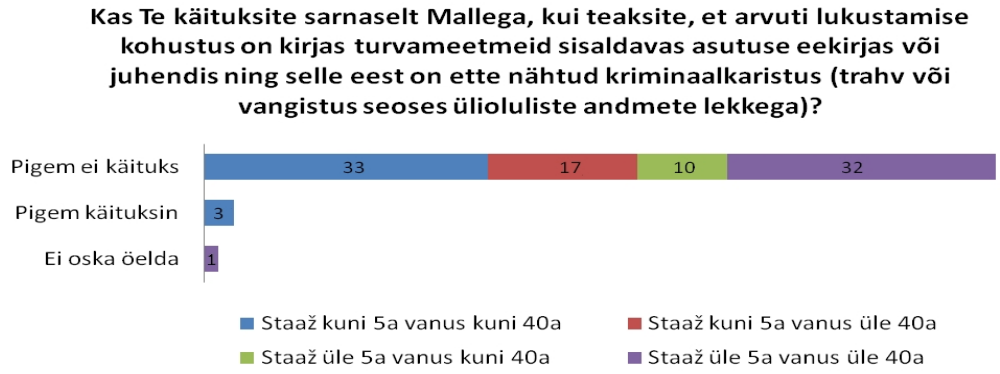
Joonis 8. Respondentide hinnang enda käitumisele kaasus 1 põhjal protsentides

Kaasuse 1 viienda küsimuse eesmärk oli selgitada välja, kas respondendid käituksid Mallega sarnaselt, kui nad oleks teadlikud, et arvuti lukustamise kohustus on kirjas turvameetmeid

sisaldavas asutuse eeskirjas või juhendis ning selle eest on ette nähtud halduskaristus seoses oluliste andmete lekkega. Jooniselt 9 nähtub, et 92% kõigist vastanutest ei käituks Mallega sarnaselt ja 3% käituks Mallega sarnaselt. 1% respondentidest ei oska öelda, kas käituksid Mallega sarnaselt. Suurem osa (92%) respondentidest ei pea tõenäoliseks käituda Mallega sarnaselt ja seejuures ei ole oluline vanus ega staaž. Eeltoodust lähtuvalt ei hakka autor eraldi seosekordajaid kontrollima.



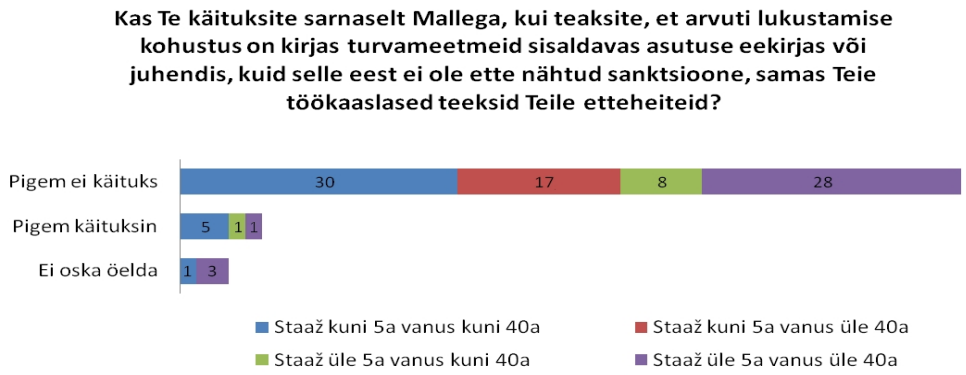
Joonis 9. Respondentide hinnang enda käitumisele kaasus 1 põhjal protsentides



Joonis 10. Respondentide hinnang enda käitumisele kaasus 1 põhjal protsentides

Kaasuse 1 kuuenda küsimuse eesmärk oli selgitada välja, kas respondendid käituksid Mallega sarnaselt, kui nad oleks teadlikud, et arvuti lukustamise kohustus on kirjas turvameetmeid sisaldavas asutuse eeskirjas või juhendis ning selle eest on ette nähtud kriminaalkaristus. Jooniselt 10 nähtub, et 92% kõigist vastanutest ei käituks Mallega sarnaselt ja 3% käituks Mallega sarnaselt. 1% respondentidest ei oska öelda, kas käituksid Mallega sarnaselt. Jooniselt 10 nähtub, et suurem osa (92%) respondentidest ei pea tõenäoliseks käituda Mallega sarnaselt ja seejuures ei ole oluline vanus ega staaž. Eeltoodust lähtuvalt ei hakka autor eraldi seosekordajaid kontrollima.

Kaasuse 1 seitsmenda küsimuse eesmärk oli selgitada välja, kas respondendid käituksid Mallega sarnaselt, kui nad oleks teadlikud, et arvuti lukustamise kohustus on kirjas turvameetmeid sisaldavas asutuse eeskirjas või juhendis, kuid selle eest ei ole ette nähtud sanktsioone, samas aga teeksid töökaaslased sellise käitumise suhtes etteheiteid. Jooniselt 11 nähtub, et 83% kõigist vastanutest ei käituks Mallega sarnaselt ja 7% käituks Mallega sarnaselt. 4% respondentidest ei oska öelda, kas käituksid Mallega sarnaselt. Suurem osa (83%) respondentidest ei pea tõenäoliseks käituda Mallega sarnaselt ja seejuures ei ole oluline vanus ega staaž. Eeltoodust lähtuvalt ei hakka autor eraldi seosekordajaid kontrollima.



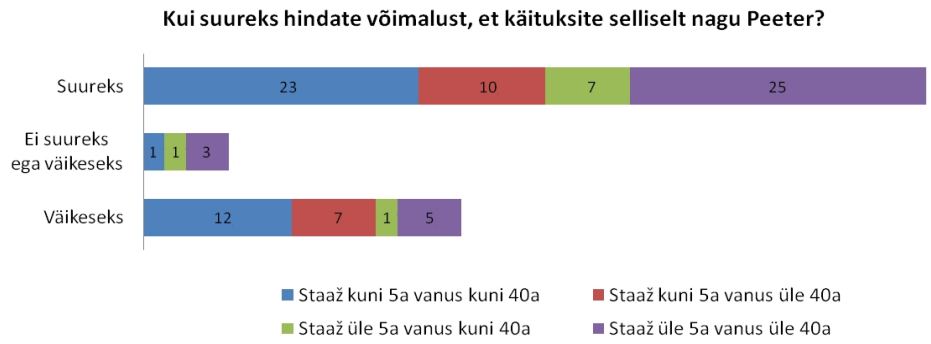
Joonis 11. Respondentide hinnang enda käitumisele kaasus 1 põhjal protsentides

Kaasuses 2 toodud stsenaarium:

„Peeter teeb kontoris arvutiga tööd, kui saab töö e-postkasti sõbralt kirja, mis sisaldab ka manust (faili). Kuna Peeter on hommikust saadik usinalt töötanud, otsustab ta sõbra kirja ja selle manuse kohe läbi lugeda. Ta teab, et e-kirjades võib sisalduda ka ohtlikke faile, kuid antud juhul pole see probleem, sest kiri on sõbralt ja Peetri arvates on tööandja arvutis kindlasti turvaprogrammid, mis kahtlased failid kahjutuks teeks. Peeter ei tea täpselt, kas erakirjade lugemise kohta on midagi kirjas turvameetmeid sisaldavas asutuse eekirjas või juhendis."

Kaasuse 2 esimese küsimuse eesmärk oli selgitada välja, kui suureks hindavad respondendid võimalust, et nad käituksid selliselt nagu Peeter (vt Joonis 12). Antud küsimuse puhul ei ole autor eeldanud, et respondendid oleksid vastamisel teadlikud olnud asutuse turvameetmeid sisaldavatest eeskirjadest või juhenditest. Joonisest 12 nähtub, et 65% kõigist vastanutest hindab tõenäosust käituda sarnaselt Peetriga suureks ja 25% väikeseks. 5% hindab seda võimalust ei suureks ega väikeseks. Joonisest 12 nähtub, et respondendid staažiga üle 5a on hinnanud tõenäosust, et nad käituksid Peetriga sarnaselt suuremaks kui respondendid staažiga kuni 5a. Eeltoodust tulenevalt peab autor vajalikuks hinnata, kas respondentide staaž mõjutab

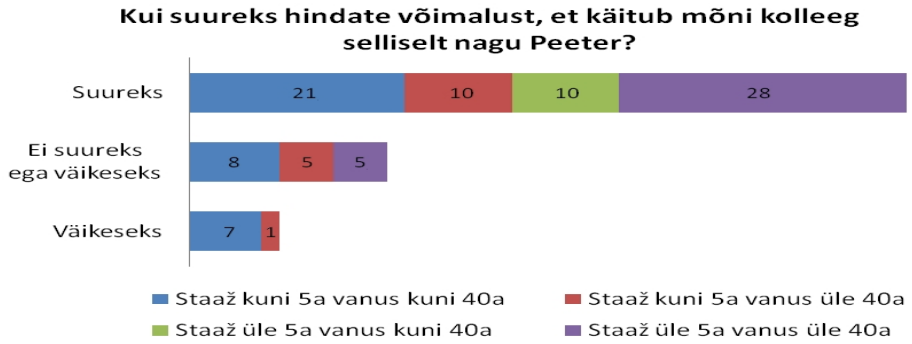
nende hinnangut Peetri käitumisele. Ehk kas respondendid staažiga kuni 5a vastavad erinevalt respondentidest staažiga üle 5a. Selle teadasaamiseks viis autor läbi Hii-ruut olulisuse testi, mille väärtuseks sai 0,157. Saadud tulemust vaatles autor olulisusnivool p<0,05. Kuna p väärtus on suurem kui tavapärane olulisusenivoo, siis ei ole see statistiliselt oluline. Hii-ruut testi tulemusest järeldub, et respondentide staaž ei mõjuta respondentide hinnangut Peetri käitumisele. Eeltoodust tulenevalt peab autor vajalikuks hinnata, kas respondentide vanus mõjutab nende hinnangut Peetri käitumisele. Ehk kas respondendid vanusega kuni 40a vastavad erinevalt respondenditest vanusega üle 40a. Selle teadasaamiseks viis autor läbi Hii-ruut olulisuse testi, mille väärtuseks sai 0,887. Saadud tulemust vaatles autor olulisusnivool p<0,05. Kuna p väärtus on suurem kui tavapärane olulisusenivoo, siis ei ole see statistiliselt oluline. Hii-ruut testi tulemusest järeldub, et respondentide vanus ei mõjuta respondentide hinnangut Peetri käitumisele. Küsimus 1 vastuste põhjal võib öelda, et vanus ega staaž ei mõjuta respondentide hinnangut Peetri käitumisele.



Joonis 12. Respondentide hinnang enda käitumisele kaasus 2 põhjal protsentides

Kaasuse 2 teise küsimuse eesmärk oli selgitada välja, kui suureks peavad respondendid võimalust, et keegi kolleegidest käitub Peetriga sarnaselt. Antud küsimuse puhul ei ole autor eeldanud, et respondendid oleksid vastamisel teadlikud olnud asutuse turvameetmeid sisaldavatest eeskirjadest või juhenditest. Joonisest 13 nähtub, et 69% kõigist vastanutest peab võimalust, et kolleegid käituvad sarnaselt Peetriga suureks ja 8% väikeseks. 18% hindab seda võimalust ei suureks ega väikeseks. Joonisest 13 nähtub, et respondendid staažiga üle 5a on hinnanud kolleegide käitumise Peetriga sarnaseks suuremaks kui respondendid staažiga kuni 5a. Eeltoodust tulenevalt peab autor vajalikuks hinnata, kas respondentide staaž mõjutab nende hinnangut kolleegide käitumisele. Selle teadasaamiseks viis autor läbi Hii-ruut olulisuse testi, mille väärtuseks sai 0,028. Saadud tulemust vaatles autor olulisusnivool p<0,05. Saadud tulemus on väiksem, kui 0,05 ja seega statistiliselt oluline. Hii-ruut testi tulemusest järeldub, et staaž mõjutab respondentide hinnangut kolleegide käitumisele.

Eeltoodust tulenevalt peab autor vajalikuks hinnata, kas respondentide vanus mõjutab nende hinnangut kolleegide käitumisele. Ehk kas respondendid vanusega kuni 40a vastavad erinevalt respondenditest vanusega üle 40a. Selle teadasaamiseks viis autor läbi Hii-ruut olulisuse testi, mille väärtuseks sai 0,315. Saadud tulemust vaatles autor olulisusnivool $p<0,05$. Kuna p väärtus on suurem kui tavapärane olulisusenivoo, siis ei ole see statistiliselt oluline. Hii-ruut testi tulemusest järeldub, et respondentide vanus ei mõjuta respondentide hinnangut kolleegide käitumisele. Küsimus 2 vastuste põhjal võib öelda, et respondendid staažiga üle 5a peab võimalust, et keegi kolleegidest käitub sarnaselt Peetriga suuremaks kui respondendid staažiga kuni 5a ning seejuures ei ole oluline respondentide vanus.

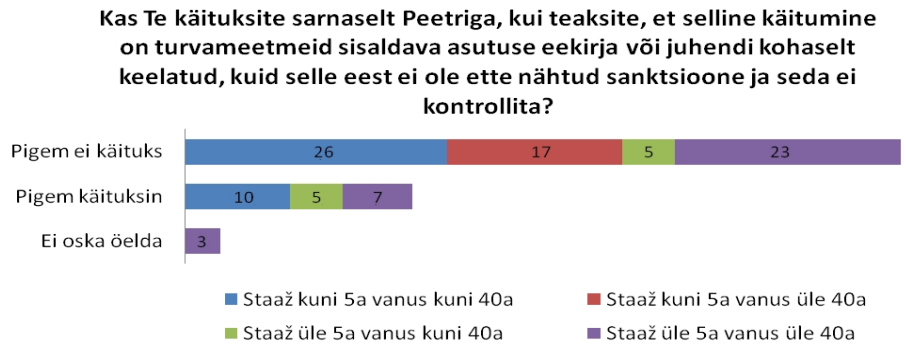


Joonis 13. Respondentide hinnang kolleegide käitumisele kaasus 2 põhjal protsentides

Eeltoodust tulenevalt soovib autor teada, kas respondentide hinnang kolleegide käitumisele on seoses hinnanguga isiklikule käitumisele. Selle teadasaamiseks viis autor läbi Hii-ruut olulisuse testi, mille väärtuseks sai 0,015. Saadud tulemust vaatles autor olulisusnivool $p<0,05$. Saadud tulemus on väiksem, kui 0,05 ja seega statistiliselt oluline. Hii-ruut testi tulemusest järeldub, et kaasus kaks puhul erineb respondentide hinnang enda ja kolleegide käitumisele. Saadud tulemuse põhjal ei ole võimalik öelda, kas respondendid hindavad kolleegide käitumise tuginedes enda käitumisele.

