Tallinna Ülikool
Informaatika Instituut

Infosüsteemide etalonturbe süsteemi ISKE rakendamise mõju IT riskidele Eesti avaliku sektori näitel

Magistriritöö

Autor: Jurga Baranauskaite

Juhendajad: Andro Kull
Peeter Normak

Tallinn 2014

Autorideklaratsioon

Deklareerin, et käesolev magistritöö on minu töö tulemus ja seda ei ole kellegi teise poolt varem kaitsmisele esitatud. Kõik töö koostamisel kasutatud teiste autorite tööd, olulised seisukohad, kirjandusallikatest ja mujalt pärinevad andmed on viidatud.

....

(kuupäev) *(allkiri)*

Töö vastab magistritööle esitatavatele nõuetele.

Kaitsmisele lubatud ..... …..... 20.... a.

Juhendaja: *Peeter Normak* .....

(allkiri)

.....

(kuupäev)

Juhendaja: *Andro Kull* .....

(allkiri)

.....

(kuupäev)

Lihtlitsents lõputöö reprodutseerimiseks ja lõputöö üldsusele kättesaadavaks tegemiseks

Mina _____ (sünnikuupäev: _____)

(*autori nimi*)

annan Tallinna Ülikoolile tasuta loa (lihtlitsentsi) enda loodud teose:

„Infosüsteemide etalonturbe süsteemi ISKE rakendamise mõju IT riskidele Eesti avaliku sektori näitel“

mille juhendajad on Peeter Normak ja Andro Kull,

säilitamiseks ja üldsusele kättesaadavaks tegemiseks Tallinna Ülikooli Akadeemilise Raamatukogu repositooriumis.

olen teadlik, et punktis 1 nimetatud õigused jäävad alles ka autorile.

kinnitan, et lihtlitsentsi andmisega ei rikuta teiste isikute intellektuaalomandi ega isikuandmete kaitse seadusest tulenevaid õigusi.

Tallinnas, _____

allkiri ja kuupäev

Sisukord

Sissejuhatus

Tänapäevases Eesti Vabariigis on e-teenuste osutamine väga populaarne ning infoturbe mahud kasvavad pidevalt, millest tuleneb nõudmine infoturbe haldamise protsesside korrigeerimiseks ning arendamiseks. Kõige populaarsemateks e-teenusteks võib pidada e-hääletamist, digi-allkirjastamist, e-kooli teenuseid, digi-retseptide väljaandmist jne. Kõigi nende teenuste kasutamiseks nõutakse tugevat infoturbe haldamisüsteemi, mille puudus või puudulikkus suurendab omakorda andmete lekkimise ja kaotsimineku ohtu. Küberrünnakud ja IT-süsteemide rikked on vaid mõned suurematest ohtudest.

Käesoleva magistritöö teemaks on valitud „Infosüsteemide etalonturbe süsteemi ISKE rakendamise mõju IT riskidele Eesti avaliku sektori näitel“. Teema on valitud lähtudes faktist, et ISKE infoturbe halduse süsteemi rakendamine on kohustuslik avaliku sektori asutuste jaoks.

Antud magistritöös on kajastatud valdkonnaks avalik sektor, mis tähendab seda, et peamised andmed ning andmebaasid, mis liiguvad sisevõrkudes, sisaldavad endas kas inimeste (elanike) või riigiasutuste informatsiooni. Nii esimene kui teine andmete liik nõuab konfidentsiaalsust ning turvalisust. Infoturbe eiramisest tulenevad IT-riskid võivad põhjustada suurt kahju ja tuua kaasa palju negatiivseid tagajärgi.

Avaliku sektori asutustele on infoturbe haldamiseks vaja kindlat haldussüsteemi, mis suudaks reguleerida ning kontrollida protsesse. Oma haldussüsteemi väljatöötamiseks oleks iga avaliku sektori asutus pidanud kulutama suuri raha- ja inimressursse ning aega. Seetõttu tuli välja valida infoturbe haldusmetoodika, mida oleks võimalik kohandada Eesti Vabariigi avaliku sektori nõuete ja spetsiifikaga. Kirjeldatud kohandamise protsessi lõpptulemuseks sai infoturbe haldamise kolmeasteline süsteem ISKE. Peamiseks magistritöö eesmärgiks on uurida, kas ISKE infoturbe süsteemi rakendamine Eesti avaliku sektori asutustes vähendab IT-riske ning nende realiseerumise tõenäosust.

Kuna infoturbe rakendamise kohta info andmine eeldab teatud tasemel konfidentsiaalsust, siis on käesolevas töös säilitatud täielik anonüümsus kõikide osalejate kohta.

1. Töös kasutatud metoodika

Peamiseks töös rakendatud hüpoteesiks on väide, et infoturbe haldussüsteemi ISKE rakendamine avaliku sektori asutustes aitab IT-riskide realiseerumise tõenäosust vähendada. Käsitletud hüpoteesi tõele vastavuse uurimiseks kasutati töös kahte meetodit, millest üks oli teoreetilise ja teine praktilise taustaga.

Uurimistöö käigus viidi läbi küsitlus avaliku sektori asutuste töötajate seas ja tehti teoreetiline riskide analüüs, mis tugines ISKE rakendamisega kaasnevate ohtude ja meetmete kataloogide analüüsile. Lisaks kasutati teoreetilises analüüsis Lansdowne ja Kendricki riski hindamise skaalasid ja üldise riskifaktori arvutamise valemi kasutamise tulemusi.

Esimeseks tööetapiks oli teoreetilise analüüsi läbiviimine (vt. p.5 ISKE ohtude ja meetmete teoreetiline analüüs), mis andis ülevaate Infosüsteemide Kolmeastmeline Etalonturbe Süsteemi kataloogides nimetatud ohtudest, rakendamiseks soovitatud meetmetest ning nende analüüsist. Teoreetilise uuringu valim koostati ISKE ohtude kataloogist (Infosüsteemide Kolmeastmeline Etalonturbe Süsteem, Ohtude kataloog ver. 7.00, 2014) võetud ohtudest ja ISKE meetmete kataloogis (Infosüsteemide Kolmeastmeline Etalonturbe Süsteem (ISKE). Meetmete kataloog ver. 7.00, 2014) olevatest vastavatest meetmetest. Igast ohugrupist oli valitud 5 ohtu, et analüüsida mitte ainult IT-valdkonnaga seotud ohusid, vaid ka teisi ISKE poolt kajastatud ohtude valdkondi.

Eelkirjeldatud ohtude ja meetmete analüüs teostati, võttes aluseks tänapäevase olukorra avaliku sektori asutustes. ISKE ohtude kataloogist võetud ohtude realiseerumise tõenäosuse hindamiseks kasutati ka Lansdowne ja Kendrick riski hindamise skaalat. See aitas võrrelda teoreetilise analüüsi tulemusi (kasutades üldist riskifaktorit) ohtude tõenäosuse hindamiseks enne ja pärast ISKE meetmete rakendamist. Kõikide ohtude ja meetmete rakendamine ning hindamine teostati antud analüüsi osas teoreetiliselt.

Teoreetilise analüüsi peamisteks eelisteks on:

1) ISKE ohtude kataloog annab põhjaliku ülevaate kõikidest potentsiaalsetest ohtudest, mis on kajastatud ISKE rakendamise protsessi käigus.

2) ISKE meetmete kataloog annab ülevaate kõikidest rakendamiseks soovitatud meetmetest, mis on struktureeritud vastavalt ISKE ohtude kataloogile. Teoreelitise analüüsi käigus oli võimalik hinnata, kas soovitatud meetme rakendamine oli piisav ohu realiseerumise tõenäosuse vähendamiseks või vastupidi, meetme rakendamine ei mõjutanud ohu realiseerumise tõenäosust.

3) Riski hindamine Lansdowne ja Kendrick süsteemi järgi näitab Üldist riskifaktorit enne ISKE-s soovitatud meetme rakendamist ja peale selle rakendamist. Nende kahe koefitsiendi võrdlemine peegeldas meetme mõju ohu realiseerumise tõenäosusele.

Osutus võimalikuks teha järeldusi, kas rakendamiseks soovitatud meetmed on piisavad rakendamiseks Eesti Vabariigi avaliku sektori asutustes või on soovitatud meetmed puudulikud.

Teiseks töös kasutatud metoodiks oli kvalitatiivne uuring, mis teostati küsitluse läbiviimisega avaliku sektori asutustes. Kasutatud küsimustik (vt. Lisa 1) oli koostatud lähtudes töös püstitatud hüpoteesist ning eesmärgist ja selle tõestamiseks või ümberlükkamiseks vajaliku informatsiooni saamiseks. Samas pidi küsimustiku vastajatele olema tagatud absoluutne anonüümsus, seega olid küsimused koostatud sellisel viisil, et küsitluses osalevate avaliku sektorite asutuste tuvastamine osutuks võimatuks.

Küsitlus koosnes üheksast küsimusest (vt. Lisa 1) ning oli saadetud 50 avaliku sektori asutustele. Asutuste valim oli koostatud juhusliku valiku alusel, kasutades Riigi Infosüsteemi haldussüsteemi andmebaasi (Riigi Infosüsteemi haldussüsteem, 2014).
Küsitluse läbiviimise meetodi rakendamise eelised on:

1) Võimalus vaadata reaalset olukorda avaliku sektori asutustes ISKE rakendamisega seoses
2) Saada hinnangut ISKE rakendumise kohta avaliku sektori töötajatelt
3) Saada ülevaade peamistest ISKE rakendamise positiivsetest ja negatiivsetest aspektidest
4) Saada ülevaade avaliku sektori töötajate isikliku arvamuse kohta ISKE rakendamise otstarbekusest
5) Teostada analüüsi ja selle põhjal teha järeldusi ja soovitusi edaspidise ISKE rakendamise kohta avaliku sektori asutustes

Esimene osa küsitluse vastustest oli kodeeritud ning tulemusi analüüsiti lähtudes vastuste protsentuaalsest osakaalust. Teine osa küsimustest oli avatud vastustega, milles vastajad avaldasid oma arvamusi, mille järgi oli võimalik teha vastavaid järeldusi (vt. p.6 Praktiline uuring). Mõlemad küsitluse analüüsi meetodid andsid võimaluse kontrollida töös püstitatud hüpoteesi. Lähtudes saadud vastustest, nende analüüsist ja hüpoteesi kinnitamise tulemustest, pakuti välja võimalused küsitluse tulemuste edasiseks kasutamiseks ja jagati soovitusi edasiste uuringute tegemiseks.

Käesoleva magistritöö raames on analüüs ja hindamine teostatud nii teoreetiliselt, kasutades ISKE kataloogide analüüsi, kui ka lähtudes praktilise küsitluse tulemustest – vaadates väljapakutud hüpoteesi tõestamist või tõestamata jätmist ning analüüsitud ISKE rakendamise mõju IT-riskide realiseerumise tõenäosusele.

2. Riskide olemusest

Riskid mängivad väga olulist rolli ettevõtete strateegilises planeerimises ja igapäevastes protsessides, sest mida paremini on tehtud riskide analüüs ning mida kvaliteetsem on riskide haldamise plaan, seda suurem on tõenäosus, et ettevõtted täidavad edukalt oma strateegilist plaani ja püstitatud eesmärke. Riskijuhtimise protsess eeldab strateegilist olulisust enamikelt organisatsioonidelt ning planeerib tegevussuuna kava, eesmärgiga vähendada sündmuse esinemise tõenäosust ja/või selle minimeerimist või sisaldab selle sündmuse tagajärgede mõju. (Keith, 1992)

2.1 Riskide käsitlemise määravad faktorid

Risk on tõenäosus, et oht kasutab turvaauke varades või varade grupis ja seeläbi kahjustab organisatsiooni (ENISA, 2006) ja seoses sellega on IT-riskide juhtimine tänapäeval üks kesksetest küsimustest infosüsteemide (IS) juhtimises. IT-riskide juhtimise eesmärgiks on kaitsta IT varasid, näiteks andmeid, riistvara, tarkvara, personali, ning vahendeid erinevate väliste (nagu loodusõnnetused) ja sisemiste (nt tehnilised rikked, sabotaaž, autoriseerimata juurdepääs) ohtude eest, sellisel moel, et minimiseerida realiseerunud ohu kahjumist tulenevad kulud. (Gottfried, 1989)

Riske määratlevad ka erinevad põhiaspektid (Keith, 1992)**:**

1) Identiteet (ingl. k. Identity): Kuvand, Teenused
2) Jätkuvus (ingl. k.Continuity): Äri jätkumine
3) Jätkusuutlikkus (ingl. k. Sustainability): Efektiivne ressursside kasutamine, moraalse kulumise ning liiasuse vähendamine
4) Kohanemisvõime (ingl. k. Adaptability): Õigus muutuseks
5) Vastutus (ingl. k. Responsibility): Kohustus hoolitseda töötajate eest, mõju keskkonnale
6) Rakendatavus (ingl. k. Viability): Alternatiivkulud

Iga faktori osakaal ettevõtte tegevuses ongi otsustav aspekt riskide määratlemise suunas. See on ka kasutatud riskide raamistiku või hindamisskaala määrajaks. *(ibid.)*

2.2 Levinumad IT-riskid ja nende määratlemine

Peamised riskid, mis vajavad kõige rohkem tähelepanu IT-spetsialistide poolt, toodi välja Vicky Haney uuringu tulemustes, kus olid kokku pandud praktilised teadmised ning IT-tippjuhtide intervjuudest saadud järeldused. Kümneks peamiseks universaalriskiks tarkvaraprojektides olid (Haney, 2009):

1) Sihtkasutaja ebapiisav kaasamine
2) Vähene täidesaatev tugi
3) Nõuete inflatsioon
4) Planeerimise vead
5) Ebarealistlikud ootused
6) Personalivoolavus
7) Ebapiisav projektijuhtimine
8) Klassifitseerimise viga
9) Vale tehnoloogia või ebakindlus selle kasutamisel
10) Teadmatus olulisusest

Tuginedes ülaltoodud riskide nimekirjale, on kõige tähtsamaks IT-riskijuhtimises riskide õige määratlemine ehk nende spetsifikatsioon. *(ibid.)*

2011. aastal teostati AICPA poolt suur uuring "22 Top Technology Initiatives (TTI)". Läbiviidud uuringu raames sertifitseeritud IT-spetsialistel (*Certified Information Technology Professionals*) ning vannutatud raamatupidajatel (*Certified Public Accountants*) paluti järjestada tänapäevased infotehnoloogilised küsimused tähtsuse järjekorras. Uuringu tulemused pidid näitama kõige olulisemaid probleeme IT-riskijuhtimise valdkonnas ning võimalikke tulevaste probleemide suundi. (Information Systems Audit and Control Association (ISACA), 2011)

Uuringu tulemustele lisati hinnangud IT küsimustest. Kui osalejaid paluti hinnata IT-probleeme, pöörati enim tähelepanu:

1) IT kaitse [78%]

2) Rist- ja tarkvara talitlushäire [63%]
3) Voolukatkestus [50%]
4) Füüsiline kaitse [40%] *(ibid.)*

Uuringu tulemuste kokkuvõtteks on see, et IT-riskide küpsuse kontroll ja hindamine viib tõhusa riskijuhtimiseni. Uuringu järgi nõuab praegune olukord objektiivset hindamist IT-riskide küpsuse osas ning tulemuste analüüsile järgnevateks soovitusteks olid:

1) Määrata IT riskide küpsus objektiivselt
2) Töötada välja multi-funktsionaalne plaan kõikide riskikategooriate jaoks (andmed, kaitse, taastamine ja uus IT)
3) Käsitleda kõiki riske ning teha plaan iga kategooria jaoks eraldi
4) Leida riskide haldajad tippspetsialistidest juhtide hulgast
5) Määratleda riskileevendusest tekkiv kasu iga riski korral.