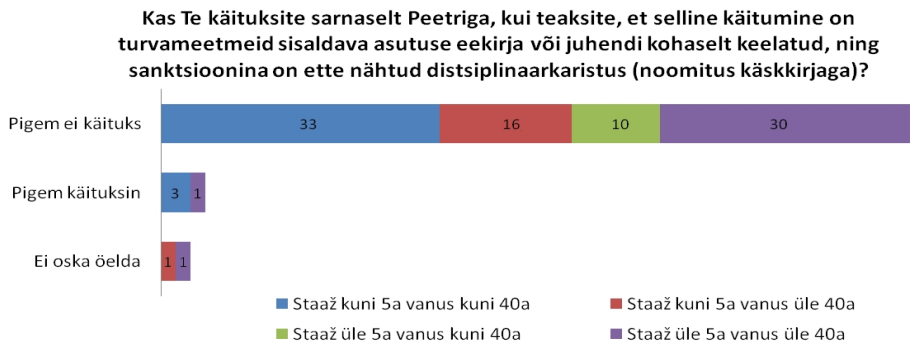
Kaasuse 2 kolmanda küsimuse eesmärk oli selgitada välja, kui tõenäoliseks hindavad respondendid enda käitumist Peetriga sarnaseks, kui respondendid on teadlikud, et kaasuses kaks kirjeldatud nõuded on kirjas turvameetmeid sisaldavas asutuse eeskirjas või juhendis, kuid selle eest ei ole ettenähtud sanktsioone ja seda ei kontrollita. Joonisest 14 nähtub, et 71% kõigist vastanutest ei käituks Peetriga sarnaselt ja 22% käituks Peetriga sarnaselt. 3% respondentidest ei oska öelda, kas nad käituksid Peetriga sarnaselt. Joonisest 14 nähtub, et respondendid staaž kuni 5a ja vanus üle 40a ei käituks selliselt nagu Peeter. Sellele järgnevad respondendid staažiga üle 5a ja vanusega üle 40a. Seevastu respondendid vanusega kuni 40a

peab Peetriga sarnast käitumist võimalikuks. Eeltoodust tulenevalt peab autor vajalikuks hinnata, kas respondentide vanus mõjutab nende hinnangut Peetri käitumisele. Selle teadasaamiseks viis autor läbi Hii-ruut olulisuse testi, mille väärtuseks sai 0,107. Saadud tulemust vaatles autor olulisusnivool $p<0,05$. Kuna p väärtus on suurem kui tavapärane olulisusenivoo, siis ei ole see statistiliselt oluline. Hii-ruut testi tulemusest järeldub, et respondentide vanus ei mõjuta respondentide hinnangut Peetri käitumisele. Eeltoodust tulenevalt peab autor vajalikuks hinnata, kas respondentide staaž mõjutab nende hinnangut Peetri käitumisele. Ehk kas respondendid staažiga kuni 5a vastavad erinevalt respondenditest staažiga üle 5a. Selle teadasaamiseks viis autor läbi Hii-ruut olulisuse testi, mille väärtuseks sai 0,000. Saadud tulemust vaatles autor olulisusnivool $p<0,05$. Saadud tulemus on väiksem, kui 0,05 ja seega statistiliselt oluline. Hii-ruut testi tulemusest järeldub, et respondentide staaž mõjutab hinnangut Peetri käitumisele. Küsimus 3 vastuste põhjal võib öelda, et respondendid staažiga kuni 5a peab enda käitumist õiguskuulekamaks kui respondendid staažiga üle 5a ja seejuures ei ole oluline respondentide vanus.



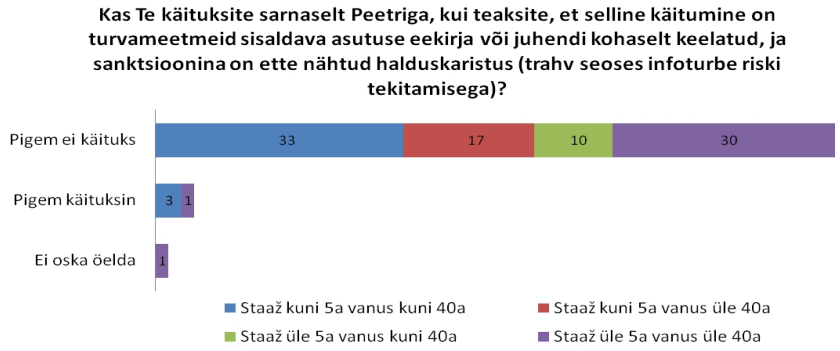
Joonis 14. Respondentide hinnang enda käitumisele kaasus 2 põhjal protsentides

Kaasuse 2 neljanda küsimuse eesmärk oli selgitada välja, kui tõenäoliseks hindavad respondendid enda käitumist Peetriga sarnaseks, kui respondendid on teadlikud, et kaasuses kaks kirjeldatud nõuded on kirjas turvameetmeid sisaldavas asutuse eeskirjas või juhendis ning selle eest on ette nähtud sanktsioonina distsiplinaarkaristus. Joonisest 15 nähtub, et 89% kõigist vastanutest ei käituks Peetriga sarnaselt ja 4% käituks Peetriga sarnaselt. 2% respondentidest ei oska öelda, kas käituksid Peetriga sarnaselt. Suurem osa (89%) respondentidest ei pea tõenäoliseks käituda Peetriga sarnaselt ja seejuures ei ole oluline vanus ega staaž. Eeltoodust tulenevalt ei hakka autor eraldi seosekordajaid kontrollima.



Joonis 15. Respondentide hinnang enda käitumisele kaasus 2 põhjal protsentides

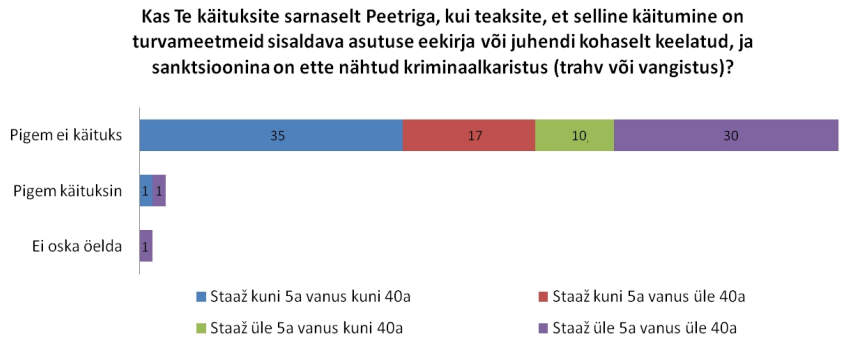
Kaasuse 2 viienda küsimuse eesmärk oli selgitada välja, kui tõenäoliseks hindavad respondendid enda käitumist Peetriga sarnaseks, kui respondendid on teadlikud, et kaasuses kaks kirjeldatud nõuded on kirjas turvameetmeid sisaldavas asutuse eeskirjas või juhendis ning selle eest on ette nähtud halduskaristus seoses oluliste andmete lekkega. Joonisest 16 nähtub, et 90% kõigist vastanutest ei käituks Peetriga sarnaselt ja 4% käituks Peetriga sarnaselt. 1% respondentidest ei oska öelda, kas käituksid Peetriga sarnaselt. Suurem osa (90%) respondentidest ei pea tõenäoliseks käituda Peetriga sarnaselt ja seejuures ei ole oluline vanus ega staaž. Eeltoodust tulenevalt ei hakka autor eraldi seosekordajaid kontrollima.



Joonis 16. Respondentide hinnang enda käitumisele kaasus 2 põhjal protsentides

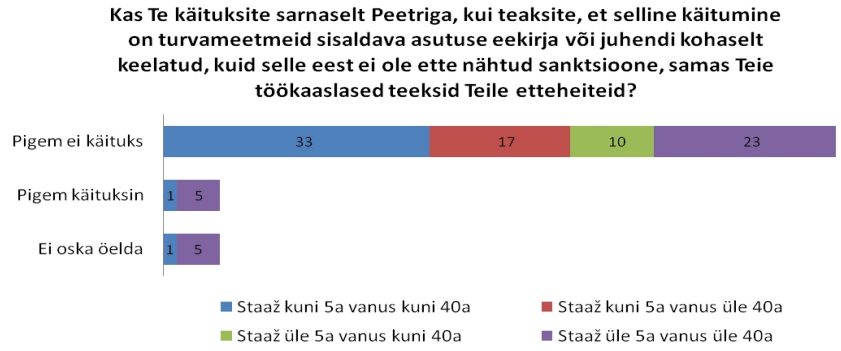
Kaasuse 2 kuuenda küsimuse eesmärk oli selgitada välja, kui tõenäoliseks hindavad respondendid enda käitumist Peetriga sarnaseks, kui respondendid on teadlikud, et et kaasuses kaks kirjeldatud nõuded on kirjas turvameetmeid sisaldavas asutuse eeskirjas või juhendis ning selle eest on ette nähtud kriminaalkaristus. Joonisest 17 nähtub, et 92% kõigist vastanutest ei käituks Peetriga sarnaselt ja 2% käituks Peetriga sarnaselt. 1% respondentidest ei oska öelda, kas käituksid Peetriga sarnaselt. Suurem osa (92%) respondentidest ei pea

tõenäoliseks käituda Peetriga sarnaselt ja seejuures ei ole oluline vanus ega staaž. Eeltoodust tulenevalt ei hakka autor eraldi seosekordajaid kontrollima.



Joonis 17. Respondentide hinnang enda käitumisele kaasus 2 põhjal protsentides

Kaasuse 2 seitsmenda küsimuse eesmärk oli selgitada välja, kui tõenäoliseks hindavad respondendid enda käitumist Peetriga sarnaseks, kui respondendid on teadlikud, et kaasuses kaks kirjeldatud nõuded on turvameetmeid sisaldavas asutuse eeskirjas või juhendis, kuid selle eest ei oleks ette nähtud sanktsioone, samas aga teeksid töökaaslased sellise käitumise suhtes etteheiteid. Joonisest 18 nähtub, et 83% kõigist vastanutest ei käituks Peetriga sarnaselt ja 6% käituks Peetriga sarnaselt. 6% respondentidest ei oska öelda, kas käituksid Peetriga sarnaselt. Suurem osa (83%) respondentidest ei pea tõenäoliseks käituda Peetriga sarnaselt ja seejuures ei ole oluline vanus ega staaž. Eeltoodust tulenevalt ei hakka autor eraldi seosekordajaid kontrollima.



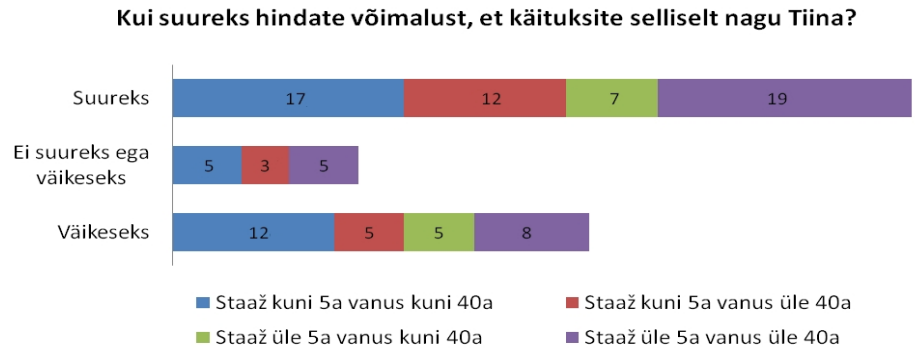
Joonis 18. Respondentide hinnang enda käitumisele kaasus 2 põhjal protsentides

Kaasuses 3 toodud stsenaarium:

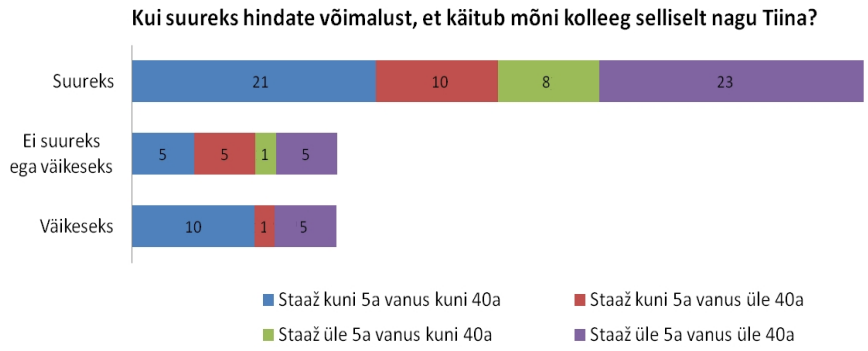
„Tiina kasutab lõunapausi ajal tööarvutit uudiste lugemiseks internetis. Ta on sirvinud erinevaid veebilehekülgi mõnda aega ning märkab ühel veebilehel huvitavat reklaami. Antud reklaamile vajutades avaneb korraga väga palju erineva sisuga veebilehekülgi. Tiina

otsustab kiirelt sulgeda kõik veebilehekülje, kuna need ei tundu talle turvalised. Veebilehekülgi sulgedes aktiveerub aga mingi faili allalaadimise protsess. Tiina katkestab allalaadimise ning sulgeb samuti kõik ülejäänud avanenud veebilehed. Ta eeldab, et suutis allalaadimise protsessi iseseisvalt katkestada ning ei räägi juhtunust kellelegi. Tiina ei tea täpselt, kas selliste juhtumite puhuks on turvameetmeid sisaldavas asutuse eeskirjas või juhendis mingeid instruktsioone."

Kaasuse 3 esimese küsimuse eesmärk oli selgitada välja, kui tõenäoliseks hindavad respondendid enda käitumist Tiinaga sarnaseks. Antud küsimuse puhul ei ole autor eeldanud, et respondendid oleksid vastamisel teadlikud olnud asutuse turvameetmeid sisaldavatest eeskirjadest või juhenditest. (vt Joonis 19) Joonisest 19 nähtub, et 55% kõigist respondentidest on hinnanud tõenäosust, et nad käituksid Tiinaga sarnaselt suureks ja 30% väikeseks. 13% hindab seda võimalust ei suureks ega väikeseks. Joonis 19 põhjal ei ole võimalik protsentide öelda, kas vanus või staaž võib mõjutada respondentide hinnangut Tiina käitumisele. Eeltoodust tulenevalt peab autor vajalikuks hinnata, kas respondentide staaž ja vanus võib mõjutada nende hinnangut Tiina käitumisele. Ehk kas respondendid staažiga kuni 5a vastavad erinevalt respondentidest staažiga üle 5a ja kas respondendid vanusega kuni 40a vastavad erinevalt respondentidest vanusega üle 40a. Nii staaži kui vanuse erinevuste teadasaamiseks viis autor läbi Hii-ruut olulisuse testi, mille väärtuseks sai vastavalt 0,889 ja 0,711. Saadud tulemusi vaatles autor olulisusnivool $p<0,05$. Kuna p väärtused on suuremad kui tavapärane olulisusenivoo, siis ei ole need statistiliselt olulised. Hii-ruut olulisuse testi tulemusest järeldub, et respondentide staaž ja vanus ei mõjuta respondentide hinnangut Tiina käitumisele.



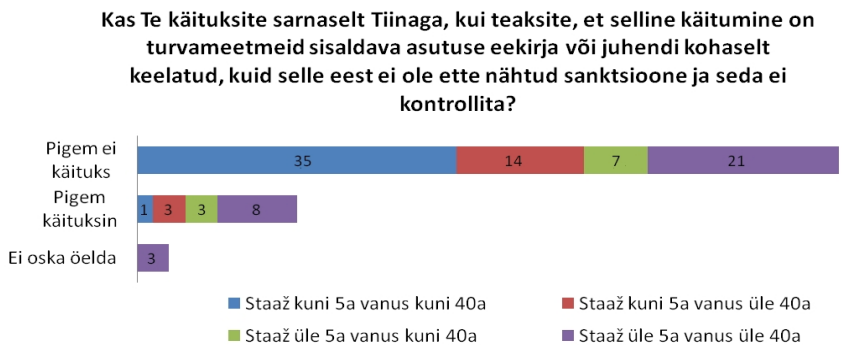
Joonis 19. Respondentide hinnang enda käitumisele kaasus 3 põhjal protsentides



Joonis 20. Respondentide hinnang kolleegide käitumisele kaasus 3 põhjal protsentides

Kaasuse 3 teise küsimuse eesmärk oli selgitada välja, kui tõenäoliseks hindavad respondendid kolleegide käitumist Tiinaga sarnaseks. Antud küsimuse puhul ei ole autor eeldanud, et respondendid oleksid vastamisel teadlikud olnud asutuse turvameetmeid sisaldavatest eeskirjadest või juhenditest. Joonisest 20 nähtub, et 62% kõigist vastanutest peab võimalust, et kolleegid käituvad sarnaselt Tiinaga suureks ja 16% väikeseks. 16% hindab seda võimalust ei suureks ega väikeseks. Eeltoodust tulenevalt peab autor vajalikuks hinnata, kas respondentide vanus mõjutab hinnangut kolleegide käitumisele. Selle teadasaamiseks viis autor läbi Hii-ruut olulisuse testi, mille väärtuseks sai 0,485. Saadud tulemust vaadeldi olulisusnivool $p<0,05$. Kuna p väärtus on suurem kui tavapärane olulisusenivoo, siis ei ole see statistiliselt oluline. Hii-ruut testi tulemusest järeldub, et vanus ei mõjuta respondentide hinnangut kolleegide käitumisele. Eeltoodust tulenevalt peab autor vajalikuks hinnata, kas respondentide staaž mõjutab nende hinnangut kolleegide käitumisele. Ehk kas respondendid staažiga kuni 5a vastavad erinevalt respondenditest staažiga üle 5a. Selle teadasaamiseks viis autor läbi Hii-ruut olulisuse testi, mille väärtuseks sai 0,503. Saadud tulemust vaadeldi olulisusnivool $p<0,05$. Kuna p väärtus on suurem kui tavapärane olulisusenivoo, siis ei ole see statistiliselt oluline. Hii-ruut testi tulemusest järeldub, et respondentide vanus ei mõjuta respondentide hinnangut kolleegide käitumisele. Küsimus 2 vastuste põhjal võib öelda, et respondentide staaž ja vanus ei mõjuta respondentide hinnangut kolleegide käitumisele.

Eeltoodust tulenevalt soovib autor teada, kas respondentide hinnang kolleegide käitumisele on seoses hinnanguga isiklikule käitumisele. Selle teadasaamiseks viis autor läbi Hii-ruut olulisuse testi, mille väärtuseks sai 0,398. Saadud tulemust vaadeldi olulisusnivool $p<0,05$. Kuna p väärtus on suurem kui tavapärane olulisusenivoo, siis ei ole see statistiliselt oluline. Hii-ruut testi tulemusest selgub, et respondentide hinnang enda ja kolleegide käitumisele ei erine. Saadud tulemusest võib järeldada, et respondendid hindavad kolleegide käitumist sarnaseks enda käitumisele.

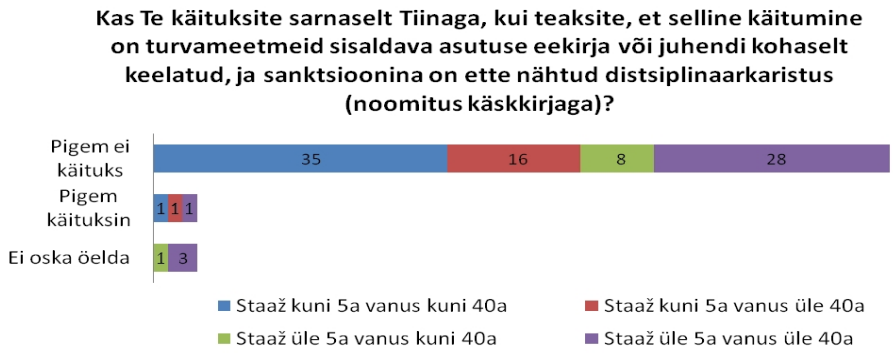


Joonis 21. Respondentide hinnang enda käitumisele kaasus 3 põhjal protsentides

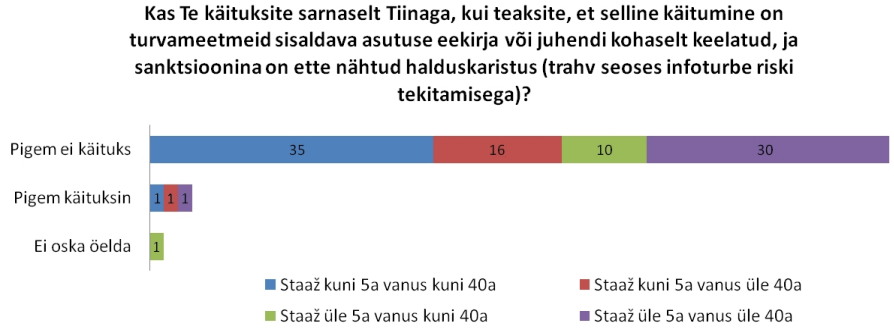
Kaasuse 3 kolmanda küsimuse eesmärk oli selgitada välja, kui tõenäoliseks hindavad respondendid enda käitumist Tiinaga sarnaseks, kui respondendid on teadlikud, et kaasuses kolm kirjeldatud nõuded on kirjas turvameetmeid sisaldavas asutuse eeskirjas või juhendis, kuid selle eest ei ole ettenähtud sanktsioone ja seda ei kontrollita. Joonisest 21 nähtub, et 77% kõigist vastanutest ei käituks Tiinaga sarnaselt ja 15% käituks Tiinaga sarnaselt. 3% respondentidest ei oska öelda, kas nad käituksid Tiinaga sarnaselt. Joonisest 21 nähtub, et respondendid staažiga kuni 5a on hinnanud enda käitumise Tiinaga sarnaselt väiksemaks kui respondendid staažiga üle 5a. Eeltoodust tulenevalt peab autor vajalikuks hinnata, kas respondentide staaž mõjutab hinnangut Tiina käitumisele. Selle teadasaamiseks viis autor läbi Hii-ruut olulisuse testi, mille väärtuseks sai 0,042. Saadud tulemust vaatles autor olulisusnivool $p<0,05$. Saadud tulemus on väiksem, kui 0,05 ja seega statistiliselt oluline. Hii-ruut testi tulemusest järeldub, et respondendid staažiga kuni 5a on hinnanud enda käitumise õiguskuulekamaks kui respondendid staažiga üle 5a. Eeltoodust tulenevalt peab autor vajalikuks hinnata, kas respondentide vanus mõjutab nende hinnangut Tiina käitumisele. Ehk kas respondendid vanusega kuni 40a vastavad erinevalt respondenditest vanusega üle 40a. Selle teadasaamiseks viis autor läbi Hii-ruut olulisuse testi, mille väärtuseks sai 0,107. Saadud tulemust vaatles autor olulisusnivool $p<0,05$. Kuna p väärtus on suurem kui tavapärane olulisusenivoo, siis ei ole see statistiliselt oluline. Hii-ruut testi tulemusest järeldub, et respondentide vanus ei mõjuta respondentide hinnangut Tiina käitumisele. Küsimus 3 vastuste põhjal võib öelda, et respondendid staažiga üle 5a peab enda käitumist õiguskuulekamaks kui respondendid staažiga kuni 5a ja seejuures hindasid enda käitumise tõenäosuse õiguskuulekamaks kui respondendid staažiga kuni 5a ja seejuures ei ole oluline respondentide vanus.

Kaasuse 3 neljanda küsimuse eesmärk oli selgitada välja, kui tõenäoliseks hindavad respondendid enda käitumist Tiinaga sarnaseks, kui respondendid on teadlikud, et kaasuses

kolm kirjeldatud nõuded on kirjas turvameetmeid sisaldavas asutuse eeskirjas või juhendis ning selle eest on ette nähtud sanktsioonina distsiplinaarkaristus. Joonisest 22 nähtub, et 87% kõigist vastanutest ei käituks Tiinaga sarnaselt ja 3% käituks Tiinaga sarnaselt. 4% respondentidest ei oska öelda, kas käituksid Tiinaga sarnaselt. Suurem osa (87%) respondentidest ei pea tõenäoliseks käituda Tiinaga sarnaselt ja seejuures ei ole oluline vanus ega staaž. Eeltoodust tulenevalt ei hakka autor eraldi seosekordajaid kontrollima.



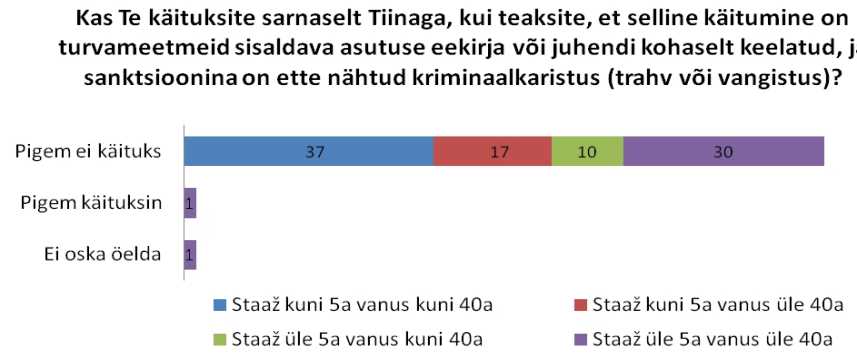
Joonis 22. Respondentide hinnang enda käitumisele kaasus 3 põhjal protsentides



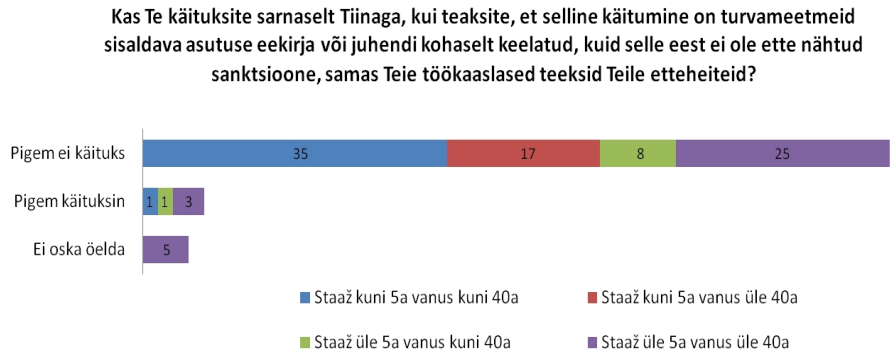
Joonis 23. Respondentide hinnang enda käitumisele kaasus 3 põhjal protsentides

Kaasuses 3 viienda küsimuse eesmärk oli selgitada välja, kui tõenäoliseks hindavad respondendid enda käitumist Tiinaga sarnaseks, kui respondendid on teadlikud, et kaasuses 3 kirjeldatud nõuded on kirjas turvameetmeid sisaldavas asutuse eeskirjas või juhendis ning selle eest on ette nähtud halduskaristus seoses oluliste andmete lekkega. Joonisest 23 nähtub, et 91% kõigist vastanutest ei käituks Tiinaga sarnaselt ja 3% käituks Tiinaga sarnaselt. 1% respondentidest ei oska öelda, kas käituksid Tiinaga sarnaselt. Suurem osa (91%) respondentidest ei pea tõenäoliseks käituda Tiinaga sarnaselt ja seejuures ei ole oluline vanus ega staaž. Eeltoodust tulenevalt ei hakka autor eraldi seosekordajaid kontrollima.

Kaasuse 3 kuuenda küsimuse eesmärk oli selgitada välja, kui tõenäoliseks hindavad respondendid enda käitumist Tiinaga sarnaseks, kui respondendid on teadlikud, et kaasuses kolm kirjeldatud nõuded on kirjas turvameetmeid sisaldavas asutuse eeskirjas või juhendis ning selle eest on ette nähtud kriminaalkaristus. Joonisest 24 nähtub, et 94% kõigist vastanutest ei käituks Tiinaga sarnaselt ja 1% käituks Tiinaga sarnaselt. 1% respondentidest ei oska öelda, kas käituksid Tiinaga sarnaselt. Suurem osa (94%) respondentidest ei pea tõenäoliseks käituda Tiinaga sarnaselt ja seejuures ei ole oluline vanus ega staaž. Eeltoodust tulenevalt ei hakka autor eraldi seosekordajaid kontrollima.



Joonis 24. Respondentide hinnang enda käitumisele kaasus 3 põhjal protsentides



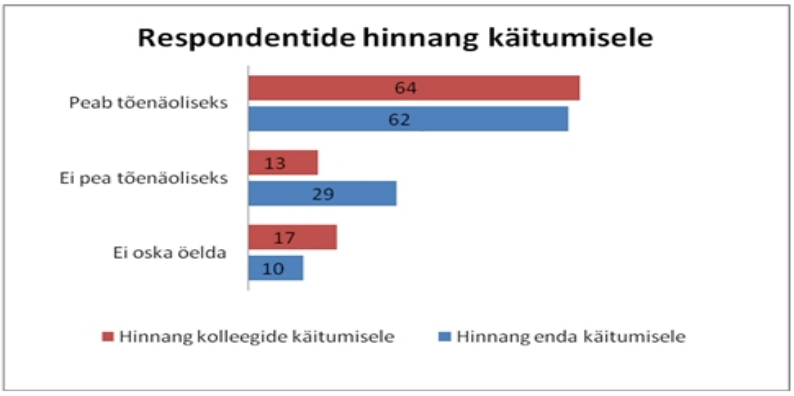
Joonis 25. Respondentide hinnang enda käitumisele kaasus 3 põhjal protsentides

Kaasuse 3 seitsmenda küsimuse eesmärk oli selgitada välja, kui tõenäoliseks hindavad respondendid enda käitumist Tiinaga sarnaseks, kui respondendid on teadlikud, et kaasuses kolm kirjeldatud nõuded on turvameetmeid sisaldavas asutuse eeskirjas või juhendis, kuid selle eest ei oleks ette nähtud sanktsioone, samas aga teeksid töökaaslased sellise käitumise suhtes etteheiteid. Joonisest 25 nähtub, et 85% kõigist vastanutest ei käituks Tiinaga sarnaselt ja 5% käituks Tiinaga sarnaselt. 5% respondentidest ei oska öelda, kas käituksid Tiinaga sarnaselt. Suurem osa (85%) respondentidest ei pea tõenäoliseks käituda Tiinaga sarnaselt ja

seejuures ei ole oluline vanus ega staaž. Eeltoodust tulenevalt ei hakka autor eraldi seosekordajaid kontrollima.

Analüüsi kokkuvõte

Empiirilisest uuringust selgub, et keskmiselt 62% kõigist respondentidest hindab tõenäoliseks ja 29% mitte, et nad käituksid sarnaselt hüpoteetilistes situatsioonkaasustes olnud tegelaskujudega. Keskmiselt 10% respondentidest ei osanud öelda, kas võiksid käituda sarnaselt tegelaskujudega või mitte. Respondentide hinnang kolleegide käitumisele oli järgnev: keskmiselt 64% hindas tõenäosust, et kolleegide käituksid sarnaselt tegelaskujudega, suureks, 13% väikeseks ning 17% ei osanud öelda, kas kolleegid võiksid käituda tegelaskujudega sarnaselt või mitte. Kui võrrelda protsentuaalselt respondentide hinnangut enda ja kolleegide käitumisele, siis väga suurt erinevust ei nähtu (vt Joonis 26).



Joonis 26. Respondentide hinnang enda ja kolleegide käitumisele protsentides (keskmine)

Saamaks kinnitust, kas respondentide hinnang enda ja kolleegide käitumisele võib olla sarnane, selgitas autor välja Hii-ruut testide olulisuse nivood (vt Tabel 2).