Identifitseeriti ka suuremaid muudatusi vajavad suunad IT riskides, millisteks olid: 1) IT riskide planeerimine toimub rangetes raamides (48%); 2) Formaalse Riskijuhtimise osakonna loomine [41%]; 3) Proaktiivne vs reaktiivne käitmine [38%]. *(Ibid..)*

3. IT-riskide juhtimine

Ettevõtte riskijuhtimine (ingl. k. Risk Management) hõlmab kõiki riskide analüüsi ning haldamisega seonduvaid tegevusi. (Keith, 1992)

Riskijuhtimist võib iseloomustada kui protsessi, mille eesmärgiks on mõistliku tasakaalu saavutamine ettevõtte kasumi ja turvariskide realiseerimisest tekkiva võimaliku kahju vahel. Riskijuhtimine on lahutamatu ja oluline osa üldisest juhtimisest ning peab olema lõputu protsess, mis toetab pidevat otsustusprotsesside täiustamist ja tulemuslikkuse parandamist. Infoturbe (ingl. k. Information Security) riskijuhtimine võib olla osa organisatsiooni laiemast riskijuhtimise protsessist või iseseisvalt teostatud protsess. Kuna infotehnoloogia ja eriti infoturbe vahendid ning tehnoloogiad on pidevas muutumises, siis on soovitatav käsitleda IT-riskijuhtimist organisatsioonisiseselt alaliselt iseseisva protsessina. (ENISA, 2006)

3.1 IT-riskijuhtimise olulisus ja etapid

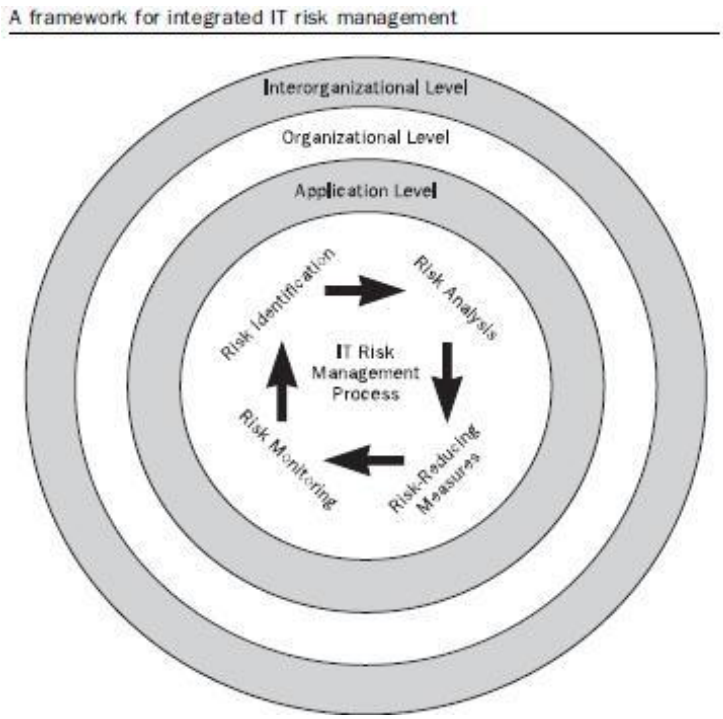
IT-riskijuhtimine annab ettevõtetele võimaluse vältida riskide mittetuvastamist ning aitab võtta vastu kiireid meetmeid käsitlemaks esinenud riske. IT-riskide prioritiseerimise ja haldamise protsessis on kõige olulisemateks aspektideks (Fraser, Simkins, 2010):

1) Võimalik riskide maandamise mõju sidumine tuludega
2) Vajalike liiasuse, varundamise ning säilitamise tasemete ehitamine
3) Pidev jälgimine, et märgata kiiresti probleemi ning võtta tarvitusele vastumeetmed
4) Informatsiooni jagamine ning selle edastamine esimesele astmele

Nagu igas protsessis, võib ka peamised riskijuhtimise etapid jagada neljaks põhietapiks (Keith, 1992):

1) Identifitseerimine*:* Tuleb kasutada erinevaid meetodeid selleks, et välja selgitada kõik ettevõtet ohustavad riskide vormid
2) Analüüs*:* Hinnata võimalike ohtude tõenäolist sagedust ja tõsidust

3) Kontroll*:* Kasutada füüsilisi meetmeid ja/või personali koolitamist, et vähendada või kõrvaldada ohte ja nende majanduslikke tagajärgi
4) Riski finantseerimine*:* Kuna riske ei saa kunagi täielikult välistada, on vaja planeerida võimaliku kahjumi rahastamist kas kindlustus- või töötamisvahenditega



Joonis1. (*Bandyopadhyay, Mykytyn, Mykytyn, 1999)*

Ülaltoodud Joonis 1. (Bandyopadhyay, Mykytyn and Mykytyn, 1999) tõestab visuaalselt väidet, et nimetatud etapid on üksteisest sõltuvad ning ükski etapp ei saa olla IT-riskijuhtimise protsessist välja jäetud. (ENISA, 2006)

3.2 IT-riskide hindamine

Riskide hindamine on üks esimestest sammudest riskijuhtimises ja see paneb aluse järgmistele etappidele. Õige riskide hindamine tagab efektiivse riskide juhtimise (Tchankova, 2002). Edaspidi on toodud näited riskide hindamise meetoditest.

LANSDOWNE RISKI HINDAMISE SKAALA

Kõige esimesena tõi riskide hindamise 5-punktilise skaalal välja Lansdowne ning tema poolt on loodud 5 põhilist riskide hindamise taset (Lansdowne, 1999):

1) Kriitilised riskid (viis punkti) – põhjustavad programmi läbikukkumise
2) Tõsised riskid (neli punkti) – põhjustavad suuri kulusid või ajakava nihkeid ning teisejärguliste nõuete mitte-täitmist
3) Kesktaseme riskid (kolm punkti) – põhjustavad mõõdukaid kulude suurenemisi ja ajakava nihkeid; olulisemad nõuded on täidetud
4) Alamriskid (kaks punkti) – põhjustavad ainult väikeseid kulude suurenemisi ja ajakava nihkeid
5) Väheolulised riskid (üks punkt) – ei avalda mingit tegelikku mõju ajakavale või kuludele

Lansdowne skaala järgi on iga risk vaadeldud kui sõltumatu muutuja projekti raames. (Cervone, 2006)

KENDRICKi RISKI HINDAMISE SKAALA

Teisena avaldas oma nägemuse riskide hindamisest Kendrick, tema käsitles kolmetasemelist skaalat riskide hindamiseks (Kendrick, 2003):

1) Kõrge tõenäosus (viis punkti) – pigem ilmnev, tõenäosusega 50% ja rohkem
2) Keskmise tõenäosus (kolm punkti) – pigem mitte-ilmnev, tõenäosusega 10% kuni 50%
3) Madal tõenäosus (üks punkt) – väga väike võimalus ilmnemiseks, tõenäosusega 10% ja vähem

Skaalas peamine rõhk on suunatud riskide realiseerumise tõenäosuse hindamisele. *(ibid.)*

KOMBINEERITUD RISKIDE HINDAMISE SKAALA

Kolmandas käsitluses on lisatud riskide eristamine, mis on loodud põhinedes unikaalsele ja lihtsale otsustuspõhisele Kendrick'u mudelile (Kendrick, 2003). Sellega pakutakse täiendavat

seisukohta, mille järgi on eesmärgiks hinnata ohu mõju kogu projekti raames. (Cervone, 2006)

Nendeks kolmeks eristamise vormiks on *(ibid.)*:

1) Tugev mõju (üks punkt) – projekti objektid on riskisurve all, risk põhjustab olulisi muudatusi projekti mahtudes, ajakavas või ressurssides
2) Keskmine mõju (kolm punkti) – projekti objektid on kättesaadavad, kuid vaja on olulist ajakava nihet.
3) Nõrk mõju (viis punkti) – ei toimu olulisi muudatusi projekti plaanides, riskid ei ole olulised või on mõõdetavad väikese ületundide mahuga

Selleks, et klassifitseerida riski ühte ülaltoodud dimensiooni, saab iga riski väärtust määrata kasutades all toodud valemit *(Ibid.)*:

Üldine riskifaktor= (Tõenäosus * Mõju) / Eristamine

Saadud üldine riskifaktor aitab edaspidises riskide hindamise analüüsis võrrelda riskifaktorite muutumist.

3.3 Peamised kasutatavad IT-juhtimises standardid ja raamistikud

Antud peatükkis antakse ülevaade IT-Riske käsitlevatest raamistikest (COBIT, ITIL ja Prince2), rahvusvahelisest standardist (ISO) ja infoturbe haldussüsteemist (ISKE), mis on seotud IT-riskijuhtimisega.

Control Objectives for Information and Related Technology (COBIT) on raamistik, mis on loodud ISACA poolt. See on toetustööriist, mis aitab juhtimisel seostada ning vahet teha kontrolli nõuetel, tehnilistel küsimustel ja äririskidel. COBIT identifitseerib riski kui potentsiaalset mõju organisatsiooni eesmärkidele, mis on tingitud planeerimata sündmustest, on tuvastatud, analüüsitud ja hinnatud. Võetakse vastu nende maandamise strateegiad, et vähendada allesjäänud riske aktsepteeritava tasemeni ja et sidusrühmad saaksid alandada riskid vastuvõetava tasemeni. (Control Objectives for Information and Related Technology (COBIT 4.1), 2007)

Projects in Controlled Environments version 2 (PRINCE2) on projektijuhtimise meetod, mille järgi saab luua raamistiku teatud projektijuhtimisele. PRINCE2 on fokuseeritud

ärimudelile, mis kirjeldab projektide ratsionaalsust ja ärilist põhjendatust. Ärimudel hõlmab kogu projektijuhtimise protsessi, selle algetapist lõppetapini. Riske käsitletakse tähtsate teguritena, mida tuleb projektijuhtimise käigus arvestada. Riski võib määratleda kui ebakindlust tulemustes (kas positiivne võimalus või negatiivne oht). Osa riske on projekti eesmärkide saavutamise protsessis vältimatud. Raamistik ei käsitle spetsiifiliselt IT-riske, kuid on ka IT-riskide puhul hästi rakendatav (Projects in Controlled Environments version 2, 3rd Edition, 2002)

The Information Technology Infrastructure Library (ITIL) on kogumik IT-teenuste juhtimisest (ingl. k. IT service management - ITSM), mis on suunatud IT-teenuste ühilduvusele sõltuvalt ärivajadustest. ITIL v3. versioonis hinnatakse riski kui võimalikku sündmust, mis võib põhjustada kahjumit või mõjutada eesmärkide saavutamist. Riski mõõdetakse ohu ilmnemise tõenäosuse või varade ohuvastuvõtlikkuse järgi ning üldist mõju mõõdetakse riski realiseerumise järgi (Information Technology Infrastructure Library (ITIL), v3, 2007)

International organization for standartization (ISO) **20000** on esimene rahvusvaheline standard IT-teenuste juhtimises. Seda rakendati 2005. aastal ISO/IEC JTC1 SC7 poolt ning muudeti 2011. aastal. ISO/IEC 20000-1:2011 (1 osa) sisaldas endas ka disaini, ülemineku-, tarne- ja teenuste parandamist, mis täidab teenuste nõudeid ning on väärtuslik nii kliendile kui ka teenusepakkujale. ISO standardis on riske käsitletud kui funktsioone varaobjektidest, ärimõjudest, ohtudest ja haavatavuse tõenäosusest. ISO määratleb igaüht nendest ja selgitab, kuidas see mõjutab varasid riski hindamise ajal. (International Organization for Standardization , ISO20000, 2011)

Eesti avalikus sektoris rakendamiseks kohustuslik **Infosüsteemide kolmeastmeline etalonturbe süsteem** (ISKE)**,** mille väljatöötamisel ja arendamisel on aluseks võetud Saksamaal BSI-s (saksa k. Bundesamt für Sicherheit in der Informationstechnik, inglise k. Federal Office for Information Security) loodud infoturbe standard – IT Baseline Protection Manual. (Infosüsteemide Kolmeastmeline Etalonturbe Süsteem (ISKE), 2014)

ISKE rakendamise eesmärk on tagada infosüsteemides töödeldavatele andmetele piisava tasemega turvalisus. Süsteem on loodud eelkõige riigi ja kohaliku omavalitsuse andmekogude pidamisel kasutatavatele infosüsteemidele ning nendega seotud infovaradele turvalisuse tagamiseks. *(ibid.)*

Järgmises peatükis antakse lähem ülevaade ISKE Eesti avalikus sektoris rakendamise kohta.

4. ISKE rakendamine Eesti avalikus sektoris

Infoturve on üks peamistest avaliku sektori asutuste tegevuse protsessidest. Kõik infoturbega seotud protsessid peavad olema kontrollitud ning järjestatud, kuna infoturbepoliitika sõnastab ideaalset infoturbe olukorda ja kaasnevaid kohustusi selle eesmärgi saavutamiseks. (Haar, Solms, 1993)

Eesti avaliku sektori infoturbe haldamise aluseks võeti IT-Grundschutz metodoloogia. The IT-Grundschutz Methodology on BSI metoodika infoturbe efektiivse juhtimise jaoks, mis on kergesti adopteeritav erinevate tegevusaladega asutustes: „Nõuetele vastavat infoturbe taset on võimalik saavutada ja säilitada vaid kõigi asjaosaliste kaasatusega ning efektiivsuse kontrollimise eelduseks on süstemaatiline tegutsemisviis.“ (Infosüsteemide Kolmeastmeline Etalonturbe Süsteem (ISKE), 2014)
Antud otsuse tegemiseks tõi Toomas Viira oma ISKE teemalises presentatsioonis välja järgmised põhjused (Viira, 2010):

1) IT-Grundschutz metoodika regulaarne uuendamine
2) Ei ole vajadust aeganõudva riskihinnangu jaoks
3) Terviklik kaitsemeetmete kogum
4) Sobiv detailsus
5) IT-Grundschutz metoodika võimaldab jagada IT-valdkonna arenguinvesteeringuid vastavalt erinevate tasandite vajadustele
6) Võimaldab välja töötada ühist arusaama avaliku sektori asutuste infosüsteemide jaoks vajaliku infoturbe turvatasemest

ISKE loomise käigus tagati kõik ülalnimetatud põhimõtted, mis aitavad tegeleda igapäevase infoturbe haldamisega ning juhtida efektiivselt kontrolliprotsesse kõikidel tasanditel (ISKE, 2014):

1) ISKE rakendamise peamiseks eesmärgiks on tagada infoturbe haldamise protsesside vastuvõetav tase ning kaitse, rakendades kindlalt organiseeritud protsesside käivitamist

2) Nõutav turvalisuse tase teostatakse läbi info, organisatsiooniliste ja tehniliste turvastandardite sisseviimise
3) Kokku on kolm turvataset, mida saab rakendada avaliku sektori asutustes: L- madal, M- keskmine, H- kõrge

Seega, ISKE infoturbe haldussüsteem paneb paika kõik infoturbega seotud protsessid ning aitab neid reguleerida ja järelvalvet teostada. Tänu pidevale uuendamisele ja arengule saab ISKE infoturbe haldussüsteemi kaudu hallata suuremat osa infoturbe protsessidest.

Vastavalt Eesti Vabariigi Valitsuse määrusele nr. 273 "Infosüsteemide turvameetmete süsteemi kehtestamine" (Eesti Vabariigi Valitsus, 2004) määrati ISKE infoturbe haldussüsteem kohustuslikuks kõikidele avaliku sektori asutustele, mis puutuvad kokku andmeregistrite ning andmebaasidega: „**§2.** Turvameetmete süsteemi rakendamine. Turvameetmete süsteemi rakendamine seisneb infoturbe eesmärkidele vastavate turvaklasside määramises ja nendele vastavate turvameetmete valimises vastavalt infosüsteemide kolmeastmelise etalonturbe süsteemi (edaspidi ISKE) rakendamisjuhendile." *(ibid.)*

ISKE infoturbe süsteemi rakendamise kontrolli eest ning ISKE pideva arendamise ja täiendamise eest oli vastutav Riigi Infosüsteemide Arenduskeskus: „**§13.** ISKE rakendamisjuhendi ajakohasuse tagamine. Etalonmeetmete ajakohasuse tagamiseks viib Riigi Infosüsteemide Arenduskeskus iga aasta 1. jaanuariks läbi ISKE ajakohasuse kontrolli ning teeb selles vajadusel muudatusi." *(ibid.)*

4.1 ISKE rakendamise vajadus avaliku sektori asutustes

Eesti Vabariigi avalik sektor on praegu kolmeastelise infoturbe süsteemi rakendamise keskteel. Tuginedes eelmises osas mainitule, on ISKE rakendamine kohustuslik avaliku sektori asutustele ning iga asutuse ISKE rakendamise taset saab avalikult kontrollida Riigi Infosüsteemi haldussüsteemis (Riigi infosüsteemi haldussüsteem, 2014). Tuginedes antud magistritöö raames püstitatud eesmärgile analüüsida, kas ISKE rakendamine avaliku sektori asutustes vähendab IT-riske ja mõjutab nende realiseerumise tõenäosust, vaadeldakse antud osas kahte reaalset juhtumit, kus ISKE inforturbe haldussüsteemi protsesside rakendamine aitas kõrvaldada toimunud rünnakuid ja ennetada nende levimist.