Tabel 2. Respondentide hinnang kolleegide käitumisele tuginedes enda käitumisele

Hinnang kolleegide käitumisele tuginedes enda käitumisele	Hii-ruut olulisuse nivoo
Kaasus 1- Tööarvuti järelevalveta jätmine (andmelekke riski tekitamine)	0, 344
Kaasus 2 - E-kirja manuses oleva ebaturvalise faili avamine (infoturberiski tekitamine)	0,015
Kaasus 3- Kahtlase päritoluga faili allalaadimine ja sellest mitteteavitamine (infoturberiski tekitamine)	0,398

*test oluline nivool $p<0,05$

Hii-ruut olulisuse nivoode tulemustest selgub, et kaasuse 1 ja 3 puhul hindasid respondendid kolleegide käitumise sarnaseks enda käitumisega. Kaasuse 2 puhul erines respondentide

hinnang enda ja kolleegide käitumisele. Kuigi kahe kaasuse puhul nähtub seose olemasolu, et respondendid hindasid kolleegide käitumise tuginedes enda käitumisele, ei võimalda käesolev uuring paraku kindlalt väita, et see alati kehtiks, kuna kaasuse 2 puhul erines respondentide hinnang enda ja kolleegide käitumisele. Eeltoodust tulenevalt on autor seisukohal, et respondendid ei hinda kolleegide käitumist alati lähtudes enda käitumisest.

Vastuste suhtelist erinemist võib seletada sellega, et vastastes situatsioonkaasuse kohta esimesele küsimusele (iseenda käitumise kohta) asetasid respondendid end tegelaskuju asemele ning vastasid lähtudes olemasolevast teabest ja oma väärtushinnangutest nii nagu nad peavad ratsionaalseks ja turvaliseks. Vastates teisele küsimusele (kolleegide käitumise kohta) arvestasid respondendid konkreetselt oma töökoha (so Häirekeskuse) keskkonda ja hindasid käitumist oma kollektiivis. Seega peegeldab vastus esimesele küsimusele enam töötajate arvutialase turvalisuse teadlikkust ja teisele küsimusele enam tegelikku töötajate käitumist Häirekeskuses. Jooniselt 26 nähtub ilmekalt respondentide hinnang enda ja kolleegide käitumisele.

Tabel 3. Respondentide hinnangute erisused vanuse järgi

Vastanute hinnang vanuse järgi	**Hii-ruut olulisuse nivoo**
1. Kui suureks hindate võimalust, et käituksite selliselt nagu Malle?	0,145
2. Kui suureks hindate võimalust, et käitub mõni kolleeg selliselt nagu Malle?	0,637
3. Kas te käituksite sarnaselt Mallega, kui teaksite, et arvuti lukustamise kohustus on kirjas turvameetmeid sisaldavas asutuse eeskirjas või juhendis, kuid selle eest ei ole ettenähtud sanktsioone ja seda ei kontrollita?	0,041
4. Kui suureks hindate võimalust, et käituksite selliselt nagu Peeter?	0,887
5. Kui suureks hindate võimalust, et käitub mõni kolleeg selliselt nagu Peeter?	0,315
6. Kas te käituksite sarnaselt Peetriga, kui teaksite, et selline käitumine on turvameetmeid sisaldava asutuse eeskirja või juhendi kohaselt keelatud, kuid selle eest ei ole ettenähtud sanktsioone ja seda ei kontrollita?	0,107
7. Kui suureks hindate võimalust, et käituksite selliselt nagu Tiina?	0,711
8. Kui suureks hindate võimalust, et käitub mõni kolleeg selliselt nagu Tiina?	0,485
9. Kas te käituksite sarnaselt Tiinaga, kui teaksite, et selline käitumine on turvameetmeid sisaldava asutuse eeskirja või juhendi kohaselt keelatud, kuid selle eest ei ole ettenähtud sanktsioone ja seda ei kontrollita?	0,107

*test oluline nivool $p<0,05$

Analüüsi käigus võrdles autor respondentide poolt antud vastuseid vanuse ja staaži alusel (Vt Tabel 3 ja Tabel 4). Tabelist 3 nähtub, et suurem osa Hii-ruut testide tulemustest (ca 91%) ei olnud statistiliselt olulised ning seega ei saa väita, et respondendid erineksid vastamisel vanuse järgi. Kuigi esimese kaasuse kolmanda küsimuse tulemus oli statistiliselt oluline, mille tulemusena jõudis autor järelduseni, et respondentide käitumist mõjutab respondentide vanus, ei ole see lõpptulemusega võrreldes statistiliselt oluline. Eeltoodust tulenevalt on autor

seisukohal, et respondentide hinnangut enda ja kolleegide käitumisele ei mõjuta respondentide vanus.

Tabel 4. Respondentide hinnangute erisused staaži järgi

Vastanute hinnang staaži järgi	Hii-ruut olulisuse nivoo
1. Kui suureks hindate võimalust, et käituksite selliselt nagu Malle?	0,029
2. Kui suureks hindate võimalust, et käitub mõni kolleeg selliselt nagu Malle?	0,042
3. Kas te käituksite sarnaselt Mallega, kui teaksite, et arvuti lukustamise kohustus on kirjas turvameetmeid sisaldavas asutuse eeskirjas või juhendis, kuid selle eest ei ole ettenähtud sanktsioone ja seda ei kontrollita?	0,418
4. Kui suureks hindate võimalust, et käituksite selliselt nagu Peeter?	0,157
5. Kui suureks hindate võimalust, et käitub mõni kolleeg selliselt nagu Peeter?	0,028
6. Kas te käituksite sarnaselt Peetriga, kui teaksite, et selline käitumine on turvameetmeid sisaldava asutuse eeskirja või juhendi kohaselt keelatud, kuid selle eest ei ole ettenähtud sanktsioone ja seda ei kontrollita?	0,000
7. Kui suureks hindate võimalust, et käituksite selliselt nagu Tiina?	0,889
8. Kui suureks hindate võimalust, et käitub mõni kolleeg selliselt nagu Tiina?	0,503
9. Kas te käituksite sarnaselt Tiinaga, kui teaksite, et selline käitumine on turvameetmeid sisaldava asutuse eeskirja või juhendi kohaselt keelatud, kuid selle eest ei ole ettenähtud sanktsioone ja seda ei kontrollita?	0,042

*test oluline nivool $p<0,05$

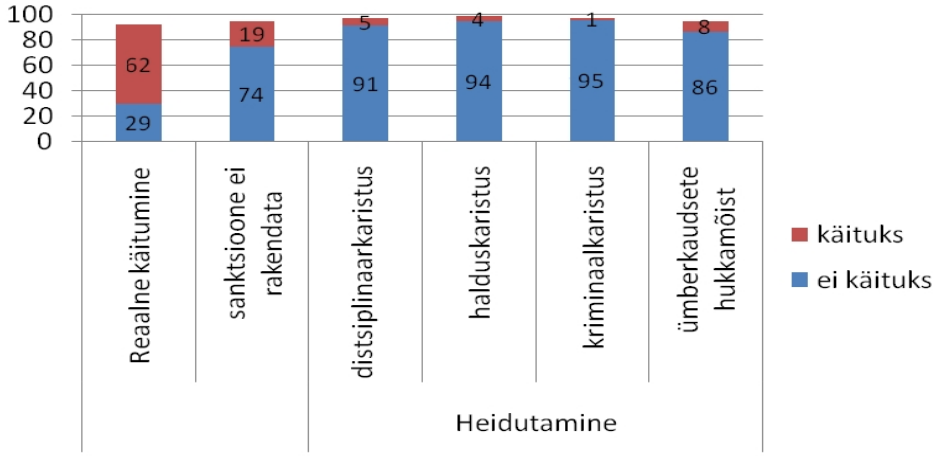
Uuringu tulemustest selgub, et vanusega võrreldes avaldas respondentide käitumisele rohkem mõju respondentide staaž. Tabelist 4 nähtub, et kaasuse 1 puhul hindasid respondendid staažiga üle 5a enda käitumise tegelaskujudele sarnasemaks võrreldes respondentidega staažiga kuni 5a. Kaasuste 2 ja 3 puhul ei avaldanud staaž respondentide käitumisele olulist mõju. Seevastu hinnangut kolleegide käitumisele mõjutas staaž rohkem. Kaasuste 1 ja 2 puhul hindasid respondendid staažiga üle 5a tõenäolisemaks kolleegide käitumist tegelaskujudega sarnaselt võrreldes respondentidega staažiga kuni 5a. Kaasuse 3 puhul seda väita ei saa, kuna respondentide hinnang kolleegide käitumisele ei olnud staaži järgi statistiliselt oluline. Respondentide hinnang enda käitumisele, kui stsenaariumites esitatud käitumine oleks vastuolus asutuse turvameetmeid sisaldava eeskirja või juhendiga (kui sellele ei järgneks sanktsioone ja seda ei kontrollita) oli järgnev. Kaasuse 1 puhul ei mõjutanud staaž respondentide käitumist. Kaasuste 2 ja 3 puhul mõjutas staaž respondentide käitumist. Respondendid staažiga üle 5a hindasid enda käitumise tegelaskujudega sarnasemaks kui respondendid staažiga kuni 5a. Kuigi staaž mõjutas vanusega võrreldes oluliselt rohkem respondenide käitumist ja hinnangut kolleegide käitumisele, ei ole uuringu tulemuste põhjal võimalik kindlalt öelda, et staaž mõjutaks alati respondentide käitumist. Autoripoolne järeldus tuleneb asjaolust, et teatud juhtudel ei olnud respondentide staaž statiliselt oluline (küsimused 3, 4, 7 ja 8). Eeltoodust tulenevalt on autor seisukohal, et respondentide staaži ei saa käsitleda olulise mõjutegurina respondentide käitumisele.

Vanuse ja staaži tulemust võib seletada sellega, et Häirekeskuse töökeskkond rajaneb suures osas töösaalide põhimõttel, kus töötatakse lähestikku olles. Kuna inimesed kujundavad enda käitumise organisatsiooni tulles enamasti kaaskolleegide käitumise eeskujul, millele viitas autor ka teooria teises peatükis käitumist mõjutavate tegurite all, võib vanus seetõttu ollagi käitumist niiväga mitte mõjutav tegur töökeskkonnas, kus inimesed töötavad lähestikku olles. Saadud tulemuste põhjal võib öelda, et lühema staažiga töötajad tuginevad vastamisel staažikamate töötajate käitumisele (niiöelda juba tavaks saanud käitumisele asutuses), mis selgitaks autori valitud vanuse kriteeriumi ebaolulisust vastanute käitumisele. Suurem osa vastanutest märkis enda ametikohaks päästekorraldaja, kelle põhiline tööülesannete täitmine leiab aset töösaalis, mis põhjendab samuti eelneva järelduse relevantsust. Teine põhjus võib olla see, et nooremad töötajad teavad rohkem arvutikasutamisega seonduvaid riske, mistõttu hindasid enda käitumise tegelaskujudele vähem sarnaseks kui vanemad töötajad, kuid mis ei nähtu analüüsi statistilisest võrdlusest väga olulise erisusena, kuna leidus ka nooremaid töötajaid, kes hindasid enda käitumise tegelaskujudele sarnaseks, mistõttu ei saa vanust käsitleda siiski väga olulise tegurina käitumisele. Staažiga seotud erisusi võib selgitada ka sellega, et pikema staažiga töötajad on enda teenistuse ajal kohanud tegelaskujudega sarnast käitumist kolleegide seas rohkem kui lühema staažiga töötajad ning seetõttu hindavad nemad kolleegide vale käitumise tõenäosust ka suuremaks.

Uuringu peamine eesmärk oli selgitada välja päästeteenistujate hinnangud heidutavatele meetmetele, mis võiksid kujundada nende infoturbe alast käitumist. Eesmärgi saavutamiseks küsis autor respondentidelt heidutavate meetmete rakendamisega seonduvaid küsimusi. Esiteks küsis autor, kuidas hindaksid respondendid enda käitumist, kui nad on teadlikud, et turvanõuete järgimist ei kontrollita ja sellele ei järgne vastutust. Teiseks küsis autor, kuidas hindaksid respondendid enda käitumist, kui nad on teadlikud, et turvanõuete järgimist kontrollitakse ja sellele võib järgneda reaalne vastutus - distsiplinaar-, haldus, kriminaalkaristus või ümberkaudsete hukkamõist. Saadud tulemusi võrdles autor omavahel. (vt Joonis 27) Uuringu käigus selgus, et respondendite suhtumisele heidutavatesse meetmetesse ei avaldanud olulist mõju respondentide staaž, ega vanus. Ehk kõik vastanud suhtusid neisse meetmetesse suures osas ühtemoodi.

Selleks, et selgitada välja kuivõrd kujundab heidutamine infoturbe alast käitumist, pidas autor vajalikuks juhtida respondentide tähelepanu asutuse turvameetmeid sisaldavate eeskirjadele ja juhenditele, mille tulemusena muutus respondentide hinnang tegelaskujude käitumisele. Respondentide tähelepanu juhtimine asutuse turvameetmeid sisaldavatele eeskirjadele või

juhenditele (eelduse lisamine, et situatsioonkaasuses esitatud käitumine on vastuolus turvanormidega) korrigeeris respondentide hinnangut tegelaskujude käitumisele kesmiselt 45%. Eeltoodust tulenevalt on autor seisukohal, et kui tõsta töötajate teadlikkust turvanõuetest, korrigeerivad töötajad oma suhtumist turvameetmete järgimisse ka ilma heidutust kohaldamata. Saadud tulemus kinnitab heidutuse teoreetiliselt käsitlusest tulnevat põhipunkti, et töötajate teadlikkus turvameetmete olemasolust parandab töötajate suhtumist turbenõuete järgimisse. Tuletatult eeltoodust võib järeldada, et kui suurendada turvameetmete nähtavust töötajatele, paraneb nende infoturbe alane käitumine.



Joonis 27. Heidutuse mõju respondentide infoturbe alasele käitumisele protsentides

Kuigi teadlikkuse tõstmine korrigeerib töötajate käitumist palju, ei taga see täielikku suhtumise muutust. Uuring näitab, et 19% respondentidest peab situatsioonkaasuste tegelaskujudele sarnast käitumist tõenäoliseks ka siis, kui ollakse teadlik turvanõuete järgimise kohustusest. Jooniselt 27 nähtub selgesti, et sanktsioonidega seotud heidutuse rakendamine korrigeeris veelgi enam respondentide hinnangut tegelaskujude käitumisele kui teadlikkuse tõstmine. Respondentide heidutamine korrigeeris respondentide suhtumist turvanõuete järgimisse keskmiselt 66%. Võrreldes teadlikkuse tõstmisega muutis heidutamine respondentide suhtumist turvanõuete järgimisse 21% enam. Heidutuse mõju infoturbe alasele käitumisele võib selgitada heidutuse eripäraga, mille laiem eesmärk põhineb preventsioonil, mis seisneb töötajatele hirmutunde tekitamisel, et valele käitumile järgneb kiire, kindel ja karm vastutus. See osa töötajatest, kelle käitumist teadlikkuse tõstmine ei korrigeerinud, muutis oma suhtumist nähes sanktsiooni või ümberkaudsete hukkamõistu negatiivse tagajärjena enda käitumisele, mille tulemusena mõjus see neile korrigeerivalt. Järeldub, et just heidutamine on väga efektiivne viis nende töötajate käitumise korrigeerimiseks, kes ei pea muid meetmeid (näiteks infoturbe alase teadlikkuse tõstmine) väga oluliseks käitumist

kujundavaks teguriks. Seega järeldub, et sanktsioonihirm ja kolleegide etteheited on väga efektiivne tegur enamike töötajate infoturbe alase käitumise õiguskuulekuse saavutamiseks.