#OpIndependence rünnak

Viimase kahe aasta kõige tähelepanuväärsemaks juhtumiks võib nimetada 2013. aasta novembris toimunud #OpIndependence rünnakut Euroopa avaliku sektori asutustele: „2013. a novembri alguses korraldasid häktivistid, Anonymous Ukraine maski taha peitudes, paralleelselt NATO õppustega kampaania #OpIndependence. Ründed sisaldasid nii hajusaid teenusetõkestusi, näotustamisi kui ka võltskirjade saatmist mitmes Euroopa riigis.“ (Riigi Infosüsteemi Amet, 2013)

Nagu selgub Riigi Infosüsteemi Ameti ametlikust CERT-EE raportist (Riigi Infosüsteemi Amet, 2013), ei saanud antud juhtumis Eesti avaliku sektori asutused eriti kannatada ning tänu kiirele reageerimisele oli kahjulik mõju minimaalne ja tagajärjed kõrvaldati kiiresti: „Olulist kahju rünnetest Eesti riigiasutuste ja ettevõtete infosüsteemidele ei sündinud. Rünnatud veebilehtede kättesaadavuses esinenud mõnetunniste katkestuste mõju oli väike.“ *(ibid.)*

Kõikidesse asutustesse saadeti võimaliku ründe hoiatus ning võimalikke rünnakuga seotud kirjasid käsitleti vastavalt protseduuridele. CERT-EE raportist tuleb selgelt välja, et igas asutuses peab olema rakendatud vastav infoturbe haldussüsteem, mis ongi otseselt seotud ISKE rakendamisega kõikides avaliku sektori asutustes: „Rakendada asutusele sobilik infoturbe juhtimise raamistik.“ (RIA CERT-EE raport, 2013)

Peale rünnaku kõrvaldamist mainiti raportis soovitusi avaliku sektori asutustele *(ibid.)*:

1) Propageerida SPFi (*sender policy framework* - e-posti saatja kontrollimise raamistik) rakendamist e-posti serverites ja oma internetidomeenides
2) Tegeleda veelgi intensiivsemalt tarkvara uuendamise vajalikkuse selgitamisega, kaaluda sanktsioonide kehtestamist pikka aega uuendamata süsteemide omanike suhtes
3) Kasutada rünnetest saadud õppetunde õppuste korraldamisel
4) Tagada, et asutuse infosüsteemide eest vastutavate spetsialistide hulk ja oskused oleksid vastavuses sellega, kui suurel määral on asutuse/ettevõtte töö nendest infosüsteemidest sõltuv

Antud soovitused näitasid selgelt ISKE täies mahus rakendamise vajadust ning selle pidevat ülevaatamist, kontrolli ning arendamist kogu avalikus sektoris. *(ibid.)*

CryptoLocker juhtum

Teine tähelepanuväärne juhtum, mis peegeldab vajadust ISKE infoturbe haldussüsteemi rakendamise järgi avalikus sektoris, toimus Eestis 2014. aasta jaanuaris. Tegu oli CryptoLocker programmiga: „Eestisse jõudis pahavara, mis muudab andmed püsivalt loetamatuks“ (Riigi Infosüsteemi Amet, 2014). Ülevaade antud juhtumist on postitatud Riigi Infosüsteemi Ameti veebilehel ning pahavara toimimise põhimõtteks oli see, et ta „muudab andmed loetamatuks ning lahtikrüpteerimise eest nõutakse bitimünte, raha MoneyPaki või teiste sarnaste teenuste kaudu.“ *(ibid.)*

Siiamaani pole leitud lahendust andmete taastamiseks, kuid selle probleemiga tegeletakse rahvusvahelisel tasemel. Eestisse jõudis antud pahavara alles 2014. aastal ning seoses sellega peavad kõik avaliku sektori töötajad jälgima infoturbe ning infojulgeoleku protseduure ning reegleid *(ibid.)*:

1) Mitte vajutada kahtlastele linkidele/failidele jne
2) Kahtlaste meilide/failide saamisel kohe pöörduda IT-spetsialistide poole
3) Kui arvuti on kahjustatud, lülitada see välja kõikidest võrkudest ning kontakteeruda IT-spetsialistidega

Nimetatud reeglid peegelduvad samamoodi ISKE protseduurides ning kui vastav infoturbe haldussüsteem on asutuses rakendatud, jälgides sisseviidud protseduure, saavad töötajad käituda vastavalt ning minimiseerida võimalikke riske.

5. ISKE ohtude ja meetmete teoreetiline analüüs

Antud osa magistritööst on pühendatud ISKE-ga kaasnevatele ohtudele, vastavate meetmete rakendamisele ning meetmete vastavusele Eesti Vabariigi avaliku sektori nõuetega. Analüüsi peamiseks eesmärgiks on välja tuua, millised soovitatud meetmed ohtude ennetamiseks ei ole rakendatavad Eesti Vabariigi avaliku sektori asutustele ja millised on kohandatud avaliku sektori nõudmistega ning vastavad vajadustele.

Võib eeldada, et meetmete nimekiri pole täielik ja vajab pidevat ülevaatamist ning täiendamist. Kuna kontrolli teostatakse ainult rakendatud meetmete alusel, peaks edaspidistes uuringutes analüüsima kõiki rakendamiseks soovitatud meetmeid ning nende kasutatavust.

Samas vaadeldakse ka analüüsis nimetatud ohtude vastavust Eesti Vabariigi avaliku sektori nõuetele ning ohtude realiseerumise tõenäosust Eesti Vabariigi kontekstis.

Praeguses ISKE infoturbe haldussüsteemi ohtude kataloogis on võimalikud ohud jagatud viieks grupiks (ISKE Ohtude kataloog, 2014):

G1: Vääramatu jõud

G2: Organisatsioonilised puudused

G3: Inimvead

G4: Tehnilised rikked ja defektid

G5: Ründed

Teoreetilise analüüsi jaoks koostati valim, mis koosnes random-valiku järgi kõikidest viiest ohugrupist. Kokku oli valitud viis ohtu igast grupist, seega analüüsiti 25 ohtu erinevatest gruppidest. Igast eelpool nimetatud võimalike ohtude gruppist valiti teoreetilise analüüsi jaoks välja allolevad ohud (ISKE Ohtude kataloog, 2014):

1. **G1: Vääramatu jõud**
    - G1.1 Personali väljalangemine
    - G1.2 IT-süsteemi avarii

- G1.5 Vesi
- G1.6 Kaablite süttimine
- G1.9 Tugevast magnetväljast tingitud andmekadu

2. **G2: Organisatsioonilised puudused**
    - G2.1 Reeglite puudumine või puudulikkus
    - G2.3 Puuduvad, puudulikud või ühildamatud ressursid
    - G2.4 Turvameetmete ebapiisav järelevalve
    - G2.6 Volitamata pääs ruumidesse
    - G2.8 Ressursside kontrollimatu kasutamine
3. **G3: Inimvead**
    - G3.1 Andmete konfidentsiaalsuse või tervikluse kadu kasutaja vea tõttu
    - G3.2 Seadme või andmete hävitamine hooletuse tõttu
    - G3.4 Lubamatud kaabliühendused
    - G3.5 Liinide juhuslik kahjustamine
    - G3.7 Käsitsemisvea tõttu tekkinud kodukeskjaama (PBX) rike
4. **G4: Tehnilised rikked ja defektid**
    - G4.2 Sisevõrkude katkestus
    - G4.3 Turvavahendi tõrge
    - G4.5 Läbikoste
    - G4.80 Bluetooth'i ebausaldusväärsed või puuduvad turvamehhanismid
    - G4.9 Sisemise toiteallika tühjenemine
5. **G5: Ründed**
    - G5.2 Andmete või tarkvara manipuleerimine
    - G5.3 Volitamatu sisenemine hoonesse
    - G5.5 Vandalism
    - G5.7 Liini pealtkuulamine
    - G5.9 IT-süsteemide volitamata kasutamine

Kõik ohud ja meetmed, mida analüüsiti teoreetilises uuringus, on võetud Riigi Infosüsteemi Ameti kodulehel (Riigi Infosüsteemi Amet, 2014) asuvast ISKE ohtude kataloogist (versioon 7.00) ning ISKE Meetmete kataloogist (versioon 7.00).

Iga eelpool mainitud ohu kohta on välja toodud vastav viis selle ennetamiseks ning kontrollimiseks ehk meetmed, mis peavad olema rakendatud infoturbe haldussüsteemi ISKE järgi.

Lisaks sellele hinnatakse kõik ohud eelnevalt esitletud hindamisskaala järgi (vt. 3.2.IT riskide hindamine), mille valemiks on:

Üldine riskifaktor = (Tõenäosus * Mõju) / Eristamine *(Cervone, 2006)*

Muutujaid hinnatakse järgmiste parameetrite järgi:

Tõenäosus (Kendrick, 2003):

1. Kõrge tõenäosus	5 punkti	Pigem ilmnev, tõenäosusega 50% ja rohkem
2. Keskmise tõenäosus	3 punkti	Pigem mitte-ilmnev, tõenäosusega 10% kuni 50%
3. Madal tõenäosus	1 punkt	Väga väike võimalus ilmnemiseks, tõenäosusega 10% ja vähem

Mõju (Lansdowne, 1999):

1. Kiitilised riskid	5 punkti	Põhjustavad programmi läbikukkumise
2. Tõsised riskid	4 punkti	Põhjustavad suuri kulusid või ajakava nihutamist pikemaks, ning teisejärguliste nõuete mitte-täitmist
3. Kesktaseme riskid	3 punkti	Põhjustavad mõõdukat kulu suurenemist või ajakava nihutamist; olulisemad nõuded on täidetud
4. Alamriskid	2 punkti	Põhjustab ainult väikest kulu suurenemist või ajakava nihutamist
5.Väheolulised riskid	1 punkt	Ei avalda mingit tegelikku mõju ajakavale või kuludele

Eristamine (Cervone, 2006):

1. Tugev mõju	1 punkt	Projekti objektid on riski all, risk põhjustab olulisi muudatusi projekti mahtudes, ajakavas või ressurssides
2. Keskmine mõju	3 punkti	Projekti objektid on kättesaadavad, kuid on nõutud oluline ajakava muutus
3. Madal mõju	5 punkti	Ei toimu olulisi muudatusi projekti plaanides, riskid ei ole olulised või võivad olla käsitletud väheste ületundidena

Teoreetilise analüüsi juures olid kõik ohtude hinnangud toodud välja avaliku sektori asutuse perspektiivis. Peamiseks muutujaks, mis eelduste kohaselt võib erineda enne ja pärast ISKE rakendamist avaliku sektori asutuses, on Tõenäosus. Mõju ja Eristamise näitajad jäävad samaks, kuna peegeldavad potentsiaalset ohtu ja selle mõju protsessidele. Allpool käsitletud ohtude tõenäosuse hinnang on teoreetiline. Hinnangu tegemisel lähtuti avalikusektori asutuste igapäevaste tegevuste hindamisest ja üldiste protsesside ülesehituse tavadest.

5.1 Teoreetilise analüüsi läbiviimine

Esimeses grupis **„G.1. Vääramatu jõud“** (ISKE Ohtude kataloog, 2014), mis sisaldab ohtusid, mida ei saa täielikult kontrollida või 100% tõenäosusega mõjutada ega ennetada, olid arvesse võetud järgmised ohud ning nendega kaasnevad meetmed (ISKE Meetmete kataloog, 2014):

Oht: G1.1 Personali väljalangemine

Meede: HK.10/HT.64 Lisanõuded personali asendamisele

Personali voolavus on vältimatu protsess igas organisatsioonis, mida ei saa 100% kontrollida ega ennetada. Kui töötaja lahkub oma ametikohalt, on väga tähtis leida samasuguste oskuste ja teadmistega asendustöötaja. Lisaks on vaja jälgida, et töötaja annaks enne lahkumist edasi oma teadmised ja oskused asendustöötajale.

Ohu hinnang riski hindamise valemi järgi:

Enne ISKE meetme rakendamist: **(Tõenäosus) 5** * (Mõju) 5 / 1 (Eristamine) = **25 (ÜRF)**

Peale ISKE meetme rakendamist: **(Tõenäosus) 3** * (Mõju) 5 / 1 (Eristamine) = **15 (ÜRF)**

Ohu realiseerumise tõenäosus on vähenenud 25-lt 15-le, mis vähendab **Üldist riskifaktorit** (ÜRF) 1,7 korda. Siit järeldub, et antud meetme rakendamine aitab vähendada ohu realiseerumise tõenäosust.

Järeldus: Nimetatud meede on liiga üldine Eesti Vabariigi avaliku sektori asutuste jaoks. Samas on antud meede universaalne ning sobib rakendamiseks peaaegu kõikides Euroopa riikides nii era- kui ka avalikus sektoris. Antud protsessi peab lähemalt analüüsima iga asutuse personaliosakonna poliitikast lähtudes. Kindlasti peavad olema rakendatud lisa-meetmed ning protsessid, mis vähendaksid nimetatud võimalikke ohte.

Oht: G1.2 IT-süsteemi avarii

Meede: HG.12 Lisanõuded valikjuhtumite hädaolukorraplaanidele

Kõik asutused sooviksid vältida probleeme IT-süsteemidega. Rakendatakse erinevaid viise probleemide tekkepõhjuste analüüsimiseks, erakorraliste situatsioonide lahendamiseks ning tagajärgede kõrvaldamise varuplaanide loomiseks.

Ohu hinnang riski hindamise valemi järgi:

Enne ISKE meetme rakendamist: **(Tõenäosus) 5** * (Mõju) 5 / 1 (Eristamine) = **25 (ÜRF)**

Peale ISKE meetme rakendamist: **(Tõenäosus) 3** * (Mõju) 5 / 1 (Eristamine) = **15 (ÜRF)**

Ohu realiseerumise tõenäosus on vähenenud 25-lt 15-le, mis vähendas **Üldist riskifaktorit** (ÜRF) 1,7 korda. Nimetatud meetme rakendamine vähendab ohu realiseerumise tõenäosust.

Järeldus: Antud meede on tehtud väga üldiseks ning nõuab spetsiifilist protseduuri kirjeldust ning täielikku analüüsi. Mõnedes gruppides ei osutu antud meede otstarbekaks (nt. personali kohta). Ohu kirjelduses on mainitud nii kesksete komponentide avarii kui ka tehnilised rikked/inimvead. Seega, lisaks hädaolukorraplaanidele peaksid olema välja töötatud ka ohu ennetamisprotsessid, mis vähendaksid võimalikult efektiivselt ohu realiseerumise tõenäosust.

Oht: G1.5 Vesi

Meede: HG.15 Tihendatud perioodiga hädaolukorraõppused

Arvestades seda, et Eestis ei ole looduskatastroofide teke tõenäoline, tuleb siiski koolitada personal *force-major* situatsioonides käitumiseks. Koolitusi peab viima läbi mitu korda aastas. Lisaks peavad personalile olema kättesaadavad vastavad juhendid. Õige käitumine *force-major* situatsioonides aitab kiiresti kõrvaldada selle tekkimise põhjused ja aitab vältida suure kahju tekkimist.

Ohu hinnang riski hindamise valemi järgi:

Enne ISKE meetme rakendamist: **(Tõenäosus) 1** * (Mõju) 4 / 2 (Eristamine) = **2 (ÜRF)**

Peale ISKE meetme rakendamist: **(Tõenäosus) 1** * (Mõju) 4 / 2 (Eristamine) = **2 (ÜRF)**

Ohu realiseerumise tõenäosus ei ole muutunud. Seega ei mõjuta meetme rakendamine nimetatud ohu realiseerumise võimalust.

Järeldus: Mõnedes aspektides ei ole antud meede Eesti kohta eriti aktuaalne, kuna antud ohtu võivad ainsana põhjustada probleemid kanalisatsiooniga (väga harva uputus, mis Eesti raames ei saa olla katastroofiline). Laias laastus on antud risk läbi mõeldud hoonete haldusettevõtete poolt, kelle teenuseid ostetakse tavaliselt sisse. Hädaolukorraõppused on kindlasti vajalikud, kuid näiteks vee- ja küttetorustike pideva kontrolli läbi viimine võib aidata veeohu vähendamisele kaasa.