Kõige suuremat heidutavat efekti respondentide käitumisele omas sanktsoonina kriminaalkaristus (66%), seejärel halduskaristus (65%) ja distsiplinaarkaristus (62%) ning viimasena ümberkaudsete hukkamõist (57%). Kui võrrelda protsentuaalselt kõiki heidutavaid meetmeid omavahel, siis väga suurt erinevust ei nähtu (vt Joonis 27). Saadud tulemustest järeldub, et heidutavate meetmete rakendamine aitab tõsta turvanõuete järgimist, mille tulemusena paraneb ka töötajate suhtumine infoturbe alasesse käitumisse. Järgnevalt toob autor välja olulisemad järeldused läbiviidud uuringu tulemustest.

Uuringu järeldused ja tulemused

Situatsioonkaasuste eesmärk oli näitlikustada soovimatut infoturbe alast käitumist, millele respondendid pidid andma hinnangu. Stenaariumid olid autori poolt koostatud selliselt, et need sobituksid Häirekeskuse infoturberiskidega. Empiirilise uuringu tulemustest selgub, et üle poolte uuringus osalenutest (62%) peab tõenäoliseks, et käituksid sarnaselt situatsioonkaasustes olnud tegelaskujudega. Autor on seisukohal, et situatsioonkaasuste stsenaariumeid tuleb käsitleda elementaarsete turvanõuete rikkumisena, kuna selliselt käitutes võib kaasneda turbeoht (näiteks arvutikontode volitamatu kasutamine, mis võib seada ohtu asutuse infosüsteemide turvalisuse).

Autor eeldab, et Häirekeskuse töökeskkonna iseärasustest tulenevalt (Häirekeskuse infosüsteemid sisaldavad suurel hulgal tundliku iseloomuga teavet) on päästeteenistujate üheks töökohustuseks vältida teiste isikute lubamatut ligipääsu isiklikule arvutikontole. Paraku saadud tulemuse põhjal võib öelda, et vastanute suhtumine käitumisse võib tekitada turberiske, kuna suurem osa vastanutest hindas tõenäoliseks enda käitumist sarnaselt kaasuste tegelaskujudega. Positiivsena toob autor välja, et kesmiselt 29% vastanutest hindas enda käitumist turvalisuse aspektist vaadatuna õigeks ning seega ei kujuta riski Häirekeskuse infosüsteemidele.

Uuringu peamine eesmärk oli uurida heidutavate meetmete rolli töötajate infoturbe alase käitumise kujundamisel. Eesmärgi saavutamiseks oli oluline teada saada, milliseks hindavad päästeteenistujad heidutavate meetmete mõju enda infoturbe alasele käitumisele. Autor võttis heidutavate meetmetena vaatluse alla erinevad sanktsioonid ja ümberkaudsete hukkamõistu. Uuringu tulemustele tuginedes võib öelda, et algselt valitud heidutavad meetmed tekitasid

kõik positiivse efekti respondentide suhtumisele infoturbe alasele käitumisele. Kuigi sanktsioonide rakendamine kutsus esile suurema õiguskuulekuse turvameetme järgimisel kui ümberkaudsete hukkamõist, ei erine see statistiliselt võrreldes väga palju. Uuritud meetmed kutsusid töötajate suhtumises käitumisse esile sarnase efekti, mistõttu puudub vajadus eristada heidutavaid meetmeid efektiivsuse järgi. Uuringust selgus, et heidutavate meetmete efektiivsust ei mõjutanud respondentide vanus ega staaž. Positiivsena toob autor välja, et heidutavate meetmete kasutamine korrigeeris vastanute suhtumist infoturbe alasesse käitumisse olulisel määral. Keskmiselt paranes heidutuse tagajärjel respondentide suhtumine turvameetmete järgimisse 66%. Uuringu tulemustele tuginedes võib öelda, et heidutavate meetmete rakendamine aitab oluliselt korrigeerida, st muuta töötajate suhtumist turvameetmete järgimisse.

Samuti selgus, et töötajate suhtumist infoturbe alasesse käitumisse on võimalik kujundada turvameetmete olemasolust teavitamise ja nende nähtavuse suurendamise kaudu. Kui autor juhtis respondentide tähelepanu asutuse turvameetmeid sisaldavate eeskirjade või juhendite sätetele, muutus nende hinnang tegelaskujude käitumisele keskmiselt 45%. Ehk kui tõsta töötajate teadlikkust asutuse turvameetmetest, suhtuvad töötajad paremini turvameetmete järgimisse.

Kokkuvõtlikult võib käesolevast alapeatükist välja tuua, et heidutavate meetmete rakendamine infoturbe valdkonnas toetub teooria põhiseisukohtadele, avaldades positiivset mõju töötajate infoturbe alasele käitumisele, mille tulemusena paraneb töötajate suhtumine turvameetmete järgimisse. Heidutamist on võimalik rakendada infoturbe alase käitumise kujundamiseks. Eeltoodust tulenevalt on autor seisukohal, et tööd on võimalik edasi arendada ning üks võimalus selleks on uurida kvantitatiivselt heidutuse teooria kehtivust infoturbe alasele käitumisele teistes sisejulgeoleku organisatsioonides, kus töökeskkond on Häirekeskusega võrreldes teistsugune. Järgnev peatükk käsitleb autoripoolseid soovitusettepanekuid Häirekeskusele töötajate infoturbe alase käitumise parendamiseks. Tehtavad ettepanekud tuginevad käesoleva töö teooria ja empiirilise uuringu tulemuste analüüsile ja sünteesile.

2.3 Ettepanekud päästeteenistujate infoturbe alase käitumise parendamiseks

Käesolev peatükk sisaldab autoripoolseid ettepanekuid Häirekeskusele päästeteenistujate infoturbe alase käitumise parendamiseks. Ettepanekud tuginevad töö teooria põhiseisukohtade ja empiirilise uuringu tulemuste analüüsile ja sünteesile. Peatükk sisaldab kokku viite ettepanekut. Iga ettepaneku kohta annab autor selgituse, milles väljendub konkreetse ettepaneku olulisus ja kuidas see aitab parendada päästeteenistujate infoturbe alast käitumist. Autoripoolsed ettepanekud Häirekeskusele on järgnevad.

1. Töötada välja selged, lihtsasti käsitletavad arvutikasutamise juhised.

Empiirilisest uuringust selgub, et keskmiselt 62% vastanutest peab tõnäoliseks käituda sarnaselt situatsioonkaasustes esitatud tegelaskujudele. Uuring näitas, et kui anda töötajatele selged teadmised, milline käitumine on asutuse turvameetmeid sisaldava eeskirja või juhendi kohaselt lubatud, avaldab see korrigeerivalt mõju nende suhtumisele käitumisse. Seepärast on oluline, et turvameetmeid sisaldavad juhised või eeskirjad oleksid selged ja kõigile töötajatele arusaadavad ning teada. Kuna ülaltoodud tulemus peegeldab autori arvates turberiski Häirekeskuse infosüsteemidele, soovitab autor Häirekeskusele töötada välja selgemad, lihtsasti käsitletavad arvutikasutamise juhised töötajatele, mis sisaldaksid ülevaadet õigetest käitumisviisidest ja infosüsteemide kasutamise nõudeid. Autorile teadaolevalt ei ole Häirekeskusel eraldiseisvat arvutikasutamise juhendit, mis koondaks lihtsasti loetavalt ja arusaadaval viisil turvanõuded arvutikasutajatele. Kuigi olemas on sisekorraeeskiri, mis sisaldab sätteid ka turvanõuetest, võib ülaltoodud tulemuse põhjal öelda, et sel juhul ei ole sisekorraeeskirjas arvutikasutamist puudutavad turvanõuded kas piisavalt selgesti sõnastatud või lihtsasti käsitletavad.

2. Teha töötajatele paremini kättesaadavaks asutuse turvameetmeid sisaldavad eeskirjad või juhised.

Empiirilisest uuringust selgus, et kui autor juhtis respondentide tähelepanu asutuse turvameetmeid sisaldavatele eeskirjade või juhendite olemasolule (situatsioonikirjeldusse lisati eeldus, et esitatud käitumine on vastuolus turvanormidega), muutus nende suhtumine turvameetmete järgimisse keskmiselt 45%. Uuringust järeldub, et kui suurendada turvameetmete nähtavust töötajatele, omab see heidutavat efekti ja töötajad eelistavad käituda juhistele vastavalt. Eeltoodust tulenevalt on autor seisukohal, et Häirekeskus peaks

suurendama olemasolevate turvameetmeid sisaldavate eeskirjade või juhendite nähtavust, tehes neid paremini kättesaadavaks töötajatele. Üks võimalus selle saavutamiseks on korraldada regulaarselt töötajatele teavitus- ja koolitusüritusi eesmärgiga tutvustada õigeid käitumisviise ja asutuse infoturbeohte. Nimetatud ohud võivad aja möödudes muutuda, mistõttu on vajalik kohandada ka töötajate käitumist turvalisemaks.

3. Võtta kasutusele heidutavad meetmed töötajate infoturbe alase käitumise mõjutamiseks.

Uuringust selgub, et sanktsioonidega kaasnev heidutus on väga efektiivne tegur kujundamaks infoturbe alast käitumist. Heidutavate meetmete lisamine situatsioonkaasustesse parandas vastanute suhtumist infoturbesse keskmiselt 66%. Heidutavate meetmete hulka kuulub lisaks ümberkaudsete hukkamõist, mis avaldas samuti olulist mõju vastanute suhtumisele käitumisse. Siiski oli selle meetme efekt väiksem kui otsestel sanktsioonidel. Seejuures oli sanktsioonide korrigeeriv efekt märgatav juba leebemate sanktsioonide puhul (distsiplinaarkaristus). Eeltoodust tulenevalt on autor seisukohal, et heidutavate meetmete rakendamine võib tõsta turvameetmete järgimist oluliselt, mistõttu võiks see kuuluda Häirekeskuse infoturbe korralduse hulka. Heidutavate meetmete rakendamisel ei ole oluline eristada erineva vanuse või staažiga töötajaid, kuna uuringust selgus, et heidutavate meetmete efektiivsust nimetatud tegurid ei mõjutanud. Samas on autor seisukohal, et turvanõuete järgimist saab nõuda üksnes siis, kui sellele eelneb töötajate informeerimine õigetest käitumisviisidest tulenevalt organisatsiooni turvariskidest. Kui töötajatel puudub teadmine õigest käitumisest, võib heidutamine mitte toimida.

4. Suurendada infotehnoloogia halduspersonali teadlikkust heidutuse olulisusest.

Üldjuhul määratakse infoturbe korraldamine organisatsioonis kindlatele isikutele, kelle ülesandeks on infoturvet välja töötada ja juurutada. Selleks, et infoturve oleks efektiivne, on oluline, et sellega tegeletakse süsteemselt ja järjepidevalt. Keskkond on pidevalt muutumas, mis võib kaasa tuua uusi turvariske. Infoturbega tegelev personal peab olema valmis rakendama parimaid abinõusid hoidmaks ära uute ja olemasolevate riskide avaldumist. Heidutus on üks abinõu muutmaks töötajate suhtumist organisatsioonis kehtivatesse turvameetmetesse. Teadlaste sõnul võib töötajate käitumine kaasa tuua suuri turvariske, mistõttu tuleb suhtuda nende käitumisse tähelepanelikkusega. On oluline, et infoturbe eest vastutav personal teaks, kuidas organisatsiooni töötajaid mõjutada parimal viisil järgima kehtivaid turvanõudeid. Autor on seisukohal, et Häirekeskuse turvanõuete järgimise efektiivsuse tõstmiseks on kõigepealt oluline anda Häirekeskuse infoturvet korraldavale

personalile teadlikkus heidutavate meetmete rakendamisest ja selle rollist töötajate käitumise kujundamisel. Käsolevat magistritööd on võimalik kasutada õppematerjalina selgitamaks heidutavate meetmete tööpõhimõtet infoturbe alase käitumise kujundamisel.

5. Korraldada süsteemselt töötajate kontrollimist.

Heidutuse eesmärk on anda töötajatele teadmine, et valele käitumisele järgneb kindlasti vastutus. Kuid heidutus ei pruugi avaldada efekti kõigi töötajate suhtumisele infoturbesse, mistõttu tuleb rakendada lisameetmeid tõhustamaks turvameetmete järgimist. Lisaabinõuna soovitab heidutuse teooria rakendada tuvastavaid tegevusi, näiteks töötajate kontrollimist. Selle eesmärk on tuvastada potentsiaalseid rikkujaid, kuna alati ei pruugi vale käitumine välja paista. Töötajate kontrollimine peab toimuma süsteemselt, see tähendab regulaarselt, et töötajatel säiliks teadmine, et neid jälgitakse. Seda mitte tehes võib pikemas perpektiivis heidutuse efektiivsus väheneda, kuna nähakse, et vale käitumise avastamise tõenäosus on suhteliselt väike. Eeltoodust tulenevalt on autor seisukohal, et Häirekeskus peaks kontrollima töötajate infoturbe alast käitumist süsteemselt.

Kokkuvõttes lähtus autor ettepanekute koostamisel põhiliselt heidutuse teooria eripärast, mis näeb seaduserikkujate mõjutamiseks ette nende vastutusele võtmist, ning empiirilise uuringu tulemustest, mis kinnitas heidutuse teooria kehtivust infoturbe alase käitumise suhtes. Uuring näitas, et töötajate praegune suhtumine võib kaasa tuua riske Häirekeskuse infosüsteemidele, mistõttu pidas autor vajalikuks teha ülaltoodud ettepanekud. Soovitused käsitlevad turvalisust puudutava regulatsiooni täiendamist, teavituse läbi viimist, sanktsioonide kehtestamist, infotehnoloogia halduspersonali informeerimist ja töötajate kontrollimist. Autor usub, et heidutavate meetmete rakendamine annab Häirekeskuse turvalisuse saavutamisele olulise lisandväärtuse, kuna selle abil on võimalik korrigeerida efektiivselt nende töötajate suhtumist infoturbe alasesse käitumisse, kes muid turvalisust puudutavaid tegevusi, nagu teavitus ja koolitusüritused, mille eesmärgiks on informeerida töötajaid õigetest käitumisviisidest ja infoturbeohtudest, väga tõsiseks mõjuteguriks ei pea. Kuid eeltoodu rakendamiseks on esmalt vaja anda Häirekeskuse infoturbe eest vastutavale personalile teadlikkus heidutuse olulisusest töötajate infoturbe alase käitumise kujundamisel, mida käesolev töö on autori arvates võimeline pakkuma.

KOKKUVÕTE

Infoturbe peamine eesmärk on tagada infovarade turvalisus, mille saavutamiseks rakendavad organisatsioonid erinevaid turvameetmeid. Lisaks sellele sõltub turvalisus paljudel juhtudel organisatsiooni töötajate käitumisest. Teadlaste hinnangul võib töötajate käitumine tekitada suuri infoturberiske, mistõttu on organisatsioonidel soovitatav suhtuda töötajate käitumisse äärmise tähelepanelikkusega ning mõista käitumist mõjutavaid tegureid. Magistritöö autor uuris heidutavaid meetmeid ja nende rolli töötajate infoturbe alase käitumise kujundamisel. Magistritöö probleem seisnes selles, et ei ole uuritud töötajate hoiakuid ja suhtumisi infoturbesse töökeskkonnas, ega käsitletud kõiki võimalusi töötajate käitumise kujundamiseks. Käesolev uurimus keskendus selle lünga täitmisel just heidutavatele meetmetele uurides, kuidas suhtuvad sisejulgeoleku töötajad heidutavate meetmete rakendamisse infoturbe alase käitumise kujundamisel.

Magistritöö eesmärgiks oli selgitada välja päästeteenistujate hinnangud heidutavatele meetmetele, mis võiksid kujundada nende infoturbe alast käitumist ja saadud tulemuste põhjal töötada välja soovitusettepanekud Häirekeskusele töötajate infoturbe alase käitumise parendamiseks. Eesmärgi saavutamiseks oli autor püstitanud kolm uurimisülesannet, mis kahes peatükis lahendati.

Esimese uurimisülesande raames, mis moodustas ühtlasi töö teoreetilise tausta, tutvustas ja analüüsis autor esimese peatüki esimeses alajaotuses infoturbe mõistet ja olemust, infoturbe riske ning turbe korraldamise protsesse infot töötlevas asutuses. Selleks avas autor põhjalikult infoturbe mõiste ning tõi välja selle iseloomulikud jooned, selgitas infoturbe riske ja nende haldamist ning tutvustas turbe korraldamise mudelit. Esimese peatüki esimeses alajaotuses selgus, et infoturbe definitsioone on väga palju, kuid neist tuntuim, milleks on teabe käideldavuse, konfidentsiaalsuse ja tervikluse säilitamine, on jäänud sageli arusaamatuks infoturbespetsialistidele. Sellest ajendatult on teadlased pakkunud välja paremaid ja arusaadavamaid definitsioone; näiteks on infoturvet määratletud kui head informeeritud kindlustunnet, et infovarasid ohustavad riskid ja kontroll on viidud tasakaalu. Infoturbe põhieesmärk on säilitada teabe käideldavus, konfidentsiaalsus ja terviklus, mis väljendub teabe ja infosüsteemide kaitsmises loata juurdepääsu, kasutamise, avaldamise, muutmise või

hävitamise eest. On oluline teada, et infovarade turvalisus ei tähenda üksnes selle kaitstust või puutumatust, vaid ka infovarade omaduste püsimist ohtude kiuste. Eeltoodust tulenevalt moodustab infoturbest olulise osa riskide haldamine, mille eesmärk on selgitada välja ohud, mis võiksid põhjustada kahju infovaradele ning rakendada abinõusid hoidmaks ära nimetatud ohtude avaldumist. Töötajate hoolimatu käitumine võib olla üks nimetatud ohtudest, mis võib organisatsioonile tekitada suuri majanduslikke kahjusid. Infoturbe korraldamiseks rakendavad asutused ja organisatsioonid infoturbe halduse süsteemi. Infoturbe halduse süsteemi mudel tuleneb rahvusvahelistest standarditest, mille eemärk on anda lähtekoht infoturbe korralduse välja töötamiseks, mida iga asutus või organisatsioon kohandab vastavalt enda turbe vajadustele.

Esimese peatüki teises alajaotuses vaatles autor töötajate infoturbe alase käitumise iseärasusi ja käitumist mõjutavaid tegureid ning uuris organisatsiooni võimalusi suurendamaks töötajate õiguskuulekust turvanõuete järgimisel. Esimese peatüki teises alajaotuses selgus, et infoturbe alast käitumist võib defineerida kui töötajate käitumist infoturbepoliitika seisukohalt, mis võib tekitada organisatsioonile suuri infoturberiske. Seepärast on organisatsioonidel soovitatav pöörata töötajate käitumisele tähelepanu ja püüda mõista infoturbe käitumist mõjutavaid tegureid. Erinevad teadlased on toonud välja mitmeid töötajate infoturbe alast käitumist mõjutavaid tegureid nagu organisatsioonikultuur, teadlikkus, ratsionaalsus jne. Kui turvalisust üksnes nende tegurite toimel ei saavutata, on organisatsiooni huvides kohaldada lisaabinõusid töötajate turvanõuete järgimise tõhustamaks. Üks efektiivsemaid viise töötajate infoturbe alase käitumise parendamiseks on infoturbe alase teadlikkuse tõstmine. Peale selle kasutatakse töötajate kontrollimist jne. Omaette abinõude grupi moodustavad heidutavad meetmed.

Esimese peatüki kolmandas alajaotuses uuris autor tulenevalt infoturbe alase käitumise mõjutavatest teguritest heidutavaid meetmeid abinõuna töötajate infoturbe alase käitumise kujundamiseks soovitavas suunas. Kolmandas alajaotuses vaatles autor heidutuse teooria olemust ja kujunemist ning analüüsis teooria rakendamise võimalusi infoturbe alase käitumise kujundamisel. Kolmandas alajaotuses selgus, et heidutavate meetmete rakendamine on üks võimalus parendada töötajate suhtumist infoturbe alasesse käitumisse. Heidutavate meetmete kasutamist selgitab heidutuse teooria, mis peab vajalikuks seaduserikkujaid vastutusele võtta neid karistades või hukkamõistes, eesmärgiga mõjutada seaduserikkujat ja hirmutada potentsiaalseid rikkujaid hoiduma valest käitumisest tulevikus. Eeltoodut silmas pidades on teadlased empiiriliselt uurinud heidutavaid meetmeid töötajate soovimatule infoturbe alasele

käitumisele ning leidnud, et töötajate õiguskuulekust turvanõuete järgimisel on võimalik suurendada, kui anda töötajatele teadmine neid heidutades, et turvameetmete eiramine toob kindasti kaasa vastutusele võtmise. Empiiriliste uurigute tulemustele toetudes on jõutud seisukohale, et heidutavate meetmete rakendamine mõjub preventiivselt soovimatule infoturbe alasele käitumisele, kuna suureneb tajutav vastutus turvanõuete eiramisele, mis omakorda toob kaasa turvanõuete järgimise tõhustamise.

Empiirilise uuringu eesmärgi saavutamiseks oli autor teise uurimisülesande eesmärgiks seadnud selgitada välja päästeteenistujate hinnangud infoturbe alasele käitumisele ja heidutavatele meetmetele käitumise kujundajana, mille lahendas töö teises peatükis. Teise uurimisülesande lahendamiseks viis autor läbi kaardistava uuringu, milles andmeid kogus kvantitatiivset andmekogumisemeetodit kasutades. Andmete kogumiseks viis autor läbi struktureeritud ankeetküsitluse kõigi Häirekeskuse päästeteenistujate seas, saamaks ülevaadet infoturbe alasest käitumisest ja päästeteenistujate suhtumisest heidutavatesse meetmetesse. Andmete töötlemiseks kasutas autor andmetöötlusprogrammi *MS Excel*, mille abil viis läbi ühe- ja mitmemõõtmelise analüüsi. Uurimisülesande lahendamise käigus saadud uurimistulemustena võib välja tuua järgneva:

1. Organisatsioonipoolsed heidutavad meetmed avaldasid positiivset mõju töötajate suhtumisele käitumisse ja kutsusid esile suurema õiguskuulekuse turvameetmete järgimises. Töötajate suhtumine turvameetmete järgimisse paranes heidutavate meetmete rakendamise tulemusena keskmiselt 66%;
2. Turvameetmete olemasolu ja nähtavus parandas töötajate suhtumist turbenõuete järgimisse. Kui autor juhtis töötajate tähelepanu asutuse turvameetmeid sisaldavatele eeskirjadele, paranes respondentide suhtumine turvameetmete järgimisse keskmiselt 45%;
3. Heidutavatest meetmetest sanktsioonide rakendamine kutsus esile suurema õiguskuulekuse turvameetme järgimisse kui ümberkaudsete hukkamõist, kuid erinevus ei olnud statistiliselt võrreldes väga suur. Uuritud heidutavad meetmed kutsusid töötajate suhtumises käitumisse esile sarnase efekti, mistõttu puudub vajadus eristada meetmeid efektiivsuse järgi;
4. Heidutavate meetmete efektiivsust ei mõjutanud autori poolt valitud kriteeriumid, milleks oli respondentide vanus ja staaž.

Teise uurimisülesande lahenduse tulemusena võib öelda, et heidutavate meetmete rakendamine infoturbe valdkonnas toetub teooria põhiseisukohtadele, avaldades positiivset

mõju töötajate infoturbe alasele käitumisele, mille tulemusena paraneb töötajate suhtumine turvanõuete järgimisse.

Kolmanda uurimisülesandena oli autor seadnud eesmärgiks töötada välja soovitusettepanekud Häirekeskusele töötajate infoturbe alase käitumise parendamiseks, mille lahendas töö teises peatükis. Kolmanda uurimisülesande lahendamiseks töötas autor tuginedes töö teoreetilisele käsitluse ja uuringu tulemuste analüüsil ja sünteesil välja viis soovitusliku iseloomuga ettepanekut, milleks olid:

1. Töötada välja selged, lihtsasti käsitletavad arvutikasutamise juhised;
2. Teha töötajatele paremini kättesaadavaks asutuse turvameetmeid sisaldavad eeskirjad või juhised;
3. Võtta kasutusele heidutavad meetmed töötajate infoturbe alase käitumise mõjutamiseks;
4. Suurendada infotehnoloogia halduspersonali teadlikkust heidutuse olulisusest;
5. Korraldada süsteemselt töötajate kontrollimist.

Ettepanekute koostamisel lähtus autor põhiliselt heidutuse teooria eripärast, mis näeb seaduserikkujate mõjutamiseks ette nende vastutusele võtmist ning empiirilise uuringu tulemustest, mis kinnitas heidutuse teooria kehtivust infoturbe alasele käitumisele. Kuid uuring näitas ka seda, et töötajate hetkeolukorra suhtumine infoturbe alasesse käitumisse võib kaasa tuua riske Häirekeskuse infosüsteemidele, mistõttu pidas autor vajalikuks teha ettepanekuid turvalisust puudutava kehtiva regulatsiooni täiendamiseks, ja viia läbi teavitusüritusi töötajate infoturbe alase teadlikkuse tõstmiseks, motiveerimaks töötajaid õiguskuulekamalt järgima Häirekeskuse turvameetmeid sisaldavaid eeskirju või juhendeid. Autor usub, et heidutavate meetmete rakendamine annab Häirekeskuse turvalisuse saavutamisele olulise lisandväärtuse, kuna selle abil on võimalik korrigeerida efektiivselt nende töötajate suhtumist käitumisse, kes muid turvalisust puudutavaid tegevusi, nagu teavitus ja koolitusüritused, mille eesmärgiks on informeerida töötajaid õigetest käitumisviisidest ja infoturbeohtudest, väga tõsiseks mõjuteguriks enda käitumisele ei pea. Heidutavate meetmete rakendamisel ei ole oluline eristada erineva vanuse või staažiga töötajaid, kuna uuringust selgus, et heidutavate meetmete efektiivsust nimetatud tegurid ei mõjutanud. Kuid eeltoodu rakendamiseks on esmalt vaja anda Häirekeskuse infoturbe eest vastutavale personalile teadlikkus heidutuse olulisusest töötajate infoturbe alase käitumise kujundamisel, mida käesolev töö on autori arvates võimeline pakkuma.

Autor on seisukohal, et käesoleva töö tulemusi on võimalik kasutada infoturbe korraldamise parendamiseks Häirekeskuses, pakkudes ühtlasi lisateadmist sisejulgeoleku organisatsioonide

infoturbespetsialistidele töötajate infoturbe alasest käitumisest. Käesolevat tööd on võimalik edasi arendada ning üks võimalus selleks on uurida kvantitatiivselt heidutuse teooria kehtivust töötajate infoturbe alasele käitumisele teistes sisejulgeoleku organisatsioonides, kus töökeskkond on Häirekeskusega võrreldes suurem. Autori arvates moodustaks sobiliku valimi näiteks Politsei- ja Piirivalveameti töökollektiiv, mis moodustub ca 6000 töötajast. Kokkuvõtlikult on võimalik öelda, et käesolev uurimistöö saavutas püstitatud uurimisülesanded ning algselt seatud eesmärk sai täidetud.

SUMMARY

The subject of this Master´s Thesis is "Rescue servant´s attitude toward deterrent measures in the field of information security using the example of Estonian Emergency Response Centre". The objective of this thesis is to present practical suggestions on how to improve employee information security behavior in Estonian Emergency Response Centre based on deterrent measures which rescue servant´s believe to influence their security behavior.

The following research tasks were raised:

1. Analyze and give an overview of information security theoretical basis, employee security behavior and deterrent measures in influencing employee information security behavior;
2. Identify, which deterrent measures influence the actions of rescue servants related to information security behavior;
3. Through the synthesis of the theoretical framework and survey results present practical suggestions for Estonian Emergency Response Centre on how to improve employee information security behavior.

To achive the research objective the author used survey research strategy and quantitative research method. Data was collected using structured questionnaires and the sample was chosen using targeted method. The survey was filled by rescue servant´s from Estonian Emergency Response Centre. Their different attitudes toward deterrent measures were analyzed and compared. As deterrent measures the author researched different sanctions and colleague´s condemnation with security behavior. Data was statistically analyzed and displayed as figures and tables.

The results of this Master´s Thesis are:

1. Deterrent measures have a positive influence on employee´s attitude and help to improve security behavior. Deterrent measures helped to improve respondent´s attitude toward security behavior 66%;
2. Security countermeasures visibility has a positive influence on employee´s security behavior. Respondent´s attitude toward security behavior improved 45%, after their attention were drawn to security countermeasures existence;

3. Sanctions as deterrent measures influence security behavior more than colleague´s condemnation, but the difference is not large. Both measures have the same influence on security behavior and therefore distinguish between them is not needed.
4. The selected criterias which were the respondent´s age and length of service did not affect the effectiveness of deterrent measures.

Based on the theoretical basis and survey results the following suggestions were presented:

1. Develop a clear, easy to deal with computer use guidelines for employee´s;
2. Make the agency security measures included rules or guidelines more accessible to employee´s;
3. Implement deterrent measures for improving employee´s security behavior;
4. Increase awareness of Information technology administrative staff of the importance of deterrence;
5. Implement systematic employee´s security behavior checks.

VIIDATUD ALLIKAD

AMA/ePolicy Institute Research, „2007 Electronic Monitoring & Surveillance Survey" (2007) <http://www.plattgroupllc.com/jun08/2007ElectronicMonitoringSurveillanceSurvey.pdf> p1-3 (06.03.2014).

Anderson, J. M., Why we need a new definition of information security, *Computers & Security*, 22, 4, 2003, 308-313.

Andmekaitse ja infoturbe seletussõnastik AKIT, Cybernetica AS, 2011-2012 <http://akit.cyber.ee/> (04.02.2014).

Andres, L., *Designing & Doing Survey Research* (London Thousand Oaks, New Delhi, Singapore: SAGE Publications, 2012).

Andress, J., *The Basics of Information Security. Understanding the Fundamentals of InfoSec in Theory and Practice* (Elsevier, 2011).

Avaliku teabe seadus , 15.11.2000, jõustunud 01.01.2001 – RT I 2000, 92, 597 ... RT I, 19.12.2012, 5.

Becker, G. S., Crime and Punishment: An Economic Approach, *The Journal of Political Economy*, 76, 2, 1968, 169-217.

Blakley, B., McDermott, E., and Geer, D. Information security is information risk management, *ACM Workshop on New Security Paradigms NSPW*, 2001, 97-104.

BSI., „Standard BSI 100-1 Infoturbehalduse süsteemid (ISMS)" (2008) <https://www.ria.ee/public/ISKE/Standard_BSI_100-1.pdf> (04.03.2014).

Bulgurcu, B., Cavusoglu, H., & Benbasat, I. Information Security Policy Compliance: An Empirical Study of Rationality-Based Beliefs and Information Security Awareness, *MIS Quarterly*, 34, 3, 2010, 523-548.

Canavan, S., Diver, S. „An Information Security Policy Development Guide for Large Companies" (2003) <http://www.sans.org/reading-room/whitepapers/policyissues/information-security-policy-adevelopment-guide-for-large-and-small-companies-1331?show=information-security-policy-a-development-guide-for-large-and-small-companies-1331&cat=policyissues> (09.02.2014).

Crossler, R. E., Johnston, A. C. Lowry, P. B., Hu, Q., Warketin, M. Baskerville, M., Future directions for behavioral information security research, *Computer & Security*, 32, 2013, 90-101.