Oht: G1.6 Kaablite süttimine

Meede: HG.16 Andmevarundusplaani perioodiline läbivaatus

Ohutusreeglite kohaselt peavad olema kaablisüsteemid pidevalt kontrollitud ning vajadusel asendatud. Igas asutuses peavad selle eest vastutama palgatud spetsialistid või peab antud teenus olema sisseostetud vastava teenusepakkuja poolt. See aitab vältida erakorralisi situatsioone ning kaabeldusega seotud probleeme.

Ohu hinnang riski hindamise valemi järgi:

Enne ISKE meetme rakendamist: **(Tõenäosus) 5** * (Mõju) 5 / 1 (Eristamine) = **25 (ÜRF)**

Peale ISKE meetme rakendamist: **(Tõenäosus) 3** * (Mõju) 5 / 1 (Eristamine) = **15 (ÜRF)**

Ohu realiseerumise tõenäosus on vähenenud 25-lt 15-le, mis vähendas **Üldist riskifaktorit** (ÜRF) 1,7 korda. Seega, meetme rakendamine vähendab nimetatud ohu realiseerumise võimalust.

Järeldus: Nimetatud meede on aktuaalne, kui lisatakse iga hoone ning kaablitesüsteemide kontrolli juurde ka põhjalik protseduuride kirjeldus, mille järgi saavad protsessi hoida kontrolli all nii asutuse töötajad kui ka hoone omanikud. Varustuse ehk antud juhul kaablite pidev uuendamine ning asendamine, võib olla tähtsaks osaks meetmete kirjelduses.

Oht: G1.9 Tugevast magnetväljast tingitud andmekadu

Meede: HG.19 Lisanõuded andmetaaste harjutamisele

Kõikidest asutuste poolt kasutatavatest andmetest peaksid olema tehtud varukoopiad, et andmekandjate vigastamisel oleksid andmed kättesaadavad. Teiselt poolt, peab olema tagatud maksimaalselt tõhusate andmekandjate kasutamine, mis minimeerib andmekandjate vigastamise tõenäosust.

Ohu hinnang riski hindamise valemi järgi:

Enne ISKE meetme rakendamist: **(Tõenäosus) 3** * (Mõju) 4 / 1 (Eristamine) = **12 (ÜRF)**

Peale ISKE meetme rakendamist: **(Tõenäosus) 1** * (Mõju) 4 / 1 (Eristamine) = **4 (ÜRF)**

Ohu realiseerumise tõenäosus on vähenenud 12-lt 4-le, mis vähendas **Üldist Riskifaktorit** (ÜRF) 3 korda. Tulemuste järgi on näha, et meetme rakendamine võimaldab oluliselt vähendada ohu realiseerumise tõenäosust.

Järeldus: Nimetatud ohtu võib kajastada hädaolukorra nimekirjas, kuna Eesti oludes ei ole see väga tõenäoline. Ohu kirjelduses on mainitud, et disketid, valmisplaadid, kassetid ja lindid on tüüpilised magnetilist salvestusmeediumit sisaldavad andmesalvestid, ent vaadates tänapäevast tehnoloogia arengut, on kogu informatsioon salvestatud turvalistele andmekandjatele, mida ei ole võimalik nii lihtsalt mõjutada ega nendelt infot kaotada.

Teises grupis **„G.2. Organisatsioonilised puudused**“ (ISKE Ohtude kataloog, 2014), mis sisaldab organisatsiooni töökorraldusesiseseid ohtusid protseduurides ning protsessides, sattusid valimisse järgmised ohud ning kaasnevad meetmed (ISKE Meetmete kataloog, 2014):

Oht: G2.1 Reeglite puudumine või puudulikkus

Meede: M 2.1 Vastutavate isikute ja reeglite kindlaksmääramine

Kõik asutustesisesed protseduurid ja reeglid peavad olema kirjas vastavates dokumentides ning olema kättesaadavad vastavatele isikutele. Reegleid tuleb pidevalt läbi vaadata ja täiendada vastavalt asutuse struktuuri, töökorralduse, reeglite jne muutmisele. Asutustes peavad olema kindlaks määratud töötajad, kes vastutaksid reeglitega sätestatud protseduuride eest. See aitab vältida segadust ja tagab tööprotsesside tõhusa toimimise.

Ohu hinnang riski hindamise valemi järgi:

Enne ISKE meetme rakendamist: **(Tõenäosus) 5** * (Mõju) 5 / 1 (Eristamine) = **25 (ÜRF)**

Peale ISKE meetme rakendamist: **(Tõenäosus) 1** * (Mõju) 5 / 1 (Eristamine) = **5 (ÜRF)**

Ohu realiseerumise tõenäosus on vähenenud 25-lt 5-le, mis vähendas **Üldist riskifaktorit** (ÜRF) 5 korda. Näitajate järgi on näha, et soovitatud meetme rakendamine vähendab väga tõhusalt ohu realiseerumise võimalust.

Järeldus: Nimetatud meedet peab pidevalt täiendama ning arendama, lisades sinna ka personali asendamise vajaduse, lisakoolitused jmt. Asutustel peab olema välja töötatud põhjalik personalijuhtimise strateegia, mis aitaks kaasa võimalike ohtude vältimisele. Peaaegu kõikides avaliku sektori asutustes täiendatakse reegleid ning ametijuhendeid pidevalt, kuna ülesannete jagamine on üks tähtsamatest osadest. On olemas ka spetsialistid, kes suunavad antud protsesse ning teostavad järelvalvet.

Oht: G2.3 Puuduvad, puudulikud või ühildamatud ressursid

Meede: M 2.3 Andmekandjate haldus

Ressursside puudumise, puudulikuse ja ühildamatuse vältimiseks peab olema teostatud pidev kontroll olemasolevate ressursside üle. See võimaldab õigeaegselt taastada vajalikke ressursse ilma hilinemiseta ja piisavas koguses. Ressursside haldamiseks peavad olema määratud kindlad isikud, kes vastutaksid pideva ressursside kontrolli eest ja tegeleksid ressursside õigeaegse täiendamisega.

Ohu hinnang riski hindamise valemi järgi:

Enne ISKE meetme rakendamist: **(Tõenäosus) 5** * (Mõju) 5 / 1 (Eristamine) = **25 (ÜRF)**

Peale ISKE meetme rakendamist: **(Tõenäosus) 1** * (Mõju) 5 / 1 (Eristamine) = **5 (ÜRF)**

Ohu realiseerumise tõenäosus on vähenenud 25-lt 5-le, mis vähendas **Üldist riskifaktorit** (ÜRF) 5 korda. Rakendamiseks soovitatud meede võimaldab oluliselt ette näha ohu realiseerumise võimalust ning viib selle peaaegu miinimumini.

Järeldus: Nimetatud meede on piisav, kui lisatakse ka põhjalik protseduuride kirjeldus.

Oht: **G2.4** Turvameetmete ebapiisav järelevalve

Meede: M 2.4 Hooldus- ja remonditööde reeglid

Pärast turvameetmete paigaldamist peab pidevalt kontrollima nende funktsioneerimist. Planeeritud remonditöid peab teostama pidevalt, sest kõik turvasüsteemid on üksteisega tihedalt seotud ning kui ilmneb rike ühe turvaseadme töös, kannatab kogu turvasüsteem.

Ohu hinnang riski hindamise valemi järgi:

Enne ISKE meetme rakendamist: **(Tõenäosus) 5** * (Mõju) 5 / 1 (Eristamine) = **25 (ÜRF)**

Peale ISKE meetme rakendamist: **(Tõenäosus) 1** * (Mõju) 5 / 1 (Eristamine) = **5 (ÜRF)**

Ohu realiseerumise tõenäosus on vähenenud 25-lt 5-le, mis vähendas **Üldist riskifaktorit** (ÜRF) 5 korda. Meetme rakendamine vähendab väga suurel määral nimetatud ohu realiseerumise võimalust.

Järeldus: Nimetatud meede on piisav tagajärgede kõrvaldamiseks või ohu realiseerumise ennetamiseks. Samas, erinevates avaliku sektori asutustes võivad drastiliselt erineda olemasolevad tehnoloogilised vahendid ning lisavarustuse soetamiseks võivad puududa rahalised ressursid. Peab arvestama asutuste eelarvega ning turvameetmete arendamise ning rakendamise plaanidega.

Oht: G2.6 Volitamata pääs ruumidesse

Meede: M 2.6 Sissepääsuõiguste andmine

Igas asutuses on olemas ruumid, kus säilitatakse salastatud ja tähtsate andmetega dokumente ning muid andmekandjaid. Nimetatud ruumidesse peaksid sisse pääsema ainult selleks volitatud isikud. Asutuse üldiseks sissepääsuks peab olema loodud kindel süsteem, mis tuvastaks kõik isikud, kellele on sisenemine lubatud. Samuti peavad olema kehtestatud reeglid, mille kohaselt oleks keelatud sissepääs kolmandatele isikutele ning reeglid juhtudeks, kui sisenemise õiguse on saanud võõras isik.

Ohu hinnang riski hindamise valemi järgi:

Enne ISKE meetme rakendamist: **(Tõenäosus) 5** * (Mõju) 5 / 1 (Eristamine) = **25 (ÜRF)**

Peale ISKE meetme rakendamist: **(Tõenäosus) 1** * (Mõju) 5 / 1 (Eristamine) = **5 (ÜRF)**

Ohu realiseerumise tõenäosus on vähenenud 25-lt 5-le, mis vähendas **Üldist riskifaktorit** (ÜRF) 5 korda. Meetme rakendamine suudab minimeerida ohu realiseerumise tõenäosust.

Järeldus: Nimetatud meede osutub piisavaks, kui lisatakse ka põhjalik protseduuride kirjeldus. Samas peaks ka toimima pidev süsteemide uuendamine.

Oht: G2.8 Ressursside kontrollimatu kasutamine

Meede: M 2.8 IT-rakendustele ja andmetele pääsuõiguste andmine

Asutusesiseselt peab olema kindlaks määratud, millistele andmetele ja ressurssidele saavad liigipääsu kõik töötajad. Selle kaudu on võimalik kontrollida IT-rakenduste ja andmete kasutamist iga töötaja lõikes. See aitab kiiresti avastada ressursside kuritarvitamise toimepanemist.

Ohu hinnang riski hindamise valemi järgi:

Enne ISKE meetme rakendamist: **(Tõenäosus) 5** * (Mõju) 5 / 1 (Eristamine) = **25 (ÜRF)**

Peale ISKE meetme rakendamist: **(Tõenäosus) 1** * (Mõju) 5 / 1 (Eristamine) = **5 (ÜRF)**

Ohu realiseerumise tõenäosus on vähenenud 25-lt 5-le, mis vähendas Üldist riskifaktorit (ÜRF) 5 korda. Meetme rakendamine mõjutab tõsiselt ohtu ning suudab vähendada nimetatud ohu realiseerumise võimalust.

Järeldus: Nimetatud meede on piisav, kui lisatakse ka põhjalik protseduuride kirjeldus ning järelvalvet teostavad koolitatud spetsialistid. Protsessi kirjeldus ning kogu süsteem peab olema pidevalt jälgimisel, täiendamisel ning vajadusel asendatav uuega.

Järgmises grupis **„G.3. Inimvead**“ (ISKE Ohtude kataloog, 2014), kuhu kuuluvad inimeste ehk töötajate vead, ebatäpsused, kuriteod jne, mida ei saa 100% kontrollida või ennetada, on analüüsitud järgmisi ohte ja meetmeid (ISKE Meetmete kataloog, 2014):

Oht: G3.1 Andmete konfidentsiaalsuse või terviklikkuse kadu kasutaja vea tõttu

Meede: M 3.1 Uute töötajate esmane juhendamine ja väljaõpe

Inimvead on üks tööaspektidest, mida on väga raske jälgida ja ennetada, mistõttu peavad kõikidele töötajatele olema kättesaadavad vastavad instruktsioonid ja koolitused, mis käsitlevad andmete kasutamist. Eelnimetatud probleem võib tulla ette eeskätt uute töötajate osas, kuna nemad pole veel kursis kõikide reeglite ja protseduuridega.

Ohu hinnang riski hindamise valemi järgi:

Enne ISKE meetme rakendamist: **(Tõenäosus) 5** * (Mõju) 5 / 1 (Eristamine) = **25 (ÜRF)**

Peale ISKE meetme rakendamist: **(Tõenäosus) 3** * (Mõju) 5 / 1 (Eristamine) = **15 (ÜRF)**

Ohu realiseerumise tõenäosus on vähenenud 25-lt 15-le, mis vähendas **Üldist riskifaktorit** (ÜRF) 1,7 korda. Seega, meetme rakendamine vähendab nimetatud ohu realiseerumise võimalust. Mõju ei ole suur aga ohu potentsiaal kahaneb.

Järeldus: Nimetatud meede osutub piisavaks juhul, kui lisatakse ka põhjalik protseduuride kirjeldus ning teostatakse pidevaid arengukoolitusi nii uutele kui ka vanadele töötajatele lähtudes vajadusest või protsesside muutustest. Tuginedes Eesti Vabariigi avaliku sektori praktikale, on täheldatud konfidentsiaalsete andmete leket, seega on antud oht Eestis väga tõenäoline. Ennetamaks lekke võimalusi ning tagamaks nende lekete võimaluste madal tase, on tarvis pidevalt olukorda analüüsida.

Oht: G3.2 Seadme või andmete hävitamine hooletuse tõttu

Meede: M 3.2 Uute töötajate kohustamine eeskirju järgima

Seadmete või andmete hävitamist just hooletuse tõttu on raske vältida, kuna see tähendab, et töötaja pole jälginud kehtestatud reegleid ja protseduure. Töötajatele peab pidevalt meelde tuletama kehtestatud reegleid ja protseduure ning rääkima võimalikest tagajärgedest, mis võivad tekkida töötajate hooletuse tõttu.

Ohu hinnang riski hindamise valemi järgi:

Enne ISKE meetme rakendamist: **(Tõenäosus) 5** * (Mõju) 4 / 1 (Eristamine) = **20 (ÜRF)**

Peale ISKE meetme rakendamist: **(Tõenäosus) 3** * (Mõju) 4 / 1 (Eristamine) = **12 (ÜRF)**

Ohu realiseerumise tõenäosus on vähenenud 20-lt 12-le, mis vähendas **Üldist riskifaktorit** (ÜRF) 1,6 korda. Meetme rakendamine vähendab nimetatud ohu realiseerumise võimalust.

Järeldus: Meede on piisav juhul, kui töötajad on kursis kõikide protsessidega, need on töötajatele selged ning töötajad saavad aru protsesside vajalikkusest. Avaliku sektori töötajate eeskirjade jälgimine peab olema pidevalt kontrollitav. Eriti teravaks osutub see probleem avaliku sektori asutustes, kuna paljudel juhtudel on tegemist tundlike andmetega ehk elanike isikliku informatsiooniga.

Oht: G3.4 Lubamatud kaabliühendused

Meede: M 3.4 Väljaõpe enne programmi tegelikku kasutamist

Iga töötaja peab saama koolituse kõikide programmide ja süsteemide töötamise kohta. Samuti peavad olema kättesaadavad ka manuaalid ja kasutusjuhendid, et töötajatel oleks igal ajal oma teadmisi võimalik täiendada.

Ohu hinnang riski hindamise valemi järgi:

Enne ISKE meetme rakendamist: **(Tõenäosus) 3** * (Mõju) 4 / 3 (Eristamine) = **4 (ÜRF)**

Peale ISKE meetme rakendamist: **(Tõenäosus) 1** * (Mõju) 4 / 3 (Eristamine) = **1.3 (ÜRF)**

Ohu realiseerumise tõenäosus on vähenenud 4-lt 1.3-le, mis vähendas **Üldist riskifaktorit** (ÜRF) 3 korda. Selle tulemusel viib meetme rakendamine ohu realiseerumise võimaluse miinimumini.

Järeldus: Kaasatud meede on piisav, kui lisatakse ka põhjalik programmide kasutamise kirjeldus ning kasutusjuhend. Kuna Eesti e-keskkonda kasutatakse nii era- kui ka avaliku sektori asutustes, peavad kõik turvameetmed olema rakendatud 100% selleks, et vältida ühenduste rikkeid või valeühendusega seotud probleeme.

Oht: **G3.5** Liinide juhuslik kahjustamine

Meede: M 3.5 IT-turvameetmete alane koolitus

Kõik asutuse töötajad, kes on seotud IT-süsteemidega, peavad saama professionaalseid koolitusi ning täiendavaid väljaõppeid, selleks et vähendada võimalikult palju vigade tekkimist ja hooletusest kahju tekitamist.

Ohu hinnang riski hindamise valemi järgi:

Enne ISKE meetme rakendamist: **(Tõenäosus) 5** * (Mõju) 5 / 1 (Eristamine) = **25 (ÜRF)**

Peale ISKE meetme rakendamist: **(Tõenäosus) 3** * (Mõju) 5 / 1 (Eristamine) = **15 (ÜRF)**

Ohu realiseerumise tõenäosus on vähenenud näitajast 25-lt 15-le, mis vähendas **Üldist riskifaktorit** (ÜRF) 1,7 korda. Selle tulemusel vähendab meetme rakendamine nimetatud ohu realiseerumise võimalust.

Järeldus: Nimetatud meede osutub piisavaks juhul, kui lisatakse ka põhjalik protseduuride kirjeldus. Antud oht on pigem seotud inimfaktoriga, mida ei saa 100% ennetada, kuid asutused peaksid tegema kõik selleks, et hoida ära samalaadsete olukordade teket personalis.

Oht: **G3.7** Käsitsemisvea tõttu tekkinud kodukeskjaama (PBX) rike

Meede: HG.37 Tarkvara tervikluskontroll igal installeerimisel

Kogu asutuste süsteemidesse installeeritud tarkvara peab olema litsentseeritud ning läbinud kontrolli. Samuti peavad olema määratud spetsialistid, kes vastutaksid kogu tarkvara uuendamise, asendamise ja paigaldamise eest.

Ohu hinnang riski hindamise valemi järgi:

Enne ISKE meetme rakendamist: **(Tõenäosus) 5** * (Mõju) 5 / 1 (Eristamine) = **25 (ÜRF)**

Peale ISKE meetme rakendamist: **(Tõenäosus) 3** * (Mõju) 5 / 1 (Eristamine) = **15 (ÜRF)**

Ohu realiseerumise tõenäosus on vähenenud näitajalt 25-lt 15-le, mis vähendas **Üldist riskifaktorit** (ÜRF) 1,7 korda. Soovitatud meetme rakendamine vähendab seega nimetatud ohu realiseerumise võimalust.

Järeldus: Nimetatud meede on piisav juhul, kui lisatakse ka põhjalik protseduuride kirjeldus.

Neljandast grupist **„G.4. Tehnilised rikked ja defektid**“ (ISKE Ohtude kataloog, 2014), mis on otseselt seotud asutuste tehniliste protsesside, võrkude, tarkvara ja andmebaaside halduse jmt ning nende tööga seotud ohtude ja riskidega, valiti samamoodi välja viis ohtu ning nendega kaasnevad meetmed (ISKE Meetmete kataloog, 2014):

Oht: G4.2 Sisevõrkude katkestus

Meede: HG.42 Nõuded traadita kohtvõrgu migratsioonietappide planeerimisele

Sisevõrkude katkestuse korral peab olema asutusel läbi mõeldud võrkude tagavaratoitmisplaan, mis oleks piisav sisevõrkude taastamiseks.

Ohu hinnang riski hindamise valemi järgi:

Enne ISKE meetme rakendamist: **(Tõenäosus) 5** * (Mõju) 5 / 1 (Eristamine) = **25 (ÜRF)**

Peale ISKE meetme rakendamist: **(Tõenäosus) 3** * (Mõju) 5 / 1 (Eristamine) = **15 (ÜRF)**

Ohu realiseerumise tõenäosus on vähenenud 25-lt 15-le, mis vähendas **Üldist riskifaktorit** (ÜRF) 1,7 korda. Meetme rakendamine vähendab nimetatud ohu realiseerumise võimalust maksimaalsest tasemest keskmisele.

Järeldus: Nimetatud meede osutub piisavaks juhul, kui lisatakse ka IT-osakonna põhjalik protseduuride kirjeldus. Kontroll peab olema teostatud pidevalt. Kõik töötajad, sõltumata ametist, peavad rakendama nimetatud meedet igapäevatöös.

Oht: G4.3 Turvavahendi tõrge

Meede: M 4.3 Viirustõrjeprogrammi regulaarne kasutamine

Kõikidel asutuste arvutitel peavad olema installeeritud viirusetõrjesüsteemid, mida peab pidevalt uuendama ja kontrollima. Seoses viiruse väga kõrge ohuga arvutitele, on vajalik luua protsess, mis võimaldaks kõige paremini antud ohtu minimeerida ja vältida.

Ohu hinnang riski hindamise valemi järgi:

Enne ISKE meetme rakendamist: **(Tõenäosus) 5** * (Mõju) 5 / 1 (Eristamine) = **25 (ÜRF)**

Peale ISKE meetme rakendamist: **(Tõenäosus) 3** * (Mõju) 5 / 1 (Eristamine) = **15 (ÜRF)**

Ohu realiseerumise tõenäosus on vähenenud 25-lt 15-le, mis vähendas **Üldist riskifaktorit** (ÜRF) 1,7 korda. Meetme rakendamine vähendab nimetatud ohu realiseerumise võimalust.

Järeldus: Kuna arvutite viirusega nakatumise oht Eestis on kõrge, nõuab antud oht kõrget tähelepanu. Nimetatud meede on piisav ohu minimeerimiseks. Seejuures tuleb aga pidevalt teostada lisaanalüüse ning protseduuri kirjeldus peab olema täidetud vastavalt analüüsile. Ka

viirusetõrje tarkvara peab pidevalt uuendama. See aitab kaasa viirusetõrje protsessile ning selle kõrgel ja efektiivsel tasemel hoidmisele.

Oht: G4.5 Läbikoste

Meede: M 4.5 Kodukeskjaama (PBX) haldustööde logi

Kõiki kaabeldussüsteeme peavad kontrollima ja jälgima vastavad spetsialistid. Pidev järelvalve aitab vältida võimalikke rikkeid, nendega kaasnevat kahju ning lisaressursside kasutamist.

Ohu hinnang riski hindamise valemi järgi:

Enne ISKE meetme rakendamist: **(Tõenäosus) 5** * (Mõju) 4 / 1 (Eristamine) = **20 (ÜRF)**

Peale ISKE meetme rakendamist: **(Tõenäosus) 1** * (Mõju) 4 / 1 (Eristamine) = **4 (ÜRF)**

Ohu realiseerumise tõenäosus on vähenenud 20-lt 4-le, mis vähendas **Üldist riskifaktorit** (ÜRF) 5 korda. Järelikult vähendab meetme rakendamine väga suurel määral nimetatud ohu realiseerumise võimalust maksimaalsest tasemest miinimumini.

Järeldus: Meetme rakendamine on väga oluline, kuna läbikostete oht võib tõsiselt häirida infoturbe kaitset ning andmete edastamist/töötlemist. Hetkel on antud oht nimetatud ainult „Kaabeldus“-moodulis.

Oht: G4.80 Bluetooth’i ebausaldusväärsed või puuduvad turvamehhanismid

Meede: M 4.80 Kaug-võrguhalduse turvalised pääsumehhanismid

Kaitsta tuleb kõiki asutuse sisevõrguga seotud ühendusi ja keelata võõrad. Turvameetmeid tuleb pidevalt kontrollida. Töötajad peavad järgima turvameetmete protseduure ning võimalike probleemide tekkimisel pöörduma vastava spetsialisti poole.

Ohu hinnang riski hindamise valemi järgi:

Enne ISKE meetme rakendamist: **(Tõenäosus) 3** * (Mõju) 4 / 1 (Eristamine) = **12 (ÜRF)**

Peale ISKE meetme rakendamist: **(Tõenäosus) 1** * (Mõju) 4 / 1 (Eristamine) = **4 (ÜRF)**

Ohu realiseerumise tõenäosus on vähenenud 12-lt 4-le, mis vähendas **Üldist riskifaktorit** (ÜRF) 3 korda. Järelikult suudab meetme rakendamine tõsiselt vähendada ohu realiseerumise tõenäosust ning viib selle miinimumtasemeni.

Järeldus: Nimetatud meede on piisav. Seejuures tuleb pidevalt teha lisa-analüüse ning protseduuri kirjeldus peab vastama läbiviidud uuendustele ja teostatud võrkude kontrollile.

Oht: G4.9 Sisemise toiteallika tühjenemine

Meede: M 4.9 X Windowsi turvamehhanismid

Toiteallikaid tuleb pidevalt kontrollida ning nende tühjenemise korraks peab olema välja töötatud vastav tegevusplaan. Vastavate protsesside ja meetmete väljatöötamiseks on vajalik kasutada spetsialiste. Samaaegselt peab kasutama turvamehhanisme, mis kaitseksid toiteallikaga seotud vahendeid võimalike vigastuste eest.

Ohu hinnang riski hindamise valemi järgi:

Enne ISKE meetme rakendamist: **(Tõenäosus) 5** * (Mõju) 5 / 1 (Eristamine) = **25 (ÜRF)**

Peale ISKE meetme rakendamist: **(Tõenäosus) 3** * (Mõju) 5 / 1 (Eristamine) = **15 (ÜRF)**

Ohu realiseerumise tõenäosus on vähenenud 25-lt 15-le, mis vähendas **Üldist riskifaktorit** (ÜRF) 1,7 korda. Meetme rakendamine vähendab nimetatud ohu realiseerumise võimalust.

Järeldus: Nimetatud meede on piisav avaliku sektori asutuste jaoks Eestis.

Viimaseks, viiendaks grupiks on **„G.5. Ründed**“ (ISKE Ohtude kataloog, 2014), millega kaasnevad nii IT-alased ja süsteemide ründed kui ka füüsilised ründed teiste isikute poolt. Sellest grupist lisati samuti viis ohtu ja nendega kaasnevad meetmed (ISKE Meetmete kataloog, 2014):

Oht: G5.2 Andmete või tarkvara manipuleerimine

Meede: HG.52 Traadita ründetuvastus- ja -tõkestussüsteemid

Kõiki kasutatavaid andmeid ja tarkvara peab kaitsma vastavate turvamehhanismidega. Viimaseid tuleb pidevalt kontrollida ja vajadusel uuendada. Seejuures on oluline, et oleksid kaasatud ka uuemad turvamehhanismid ja süsteemid. Rünnete tekkimisel peavad rakenduma

vastavad protseduurid, mis aitaksid neid õigeaegselt kõrvaldada ja minimeerida rünnete mõju.

Ohu hinnang riski hindamise valemi järgi:

Enne ISKE meetme rakendamist: **(Tõenäosus) 5** * (Mõju) 5 / 1 (Eristamine) = **25 (ÜRF)**

Peale ISKE meetme rakendamist: **(Tõenäosus) 1** * (Mõju) 5 / 1 (Eristamine) = **5 (ÜRF)**

Ohu realiseerumise tõenäosus on vähenenud 25-lt 5-le, mis vähendas **Üldist riskifaktorit** (ÜRF) **5 korda**. Antud meede aitab viia ohu realiseerumise potentsiaali peaaegu minimumtasemeni.

Järeldus: Nimetatud meede osutub piisavaks juhul, kui sellele lisatakse ka põhjalik protseduuride kirjeldus. Seejuures peab pidevalt teostama lisa-analüüse ning uuendama ja arendama turvasüsteeme. Antud ohu tõenäosus avaliku sektori asutustes on kõrge ning meetme rakendamine peab olema pidev tähtajatu protsess.

Oht: G5.3 Volitamatu sisenemine hoonesse

Meede: HG.53 Avalike pääsupunktide kasutamise piiramine

Kõik sissepääsud asutustesse peavad olema varustatud turva- ja jälgimismehhanismidega. See aitab kontrollida sisenevaid isikuid ning vajadusel tuvastada võõraid. Kõiki turvasüsteeme tuleb pidevalt kontrollida ning hoida töökorras.

Ohu hinnang riski hindamise valemi järgi:

Enne ISKE meetme rakendamist: **(Tõenäosus) 5** * (Mõju) 5 / 1 (Eristamine) = **25 (ÜRF)**

Peale ISKE meetme rakendamist: **(Tõenäosus) 1** * (Mõju) 5 / 1 (Eristamine) = **5 (ÜRF)**

Ohu realiseerumise tõenäosus on vähenenud näitajalt 25-lt 5-le, mis vähendas **Üldist riskifaktorit** (ÜRF) **5 korda**. Seega võib öelda, et meetme rakendamine suudab minimeerida ohu realiseerumise tõenäosust.

Järeldus: Avaliku sektori asutuste puhul tundub meede olevat piisav, kuna paljudes asutustes on sisseostetud ka järelvalve- ning turvafirmade teenused.

Oht: G5.5 Vandalism

Meede: HG.55 Esemete tõstetud hoidmine serveri- ja arhiiviruumides

Kõiki esemeid ja andmeid tuleb hoida ruumides, kuhu ei pääse kõik töötajad ligi ning mille uksed peavad olema lukustatud ajal, mil asutus on suletud. See aitab vältida kõrvaliste isikute ligipääsu arhiividele või teistele ruumidele, kus asuvad vastavad esemed või andmekandjad.

Ohu hinnang riski hindamise valemi järgi:

Enne ISKE meetme rakendamist: **(Tõenäosus) 1** * (Mõju) 5 / 1 (Eristamine) = **5 (ÜRF)**

Peale ISKE meetme rakendamist: **(Tõenäosus) 1** * (Mõju) 5 / 1 (Eristamine) = **5 (ÜRF)**

Ohu realiseerumise tõenäosus ei ole muutunud. Seega võib öelda, et meetme rakendamine ei mõjuta nimetatud ohu realiseerumise võimalust, kuna selle tõenäosus on mõlemal juhul minimaalne.

Järeldus: Antud oht ei osutunud Eesti avaliku sektori raames aktuaalseks ning seda võib käsitleda kui lisaohtu, mille tõenäosus on väga väike. Vandalismi aktid avaliku sektori asutustes on pigem erand kui korduv praktika.

Oht: G5.7 Liini pealtkuulamine

Meede: HG.57 Muudatuste haldusinstrumentide pääsuõiguste määramine

Kõik võrgud peavad olema kaitstud turvasüsteemidega, mis on hallatud vastavate spetsialistide poolt ning plaanikohaselt kontrollitud. Kõikide kahtlaste ühenduste tekkimisel peab olema teavitatud vastav osakond.

Ohu hinnang riski hindamise valemi järgi:

Enne ISKE meetme rakendamist: **(Tõenäosus) 3** * (Mõju) 5 / 1 (Eristamine) = **15 (ÜRF)**

Peale ISKE meetme rakendamist: **(Tõenäosus) 1** * (Mõju) 5 / 1 (Eristamine) = **5 (ÜRF)**

Ohu realiseerumise tõenäosus on vähenenud näitajalt 15-lt 5-le, mis vähendas **Üldist riskifaktorit** (ÜRF) **3 korda**. Meetme rakendamine vähendab nimetatud ohu realiseerumise tõenäosust.

Järeldus: Pealtkuulamise oht on Eesti avaliku sektori asutustes võrreldes suuremate ning võimsamate Euroopa riikidega, päris väike. Strateegiliselt tähtsate asutuste tasemel nimetatud

meetmest piisab. Lisaks peavad olema rakendatud lisa-kaitse ning ennetamise protseduurid ja protsessid.

Oht: G5.9 IT-süsteemide volitamata kasutamine

Meede: HG.59 Sagedasem turvameetmete läbivaatus

Kõiki IT-süsteeme tuleb kaitsta vastavate turvameetmetega. Kasutusel olevaid turvameetmeid peab pidevalt kontrollima ja uuendama selleks, et nad vastaksid turvataseme nõuetele.

Ohu hinnang riski hindamise valemi järgi:

Enne ISKE meetme rakendamist: **(Tõenäosus) 5** * (Mõju) 5 / 1 (Eristamine) = **25 (ÜRF)**

Peale ISKE meetme rakendamist: **(Tõenäosus) 1** * (Mõju) 5 / 1 (Eristamine) = **5 (ÜRF)**

Ohu realiseerumise tõenäosus on vähenenud 25-lt 5-le, mis vähendas **Üldist riskifaktorit** (ÜRF) **5 korda**. Meetme rakendamine viis ohu realiseerumise tõenäosuse maksimaalsest miinimumtasemeni. See tähendab, et meetme rakendamine on väga tähtis protseduur kogu asutuse tegevuses.