D'Arcy, J. and Hovav, A. Deterring internal information systems misuse: An end user perspective, *Communications of the ACM*, 50, 10, 2007, 113-117.

Eesti Standard EVS-ISO/IEC 27001: 2006, Infotehnoloogia. Turbemeetodid. Infoturbe halduse süsteemid. Nõuded <http://www.evs.ee/tooted/evs-iso-iec-27001-2006> (02.02.2014)

Ernst & Young, „Global information security survey 2008" <http://www.continuitycentral.com/news04217.html > (01.02.2014).

Esinurm, J., "Infoturbe alane teadlikkus sisejulgeolekuorganisatsioonis", magistritöö, Sisekaitseakadeemia, (2013).

Fung, P., Kwok, L.-F., Longley, D. Electronic Information Security Documentation (2003) < http://crpit.com/confpapers/CRPITV21AFung.pdf> (04.03.2014).

GFI, Security Survey in the United States (2007) <http://www.gfi.com/documents/rv/smbsurvey.pdf> (06.03.2014).

Gopal, R. D., Sanders, G. L., Preventive and Deterrent Controls for Software Piracy, *Journal of Management Information Systems*, 3, 4, 1997, 29-47.

Hanson, V., Laur, M., Oit, M., Alliksoo, *Infosüsteemide turve 1. Turvarisk* (Cybernetica AS, 2009).

Harrington, S. J., The effect of codes of ethics and personal denial of responsibility on computer abuse judgments and intentions, *MIS Quart*, 20, 3, 1996, 257-258.

Henry, K., "Risk Management and Analysis", *Information Security Management Handbook 5th Edition*, Ed. Tipton, H. & Krause, M. (CRC Press, Boca Raton,2004).

Herath, T., Rao, H. R., Encouraging information security behaviors in organizations: Role of penalties, pressures and perceiced effectiveness, *Decision Support Systems*, 47, 2009, 154-165.

Herley, C., So Long, And No Thanks fo the Externalities: The Rational Rejection Security Advice Users (2009) <http://research.microsoft.com/en-us/um/people/cormac/papers/2009/SoLongAndNoThanks.pdf> (05.03.2014).

Hoffer, J. A., & Straub, D. W., The 9 to 5 underground: Are you policing computer crimes?, *Sloan Management Review*, 30, 4, 1989, 35.

Hone, K., & Eloff, J. H., What Makes an Effective Information Security Policy?, *Network Security*, 20,6, 2002, 14-16.

Hu, Q., Xu, Z., Dinev, T. and Ling, H., Does Deterrence Work in Reducing Information Security Policy Abuse by Employees?, *Communication of the ACM*, 54, 6, 2011, 54-60.

Infoturbe juhtimise süsteem, vastu võetud Vabariigi Valitsuse määrusega 15.03.2012 nr 26, jõustunud 01.01.2013 – RT I, 19.03.2012, 4.
Isikuandmete kaitse seadus, 15.02.2007, jõustunud 01.01.2008 – RT I 2007, 24, 127 … RT I, 30.12.2010, 11.

Joinson, A. & Whitty, M., Watched in workplace, *Infosecurity*, 5, 1, 2008, 38-40.

Jolibert, A., & Baumgartner, G., Values, Motivation and Personal Goals: Revisited, *Psychology & Marketing*, 14, 17, 1997, 675-688.
Kabay, M. E., "Using Social Psychology to Implement Security Policies", (2009) <www.mekabay.com/infosecmgmt/Soc_Psych_INFOSEC.pdf> p12-13 (20.02.2014).

Kivi, L. Sootak, J., Karistuse kohaldamise alused karistusseadustikus, *Juridica*, 2001, 7, 475-484.

Kotulic, A. G., Clark, J. G. Why there aren't more information security research studies. *Information & Management*, 41, 5, 2004, 597-607.

Lampson, B. W, Computer Security in the Real World, *Principles of Computer Systems*, 37, 6, 2002, 37-46.

Lavrakas, P., *Encyclopedia of Survey Research Methods Vol 1-2* (Thousand oaks, London, New Delhi, Singapore: Sage Publications, 2008).

Leach, J, Improving User Security Behaviour, *Computer & Security*, 22, 8, 2003, 685-692.

Lee, S. M., Lee, S. and Yoo, S. An Integrative Model of Computer Abuse Based on Social Control and Deterrence theories, *Information & Management*, 41, 2004, 707-718.

Leelo, E., "Efektiivne andmekaitse algab suhtumisest" (2005) <http://www.hlp.ee/media/ITee_0905_Lee go.pdfZ> (10.12.2013).

Lotz, D. "Pärast valgustusajastut ja postmodernismi. Karistuse kutse, mis juhatab õiget mõistust, õigeid südameid ja õigeid käsi!" (2000) <ekklesia.ee/vana/elu/d5.pdf> (20.02.2014)

Nagin, D. S., Pogardsky, G., Integrating celerity, impulsivity and extralegal sanction threats into a model of general deterrence and evidence, *Criminology*, 39, 4, 2001, 865-891.

Neuman, W. L., *Social Research Methods. Qualitative and Quantitative Approaches* (Boston: Allyn & Bacon, 2011).

Onwudiwe, I. D., Odo, J and Onyeozili, C., „Deterrence Theory", *Encyclopedia of Prison & Correctional Facilities*, Ed. Bosworth, M. (Thousand Oaks, CA, SAGE Publications, 2005).

Oslan, G., "People, processes and technology: A winning combination in the fight against cyber crime", *GSN Government Security News*, 14.08.2011 <http://www.gsnmagazine.com/node/24210?c=cyber_security> (08.01.2014).
P.J., Why is Information Security important? (07.01.2009) <http://mindfulsecurity.com/2009/07/01/why-is-information-security-important/> 03.03.2014

Prenzler, T., The Human Side of Security, *Security Journal*, 20, 2007, 35-39.

Päästeinfosüsteemi pidamise põhimäärus, vastu võetud siseministri määrusega 31.01.2012 nr 2, jõustunud 05.02.2012 – RT I, 02.02.2012, 6... RT I, 05.04.2013, 17.

Riigi Infosüsteemid, "Asutuse Infoturbepoliitika" <http://www.riso.ee/sites/default /files/soovitused/ti nfoturbpol.htm> (05.03.2014)

Riigisaladuse ja salastatud välisteabe seadus, 25.01.2007, jõustunud 01.01.2008, RT I 2007, 16, 77 … RT I, 22.12.2011, 24.

Ruighaver, A. B., Maynard, S. B., & Chang, S., Organisational Security Culture: Extending the End User Perspective, *Computers & Security, 26*, 2007, 56-62.

Sandhu, R., Good-Enough Security: Toward a Pragmatic Business-Driven Discipline, *IEEE Internet Computing*, 3, 2003, 66-68.

Schein, E. H., *Organizational Culture & Leadership Third Edition* (San Francisco, CA:Jossey-Bass, 2004).

Schneier, B., Managed Security Monitoring: Network Security for the 21st Century. *Computers & Security*, 20, 2001, 491-503.

Siegel, L. J., *Criminology, Ninth Edition* (Thomson Wadsworth, 2008).

Silowash, G. J., Cappelli, D. M., Moore, A. P., Trzeciak., R. F., Shimeall. T., Common Sense Guide to Mitigating Insider Threats, 4th Edition, *Software Engineering Institutem Paper 677* (2012) <http://repository.cmu.edu/cgi/viewcontent.cgi?article=1669&conte xt=sei> (06.02.2014)

Siponen, M. T., A Conceptual Foundation for Organizational Information Security Awareness, *Information Management & Computer Security*, 8, 1, 2000, 31-41.

Stanton, J. M., Stam, K. R., Mastrangelo, P. and Jolton, J., Analysis of end user security behaviors, *Computers & Security*, 24, 2, 2005, 124–133.

Straub, D. W., & Nance, W. D. Discovering and disciplining computer abuse in organizations: A field study, *Managemet Information Systems Quarterly*, 14, 1, 1990, 46-62.

Straub, D. W., Welke, R. J., Coping with systems risk: Security planning models for management decisions making, *MIS Quart*, 22, 4, 1998, 441- 469.

Straub, D.W. Computer abuse and computer security: Update on an empirical study, *Security, Audit and Control Review*, 4, 2, 1986, 21-31.

Tallinna linna asutuste infoturbe põhimõtted, vastu võetud Tallinna Linnavalitsuse määrusega 15.12.2010 nr 104, jõustunud 20.12.2010 – RT IV, 24.05.2013, 38.

Teddlie, C., Yu, F., Mixed Methods Sampling A Typology With Examples, *Journal of Mixed Methods Research*, 1, 1, 2007, 77-100.

Thomson, K., von Solms, R., Louw, L., „Toward Corporate Information Security Obedience" <http://dl.ifip.org/index.php/AICT/article/viewFile/32363/1084> (10.02.2014).

Tryfonas, T., Kiountouzis, E., & Poulymenakou, A., Embedding Security Practicies in Contemporary Information Systems Development Approaches, *Information Management & Computer Security*, 9, 4, 2001, 183-197.

Warkentin, M., and Willison, R., Behavioral and policy issues in information systems security: the insider threat, *European Journal of Information Systems*, 18, 2, 2009, 101-105.

Varney, C. A., „Consumer Privacy in the Information Age: A View from the United States, The Privacy & American Business National Conference, Omni Shoreham Hotel, Washington, D.C." (1996) <http://www.ftc.gov/public-statements/1996/10/consumer-privacy-information-age-view-united-states> (12.11.2013).

Verdon, D., Security Policies and the Software Developer, *IEEE Security&Privacy*, 2006, 42-49.

West, R. The Psychology of Security – Why do good users make bad decisions?, *Communication of the ACM* , 51, 5, 2008, 34-40.

Whitman, M. E., Enemy at the Gate: Threats to Information Security, *Communications of the ACM*, 46, 8, 2003, 91-95.

Whitman, M. E., In Defense of the Realm: Understanding the Threats to Information Security, *International Journal of Information Management*, 24, 2004, 43-57.

Vito, G. F., Maahs, J. R., *Criminology Theory, Research and Policy, Third Edition* (Jones & Bartlett Learning Publication, 2011).

Von Solms, B., & von Solms, R., The 10 Deadly Sins of Information Security Management, *Computer & Security*, 23, 2004, 371-376.

Von Solms, R., Information Security Management: The Second Generation, *Computer & Security*, 15, 1996, 281-288.

Wakefield, R. L., Employee Monitoring and Surveillance – The Growing Trend, *Information Systems Control Journal*, 1, 2004, 1-3.

Wood, M. B., *Introducing Computer Security* (NCC Publications, 1982).

Workman, M., Gaining Access with Social Engineering: An Empirical Study of the Threat, *Information Systems Security Journal*, 16, 6, 2007, 315-331.

TABELITE JA JOONISTE LOETELU

LISA 1. PÄÄSTETEENISTUJATE ANKEETKÜSIMUSTIK

KAASUS 1

Malle teeb kontoris arvutiga tööd kui tema juurde tuleb kolleeg ja kutsub kohvipausile. Kuna Malle on hommikust saadik usinalt töötanud, otsustab ta kutse vastu võtta. Ta lahkub töölaua tagant, kuid ei lukusta arvutit. Malle ei tea täpselt, kas arvuti lukustamine on kohustusena kirjas mõnes asutuse eeskirjas või juhendis. Samas eeldab ta, et kohvipaus võtab vähe aega ja et selle aja jooksul ei satu kedagi teist tema arvuti juurde.

1. Kui suureks hindate võimalust, et käituksite selliselt nagu Malle?

□ Väga suureks □ Pigem suureks □ Ei suureks ega väikeseks
□ Pigem väikeseks □ Väga väikeseks

2. Kui suureks hindate võimalust, et käitub mõni kolleeg selliselt nagu Malle?

□ Väga suureks □ Pigem suureks □ Ei suureks ega väikeseks
□ Pigem väikeseks □ Väga väikeseks

3. Kas Te käituksite sarnaselt Mallega, kui teaksite, et arvuti lukustamise kohustus on kirjas asutuse turvameetmeid sisaldavas eekirjas või juhendis, kuid selle eest ei ole ette nähtud sanktsioone ja seda ei kontrollita?

□ Jah, käituksin □ Pigem käituksin □ Pigem ei käituks
□ Ei käituks □ Ei oska öelda

4. Kas Te käituksite sarnaselt Mallega, kui teaksite, et arvuti lukustamise kohustus on kirjas asutuse turvameetmeid sisaldavas eekirjas või juhendis ning selle eest on ette nähtud sanktsioonina distsiplinaarkaristus (noomitus käskkirjaga)?

□ Jah, käituksin □ Pigem käituksin □ Pigem ei käituks
□ Ei käituks □ Ei oska öelda

5. Kas Te käituksite sarnaselt Mallega, kui teaksite, et arvuti lukustamise kohustus on kirjas asutuse turvameetmeid sisaldavas eekirjas või juhendis ning selle eest on ette nähtud halduskaristus (trahv seoses oluliste andmete lekkega)?

□ Jah, käituksin □ Pigem käituksin □ Pigem ei käituks
□ Ei käituks □ Ei oska öelda

6. Kas Te käituksite sarnaselt Mallega, kui teaksite, et arvuti lukustamise kohustus on kirjas asutuse turvameetmeid sisaldavas eekirjas või juhendis ning selle eest on ette nähtud kriminaalkaristus (trahv või vangistus seoses üliolulistе andmete lekkega)?
□ Jah, käituksin □ Pigem käituksin □ Pigem ei käituks
□ Ei käituks □ Ei oska öelda

7. Kas Te käituksite sarnaselt Mallega, kui teaksite, et arvuti lukustamise kohustus on kirjas asutuse turvameetmeid sisaldavas eekirjas või juhendis, kuid selle eest ei ole ette nähtud sanktsioone, samas Teie töökaaslased teeksid Teile etteheiteid ja nende suhtumine Teisse halveneks?

□ Jah, käituksin □ Pigem käituksin □ Pigem ei käituks
□ Ei käituks □ Ei oska öelda

KAASUS 2

Peeter teeb kontoris arvutiga tööd, kui saab töö e-postkasti sõbralt kirja, mis sisaldab ka manust (faili). Kuna Peeter on hommikust saadik usinalt töötanud, otsustab ta sõbra kirjaja selle manuse kohe läbi lugeda. Ta teab et e-kirjades võib sisalduda ka ohtlikke faile, kuid antud juhul pole see probleem, sest kiri on sõbralt ja Peetri arvates on tööandja arvutis kindlasti turvaprogrammid, mis kahtlased failid kahjutuks teeks. Peeter ei tea täpselt, kas erakirjade lugemise kohta on midagi kirjas mõnes asutuse eeskirjas või juhendis.

8. Kui suureks hindate võimalust, et käituksite selliselt nagu Peeter?

□ Väga suureks □ Pigem suureks □ Ei suureks ega väikeseks
□ Pigem väikeseks □ Väga väikeseks

9. Kui suureks hindate võimalust, et käitub mõni kolleeg selliselt nagu Peeter?

□ Väga suureks □ Pigem suureks □ Ei suureks ega väikeseks
□ Pigem väikeseks □ Väga väikeseks

10. Kas Te käituksite sarnaselt Peetriga, kui teaksite, et selline käitumine on asutuse turvameetmeid sisaldava eekirja või juhendi kohaselt keelatud, kuid selle eest ei ole ette nähtud sankatsioone ja seda ei kontrollita?

□ Jah, käituksin □ Pigem käituksin □ Pigem ei käituks
□ Ei käituks □ Ei oska öelda

11. Kas Te käituksite sarnaselt Peetriga, kui teaksite, et selline käitumine on asutuse turvameetmeid sisaldava eekirja või juhendi kohaselt keelatud ning sanktsioonina on ette nähtud distsiplinaarkaristus (noomitus käskkirjaga)?