Järeldus: Meede on üldine, kuid väga aktuaalne ja tähtis. Tänapäeval, vaatavad kõrgema turvatasemega (H-tasemega) avaliku sektori asutused pidevalt läbi kasutusel olevaid turvameetmeid, et võimalusel ennetada IT-süsteemide volitamata kasutamist. Kõigil tasemetel peab meetme rakendamine olema ühesugune. Madala turvatasemega (L-tasemega) asutused peavad antud ohule pöörama rohkem tähelepanu ning investeerima turvameetmete arendusse.

5.2 Järeldus teoreetilisest analüüsist

Tuginedes teoreetilise analüüsi tulemustele, võib järeldada, et mõned ohud ja meetmed on ennetamiseks liiga ulatuslikud ning üldistavad. Mõned nimetatud ohtudest saab vaevalt ennetada või kõrvaldada, kasutades ainult kataloogis nimetatud meetmete abi. Asutused peavad ise pidevalt teostama sissekontrolli kõikide tõenäolisemate ohtude üle ning püüdma võimalusel rakendada efektiivseid protseduure. Mõnede valimis olevate ohtude realiseerumise tõenäosust ei saa vähendada vastavate meetmete rakendamise kaudu, kuna ohtude põhitegurid ei ole üldse mõjutatavad ega kontrollitavad.

Kuna uuritavate ohtude valim moodustati juhusliku valiku meetodiga, on sinna sattunud paar ohtu, mille tõenäosus Eestis on väga madal (nt. vandalism). Samas ei tähenda madal tõenäosus seda, et antud ohtusid võib ignoreerida või need eemaldada, sest see annab asutustele ISKE rakendamise protsessi teaduslikud alused selle kohta, missugused ohud on väikese tõenäosusega kategoorias. Viimase alusel saavad nad kaudselt valmis olla ootamatuteks ohtudeks.

Teoreetilise uuringu käigus tõestati hüpoteesi kehtivus. Enamikel juhtudel ISKE poolt rakendamiseks soovitatud meetmed vähendasid ohu realiseerumise tõenäosust. Seda näitab ka URF koefitsientide suhe enne ja pärast ISKE meetme rakendamist.

5.3 Teoreetilise analüüsi kokkuvõte

Teoreetilise analüüsi kaudu tuli välja ISKE kataloogis olevate meetmete puudulikkus ja vajadus pidevate uuenduste, ülevaatamise ja analüüsi järele. Eesti Vabariigi avalik sektor areneb sama kiiresti kui tehnoloogia ja maailm üldiselt, mistõttu tuleb avaliku sektori otstarbeka toimimise jaoks rakendada protseduure, mis oleksid kaasaegsed ja vastaksid mitte ainult Eesti sisesele kliimale ja olukorrale, vaid oleksid ka Euroopa juhtivate riikide tasemel.

Ohtude nimekirja täiendatakse ja korrigeeritakse pideval (ISKE, 2014)t, kuid antud tegevust peaks teostama sagedamini. Ühtlasi peaks sooritama kontrolli igas avaliku sektori asutuses, hoolimata selle turvatasemest, käideldavatest andmetest või tegevusalast.

6. Praktiline uuring

Selleks, et kohandada ISKE raamistik Eesti avaliku sektori IT-keskkonnaga, seda pidevalt täindatakse ja muudatakse. (ISKE, 2014) Muudatuste sisseviimine on seotud mitmete faktoritega:

1) Muutuv keskkond IT-maailmas
2) Muudatused Eesti Vabariigi seadusandluses, mis on seotud andmete käsitlemise ning kaitsmisega
3) Kasvavad nõuded andmeturbe poliitikas
4) Muudatused ning areng andmeturbe kaitsmises maailmatasandil

Eesti tasemel pole ISKE raamistiku rakendamine veel jõudnud nõutud tasemeni ning paljudes avaliku sektori asutustes pole ISKE infoturbe haldussüsteemi vaatamata selle kohustuslikkusele (Eesti Vabariigi Valitsus, 2004) siiani rakendatud.

Läbiviidud praktilise uuringu küsimustikuga uuritakse, kas avaliku sektori asutuses on realiseerunud IT-riske või mitte, mis on asutuste turvaaste ISKE infoturbe haldussüsteemi kohaselt ning millisel määral on rakendatud ISKE asutuses. Lisaks, uuringus küsitakse arvamust ISKE mõju IT-riskidele asutuse tegevuses ja isiklikku arvamust ISKE rakendamise kasulikkusest ja mõjust IT-riskidele (vt. Lisa 1).

6.1 Praktilise uuringu hüpotees

Enne küsimustiku koostamist ja uuringu läbiviimist püstitati hüpotees, millele tugines kogu uuringu käik. Sama hüpotees võeti ka eelneva teoreetilise analüüsi aluseks.

Uuringu eesmärgiks on tõestada või ümber lükata töös esitatud peamine hüpotees ning tulemuse eelduseks oli leida kinnitus peamisele töös esitatud hüpoteesile - et ISKE süsteemi rakendamine avaliku sektori ettevõtetes aitab vähendada IT-riskide realiseerumise tõenäosust ning mõjutab IT-riskide realiseerumise osakaalu.

6.2 Praktilise uuringu läbiviimine

Küsitluse läbiviimise eesmärgiga koostati küsimustik, mille põhjal poleks võimalik tuvastada, missuguse avaliku struktuuri asutusest on tulnud vastused küsimustikule. Küsimustiku koostamisel lähtuti eesmärgist, et küsimused sisaldaksid nii ISKE rakendamist puudutavat temaatikat kui ka asutuses olevate IT-riskide määramist ja ISKE rakendamise tulemusi IT-riskide vähendamiseks. Esiteks uuriti, kas asutus on rakendanud ISKE süsteemi. Edaspidi uuriti, millised IT-riskidest on tegelikult realiseerunud enne ISKE rakendamist ning kuidas võib hinnata IT-riskide realiseerumise tõenäosust peale ISKE süsteemi rakendamist.

Valim koosnes erinevatel tasemetel olevatest avaliku sektori asutustest. Sinna kuuluvad ministeeriumid, sotsiaalvaldkonna asutused, kaitse- ja järelvalve asutused, kohalikud omavalitsused jne. Asutuse esindajad said küsitluse, mis koosneb üheksast küsimusest ISKE rakendamise kohta (vt.Lisa 1) ning uuriti asutuse esindajate arvamust selle kohta, kas ISKE rakendamine oli abiks IT-riskide realiseerimise vähendamisele või mitte. Küsitluse läbiviimisel ei esitatud tundlikke ega liiga spetsiifilisi küsimusi selleks, et oleks võimalik tagada anonüümsus vastajate hulgas ning et oleks võimalik saada ainult uuringu jaoks vajaliku informatsiooni.

Esialgses valimis oli 50 avaliku sektori asutust, mille infoturbe turvalisuse tasemed olid enamasti M- ja H-tasemetel ehk siis keskmisel ja kõrgel turvalisuse astmel. Kokku vastas 50st avaliku sektori asutustest uuringu küsimustikule 10 asutust, mis annab 20% kogu esialgsest valimist. Seega põhjalikumate järelduste jaoks oleks vaja läbi viia suurema grupi analüüs.

Uuringu ajal ilmnes ootamatu asjaolu, mis on otseselt seotud ISKE rakendamise protsessidega. Küsitluse käigus tuli välja, et mõnedes asutustes on ISKE rakendamist puudutav informatsioon salastatud vaatamata sellele, et avalikus ligipääsus on olemas andmed ISKE rakendamise staatuse ning infoturbe kaitsmise tasandite kohta. Lisaks, kuna uuring oli mitteametlik ning sooritatud magistritöö raames, keeldusid paljud asutused vastamast, mainides uuritava informatsiooni konfidentsiaalsust või lihtsalt ignoreerisid antud uuringut.

6.3 Praktilise uuringu tulemused

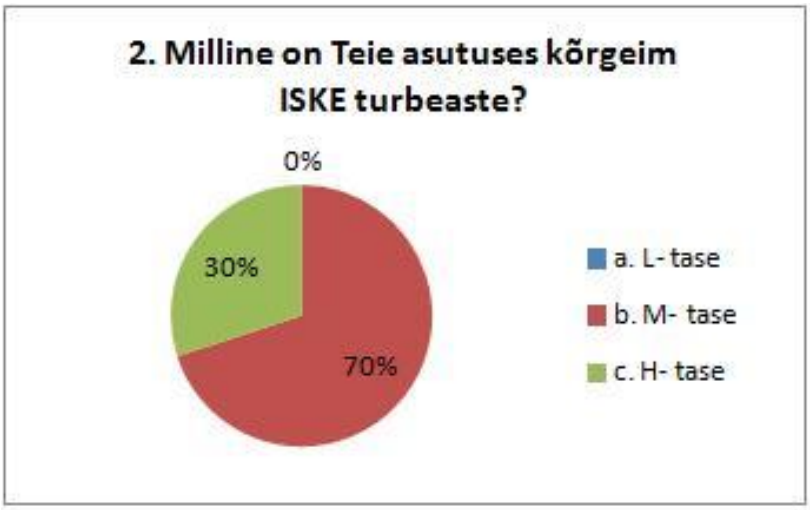
Kokku oli küsimustikus üheksa küsimust (vt.Lisa 1), millest seitse olid statistiliselt analüüsitavad (ehk kodeeritud) ja kaks viimast olid lahtiste vastustega, mis avaldasid vastava inimese isiklikku ning professionaalset arvamust.

KÜSIMUS Nr. 1

Graafik Nr.1

Esimese küsimuse **„Kas Teie asutuses on formaalselt ja sisuliselt IT-riske analüüsitud?“** olid kõik vastusevariandid kodeeritud vastustega „jah“ või „ei“. Vastanud asutuste hulgas vastasid „Jah“ 90% asutuste esindajatest. Seega võib väita, et IT-riskide analüüsiga avalikus sektoris tegeletakse ning seda võetakse tõsiselt. Läbi viidud küsitluse anonüümsuse tõttu ei ole võimalik välja tuua, mis tüüpi asutustes ei olnud IT-riske formaalselt ega sisuliselt analüüsitud.

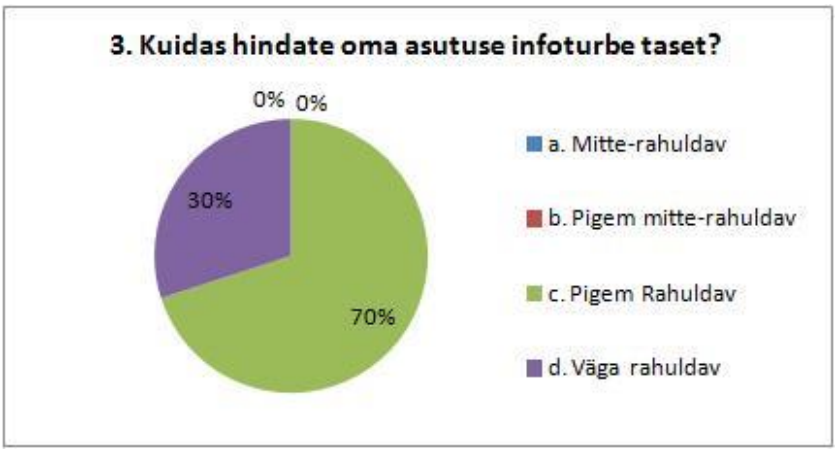
KÜSIMUS Nr. 2



Graafik Nr.2

Teine küsimus **„Milline on Teie asutuses kõrgeim ISKE turbeaste?“** jagas kogu valimi kolmeks turbeaste tüübiks: L-madal, M-keskmine, H-kõrge. Vastanute hulgas puudusid madala turbeastmega avaliku sektori asutused. 70% olid keskmise ehk siis M-turbeastmega ja ülejäänud 30% olid kõrge ehk H-turbeastmega asutused. See näitab, et M- ja H-turbeastmega asutused on IT-riskide analüüsist rohkem huvitatud kui võrrelda esimese küsimuse tulemustega.

KÜSIMUS Nr. 3



Graafik Nr.3

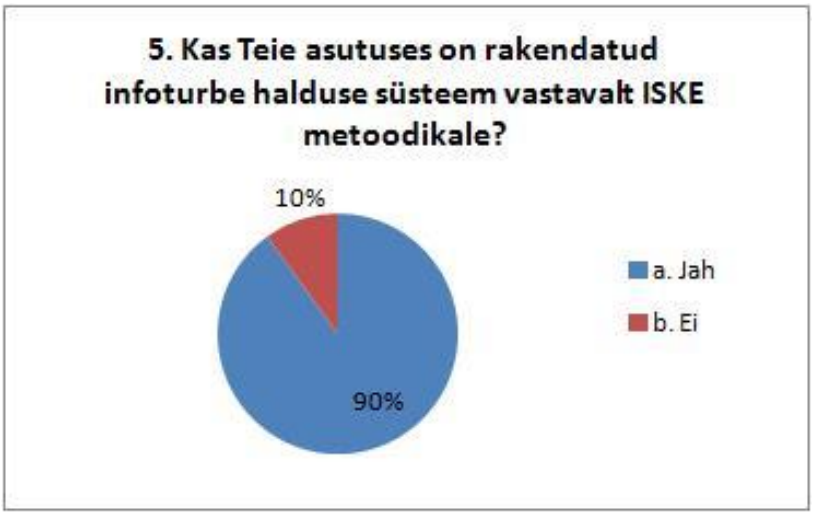
Kolmanda küsimuse **“Kuidas hindate oma asutuse infoturbe taset?”** vastused olid kodeeritud neljaks vastusevariandiks: 1. „mitte-rahuldav“, 2. „pigem mitte-rahuldav“, 3. „pigem rahuldav“, 4. „väga rahuldav“. Vastuste hulgas oli nii „mitte-rahuldav“ kui ka „pigem mitte-rahuldav“ vastuseid 0%. 70% vastajatest hindasid oma avaliku sektori asutuse infoturbe taset „pigem rahuldav“ ning 30% andsid hinnangu „väga rahuldav“.

KÜSIMUS Nr. 4

Graafik Nr.4

Neljanda IT-riskide alase küsimuse **„Kas Teie asutuses on viimase kolme aasta jooksul realiseerunud olulisi IT-riske ja milliseid?“,** vastajate vastused olid jagatud kaheks: 1. „Jah, on realiseerunud IT-riske“, 2. „IT-riske ei ole realiseerunud”. 40% vastajatest tunnistasid, et viimase kolme aasta jooksul realiseerunud IT-riske ning 60% väitsid, et pole realiseerinud ühtegi IT-riski.

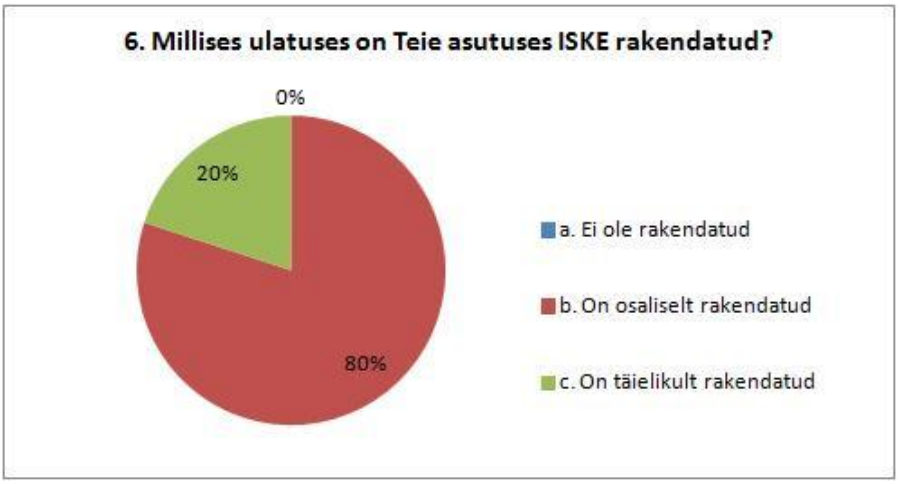
KÜSIMUS Nr. 5



Graafik Nr.5

Viienda küsimuse **"Kas Teie asutuses on rakendatud infoturbe halduse süsteem vastavalt ISKE metoodikale?"** vastused olid samamoodi nagu eelmises küsimuses kodeeritud "Jah" ja "Ei" vastusteks. 90% vastanutest väitsid, et infoturbe haldussüsteem on nende asutuses rakendatud vastavalt ISKE metoodikale. 10% ehk üks asutus valimist vastas, et infoturvet rakendatakse mõne muu infoturbe haldusmetoodika järgi.

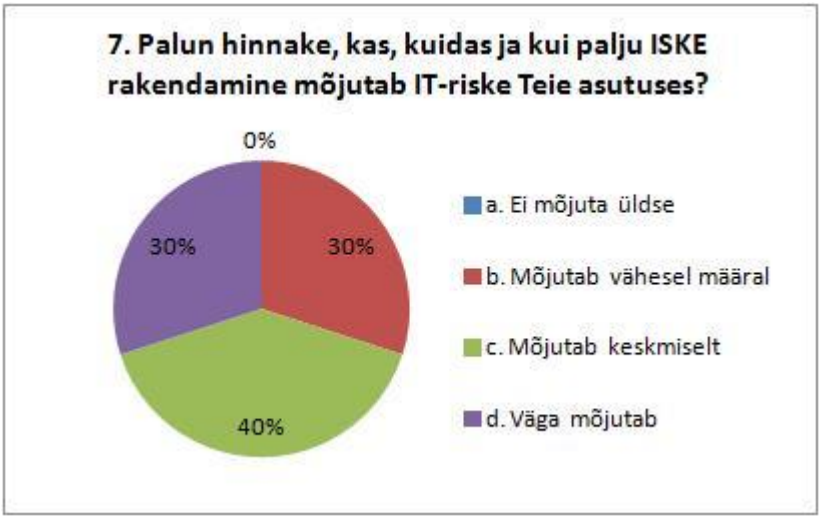
KÜSIMUS Nr. 6



Graafik Nr.6

Kuues küsimus, **“Millises ulatuses on Teie asutuses ISKE rakendatud”** oli valikvastustega küsimus. Mitte ükski asutus ei väitnud, et ISKE-t pole rakendatud. 80% vastasid, et ISKE infoturbe haldussüsteem on nende asutuses rakendatud osaliselt ning 20% vastasid, et ISKE on asututses täielikult rakendatud.

KÜSIMUS Nr. 7



Graafik Nr.7

Seitsmenda küsimuse **“Palun hinnake, kas, kuidas ja kui palju ISKE rakendamine mõjutab IT-riske Teie asutuses?”** vastused olid töödeldud kahel viisil. Esialgselt kodeeriti need neljaks variandiks: 1. “Ei mõjuta üldse”, 2. ”Mõjutab vähesel määral”, 3. “Mõjutab keskmiselt”, 4. “Väga mõjutab”. Antud kodeerimine andis vastuse küsimuse teisele osale, mis palus hinnata, kui palju mõjutab ISKE IT-riske asutuses. 0% vastas, et ISKE ei mõjuta üldse IT-riske. Edasi jagunesid arvamused peaaegu võrdselt. Esimesed 30% vastasid, et ISKE “mõjutab vähesel määral”. 40% valisid kolmanda vastuse, et ISKE avaldab “keskmist mõju” IT-riskidele. Viimased 30% vastajatest arvasid, et ISKE mõju IT-riskidele on väga tugev.

Teises küsimuse osas pöörati tähelepanu just nimelt sellele, kuidas ISKE rakendamine mõjutab IT-riske.

Vastajad, kelle vastused olid kodeeritud “mõjutab vähesel määral“ alla, tõid välja järgmised põhjused:

- “Olulised riskid olid ka enne ISKE-t vajalikul määral maandatud. ISKE rakendamisega on kaasnenud protsesside ja tegevuste põhjalikum dokumenteerimine ja reeglite kirjapanemine.”
- “ Mõju ei ole otsene vaid kaudne. ISKE pakub rohkem teadlikkust võimalikestest IT-riskidest.”

Need, kes hindasid ISKE mõju oma asutusele kui „keskmine“, seletasid oma positsiooni järgmiselt:

- “… oleme tavaks võtnud valida riskide maandamiseks meetmeid ISKE kataloogidest, vajadusel täiendades neid lisategevustega.”
- “Ilmselt ei mõjuta riske niivõrd ISKE formaalne rakendamine kuivõrd nende teadmiste kasutamine igapäevases töös riskide ärahoidmiseks.”
- “ Minimeerib mingi tasemeni IT-riske, reguleerib protsessi reegleid. Kahjuks ei kattu IT-rakenduste standarditega täies mahus ning ei kata kõiki rakendustsükleid. ISKE omab suurt mõju kõrge küpsusastmega asutuste IT-riskidele.”

Vastajad, kes olid nõus, et ISKE mõju IT-riskidele on tugev, seletasid oma nägemust alltoodud arvamustega:

- “…ISKE-s on palju meetmeid, mis aitavad IT riske maandada…”
- “… tagab IT-süsteemide häireteta töö ning asutuse ettenähtud tööülesannete täitmise ning klientide teenindamise, kontrolli läbiviimisel on tagatud tõrgeteta töö...”

Vastustest võib välja tuua, et enamust vastajatest olid nõus, et ISKE rakendamine avaldab keskmist või tugevat mõju IT-riskidele.

KÜSIMUS Nr. 8

Kaheksandale küsimusele **“Kirjeldage, milline on ISKE rakendamisest saadav kasu Teie asutusele?”** vastasid kõik uuringus osalejad vabas vormis. Edaspidi on välja toodud arvamused, mis olid kõige populaarsemad:

- “ Etalonturbe metoodika olemasolu aitab reguleerida lähenemist infoturbe haldusele ning reguleerida infoturbe valdkonna rakendamise suuniseid. Erinevate infoturbe tegevuste teostamiseks on ressursse lihtsam kätte saada, sest on olemas selge

põhjendus, milleks on vaja mingit projekti/tegevust läbi viia. Vajadusel saab kohe näidata, millised ohud on seotud teatud meetmete mitterakendamisega."

- "…omal tekib süsteemist ülevaade kui tervikust, on ülevaade nõrkadest kohtadest ning ISKE on argument eelarvest raha taotlemiseks süsteemi arendamiseks."
- " Kasu on pigem kaudne, mis väljendub eelkõige infoturbe teadlikkuse suurenemises, mõned kriitilised protsessid on paremini reguleeritud ja riskid on seetõttu teoreetiliselt madalamad."
- " Annab selgema ülevaate rakendatud infoturbe meetmetest ning IT-riskidest."
- " ISKE meetmete rakendamisel on tagatud infosüsteemide ja IT riistvara häireteta töö ning vähenevad kulutused võimalike väärkasutuste ja küberrünnete tagajärjel tekitatud rikete kõrvaldamiseks..."

Kõikidest arvamustest võib välja tuua üldise mõtte, et ISKE rakendamine on avaliku sektori asutustele pigem kasulik, sobib nende igapäevase töö parendamiseks ning IT-riskide haldamise protsessid on selgemad ja muutuvad süstemaatilisteks.

KÜSIMUS Nr. 9

Vastajate isiklikku arvamust ISKE infoturbe haldussüsteemi kohta küsiti üheksandas küsimuses **"Teie isiklik arvamus ISKE rakendamise mõjust IT-riskidele?"**. Peamiselt olid kõik arvamused positiivsed ning ISKE infoturbe süsteemi rakendamist iseloomustati kui positiivset asjaolu avaliku sektori ettevõtete tegevusele:

- "…rakendatud ISKE teeb IT-mehe elu mõnusamaks ja vähendab riske."
- " Kõik töötajad on teadlikud infoturbest ning oskavad seda hinnata, st kas on piisav või ei…"
- "ISKE on vajalik. Tõsi, tihtipeale tuleb sealseid meetmeid oma organisatsiooni eripärasid silmas pidades painutada …"
- " ISKE rakendamine aitab kindlasti vältida paljusid IT riske, mis on seotud füüsilise turbega, häkkerluse, küberrünnakutega ja muude kaasnevate probleemidega"

Siiski, ilmnesid ka negatiivsed ISKE rakendamisega seotud aspektid, mis puudutasid selle keerulisust, vajalikke inim- ja majandusressursse, vajalikke muudatusi ning paremat kohandumist Eesti avaliku sektori asutuste tegevusega:

- “ ISKE pingutab mõnes kohas üle ja mõnes kohas on natuke puudulik. Seega osasid riske maandab ta liiga palju (bürokraatia, personal), st pole kuluefektiivne ja osasid riske liiga vähe (näiteks rakenduste arendamine). ISKE on rõhuga väga suurrele asutusele ja Saksamaa mentaliteeti arvestades tehtud. Eesti võiks kohandada ISKE enda jaoks natuke „kergemaks“.”
- “ISKE rakendamine kindlasti maandab teatud riske. Samas alati jääb oht, et spetsiifilised, harvaesinevad või asutuse-kesksed riskid jäävad tuvastamata. Selleks on kindlasti vaja perioodiliselt ka riskide hindamist teostada…”
- “Kuna ISKE on enamuse Eesti riigiasutuste jaoks täismahus rakendamiseks liiga keerukas ja mahukas ning seetõttu ka liiga kallis, siis on mõju kindlasti väiksem kui võiks eeldada.”
- “Liiga mahukas süsteem, ei pea vajalikuks, et kõiki protsesse peaks nii detailselt käsitlema.”
- “Idee on hea, aga sellel on mitmeid tehnilisi puudusi.”

Antud praktilises uuringus osalenud avaliku sektori esindajad nõustusid, et ISKE rakendamine vähendab IT-riskide ilmnemise tõenäosust. ISKE rakendamisega kaasnevad protseduurid aitavad struktureerida, analüüsida ning mõjutada riskide haldamise protsesse, mis omakorda mõjutavad ka infoturbe õiget käsitlemist ning haldamist. ISKE mõju IT-riskidele hinnati erinevalt, kuid ükski vastaja ei eiranud seda. See kinnitab püstitatud hüpoteesi.

Samas tuli välja, et täielikult rakendada on ISKE-t võimatu, kuna mõned protseduurid ei vasta avaliku sektori asutuste nõuetele. Selgusid ka peamised põhjused ISKE mitterakendamiseks. Peamisteks olid majanduslikud põhjused, ISKE protseduuride puudulikkus ning ISKE protsessidega kaasnevad bürokraatlikud protseduurid.

Kui ühendada kõik eelpool mainitud märkused võib väita, et ISKE infoturbe haldussüsteemi rakendamine täies mahus pole Eesti avalikus sektoris nii efektiivne kui see võiks olla, kuna protseduurid muutuvad ajaliselt ning majanduslikult ülimahukaks, mis omakorda ei vasta täielikult Eesti avaliku struktuuri suurusele ning ülesehitusele.

Teiselt poolt toob ISKE rakendamine kaasa väga palju positiivseid aspekte, muutes avaliku sektori infoturbe haldust mugavamaks ja efektiivsemaks, ning vähendades IT-riskide realiseerumist. ISKE rakendamise tõhusamaks muutmiseks on vaja muuta antud süsteem

kergemini kasutatavaks, võttes arvesse kõiki puudusi ja täiendamist vajavaid aspekte, mis on välja tulnud uuringu käigus.

6.4 Praktilise uuringu tulemuste rakendamise soovitused

Läbiviidud uuringut võib liigitada antud valdkonnas piloot-uuringuks, kuna siiamaani uuriti ISKE infoturbe haldussüsteemi ainult maavalitsuste tasemel (Laks, 2013). Tulevikus tuleks läbi viia suurem uuring, mis hõlmaks kõiki avaliku sektori asutusi, millest osavõtt oleks kohustuslik ning ei oleks anonüümne nagu oli antud magistritöö raames teostatud uuring. Tulevases uuringus peaksid vastama umbes 80-90% kõikidest avaliku sektori asutustest, et oleks tagatud tulemuste piisav usaldusväärsus.

Läbiviidud uuringus leidis kinnitust esialgne hüpotees, et infoturbe haldussüsteem ISKE mitte ainult ei mõjuta, vaid aitab ka vähendada IT-riskide realiseerumise tõenäosust avaliku sektori asutustes.

Tulemuste järgi aitab ISKE infoturbe haldussüsteem süstematiseerida IT-riskide analüüsi ning nende edasisi käsitlemisprotsesse, aitab süstematiseerida IT-riskide eest kaitsvaid tegevusi ning annab võimaluse süstemaatiliselt üles ehitada ning kontrollida vastavaid protsesse.

Praktiline uuring aitas välja tuua esialgsed ISKE rakendamise ning ülesehituse puudused ning ebatäpsused, mis ei vasta Eesti Vabariigi avaliku sektori nõuetele. Ilmnes ISKE süsteemi ebapiisavus ning tekkis võimalus tuua välja peamised puudused, mida rõhutasid ISKE rakendamisega seotud isikud.

Kokku esines kuus peamist puudust, mida soovitatakse ISKE arendamisega seotud organisatsioonidel ning spetsialistidel parandada:

1) Kõige esimeseks puudujäägiks on see, et ISKE ei anna ülevaadet kogu protsessist, puudused on näiteks arendusprotsessides. Mõned aspektid kogu protsessist jäävad katmata ning asutused peavad ise täiendama puuduvaid osasid.
2) ISKE ei hõlma kõiki avaliku sektori asutuste nõudeid.
    a) Mõned protsessid on liiga mahukad või ei ole üldse kasutusel Eesti avaliku sektori tegevuse raamides. Siin osutub probleemiks ka liiga mahukas protseduuride kirjeldus

ning dokumenteerimine. Teatud protsesside üleliigselt bürokraatlik käsitlemine pidurdab aktiivseid tegevusi ISKE rakendamise osas.

b) Tihti on ISKE infoturbe haldussüsteemi rakendamisega seotud liiga kõrged kulud, mida mõned avaliku sektori asutused ei saa endale lubada. Seega jäetakse rakendamise protsess pooleli või rakendatakse mittetäiuslikul viisil, mis võib kaasa tuua teatud puudused ning vead protsesside haldamises ning ülesehituses. ISKE infoturbe haldussüsteem ei ole tähtajaline projekt, vaid pidev protsess, mida peab jälgima, analüüsima ning toetama. Seda ei saa piirata ega peatada, sest muidu osutub eelnevalt tehtud töö lihtsalt kasutuks.

3) IT-riskide käsitlemise protsesside kohta tuleks teostada põhjalikum analüüs, mis peab olema kohustuslik, kuna mitte kõik avaliku sektori asutused infoturbe kaitse H- ja M-tasemega ei tegele piisavalt IT-riskide analüüsiga, mis ohustab omakorda kasutatavaid andmeid.
4) IT-riskide ennetussüsteemi peab rohkem arendama ning avaliku sektori asutustele peab andma antud teema kohta parema ülevaate. Mitte kõikides avaliku sektori asutustes ei ole spetsialiste, kes oskaks IT-riske piisavalt analüüsida ning anda head ülevaadet potentsiaalsetest ning võimalikest riskidest.
5) Peab olema teostatud parem ning tõhusam kontroll ISKE rakendamise üle avaliku sektori asutustes. Praeguseks ei ole kontroll piisavalt sügav ning süstemaatiline, mis toob kaasa mõnedes asutustes ebapiisava ISKE rakendamise protsessi, mis võib omakorda jääda teatud staadiumis lihtsalt seisma. Iga asutuse kohta peaksid olema uuritud peamised takistused, mis segavad ISKE täiemahulist rakendamist. Peale antud analüüsi saab uurida, missugused ISKE protsessid ei ole rakendamiseks otstarbekad. See aitab vähendada koormust nii protsesside dokumenteerimisega seoses kui ka majanduslikus aspektis.
6) Võimalik, et peaks olema välja töötatud ISKE rakendamise M- ja H-tasemega infoturbekaitse asutuste rahastamise plaan ehk eraldi eelarve, mis oleks täies mahus suunatud ISKE infoturbe haldussüsteemi sisseviimiseks, arenguks ning toetamiseks.

Avaliku sektori asutustele oleks väga kasulik jätkata ISKE rakendamisega seotud probleemidega ning pöörata rohkem tähelepanu ISKE infoturbe haldussüsteemi edaspidisele rakendamisele.

Parema kontrolli ja analüüsi teostamine suudab muuta ISKE rakendamise protsessi avaliku sektori asutuste jaoks kergemaks ning tagada kõikide protseduuride jälgimise.