□ Jah, käituksin □ Pigem käituksin □ Pigem ei käituks
□ Ei käituks □ Ei oska öelda

12. Kas Te käituksite sarnaselt Peetriga, kui teaksite, et selline käitumine on asutuse turvameetmeid sisaldava eekirja või juhendi kohaselt keelatud ja sanktsioonina on ette nähtud halduskaristus (trahv seoses infoturbe riski tekitamisega)?

□ Jah, käituksin □ Pigem käituksin □ Pigem ei käituks
□ Ei käituks □ Ei oska öelda

13. Kas Te käituksite sarnaselt Peetriga, kui teaksite, et selline käitumine on asutuse turvameetmeid sisaldava eekirja või juhendi kohaselt keelatud ja sanktsioonina on ette nähtud kriminaalkaristus (trahv või vangistus seoses suure infoturbe riski tekitamisega)?

□ Jah, käituksin □ Pigem käituksin □ Pigem ei käituks
□ Ei käituks □ Ei oska öelda

14. Kas Te käituksite sarnaselt Peetriga, kui teaksite, et selline käitumine on asutuse turvameetmeid sisaldava eekirja või juhendi kohaselt keelatud, kuid selle eest ei ole ette nähtud sankatsioone, samas Teie töökaaslased teeksid Teile etteheiteid ja nende suhtumine Teisse halvaneks?

□ Jah, käituksin □ Pigem käituksin □ Pigem ei käituks
□ Ei käituks □ Ei oska öelda

KAASUS 3

Tiina kasutab lõunapausi ajal tööarvutit uudiste lugemiseks internetis. Ta on sirvinud erinevaid veebilehekülgi mõnda aega ning märkab ühel veebilehel huvitavat reklaami. Antud reklaamile vajutades avaneb korraga väga palju erineva sisuga veebilehekülgi. Tiina otsustab kiirelt sulgeda kõik veebileheküljed, kuna need ei tundu talle turvalised. Veebilehekülgi sulgedes aktiveerub aga mingi faili allalaadimise protsess. Tiina katkestab allalaadimise ning sulgeb samuti kõik ülejäänud avanenud veebilehed. Ta eeldab, et suutis allalaadimise protsessi iseseisvalt katkestada ning ei räägi juhtunust kellelegi. Tiina ei tea täpselt, kas selliste juhtumite puhuks on asutuse eeskirjades või juhendites mingeid instruktsioone.

15. Kui suureks hindate võimalust, et käituksite selliselt nagu Tiina?

□ Väga suureks □ Pigem suureks □ Ei suureks ega väikeseks
□ Pigem väikeseks □ Väga väikeseks

16. Kui suureks hindate võimalust, et käitub mõni kolleeg selliselt nagu Tiina?

□ Väga suureks □ Pigem suureks □ Ei suureks ega väikeseks
□ Pigem väikeseks □ Väga väikeseks

17. Kas Te käituksite sarnaselt Tiinaga, kui teaksite, et selline käitumine on asutuse turvameetmeid sisaldava eekirja või juhendi kohaselt keelatud, kuid selle eest ei ole ette nähtud sanktsioone ja seda ei kontrollita?

□ Jah, käituksin □ Pigem käituksin □ Pigem ei käituks
□ Ei käituks □ Ei oska öelda

18. Kas Te käituksite sarnaselt Tiinaga, kui teaksite, et selline käitumine on asutuse turvameetmeid sisaldava eekirja või juhendi kohaselt keelatud ja sanktsioonina on ette nähtud distsiplinaarkaristus (noomitus käskkirjaga)?

□ Jah, käituksin □ Pigem käituksin □ Pigem ei käituks
□ Ei käituks □ Ei oska öelda

19. Kas Te käituksite sarnaselt Tiinaga, kui teaksite, et selline käitumine on asutuse turvameetmeid sisaldava eekirja või juhendi kohaselt keelatud ja sanktsioonina on ette nähtud halduskaristus (trahv seoses infoturbe riski tekitamisega)?

□ Jah, käituksin □ Pigem käituksin □ Pigem ei käituks

□ Ei käituks □ Ei oska öelda

20. Kas Te käituksite sarnaselt Tiinaga, kui teaksite, et selline käitumine on asutuse turvameetmeid sisaldava eekirja või juhendi kohaselt keelatud ja sanktsioonina on ette nähtud kriminaalkaristus (trahv või vangistus seoses suure infoturbe riski tekitamisega)?

□ Jah, käituksin □ Pigem käituksin □ Pigem ei käituks
□ Ei käituks □ Ei oska öelda

21. Kas Te käituksite sarnaselt Tiinaga, kui teaksite, et selline käitumine on asutuse turvameetmeid sisaldava eekirja või juhendi kohaselt keelatud, kuid selle eest ei ole ette nähtud sankatsioone, samas Teie töökaaslased teeksid Teile etteheiteid ja nende suhtumine Teisse halvaneks?

□ Jah, käituksin □ Pigem käituksin □ Pigem ei käituks
□ Ei käituks □ Ei oska öelda

Palun vastata täiendavalt ka järgmistele küsimustele:

22. Teie vanus

□ kuni 20 a □ 21-30 a □ 31-40 a
□ 41-50 a □ 51-65 a

23. Teie sugu

□ Mees
□ Naine

24. Teie teenistusstaaž Häirekeskuses

□ kuni 1a □ 2-5 a
□ 6-10 a □ üle 10 a

LISA 2. PÄÄSTETEENISTUJATE ANKEETKÜSITLUSE TULEMUSED

1. Kui suureks hindate võimalust, et käituksite selliselt nagu Malle?			**2. Kui suureks hindate võimalust, et käitub mõni kolleeg selliselt nagu Malle?**		
Vastuse variant	**Vastajaid**	**%**	**Vastuse variant**	**Vastajaid**	**%**
Väga suureks	20	35,7	Väga suureks	17	30,4
Pigem suureks	16	28,6	Pigem suureks	23	41,1
Ei suureks ega väikeseks	6	10,7	Ei suureks ega väikeseks	8	14,3
Pigem väikeseks	8	14,3	Pigem väikeseks	6	10,7
Väga väikeseks	6	10,7	Väga väikeseks	2	3,6
3. Kas Te käituksite sarnaselt Mallega, kui teaksite, et arvuti lukustamise kohustus on kirjas asutuse turvameetmeid sisaldavas eekirjas või juhendis, kuid selle eest ei ole ette nähtud sanktsioone ja seda ei kontrollita?			**4. Kas Te käituksite sarnaselt Mallega, kui teaksite, et arvuti lukustamise kohustus on kirjas asutuse turvameetmeid sisaldavas eekirjas või juhendis ning selle eest on ette nähtud sanktsioonina distsiplinaarkaristus (noomitus käskkirjaga)?**		
Vastuse variant	**Vastajaid**	**%**	**Vastuse variant**	**Vastajaid**	**%**
Jah, käituksin	4	7,1	Jah, käituksin	2	3,6
Pigem käituksin	6	10,7	Pigem käituksin	1	1,8
Pigem ei käituks	22	39,3	Pigem ei käituks	8	14,3
Ei käituks	22	39,3	Ei käituks	43	76,8
Ei oska öelda	2	3,6	Ei oska öelda	2	3,6
5. Kas Te käituksite sarnaselt Mallega, kui teaksite, et arvuti lukustamise kohustus on kirjas asutuse turvameetmeid sisaldavas eekirjas või juhendis ning selle eest on ette nähtud halduskaristus (trahv seoses oluliste andmete lekkega)?			**6. Kas Te käituksite sarnaselt Mallega, kui teaksite, et arvuti lukustamise kohustus on kirjas asutuse turvameetmeid sisaldavas eekirjas või juhendis ning selle eest on ette nähtud kriminaalkaristus (trahv või vangistus seoses üliolulistе andmete lekkega)?**		
Vastuse variant	**Vastajaid**	**%**	**Vastuse variant**	**Vastajaid**	**%**
Jah, käituksin	1	1,8	Jah, käituksin	1	1,8
Pigem käituksin	1	1,8	Pigem käituksin	1	1,8
Pigem ei käituks	3	5,4	Pigem ei käituks	2	3,6
Ei käituks	50	89,3	Ei käituks	51	91,1
Ei oska öelda	1	1,8	Ei oska öelda	1	1,8

7. Kas Te käituksite sarnaselt Mallega, kui teaksite, et arvuti lukustamise kohustus on kirjas asutuse turvameetmeid sisaldavas eekirjas või juhendis, kuid selle eest ei ole ette nähtud sanktsioone, samas Teie töökaaslased teeksid Teile etteheiteid ja nende suhtumine Teisse halveneks?			**8. Kui suureks hindate võimalust, et käituksite selliselt nagu Peeter?**		
Vastuse variant	**Vastajaid**	**%**	**Vastuse variant**	**Vastajaid**	**%**
Jah, käituksin	3	5,4	Väga suureks	18	32,1
Pigem käituksin	2	3,6	Pigem suureks	19	33,9
Pigem ei käituks	9	16,1	Ei suureks ega väikeseks	4	7,1
Ei käituks	39	69,6	Pigem väikeseks	11	19,6
Ei oska öelda	3	5,4	Väga väikeseks	4	7,1
9. Kui suureks hindate võimalust, et käitub mõni kolleeg selliselt nagu Peeter?			**10. Kas Te käituksite sarnaselt Peetriga, kui teaksite, et selline käitumine on asutuse turvameetmeid sisaldava eekirja või juhendi kohaselt keelatud, kuid selle eest ei ole ette nähtud sankatsioone ja seda ei kontrollita?**		
Vastuse variant	**Vastajaid**	**%**	**Vastuse variant**	**Vastajaid**	**%**
Väga suureks	20	35,7	Jah, käituksin	4	7,1
Pigem suureks	20	35,7	Pigem käituksin	9	16,1
Ei suureks ega väikeseks	1	1,8	Pigem ei käituks	15	26,8
Pigem väikeseks	4	7,1	Ei käituks	26	46,4
Väga väikeseks	1	1,8	Ei oska öelda	2	3,6
11. Kas Te käituksite sarnaselt Peetriga, kui teaksite, et selline käitumine on asutuse turvameetmeid sisaldava eekirja või juhendi kohaselt keelatud ning sanktsioonina on ette nähtud distsiplinaarkaristus (noomitus käskkirjaga)?			**12. Kas Te käituksite sarnaselt Peetriga, kui teaksite, et selline käitumine on asutuse turvameetmeid sisaldava eekirja või juhendi kohaselt keelatud ja sanktsioonina on ette nähtud halduskaristus (trahv seoses infoturbe riski tekitamisega)?**		
Vastuse variant	**Vastajaid**	**%**	**Vastuse variant**	**Vastajaid**	**%**
Jah, käituksin	1	1,8	Jah, käituksin	0	0,0
Pigem käituksin	2	3,6	Pigem käituksin	3	5,4
Pigem ei käituks	4	7,1	Pigem ei käituks	1	1,8
Ei käituks	47	83,9	Ei käituks	47	83,9
Ei oska öelda	2	3,6	Ei oska öelda	5	8,9

13. Kas Te käituksite sarnaselt Peetriga, kui teaksite, et selline käitumine on asutuse turvameetmeid sisaldava eekirja või juhendi kohaselt keelatud, ja sanktsioonina on ette nähtud kriminaalkaristus (trahv või vangistus seoses suure infoturbe riski tekitamisega)?			**14. . Kas Te käituksite sarnaselt Peetriga, kui teaksite, et selline käitumine on asutuse turvameetmeid sisaldava eekirja või juhendi kohaselt keelatud, kuid selle eest ei ole ette nähtud sankatsioone, samas Teie töökaaslased teeksid Teile etteheiteid ja nende suhtumine Teisse halvaneks?**		
Vastuse variant	**Vastajaid**	**%**	**Vastuse variant**	**Vastajaid**	**%**
Jah, käituksin	0	0,0	Jah, käituksin	1	1,8
Pigem käituksin	2	3,6	Pigem käituksin	3	5,4
Pigem ei käituks	1	1,8	Pigem ei käituks	8	14,3
Ei käituks	52	92,9	Ei käituks	40	71,4
Ei oska öelda	1	1,8	Ei oska öelda	4	7,1
15.Kui suureks hindate võimalust, et käituksite selliselt nagu Tiina?			**16.Kui suureks hindate võimalust, et käitub mõni kolleeg selliselt nagu Tiina?**		
Vastuse variant	**Vastajaid**	**%**	**Vastuse variant**	**Vastajaid**	**%**
Väga suureks	10	17,9	Väga suureks	11	19,6
Pigem suureks	22	39,3	Pigem suureks	25	44,6
Ei suureks ega väikeseks	8	14,3	Ei suureks ega väikeseks	10	17,9
Pigem väikeseks	11	19,6	Pigem väikeseks	8	14,3
Väga väikeseks	5	8,9	Väga väikeseks	2	3,6
17.Kas Te käituksite sarnaselt Tiinaga, kui teaksite, et selline käitumine on asutuse turvameetmeid sisaldava eekirja või juhendi kohaselt keelatud, kuid selle eest ei ole ette nähtud sanktsioone ja seda ei kontrollita?			**18. Kas Te käituksite sarnaselt Tiinaga, kui teaksite, et selline käitumine on asutuse turvameetmeid sisaldava eekirja või juhendi kohaselt keelatud ja sanktsioonina on ette nähtud distsiplinaarkaristus (noomitus käskkirjaga)?**		
Vastuse variant	**Vastajaid**	**%**	**Vastuse variant**	**Vastajaid**	**%**
Jah, käituksin	2	3,6	Jah, käituksin	2	3,6
Pigem käituksin	8	14,3	Pigem käituksin	1	1,8
Pigem ei käituks	11	19,6	Pigem ei käituks	3	5,4
Ei käituks	33	58,9	Ei käituks	47	83,9
Ei oska öelda	2	3,6	Ei oska öelda	3	5,4

19.Kas Te käituksite sarnaselt Tiinaga, kui teaksite, et selline käitumine on asutuse turvameetmeid sisaldava eekirja või juhendi kohaselt keelatud ja sanktsioonina on ette nähtud halduskaristus (trahv seoses infoturbe riski tekitamisega)?		
Vastuse variant	**Vastajaid**	**%**
Jah, käituksin	1	1,8
Pigem käituksin	2	3,6
Pigem ei käituks	5	8,9
Ei käituks	47	83,9
Ei oska öelda	1	1,8

20.Kas Te käituksite sarnaselt Tiinaga, kui teaksite, et selline käitumine on asutuse turvameetmeid sisaldava eekirja või juhendi kohaselt keelatud ja sanktsioonina on ette nähtud kriminaalkaristus (trahv või vangistus seoses suure infoturbe riski tekitamisega)?		
Vastuse variant	**Vastajaid**	**%**
Jah, käituksin	1	1,8
Pigem käituksin	0	0,0
Pigem ei käituks	4	7,1
Ei käituks	50	89,3
Ei oska öelda	1	1,8

21.Kas Te käituksite sarnaselt Tiinaga, kui teaksite, et selline käitumine on asutuse turvameetmeid sisaldava eekirja või juhendi kohaselt keelatud, kuid selle eest ei ole ette nähtud sankatsioone, samas Teie töökaaslased teeksid Teile etteheiteid ja nende suhtumine Teisse halvaneks?		
Vastuse variant	**Vastajaid**	**%**
Jah, käituksin	2	3,6
Pigem käituksin	2	3,6
Pigem ei käituks	10	17,9
Ei käituks	41	73,2
Ei oska öelda	3	5,4