KOKKUVÕTE

Antud "Infosüsteemide etalonturbe süsteemi ISKE rakendamise mõju IT riskidele Eesti avaliku sektori näitel" magistritöö raames käsitleti ning vaadati läbi väga paljud aspektid, mis on seotud tänapäevase olukorraga Eesti Vabariigi avalikus sektoris.

Esiteks, vaadati üle üldine IT-riskide juhtimise, analüüsi ja kontrolli protsessi vajadus. Kirjeldati peamisi IT-juhtimise põhimõtteid ja reegleid. Toodi välja peamised raamistikud ja standardid, mida on võimalik kohandada, lähtudes asutuse spetsiifikast ning mida on võimalik rakendada ettevõtetes ja asutustes riskide ülese kontrolli teostamiseks.

Nimetati ka võimalikke riskianalüüsi meetodeid ja lähenemisi, mis tulevad kasuks uue IT-riskijuhtimise strateegia loomise ja elluviimise protsessi käigus.

Anti ülevaade tänapäevasest olukorrast Eesti Vabariigi avalikus sektoris ning selle vajadustest IT-riskide käsitlemisel ja analüüsil. Praegusel ajal on avaliku sektori asutustele rakendamiseks kohustuslik Infosüsteemide Kolmastmeline Etaloniturbe Süsteem (ISKE). Analüüsiti ka IT-riskide realiseerumise juhtumeid Eesti avalikus sektoris, mis tõid välja ka ISKE infoturbe haldussüsteemi vajaduse IT-riskide ennetamiseks ja kõrvaldamiseks.

Magistritöö raames teostati teoreetiline analüüs sellest, kui palju vastab ISKE infoturbe haldussüsteem avaliku sektori asutuste vajadustele ja nõuetele. Teoreetilise analüüsi läbiviimiseks oli koostatud juhusliku valikuga valim, mis sisaldas viit ohtu ISKE ohtude kataloogist. Igast grupist võeti viis ohtu ja nendega kaasnevad meetmed ohtude ennetamiseks. Analüüsi käigus selgus, et enamikel juhtudel vastasid nimetatud ohud avaliku sektori asutuste tõenäoliselt potentsiaalsetele ohtudele. Samas peavad ohud ja meetmed olema pidevalt analüüsitud, uuendatud ja kõik protsessid nõuavad katkematut kontrolli ja ülevaatamist.

Peamiseks magistritöö eesmärgiks oli analüüsida, kas Infosüsteemide Kolmastmeline Etaloniturbe Süsteem (ISKE) avaldab mõju IT-riskidele Eesti avaliku sektori asutuste tegevuses või mitte. Peamiseks püstitatud hüpoteesiks oli see, et ISKE süsteemi rakendamine avaliku sektori asutustes aitab vähendada IT-riskide realiseerimise tõenäosust. Antud hüpoteesi tõestuseks koostati valim 50st erineva turvatasemega avaliku sektori asutusest ning oli laiali saadetud küsimustik, mis koosnes üheksast küsimusest. Küsimustikule vastamine oli

vabatahtlik ning vastajate seas oli tagatud 100% anonüümsus. Tulemusena tagastati kümme täidetud küsimustikku, mis moodustas 20% esialgsest valimist.

Uuringu tulemuste analüüsi jooksul leidis kinnitust esialgne hüpotees, et infoturbe haldussüsteemi ISKE rakendamine avaliku sektori asutustes tõepoolest aitab vähendada IT-riskide realiseerumise tõenäosust.

Uuringu käigus selgusid ka peamised takistused, mida näevad avaliku sektori asutused ISKE rakendamise protsessi jooksul. Esiteks, tihti osutub ISKE rakendamine võimatuks ebapiisavate rahaliste ressursside tõttu. Rakendamise protsess ning pidev kontroll kõikide protseduuride ja protsesside üle nõuab suuri investeeringuid, uute spetsialistide palkamist jne. Kogu kulu ISKE rakendamiseks osutub liiga koormavaks avaliku sektori asutustele ja mitte kõik saavad endale nimetatud investeeringud lubada. Teiseks, väga tähtsaks takistuseks on see, et ISKE ei vasta 100% Eesti avaliku sektori asutuste nõuetele. Eriti puudutab see protsesside kirjeldust ja esitatud nõudeid. Mõned protsessid osutuvad liiga mahukateks ning nõuavad liiga palju dokumenteerimist ja bürokraatliku lähenemist, mis on aeganõudev protsess ning ületab mõnikord avaliku sektori asutuse tegevuse mahtusid. Siit tulenevad olukorrad, mil mõned etapid ISKE rakendamise projektist jäetakse pooleli või jäetakse üldse rakendamata. Tõsiseks puudujäägiks on olukord, et tänapäeval ja tulevikus peab rakendama paremat infoturbe haldussüsteemi kontrolli ning auditeerimise protseduuri. Praegusel hetkel pole nii välis- kui ka sisekontrolli protsesside mahud nii sügavad ja süstemaatilised, kui peaksid olema.

Pärast teostatud uuringu tulemuste analüüsi olid välja pakutud uuringu tulemuste rakendamise soovitused avaliku sektori asutustele.

Üldiselt võib öelda, et püstitatud küsimuse laiemaks ja põhjalikumaks uurimiseks peab küsitlema kõiki avaliku sektori asutusi ning läbi viima tõhusamat analüüsi, mis saab teha veelgi edukamaks ISKE arendamist ja täiendamist.

SUMMARY

"The Impact of Application of the IT Baseline Security System ISKE to the IT Risks on the Example of Estonian Public Sector"

In the framework of the present master's thesis „ The Impact of Application of the IT Baseline Security System ISKE to the IT Risks on the Example of Estonian Public Sector" different aspects connected to the current situation in the Estonian public sector were examined.

Firstly, the overall necessity for the risk control, analysis and management was overviewed: were described the most important principles and rules of the IT risk management. Secondly, were listed the most important frameworks and standards that can be implemented and used to control the IT risks at the enterprises and establishments, taking into consideration specifics of these establishments.

Moreover, were examined possible methods and approaches of the risk analysis, which might be useful when creating and implementing a new strategy of the IT risk management. Was also reviewed the situation in the current Estonian public sector and its necessity for the management and analysis of the IT risks. Today, the public sector establishments are obliged to use the Three-level IT Baseline Security System ISKE.

In the framework of the present master's thesis the cases of the realization of the IT risks in the Estonian public sector were analysed, which also underlined the necessity for the ISKE information security system for preventing and deletion of the IT risks.

In the framework of this master's thesis, was conducted a theoretical analysis in order to establish to which extent the ISKE's administrative system satisfies the requirements and demands of the establishments in the public sector. A random sample containing 5 risks from the ISKE risk catalogue was created, and then five additional risks together with the measures to prevent them were taken from each group.

In the course of the analysis, it was established that the risks referred to do in the most part correspond to the potential risks of the establishments in the public sector, however, they should be constantly analysed, renewed and all the processes require a constant control and monitoring.

The main purpose of the present master's thesis was to analyse whether the ISKE system influences the IT risks in the Estonian public sector's enterprises' activity. The main hypothesis was "The implementation of the ISKE system in the public sector's establishments helps decrease the probability of the IT risks realization".

In order for this hypothesis to be proven true, was created a sampling with 50 public sector establishments with different level of security and was sent to them a nine-question questionnaire. The participation in the survey was voluntary and was guaranteed 100% anonymity among the respondents. As the result, ten filled out questionnaires were received, i.e. 20% of the initial sampling.

While analysing the research results, the initial hypothesis, which stated that the implementation of the ISKE system in the public sector establishments does indeed help decrease the probability of the IT risks realization was confirmed.

In the course of the research, there were also established the main obstacles for the implementation of the ISKE system at the public sector establishments. Were pointed out the main and the most frequently occurring ones. First of all, the implementation of the ISKE system is often impossible due to the insufficient means. The implementation process and constant control require big investments, new specialists, etc. These costs result to be overwhelming for some public sector establishments. Secondly, a very important issue is that the ISKE does not satisfy the requirements of the Estonian public sector establishments for 100%. Some of the processes are too voluminous and require too much paperwork and bureaucracy, therefore, too much time and often it exceeds the overall work volume of an establishment. This issue creates situations where some of the ISKE implementation stages are not finished or not completed at all. An important disadvantage is connected to the need for a better control and audit procedures of the information security system today and in the future. The internal and external control procedures are not as thorough and systematic as they should be.

In addition to the analysis of the research results, there were provided some suggestions for the implementation of these results at the public sector establishments.

In general, the objective of the present master's thesis "The Impact of Application of the IT Baseline Security System ISKE to the IT Risks on the Example of Estonian Public Sector" was met and in the course of the conducted survey the hypothesis was proven to be true. However, for a more effective analysis of the questions raised, it is necessary to conduct a bigger research with the maximum amount of respondents. Desirable research should be conducted at the state level at all of the public sector establishments for further development and improvement of the ISKE system.

LISA 1

PRAKTILISE UURINGU KÜSIMUSTIK:

1. Kas Teie asutuses on formaalselt ja sisuliselt IT-riske analüüsitud?
2. Milline on Teie asutuses kõrgeim ISKE turbeaste?
3. Kuidas hindate oma asutuse infoturbe taset?
4. Kas Teie asutuses on viimase kolme aasta jooksul realiseerunud olulisi IT-riske ja milliseid?
5. Kas Teie asutuses on rakendatud infoturbe halduse süsteem vastavalt ISKE metoodikale?
6. Millises ulatuses on Teie asutuses ISKE rakendatud:
    a. ei ole rakendatud
    b. on osaliselt rakendatud
    c. on täielikult rakendatud
7. Palun hinnake, kas, kuidas ja kui palju ISKE rakendamine mõjutab IT-riske Teie asutuses?
8. Palun kirjeldage, milline on ISKE rakendamisest saadav kasu Teie asutusele?
9. Teie isiklik arvamus ISKE rakendamise mõjust IT-riskidele?

KASUTATUD KIRJANDUS

1. RIA. Eestisse jõudis pahavara, mis muudab andmed püsivalt loetamatuks, 2014. [https://www.ria.ee/eestisse-joudis-pahavara-cryptolocker/] (29.04.2014)

2. Control Objectives for Information and Related Technology (COBIT 4.1). 2007. [http://www.isaca.org/Knowledge-Center/Research/ResearchDeliverables/Pages/COBIT-4-1.aspx] (29.04.2014)

3. ENISA Work Programme 2006. Risk Management: Implementation principles and Inventories for Risk Management/Risk Assessment methods and tools. [http://www.enisa.europa.eu/activities/risk-management/current-risk/risk-management-inventory/files/deliverables/risk-management-principles-and-inventories-for-risk-management-risk-assessment-methods-and-tools] (30.04.2014)

4. Bandyopadhyay, K., Mykytyn, P. , Mykytyn, K. A framework for integrated risk management in information technology. (1999). Management Decision, Vol. 37, No. 5, p.437 - 445 [http://www.emeraldinsight.com/journals.htm?articleid=865080] (30.04.2014)

5. Gottfried, I.S. (1989). When disaster strikes. Journal of Information Systems Management, p. 9-86.

6. Haar, H. and Solms, R. „A Tool for Information Security Management“. 1993. Information Management & Computer Security, Vol.1 No.1, p. 4-10. MCB University Press Limited.

7. Haney V., MBA, PMP®, CBAP® „Top IT Project Risks and What to do about them“. 2009. [http://www.vbhconsulting.com/Articles/Top%20IT%20Project%20Risks%20and%20What%20to%20do%20about%20them-3.pdf] (30.04.2014)

8. H. Frank Cervone. Project risk management. 2006, Information Technology Division, Northwestern University Library, Evanston, Illinois, USA. [http://www.emeraldinsight.com/journals.htm?articleid=1580860] (29.04.2014)

9. Infosüsteemide Kolmeastmeline Etalonturbe Süsteem (ISKE). 2014. [https://www.ria.ee/iske/] (29.04.2014)

10. Infosüsteemide Kolmeastmeline Etalonturbe Süsteem (ISKE). Rakendusjuhendi kataloog. 2014. [https://www.ria.ee/public/ISKE/iske_rakendusjuhend_7_00.pdf] (29.04.2014)

11. Infosüsteemide Kolmeastmeline Etalonturbe Süsteem (ISKE). Meetmete kataloog ver. 7.00, RIA. 2014. [https://www.ria.ee/public/ISKE/ISKE_meetmed_7_00.ods] (29.04.2014)

12. Infosüsteemide Kolmeastmeline Etalonturbe Süsteem (ISKE). Ohtude kataloog ver. 7.00. 2014. [https://www.ria.ee/public/ISKE/ISKE_ohtude_kataloog_ver_7.pdf] (29.04.2014)

13. Infosüsteemide Kolmeastmeline Etalonturbe Süsteem (ISKE) juhendid ja materjalid: ISKE rakendusjuhend, RIA. 2014. [https://www.ria.ee/iske-dokumentatsioon/] (29.04.2014)

14. Infosüsteemide turvameetmete süsteemi kehtestamine (2004) – *Riigi Teataja* I 2004, 63, 443

15. International Organization for Standardization. ISO/IEC 20000-1:2011. 2011. [http://www.iso.org/iso/catalogue_detail?csnumber=51986] (29.04.2014)

16. Information Technology Infrastructure Library (ITIL) v3. 2007. [http://www.itil-officialsite.com/] (29.04.2014)

17. John Fraser and Betty J. Simkins. Enterprise Risk Management: Today's Leading Research and Best Practices for Tomorrow's Executives. 2010. [http://wafaa-sherif.com/new/ar/wp-content/uploads/2012/11/Enterprise%20Risk%20Management.pdf] (29.04.2014)

18. Keith, A. Facilities Risk Management. 1992. Facilities, Vol. 10, No. 4, p.14 – 18. [http://www.emeraldinsight.com/journals.htm?articleid=843888] (30.04.2014)

19. Kendrick, T. Identifying and Managing Project Risk, American Management Association, 2003, New York, NY. [http://books.google.ee/books/about/Identifying_and_Managing_Project_Risk.html?id=I_QpIKTMkS4C&redir_esc=y] (30.04.2014)

20. Laks, K. (2013) ISKE rakendamine maavalitsuses: bakalaureusetöö. Tallinna Tehnikaülikool, Tallinn.

21. Lansdowne, Z.F. „Risk matrix: an approach for prioritizing risks and tracking risk mitigation progress“. 1999. Proceedings of the 30th Annual Project Management Institute, Philadelphia, PA, October 10-16.

22. Projects in Controlled Environments, version 2 (Prince2), 3rd Edition. 2002. [http://www.slideshare.net/spouf/prince2-manual-3rd-edition-2002] (29.04.2014)

23. Riigi Infosüsteemi Amet (RIA). CERT-EE kokkuvõte: hajusad ummistusründed, võltsitud saatjaga e-kirjad ning näotustamised 1.–7.novembril 2013 aka #OpIndependence, RIA, 2013. [https://www.ria.ee/public/CERT/opindependence.pdf] (29.04.2014)

24. Riigi Infosüsteemi Amet (RIA). CERT-EE raport: #opindependence 1.–7. November, 2013. [https://www.ria.ee/cert-ee-raport-opindependence-17-novembril] (29.04.2014)

25. Riigi Infosüsteemi Haldussüsteem (RIHA). 2014. [https://riha.eesti.ee] (30.04.2014)

26. Tchankova, L. „Risk identification- basic stage in risk management“. 2002. Environmental Management and Health, Vol.13, No.3, p.290-297. MCB UP Limited.

27. The Information Systems Audit and Control Association (ISACA). 2011. [http://www.isaca.org/Journal/Past-Issues/2011/Volume-4/Pages/IT-Risks-Present-and-Future.aspx] (29.04.2014)

28. The Information Security Forum (ISF), 2014. [https://www.securityforum.org/] (29.04.2014)

29. The International Organization for Standardization. 2014. [http://www.iso.org] (29.04.2014)

30. The National Information Assurance Training and Education Center (NIATEC). 2014. [http://niatec.info/ViewPage.aspx?id=0] (29.04.2014)

31. Viira, T. ISKE: IT Grundschutz in Estonia. 2010. [https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Veranstaltungen/Grundschutz/3GS_Tag2010/ISKE.pdf?__blob=publicationFile] (20.04.2014)

32. Tchankova, L. „Risk identification- basic stage in risk management“. 2002. Environmental Management and Health, Vol.13, No.3, p.290-297. MCB UP Limited.